



Threats on the Horizon:

The Rise of the Advanced Persistent Threat

APTs Then and Now

APT technology, has evolved at a Moore's Law clip since magician Nevil Maskelyne hacked a public demonstration of apparently secure wireless telegraphy technology in 1903, sending insulting Morse code messages through an auditorium's projector.² Since the dawn of the computer age, people have used *advanced* software to *target* specific companies or individuals in an *attack* designed to either damage or steal data. What makes today's APTs unique and frightening are the sophistication of the malware, the vectors they're choosing for attack and the perseverance with which they're going after their targets.

In the following whitepaper, we're going to examine:

- The history of Advanced Persistent Threats (APTs)
- Fast facts and figures
- The groups behind these types of attacks
- How the attacks work
- How to protect against them

The Greatest Bad for the Greatest Number

Historically and even today, most cyber criminals attempt to infect as many systems as they can in order to destroy or steal data, make money or a

Key Points

- No companies and government agencies are immune to infiltration and data theft
- The international nature of global trade and commerce and the theft of trade secrets make businesses a popular choice for targeted attacks
- Threats come from sources across the globe

Objectives

- Understand what an Advanced Persistent Threat is, how they typically operate, and what steps an organization can take to protect itself

The Advanced Persistent Threat can be difficult to detect and protect against. Companies and organizations must be agile enough to respond to attack attempts and ready to react to an attack in progress. Ensuring employees are properly trained in watching for suspicious activity or events is critical to ensuring your confidential information remains secure.

combination of all three. It's a numbers game to them. To infect those systems, they employ any number of deceptive practices such as directing people to a malicious Website where malware is silently installed on a user's system. Or they might send spam email with a malicious attachment that infects a user's system as soon as they click on it. Regardless of the methods they use to grow their infected user base, it's a random, scattershot approach at best. And that approach makes it fairly easy for network security vendors to quickly identify vulnerabilities and push out protective signatures to their customers in order to guard against them and, in many cases, future iterations of the malware.

Origins of the Term

The US Air Force is generally credited with coining the phrase Advanced Persistent Threat. Mike Cloppert with Lockheed Martin said, "I first heard this term used by the USAF's 8th Air Force in a small meeting room in 2006... I give them credit for coining this term, which is any sophisticated adversary engaged in information warfare in support of long-term strategic goals."

Zeroing in on the Problem

Where things get tricky is when a vulnerability, such as a zero-day, is discovered but isn't widely made available, or an exploit has been patched but hasn't been widely updated by businesses and computer users. A zero-day is an undiscovered vulnerability in an existing computer application. Many zero-days today are sold on the black market to the highest bidder. In March 2012, for example, *Forbes* reported an iOS zero-day was selling for as much as \$250,000³. With this kind of buy-in for a seat at the table, it's no surprise to learn that among the entities that can afford to drop six figures on a zero-day, or hire a team of internal hackers to find them, are governments.

Playing with Fire

A low-profile zero day combined with social engineering, such as a spear phishing attack, is highly combustible. Once a hacker has penetrated a target's systems, they then use other attack methods to move throughout their target's infrastructure to steal or destroy data. In June 2012 for example, the *New York Times* published a story⁴ revealing the United States, with the assistance of an ally, had actually teamed up to develop Stuxnet, an APT that was successfully used to disrupt Iran's nuclear enrichment facilities.

Beyond destroying data, APTs are also widely used to exfiltrate data. For example, it was reported in May of this year that Chinese hackers had stolen designs for more than two dozen major U.S. weapons systems.

On May 31st, 2013 Daniel Ives, an analyst at FBR Capital Markets told *CNBC*⁵, "There's more potential data being lost in this country than we saw throughout the whole Cold War. It may not be physical, you may not be able to see it, but the amount of data being taken is the equivalent of cargo ships docking on our shore and leaving with our goods." He goes on to warn that the scope of these types of attacks is actually much larger than anyone realizes and suggests, "There [are] not 50 companies compromised. There are thousands of companies compromised. Actively, right now."

Staying Under the Radar

Even more concerning, APTs don't have a typical attack pattern. Once malware is in place on a target computer, it can lay dormant for months or years at a time. This becomes especially concerning when thinking about APTs from a national infrastructure standpoint. It's very possible that a site, such as a major city power grid, is compromised right now and the malware is just waiting for someone to press a button. And if that's possible, then it's not a stretch to envision every municipal grid in the western world compromised by

the same malware. If this doomsday scenario sounds farfetched, it was actually first reported by *The Wall Street Journal* back in April 2009⁶.

Hard to Pin Down

As much as we know about APTs and their origins, the truth is that it's very difficult to pinpoint the origin of an attack. For example, a hacker in Denmark could purchase a Chinese language software development kit to build a piece of malware and include text references to particular Chinese military organizations. From there, they could host the malware on a Website in Russia, but route the attack so that it looks like it's originating from China. From there, the hacker could launch an attack at another nation. Once the attack is discovered, forensic analysis would see the code was written in Chinese and that the attack originated from a Chinese IP address.

It's Mainly Nations that are Doing it

There are only a few groups globally that have the capability, skills, funding and infrastructure to launch an APT:

China: China's information warfare and electronic intelligence gathering has been brought to light recently. Mandiant released a comprehensive report on one of China's military organizations, the People's Liberation Army Unit 61398, or what they labeled as APT1⁷. APT1 is one of perhaps two dozen such outfits based out of China. It appears that China's APT interests are quite comprehensive: they target foreign corporations and governments in order to steal both state and trade secrets. Attacks on media outlets in order to track down domestic dissidents and whistle blowers have also been attributed to Chinese APT teams. The Chinese government emphatically denies any involvement in APT operations or cyber warfare in general.

Russia: It is clear Russia maintains the ability to

launch sophisticated attacks, but as of yet there is no smoking gun linking the Russian government with a specific attack. Attacks on the Internet infrastructure of Estonia in 2007 were attributed by sources to have Russian origins. It is safe to assume, based on Russia's known abilities to produce some of the world's best computer crackers, that Russia's Federal Security Service (FSB) has a team or teams in place to monitor and infiltrate organizations or nations it deems worthy of observation.

United States: The United States has an extensive "cyber army." The United States Cyber Command (USCYBERCOM) is part of the US Strategic Command and was established in 2010.

Shortly after it was revealed that Stuxnet was the brainchild of the United States, two other worms were discovered, known as Duqu and Flame. Duqu is believed to be related to Stuxnet, but was used to monitor infected systems and report both system information and keystrokes entered. Flame was a much more advanced piece of malware and had the ability to take screenshots, record audio through an infected machine's microphone, steal documents and technical drawings, log keystrokes and monitor network traffic. Flame also incorporated a rather novel "kill" ability, which when activated would delete all traces of the malware's infection on its target system. The *Washington Post* reported⁹ in June 2012 that Flame was developed by the Central Intelligence Agency and the National Security Agency, with assistance from an ally. Current US APT development capabilities are unknown, but it is safe to speculate that they are very advanced and difficult to detect.

Other Nations: Other countries may also have developed their own cyber armies and APT groups. Little is known about the capabilities of the rest of the G20 nations and states such as Syria, North Korea,

Fast Facts and Figures

Solution Brief: Threats on the Horizon - The Rise of the Advanced Persistent Threat

In the first half of 2013, companies reported:



Unsuccessful Hacking Attempts:

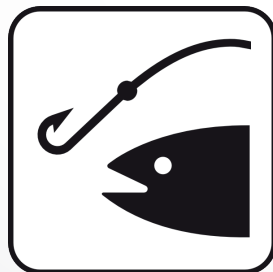
142 MILLION

Number of times a user is tricked into trying to visit a potentially malicious site:



3.14 BILLION

Blocked
Phishing
Emails:



4.45 MILLION

Common Phishing
Themes:

Account Statements

Online Account
Suspension

Infected
Documents

Verification of
Account Info

Social Media Alerts



Top Vulnerabilities and Tools
Used in an Attempted Attack

1. ZmEu.Vulnerability.Scanner
2. HTTP.Chunk.Overflow
3. HTTP.Negative.Data.Length
4. ESVA.CGI.Argument.Injection
5. PHP.CGI.Argument.Injection
6. Wmware.Server.Directory.Traversal
7. MS.IE.DHTML.Script.Function.Memory.Corruption
8. Cisco.IOS.HTTP.Command.Execution
9. Joomla.JCE.Extension.Remote.File.Upload
10. MS.DCERPC.NETAPI32.Buffer.Overflow

Note: Data collected from FortiGate devices located around the world and reporting incidents to FortiGuard from Dec 1/12 - Jun 1/13

Iran and other nations in the Middle East. It's safe to say that most of these nations have at the very least researched the option.

The Stages of an Attack

There are many steps that must be taken in order for an APT attack to be successful.

Choosing a Target: The attacker first determines whom they wish to infiltrate and what they wish to steal. Is the attacker after confidential financial data? Source code? Technical drawings? All of these help determine a specific target.

Target Research: Once a target has been selected, the attacker will do extensive background research on his target. By combing through search engines, employee social network activity, public email and phone directories and other sources of easily obtained data, the attacker can build a profile as well as a detailed list of other potential human targets inside an organization.

Penetration: After a target has been acquired, the attacker typically creates a customized phishing email in the hope that their target will open an attachment that contains an exploit that allows the attacker to plant remote access malware on the target's computer.

Elevation of Privileges: Once the attacker has gained a foothold inside a target's network, an attempt is made to exploit vulnerabilities on other internal computers to gain further access on the network. Once access has been gained, the attacker can then move deeper into the target's network.

Internal Network Movement: If the attacker was successful in gaining further access inside the network, they can then expand their control to other machines on the network and compromise other

computers and servers, allowing them to access data throughout the network.

Data Theft: Once network access has been achieved, data can be easily stolen. Passwords, files, databases, email accounts and other potentially valuable data can all be sent back to the attacker.

Maintenance and Administration: Even after the requisite data has been stolen, an attacker may decide to remain present on the target's network. This requires vigilance on the attacker's part in order to evade detection and maintain surveillance on the target's data assets to ensure further data can be stolen.

The APT Toolkit

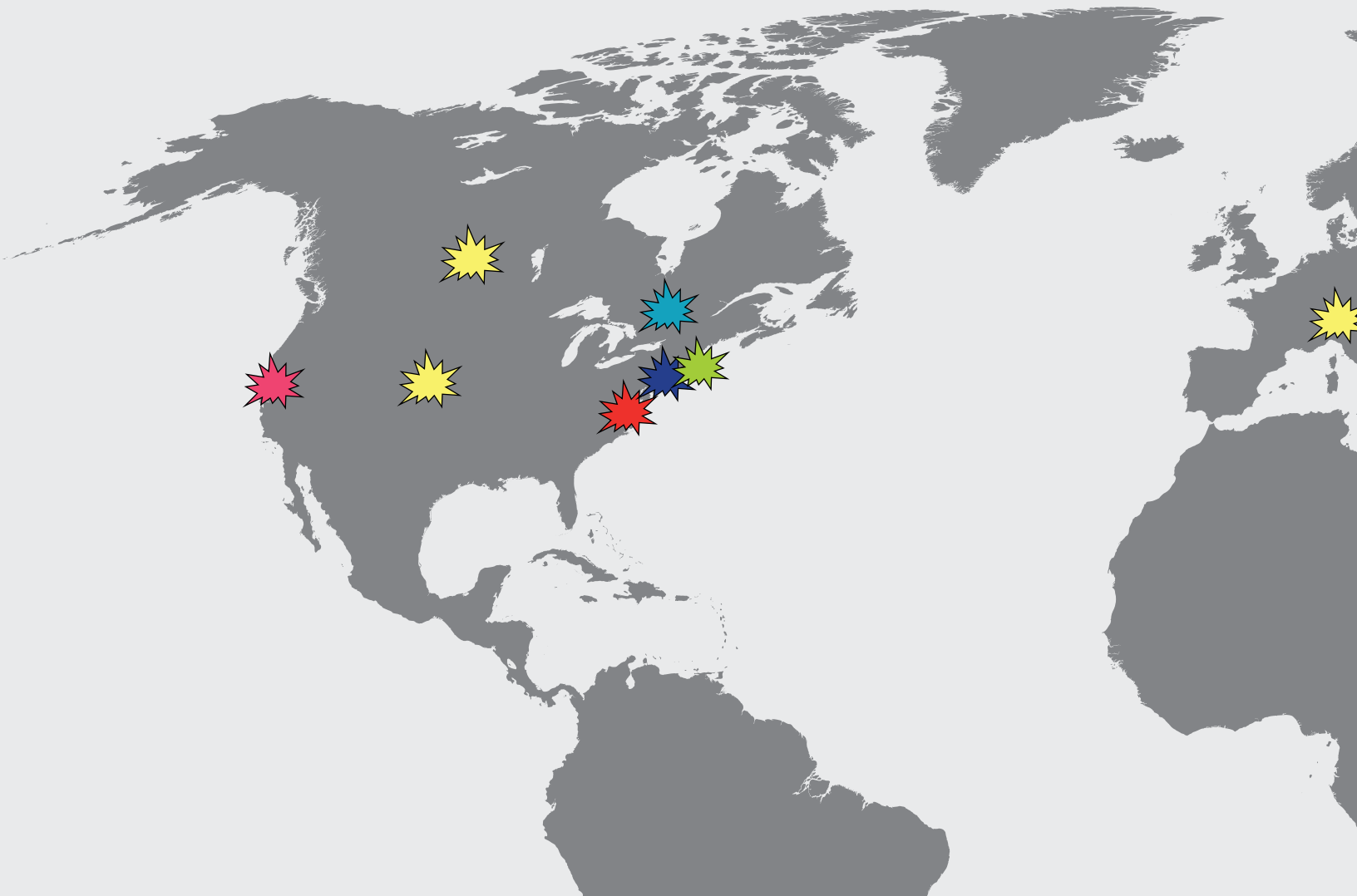
An attacker has a substantial arsenal of tools at the ready in order to launch and maintain their attack.

Malware: Some hackers use specially crafted malware to exploit a victim's computer, while others use "off the shelf" malware tools that are easily obtainable online and on many underground hacking forums.

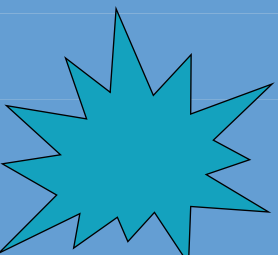
Social Engineering: A key component in any attack is the ability to make a human target believe an attack is coming from a trusted source. Using previously obtained research, an attacker may craft very specific spear-phishing emails with seemingly innocuous attachments that the target will likely open. Links to Web pages with malicious code embedded (known as a watering hole attack), spreadsheets and other documents such as text files and PDF files that take advantage of exploits in order to execute malicious software are also oftentimes used.

Zero-Day and Other Exploits: As mentioned earlier, a zero-day exploit is a vulnerability in a software product that allows an attacker to execute unintended code or

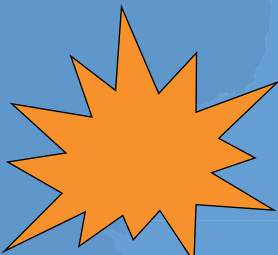
Famous APT Incidents Around



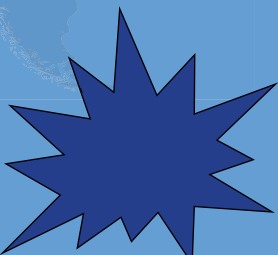
U.S. Department of Defense: On May 27, 2013, The *Washington Post* reported that Chinese hackers broke into Department of Defense computers and stole designs for several weapons systems.¹⁰ These systems included anti-missile and ballistic missile defense systems. Aircraft and ship designs were also taken. As is a hallmark to an ATA, it was discovered that the theft took place some time ago before the breach was discovered. Earlier in the year, the Defense Science Board, which is made up of government and civilian experts, concluded the U.S. is not prepared for a full-scale cyber war.



Government of Canada: In January of 2011, an attack on multiple Canadian Government agencies was discovered.¹¹ The initial attack focused on carefully-crafted phishing emails that appeared to come from other government employees. The Treasury Board, a Department of National Defense advisory agency and the Federal Department of Finance were among the agencies targeted. The true amount of information taken isn't known, but forensic investigation of the attacks led to IP addresses located inside China.

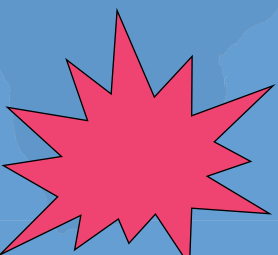
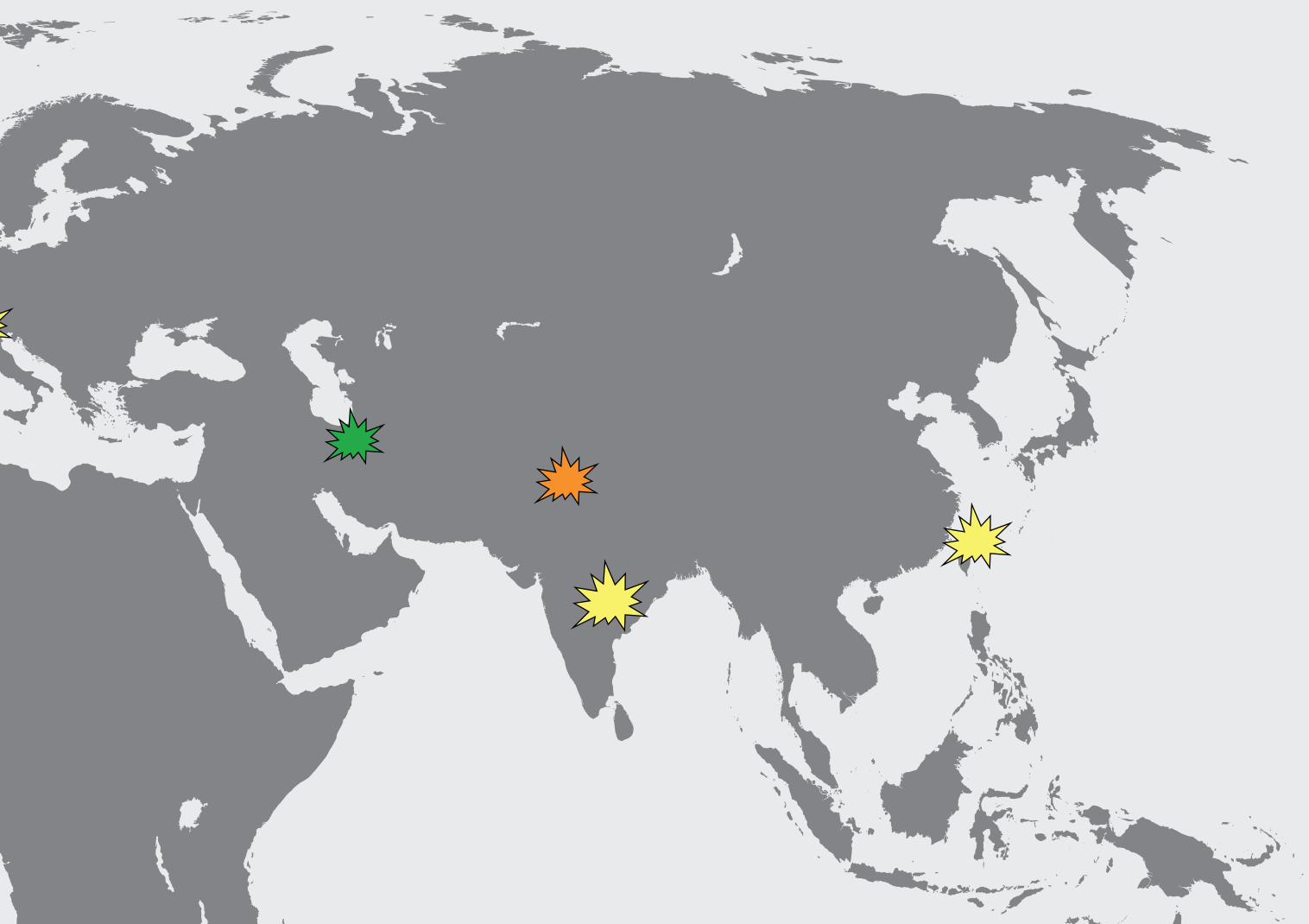


Government of Pakistan: On May 21, 2013, Information Week reported a multi-year APT was launched against the Pakistani government and global mining, automotive, military and engineering businesses.¹² It's suggested that the attacks originated from India and started sometime in 2010 (and perhaps earlier) and was used primarily for surveillance purposes. This particular attack was quite large, consisting of more than 600 domains and 800 pieces of malware, some of which were customized for specific targets.

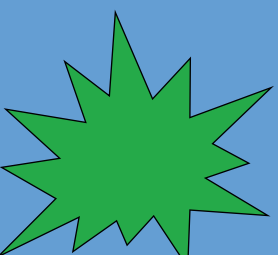


New York Times: In January of 2013, the *New York Times* published a report claiming Chinese hackers, who were suspected to be state-sponsored, had infiltrated their networks.¹³ The attack appeared to be the result of an investigation that found relatives of China's then Prime Minister, had accumulated a massive fortune through extensive dealings. The initial attack is believed to have been launched by a targeted spear-phishing campaign, which allowed the attackers to infiltrate their networks and plant remote access tools in order to facilitate further access. The attacks seem to have been designed to search out emails and documents related to the NYT's story in the hopes of discovering their sources. The NYT claims that the Chinese were unsuccessful in their attacks and were allowed to continue their operations while being closely monitored. After the Times' report, *Bloomberg LP*, *The Wall Street Journal* and the *Washington Post* all reported that they were also targeted by what they believed to be Chinese attackers.

the World



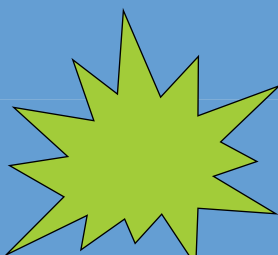
Operation Aurora: In January of 2010, Google revealed¹⁴ that it had been the victim of a highly orchestrated and planned attack by a group that was labeled by McAfee as the Elderwood Group. Google believes the attack started in mid-2009 and persisted until the end of the year. Google claimed that valuable intellectual property was stolen and attempts were made to access the Google Mail accounts of suspected Chinese dissidents. Some of the almost three dozen purported targets of Operation Aurora included Adobe, Juniper Networks, Symantec and Rackspace.



Operation Olympic Games: It is well known that Iran has made it a strategic objective to develop nuclear arms capabilities. While the United States has never publicly acknowledged the operation, it appears that in 2006, former President George W. Bush was presented with a plan to launch a cyber attack on Iran's main uranium enrichment facility in order to disrupt their nuclear program. It is believed that the United States developed this attack to prevent Israel from launching a military strike on the facility, which may have led to significant political destabilization in the Middle East. The Stuxnet worm is believed to be the initial worm that was used to attack Iranian industrial control machinery being used to enrich uranium. Other pieces of malware such as Flame, Gauss and Duqu may have been developed under Operation Olympic Games and have been used to spy on targets throughout the Middle East.



Operation Shady RAT: In 2011, McAfee released a report¹⁵ stating that starting in 2006 an extensive attack campaign was launched on over 70 different companies, government agencies and organizations in an attempt to monitor and steal information. Targets included government organizations in the United States, Canada, India and Taiwan, various industries such as defense contractors, electronics manufacturers, energy companies and computer security groups. Other targets included global organizations such as the International Monetary Fund, think tanks and the International Olympic Committee.



RSA Attack: In March 2011, RSA, the security division of EMC, announced they were the victims of a sophisticated attack that breached their network and allowed the attacker to reportedly exfiltrate data relating to RSA's SecureID two-factor authentication token system. It was reported soon after that Lockheed Martin, Northrop Grumman and L-3 Communications may have been attacked using information obtained in the RSA breach. RSA offered to replace every SecureID token in use, some 40 million of them, if requested by customers. The source of the attacks on RSA has never been conclusively proven.

ADVANCED

1

THREAT
PRODU

Data Link

Custom-Built malware is produced for a targeted organization using Zero-Day exploits. Government and Corporate networks are prime targets for the sensitive information they contain.

4

MISSION
EXECUTION

The infected systems can now "phone home" and intelligently subvert other networks using its stolen credentials.

NEXT STEPS

2nd Stage Attack

Espionage

Blackmail

ADVANCED PERSISTENT THREATS (APTs) - A TIMELINE

AT
ACTION

duced for the
ro-Day and
nt and
ets due
ntain.

2

RECON



Government
Officials



Corporate C-Level
Admin Access



3

LAUNCH
ATTACK

SOCIAL ENGINEERING

Targeted Phishing Emails

Malicious Links

Social Media Attack



gain control of a target computer. These exploits are usually included in spear-phishing and watering hole attacks. In some cases, exploits are used that have recently been fixed by vendors but have not yet been patched by the target organization. Both have been shown to be very successful in attacks.

Insiders and Recruits: Sometimes an attacker will recruit an insider to assist in launching an attack. In the case of Stuxnet, it is believed an insider sympathetic to the attacker's goals was recruited to launch the initial attack by plugging in a specially created USB key that contained the malware used in the attack. This is often the only way an attacker can reach a target computer that is not connected to the Internet (or what's known as an air gapped network).

Forged and Fake Certificates: An attacker may attempt to forge or fake an SSL certificate in order to get a victim to visit a page that pretends to be from a safe site. In 2011, the certificate authority Comodo was compromised and fake certificates were issued for popular sites such as Google, Skype and Yahoo.

The Critical Infrastructure Connection

A 35-page report by U.S. Congressmen, Edward J. Markey (D-MA) and Henry A. Waxman (D-CA) titled, "Electric Grid Vulnerability: Industry Responses Reveal Security Gap" s and published on May 21, 2013, revealed some interesting statistics.¹⁶ 115 energy companies were asked a series of questions about cyber security. More than a dozen replied that they were under almost continual assault from Internet-based attacks. The report concluded that Infiltration by an APT group could lead to significant damage or disruption to power distribution, water treatment plants, dams, traffic control systems, oil and gas pipelines and other infrastructure. The report

suggests that a state-sponsored APT group could penetrate an infrastructure asset and hide malware that could disrupt those systems.

The rationales for these attacks are likely twofold: another nation may want to gather intelligence on the critical infrastructure on a target, and they may want to plant hidden "kill switches" to function as a weapon in the unlikely scenario of a military conflict.

Devices are Everywhere

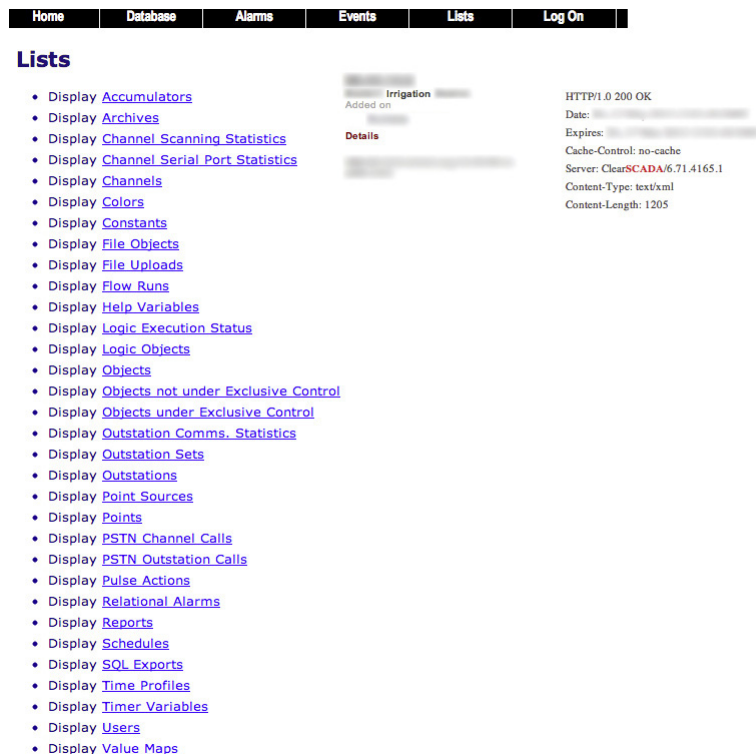
As companies looked to better manage their infrastructure, they turned to the Internet because the technology offered the ability to significantly reduce costs and improve efficiencies. For example, in a rural area, there might be three sewage pumping stations within a 200 mile radius. Logistically, each plant needed one full-time technician to manage day-to-day operations. By tapping the Internet, it was soon discovered that those same three technicians could be easily condensed into one remote worker who could manage all three sites using a notebook computer. However, that remote notebook is now the weakest chain in the armor and vulnerable to attacks. Online search tools are now available that allows an attacker to search wide swaths of the public IP address space looking for telltale signatures of connected machinery and devices.

Many of these devices were installed with little to no thought of security and will allow complete access to the device if connected to it in the right way. For example, connecting via Telnet to a specific port may grant access to a command shell.

Even devices that are protected by a login and password are not secure. Recent leaks of millions of passwords by companies have given attackers significant insight into how people choose passwords. Many of these connected devices allow unlimited

attempts to enter a correct login and password. An attacker only needs to write a script to continually throw passwords at the device in the hopes that one will grant access.

What follows are a few real world examples of Canadian infrastructure companies that have incredibly weak security protecting them. These were found using an online search tool that's easily found on the Internet.



This is a screenshot of an irrigation system. This screen provides a significant wealth of information for an attacker. Not only do we know the software and version that this device is running (ClearSCADA 6.71.4165.1), but we can modify a number of settings, read reports, look at flow rates and add users. While an attacker could spend time researching ClearSCADA for any known vulnerabilities or exploits to gain access, it's clearly not needed: we have full access to the device already.



This is a screenshot for an “information service.” Among the revealing information here is the type of server it's running on. In this case, it's a FreeBSD server running Apache 2.2.17. As of this writing, there are known

Denial of Service and Privilege Escalation vulnerabilities in this version of Apache. It is also running SSL and Python. All of this information would be very useful in planning an attack.

The screenshot shows the Lantronix Network Settings web interface. The top header includes the Lantronix logo and fields for Firmware Version and MAC Address. A left sidebar contains a menu with options: Network, Server, Serial Tunnel, Hostlist, Channel 1, Serial Settings, Connection, Apply Settings, and Apply Defaults. The main content area is titled 'Network Settings' and contains two sections: 'IP Configuration' and 'Ethernet Configuration'. In the 'IP Configuration' section, 'Network Mode' is set to 'Wired Only'. There are radio buttons for 'Obtain IP address automatically' and 'Use the following IP configuration:'. Under 'Auto Configuration Methods', there are radio buttons for 'Enable' and 'Disable' for BOOTP, DHCP, and AutoIP. Below these are input fields for 'DHCP Host Name', 'IP Address', 'Subnet Mask', 'Default Gateway', and 'DNS Server'. The 'Ethernet Configuration' section has a checked 'Auto Negotiate' checkbox, and radio buttons for 'Speed' (100 Mbps, 10 Mbps) and 'Duplex' (Full, Half). An 'OK' button is at the bottom right.

This is a screenshot from a Lantronix UDS1100 External Device Server. Full access to the device was given with no password required. This device is designed to “connect, manage and control just about any piece of equipment with a serial port from virtually anywhere...” It’s easy to imagine what someone with nefarious intent might be able to do once they’ve gained access.

The screenshot shows the Schneider Electric login page. At the top is the Schneider Electric logo. Below it is a navigation bar with links: Home, Database, Alarms, Events, Lists, and Log On. The main area contains a 'Username:' label followed by a text input field, a 'Password:' label followed by a text input field, and a 'Log On' button. At the bottom, there is a grey bar with the text 'All rights reserved.'

This is a screenshot from Telvent Canada (now Schneider Electric), which manufactures switches and other types of networked products serving the oil and gas industry. China’s APT1 group is alleged to have hacked into many of their systems. While APT1’s intent isn’t known, a large number of devices still remain online and ready for access.

Summary

IP: [REDACTED]
 Location: [REDACTED]
 Latitude/Longitude: [REDACTED]

FTP

220 01-32-48-09W5 SCADA (00:0F:92:00:73:51) FTP server ready.
 214- The following commands are recognized (* =>s unimplemented).
 USER PORT STOR MSAM* RNTD NLST MKD CDUP
 PASS PASV APPE MRSQ* ABOR SITE XMKD XCUP
 ACCT* TYPE MLFL* MRCP* DELE SYST RMD STOU
 SMNT* STRU MAIL* ALLO CWD STAT XRM D SIZE
 REIN* MODE MSND* REST XCWD HELP PWD MDTM
 QUIT RETR MSOM* RNFR LIST NOOP XPWD

HTTP

Server: httpd-ssl-1.0.0
 Cache-Control: no-cache,no-store
 WWW-Authenticate: Basic realm="WebUI"
 Content-Type: text/html; charset=%s

SMB

Anonymous login successful

Sharename Type Comment

 Error returning browse list:
 session request to [REDACTED]
 session request to [REDACTED]
 Anonymous login successful

Server Comment

 SCADA-1

Workgroup Master

 WORKGROUP SCADA-1

NetBIOS

NetBIOS Response
 Servername: SCADA-1
 MAC: [REDACTED]

Names:
 SCADA-1 <0x0>
 WORKGROUP <0x0>
 SCADA-1 <0x20>
 WORKGROUP <0x1c>
 WORKGROUP <0x1d>
 MSBROWSE <0x1>

This device is a virtual buffet of various services and technologies available to penetrate. In this case, this server was a gateway to a number of PLC-controlled machines.

Defending Against an Attack

Just as an APT requires multiple attack layers to be successful, companies wishing to protect themselves from falling prey to an APT must implement a defense strategy that incorporates multiple layers of protection. It is critical to understand that no single network security feature will stop an APT.

Security Partnerships: Attackers don't rest on their laurels and neither should an organization. It is essential that organizations ensure they expend resources to keep IT staff as up-to-date as possible on new threats and potential avenues of attack. Having a strong partnership with a security organization can provide up-to-date information and threat intelligence as well as clearly-defined escalation path when an incident is detected.

End User Education: attackers target end users because they find the greatest chance of success focusing their initial attacks there. Much like the

maxim of the bank robber, the attacker "goes where the money is." Educating end users on proper use of social media to prevent confidential information from becoming publicly available is one component. It's also critical to ensure employees who have access to sensitive information are specially trained to know how to deal with that data. Internal awareness training and regular testing by IT staff can help mitigate an attack.

Network Segregation: If there is no reason for an employee to have network access to particular resources that may contain sensitive data, then basic network segregation can help prevent lateral movement inside the network. By placing resources on segments that cannot be reached from end users, an organization can potentially prevent an attacker from moving beyond the initial foothold.

Web Filtering/IP Reputation: By using a solution that provides current IP reputation data and Web filtering rules, an organization may be able to stop some

attacks. For example, if the accounting team has no reason to visit Websites or IP addresses on the other side of the globe, creating filtering rules that prevent access to those sites can stymie certain attacks. By using an IP reputation service, an organization may be able to stop an attacker that has launched attacks on other organizations using the same network resources.

Whitelisting: Whitelisting can be used in multiple ways. For example, network whitelisting can be used to only allow certain internal traffic to reach other network resources. This can prevent an attacker from moving laterally inside a network. Network whitelists can also prevent a user from accessing any sites online that are not explicitly approved. Application whitelisting can be used to allow only a set list of applications from running on a computer, preventing all other software from running. This can prevent an attacker from running new programs on the target's computer.

Blacklisting: While a whitelist is a list of things that are explicitly allowed to execute or access resources, a blacklist explicitly blocks items on the list from accessing resources, sites or applications deemed unsafe.

Application Control: Employees are using Web services like Facebook, Twitter and Skype on a frequent basis today. While many companies have embraced and allow use of these platforms, complete and unfettered access to these technologies can expose your organization to a new generation of Web-based threats and malware. Application Control allows you to identify and control applications on your network, regardless of port, protocol or IP address. Using tools such as behavioural analysis, end-user association and application classification can identify and block potentially malicious applications and malware.

Cloud-based Sandboxing: As cloud-based

resources have evolved, the ability to “farm out” analysis and detection has become a good tool to detect potential threats. A cloud-based sandbox can execute unknown files and URLs in a controlled system that analyzes the behavior of those files and URLs to detect suspicious or anomalous activity.

Endpoint Control/AV: The old guard of client-based antivirus and antimalware solutions continues to provide a solid layer of defense against threats. While most client applications are unable to protect against zero-day attacks, they can block hackers who have used identical or similar attacks in the past.

Data Leak Prevention (DLP): By properly identifying sensitive data and implementing a DLP solution, an organization can prevent sensitive information from leaving a network. Data being used at the endpoint, data moving inside a network and data being stored can all be protected from theft or improper use by implementing a DLP solution.

Intrusion Prevention (IPS) / Intrusion Detection (IDS): By using a product that provides IPS and IDS, an organization can add another layer of traffic monitoring to watch for suspicious activity. A good IPS/IDS system will also alert IT staff of potential threats in progress.

Proactive Patching: A computer is only as secure as the software on it. It is essential for companies to deploy patches to their systems as quickly as possible. Attackers and cyber criminals waste no time integrating proof-of-concept code into their malware and exploit kits – in some cases exploits have been added to an exploit kit within hours or days of a patch being available. By delaying deployment of critical patches, an organization risks becoming vulnerable to attack. For business intelligence or in-house applications that require almost constant uptime, it's critical to keep test machines available to deploy

patches to and test mission critical applications without impacting the main network.

Restricting Administrative Rights: Some companies provide employees with local administrative rights in order to install drivers or software on an as-needed basis. This can be a double-edged sword. While it can reduce support calls and empower employees, it can also lead to easier access for attackers to install malware and remote access tools (also known as RATs) on a victim's computer. By limiting access to administrative rights whenever possible, an organization may be able to mitigate many attacks.

Network Access Control (NAC): NAC is a solution that can prevent computers on a network from accessing resources unless certain rules or policies are met. For example, if a computer hasn't been patched recently, NAC can place that computer on a segregated subnet that blocks access to resources until the machine has been properly patched.

Two-Factor Authentication: There are many forms of two-factor authentication available for end users. A free, in-depth report on the topic can be found here: http://www.fortinet.com/resource_center/solution_briefs/two-factor-authentication.html. By implementing two-factor authentication for remote users or users that require access to sensitive information, an organization can make it difficult for an attacker to take advantage of lost or stolen credentials, as the attacker would need to provide a second form of identification in order to gain network access. Commonly used two-factor authentication methods include the standard username and password plus a hardware- or software-based authentication token, which provides a one-time, time-sensitive password that must be entered when the username and password is presented to the authentication server.

USB Drive Restrictions: Many computers will

accept a USB thumb drive implicitly and execute any autorun applications located on the drive. A drive that has malicious code planted on it can be all an attacker needs to gain an initial foothold in a network. Limiting USB drive access to employees on an as-needed and justified basis is a good idea; banning them outright is even safer. If USB drive access is necessary, enabling a proper Group Policy to prevent a drive from autorunning is essential.

Limiting Access to Cloud-based File Sharing: Services such as Dropbox have enjoyed wide scale adoption both at home and in the workplace. As with USB drive access, it is important to limit access to these programs unless absolutely necessary. Cloud-based file sharing and syncing applications can make it trivial for an attacker to compromise a home computer and move malware into a corporate network when a user syncs the files they took home the night before.

Putting It All Together

It's clear that some groups will stop at nothing to get their hands on data they are interested in.

While there is no panacea that will eradicate the risk of APTs, organizations can put the odds in their favor by adopting a multi-layer and integrated defense strategy. While firewalls and intrusion prevention technologies are necessary, they are just the beginning of a comprehensive and effective security posture. That holistic strategy should also include antimalware technologies, combined with robust data leakage and role-based security policies. Meanwhile, in addition to antispyware and Web filtering solutions, enterprises also need to implement application control mechanisms in order to block APTs at various stages of the attack process.

References

- 1 <http://www.cbc.ca/news/canada/story/2010/05/17/cyber-security-hack-csis.html>
- 2 http://www.tomsitpro.com/articles/hackers-hacking_history-IT_security,5-39-2.html
- 3 <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>
- 4 <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html>
- 5 <http://www.cnn.com/id/100777039>
- 6 <http://news.investors.com/040109-472919-not-so-smart-grid.htm>
- 7 http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
- 8 http://www.stratcom.mil/factsheets/Cyber_Command/
- 9 http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware
- 10 http://articles.washingtonpost.com/2013-05-27/world/39554997_1_u-s-missile-defenses-weapons-combat-aircraft
- 11 <http://www.cbc.ca/news/politics/story/2011/02/16/pol-weston-hacking.html>
- 12 <http://www.informationweek.com/security/attacks/apt-attacks-trace-to-india-researcher-sa/240155225>
- 13 <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html>
- 14 <http://googleblog.blogspot.ca/2010/01/new-approach-to-china.html>
- 15 <http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>
- 16 http://markey.house.gov/sites/markey.house.gov/files/documents/Markey%20Grid%20Report_05.21.13.pdf



GLOBAL HEADQUARTERS

Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE

120 rue Albert Caquot
06560, Sophia Antipolis
France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE

300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE

Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480