Sponsored by McAfee and Nitro Security


A SANS Whitepaper – December 2010

Written by Jonathan Pollet, CISSP, CAP, PCIP • Advisor: Eric Cole, PhD

APT–New and Evolving

Tips to Prevent an APT Attack

Detection and Assessment
People take for granted that electric power, water, telecommunications, gas supply, and other critical infrastructure systems are available to serve their everyday needs. Of all the utilities most people rely on, power is most critical because a significant power failure can disrupt all other utility services in the affected region.

Power generation, along with its transmission and distribution, relies on SCADA (Supervisory Control and Data Acquisition) systems for process management and control. SCADA applications share real-time generation, transmission and distribution data with regional load-balancing entities, marketing partners, trading teams, and other departments outside of the cloistered control network.

Given the criticality of their function to the well-being of society, SCADA systems were built to use proprietary protocols and operate in closed networks. However, over time, SCADA systems have evolved to using the same operating systems and TCP/IP protocols as those used in corporate IT networks. Now, these once-closed control systems are also exposed to the same advanced persistent threats (APTs) being experienced by other target-rich industries.

This was the case with the SQL Slammer worm that was released in 2004, which targeted Microsoft SQL Server. Even though SCADA systems were not the focus of the worm, SCADA systems using Microsoft components experienced immediate outages when Slammer hit. The same thing happened again with the Conflicker virus in 2009.

Most recently, Stuxnet in 2010 proved that worms with multiple attack vectors can target specific control systems. Before that, in January of 2008, CIA senior analyst Tom Donahue spoke at the SANS SCADA Summit and made it public that attackers have targeted computers that operate at power companies worldwide, causing at least one widespread power outage. In his statement at the conference, he said:

“We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands.”

This paper, the second in the SANS series1 on SCADA and utility control security, explains the advanced persistent threats being aimed at SCADA and utility control systems, followed by advanced measures to take against these threats.

1 www.sans.org/reading_room/analysts_program/NitroSecurity_Securing_Smarter_Grid.pdf
APT–New and Evolving

Threats today are advanced, automated, targeted persistent—thus gaining the classification of Advanced persistent threat (APT). Many of the recent well-known cyber attacks such as the Russia-Georgia conflict, Operation Aurora, GhostNet, and Stuxnet all utilize advanced, persistent attack methodologies.

Advanced persistent threats leverage the latest cyber security and espionage techniques to gain a foothold on a system and spread to the network. They are persistent because they leave behind back doors and rootkits that allow attackers to move effortlessly in and out of the system, restart malware that’s supposedly been erased, and hide from anti-malware tools on the system.

Earlier this year, the news covered at least three energy companies in the United States that were targets of a series of previously undisclosed cyber attacks that may have originated in China—attacks that were advanced, persistent and successful. In these cases, it was verified that proprietary information had been flowing out to computers overseas, including emails and large zipped-up data files. The foreign attackers were attempting to gain access to technical diagrams, schematics and process control real-time variables related to energy production. Other news articles reported targeted attacks on oil companies whereby the attackers were targeting valuable “bid data” detailing the quantity, value and location of oil discoveries worldwide.  

These recent attacks on utility companies are utilizing an entirely new methodology that goes beyond simply banging away at the firewall with automated bots. APT’s are well-planned, sophisticated, and involve custom malware that is virtually undetectable by legacy anti-virus technologies. In most cases, an APT can start small, but then the victim realizes while changing core administrator accounts that someone or something is changing them back. Any attempt to root out the malware or attacker is quickly foiled. Then the threat advances to the point where the user/administrator is no longer in control of the system.

Figure 1 shows the various internal subcomponents of most APT malware.
Figure 1 – Anatomy of Advanced Persistent Threat Malware

**APT Methodology**

Cyber attacks based on APT methodology typically leverage the following steps:

1. **Intelligence Gathering.** Advanced persistent threats make use of various public source intelligence-gathering techniques to research utility employees. In many cases, the initial intrusion is made through a spear-phishing email or social networking campaign that makes use of public information to target the attack on employees with strong credentials.

2. **Initial Attack Vector.** The initial infection is most commonly achieved through a phishing attack on these employees that sounds believable since the phisher seems to know a lot about the target. The initial contact comes in the form of email, or from the web (through infected search results, social networks, or infected/malicious websites). It’s important to note here that the authorized end point from inside the firewall makes the request to let in malware or attackers, or even give away network credentials.

Malicious insiders may also be part of the initial attack vector. It’s been further surmised that Stuxnet must have involved the use of insiders to target the specific Siemens system by knowing the codes it required. Stuxnet also involved a USB stick that an insider would need carry into the control room to access the servers physically and install it.
3. **Hide.** The APT malware or payload often hooks to known system services in an attempt to hide its presence behind those approved services. This allows the attacker to evade detection and also makes it difficult to determine if a system has been compromised. The malware usually contains command and control capabilities as well as the ability for the attacker to gain remote access to the compromised system again in the future, often referred to as a “back door.”

4. **Achieve Persistence.** Once the malware reaches the internal end point, it usually hooks or injects itself into known normal operating system executable or DLL (data link library) files that are always called upon by the system. Injecting itself into well-known system files not only allows the malware to hide, but also achieves persistence, since the common system executables/DLL files will be called upon when the desktop is rebooted.

5. **Escalate.** Once their presence is sustained on the network, APT attacks will escalate their privileges on the system and expand the attack footprint to other systems both on the enterprise IT network and into the control network.

6. **Setup Command Posts.** Setting up command and control drones is often achieved by deploying C&C (command and control) nodes. The local commanders on the network can be used to provide localized command and control capabilities deep within the targeted networks. These commanders have the ability to create drones, set up communications to external servers, and instruct drones on what specific systems to search for.

7. **Launch Internal Attacks.** In some cases, drones have been known to stay dormant for longer than 12 months while waiting to be awakened. The commanders use various short-form communications methods including Twitter, IRC, IM and HTTP-formatted messages to send and receive information. These communication methods to external servers are preferred because they are already typically allowed as outbound traffic.
8. **Locate Control Systems.** The attack leverages a local presence to extract useful information or locate mission critical systems such as building automation controls; security alarm systems; badge access systems; SCADA, distributed control systems, other process control systems, and anything else that can be useful to have remote command and control over. To do this, the drones perform many tasks, including:

a. Spreading the surface of the attack to other systems on the network.

b. Locating interesting data, such as corporate emails, sensitive documents, batch recipes, and any intellectual property that might be valuable.

c. Scanning known SCADA protocols and UDP and TCP ports to locate SCADA Data Historians, OPC (OLE for Process Control) Servers, Protocol Front-End Servers, HMI (Human Machine Interface) stations, or field embedded devices such as PLCs (Programmable Logic Controllers) and RTUs (Remote Terminal Units). Each SCADA protocol uses a unique port, making it easier for searching.

d. Extracting internal sensitive data, emails, and real-time SCADA tag values and sending the data (often encrypted over the above-mentioned channels) to external servers. The data extracted can be sold to other parties or used to aid in future targeted attacks, including attempts at sabotage and terrorism.

The typical APT attack methodology is depicted in Figure 2.

![Figure 2 – Advanced Persistent Threat Attack Methodology](image-url)
Stuxnet is an excellent example of how these new threats are aimed at utility control systems. Figure 3 dissects some of the major components of Stuxnet. There is still ongoing work by security researchers to peel back more layers and obtain a better understanding of this threat.

With Stuxnet, we know that the attacker was able to update the code remotely. Based on research and reverse engineering, the intent of the Stuxnet-injected PLC STL (Structured Text Language) code was to cause centrifuge motors to spin or rotate at much higher speeds than system operators intended, all while reporting back to the system operators that the centrifuge motors were at normal speeds. While the actual intent or target of the Stuxnet attack has not been proven, most cyber security researchers agree that slowly contaminating the nuclear enrichment process was one of the likely purposes of the virus.

Regardless of the actual purpose or intent of the Stuxnet virus, what is more important to the utility control system security community is the sophistication and capabilities represented in the malware framework. Stuxnet has proven that utilities need to step up defenses. The next section provides some helpful tips on how to prevent an APT attack.
Utilities need more than legacy firewalls and anti-malware to protect against APTs. They need advanced firewall and anti-malware capabilities, along with other integrated security and monitoring components. These include application whitelisting, vulnerability assessment, advanced host and network IPS/IDS, as well as security event logging and reporting. These expanding security and compliance components will ultimately need to fall under the management of a SIEM system in order to provide important situational awareness about compliance, system state and network traffic.

These and other controls are offered and explained in more detail, below:

1. **Assess public information on your organization and employees.** Processes and controls should be implemented to reduce and redact potentially useful public information for attackers. Open source data aggregation tools like Maltego can search across Google, user forums, and social networks (Facebook, Twitter, Myspace, Linkedin, etc.) to determine what information about the company is exposed for public view that external attackers can leverage for targeted attacks. Redact what data is possible to remove and make internal changes in cases where information cannot be removed.

2. **Start with training and awareness.** Because the initial intrusion for APT attacks tends to start with specially-crafted email or social network phishing or infection campaigns, security awareness training should include how to detect increasingly-sophisticated phishing and web-based malware installer tactics.

3. **Secure builds.** Best practices start with secure configuration of end points—including servers and systems used in control networks. All variants of APT attacks so far require access to a host system to progress the attack. Organizations like NIST (National Institute of Standards and Technology) offer clean builds of all Microsoft operating systems that can be downloaded for free from their site.

4. **Securely manage servers and end points.** End points need Unified Threat Management (UTM) that also includes browser application protections, malicious website blocking, application whitelisting, host IDS/IPS, and data leakage protections (device controls, email security, etc.).

---

3 [www.nist.gov/index.html](http://www.nist.gov/index.html)
5. **Block unapproved applications.** Application whitelisting allows only known and authorized applications to run on protected assets. This approach allows organizations to restrict unapproved programs from executing, regardless of whether they are initiated maliciously by an internal operator, by accident or through malware.

6. **Make use of host and network-based IDS/IPS.** Monitoring for both known and unknown threats should happen at the network and host layers. This includes use of advanced detection methods such as network intrusion detection systems (NIDS), intrusion protection system appliances (IPS), and host intrusion detection/protection systems (HIDS/HIPS). These technologies can detect malicious intent at the network and host layer, alert on the malicious activity, and, working with whitelisting, can actually prevent the malware from executing on the host computer.

7. **Manage firewalls.** Improve effectiveness of firewalls and access control list rules by reducing the number of open ports and communications to only those that are needed. Firewall and access control list rules should use deny-all rules, and then only open specific TCP and UDP ports to known entities on each side of the firewall. Because APT malware utilizes C&C (command and control) capabilities over normal channels, reduce the number and type of outbound communications allowed through. Then set up traffic monitoring.

8. **Segment secure zones.** Effective network segmentation between and within the corporate and process control networks will further reduce the ability for APT attacks to spread to critical control systems. In these environments, proper network segmentation can facilitate secure access to real-time utility information. SCADA systems can push data from control systems up to a secure historian inside a DMZ. External users can access the historian in the DMZ for their data rather than connecting into the control systems directly.

9. **Make use of all valuable system and security data.** Configuring SIEM tools to understand the secure zones described above, as well as critical assets (applications, logs) and authorized users and roles, can make preventing APT easier by facilitating each of the above steps. SIEM needs to hook into these and other security/operational processes, normalize, correlate and store data for reports, including fine-grained drill down of full event information when required.

As we follow the above recommendations, we should also never lose sight of passive, continuous detection capabilities that can alert us should those active defenses ever become comprised.
Figure 4 shows how the Blue Team or systems administrators can improve their ability to defend against APT threats by using advanced persistent diligence or APD.

**Figure 4 – Advanced Persistent Threat vs. Advanced Persistent Diligence**

By routinely checking public information sources, a systems administrator can often get notified ahead of time when there is chatter out in the Internet about a particular target. In the figure, APT is visualized against mechanisms that help maintain advanced persistent diligence.
Detection and Assessment

The best way to verify if there has been an APT compromise is to place a sniffer on the outbound side of the Internet firewall. Start to model what the normal destinations are for network traffic, and use a process of elimination to get to the point where suspicious outbound traffic can be further evaluated.

Network IDS/IPS, packet captures, network device logs, and internal host event log activity all provide security information that can be sorted and analyzed to get a better picture of an advanced attack inside the network. Make sure that all critical host systems have logging enabled and are configured to send log data to a secure SIEM on another server. This step is important because many times the attacker will be smart enough to clean up his or her tracks, thus making the attacker able to lock and unlock accounts leaving little trace on the system. While the logs on the local servers and workstations may look clean, transferring logs and correlating them with other event/security information on a secondary (SIEM) system would make it possible to uncover these discrepancies and launch an investigation.

When it comes to investigating APT incidents in the network, the following detection and remediation methods can help:

- **Watch for unauthorized changes being made to any system accounts.** If new domain controller accounts are added to the system, or if user accounts are randomly locked and then unlocked, or if the administrator account starts to be used when the administrators are clearly not on the network, then the APT attacker has already established a bidirectional link with the network.

- **Compare suspect systems against gold build.** APT malware also has a very effective way of hiding itself; so the best method to determine whether your systems are compromised is to compare the running state of the systems to a known clean system build. Analyze the server(s) or workstation(s) involved. Typically the logs will point out specific systems by IP address that are exporting data or used to escalate system privileges. Malware and C&C rootkits used by APT are usually not discovered by rootkit detectors because they hook into and hide behind known services. On Windows systems, commonly-used services files should be analyzed for size (to see if they’re too large) and number of instances (too many) on Windows systems.

Some common files to look for APT hiding behind include:
- `svchost.exe`
- `iexplore.exe`
- `iprinp.dll`
- `winzf32.dll`
• **Investigate further.** Before pulling the plug on the APT attack, it is important to understand its full spread and scope, including what critical systems and data are impacted. By using a combination of network and host investigative tools, determine how many instances of these files are running in memory, the size of those files, and what specific process identifiers (PIPs) are associated with them. Leverage both network and host-based tools to identify how far the infection has spread and where. This requires a passive approach to detect the presence of APT without affecting the performance of the system or alerting the attacker to the discovery techniques.

One passive method for detecting APT attacks is to capture traffic off the network and then analyze the traffic with offline network analysis tools. Then, compare the results to the configuration and running state of the servers and desktops in question.

Analyzing traffic in real-time is also just as important as post-analysis of network traffic offline after an infection, and can help control the spread of the infection as well. Network analysis tools such as SIEM systems can utilize security information from multiple sources to correlate and detect violations. Another good indicator of an abnormal state is when network sessions include source or destination systems that typically do not communicate with the SCADA or utility control systems.

Making use of SIEM-collected system, security and event information can help identify where else in the network that attack is attempting to spread. For example, if the attack is an attempt to open an HTTP session, the SIEM system can actively look for other instances of port 80 traffic originating from servers that are not supposed to be running web services.
Conclusion

Today, security attacks are common among utility-related companies; they are just not commonly reported or detected. However, Stuxnet proves that these attacks can be highly automated, sophisticated, targeted directly at SCADA and other utility control systems, and easily spread between utility control organizations.

Advanced Persistent Threats consist of many moving parts, all specifically designed to stay one step ahead of the many moving parts of our security controls and systems. Protection and remediation also includes many parts, including employee training, UTM for end points and critical servers, application whitelisting, segmentation, monitoring devices for changes, and monitoring network control channels and other network activity. Using centralized management or SIEM will then enable better prevention, detection, recovery and compliance by organizing and prioritizing system, security and monitoring data into actionable information.

These tools are mature and are standardizing in enterprise IT environments outside the utility sector, where best practices are also maturing. In addition, SCADA-specific standards and best practices are also emerging from NIST, NERC and other agencies. Tools, however, will need to be more effectively customized to continue to meet SCADA-specific logging and management demands to help control system operators gain better visibility into and between their corporate and control network traffic and applications.
Jonathan Pollet is founder and principal consultant of Red Tiger Security, a security consultancy and training firm focused on critical infrastructure organizations. He has held several positions, from engineer to operations director, at companies including PLCs Plus, Chevron and others. In the past, he founded PlantData Technologies for the industrial engineering sector and held VP positions at other industrial engineering services firms. He has written and presented extensively about SCADA security, including at Black Hat 2010, where a team from Red Tiger delivered findings that 38,753 vulnerabilities existed in 120 SCADA systems reviewed.
SANS would like to thank this paper’s sponsors

McAfee

nitrosecurity
## Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Oslo 2015</td>
<td>Oslo, NO</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS 2015</td>
<td>Orlando, FLUS</td>
<td>Apr 11, 2015 - Apr 18, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>RSA Conference 2015</td>
<td>San Francisco, CAUS</td>
<td>Apr 19, 2015 - Apr 22, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>Security Operations Center Summit &amp; Training</td>
<td>Washington, DCUS</td>
<td>Apr 24, 2015 - May 01, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS London 2015</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC401 London</td>
<td>London, GB</td>
<td>Apr 27, 2015 - May 02, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain 2015</td>
<td>Manama, BH</td>
<td>May 02, 2015 - May 07, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security West 2015</td>
<td>San Diego, CAUS</td>
<td>May 03, 2015 - May 12, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2015</td>
<td>Bangalore, IN</td>
<td>May 04, 2015 - May 16, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Europe 2015</td>
<td>Amsterdam, NL</td>
<td>May 05, 2015 - May 25, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS/NH-ISAC Healthcare Cybersecurity Summit</td>
<td>Atlanta, GAUS</td>
<td>May 12, 2015 - May 19, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Pen Test Austin 2015</td>
<td>Austin, TXUS</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Melbourne 2015</td>
<td>Melbourne, AU</td>
<td>May 18, 2015 - May 23, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS Security Training - Houston</td>
<td>Houston, TXUS</td>
<td>Jun 01, 2015 - Jun 05, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS ICS410 Vienna in Association with IAEA</td>
<td>Vienna, AT</td>
<td>Jun 06, 2015 - Jun 10, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dublin 2015</td>
<td>Dublin, IE</td>
<td>Jun 08, 2015 - Jun 13, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Houston 2015</td>
<td>Online TXUS</td>
<td>Mar 23, 2015 - Mar 28, 2015</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>