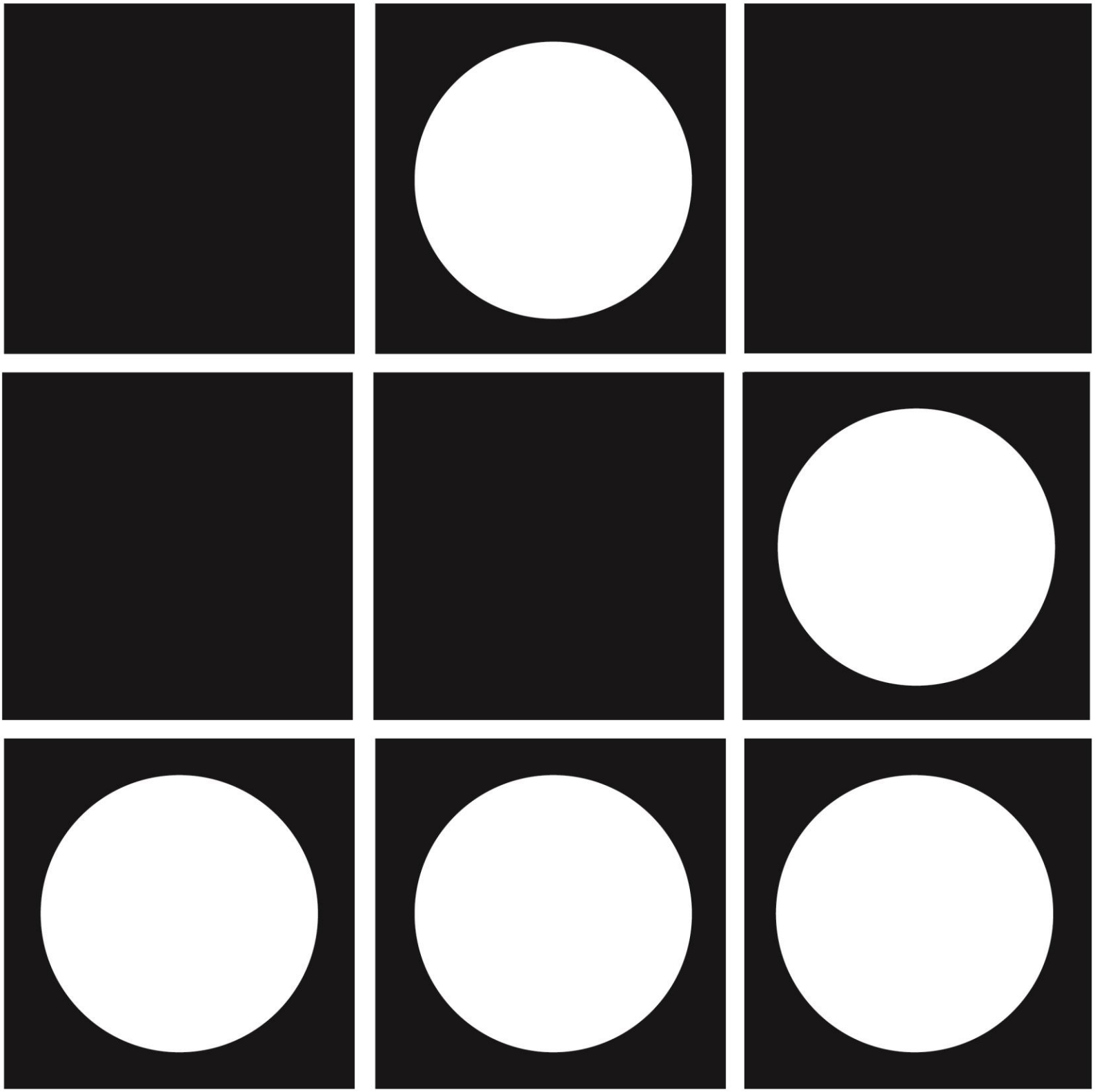
ICIT | Institute for Critical Infrastructure Technology

KNOW YOUR ENEMIES

A Primer on Advanced Persistent Threat Groups

NOVEMBER 2015



Know Your Enemies

A Primer on Advanced Persistent Threat Groups

November 2015

Authors:

James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)

Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)

Introduction

Every system connected to the internet in every home, organization, and government entity is relentlessly subject to the attempts of malicious actors to steal their data or exploit their system. Cyber-attacks are prevalent in the digital age because computers (including mobile devices) are ubiquitous in society, because identification of an attacker and attribution is difficult, and because judicial rulings for cyber-crimes are nebulous. Most cyber-attacks are prevented by basic security measures such as firewalls and antivirus applications. However, an elite percentile of the sea of cyber attackers is more persistent, more resourceful, and more sophisticated than the rest. These elite factions are known as Advanced Persistent Threats, and basic security measures are not enough to stop them from compromising some of the best-secured systems around the world.

Globally, at least a hundred advanced persistent threat groups are currently operational as criminal operations, mercenary groups, or nation-state sponsored divisions. Criminal operations typically target organizations or individuals for financial data or personal identifiable information for identity theft. Mercenary groups steal financial information or specific information from specific targets, as requested by their client. State sponsored groups may target organizations or governments to steal financial information, defense information, information that would grant a geopolitical economic or technological advantage, or any information that would be of use in intelligence or counterintelligence operations.

Nation state actors have been known to compromise enemy systems in order to plant malicious code that could enable the attacker to fully control the target systems or sabotage the systems altogether. While only limited application has been seen in the 2008 conflict between Russia and Georgia, the possibility of a joint cyber-physical war exists. An invading force can gain significant advantage over its enemy if it cripples their critical infrastructure prior to the attack.

Attribution of attacks is difficult. Researchers learn to think like attackers and to retrace the steps of a campaign. Security firms identify advanced persistent groups according to their tools, techniques, and characteristics. Advanced groups tend to develop and update their own sets of tools and malware. The keyboard language settings that remain in the code or the file names can reveal the attackers' nationality. Strings left in the code can reveal aspects of the development environment and the available resources. Who the group targets or does not target (especially in the case of nation state actors) can reveal the agenda of the adversary. The infrastructure, domain, and network of attackers can reveal their location, resources, and sophistication. Finally, the specific information stolen and whether that data is sold, used, or stored can also assist in profiling an adversary.

Cyber-attacks deal significant damage to nations and citizens alike in the form of breaches and compromised systems. Most of the time, the adversary is an unknown phantom menace and security professionals analyze forensic data to attribute the crime to a specific actor. This primer aims to pull the veil from prominent actors and to assist in attribution attempts. This primer offers an introductory view of some of the most prolific advanced persistent threat groups in recent history. It also intends to give a top level view of the threat landscape and attack process. This primer is not a sole source of attribution information. Old actors falter about as quickly as new, identified groups emerge. Further, new groups often develop from or mimic their predecessors. It would be erroneous to rely upon a static document for attribution purposes. This primer cannot provide the whole view of an actor. Each actor is an extremely complex group. Even security firms rarely possess complete knowledge of an active adversary. Different firms identify different portions of actors and refer to them with different names. Malware can be copied or purchased by a new adversary. The adversaries update their malware and exploit kits, along with their attack vectors in order to stay ahead of detection efforts. Finally, different organizations and governments evaluate and fear APT groups differently. As a result, this primer will not serve as a ranking system just as it does not serve as a comprehensive list of all attackers. Instead, the information below is offered to raise awareness about the groups that populate the cyber landscape. We have categorized these APT groups by country so that the reader can more easily identify the characteristic similarities of the attack components.

China:

The Elderwood Platform:

The Elderwood Platform is the name given to a set of zero-day exploits that is either used within a large organization or sold as a package to many attackers. The Elderwood platform was discovered by Symantec in 2009-2012, following the actor's 2009 compromise of Google with the Hydra (Aurora) Trojan. It is not clear whether Elderwood is a single criminal group that distributes its platform or if it is part of a major organization that distributes its platform to its subdivisions. In the former scenario, the Elderwood distributor may preferentially sell its platform to separate criminal entities at the same time. In most cases, the "buyers" receive the exploit around the same time. This could be an operational choice on behalf of the seller, a systematic choice (i.e. the "seller" sells once they find an exploit), or a procedure meant to obfuscate the activities of any one "buyer." In the latter scenario, Symantec theorizes that a parent organization may distribute the platform and it may task its

subdivisions with targeting particular industries or sectors. Each subgroup then utilizes their own infrastructure to stage the attacks using the shared platform.

Zero-day exploits are rare and valuable and the Elderwood platform relies upon zero-day exploits to compromise its victims. Somehow the Elderwood platform has consistently been updated with new zero-day exploits since 2009. In fact, no other actor has been able to obtain and utilize as many zero-day exploits as the actor behind the Elderwood platform. This suggests that either the actor behind the Elderwood platform has a highly sophisticated technical team that is capable of farming zero-day exploits or that Elderwood is funded by a criminal organization or state sponsor that possess significant resources. Unless the technical team that farms the exploits is paid an extremely high sum, neither theory explains why the exploits do not appear on underground markets until long after Elderwood has used the exploit.

A hybrid theory is possible. Perhaps the Elderwood group sells their platform to a third party for one reason or another, and that party then resells the platform to smaller groups. The hybrid model could explain how the Elderwood platform continues to utilize new and unique zero-day exploits because an exploit could be sold whenever the group feels that it has served its purpose and then they can purchase new exploits using the money received from selling the previous exploit to numerous other buyers. Alternately, perhaps a simpler solution exists. Zero-day exploits are juicy pieces of information. It is possible that Elderwood activity attracts the notice of other groups who watch the attacks and reverse engineer the exploits. The lower tier attackers would need inside knowledge of Elderwood activity and they would have to outpace cybersecurity response teams, else the exploits would be of little value.

In recent years, other notable campaigns have utilized the Elderwood platform or its exploits. Hidden Lynx used internet explorer exploits and its ZXshell backdoor in attacks against the defense industry. Vidgrab exploited internet explorer to install the vidgrab backdoor on systems belonging to Japanese users and it exploited Adobe flash to install the Jolob backdoor on systems belonging to Uyghur dissidents. Icefog exploited both Adobe Flash and Internet Explorer to install the Linfo and Hormesu backdoors respectively on systems in the manufacturing industry. Sakurel used multiple Internet Explorer exploits and an Adobe Flash exploit to compromise Aerospace engine manufacturer systems with the Sakurel Trojan.

The Elderwood platform is used against targets in a large number of sectors. Most frequently, the Elderwood platform is employed against organizations involved in defense, defense supply chain manufacturing, IT, and Human Rights. Organizations are attacked through watering hole attacks, spear phishing emails, and web exploits. Symantec believes that it is possible that manufacturers and tangential sector organizations and sites are compromised to target top tier primary targets. In this case, organizations in Manufacturing, Engineering, Electronic, Energy, Arms, Shipping or Aeronautics industries may be targeted as stepping stones

to compromise Defense organizations. Additionally, Software or Financial firms might be targeted so the attacker can compromise NGOs.

The Elderwood platform predominantly targets United States organizations. Firms in Canada, China, Hong Kong, and Australia have also been frequently targeted. Organizations based in Taiwan, United Kingdom, Switzerland, India, and Denmark have been sporadically targeted. Victims are targeted for information and intellectual property contained on their systems. The lack of theft of financial information complicates the actor profile because a mercenary distributor is less likely to steal nation-state information over financial information. One could argue that information is stolen with the Elderwood platform to assist in other breaches; however, a mercenary group would likely not be able to analyze information as rapidly as the Elderwood group has.

Between 2009 and 2014, the Elderwood platform has featured numerous Adobe Flash and Internet Explorer zero-day exploits. Adobe Flash and Internet Explorer are notoriously vulnerable applications. Typically, Adobe Flash, Internet Explorer, or both are present on a system. The attack platform also contains a document creation kit which enables the attacker to combine a clean document with a Trojan of their choice to create a malicious document. These documents are then used in spear phishing campaigns. The platform also contains a Shockwave Flash file that ensures that Trojans are downloaded onto target machines in the correct locations. The platform could contain information gathering tools such as keyloggers, automated domain name and account generators, and an information analysis platform.

Axiom:

The Axiom group is a Chinese, potentially state-sponsored, threat actor that compromises systems that contain information of value to advancing China's 12th Five Year Plan. Axiom was investigated in the October 2014 Operation SMN, a joint operation between private firms, led by Novetta which released information and led to the removal of Axiom malware from over 43,000 systems.

Since 2009, Axiom has been targeting networks in a broad range of sectors who possess confidential or classified information. Axiom campaigns share infrastructure, malware, or attack techniques with Operation Aurora (2009), the Elderwood Project (2009-2014), the VOHO campaign (2012), the Shell_Crew attacks on ColdFusion servers (2013), Operation Ephemeral Hydra (2013), Operation Snowman (2014), and 2014 attacks on American Middle Eastern Policy think tanks. Axiom could be connected to some of these other groups; however, it is more likely that Axiom advantageously adopts zero-day exploits or malware that are effective in other campaigns. It is possible that Axiom acquires its malware on deepnet or through underground trade.

Axiom is likely Chinese state sponsored, but there are no definitive links connecting it to the Third Department, which houses China's offensive threat groups Putter Panda and APT1. Axiom malware was configured to use simplified Chinese language settings and some of the filenames are in Chinese. Axiom is more sophisticated in its operations than the aforementioned Third Department groups. It utilizes different resources, and it may have a different mission than Third Department groups. Novetta hypothesizes that based on Axiom's domestic monitoring trends that it might be charged with domestic operations and targeting Chinese dissidents in other countries. Universities and research institutions in Hong Kong and mainland China have been targeted with Hikit malware for persistent operations. This could indicate state-sponsored concern over liberal academics and students.

Novetta has found that Axiom targets a wide variety of entities inside and outside governments. Axiom targets a wide variety of sectors, but it only targets specific entities in those sectors. Within Asian and Western governments, Axiom targets law enforcement, governmental records and communication agencies, environmental policy agencies, personnel management divisions, space and aerospace exploration and research entities, government auditing and internal affairs divisions. In the science and technology sectors, Axiom targets networks belonging to electronics and integrated circuitry manufacturers, networking equipment manufacturers, internet based service companies, software vendors, cloud computing companies, energy firms, meteorological service companies, telecommunications firms, and pharmaceutical companies. Additionally, Axiom has targeted journalism and media outlets, Human Rights NGOs, international law firms, international consulting and analysis firms, and high ranking United States academic institutions. Most of the target's organizations have been located in the United States, South Korea, Taiwan, Japan, and the European Union, with a majority of the breaches along the Eastern seaboard of the United States and Western Europe.

Axiom targeting coincides with interests reflected in China's 2006 and 2011 Five Year Plans, which push for advanced technology and advanced R&D efforts. As China shifts away from foreign technology, more organizations may be targeted by Axiom. The actor may target semiconductor and networking technology firms with offices in China because China wants to reduce its dependency on foreign technology. Western and Asian organizations may be targeted in intelligence and counterintelligence operations. Axiom targets NGOs concerned with international politics, environmental policy, pro-democracy movements, or human rights movements. In some instances, Axiom will target a satellite office and move laterally through the compromised network to the main office. Novetta theorizes that Axiom targets NGOs as a means of the Chinese ruling party keeping track of watchdog organizations and other groups who may publish claims that challenge the authority or "soft power" of the party. Targeting NGOs may also enable the party to suppress dissidents or intimidate whistleblowers.

Novetta believes that Axiom has a six stage victim lifecycle that uses a different team for each stage of the attack. This indicates large scale organization and coordination. Initially, the target is identified and the actor conducts reconnaissance. Then the system is compromised, confirmed to be a valuable target, and the network is surveyed. The actor laterally moves through the network and creates additional footholds. Compromised C2 infrastructure is connected to the victim network. Finally, valuable data is identified and exfiltrated.

Axiom initially compromises systems through web based attacks, targeted attacks against public facing infrastructure, zero-day exploits, watering hole attacks and phishing emails. Once a system is compromised, Axiom spends a few days determining whether it is valuable. If it is determined to contain useful information, then the group installs persistent malware platforms. Otherwise, the group tries to move laterally through the network to locate more valuable systems. Axiom has proven capable of compromising large pools of machines and sifting through them in hours or days to find the valuable ones. This indicates dedicated resources, possibly a dedicated targeting team and a deterministic set of criteria. After the initial compromise, Axiom begins reconnaissance to identify where they are in the target network and to identify any changes that have been made to the network. Axiom then escalates privileges using previously compromised administrative accounts, local exploits, or remote exploits as demonstrated in ZoxRPC malware. Then, over the course of minutes or months, they try to dump the latest user credentials and exfiltrate the data. Once inside the network, Axiom can also exploit Remote Desktop Protocol or exploit vulnerabilities in the custom tools designed by the organization itself. This allows Axiom to “fly under the radar” and not alert antivirus or IDS systems to the compromise.

As the campaign continues, Axiom may install additional families of malware as a mechanism of remaining in the system even if one malware is discovered by the target. Compromised systems have featured up to four layers of malware ranging from extremely common (Poison Ivy, Gh0st, ZXshell) to focused tools used by threat groups (Derusbi, Fexel) to custom Axiom malware (ZoxPNG/ZoxRPC, Hikit). Axiom routes its activity through compromised proxy infrastructure in the United States, South Korea, Taiwan, Hong Kong, and Japan to try to disguise its traffic as legitimate to casual observation.

Novetta observes that the Hikit malware is unique to Axiom and is only used on high value targets at the height of the victim’s operational lifecycle. Of the 43,000 compromised systems discovered in Operation SMN, only 180 systems were infected with the Hikit malware. Hikit is a late stage persistence and data exfiltration tool that is capable of uploading and downloading files, generating a remote shell, tunneling into the network, and connecting to other infected machines to generate a secondary network.

Hidden Lynx / Aurora:

Hidden Lynx is a professional "hackers for hire" group that has operated since 2009 and that is believed to be based out of China. Hidden Lynx steals specific information from select targets from a wide range of sectors and governments. The 50-100 member group has proven themselves capable of breaching some of the best defended systems in the world. The adversary can conduct multiple persistent campaigns concurrently against a variety of well defended targets. Hidden Lynx has been associated with 2010 Operation Aurora and the 2012 VOHO campaign.

In the past three years, Hidden Lynx has conducted hundreds of attacks against commercial organizations and governments across the globe. The sectors most targeted are the financial sector, the education sector, and government entities. Within the financial sector, investment banks and asset management agencies are the primary targets. In their 2013 report on the group, Symantec points out that "[t]he absence of certain types of financial institutions, such as those operating as commercial banks, clearly indicates that the attacks are focusing on specific areas." With less frequency, the group has also targeted stock trading firms and indirect attacks on organizations that supply hardware, secure network communications, and specific services to the financial sector. Overall, the targets share the characteristics of possessing valuable information such as confidential financial data, specific knowledge of potential mergers or acquisitions, or other information that could give the client of the attacker a competitive advantage in the sector or specific knowledge of ongoing negotiations or business deals.

Outside of the financial sector, Hidden Lynx largely targets all levels of government and government contractors. Exfiltrated information from the defense industry sector or from an opposing government could grant a nation state the ability to close a technological gap or the ability to gear intelligence and counterintelligence efforts towards a specific country. Alternately, the information could allow private organizations to spy on competitors or to gain unfair competitive advantage by speculating on government technological research and interest. Microsoft claims that during Operation Aurora Hidden Lynx targeted databases containing court order emails.

Over half of Hidden Lynx attacks target United States organizations, while another quarter of the attacks target organizations in Taiwan or China. The broad range of targets accompanied by the specificity of the information targeted indicates the mercenary nature of the attacker. The information stolen is not processed by the attacker or used for direct financial gain, so it is likely that the information is stolen on behalf of a third party. The stolen information, predominately financial or technological in nature, would be valuable to corporations and nation states alike.

Hidden Lynx targets organizations and government entities in wealthy and technologically advanced countries. Most of the Lynx attacks originate from infrastructure located in China. The group initiates campaigns with a two pronged approach. Hidden Lynx usually infects compromised systems with multiple Trojans, a mass exploitation Trojan (Trojan Moudoor) and a targeted Trojan (Trojan Naid). Each Trojan may be managed by a different team. Trojan Moudoor deploys the Moudoor backdoor, which is a modified version of the "Gh0st RAT" malware. The remote access Trojan is used to control machines in significant campaigns against multiple large companies across several sectors. The Moudoor team must be sizable because the attack vector requires attackers to breach individual targets and to extract valuable and specific data from compromised networks. Trojan Naid is used in limited attacks against valuable targets. Given its limited use and the sophistication of its application, each team behind it is likely a highly skilled special operations team within the overall group. In recent years, Hidden Lynx added the Gresim backdoor, the Fexel backdoor, the Hikit backdoor, and the Derusbi malware to their exploit kit.

The adversary regularly exploits zero-day vulnerabilities, which are purchased, discovered, or reworked from other groups' attacks. Ultimately, Hidden Lynx is methodical and it tailors its exploit kit in each attack to its victim. Hidden Lynx adapts and it will develop custom tools or perfect new techniques if necessary. Most attacks begin as a watering hole attack or a spear phishing email; however, Hidden Lynx has also been known to attack public facing infrastructure or hack the supply chain in order to distribute their malware.

Deep Panda / Black Vine / Pupa:

Deep Panda began attacking the healthcare, aerospace, and energy sectors around 2012. Deep Panda is believed to be a Chinese state sponsored group. Symantec believes that Black Vine may be affiliated with a Beijing IT security organization called Topsec. Topsec is a research institute with sites across China. Topsec focuses on information security research, training, auditing, and security products. It also hosts a hacking competition (from which they hire hackers). It is possible that some members of Topsec are affiliated with Deep Panda.

Deep Panda attacks tend to have massive impacts and they accrue proportional media attention. In order to conduct multiple sizable campaigns against United States Federal government agencies and major western health care providers for extended time periods, Deep Panda must have considerable resources at their disposal. In illustration, it is possible that Deep Panda was concurrently engaged in cyber-attacks against the United States Office of Personnel Management, the Anthem healthcare network, United Airlines, and other entities.

Deep Panda conducts watering hole attacks; zero-day exploits, and spear phishing campaigns. The group also utilizes some of the exploits and tools from the Elderwood platform.

A vast majority, ~80%, of Deep Panda targets are American. Deep Panda targets government agencies, the aerospace sector, the healthcare sector, financial organizations, technology firms, and energy entities (primarily gas and electric manufacturers).

In the United States health care sector, Deep Panda has attacked VAE, Anthem, Empire Blue Cross Blue Shield, and Carefirst. In the recent 2014-2015 Anthem breach, the group exfiltrated ~80 million patient records. Information exfiltrated from Anthem includes social security numbers and other personal identifiable information or personal health information. It is believed that the Axiom group also attacked Anthem at the same time as Deep Panda, but with a different malware and along different vectors. The attack appears as a coordinated effort. Further, enough similarities exist between the meticulous planning and malware employed by the two groups, that many security firms hypothesize that they are both part of the same group. There is a strong possibility that the groups are affiliated.

Deep Panda is also believed to be responsible for the two 2015 OPM breaches. The breaches resulted in the exposure of the personal information contained in the SF-86 forms of 22.1 million current and former United States Federal employees. 5.6 million fingerprint files were also stolen. Deep Panda breached United Airlines in 2015 and stole departure and destination records. The health, OPM, and travel records stolen by Deep Panda can be aggregated to catastrophically impact the United States government over time. The adversary or their parent nation state, can build a database of US employees for espionage purposes. Further, the information can be used to identify United States agents in the country or to identify Chinese assets who assist United States intelligence efforts. Even though their systems were not compromised and their agents' information was not included in the breach, the CIA has already began retracting agents from the field in response to the cyber-attacks. The CIA made this decision because State Department records were stolen in the breach and the attacker could thereby discover embassy employees who were not included in the State Department records and capture those individuals as spies or coerce their behavior. In this manner, Deep Panda has pushed forward the boundaries of cyber-warfare to achieve a measurable "physical" nation-state response. Further, physical warfare has been suggested in the United States in response to the cyber-attacks.

Deep Panda relies on the Sakurel Trojan, the Hurex Trojan, and the Mivast backdoor in its attacks. Deep Panda is believed to have developed all of the malware themselves. Characteristics in the malware code are shared between all three malware. Further, each malware is capable of opening a named pipe back door, tools to collect and exfiltrate system data, the ability to execute arbitrary code, the ability to create, modify, and delete registry keys.

The malwares are similar in that they utilized droppers that masquerade as installers for legitimate software applications like Adobe Reader, Juniper VPN, and Microsoft ActiveX

Control. In some cases, a loading bar is displayed and then the user is directed to a login page for the associated software. The malwares contain measures to avoid detection. The malwares self-obfuscates as technology related applications such as media applications or VPN technologies. The malwares establish persistent presence on the system, deploys remote access Trojans (RATs) such as the Derusbi malware, and features tools to record and seize user sessions. Tools such as PwDump and Scanline are included to steal user credentials, to allow the actor to escalate their privileges, to let the actor create unmonitored accounts, and to assist the attacker in lateral movements to systems across the network. Symantec believes that all three malware belong to the same family and that they have been updated and differentially developed over time by the same team. The malware is usually signed by the DTOPTOOLZ Co. signature belonging to a Korean software company. Domains and C2 servers often feature the names of Marvel comic book characters as the register.

PLA Unit 61398/ Comment Crew/ APT1

The 3rd and 4th Departments of the People's Liberation Army (PLA) General Staff Department (GSD) supposedly houses China's electronic warfare operations. Unit 61398 is the Military Unit Cover Designator of the Chinese state sponsored advanced persistent threat that operates out of the 2nd Bureau of the 3rd Department of PLA GSD, located off Datong road in Pudong in Shanghai.

Unit 61398 is tasked with computer network operations. It operates on four large networks in Shanghai. Two of these networks serve the Pudong region. The Unit has a dedicated fiber optics connection that was paid for in the name of national defense. The 3rd Department employs over 130,000 employees. Unit 61398 consists of personnel who are proficient in English and trained in computer security and computer network operations. Members of Unit 61398 use Chinese (Simplified) keyboard settings. Most of the IP addresses and the infrastructure used in the attacks trace back to China.

Unit 61398 targets sectors that are of interest to China's 12th Five Year Plan. They are large enough and well-resourced enough that it can simultaneously compromise dozens of organizations. This adversary has breached over 150 organizations since its inception in 2002. The majority of victims are located in the United States. Information Technology organizations, Aerospace firms, Public Administration agencies and other technology heavy sector are targets for Unit 61398. The adversary targets intellectual property data and financial data. It exfiltrates intellectual property data, proprietary documents, business plans, emails, and contacts.

Attacks begin with spear phishing emails that contain a malicious file or a malicious link. The emails are personalized to the target and may not easily be distinguished from legitimate emails. Attachments are usually in the ZIP format. Once the victim system is compromised, the

attacker establishes a persistent presence by installing a backdoor from the dropper delivered from the email. The backdoor initiates contact with the C2C infrastructure from inside the network so that the traffic can bypass internal firewalls. The actor typically relies upon WEBC2 backdoors, which are minimally featured beachhead backdoors. WEBC2 can only communicate with a C2C server through comments. Sometimes the BISCUIT backdoor is used if more functionality is needed. BISCUIT uses the HTTP protocol for communication and it features modules to capture screenshots, log keystrokes, record system information, modify processes, modify the registry, execute code, log off or shut down the session, and other features. Unit 61398 remains persistent on the compromised system and it may revisit the system over the course of months or years. The group remains on the network for 1-5 years. During this time, the group escalates their privileges using login credentials that it gathers from publicly available tools built into the initial malware. Next, they conduct network reconnaissance, by typing commands into the command shell. Finally, they laterally move across the network to infect new systems and they maintain their presence on the infected network. Unit 61398 compresses stolen data into multiple files with a RAR archiving utility and exfiltrates the data through their backdoor or through File Transfer Protocol (FTP).

Putter Panda/ APT2/ PLA Unit 61486:

Putter Panda is connected to the People's Liberation Army's (PLA) Third General Staff Department (GSD) 12th Bureau Military Unit Cover Designator (MUCD) 61486. Unit 61486 supports China's space surveillance network. The group may be responsible for space based signal intelligence (SIGINT) collection. The group has been actively conducting attacks since at least 2007 and is based out of the Zhabai district of Shanghai, China. Unit 61486 shares some infrastructure with Unit 61398.

Putter Panda targets the United States Government, Defense sector, Research sector, and Technologies sectors. According to CrowdStrike, the United States Defense industry, communication industries, and European satellite and aerospace industries are particularly targeted.

Putter Panda relies on spear phishing emails containing malicious PDFs and Microsoft Word Documents to infect its target. Putter Panda's exploit kit includes two droppers, two RATs, and two tools. One dropper delivers a payload, such as the 4H RAT, to the victim system and installs it. The other dropper exclusively delivers the PNGDOWNER tool. Putter Panda uses the 4H RAT and the 3PARA RAT. The 4H RAT can initiate a remote shell, enumerate running processes, terminate processes, list files and directories, modify timestamps, upload files, download files, and delete files. The RAT communicates over HTTP and the communication is obfuscated by an operation, 1-byte XOR with the key 0xBE. The 3PARA RAT is a second stage, failsafe tool that allows the attacker to regain control of the system if their initial access vector

is removed. The 3PARA RAT creates a file map at startup to verify that there is not another instance of the RAT running. The RAT is capable of remaining dormant for prearranged or commanded periods of time. The RAT only has limited commands which include retrieving file or disk metadata, changing the working directory of the current C2 session, executing a command, and listing the current working directory. The first tool, PNGDOWNER is a simple download and execute tool. The second tool, HTTPCLIENT is a backup tool. The 3PARA RAT communicates over HTTP and authenticates with a 256-byte hash and a hard-coded string.

Iran

Tarh Andishan/ Operation Cleaver:

In April 2010, a worm called Stuxnet, allegedly jointly developed by the United States and Israel, targeted Siemens industrial control systems (ICS) in developing nations such as Iran (~59%), Indonesia (~18%), and India (~8%). Stuxnet contained a programmable logic controller (PLC) rootkit designed to spy upon, subvert, and in some cases sabotage Siemens supervisory control and data acquisition (SCADA) systems that regulated specific industrial systems. In particular, Stuxnet variants were deployed by a nation state actor against Iranian industrial facilities associated with its nuclear program, such as uranium enrichment facilities. The Stuxnet infection was discovered three months later, but variants continued to compromise Iranian systems through 2012. Iran's nuclear infrastructure and its oil and gas infrastructure was also targeted by the Duqu malware from 2009-2011, and the Flame malware in 2012. As a result of adversarial cyber campaigns, Iran began rapidly developing its cyber infrastructure.

In December 2014, ICIT Fellow Cylance exposed Iranian threat actor, Tarh Andishan in the white paper of their 2-year Operation Cleaver investigation. Tarh Andishan was likely developed in response to the Stuxnet, Duqu, and Flame campaigns. Iran could be demonstrating to global targets that it is a major cyber power, capable of competing with countries such as the United States, China, and Russia, on the global cyber landscape. Cylance released Operation Cleaver early to allow potential targets the opportunity to mitigate the threat to their systems, so they estimate that they only discovered a portion of the activity of Tarh Andishan. Nevertheless, Cylance managed to build an impressive profile of Tarh Andishan's operation, including hacker profiles, domain names, internal infrastructure, and indicators of compromise.

The infrastructure used to host the attacks belonged to the corporate entity Tarh Andishan in Iran, after which the threat group is named. The infrastructure was hosted by an Iranian provider (Netafraz.com), and Autonomous System Networks (ASNs), IP source

netblocks, and domains were registered in Iran. The netblocks utilized had strong associations to state-owned oil and gas companies that employ individuals with expert knowledge of ICS systems.

Further, tools in the malware warn the attackers if their outward facing IP address traces back to Iran. The infrastructure utilized by the group is too robust and too centralized to have belonged to an individual or small "grass-roots" hacktivist group. This leads leading security firms, such as Cylance, to believe that Tarh Andishan is either state sponsored or a well-funded mercenary hacker group.

In Farsi, "Tarh Andishan" translates as "Thinkers", "Innovators", or "Inventors". Tarh Andishan consists of at least 20 dedicated hackers and developers, believed to be located in Tehran, Iran. Additional, members or hired associates operate out of the Netherlands, Canada, and the United Kingdom. Persian names (Salman Ghazikhani, Bahman Mohebbi, etc) were used as hacker monikers. Most targets of Tarh Andishan speak English as a primary language and it appears that members of the group are proficient in reading and writing in English. Different members of the group specialize in different malware, different malware development tools, different programming languages and different adversary techniques.

Tarh Andishan targets government entities and critical infrastructure facilities in Canada, China, England, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey, United Arab Emirates, and the United States. Specifically, Tarh Andishan has been known to target: military installations, oil and gas facilities, energy facilities, utility facilities, transportation facilities, airlines, airports, hospitals, telecommunication companies, technology firms, institutions of education and research, aerospace and defense facilities, chemical companies, and governments. The expansive range of targets across the globe indicates that the Tarh Andishan campaign is likely a mechanism for gaining geopolitical leverage and establishing Iran as a cyber-power. Iran may be demonstrating that it can retaliate against any country that compromises its cyber-security.

Academic institution networks are often targeted by malware because universities, especially those that work with their government in some capacity, sponsor valuable research. Universities often store sensitive PII documents and research on local servers. Yet, university networks are de-centralized and often poorly secured because different schools on campuses host different networks that are supported by different IT teams and each network needs to be accessible to thousands of users with varying needs. While the origins of Stuxnet have never been definitively confirmed, it is believed to have originated out of a university research program. Tarh Andishan targets university networks for research, but according to Operation Cleaver, it also attempts to steal student PII, student photos for identification cards, and passport information from universities in the United States, India, Israel, and South Korea.

Student PII and photos could be used for identity theft, but it could also be used for intelligence purposes because the next generation of government recruits and security researchers are currently students.

Tarh Andishan targeted airlines, airports, and transportation networks in South Korea, Saudi Arabia, and Pakistan by compromising Windows Active Directory and physical internal infrastructure such as Cisco edge switches, and routers. From there, the attackers stole VPN credentials so that they could establish a persistent presence and so that they could remotely access the entire infrastructure and supply chain. Tarh Andishan used the compromised credentials and VPN access to compromise airport gates, access security control systems, make fraudulent payments with Paypal and Go Daddy, and to infect other internal infrastructure. Overall, Operation Cleaver saw Tarh Andishan dangerously compromise airline networks without encountering major resistance. Information exfiltrated by Tarh Andishan could put airline passengers at risk if Tarh Andishan used its access to compromise airline ICS, SCADA systems, or other critical infrastructure. Further, Windows Active Directory, Cisco edge switches, and routers are components of networks in almost every organization in almost every sector. Given its success, Tarh Andishan may easily adapt this technique to attack networks in other sectors of its attack profile, if it has not done so already.

According to Cylance, Tarh Andishan's "[i]nitial compromise techniques include SQL injection, web attacks, and creative deception based attacks – all of which have been implemented in the past by Chinese and Russian hacking teams." Tarh Andishan did not appear to utilize zero-day exploits. The SQL injection attacks were made possible by attacking vulnerable applications that failed to sanitize input prior to passing it to a database in an SQL query. Later Tarh Andishan began spear phishing attacks, which involved sending victims an email with a malicious link. One such attack told targets that they had been selected to apply for a new position at an industrial conglomerate and the link directed them to a copy of a legitimate resume creation website. The resume tool was combined with a binder tool that loaded malware onto created documents. The malware runs in the background of the victim's system and logs keystrokes and the information entered into forms. After the malware infected a host, the attackers would leverage existing, publically available, exploits (such as MS08-067) to escalate their privileges on Windows systems. The malware then propagated through the network like a worm, to compromise other systems on the network. Tarh Andishan compromises Microsoft Windows web servers that run Internet Information Services (IIS) and Coldfusion, Apache servers with PHP, Microsoft Windows desktops, and Linux servers. The group also targets popular network infrastructure such as Cisco VPNs, Cisco switches, and routers.

Tarh Andishan's most utilized malware, TinyZBot, gathers information from infected systems and it establishes backdoors for persistent access. TinyZBot uses the SOAP sub-protocol of HTTP to communicate with the C&C infrastructure and it abuses SMTP to exfiltrate data to the C&C servers. Among other capabilities, TinyZBot can also take screenshots of the system, download and execute arbitrary code, detect security software, disable some anti-virus, and modify PE resources. Once the malware has infected the system, Tarh Andishan can use customized tools to poison ARP caches, encrypt data, steal credentials, create backdoors, create ASP.Net shells, enumerate processes, record HTTP and SMB communications, detail the network environment, query Windows Management Instrumentation (WMI), log keystrokes, and more. Effectively, Tarh Andishan can customize their tools to suit any target. The Net Crawler tool, which combines popular attacker tools Windows Credential Editor, Mimikat, and PsExec, was used to gather the cached credentials from every accessible computer on the infected network. Shell Creator 2 was used to generate an ASPX web shell to protect the attacker from revealing internal information such as location by human error. The nbrute utility uses NMap to map the network and then it attempts to determine network credentials via brute force. The attackers can also use tools such as the PVZ bot tool to log keystrokes on specific botted systems and save information on infected systems to specific locations.

Ajax/ FLYING KITTEN/ Saffron Rose:

The Ajax group began in 2010 with website defacement attacks, but their activity escalated to cyber-espionage by 2013. The group's C&C infrastructure was set to Iran Standard Time and used the Persian language. The Ajax team consists of 5-10 members and it is unclear if the group is part of a larger movement such as the Iranian Cyber Army. The group may have been founded by members using the monikers "HUrr!c4nE!" and "Cair3x." The group uses custom malware, but they do not leverage software exploits. The lack of exploits indicates that the group is more likely a patriotic hacktivist group than a state sponsored threat.

Ajax primarily targets United States defense contractors, firms that developed technologies that bypassed the Iranian censorship policies, and Iranian dissidents. The group has also participated in attacks against Israel with the Anonymous group.

The group tries to lure victims into revealing login credentials or self-installing malware through basic social engineering instead of leveraging software exploits. These social engineering attacks proceed through email, instant messages, private messages on social media, fake login pages, and anti-censorship technology that has been pre-loaded with malware. Past messages have directed targets to a fake login or conference page. The page spoofs a legitimate organization or application and it collects user login credentials. After the user logs in, they are directed to a different page that tells users that their browser is missing a plugin or that they need to install proxy software, which is actually the malware. In some cases,

the messages just send the user to the latter page. Iranian Internet Service Providers (ISPs) block “unacceptable content” such as pornography or sources of political dissidence. Ajax team has been infecting anti-censorship software, such as Psiphon and Ultrasurf, with malware and redistributing it.

Ajax relies on the Stealer malware which consists of a backdoor and tools. Using one tool, the attackers can create new backdoors and bind them to legitimate applications. Stealer collects system data, logs keystrokes, grabs screenshots, collects credentials, cookies, plugin information, and bookmarks from major browsers, collects email and instant messenger information along with any saved conversations. Stealer also has components that acquire Remote Desktop Protocol (RDP) accounts from Windows vault and collects user browsing history. Data is encrypted using symmetric encryption (AES-256) using a hardcoded encryption key. The information is then exfiltrated using FTP with a built in client (AppTransferWiz.dll).

A new version of the Stealer malware, dubbed Sayad, surfaced in July 2014. The variant includes a dropper called Binder and new communication modules that allow it to exfiltrate data using HTTP POST requests. Binder checks the .NET runtime version of the target machine and drops the relevant version of the malware. The malware is now more modular and contains development files suggesting the future capability to exfiltrate files from the target system.

North Korea

Bureau 121/ Guardians of Peace/ Dark Seoul:

According to defectors, Bureau 121 is one of six divisions of North Korea’s General Bureau of Reconnaissance that is charged with cyber-intelligence operations. The bureau was created in 1998 and it consists of ~1800 handpicked hackers who are allegedly the “most talented and rewarded personnel within the North Korean military” according to a Reuters interview with a defector known as Jang Se-yul. Students are recruited directly from the University of Automation and paid relatively significant sums.

North Korea uses cyber-warfare as a cost effective intelligence branch of their military. Many in North Korea see cyber-warfare as the strongest weapon. Bureau 121 most frequently targets South Korea, Japan, and the United States. Bureau 121 targets financial institutions and media companies. In one March 2014 attack, 30,000 South Korean servers associated with banking and media broadcasting outlets were damaged. These systems were infected with DarkSeoul malware and they displayed messages claiming that they were hacked by the Whois Team. In November 2014, Sony Pictures’ email server was hacked by a group claiming to be

called the Guardians of Peace, in response to the upcoming release of the movie "The Interview" because it portrays a story and portrayal that is unflattering to Kim Jong-un. An estimated 100 terabytes of data was exfiltrated from Sony before the Wiper Trojan was used to delete the servers. The information contained emails, unreleased films, employees' personal information and financial information. Threats were also made against Sony that contained imagery reminiscent of the September 11, 2001 attacks.

The FBI, Obama Administration, and the NSA have attributed the Sony breach to North Korea. Members of the press and some security researchers doubt the evidence attributing the Sony attack to North Korea. North Korea may not have been capable of exfiltrating hundreds of terabytes of data.

The Whois Team and the Guardians of Peace attacks are very similar. Both attacks were relatively unsophisticated and both attacks offered a moniker of a previously unheard of group. The procedure of each attack was to install malware through phishing campaigns, steal data, lock down the infected systems, display a banner message claiming responsibility, and then using malware to wipe the system.

Russia:

Energetic Bear/ Dragonfly/ Havex Crouching Yeti/ Koala Team/:

Since 2011, Energetic Bear, an Eastern European threat actor, has targeted the Defense Industry, Energy Industry, and ICS equipment manufacturers, with highly technical prolonged attacks that are suggestive of a state sponsor. Energetic Bear's exploit kit features specialized malware, likely developed or adapted by the attackers, that was compiled during business hours (Monday – Friday, 9am – 6pm) UTC+4, which corresponds to working hours in Russia or Eastern Europe. Most security firms conclude that Energetic Bear is a Russian state-sponsored group because the group targets nation states who are politically opposed to Russia. Further, the malware primarily compromises petroleum and energy systems that compete with Russia's energy complex in the economical arena.

Based on its choice of targets and the malware deployed, Energetic Bear seems primarily interested in gathering intelligence on its victims or their country of origin and establishing persistent access to compromised systems. The sophisticated exploit kit could easily be used to sabotage targets' operations to cause damage or disruption in critical infrastructure sectors that depend on ICS and SCADA systems. So far, while the malware has been positioned ideally to sabotage ICS and SCADA systems, investigations by Symantec and

other leading firms witness more uses of the exploit kit for espionage purposes than the sabotage purposes. The threat actors may prefer not to utilize this capability or sabotage campaigns may occur, appearing as system failures that are not investigated as cyber-attacks. More likely, Energetic Bear may be pre-positioning its malware in compromised systems to grant the greatest utility while allowing for every attack vector. Given its selection of targets and its exploit kit, both of which are detailed below, Energetic Bear is uniquely positioned to assist in a combination of Digital and Physical warfare for military or political purposes. Notably, Russia conducted such a campaign in its 2008 conflict with Georgia.

When Energetic Bear was discovered in 2011, the group targeted aviation and defense companies in the United States and Canada; however, in 2013, energy firms in the United States and Europe became the primary targets of Energetic Bear. In particular, the exploit kit targets the systems of ICS equipment manufacturers and petroleum pipeline operators. Energy grid operators, electricity generation facilities, and industrial equipment providers are also susceptible to compromise. By ingeniously targeting the smaller, less protected ICS manufacturing companies and antiquated SCADA systems, Energetic Bear is able to circumnavigate the massive state-sponsored cyber-security systems that typically protect critical infrastructure systems.

The exploit kit mimics the Stuxnet worm (which monitored and sabotaged the Iranian Nuclear program in 2011) in potential impact. If the sabotage potential of the malware were realized, then Energetic Bear could disrupt and seriously damage energy supply and regulation systems in countries such as: the United States, Spain, France, Germany, Turkey, and Poland. Consider the tragedy that a malicious actor could wrought with the ability to remotely destroy oilrigs, energy generation facilities, or electrical grids. The smallest city-wide power outage has the potential to result in many deaths related to loss in electricity needed for in-home medical care, heating, and other technologies that assist in citizens' daily lives. Even if an attack is controlled well enough or mitigated soon enough to prevent serious physical damage to the facility, imagine the economic ramifications that the actor could inflict upon a nation state through repeated targeted attacks on its energy systems. The gas price hikes of the mid 2000's might seem a minor inconvenience in comparison to the damage caused by a persistent sabotage campaign.

From February to June 2013, Energetic Bear launched a spam campaign against the United States and European energy sectors. Executives and senior employees in seven organizations received emails, sent from a Gmail account, containing a malicious pdf. If the pdf was opened, then the malware spread to the network. The emails were made to look as if they came from a known source (such as the victims' boss) and organizations were targeted with anywhere between 1 and 84 emails. In a more ambitious spear phishing campaign, emails

containing remote access Trojans (RATs) were sent to personnel in three ICS equipment manufacturers who dominated their markets. The malware injected malicious code into the ICS software update bundles that were later posted for download from the manufacturer's website. The targeted equipment which would receive the update are used in a number of sectors, including energy. The Trojan managed to compromise the bundles of two companies and infect the programmable logic controllers of devices produced by those manufacturers, before the infection was discovered.

Later, watering hole attacks were added to the campaign. In these attacks, websites often visited by personnel of the target organization were compromised (usually with an injected iframe) and set to redirect victims to a site that delivered an exploit kit that installed the malware on the victim's PC. The development of additional attack vector(s) and the resources to compromise third party sites as "stepping stones" to desired targets suggests that the group is state sponsored. In either attack, the malware was configured to search victims' systems for ICS software and updates and to trojanize the software so that the adversaries could compromise guarded ICS systems the next time the software was downloaded or they were updated by trusted personnel.

The group employs two exploit kits (LightOut and Hello) and two malware (Trojan.Karagany and Backdoor.Oldrea). The exploit kits are used to initially compromise the system and install the malware. The malware is used for espionage, persistent access, or sabotage. LightsOut exploits vulnerabilities in Java or in Microsoft Internet Explorer to deploy the Karagany or Oldrea malware onto a user's system. In September 2013, the Hello exploit kit replaced the LightsOut kit. The Hello kit is combined with watering hole attacks to redirect victims to a landing page, where a JavaScript fingerprints their system to determine details such as operating system, browser, and installed plugins. The victim is then redirected to the site that contains the exploit most likely to achieve the adversaries' goals.

Trojan.Karagany and Backdoor.Oldrea are remote access Trojans (RATs) that are used to install additional tools or malware, to search the system for valuable data, and to exfiltrate data from the system. In an attack, the group uses either Karagany or Oldea, but never both, because the malware serve the same purpose. The Karagany malware is only used in 5% of attacks. Karagany is a widely available exploit for purchase or source code recompilation on the internet underground because its code was leaked in 2010. Karagany features tools for indexing documents, taking screenshots of the system, and collecting passwords. At the adversary's instruction, it can also download new tools or files, run plugins or executables, or exfiltrate data to a designated C&C server. Oldrea, also widely known as the Havex malware, appears to be used in most attacks and it appears to have been written by or written for the attackers. Once installed, Oldrea profiles the system by collecting system information, harvesting outlook

address book information, noting VPN configuration files, and indexing files, programs, and the root of available drives. The data is compiled into a temporary file, encrypted, and sent to an adversary C&C server. Oldrea features a control panel that the adversaries can use to authenticate to a C&C server and download a compressed copy of each specific victim's data. The servers hijacked by Energetic Bear to serve as C&C servers may have been compromised using the same exploit of content management systems.

Uroburos / Epic Turla/ Snake / SnakeNet:

In 2008, malicious code known as Agent.BTZ was placed on USB drives that were dropped in the parking lots of defense facilities, such as a United States Department of Defense in the Middle East, in what was considered the "worst breach of U.S. military computers in history" at the time. Agent.BTZ infected systems running Microsoft Windows and allowed attackers to log personal information, cached credentials, and user keystrokes. The infection propogated and lasted in United States government systems for over a year. The Agent.btz infection led to the creation of the United States Cyber Command. The Uroburos malware, which appeared in 2011 (or earlier) and was discovered in 2014, scans for the presence of Agent.BTZ on target systems and remains inactive if Agent.BTZ is installed. Comments and code itself indicate that the authors of both Agent.BTZ and Uroburos are proficient in Russian. Some file names, encryption keys, and other technical indicators are shared between the Agent.btz and Uroburos malwares. Although other possibilities exist, Agent.BTZ and Uroburos were likely developed by the same group or associated groups.

The Uroburos rootkit is a very advanced and very sophisticated modular malware designed to infect entire networks and exfiltrate confidential data. The sophistication and flexibility of the Uroburos malware suggests that a highly skilled team, who had access to considerable resources, developed it. The significant monetary investment necessary to develop the Uroburos platform suggests that it was developed to target businesses, nation states, and intelligence agencies, rather than average citizens. Based on the exploit kit, the Uroburos group likely has a political or espionage agenda. The Uroburos malware typically infects 32-bit and 64-bit Microsoft Windows systems that belong to governments, embassies, defense industries, pharmaceutical companies, research and education facilities, and other large companies.

The Uroburos group uses spear phishing campaigns, drive-by-infections, watering hole attacks, and social engineering to push their malware onto target networks. In spear phishing campaigns, the target receives a tailored email containing an executable RAR self-extracting archive (SFX). If opened, then the malware unpacks and installs itself (a .SCR executable) on the user system. When the Uroburos rootkit infects a machine, it can: execute arbitrary code, hide its activity on a system, identify and exfiltrate information such as files, capture network traffic,

and infect other systems on the network. Uroburos consists of a driver (.sys file) and an encrypted virtual file system (.dat file). The complex driver seems to be specifically designed to be discrete and difficult to identify.

Remote attackers use Uroburos to infect other machines on the network and to communicate between infected hosts using a peer-to-peer architecture. Uroburos opportunistically propagates through the network. If Uroburos infects at least one system on a network that has an active internet connection and that host is connected to other systems within the network, then the attacker can infect as many systems as their resources allow. The malware spies on each system for useful information and uses the P2P architecture to relay information to the attackers. As such, information can be retrieved from air-gapped systems, transferred from infected host to infected host until it reaches a host with an active internet connection, and then exfiltrated to the adversary. This methodology allows the malware to bypass many security controls.

The Uroburos rootkit aspires to hide its elements and remain undetected and persistent on the compromised system. Upon installation, the malware establishes a service (usually Ultra3.sys) that automatically executes during the startup of the system. This driver is necessary to decrypt the malware's virtual file systems, create additional hooks, inject code into user libraries and applications, and manage communication between the adversary and the malware. The driver hooks the malware into the system by injecting code into a running process and then redirecting the rest of the running code to execute at the end of the malicious code. As non-technical simplification, this process, known as inline patching, can be visualized as inserting an extension cord (the malicious code) between another cord and a wall socket. By doing this, the malware can better remain undiscovered because malicious activity is attached to legitimate processes.

The rootkit consists of two virtual file systems (a NTFS file system and a FAT file system) that are encrypted with CAST-128 and stored locally on the user system. The encryption key is hardcoded in the driver file. The virtual file system (a .dat file) has a random name and it is stored with the driver file. The encrypted file systems function as a work environment for the attackers. Third party tools, post-exploitation tools, temporary files, and binary output are stored in the file systems. The NTFS file contains bat scripts which enable the attacker to map remote servers, execute netstat commands, gather system information, log output of tools, tools to steal documents, encrypt stolen documents, and RAR tools to compress and archive stolen documents for exfiltration. A queue and library injection tool, which acts as a buffer between the queue and the user system, can pcap or snapshot network traffic.

The virtual file system contains protocol information to exfiltrate information through HTTP (external website with GET and POST requests), through ICMP (ping), through SMTP

(email), and through named pipe to another infected systems. New libraries and tools can be added by adjusting the built in queue, without reinstalling the malware. Airgapped systems can be infected through named pipe connections or through USB devices. In the former case, an infected system serves as a proxy node and it appears passive as it spreads the infection to other systems on the network. Any infected system can serve as a proxy node, so even if one point of infection is discovered, a tangential system can continue to infect the network as the new proxy node. The peer-to-peer modular design is resilient to removal, scalable on any network, and reliable. Further, the framework can be extended to include new features and perform further attacks against the infected host or networks associated with the infected network. The design of the malware as a driver and a multi-file virtual file system that can only work in combination is an elegant, but sophisticated design that complicates analysis efforts. Without the driver, the other two files cannot be decrypted. Without the files systems, the driver is innocuous. The design is too sophisticated and too expensive to develop to be common spyware.

APT 28/ Sofacy Group/ Sednit Group/ Tsar Team/ Fancy Bear/ Operation Pawnstorm:

APT 28 is believed to be a state sponsored group that has been active since 2007. The majority of the APT 28 malware was compiled between Monday – Friday from 8 a.m. – 6 p.m. in UTC+4. This parallels working hours in Eastern Europe, Moscow, and Saint Petersburg. Over half the malware contained portable executable information that indicated that it was programmed with Russian keyboard settings, while the remaining samples were coded using English or Neutral keyboard settings.

Unlike Russian cyber-criminal groups, APT 28 does not exfiltrate financial information from targets and it does not sell the information that it gathers for profit. Instead, APT 28 gathers geopolitical information that would be specifically relevant to Russia and it uses the information to leverage future attacks. APT 28 uses spear phishing campaigns, sophisticated malware, and zero-day exploits to infiltrate systems belonging to European governments, NATO affiliates, militaries, security organizations, and media organizations with the intent of exfiltrating state information that could be used to influence policy decisions, public opinion, or geopolitical issues. Most of the activity has centered on targets “of specific interest to a European government,” focusing on the Caucasus region and countries along the eastern European border.

APT28 relies upon spear phishing emails or zero-day vulnerabilities to initially compromise victim systems. APT28 spear phishing emails often originate from a typo-squatted mail server and they typically contain either a decoy document relevant to the target or the link to a typo-squatted malicious domain. The least sophisticated aspect of APT28’s more popular attack vectors is its reliance on user error to deploy its malware. Unsuspecting users must be

tricked into opening the attachment or following the malicious link. Decoy documents are tailored to the target and they often contain a user specific title, to entice the user to open the attachment, or confidential information, likely obtained through previous breaches, to lend credibility to the document. In fact, the titles of the decoy documents submitted or found online are so specific that the targets can often be retroactively guessed by security firms, such Trend Micro, using only contextual information. Variations in the distributed decoy documents suggest that the actors are fluent in multiple languages (at least Russian and English) however; grammatical mistakes indicate that English is not their native language. While all signs in the malware indicate that Russian is the actors' native language some Russian researchers at the 2013 PHDays conference in Moscow argued that the dialect is not native Russian. APT28 uses specialized information about its targets to focus its attacks and limit detection. Only a limited number of personnel of the target organization receive the decoy documents. In one notable case, spear phishing emails were sent to only three employees of a billion dollar multinational firm, whose email addresses were not publicly available or advertised online.

The Sednit platform consists of the SOURFACE/ CORESHELL downloader, the EVILTOSS backdoor, and the CHOPSTICK modular implant. SOURFACE (also known as Sofacy) or CORESHELL performs runtime checks and reverse engineering counter operations before verifying that the infected machine matches the system profile of the target. If the target is verified, then the SOURFACE/CORESHELL dropper obtains a second stage backdoor from the C2 server and installs it on the victim's system. The backdoor, EVILTOSS, is used to steal credentials and execute shellcode. EVILTOSS uploads an RSA public key and encrypts the stolen data. Then the data is sent via email as an attachment. EVILTOSS then delivers CHOPSTICK to the victim's system and installs it. CHOPSTICK is comprised of custom implants and tools that are tailored to the target system. CHOPSTICK actively monitors the victim's system by logging keystrokes, taking screenshots, and monitoring network traffic.

APT29/ Hammertoss:

APT29 is a new threat actor that operates during UTC+3 work hours. APT29 targets government organizations in an attempt to collect geopolitical data that could be of interest to Russia. APT29 might be a state sponsored threat group; however, the group is too new to exhibit definitive signs of state sponsorship.

APT29 employs anti-forensic techniques, they monitor analysis and remediation efforts, and they rely upon compromised C2C infrastructure. Apt29 embeds the Hammertoss commands into images using steganography. APT29 programs Hammertoss to operate to blend into normal target network traffic and normal target network traffic patterns. The group preconfigures Hammertoss to activate after a predetermined date and only communicates during specified hours.

There are two variants of Hammertoss , Uploader and tDiscoverer. Both variants receive their instructions from an embedded image. Uploader goes to a hard-coded C2C server address and downloads an image of a specific file size. tDiscoverer generates and visits a new Twitter handle every day from a preconfigured algorithm. It attempts to visit that page. If the actor has registered the handle, then it visits the page and looks for a tweet with a URL that indicates the location of its instructions and a hashtag that specifies the minimum size of the image file. After the number of bytes, the hashtag may also contain a string that the malware adds to its encryption key so that it can decrypt the data. If the actor has not registered the handle, then the malware waits until the next day and repeats the process with the next handle generated by the algorithm. The malware fetches the image from the URL. Uploader or tDiscoverer decrypts the data hidden in the image and processes the attackers' command. Commands include conducting reconnaissance on the victim system, executing commands via PowerShell, or uploading stolen data to a cloud storage service.

CozyDuke/ CozyCar/ CozyBear/ Office Monkeys/ Cozer/ EuroAPT

The CozyDuke group began attacking governments and associated organizations around 2011. CozyDuke is a very precise group and it has not been extensively profiled. It may have been developed or used by actors of the MiniDuke or OnionDuke APT groups. CozyDuke shares at least some infrastructure with these groups. Security firm F-Secure reports that CozyDuke, like the rest of the Duke family of malware, originates from a seven year campaign that is affiliated with the Russian government. It is unclear whether the Duke family of malware is sponsored by the Russian government or developed and used by a mercenary criminal organization.

Cozy Duke attacks very specific governmental organizations and affiliated entities. CozyDuke mostly targets United States entities; however, government and commercial entities in Chechnya, Germany, South Korea, and Uzbekistan have also been targeted. CozyDuke is believed to be behind the late 2014 attacks on the United States Department of State and attacks against the White House.

Like most APT's, CozyDuke attacks typically begin with a spear phishing email. Sometimes the emails are loaded with malicious Adobe Flash video attachments. In the past, the videos have been funny animal videos. Other times, the emails contain malicious links that deliver the user to websites that the attackers created to look like real sites. Otherwise, the email contains a ZIP file containing a decoy PDF document and a self-extracting RAR file. Once the user opens the attachment or visits the link, the initial dropper is installed on the system. The initial dropper checks the system for security products, and will not install further malware if a program on the system matches software on its list. The dropper also runs processes to check if it is being run in a virtual machine or sandbox environment. If either check indicates an

analysis environment, then the dropper exits. Otherwise, the dropper delivers an encrypted configuration file, and installs the CozyDuke components. The CozyDuke malware is signed with fake Intel and AMD digital certificates so that it appears legitimate to some security solutions.

The CozyDuke malware is a modular platform that consists of a core component, the CozyDuke backdoor, and modules tailored to its target. The platform includes multiple malware droppers and additional custom and open-source spyware tools. The CozyDuke main component establishes a persistent beachhead on the victim system, gathers system information, communicates with the C2 infrastructure, and manages the accompanying modules and scripts. The main component adds a registry value that is executed at system startup. It also obfuscates itself as a Windows service or scheduled task. Variants of the main component may also hijack the registry entry of a COM object “SharedTaskScheduler” so that the malware loads with the COM object.

CozyDuke modules can execute arbitrary code, harvest victim credentials, gather system information, and take screenshots of the victim system. Some of the CozyDuke modules appear to have been developed in the same development environment as MiniDuke and OnionDuke. The platform also contains the CORESHELL and CHOPSTICK modules made popular in the Russian state-sponsored APT28 attacks. CORESHELL is a second stage backdoor that runs numerous anti-analysis procedures. CHOPSTICK is a modular implant that logs keystrokes, takes screenshots, and monitors network traffic.

Recent variants of CozyDuke deliver SeaDuke and HammerDuke. SeaDuke is a cross platform backdoor that is written in Python. This expands the attackers’ pool of victims to include Linux users. HammerDuke is a backdoor that connects to a Twitter account name and uses tweets from the account to locate C2 server addresses from which it receives commands or to which to delivers data.

Sandworm/ Quedagh/ BlackEnergy

The Sandworm team is a Russian advanced persistent threat group that targets systems of political targets of interest to the Russian Federation. Sandworm is likely state-sponsored. The group’s name originates from strings in their code and names of their C&C servers that reference the Dune fantasy book series.

Sandworm has targeted governments and political organizations since at least 2009; but the group also may have been behind the 2008 cyber-attacks against Georgia. The Ukrainian government, NATO, the European Union, the European Telecommunications sector, European Energy companies, and Poland are among the group’s top targets. Attendees of the May 2014 Globesec conference were also targeted. Many of the decoy documents used to deploy the malware were spoofed news coverage of political or economic situations in Europe.

The new variant of the BlackEnergy malware, which is now capable of stealing documents from targets, has been used against government institutions in Ukraine and Eastern Europe. The initial appearance of the malware coincides with the conflict between Russia and Ukraine. Trend Micro discovered that the newest variant of the malware, customized by the group, can target ICS and SCADA systems. The group may have infected these systems to monitor or sabotage systems that compete with Russia's energy interests.

Sandworm delivers malware through spear phishing emails containing malicious document, such as a Microsoft PowerPoint attachment. The attachments either deliver the initial dropper or exploit a zero-day vulnerability to install the malware. In some cases, legitimate applications were trojanized to perform the installation. Through zero-day exploits, the malware infects any system running a Windows Operating System ranging from Vista to Windows, including Windows server systems. The malware only infects the victim system if the current user is a member of the local administrator group. If the user is not an administrator, then the malware will attempt to re-launch itself as Administrator or exploit the Windows backward compatibility features to bypass UAC.

The BlackEnergy crimeware appeared for sale in underground Russian cyber-markets around 2007. The malware was designed to create botnets for Distributed Denial of Service attacks (DDoS), but it has since evolved to support other capabilities. BlackEnergy can create botnets to send spam emails for phishing campaigns and it has tools to harvest passwords and banking credentials from infected computers.

The BlackEnergy toolkit gained notoriety during the 2008 cyber-attacks on Georgia during the conflict between Russia and Georgia. The BlackEnergy malware is available for purchase in cyber underground communities; however, the variant used in Sandworm attacks has been modified with custom code, incorporates a proxy server infrastructure, techniques to User Account Control and driver signing features in 64-bit Windows systems, and tools to collect documents. F-Secure notes BlackEnergy is used by a variety of criminal and cyber espionage groups; so, Sandworm's adoption of BlackEnergy, instead of writing custom malware, may have been an attempt to shirk attribution and blend into the crowd of nefarious actors to remain undiscovered.

The BlackEnergy toolkit features a builder application that generates the clients used to infect victim systems, it features server-side scripts to create C&C servers, and it includes an interface for the attacker to communicate with their botnet. F-Secure comments that the toolkit is simple enough and convenient enough that anyone can build a botnet without possessing extensive skills. The information stealing plugin of the toolkit gathers system information, session information, a list of installed applications, a list of registered mail, browser, and instant messaging clients, a list of network connections, and stored user

credentials for online and offline accounts, and exfiltrates the information back to the C&C server via a HTTP POST request. New variants of the malware may also be able to capture screenshots and record audio.

Syria

The Syrian Electronic Army (SEA):

The Syrian Electronic Army is a public online political group that emerged in 2011 to support Syrian President Bashar al-Assad and his regime. The army arose days after Syria lifted its online ban of Facebook and YouTube. SEA was once managed by the Syrian Computer Society, which was headed by President al-Assad in the 1990s. The Syrian Computer Society, which regulates the internet within Syria, even registered the SEA website. The SEA may be partially or entirely supported by the Syrian government. At present, the SEA's domain is no longer hosted by the Syrian Computer Society and it claims no ties to the government. Based on the aptitude at social media and the humor used on defaced sites, the army likely consists of young adult males. One "inside source" claimed that the group consisted of nine Syrian college students; however no other sources have verified this claim.

By all appearances, the SEA conducts attacks to garner global attention rather than to steal data or financial information. The SEA primarily targets media outlets and journalists, political groups that oppose al-Assad's regime, human rights groups, and western organizations. Most SEA attacks target the websites and social media accounts of United States news organizations because it argues that the outlets spread anti-Syria propaganda. The SEA uses malware and phishing campaigns to actively monitor Syrian rebels and members of Human Rights groups.

SEA attacks begin with phishing through spam or spear phishing using detailed information obtained from previous campaigns. The SEA attempt to gain user credentials, which it then uses to seize control of the websites and social media accounts of prominent organizations. The army has attacked the websites and/or social media accounts of: "60 Minutes," Al-Jazeera, Associated Press, BBC News, CBC News, CNN, The Daily Telegraph, Financial Times, The Guardian, The Onion, National Public Radio, The New York Times, Reuters, Time, and The Washington Post. Once it has control, The SEA posts fake stories or news and collects any confidential information that could be useful in future attacks, such as contact names. When phishing attempts fail, SEA may resort to malware, website defacement through web exploits, or denial of service attacks leveraging botnets. If no attack vector succeeds, then the SEA resorts to bombarding the social media accounts of its target with pro-Syria messages.

Most attacks amount to a banner ad or redirection to a site that supports al-Assad; however, the attacks can have tangible impacts. When the SEA hacked the Associated Press Twitter account in 2013, they posted a message that the White House had been bombed and that President Obama was injured. The post resulted in a noticeable impact on the DOW Jones and the S&P 500 Index (~$136.5 billion).

In their attack on the New York Times, the SEA demonstrated the ability to breach a major domain registrar, Melbourne IT, using stolen credentials and redirect internet traffic or seize ownership of domains, such as Twitter. The SEA has also compromised the GoDaddy domain registrar, social media management services, and third party applications that serve news articles. The attack on a registrar indicates that the SEA may begin to attack third party services and underlying infrastructure in order to compromise its target. Recently, the SEA has attacked larger targets such as Microsoft, Facebook, EBay, and PayPal through the underlying infrastructure.

Global

Anonymous

Anonymous is a collective of hacktivists and script kiddies which originated in 2003 on the website 4chan. In the traditional sense, Anonymous is more of a cyber-mob than an advanced persistent threat; however, the group's construction and global membership afford it significant influence and resilience to law enforcement efforts. Anonymous has established a brand name with the physical weight of a cohesive advanced persistent threat group. Anonymous has a decentralized command structure and it unties its members through anarchic ideology. Essentially, the loosely affiliated members or member groups work towards goals that they agree upon or remain inactive or split off, if they do not agree. Dissent is common within the group and one of the largest difficulties in profiling Anonymous is that the only absolutely unifying characteristic is membership in the group. Some members participate to deface websites and prank organizations while other members participate because Anonymous affords them a serious political activism platform. Most of the members support the foundational anti-censorship and anti-control platform and they target entities accused of censoring the people. Members, Anons, range from non-technical supporters to active blackhat hackers. Essentially, if an individual believes in the Anonymous cause or simply says that they are a member, then they are part of the collective. Anonymous members are told to neither reveal their identity or to discuss the group. The sense of membership and ease of access has allowed a few skilled hackers in Anonymous to hide amongst massive crowds of protesters.

Anonymous began by attacking the Church of Scientology, but its scope rapidly expanded. Since then, Anonymous has protested mass surveillance, anti-digital privacy efforts, governments, financial institutions, and individual users. More specifically, Anonymous has targeted the MPAA, the RIAA, Sony, the Church of Scientology, the Westburo Baptist Church, government entities in the United States, Canada, Israel, Tunisia, and Uganda, PayPal, MasterCard, Visa, and child smuggling and child prostitution rings. Anonymous supported the Occupy movement against large businesses, and it supported the Arab Springs movement against oppressive regimes in the Arab region. The media is the only sector that Anonymous members are prohibited from targeting.

Anonymous defaces websites and organizes distributed denial of service attacks (DDoS). Hacked websites may feature the pivotal picture of the Guy Fawkes mask, it may feature a manifesto claiming responsibility for the attack, or it may simply display an internet meme. DDoS attacks are conducted with Gigaloader, JMeter, or the Low Orbit Ion Cannon (LOIC) applications. These tools flood a server with inbound TCP or UDP packets. Botnets belonging to members of the group are often added to DDoS campaigns. In some attacks, these botnets account for up to 90% of the malicious traffic.

America:

Butterfly Group/ Morpho

The Butterfly group performs corporate espionage campaigns against organizations containing proprietary intellectual property. Stolen information is likely sold for fiscal gain. The Butterfly group is organized and efficient. It is likely that the group consists of only a few individuals (~3-10 members). According to Symantec, “[t]here are some indications that this group may be made up of native English speakers, are familiar with Western culture, and may operate from an Eastern Standard Time (EST) time zone.” The emergence of the Butterfly group should remind organizations that corporate espionage groups and non-state sponsored APTs still exist. In fact, in certain aspects, they are more dangerous than state sponsored groups. Mercenary and espionage groups may possess specific knowledge of what information to steal or from what systems to steal data. This information may come from competitors or it may come from insider threats within the organization. APTs, like the Butterfly group, are more likely to profit from exfiltrated data and stolen intellectual property than an enemy nation state might. Auction of stolen information to a third party will likely occur immediately after a breach because the group maximizes their potential by realizing profit and redirecting their resources to the next target. Few concurrent campaigns were observed. Once information is sold to a third party, attribution of the attack becomes more difficult. The realized impact of lost financial data or stolen intellectual property could cripple the organization.

The Butterfly group has targeted pharmaceutical companies, technology firms, law practices, oil and precious metal mining organizations, Twitter, Facebook, Apple, and Microsoft. Since their creation in 2012, the group has compromised at least 49 organizations. There was only one government victim and they may have been collateral damage of a different campaign. Butterfly does not appear interested in nation state intelligence. After the attacks against Twitter, Facebook, Apple, and Microsoft in February 2013 drew the attention of security researchers, the group went dormant. They reemerged in August 2013 and have been gradually increasing their number of attacks per year. Of the 49 companies targeted, 17 are based in the United States, 12 are based in Europe, and 4 are based in Canada. The remaining 16 victims are located in Brazil, China, Hong Kong, India, Israel, Japan, Kazakhstan, Malaysia, Morocco, Nigeria, Taiwan, Thailand, South Korea, and the United Arab Emirates.

In attacks against pharmaceutical companies, the attackers breached small regional offices and then slowly moved across the network to the main network. In late 2014, two natural resource organizations that specialize in gold and oil were compromised. In June 2015, a Central Asian global law firm was compromised and financial information and information about regional natural resources may have been targeted. This has led to speculation that the attackers may be focusing on information that is valuable in the commodities market. The behavior may also indicate direction from a third party client who is invested in the commodities market.

Attacks seem to be focused on specific systems that are of interest to the attackers, such as Microsoft Exchange or Lotus Domino email servers. The attackers may want to monitor emails or they may want to inject messages into the server. Content management servers, which index and store documents and digital assets, were also targeted. According to Symantec, these servers likely contained legal documents, internal policies, training documents, product descriptions, and financial records. The actor may gauge the value of a target based on training materials and presentations for related technologies under development at the organization. In at least one instance, the group hacked a Physical Security Information Management (PSIM) system which collects, processes, and stores data from physical security devices such as CCTV, magnetic card systems, HVAC, and building security systems. The actor could have been monitoring employees throughout their daily activities, or the system could have been compromised by mistake.

The Butterfly group exploits zero-day vulnerabilities from a water hole website. In February 2013 Twitter, Facebook, Apple, and Microsoft were attacked within a three week period. The Butterfly group initiated their campaign with a Java zero-day exploit that was delivered from a popular iPhone mobile development website. For some of the attacks, F-Secure believes that the payload delivered after the breach may have been a Mac OS X

backdoor, dubbed OSX Pintsized. Attacks against Windows systems likely featured the Jripbot backdoor. Symantec believes that the group may also exploit Internet Explorer 10 or an Internet Explorer plugin. At least one recent attack suggests that the group might also conduct SQL injection attacks.

After a network is compromised, the group carefully adapts to the environment and utilizes remote access tools and management systems to laterally move across the network. The adversaries have used native Citrix systems and the TeamViewer applications to move across some networks. The attackers are able to rapidly assess whether a system is valuable or whether they should move to a new system on the network. The Butterfly group uses a unique set of tools, which seem to have been developed by or developed for the attackers. Symantec could not find any open source data on the tools. The tools all contain use documentation. One tool, bj.dat, (called "Banner Jack.") is used to locate vulnerable network servers, printers, routers, HTTP servers, or TCP servers. Banner Jack retrieves default messages from Telnet, HTTP, and TCP servers. Banner Jack accepts an input IP range and port and then it connects to each IP address to a port. Then it retrieves and logs any data printed by the server. The Proxy.A tool creates a proxy connection so that the actor can route traffic through a proxy node to a destination node. The Eventlog tool parses event logs, dumps interesting logs and deletes incriminating logs. The tool can also end processes and delete itself. The Multipurpose tool edits event logs, dumps passwords, securely deletes files, encrypts files, enumerates the network, and assists the attacker in moving across the network.

The Butterfly group exhibits intense operational security. Many of their tools self-delete, and others are securely deleted by a GNU Shred tool used by the attackers. Event logs are modified or deleted to hide the intrusion. Uninteresting computers are fully purged of all traces of the attacker's presence. C&C domains are registered with disposable names and emails. Hosts of C&C servers are paid using the Bitcoin anonymous digital currency. Symantec observed that the group "uses encrypted virtual machines and multi-staged C&C servers" to make it more difficult to investigate their middle infrastructure. Symantec managed to track activity through proxies to a C&C server that was digitally sterilized. No activity was logged and the system featured Truecrypt and a Virtual Box virtual machine. Compromised systems were likely attacked from within the virtual machine; consequently, analysis is difficult when the image is not live.

America's Most Elite Line of Cyber-Defense: Tailored Access Operations (TAO)

As the most targeted Nation in the world, The United States intelligence community has been continuously raising the bar to combat global bad actors. Tailored Access Operations is the largest operative component of the Signal Intelligence Directorate of the United States National Security Agency (NSA), consisting of over 1000 military and civilian cyber security

professionals, hackers, technology specialists, and hardware and software designers. Approximately 600 of TAO's Computer Network Exploitation (CNE) operators work in rotating 24 hour, seven day a week, shifts out of the Remote Operations Center at Fort Meade.

The Office of Tailored Access Operations produces some of the best intelligence for the United States government and its work has been pivotal to the success of numerous operations. TAO is credited with delivering critical information to the 2007 U.S. Army operations in Iraq and in the 2007 operations to prevent Iran from obtaining nuclear weapons.

TAO is comprised of four main divisions. The Data Network Technologies Branch develops the infiltration and collection software utilized by the TAO. The Telecommunications Network Technologies Branch curates infiltration techniques. The Mission Infrastructure Technologies Branch combines the spyware and techniques to use in campaigns and they develop and build the computer and telecommunications hardware. The Access Technologies Branch, which contains personnel seconded by the CIA and FBI, performs "off-net operations." TAO is headed by U.S. Cyber Command and the director of the NSA.

The NSA describes TAO operations as computer network exploitation. TAO conducts counterterrorism and traditional espionage operations, but they also conduct cyber-attacks on behalf of the United States. Supposedly, TAO is able to compromise even the hardest targets. TAO is tasked with monitoring foreign entities, infiltrating their networks, and gathering information. It accomplishes its task through spyware or by compromising network devices such as routers, switches, or firewalls, and monitoring the network traffic. TAO is also tasked with developing malware or information profiles that would enable the United States to cripple foreign network infrastructure or telecommunications if directed to do so by President Obama.

The NSA is not authorized to conduct operations against domestic targets; however, some are concerned about the massive telecommunications monitoring programs that were revealed as a result of the Snowden leaks. The NSA monitors domestic traffic to capture communications in which at least one party originates from outside the United States.

When CNE operators identify a network or system belonging to a nefarious foreign entity, they attempt to compromise its security, download a copy of its hard drive for analysis, and plant malware tools to monitor email and network traffic from the machine.

The main attack suite developed by the TAO and made public by the Snowden leak is dubbed QUANTUM. QUANTUM features a suite of attack tools that enable DNS injection attacks, HTTP injection attacks, and the ability to inject into MySQL connections. It also contains tools to hijack IRC and HTTP-based criminal botnets and tools to create phantom servers. The QUANTUMDEFENSE portion of the program searches tapped connections for DNS requests for NIPRnet addresses and initiates a packet-injection attack on a DNS reply to redirect the target

to an NSA controlled site. This site may be a FOXACID server, which probes the victim's browser for weaknesses. The TAO can exploit any weaknesses with the QUANTUMINSERT program and seize control of the victim system. QUANTUMSMACKDOWN conducts packet injection attacks against attacks aimed at Department of Defense assets. QUANTUMCOOKIE is used to de-anonymize Tor users through web cookies and fetch requests. Finally, the QUANTUMSQIRREL program lets TAO pose as any authenticated user on virtually any site by spoofing the IPv4 or IPv6 address of the host. Through this, TAO can monitor most digital communication, create posts from a "trusted" account, or pose as specific users in online transactions.

Conclusion:

The conglomeration of hacktivists, state sponsored hackers and cyber mercenaries are continuously targeting American corporations, organizations, Universities and government networks. The malicious element is winning because the United States lacks proper cyber hygiene and has yet to expedite a path to a cybersecurity-centric culture. Metaphors matter as the language to describe cyberattacks today, shape the legislative community's constitutional adherence in future policy. The reader is cautioned to be weary of the new cliché "Cyberwar" continuously being used as a kneejerk reaction in times of panic. As we experience warlike tactics being used by a wide variety of bad actors (with a multitude of motivations) in a cyber setting it will be important to distinctively separate what defines cyberwar from cyber conflict, cyberattack and cyber espionage as each term holds a different variant of retribution and/or penalties.

American industry as a whole is an easy target because seasoned adversaries are breaching virtually defenseless networks. Organizations are encouraged to follow, at a minimum the latest NIST Standards for Critical Infrastructure Cybersecurity. A vigilant approach to cyber and social engineering education, application patching, technical abnormality notifications etc. are paramount for organizations striving to minimize attack surface and maximize defenses.

Even with multi-factor authentication and cybersecurity protocols in place, breaches will happen. Optimized cybersecurity strategies will use early warning mechanisms such as behavioral analytics and behavioral biometrics coupled with multilayered encryption. This 'Tar Pit' method will slow down a breach, alert the proper administrator and minimize threat. That said, even the most robust cybersecurity strategy is useless if the bad actor has obtained legitimate admin credentials, therefore education is essential. Spear Phishing is one commonality shared by a majority of hacking events. Spoofed URL's, watering hole attacks etc. are all dependent on getting the target to click on a link or open an attachment that carries the malicious code that will infect one's network; the objective is to train staff to identify these subtleties that will have catastrophic impact.

Targeted advanced persistent threats will continue to multiply and become more sophisticated. Optimal application of the most up-to-date defense technologies is the first step in demotivating hackers from attempting to breach one's network as attackers will typically pick the path of least resistance and complexity. Understanding the enemy, learning from past mistakes while planning for new threats based on reliable research must be part of every association's cyber strategy.

Terms:

Malware – Malware is the catch-all term for any malicious code. Malware can take the form of viruses, Trojan horses, worms, ransomware, spyware, adware, scareware, or malicious programs.

Virus – A computer virus is malicious code that replicates itself when executed, and may infect other programs or systems.

Trojan – A Trojan horse is a malicious program that tricks the user into installing it, by misrepresenting itself as a useful or desirable process or program.

Worm – A computer worm is a self-replicating malicious program that may spread to other computers and other networks.

Rootkit – A rootkit is malicious software that obfuscates its existence and that enables an attacker to access a system or its files.

Vulnerability – A vulnerability consists of a flaw in system (e.g. a flaw in the code), attackers' access to that flaw, and the attackers' ability to exploit the flaw.

Zero-day Vulnerability – A software flaw is that present at launch, but unknown to the software vendor. Often, zero-day vulnerabilities are repaired by the vendor through software patches.

Zero-day Exploit – Zero-day exploits are harmful vulnerabilities that are not discovered or are not repaired by the vendor. Zero-day exploits tend to be rare and expensive since the knowledge of their existence must remain secret lest vendors repair the vulnerability.

Backdoor – A hidden program, or program component, that allows unauthorized remote access to a computer.

Registry – The system registry is the database of system hardware information, profile information, installed programs, and settings.

Privilege Escalation – Privilege escalation is the exploitation of a bug, design flaw, or configuration oversight which grants elevated access to resources that are normally protected from an application or user.

Command and Control Server – Command and control servers are also referred to as a C2 server or a C&C server. C2 servers are the centralized system that issues commands and receives outputs from infected machines (a botnet).

Legacy System – Legacy systems are old or outdated systems that are not compatible with modern applications or programs.

SCADA System – A Supervisory Control and Data Acquisition (SCADA) system operates with coded signals over communication channels to provide control of remote equipment.

Virtual File System – A virtual file system is an abstract layer on top of the user file system. A virtual file system allows its user to access applications across multiple file systems.

Air-gapped System – An airgapped system is not connected to the internet and is not directly connected to any systems that are connected to the internet.

Exfiltration – The process of removing data from a system.

Adversary – The attacker, hacker, enemy nation-state, or malicious actor targeting a system.

Advanced Persistent Threat – A group of attackers or developers who are sophisticated, persistent, and who have access to significant resources.

Common Attack Vectors:

Phishing (spam) – Most breaches are the result of human error, such as an employee opening a malicious email. Phishing campaigns consist of sending massive amounts of malicious emails which contain either malicious links or malicious attachments. The user

system is infected with malware if they follow the link to a landing page or if they open the attachment. Even though most recipients of the email will ignore it, phishing is successful because it is cheap and the relative gain of even one infected computer resulting from millions of sent emails is high.

Spear Phishing – Spear Phishing is the process of sending tailored emails to specific targets of value to the attackers. Spear phishing emails require the attacker to know more information about the target and as a result, they can be very convincing, even to trained security professionals.

Watering hole Attack – In a watering hole attack, the adversary either infects or spoofs websites that are often visited by members of the target organization. When users visit the website, the adversary can infect their system with malware.

USB/ Air-gapped Attack – Airgapped network attacks are sophisticated techniques of infecting systems that are not connected to the internet, and in some cases not connected to other systems, with malware. Attackers can infect storage media in hopes that it will be plugged into the system, they can infect software updates to the system, or they can infect systems connected to the target and exploit the connection to install malware.

This Brief was authored by:

- James Scott (ICIT Senior Fellow – Institute for Critical Infrastructure Technology)
- Drew Spaniel (ICIT Visiting Scholar, Carnegie Mellon University)

Contact Information

Legislative Branch Inquiries:

- James Scott, Senior Fellow, ICIT (james@icitech.org, 202-774-0848)

Federal Agencies, Executive Branch and Fellow Inquiries:

- Parham Eftekhari, Senior Fellow, ICIT (parham@icitech.org, 773-517-8534)

Links

Website: www.icitech.org

Social Media:

https://twitter.com/ICITorg

https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit-

https://www.facebook.com/ICITorg

Sources

ARS Technica:

http://arstechnica.com/security/2014/11/sony-pictures-hackers-release-list-of-stolen-corporate-files/

http://arstechnica.com/security/2015/06/us-army-website-defaced-by-syrian-electronic-army/

http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/

http://arstechnica.com/security/2015/03/new-smoking-gun-further-ties-nsa-to-omnipotent-equation-group-hackers/

http://arstechnica.com/tech-policy/2015/09/cia-officers-pulled-from-china-because-of-opm-breach/

http://arstechnica.com/security/2015/09/dhs-infosec-chief-we-should-pull-clearance-of-feds-who-fail-phish-test/

http://arstechnica.com/security/2015/09/us-counterintelligence-czar-tells-government-employees-raise-your-shields/

http://arstechnica.com/security/2015/08/china-and-russia-cross-referencing-opm-data-other-hacks-to-out-us-spies/

http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/

http://arstechnica.com/security/2015/09/seven-years-of-malware-linked-to-russian-state-backed-cyberespionage/

http://arstechnica.com/security/2015/09/how-highly-advanced-hackers-abused-satellites-to-stay-under-the-radar/

The Atlantic:

http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/

BBC News:

http://www.bbc.com/news/technology-30189029

Beta News:

http://betanews.com/2015/04/22/anonymous-lulzsec-guardians-of-peace-a-guide-to-the-most-notorious-hacking-groups/

Bloomberg Business:

http://www.bloomberg.com/bw/articles/2013-05-23/how-the-u-dot-s-dot-government-hacks-the-world

http://www.bloomberg.com/news/articles/2013-06-25/s-korea-president-s-websites-closed-for-review

Berkeley Varitronics Systems:

https://www.bvsystems.com/WordPress/?tag=guardians-of-peace

CNet:

http://www.cnet.com/news/us-army-website-offline-after-hack-by-syrian-electronic-army/

CrowdStrike:

http://blog.crowdstrike.com/ironman-deep-panda-uses-sakula-malware-target-organizations-multiple-sectors/

http://blog.crowdstrike.com/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/

Cyber War Zone:

http://cyberwarzone.com/whitepaper-russian-cyber-espionage-campaign-sandworm-team-2014-free-download/

Cylance:

http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf.

Electronic Frontier Foundation:

https://www.eff.org/deeplinks/2014/03/new-nsa-slides-reveal-tailored-access-run-amok

F-Secure Labs:

https://www.f-secure.com/weblog/archives/00002718.html?tduid=ff8c6c422cb66b85a8ae21edb2f35886

https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf f secure black energy

https://www.f-secure.com/documents/996508/%201030745/CozyDuke.

https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf.

FireEye:

https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf.

Forbes:

http://www.forbes.com/sites/katevinton/2015/06/08/syrian-electronic-army-claims-responsibility-for-hacking-army-website/

GData:

https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf.

HIS talk:

http://histalk2.com/2015/02/09/readers-write-fact-and-fiction-about-anthems-breach/

The Huffington Post:

http://www.huffingtonpost.com/2015/05/14/washington-post-hacked-syrian-army_n_7285382.html

Information Week Dark Reading:

http://www.darkreading.com/security-companies-team-up-take-down-chinese-hacking-group/d/d-id/1317006

http://www.darkreading.com/attacks-breaches/with-operation-cleaver-iran-emerges-as-a-cyberthreat/d/d-id/1317861

Infosec Institute:

http://resources.infosecinstitute.com/equation-group-apt-tao-nsa-two-hacking-arsenals-similar/

International Business Times:

http://www.ibtimes.com/deep-panda-group-wasnt-behind-massive-opm-hack-other-chinese-hackers-were-fireeye-1975658

http://www.ibtimes.com/fbi-formally-blames-north-korea-sony-hack-chinese-involvement-under-investigation-1763579

ISight Partners:

http://www.isightpartners.com/2014/10/sandworm-team-targeting-scada-systems/

http://www.isightpartners.com/2014/07/weeks-threatscape-media-highlights-update-14/

Kaspersky Lab

http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage

Krebs on Security:

http://krebsonsecurity.com/tag/the-elderwood-project/

The New Yorker:

http://www.newyorker.com/tech/elements/syrias-other-army-how-the-hackers-wage-war

NCC Group:

https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/july/a-new-flying-kitten/

Novetta:

http://www.novetta.com/files/5614/1329/6232/novetta_cybersecurity_exec_summary-3.pdf

Recorded Future:

https://www.recordedfuture.com/russian-malware-analysis/

Reuters:

http://www.reuters.com/article/2015/06/21/us-cybersecurity-usa-deep-panda-idUSKBN0P102320150621

http://www.reuters.com/article/2014/12/05/us-sony-cybersecurity-northkorea-idUSKCN0JJ08B20141205

Schneier on Security:

https://www.schneier.com/blog/archives/2013/12/more_about_the.html

Secure List:

https://securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/

https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf.

Security Affairs:

http://securityaffairs.co/wordpress/29290/cyber-crime/security-firms-vs-hidden-lynx.html

http://securityaffairs.co/wordpress/36195/cyber-crime/cozyduke-russian-apt-group.html

Security Week:

http://www.securityweek.com/cozyduke-apt-responsible-white-house-state-department-attacks-kaspersky

Spiegel Online International:

http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-3.html

Symantec:

http://www.symantec.com/connect/blogs/how-elderwood-platform-fueling-2014-s-zero-day-attacks

http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

http://www.symantec.com/connect/blogs/security-vendors-take-action-against-hidden-lynx-malware

http://www.symantec.com/security_response/publications/whitepapers.jsp

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/butterfly-corporate-spies-out-for-financial-gain.pdf.

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf.

Tech Times:

http://www.techtimes.com/articles/22160/20141215/operation-cleaver-is-bigger-threat-than-previously-thought-fbi-warns-us-businesses.htm

TechWorm:

http://www.techworm.net/2014/12/bureau-121.html

Trend Micro TrendLabs Security Intelligence Blog:

http://blog.trendmicro.com/trendlabs-security-intelligence/sandworm-to-blacken-the-scada-connection/

The Washington Post:

https://www.washingtonpost.com/news/the-switch/wp/2015/05/14/the-syrian-electronic-army-just-hacked-the-washington-post-again/

https://www.washingtonpost.com/news/the-switch/wp/2014/12/29/a-qa-with-the-hackers-who-say-they-helped-break-in-to-sonys-network/

https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/

https://www.washingtonpost.com/world/national-security/researchers-identify-sophisticated-chinese-cyberespionage-group/2014/10/27/de30bc9a-5e00-11e4-8b9e-2ccdac31a031_story.html

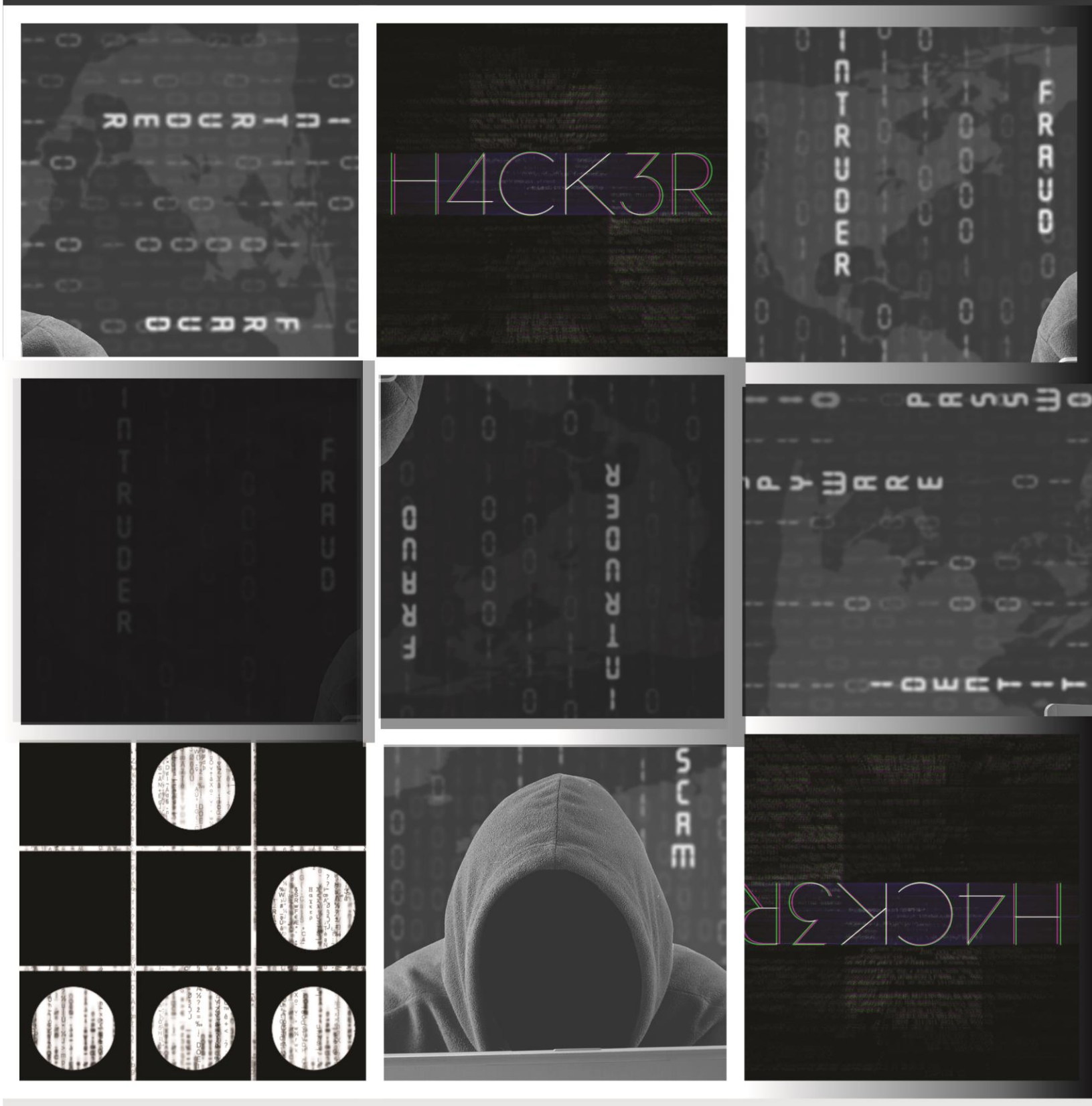
https://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html

Wired Magazine:

http://www.wired.com/2014/10/russian-sandworm-hack-isight/

http://www.wired.com/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon/

http://www.wired.com/2014/03/quantum/



ICIT | Institute for Critical Infrastructure Technology