Sponsored by F5 Networks

APT Dot Gov: Protecting Federal Systems from Advanced Threats

October 2011

A SANS Whitepaper

Written by: G. Mark Hardy

Introduction

It's 0247 local time in a nondescript government building. The young private sits attentively in front of her screen, watching the softly glowing display. A supervisor lazily smokes a cigarette and walks slowly behind the stations of dozens of cyber warriors. Suddenly, an alert appears on the monitor.

"Sir," the private says excitedly, a bit too loudly.

"Report," says the lieutenant.

"The objective has opened the attachment. We're in!"

The officer glances down at his cigarette and smiles. "Americans," he muses. "They make great cigarettes—and even better targets."

The above scenario is played out by organized, sponsored antagonists who've become adept at breaking into U.S. federal systems and staying hidden for long periods of time without detection. All the while, they're siphoning information.

In addition to protecting their intellectual property and secrets, many government agencies are entrusted with gathering, processing, and protecting sensitive information about citizens, patients and businesses. This information, along with the people and systems that process it, are increasingly becoming targets for exploitation through the emerging class of threat known as Advanced Persistent Threat (APT).

Why do attackers target federal systems? They seek intelligence, advantage and political gain. The possibilities are endless: intelligence about an opponent's military capabilities, movement of high-value individuals or national economic strategies; advantage by disabling or crippling sensors and systems or prelaunching a cyber attack as a prelude to kinetic warfare; and political gain by embarrassing a rival, manipulating public perception prior to a key election, or suppressing suspected dissident citizen groups.

One example of such an attack is Operation Shady RAT, reported in August 2011, which uncovered a five-year cyberspying operation inside U.S government agencies and their contractors' systems.[1] Some of these intrusions lasted over two years! Remember, experts determined the systems were all victims of the same attackers.

An example of APTs as a prelude to warfare is the Russia–Georgia conflict. In August 2008, Russian cyber attacks against the nation of Georgia's infrastructure preceded conventional warfare in which tanks rolled on South Ossetia and Abkhazia. Military campaigns require extensive planning; it is not unreasonable to presume Russian agents had been probing Georgian systems for months in advance, identifying weak points and vulnerabilities.

This paper describes advanced threats against federal and other governmental systems and provides advice on how to identify and protect the data at risk.

---

1 Dmitri Alperovitch, "Revealed: Operation Shady RAT," White Paper, McAfee , August 2011, www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

About APTs and Why They're Hard to Detect

Control of the remotely placed malware now rested with a young man who had recently been promoted to Sergeant after a series of successful penetrations against U.S. government targets.

Fluent in English, he quickly went to work, sending a series of commands to establish an untraceable path through more than a dozen compromised systems scattered throughout the globe. Once his tracks were certain to be obscured, he uploaded a custom rootkit designed to hide on the American server while quietly reporting back internal network configurations.

"No hurry," he thought. "Last time I was in for over a year before they detected me. By then, we had everything of value."

APTs are as much entities as techniques. Let's look at each component:

- **Advanced:** The attacker utilizes a range of tactics, procedures and tools to engage a target. In addition to basic hacker tools, attackers often craft custom software or methodologies to penetrate a specific target. These often involve zero-days and specially crafted messages that even discriminating employees would find believable.
- **Persistent:** The threat continues for long periods of time, unlike a typical "smash and grab" hack. By installing backdoors and monitoring tools or waiting patiently for specialized tools to work their way to their target, attackers seek to exfiltrate or modify information over months or even years.
- **Threat:** Opponents are motivated, focused, and active. Unlike malware that executes a defined function, this type of threat involves human planning, coordination and involvement. A typical attacker has significant financial resources, trained personnel and intelligence capabilities. APTs are launched with deliberate objectives.

These trademarks of an APT are exactly why they are so hard to detect and protect against. APTs also enjoy many tactical advantages, including lack of attribution, vulnerabilities in applications, confusion in systems, human nature and use of previously unknown threats.

Lack of Attribution

How does one defend against an attacker that lurks silently in the wire, waiting patiently for an opportune time to strike? Sun Tzu advised, "Know your enemy and know yourself." Self-knowledge rarely is sufficient to achieve success; so gathering information about your enemy is critical. After all, adversaries are targeting us, so why not learn something about them? Yet, remarkably, we know little for certain about most APT attackers due to the problem of *attribution*.

Although an attack may be traced to a particular IP address, that machine might have been used as a relay from another, which, in turn, could be a part of a long chain of compromised systems. Besides, knowing what machine did the deed really isn't the final goal. Without binding the identity of the human attacker to the exploit, most investigations become dead ends. No judge is going to sentence a computer to having half its memory chips removed or its clock speed reduced as punishment for a crime.

We can surmise the identity of an attacker based upon the information targeted, but proving it is difficult. For example, Operation Shady RAT also targeted the International Olympic Committee and three national Olympic Committees in the months prior to the 2008 Olympics, as well as the World Anti-Doping Agency. It is plausible to conclude that a certain government sponsored the attacks, but that government is certain to deny it. *Plausible deniability* is an important factor in any APT evolution. Thus, knowing what information or resources are entrusted to your agency and who can benefit by compromising them helps you predict who might come after your systems.

An allegedly leaked classified FBI report[2] estimated that the Chinese Red Army has deployed 180,000 cyberspies. It's also claimed that Microsoft was required to surrender its Microsoft Office source code as a precondition of doing business in China. With well over 90 percent of government PCs running Microsoft Windows and Office, this creates a perfect storm for the attacker. However, it is wrong to assume China is always the culprit. Such xenophobia or prejudices can lead to incorrect decisions about how and what to defend. Understanding the tools used in APT attacks allows defenders to choose countermeasures that can be effective against all foes.

There are many resources in the APT arsenal. Common hacking tools continue to work surprisingly well against average targets, so in most cases, fully patched and up-to-date registered software is the best defense. Many of the Windows systems compromised in Operation Shady RAT were months or even years behind in security patches.

Vulnerabilities in Applications

Exploiting insecure code is a primary attack vector for advanced threats. Many websites are an amalgamation of software and tools from different vendors so common vulnerabilities can extend across a large number of systems. It's nearly impossible for anyone to keep up with adjusting and patching the ever-increasing attack surface. In addition, auto updates of third-party components introduce changes without notice. These are not small patches. Microsoft's September 2011 auto-update for Windows XP and Office was over 40 million bytes of code! Patches and fixes are often bundled for the convenience of the vendor and can affect multiple issues and open new vulnerabilities. Yet, unless a vendor makes detailed technical notes available, the recipient doesn't know what other changes were introduced beyond the published reason for the patches—until they are installed and problems surface.

2 Gerald Posner, "China's Secret Cyberterrorism," The Daily Beast, January 12, 2010, www.thedailybeast.com/articles/2010/01/13/chinas-secret-cyber-terrorism.html

A common attack against web applications is Standard Query Language (SQL) injection. *SQL injection* involves embedding a SQL statement into an input field, where insecurely written code can execute that statement with the privileges of the web application. One technique of SQL injection is inserting an escape character (e.g., single quote) followed by a tautology (i.e., something that is always true) into an input field. For example, typing:

```
' or '1'='1' /* '
```

where a name input is expected could result in a SQL statement that is always true, and everything to the right of that input would be disregarded as a comment. However, simply stripping escape characters means names like *O'Brien* or contractions like *can't* will not work. Developers must know and use secure programming techniques to guard against this type of attack.

Easily Confused Systems

Some attacks try to disable a target rather than steal its information. Denial-of-Service (DOS) and Distributed Denial-of-Service (DDOS) attacks attempt to overload a target's system, causing it to become so preoccupied with responding to attacker-generated connection requests that the system can't serve legitimate users. By compromising a large number of machines (think unattended home PCs with high-speed connections and expired antivirus), an attacker can build a botnet and program it to launch coordinated attacks at a single target. Conventional systems might succumb to this, but agility with DNS updates and specialized tools offer strong resistance.

Manipulating Humans

One of the key entry points for APT, known as *spearphishing*, targets carbon-based network components (i.e., people) as compared to silicon-based attacks. Whereas phishing attempts to deceive unsuspecting victims into opening hostile attachments or revealing sensitive information, spearphishing targets specific individuals, luring them with information gathered through intelligence collection or clever guessing. For example, if an attacker knows a CIO has a young daughter at daycare, an e-mail that says, "Medical problem with your Daughter; Hospital Emergency Room report attached" might convince even the most wary executive to click on an infected link immediately in a moment of panic. Attackers gather this information about their targets in a variety of public venues, including social networking accounts, Internet postings, and subscription-based online groups and organizations.

Using Unknown Threats

The most powerful APT weapon is the zero-day (0-day) attack that can compromise a fully-patched system by exploiting a previously unknown vulnerability. This attack method gets its name from the amount of advance notice victims receive before being exploited. Zero-days are the Holy Grail of cyberweaponry. APT research teams that generate 0-days hold them very closely to keep the exploit going as long as possible. Clever hackers who discover them can find a black market for purchasers, some of whom are APT attackers. Once divulged or discovered, however, 0-day attacks can be recognized and patched; so, a 0-day can be used only once against a vigilant target.

The defender's challenge is to guard against all vulnerabilities, whereas the attacker needs to exploit only one. It's not a fair fight, and it's unlikely to become one. The odds of surviving an attack decrease if defenders protect the wrong things. Gartner estimated that 90 percent of security expenditures are used to protect the network; however, nearly 75 percent of attacks are against applications.[3] A proper defense may not prevent all attacks (particularly 0-days), but early detection and rapid response (see next section) can help control damage and isolate problems.

3 Theresa Lanowitz, "Now Is the Time for Security at the Application Level," Gartner Group, December 2005, www.gartner.com/DisplayDocument?id=487227

"Hmm," thought the sergeant. "Something's wrong."

The control channel for the remote software didn't seem to be working properly. He shifted to an alternate channel, which tunneled back through a port 80 connection that the remote system had opened hours earlier. That, too, wasn't working. The sergeant began to shift nervously in his seat. He had never heard of anyone failing so early in a reconnaissance mission against an American target. His superiors were not going to be pleased.

Government and contractor employees have a responsibility to protect American interests. Part of that responsibility involves fielding effective security measures to protect information. From a legal perspective, compliance ranks number one on most agencies' priority lists. FISMA, SOX, PCI, HIPAA, HI-TECH, and NERC CIP[4] are more than acronyms; they represent legal or industry requirements that do not offer an opt-out for disinterested parties. Information security is a component of each requirement.

There is a danger in seeking mere compliance, though. Compliant systems can and do get compromised all the time. To field a robust defense, you must go beyond the minimums, particularly with the rise of telecommuting and remote access into what was once a tightly controlled network. Whereas internal systems can be tightly managed to enforce policy through automatic updates, remote systems may be noncompliant, through which APTs find their way to internal systems.

Because common entry points for APT include applications and humans operating them, place strong protection around the end points and access points into the network. These protections should include the following strategies:

1. **Secure remote access.** Allowing unencrypted remote connections to internal servers is suicidal. Although there is an array of remote security access devices, Secure Socket Layer Virtual Private Networks (SSL VPNs) make remote access inexpensive because they require only a web browser to access. However, this is only a secure wrapper. A *dual-homed host* (a PC with two Internet connections—one to the VPN and one to the web) can become a secure conduit for an attacker. Thus, secure access requires more than just encrypted communications.

2. **Check and remediate end points.** To ensure users do not introduce dangers to their networks, organizations must go beyond SSL VPN tunnel protections and implement endpoint security checking. This technology can verify that a PC has up-to-date antivirus, screen for infected file uploads, and even protect against key loggers by implementing a secure virtual keyboard (software that displays an image of a randomized keyboard so that passwords can be entered through mouse clicks). In addition to performing prelogin checks, end point controls can mediate time-of-day access, restrict system access based on remote location, and even force the browser to erase its cache upon disconnect. Such tools reduce the likelihood that an attacker can spoof the identity of a valid user from an unknown location.

4 These acronyms stand for Federal Information Security Management Act, Sarbanes-Oxley, Payment Card Industry Data Security Standard, Health Insurance Portability and Accountability Act, Health Information Technology for Economic and Clinical Health Act, and North American Electric Reliability Corporation Critical Infrastructure Protection standards, respectively.

3. **Use DNSSEC signing services to improve security.** The domain name system (DNS) is the Internet's directory assistance. It translates human-readable names such as *www.sans.org* into their digital equivalent (e.g., 66.35.45.201). This lookup takes place automatically when a system requests a connection to another system. Attackers can compromise DNS servers to redirect traffic away from legitimate destinations. By relying on untrusted DNS information, applications become unwitting accomplices to attacks. Security researcher Dan Kaminsky points to DNS as the source of "authentication flaws that are implicated in over half of all data breaches."[5]

   So, what's the remedy? DNS Security Extensions (DNSSEC) provides a cryptographically signed and valid response that represents a chain of trust. Although the Bush administration mandated all federal agencies to implement DNSSEC by December 2009,[6] less than half have done so.[7] Earlier this year, GSA selected VeriSign to administer the .gov registry, which includes deploying DNSSEC.

4. **Focus on applications.** The application environment is highly complex and presents a number of vulnerabilities. Although network attacks typically occur at or below Layer 3, application and browser attacks take place at Layer 7. An attacker can use a one-two punch to launch a DOS attack to overload the network and, while responders focus on remediating that problem, release a second attack against web applications that may not be detected.

   The conventional wisdom of early computer security plans held that if you had an internal network, you needed a firewall to defend it. Early firewalls filtered traffic at the physical to network layers (Layers 1 to 3 in the OSI model). The result of successful defenses at these layers caused attackers to move their way up the stack. Today, the majority of attacks are at the application layer (Layer 7). With hundreds, potentially thousands of applications traversing the network, the task of protecting against these attack vectors grows significantly. If your agency utilizes web applications, consider a web application firewall appliance that protects against a range of web-based vulnerabilities such as buffer overflows, SQL injection and cross-site scripting. Web application firewalls are programmed to learn at line speed and adapt to threats and new vulnerabilities, which could help protect against many 0-day attacks based on their behaviors rather than merely signatures.

5 Dan Kaminsky, "DNS Filtering Threatens the Security and Stability of the Internet," May 26, 2011 blog entry, http://dankaminsky.com

6 Karen Evans, Memorandum for Chief Information Officers M-08-23, Executive Office of the President, August 22, 2008, www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf

7 FOSE Conference and Exhibition Workshop, "The Deployment Diaries: DNSSEC in U.S. Federal Systems and Beyond," July 20, 2011, http://fose.com/events/fose-2011/sessions/wednesday/the-deployment-diaries.aspx

To protect applications, organizations must implement systemic policy around their software development life cycle. However, the programming environment is characterized by rapid component changes to the web, application, and third-party products. The level of complexity for modern applications creates a number of problems. Ten years ago Bruce Schneier observed, "Complexity is the enemy of security,"[8] and time has proven him correct. Back then, he was referring to operating systems. Today, the complexity is also in application suites. Millions of lines of code developed over several years create an impossible security proposition. Newer applications developed without the discipline of secure coding practices will experience the same fate.

A good resource for development teams is Carnegie Mellon's Computer Emergency Response Team (CERT) secure coding standards[9] for many programming languages. The Open Web Application Security Project (OWASP) is another good resource, and its "Top Ten" critical web application security risks report is now included in the best practices the Defense Information System Agency (DISA), according to OWASP.[10]

5. **Think virtual.** With the push toward virtualization, agencies can place a web application firewall onto a virtual machine and deploy it in the cloud along with other applications. The Obama administration's Federal Cloud Computing Strategy[11] has also resulted in more use of cloud hosting among government agencies. Many of the services being migrated (e.g., e-mail) are web applications. The Federal Information Security Management Act (FISMA) requires vulnerability and security event monitoring, logging and reporting, which means government agencies require more web application protection. Web application firewall technology does this well and can help protect the next generation of government systems and information.

6. **Educate users.** User education remains the last line of defense against technology failures and compromises. The Department of Homeland Security (DHS) has trademarked the phrase, "If You See Something, Say Something™" as part of their awareness campaign about terrorism and violent crime. The same motto can be useful for government networks.

   Most people want to do the right thing, but when it comes to security, most people are bad guessers. Invest in user education and training. Utilize awareness resources to raise people's level of understanding. Conduct periodic tests using social engineering (persons using a pretext to convince legitimate users to do something that compromises security.) Assist your security staff in earning industry certifications that document a level of skill and comprehension. Make every employee part of your front-line defense. Teach employees to stop and ask if something doesn't seem right. By combining technology solutions with education, you can field a robust defense against APTs and, ideally, drive the cost of compromising a system higher than the value of is the information being sought.

---

8 Kim Zetter, "Three Minutes With Security Expert Bruce Schneier," PC World, September 28, 2001, www.schneier.com/news-038.html

9 www.securecoding.cert.org/.

10 www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

11 Vivek Kundra, "Federal Cloud Computing Strategy," The White House, February 8, 2011, www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf

Conclusions

In 1990, Bill Cheswick described early network security efforts as "a sort of crunchy shell around a soft, chewy center."[12] Twenty years later, we wonder what progress has been made, especially when an Army private was allegedly able to download volumes of classified Department of Defense (DoD) information and pass it to WikiLeaks. That private described DoD security as an environment of "weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis … a perfect storm."[13]

We are still poorly equipped to defend against internal attacks. Technology can do only so much; and government agencies cannot solve security issues by changing user behavior. A popular hacker t-shirt with "Social Engineer" on the front says, "Because there is no patch for human stupidity" on the back. It takes only one person to compromise a large network. The RSA breach was instigated by a single employee who opened an infected Excel spreadsheet.[14] HBGary Federal was hacked with a SQL injection attack followed by social engineering of an employee.[15] The thumb drive attack against the military that spawned Operation BUCKSHOT YANKEE succeeded because it exploited users' desire for convenience.[16]

Technology and user education are necessary but not sufficient to counter the emerging threat. Government leaders need to address emerging threats with flexible policies that address internal human and technological risks. As well, security, compliance and defense teams need to understand their adversaries, who continue to advance their attack methodologies. New attack vectors are faster, more dangerous and omnipresent. Combating them requires newer, more sophisticated defenses that can automatically respond and adapt to threat vectors in real time.

12 Bill Cheswick, "The Design of a Secure Internet Gateway," AT&T Bell Laboratories, April 1990, www.cheswick.com/ches/papers/gateway.pdf

13 Evan Hansen, "Manning-Lamo Chat Logs Revealed," Wired.com, July 13, 2011, log entry at 02:17:56 PM, www.wired.com/threatlevel/2011/07/manning-lamo-logs

14 Richard Adhikari, "RSA 'Explanation' Foggy About Breach Details," TechNews World, April 4, 2011, www.technewsworld.com/story/72203.html

15 Peter Bright, "Anonymous speaks: the inside story of the HBGary hack," Ars Technica, February 15, 2011, http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars

16 William J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," Foreign Affairs, September/October 2010, www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

About the Author

G. Mark Hardy serves as President of National Security Corporation. He has been providing cybersecurity expertise to government, military and commercial clients for over 25 years and is the author of over 100 articles and presentations. He serves on the National Science Foundation's CyberWATCH Advisory Board and is a recently retired Navy Captain. A graduate of Northwestern University, he holds a BS in computer science, a BA in mathematics, an MBA and a masters in strategic studies. Hardy is designated as a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM).

SANS would like to thank its sponsor:

www.f5.com