MANDIANT®

A FireEye™ Company

M Trends®

Beyond the Breach

CONTENTS

INTRODUCTION

Cyber security has gone mainstream. It is hard to overstate how quickly cyber security has gone from a niche IT issue to a consumer issue and boardroom priority. Everyone now knows what seasoned security professionals have long been aware of: **there is no such thing as perfect security**. Security breaches are inevitable, because determined threat actors will always find a way through the gap.

Over the past year, Mandiant has seen companies make modest improvements in their ability to attack the security gap. On the positive side, organizations are discovering compromises more quickly. In 2013, the median number of days attackers were present on a victim network before they were discovered was 229 days, down from 243 days in 2012. On the other hand, organizations still have difficulty detecting when they've been breached. In 2013, only 33% of the organizations to which Mandiant responded had discovered the intrusion themselves, versus 37% of the organizations we helped in 2012.

One thing that has changed dramatically, however, is the willingness of victim organizations and policymakers to speak more openly about the breaches they experience. *The New York Times* and other media organizations have published stories about their own incidents. President Obama addressed concerns about cyber threats in his annual State of the Union address. Add to that the proliferation of large-scale retail intrusions, and it is a rare individual who has not experienced the consequences of a security breach — either through the theft of their credit card data or credentials to a consumer website.

In this year's M-Trends, we provide you with Mandiant's perspective on the evolving threat landscape. Our insights and analysis are drawn directly from our experience responding to security incidents with hundreds of clients in more than 30 industry sectors. In addition, we track a variety of publicly discussed actors and indicators, and contextualize our analysis where relevant.

One conclusion is inescapable: the list of potential targets has increased, and the playing field has grown. Cyber threat actors are expanding the uses of computer network exploitation to fulfill an array of objectives, from the economic to the political. Threat actors are not only interested in seizing the corporate crown jewels but are also looking for ways to publicize their views, cause physical destruction, and influence global decision makers.

Private organizations have increasingly become collateral damage in political conflicts. With no diplomatic solution in sight, the ability to detect and respond to attacks has never been more important.
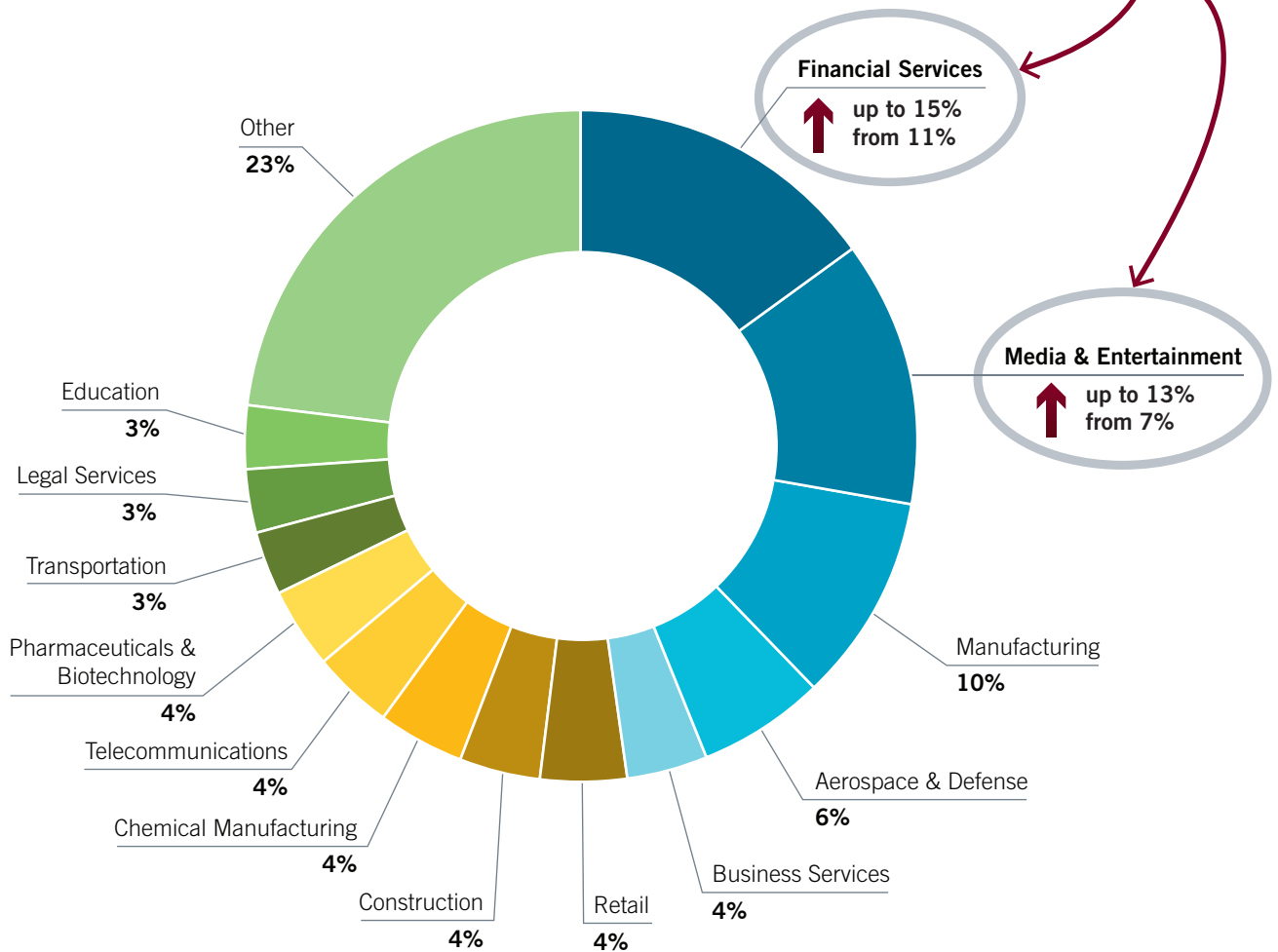
VICTIMS BY THE NUMBERS

Cyber threat actors continued to target a diverse array of industries. While organizations are detecting compromises two weeks sooner than they did a year ago, they are less likely to discover a breach on their own compared to a year ago.
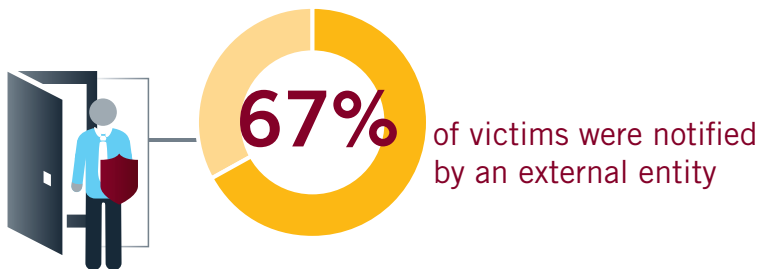
Industries Targeted by Cyber Threat Actors

In 2013 Mandiant noted an increase in threat actor activity in two key industries.

Financial Services
up to 15%
from 11%

Media & Entertainment
up to 13%
from 7%

Other
23%

Education
3%

Legal Services
3%

Transportation
3%

Pharmaceuticals & Biotechnology
4%

Telecommunications
4%

Chemical Manufacturing
4%

Construction
4%

Retail
4%

Business Services
4%

Aerospace & Defense
6%

Manufacturing
10%

How Compromises Are Detected

33% of victims discovered the breach internally

↓ **Down from 37% in 2012**

67% of victims were notified by an external entity
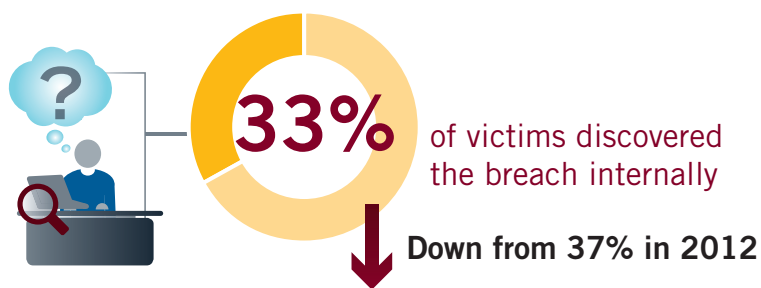
Time from Earliest Evidence of Compromise to Discovery of Compromise

229 median number of days that threat groups were present on a victim's network before detection

↓ **14 days less than 2012**

Longest Presence: 2,287 days

Phishing Email Trends

44% of observed phishing emails were IT related, often attempting to impersonate the targeted company's IT department

93% of phishing emails were sent on weekdays

Mon
Tue
Wed
Thur
Fri
Sat
Sun
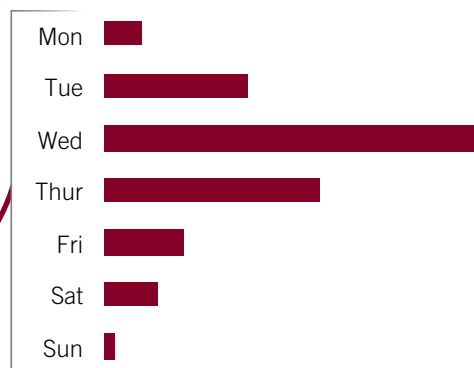
Across the Cyber Threat Landscape

	NUISANCE	**DATA THEFT**	**CYBER CRIME**	**HACKTIVISM**	**NETWORK ATTACK**
Objective	Access & Propagation	Economic, Political Advantage	Financial Gain	Defamation, Press & Policy	Escalation, Destruction
Example	Botnets & Spam	Intellectual Property Theft	Credit Card Theft	Website Defacements	Destroy Critical Infrastructure
Targeted	✗	✓	✓	✓	✓
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict Driven

COLLATERAL DAMAGE: THE SYRIAN ELECTRONIC ARMY STEALS HEADLINES, LITERALLY

Over the past year, political conflicts between nations spawned cyber attacks that hit the private sector. Mandiant responded to an increased number of incidents where the Syrian Electronic Army (SEA) compromised external-facing websites and social media accounts of organizations with the primary motive of raising awareness for their political cause.

Mandiant's observations of SEA activity over the course of 2013 revealed that the group used two tactics to gain access to victim organizations: sending phishing emails from internal accounts and, starting in August 2013, compromising service providers as a way to target victim organizations.

Mandiant believes the SEA will continue to penetrate high-profile targets in an effort to increase publicity for the Syrian regime and demonstrate support for its embattled president, Bashar al-Assad. Although these SEA intrusions have resulted in little more than websites defaced with the SEA logo and images of Assad, they have nonetheless brought the group to the world's attention. More significantly, they have increased fear of cyber compromise among governments and corporations alike.

WHO IS THE SEA AND WHAT ARE THEIR MOTIVES?

Syrian President Bashar al-Assad spent the bulk of 2013 fighting to maintain control over the country. Meanwhile, the Syrian Electronic Army, a hacktivist group claiming ties to the Syrian regime, waged a parallel online campaign against Assad's detractors. Since its inception in 2011, the SEA has successfully infiltrated more than 40 organizations, primarily targeting the websites and social media accounts of major Western news agencies.

The motives behind the SEA's cyber activity appear to be aimed at gaining publicity and support for the embattled president by targeting perceived opponents of his regime and defacing their websites. The SEA has mainly targeted Western news organizations, in some cases for publishing articles the SEA perceived as biased against the controversial leader.

The SEA grew increasingly prominent throughout 2013, due to an increased number of intrusions and highly visible compromises of targeted organizations.

Publicly discussed SEA intrusions revealed how the group used phishing emails to harvest valid login credentials for targeted networks. Although Western news agencies remain the SEA's primary focus, August 2013 marked a distinct shift in the SEA's tactics as the group began attacking more service providers, including SocialFlow, Outbrain, Melbourne IT, and the Qatar Domains Registry.

Through its October intrusion into the Qatar Domains Registry, the SEA compromised both popular and official Qatar government sites, including Al Jazeera and the Ministry of Foreign Affairs. The SEA has continued to use phishing emails as a method of achieving an initial compromise.
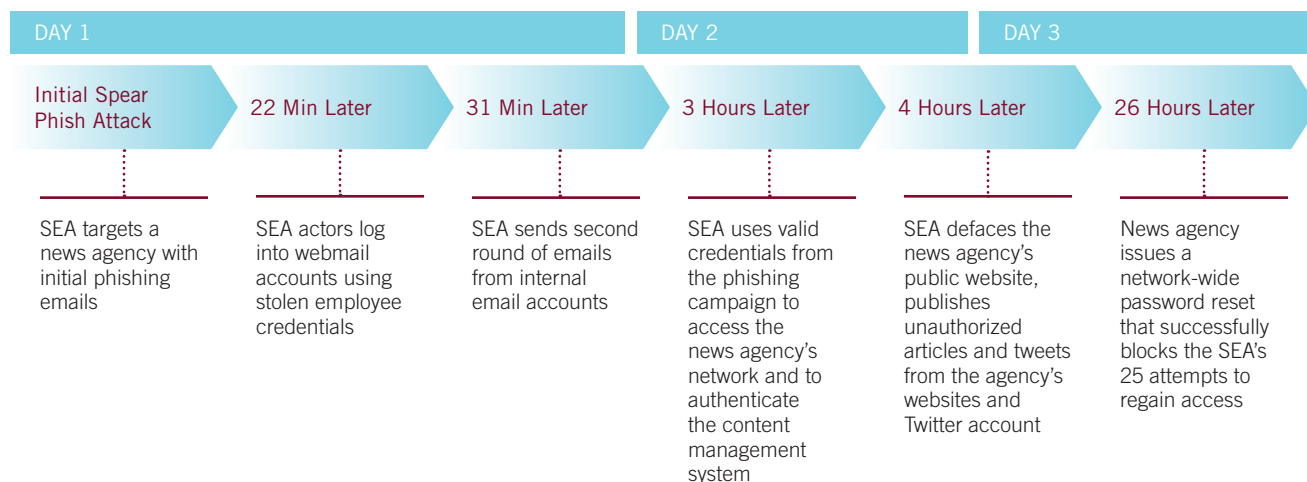
CASE STUDY: SEA COMPROMISES A NEWS AGENCY

In 2013, the SEA defaced a news agency's public website, and posted messages from the agency's Twitter accounts declaring that the "Syrian Electronic Army Was Here." The SEA utilized a rapid-fire phishing campaign that allowed the group to compromise multiple employee email accounts, a content management system (CMS), and the company's Twitter account. The phishing emails contained a link to a website that mimicked the news agency's external email login page. The website harvested the credentials of unsuspecting employees who entered their login information.

The SEA phishing emails were brief, and contained various news-oriented lures with visible URLs to apparent news stories. The visible URLs concealed

embedded links that pointed to a malicious site. The topics were consistent with breaking news that had occurred earlier that day. This tecÚique was consistent across all of the phishing emails.

After the initial phishing campaign, the SEA used the compromised credentials to access the news agency's externally available email system, which did not require two-factor authentication. Using the newly compromised accounts, the SEA began a secondary phishing campaign that initially targeted specific email distribution lists. The motive: obtain credentials to user accounts that had access to the main news site's CMS and the company's Twitter account. All told, the SEA sent thousands of phishing emails to a large number of employees over the span of three hours. Despite having

DAY 1			DAY 2	DAY 3
Initial Spear Phish Attack	22 Min Later	31 Min Later	3 Hours Later	4 Hours Later	26 Hours Later

SEA targets a news agency with initial phishing emails	SEA actors log into webmail accounts using stolen employee credentials	SEA sends second round of emails from internal email accounts	SEA uses valid credentials from the phishing campaign to access the news agency's network and to authenticate the content management system	SEA defaces the news agency's public website, publishes unauthorized articles and tweets from the agency's websites and Twitter account	News agency issues a network-wide password reset that successfully blocks the SEA's 25 attempts to regain access

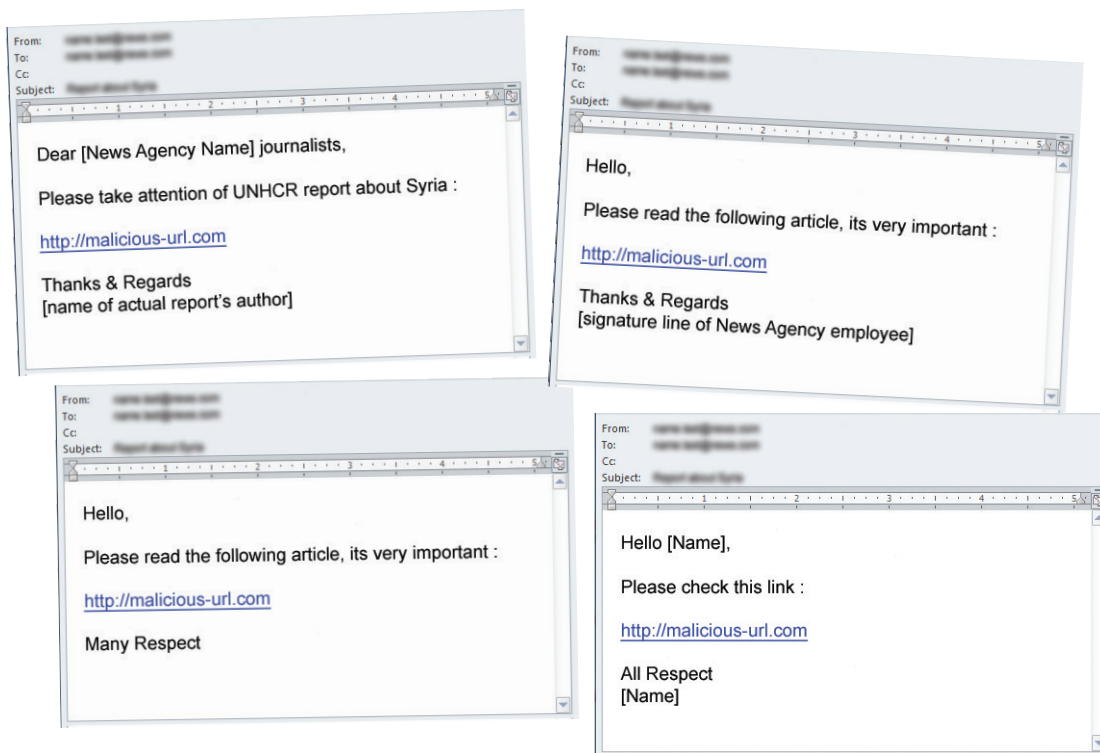a success rate of only 0.04%, the phishing emails still allowed the SEA to harvest the credentials necessary to access the targeted resources.

Within two hours of the first phishing email, the SEA obtained credentials for the news agency's main website. The company authenticated users through its LDAP infrastructure. Using the compromised credentials, the SEA leveraged this setup to authenticate directly to the CMS, which was external facing. From there, the SEA could deface existing news articles.

Three hours into the compromise, the SEA had gained access to a marketing email account that tied into the company's Twitter account. The issue here was that the Twitter account did not have the same password as any of the already compromised CMS accounts. To work around this obstacle, the SEA leveraged the marketing email account to reset the agency's Twitter password. At the time of the attack, Twitter did not offer two-factor authentication. With the newly reset Twitter passwords, the actor simply logged into Twitter and began sending unauthorized tweets.

Within two hours of the first phishing email, the SEA obtained credentials for the news agency's main website.

From:
To:
Cc:
Subject: Report about Syria

Dear [News Agency Name] journalists,

Please take attention of UNHCR report about Syria :

http://malicious-url.com

Thanks & Regards
[name of actual report's author]

From:
To:
Cc:
Subject: Report about Syria

Hello,

Please read the following article, its very important :

http://malicious-url.com

Thanks & Regards
[signature line of News Agency employee]

From:
To:
Cc:
Subject: Report about Syria

Hello,

Please read the following article, its very important :

http://malicious-url.com

Many Respect

From:
To:
Cc:
Subject: Report about Syria

Hello [Name],

Please check this link :

http://malicious-url.com

All Respect
[Name]

An Attack Timeline

Mandiant's investigation of the incident found that the SEA actors did not attempt to gain access to the news agency's underlying network. However, the SEA did make at least 25 failed attempts to authenticate to the external email instance with valid user credentials two days after the initial compromise. By then, the company had reset credentials for all compromised user accounts. Based on the level of account activity and timing, Mandiant believes the intrusion was the work of one or two SEA operatives.

THE TAKEAWAY   Going forward, organizations should be aware that they could become collateral damage in political conflicts that include a cyber component.
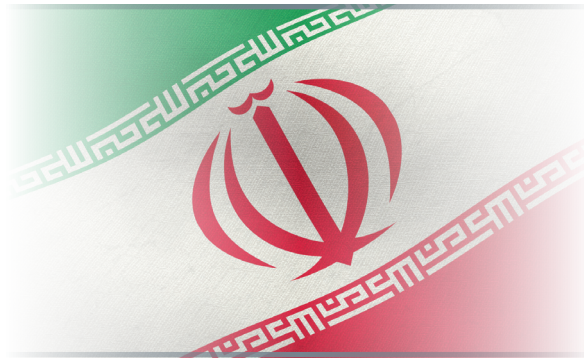
IRAN-BASED ACTIVITY

The majority of these suspected Iran-based actors targeted the energy sector. We have also seen these threat actors target the networks of several U.S. state government agencies.

Iran-based threat actors have also grown more active over the past year. Although Iran has long been considered a second-tier actor behind China and Russia, recent speculation has focused on Iran's interest in perpetrating offensive network attacks against critical infrastructure targets.[1] Iran is widely suspected to have been behind the August 2012 malware infections that targeted the networks of two energy companies, Saudi Aramco and the Qatar-based RasGas. Industry observers suggested that the Iranian government sponsored the attack after an Iranian nuclear facility was infected with the Stuxnet virus, widely believed to have been the work of the U.S. and Israel.

In an online posting, the group Izz ad-Din al-Qassam claimed responsibility for the 2012 DDOS attacks on U.S. banks, which they claimed were in retaliation for an anti-Islam video created by an individual in the U.S.[2] After the attacks, senior U.S. defense officials said they suspect that the group operates out of Iran.[3, 4]

We have not directly observed these Iran-based actors destroy or degrade our clients' networks. However, Mandiant has investigated multiple incidents of what we suspect is Iran-based network reconnaissance activity. The majority of these incidents targeted

the energy sector, although we have also seen these threat actors target the networks of several U.S. state government agencies.

Suspected Iran-Based Actors Target a State Government Agency

Employees at a state government office found evidence that someone had accessed multiple systems within their network without authorization. An internal IT department investigation found indications of data theft and unauthorized use of privileged credentials.

Mandiant's incident response investigation revealed that the threat actor:

» Maintained local administrative access

» Infected about a quarter of the systems with malware

» Transferred more than 150 gigabytes of data, which contained network diagrams, user passwords, and data from the network and system administrators' accounts (information consistent with network reconnaissance)

Mandiant has observed the following linguistic and tecÚical details over the course of our investigations involving suspected Iran-based activity:

» Use of a distributed denial-of-service (DDoS) tool in a client environment that was previously used in the 2012 attacks on U.S. banking institutions widely attributed to Iran-based actors

» Use of Web shells in which English command terms had been translated into Farsi

» Visits to Iranian-Farsi language blogs and hacker forums, while conducting intrusions from numerous non-Iranian IP addresses

» Multiple individuals who identify their location as Tehran and appear to actively create exploits that we have seen in intrusions into our clients' networks

Mandiant's observations of suspected Iranian actors have not provided any indication that they possess the range of tools or capabilities that are hallmarks of a capable, full-scope cyber actor. They rely on publicly available tools and capitalize solely on Web-based vulnerabilities — constraints that suggest these cyber actors have relatively limited capabilities.

Indications of these actors' limited capabilities include:

» Actors use only a small set of off-the-shelf tools and a few custom tools compiled from code found in other publicly available exploits. A more capable actor would likely utilize more effective, tailored tools such as a zero-day exploit or a custom-written exploit.

» Actors use IP addresses and domains for a year or more, even though public knowledge of these malicious addresses and domains hamper their success. This behavior indicates the actors lack either the incentive or resources to change infrastructure.

» Actors rarely attempt to obscure evidence of their activity, use anti-forensic tecÚiques, or return to the targeted environment after the victim has remediated the compromised systems. As a result, targets have been able to detect the intrusion.

» Actors primarily exploit Web-based vulnerabilities from public-facing websites, typically using one of two publicly available tools designed to exploit dated vulnerabilities.

To date, Mandiant has observed these threat actors compromising only networks that are vulnerable to publicly available tools. Mandiant has observed actors abandon a target after failing to compromise its network, suggesting that they were unable to adapt to the target's environment. The data that these actors stole lacked a discernible focus or demonstrated intent, leading us to believe that the mission's purpose was likely reconnaissance of the potential target's networks.

FIGURE 3: MANDIANT OBSERVATIONS OF SUSPECTED IRAN-BASED ACTIVITY V. CHINA-BASED THREAT GROUPS

	IRAN-BASED	CHINA-BASED
Industries Targeted	2 Energy, state government agencies	33 Most industry sectors
Victim Selection	Limited based on vulnerabilities	Varied and independent of vulnerabilities
Available Tools	Publicly available	Specially created, customized, publicly available
Date of Initial Mandiant Observation	2012	At least 2006
Detected by Victim	75%	33%
Average Time Spent in a Victim Organization	28 days	243 days
Re-Compromise After the Initial Security Incident	Not witnessed	40% of cases

Although we do not believe these suspected Iran-based actors are particularly capable now, nothing stands in the way of them testing and improving their capabilities. The U.S. and other nation-states' increasingly public discussions of their offensive cyber capabilities might very well encourage other interested actors to develop and test their own skills.

THE TAKEAWAY   Although the suspected Iran-based threat actors that Mandiant has observed appear to be less sophisticated than other threat actors, they pose an ever increasing threat due to Iran's historical hostility towards U.S. business and government interests. The outcome of diplomatic negotiations between Iran and Western powers over their nuclear program could play an important role in Iran-based threat actors' ultimate impact.
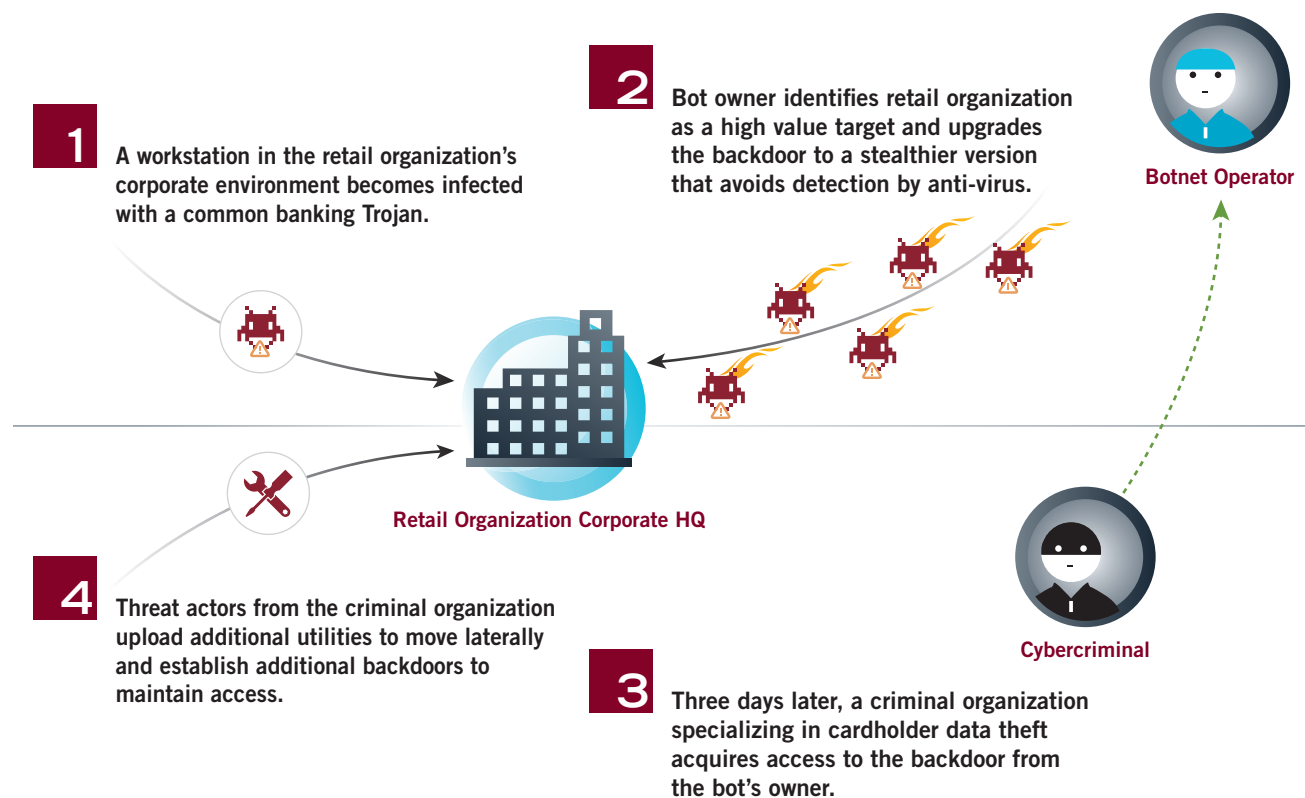
TURNING CREDIT INTO CASH

2013 was about more than political cyber operations. Mandiant responded to a growing number of financial theft incidents, many of which targeted the retail sector. In each of the incidents we investigated, a third party — typically one of the major banks or card brands — had notified the retailers of the compromise. But in some instances, federal law enforcement notified the victims. The threat actors maintained access to the compromised systems for up to six months.

The threat actors sought the track data that is stored in the magnetic strip of credit cards. There are two types of track data: track 1 and track 2. Track 1 data contains information such as the primary account number, expiration date, and cardholder name. Track 2 data contains the primary account number and expiration date, among other data. The threat actors targeted Windows-based point of sale (POS) terminals, controllers and servers in order to obtain this information which would allow them to counterfeit credit cards. Over the last ten years, Mandiant has responded to a number of retail intrusions, many of which were similarly executed. However, two significant differences characterized the incidents we responded to in 2013: the initial compromise vector and the method criminals used to extract the cardholder data from the remote POS systems.

In 2013, intrusions in the retail industry utilized a new initial compromise vector and criminals used new methods to extract cardholder data from remote point-of-sale (POS) systems.

1 A workstation in the retail organization's corporate environment becomes infected with a common banking Trojan.

2 Bot owner identifies retail organization as a high value target and upgrades the backdoor to a stealthier version that avoids detection by anti-virus.

Botnet Operator

Retail Organization Corporate HQ

Cybercriminal

4 Threat actors from the criminal organization upload additional utilities to move laterally and establish additional backdoors to maintain access.

3 Three days later, a criminal organization specializing in cardholder data theft acquires access to the backdoor from the bot's owner.

Initial Compromise Vector

Traditionally, cybercriminals targeted and exploited victim organizations' external Web applications. After compromising the Web applications, the threat actors would move laterally throughout the environment. In the incidents Mandiant responded to in 2013, the threat actors found much easier entry methods — they simply gained direct access to systems previously compromised and infected by a botnet herder. Although Mandiant does not have any conclusive proof of how these transactions occur, it seems likely that the attacker is purchasing access or trading for this access.

We identified a user's workstation in the retail victim's corporate environment that had become infected with a common banking Trojan, a commodity piece of malware that typically targets an individual's banking credentials. Less than 24 hours after the initial infection, the bot owner upgraded the backdoor to a stealthier version designed to avoid detection by anti-virus (AV) products.

Three days later, a criminal organization specializing in cardholder data theft accessed the modified Trojan to enter the victim's environment and upload additional utilities to move laterally. These actors also uploaded backdoors that they had acquired from the bot owner. These backdoors allowed the threat actors to maintain access to the victim's environment.

FIGURE 5: HOW THREAT ACTORS GAINED ACCESS TO RETAIL POS SYSTEMS

1 Cybercriminals leveraged minor misconfigurations in the infrastructure to identify systems with direct access to the POS systems.

2 A domain controller, which provided authentication for corporate offices and retail stores, provided the vulnerable pivot point.

3 The card-harvesting malware deployed on each register searched the process memory of the POS application for magnetic stripe data stored in ISO/IEC 7813 track 1 and track 2 formats.
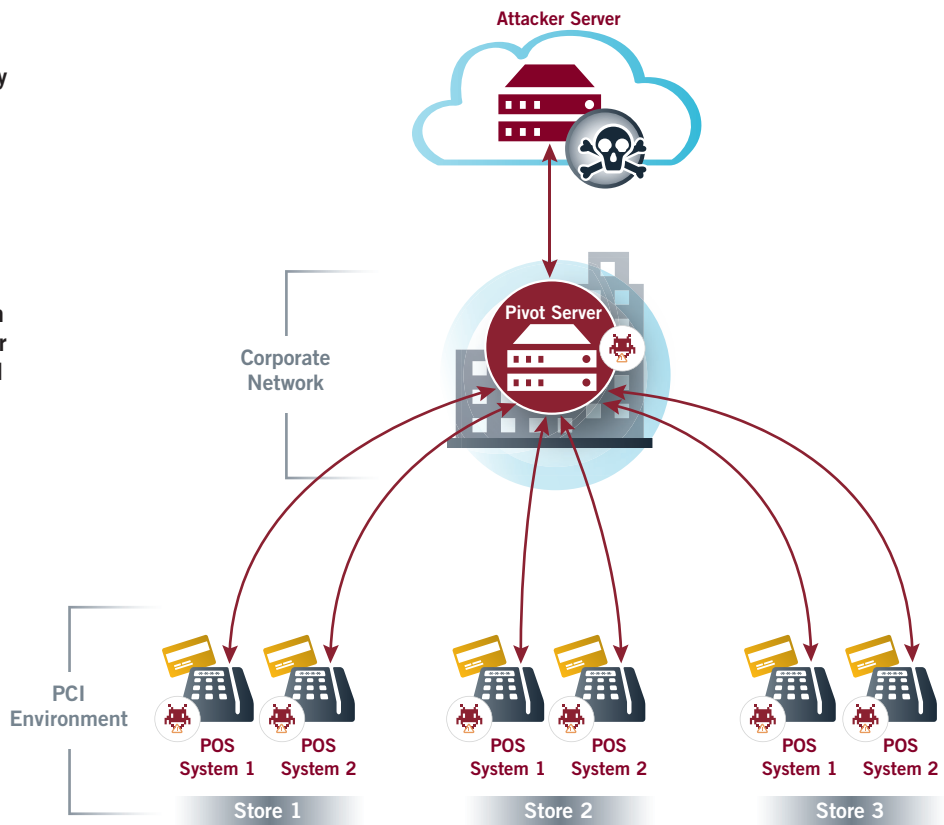
Deploying Data Collection Tool to Remote Registers

Each of the victims which Mandiant responded to in 2013 operated a PCI-compliant environment. In this instance, the threat actors leveraged minor misconfigurations in the infrastructure to identify systems with direct access to the POS systems. A domain controller, which provided authentication for corporate offices and retail stores, provided the vulnerable pivot point.

The threat actors used compromised domain administrator credentials to execute a Windows batch script on the domain controller server and deploy card-harvesting malware. In one instance, the malware infected more than 1000 registers running POS software on Microsoft® Windows® XP systems in hundreds of stores.

Obtaining the Cardholder Data

The card-harvesting malware deployed on each register searched the process memory of the POS application for magnetic strip data stored in ISO/IEC 7813 track 1 and track 2 formats. The threat actors leveraged Windows scheduled tasks to execute the malware once an hour during the retailer's business hours. The

RECOMMENDATIONS FOR IMMEDIATE ACTION

Instances of cybercrime targeting U.S. retailers are escalating, in part, because chip and PIN tecÚology aimed at reducing credit card fraud has not yet been broadly adopted in the United States. This switch to a more secure credit card tecÚology is imminent. But in the meantime, merchants can take steps now to enhance their own security posture. We recommend the following:

» **Implement strict network segmentation of the PCI environment:** Segment any system that handles cardholder data from the rest of the corporate environment. Require two-factor authentication for access to the PCI environment.

» **Manage privileged accounts:** Each system in the PCI environment should have its own unique local administrator password. Employ the principle of "least privilege" to all account and group permissions, including the service accounts.

» **Encrypt cardholder data:** Consider a POS solution with end-to-end asymmetric encryption, starting at the PIN pad reader.

» **Secure endpoints:** Ensure that all critical systems in the environment implement application whitelisting. Patch all third-party applications and operating systems. Install an endpoint threat detection and response solution. Consider implementing a file monitoring solution that tracks when files have been created on a system.

» **Actively monitor:** Monitor the PCI environment regularly for abnormal activity, such as suspicious logons, creation of unexpected files, or unusual traffic flow.

Tip: In the majority of Mandiant's investigations, cybercriminals used Windows scheduled tasks during the compromise. You can identify early signs that a threat actor may be in your environment by collecting scheduled tasks from all systems and looking for suspicious activity.

malware extracted the data, encoded it, and stored it in a temporary database table on the register.

From the compromised system at the corporate office, the threat actors used the Microsoft osql.exe utility to query the temporary SQL databases created on the registers. The results were written to a flat file on the pivot machine and compressed using the 7-zip archive utility. The zipped archive was then uploaded to a public file transfer website.

This method of storing the stolen data in a temporary database before extracting it from the remote machines using a SQL query is an interesting approach. We have seen other cases where the data collection malware outputs directly to a file and/or automatically transfers the data to an external FTP site.

THE TAKEAWAY   Systems that store cardholder data are large, lucrative targets. Cybercriminals will innovate and make substantial investments in new tools and tactics to steal card data in large quantities. We expect they will reuse these tactics across as many victim organizations as possible — often during high-traffic periods such as the holiday shopping season.
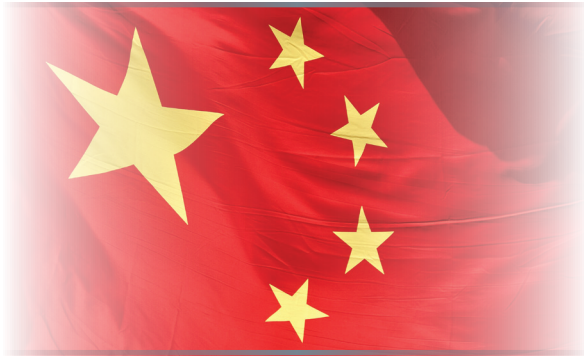
DATA THEFT: TAKE EVERYTHING BUT THE KITCHEN SINK

When Mandiant responds to an incident, the first question clients often ask is "why am I a target?" That's often followed by "I don't have anything that anyone would want." Our answer, borne out through many investigations over the past few years, is increasingly, "yes, you do!" The Chinese government is expanding the scope of its cyber operations, and China-based advanced threat actors are keen to acquire data about how businesses operate — not just about how they make their products.

We have written in past M-Trends reports that China-based threat actors have expanded their targeting well beyond the defense industrial base. Across numerous industries, we've increasingly observed the Chinese government conduct expansive intrusion campaigns to obtain information to support state-owned enterprises. This translates into data theft that goes far beyond the core intellectual property of a company, to include information about how these businesses work and how executives and key figures make decisions.

Manufacturer

A power systems manufacturer suffered a network compromise resulting in the loss of data relating to **manufacturing optimization processes**. Threat actors stole the contents of **email accounts of project managers** working in the company's technology and development division.

Media Organization

A media company had **financial records, calendar items, research files, e-mails** and **address book information stolen from high-level executives and journalists** reporting exclusively on China.

Energy Company

An energy company, **whose executives and managers had their email accounts compromised**, experienced data theft which included **information on a joint venture** with a regional Chinese government for a clean energy project.

NGO

A NGO had hundreds of files including **emails, programs and initiatives, strategic plans and goals, human resource records, grant information,** and **meeting minutes** stolen as a result of compromise.

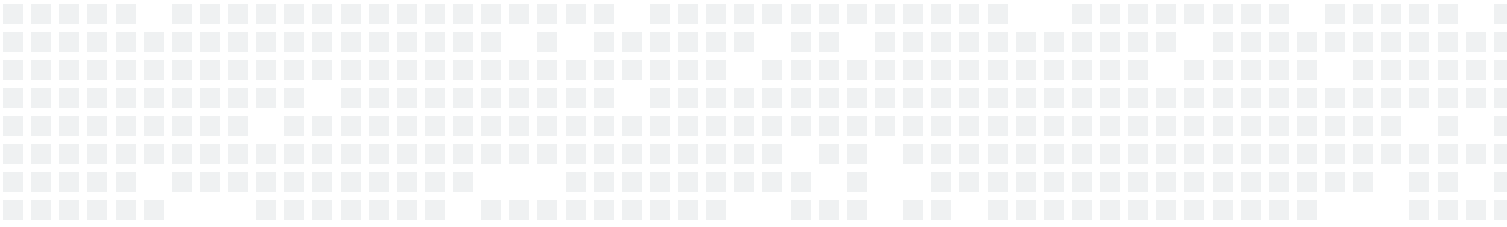| WHAT MAKES THE HEADLINES...	AND WHAT DOESN'T:
Compromised U.S. DoD weapons systems:[5]	China-based APT data theft of a broader nature:
» PAC-3	» Executive emails
» F-35	» Business processes
» THAAD	» Negotiations plans
» Navy's Aegis ballistic-missile defense system	» Budgetary information
» F/A-18	» Organizational charts
» V-22 Osprey	» Meeting minutes
» Black Hawk helicopter	» Human resources records
» Littoral combat ship	» Programs & initiatives
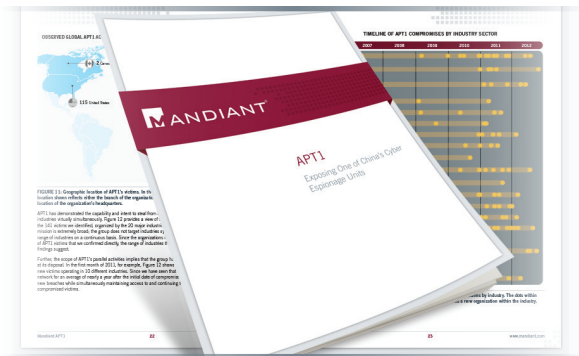
ONE YEAR AFTER THE APT1 REPORT: WHAT DIFFERENCE DOES A YEAR MAKE?

Mandiant's release of the APT1 report in February 2013 provided a unique opportunity to observe whether revelations of China's state-sponsored cyber activity could spur a diplomatic solution to the problem of nation-state cyber espionage on behalf of private sector entities. Could this raise the discourse to a presidential level and achieve tangible progress? Within a short period of time we had our answer: no.

January 2013 marked the first large-scale public disclosure that an advanced persistent threat (APT) group with suspected ties to the People's Republic of China (PRC) had compromised a key U.S. media company: *The New York Times*. In a front-page article released on January 30, 2013, the *Times* revealed that a China-based cyber threat group, known as APT12, had compromised its networks over the course of the past four months.[6] The article prompted a defiant response from the PRC, which stated "Chinese laws prohibit any action including hacking that damages Internet security," and added, "to accuse the Chinese military of launching cyber attacks without solid proof is unprofessional and baseless."[7]

Defining "Activity":
We based our observations of APT1 and APT12's activity on active command-and-control (C2) sessions. A cyber threat actor communicates with malware in the victim's network to conduct a network operation. C2 sessions show that an operator is actively engaging the network.

No sooner had the PRC dismissed the *Times'* story than Mandiant released the APT1 report, providing evidence linking the China-based cyber threat group to the PRC — specifically to Unit 61398 of the People's Liberation Army.[8] The PRC once again denied involvement, and was quick to describe the APT1 report as "amateurish" and "full of loopholes."[9]

Yet Mandiant's continued observations of APT1 and APT12 activity, measured by command and control (C2) sessions, revealed a different response behind the scenes, suggesting a possible acknowledgement that both groups had been exposed.

Based on comparisons between APT1 and APT12 activity during 2013 and the previous three years, Mandiant believes that these threat groups responded to their public exposure in two ways. First, both groups delayed their return to normal operations following the end of the Chinese New Year holidays in February. Second, both groups quickly shifted their operational infrastructure to continue their activities.

Despite the recent accusations and subsequent international attention, APT1 and APT12's reactions indicate a PRC interest in both obscuring and continuing its data theft. This suggests the PRC believes the benefits of its cyber espionage campaigns outweigh the potential costs of an international backlash.

APT1 AND APT12 PAUSE OPERATIONS

Mandiant observed significantly longer periods of inactivity for both APT1 and APT12 following *The New York Times* article and APT1 report when compared to both groups' baseline activity over the previous three years. APT12 briefly resumed operations five days after its exposure in *The New York Times* article, but did not return to consistent intrusion activity until 81 days later. Even then, APT12 waited until roughly 150 days after the article's release to resume pre-disclosure levels of activity. Figure 8 shows observed activities from January to September 2013 (red line) compared to average observed activities seen between 2011 and 2012 (blue line).

APT1 had similarly longer periods of inactivity after its exposure in Mandiant's report. Mandiant's release of the APT1 report coincided with the end of Golden Week, a seven-day government holiday that follows Chinese New Year. APT1 was inactive for 41 days longer than normal following Golden Week and the release of Mandiant's report compared to patterns of activity from 2010–2012.

When APT1 did become active again, it operated at lower-than-normal levels before returning to consistent intrusion activity nearly 160 days after its exposure. Figure 7 shows APT1 activity from January to September 2013 (red line), overlaid on the average observed activities seen between 2010 and 2012 (blue line).

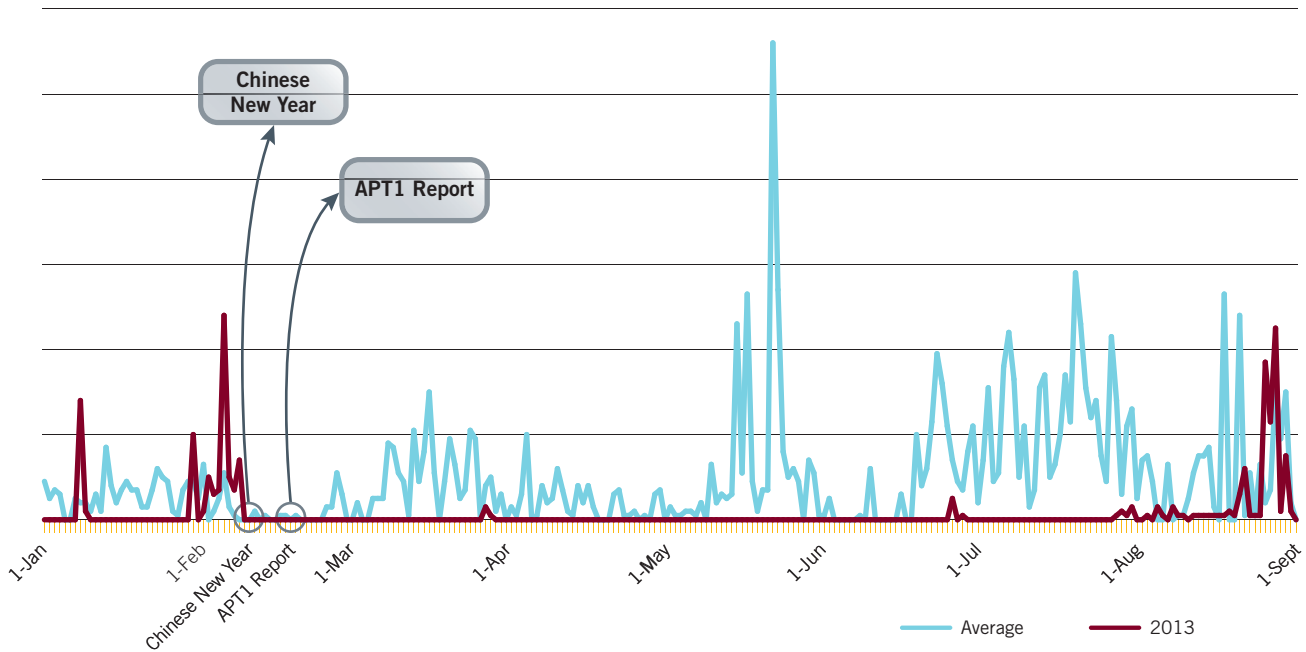**FIGURE 7:** NUMBER OF APT1'S 2013 C2 SESSIONS COMPARED TO BASELINE ACTIVITY FROM 2010–12

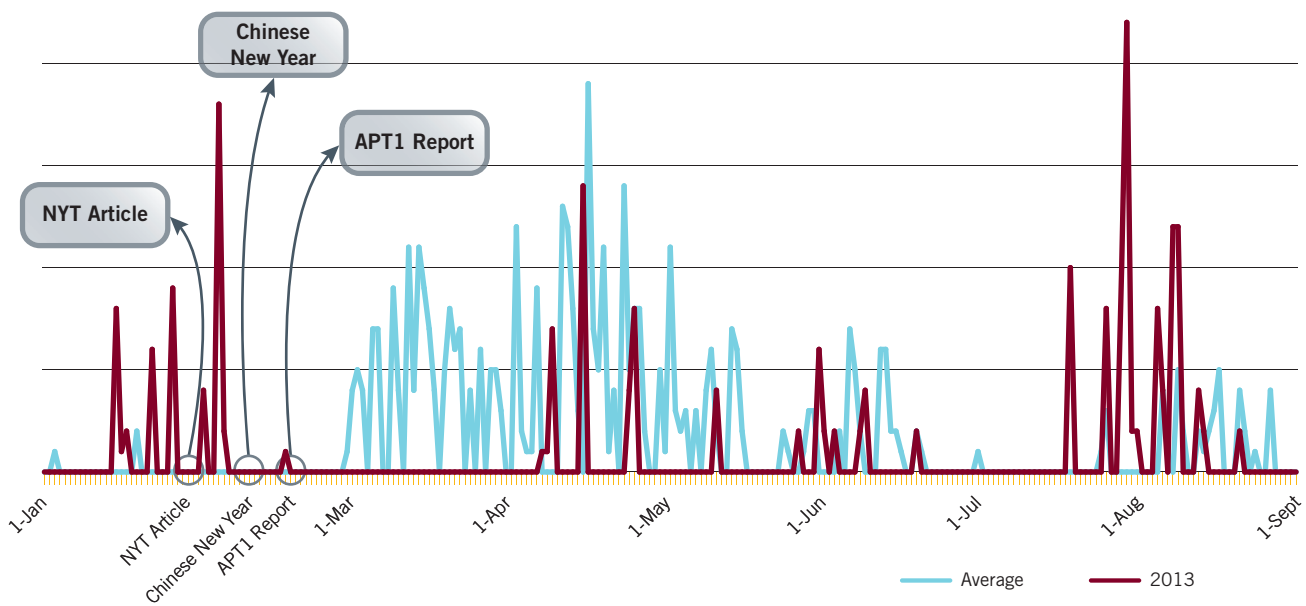**FIGURE 8:** NUMBER OF APT12'S 2013 C2 SESSIONS COMPARED TO BASELINE ACTIVITY FROM 2011 AND 2012
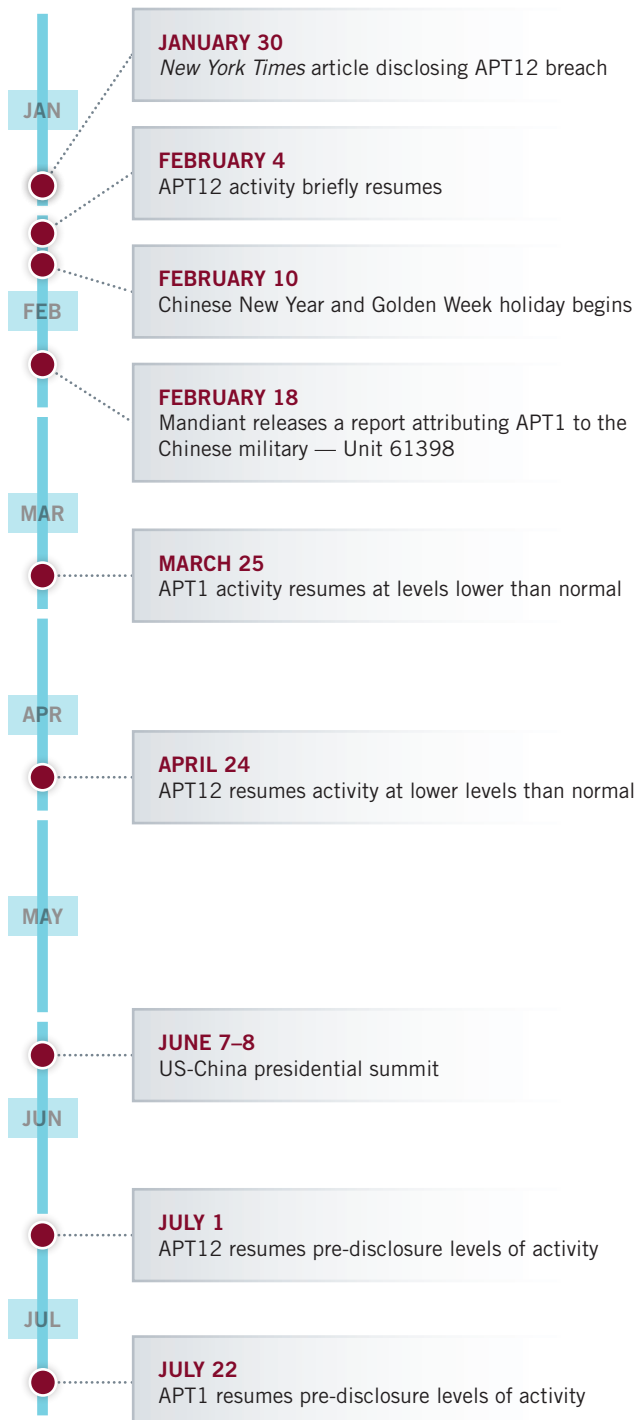
FIGURE 9: 2013 TIMELINE OF EVENTS — APT1 AND APT12

JAN

JANUARY 30
New York Times article disclosing APT12 breach

FEBRUARY 4
APT12 activity briefly resumes

FEB

FEBRUARY 10
Chinese New Year and Golden Week holiday begins

FEBRUARY 18
Mandiant releases a report attributing APT1 to the Chinese military — Unit 61398

MAR

MARCH 25
APT1 activity resumes at levels lower than normal

APR

APRIL 24
APT12 resumes activity at lower levels than normal

MAY

JUNE 7–8
US-China presidential summit

JUN

JULY 1
APT12 resumes pre-disclosure levels of activity

JUL

JULY 22
APT1 resumes pre-disclosure levels of activity

Both APT1 and APT12's prolonged periods of inactivity in response to the public exposures may have been the PRC's attempt to assess any political damage following the publications and to reorganize its cyber operations to better hide its activities.

APT1 AND APT12 CHANGED OPERATIONAL INFRASTRUCTURE

Mandiant's observations of APT1 and APT12 showed that both groups changed infrastructure following the disclosures in *The New York Times* article and the Mandiant report.

The APT1 report included more than 3,000 indicators, including domain names, IP addresses, encryption certificates, and MD5 malware hashes. After releasing the report, Mandiant observed APT1 change a large amount of its operational architecture, replacing what had been exposed in the APT1 report.

Although the *Times'* article had not exposed APT12's operational infrastructure, Mandiant observed the group also making changes in its operational architecture, replacing any infrastructure that researchers may have exposed following the article's release.[10, 11] Mandiant believes APT1 and APT12's infrastructure changes were a direct reaction to their public exposure, as both groups changed that which had been revealed, while keeping other infrastructure in place. We believe APT1 and APT12 changed their exposed operational architecture in an attempt to obscure their future data theft operations.

APT1 Changes to IP Addresses Used by One Malware Family
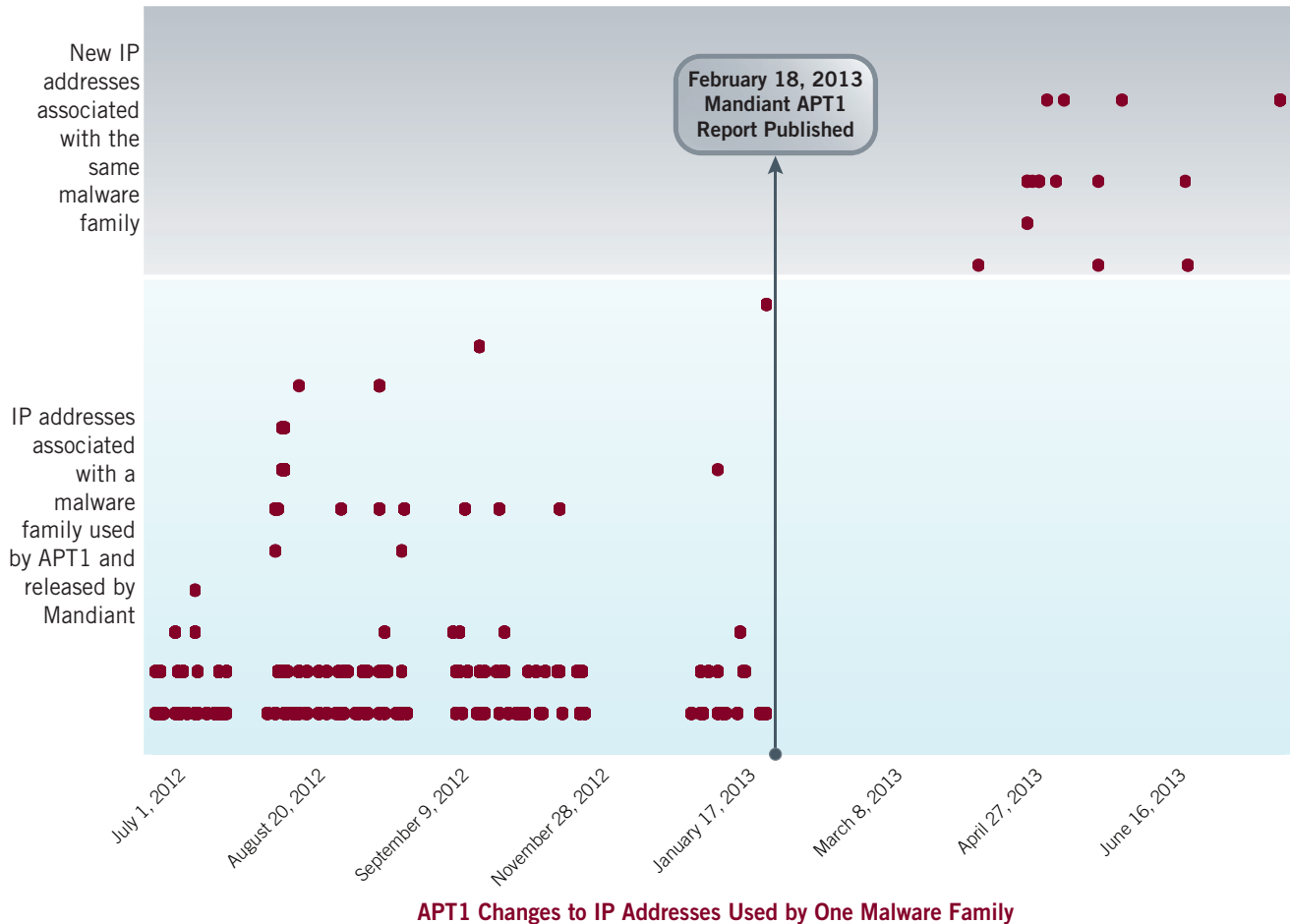
CAN'T STOP, (PROBABLY) WON'T STOP

APT1 and APT12's reactions to their public exposure suggest that the PRC, despite publicly denying engaging in state-sponsored data theft, is unwilling to permanently cease its use of intrusive cyber operations. The PRC's continued reliance on cyber operations has the potential to jeopardize China's future relationship with the U.S. President Obama made China's cyber espionage the primary focus of the June 2013 U.S.-China presidential summit, bringing high-level attention to an issue national security adviser Tom Donilon described as the "key to the future" of the U.S.-China relationship.[12] However, Mandiant's recent observations of China-based APT activity indicate that the PRC has no intention of abandoning its cyber campaigns, despite the Obama administration's specific warnings that China's continued cyber espionage "was going to be [a] very difficult problem in the economic relationship" between the two countries.[13]

CONCLUSION

Over the last year, we saw a dramatic change in the amount of public discussion regarding breaches. Victim organizations have become more willing to speak openly about the intrusions they suffer, and policymakers are voicing their own concerns at both the national and international level. But the increased discussion and awareness of security breaches has done little to change the current reality: security breaches are inevitable.

One trend is clear: while organizations are more aware of cyber threats than ever, threat actors have also evolved to encompass a larger scope of targets and are using a broader skillset to achieve their goals. In this report, we have discussed recent cases that involved hacktivists, emerging actors, cybercriminals, and nation-state groups targeting media organizations, government agencies, companies and nonprofits. While targeted organizations have improved their network defenses, the typical attacker still compromises and navigates networks undetected for more than eight months. Meanwhile, other actors, such as hacktivists, are able to project their message and impact an organization with simple tactics and a bit of determination.

But this evolving threat landscape, while complicated, need not be discouraging. To attack the security gap, organizations need smart people, visibility into their networks, endpoints, and logs. Organizations also need actionable threat intelligence that identifies malicious activity faster. When the inevitable happens, the speed and manner in which you respond is critical. Breaches are inevitable — how will you respond?

ENDNOTES

1   U.S. Congress: Subcommittee Hearing: Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure, 20 March 2013 http://homeland.house.gov/hearing/subcommittee-hearing-cyber-threats-china-russia-and-iran-protecting-american-critical

2   Perlroth, Nicole. Hardy, Quentin. "Bank Hacking was the Work of Iranians, Officials Say." *The New York Times*, The New York Times Company. 8 January 2013. Web. 19 Dec. 2013. http://www.nytimes.com/2013/01/09/tecÚology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0

3   Perlroth, Nicole. Hardy, Quentin. "Bank Hacking was the Work of Iranians, Officials Say." *The New York Times*, The New York Times Company. 8 January 2013. Web. 19 Dec. 2013. http://www.nytimes.com/2013/01/09/tecÚology/online-banking-attacks-were-work-of-iran-us-officials-say.html?_r=0

4   Gorman, Siobhan. "Iran Renews Internet Attacks on U.S. Banks." *The Wall Street Journal*, Dow Jones & Company. 17 Oct. 2012. Web. 19 Dec. 2013.

5   "Plans for More Than Two Dozen U.S. Weapons Systems — Including an F-35 Fighter — Have Been Stolen by Chinese Hackers, Claims Pentagon." *The Daily Mail*, Associated Newspapers, Ltd. 28 May 2013. Web. 12 Nov. 2013.

6   Perlroth, Nicole. "Hackers in China Attacked the Times for Last 4 Months." *The New York Times*, The New York Times Company. 30 January 2013. Web. 16 Dec. 2013.

7   Perlroth, Nicole. "Hackers in China Attacked the Times for Last 4 Months." *The New York Times*, The New York Times Company. 30 January 2013. Web. 16 Dec. 2013.

8   "APT1: Exposing One of China's Cyber Espionage Units." Mandiant. 18 February 2013. Web. 16 Dec. 2013.

9   "Chinese Media Slam Cyber-Hacking Report." Voice of America News, Voice of America. 21 February 2013. Web. 16 Dec. 2013.

10 Fireeye blog: http://www.fireeye.com/blog/tecÚical/malware-research/2013/02/an-encounter-with-trojan-nap.html

11 Trendmicro: "http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_ixeshe.pdf"

12 Neuman, Scott. "Chinese Cyber-Hacking Discussed at Obama-Xi Summit." The Two-Way, National Public Radio. 9 June, 2013. Web. 17 Dec. 2013.

13 Neuman, Scott. "Chinese Cyber-Hacking Discussed at Obama-Xi Summit." The Two-Way, National Public Radio. 9 June, 2013. Web. 17 Dec. 2013.

ABOUT MANDIANT®

Mandiant has driven threat actors out of the computer networks and endpoints of hundreds of clients across every major industry. We are the go-to company for the Fortune 500 and government agencies that want to defend against and respond to critical security incidents of all kinds.

The majority of advanced targeted operations proceed undetected and proliferate undefended. When intrusions are successful, Mandiant's unique combination of human intelligence and tecÚology leadership, combined with threat intelligence from FireEye, help organizations detect, respond to and contain them before the threat actors reach their objective. Our engineers and security consultants hold top government security clearances, have written 11 books, and are regularly quoted by leading media organizations. Mandiant is headquartered in Alexandria, VA, with offices in New York, Los Angeles and San Francisco.

To learn more about Mandiant visit www.mandiant.com, read our blog, M-Unition, follow us on Twitter @Mandiant or Facebook at www.facebook.com/mandiantcorp.

ABOUT FIREEYE™

FireEye helps organizations defend themselves against the newest generation of cyber attacks. The combination of FireEye's threat prevention platform, people and intelligence helps eliminate the consequences of security breaches by stopping attacks, communicating the risk, and equipping you to rapidly resolve incidents when they arise.