websense

FIVE ESSENTIALS FOR PROTECTING AGAINST ADVANCED PERSISTENT THREATS (APTS)

websense TRITON

Advanced persistent threats (APTs) have become a major concern for IT security professionals world-wide, and for good reason. Recent attacks have targeted a multitude of diverse companies. This paper clarifies the nature of APT risks and provides recommendations on how organizations can better protect themselves. More specifically, it:

- Provides a practical understanding of APTs for security professionals.
- Outlines best-practice APT security strategies and tactics.
- Describes unique Websense defenses against APTs.

OVERVIEW

The term APT originally was used to describe nation-states stealing data or causing damage to other nation-states for strategic gain. Since then, the definition has been expanded by security vendors and media to include similar attacks carried out by cybercriminals stealing data from businesses for profit. Attackers are using APTs to go after customer records, blueprints, product roadmaps, source code and other confidential information.

From a practical perspective, the important thing for security professionals to understand is that the same APT techniques used by nation-states for strategic gain are used by cybercriminals to steal data from businesses for financial gain.

BELOW IS A PARTIAL LIST OF APT ATTACKS:

- **Attacks on Financial Sectors**: In September 2013, malicious emails targeted financial (FOREX) institutions in the Middle East, Pakistan and Nepal. The emails contained ZIP attachments with executables. For more information please refer to the Websense Security Labs™ Blog.

- **Attacks on News Agencies:** Earlier in 2013, *The New York Times* and *Wall Street Journal* reported a sophisticated cyber attack that used a combination of spear-phishing and 45 pieces of custom malware. Click here for more information.

- **Attacks on Multiple Industries:** A Websense Security Labs blog post in February 2013 highlighted that over 2,000 unique cases of APT1, a specific attack family of threats, had been reported since 2011 against all major industry segments. It also showed the ineffectiveness of traditional (signature-based) defenses against APTs.

- **Targeted Attacks include compromising legitimate domains:** In August 2013, a waterholing attack was discovered, highlighting the trend of APTs to compromise legitimate domains with malware to target users meeting a specific profile and install data-stealing malware on visitors of the legitimate domain. Click here for more information.

The list of examples is endless. The bottom line is that whether you work for a government agency or a private business, you need to clearly understand and protect against APT techniques, and traditional defenses are not the answer.

APT CHARACTERISTICS

Targeted

APTs target specific organizations with the purpose of stealing specific data or causing specific damage.

Persistent

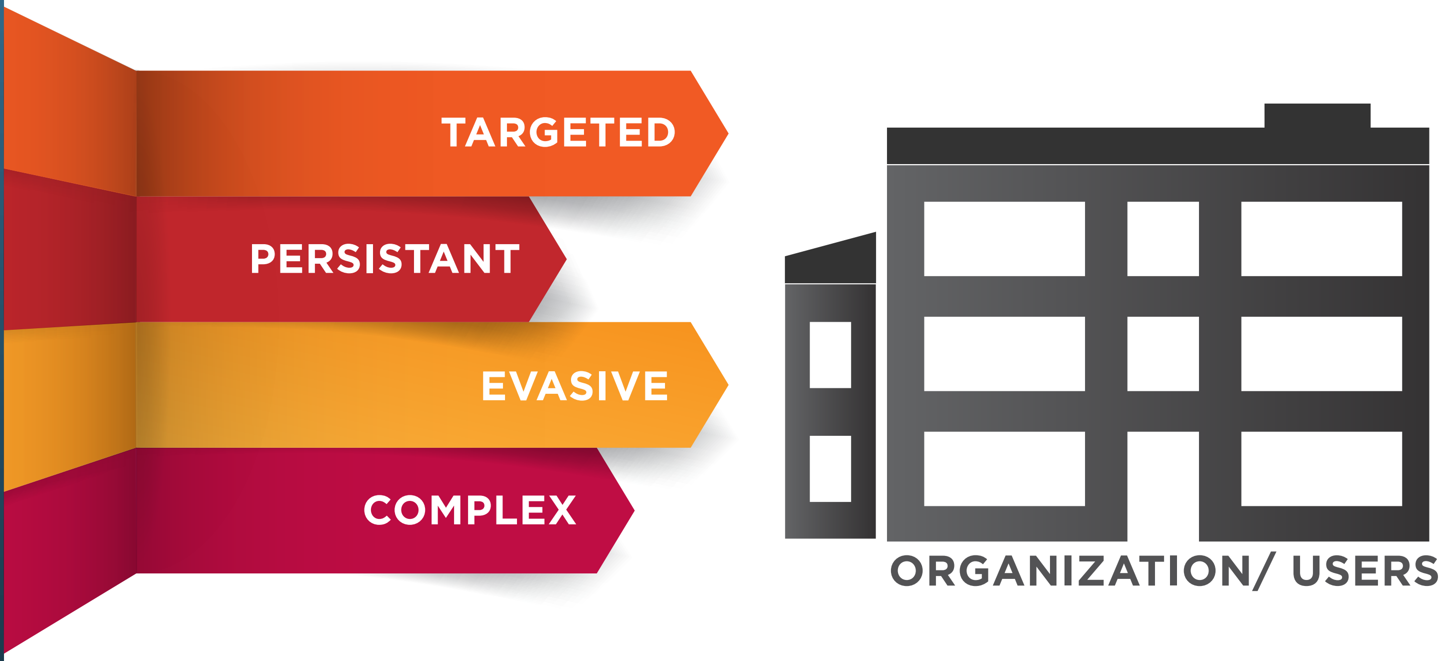
APTs play out in multiple phases over a long period of time. Prior to the actual attack, attackers only know the target organization and objective. To steal the data, the attacker must identify vulnerabilities, evaluate existing security controls, gain trusted access to privileged hosts within the target network, find target data and, finally, extract data from the network. The entire process may take months or even years.

Evasive

APTs are systematically designed to evade the traditional security products that most organizations have relied on for years.

Complex

APTs apply a complex mix of attack methods targeting multiple vulnerabilities identified within the organization. For example, an APT may involve telephone-based social engineering to identify key individuals within the target organization; phishing emails sent to those key individuals with links to a website that executes custom JavaScript code to install a remote access tool; binary command-and-control code (either custom code or code generated by commonly available malware kits); and custom encryption technology.



APT PROCESS FOLLOWS A SEVEN STAGE ATTACK MODEL

APTs, like other advanced threats, occur in "kill chains" of up to seven stages. Not all threats need to use every stage, and stages may loop back to prior stages extending the seven stage process significantly. These provide cybercriminals with hundreds or even thousands of ways to create and execute APTs over extended periods of time.

Stage 1: Recon

In the RECON stage, cybercriminals research their intended victims using personal, professional and social media websites. They're looking for information to help them create seemingly trustworthy "lures" that contain links to compromised websites under their control. Some lures use recent disasters, social drama or celebrity deaths to draw on human curiosity.

Stage 2: Lure

Using information collected in the RECON stage, cybercriminals create innocuous-looking "lures" that can fool users into clicking links to compromised websites. The lures are dangled via email, social media posts or other content that appear to come from trustworthy sources.

Stage 3: Redirect

In their lures, cybercriminals may use links that "redirect" users to safe-looking or hidden web pages that contain exploit kits, exploit code or obfuscated scripts. A redirect can analyze a target system or openly prompt a user to make a software update.

Stage 4: Exploit Kit

Once a user has clicked on a link to a compromised website, software known as an exploit kit scans the victim's system to find open vulnerabilities or zero-day threats. These weaknesses can become open doors for delivering malware, key loggers or other advanced tools that enable cybercriminals to further infiltrate networks.

Stage 5: Dropper File

Once the exploit kit has found a path for delivering malware, the cybercriminal delivers a "dropper file," typically from another compromised server, to infect the victim's system. The dropper file may contain software that executes on the victim's system to begin the process of finding and extracting valuable data. Some dropper files remain dormant for up to a week to avoid detection, and may include downloaders to deliver malware in the future.

Stage 6: Call Home

Once the dropper file infects the target system, it "calls home" to a command-and-control server to download additional programs, tools or instructions. This is the first point at which a direct connection is made between the attacker and the infected system.

Stage 7: Data Theft

The end-game of most modern cyber attacks, the data theft stage completes the threat kill chain. Cybercriminals steal intellectual property, personally identifiable information or other valuable data for financial gain or for use in other attacks.

For more information on the seven stages, visit http://www.websense.com/sevenstages

APT DEFENSE REQUIREMENTS

By analyzing the characteristics of APTs as described above, we can describe the key requirements of an effective security solution:

- **Content-aware:** Because APTs uniformly penetrate network firewall defenses by embedding exploits within *content* carried over commonly allowed protocols, APT defense solutions require deep content awareness across all seven stages of the kill chain.
- **Context-aware:** Because most APTs use custom-developed code or target zero-day vulnerabilities, no single IPS or anti-virus signature is likely to positively identify the threat. Without definitive attack signatures, we must rely on less definitive indicators. Although a single suspicious indicator is not enough to identify an attack, if we evaluate each suspicious indicator in the *context* of other indicators, we can amass enough evidence to reliably identify malicious activity.
- **Data-aware:** Although target organizations may not know exactly what an individual APT looks like (they are all unique), most organizations can identify their own sensitive *data*. Therefore, data loss prevention (DLP) technology can be applied as a layer of defense in Stage 7 (see above) to identify sensitive data and prevent outbound transfers of that data. Identifying the use of proprietary encryption on outbound web traffic is also important to an APT defense.

STRATEGIES TO IMPROVE PROTECTION AGAINST APTS

Today, most IT security budgets are largely consumed by anti-virus, firewall, and IDS/IPS products, yet the news is filled with stories of targeted attacks — including APTs — that elude these defenses. Traditional security measures do not adequately address today's threats. Without a new security posture, many more attacks using APT techniques will succeed in victimizing their targets. Traditional defenses such as firewall and anti-virus are necessary because they block known threat vectors; however, they are not sufficient and their limitations against APT techniques and targeted attacks must be recognized and fixed.

A sound defense against APT techniques needs to monitor inbound and outbound traffic for content, context and data, preferably for both email and web communications. More specifically, the defense layer should monitor outbound communications for the detection of data-theft behavior. Some examples of malicious outbound behavior are command-and-control traffic; requests to dynamic DNS hosts; requests to known bad web locations; movement of sensitive files that should never be sent outside the organization (e.g., SAM database); and the use of proprietary encryption.

In research on best practices for mitigating APTs, industry analysts point out that a comprehensive strategy to combat and prevent APTs needs to span across networks, edge, endpoints and data security. In other words, the strategy needs to include the right mix of technologies. This mix includes **secure web gateways** with real-time analytics and DLP technology, as well as **threat monitoring solutions** with sandboxing and forensic reporting capabilities.

- **Secure web gateways** are a corner stone to protect effectively against advanced threats and data theft by analyzing all incoming and outgoing traffic to combat advanced threats, including the ability to analyze SSL traffic.
- **Threat monitoring solutions**, sometimes called breach detection systems (BDS), are also a crucial component in combating APTs, because these services provide security professionals with valuable insight into threat levels, the behavior of malware and complete forensic analysis with easy-to-read reporting. A good threat monitoring solution provides IT departments with the knowledge and tools to improve the threat exposure of their networks.

TO PROTECT AGAINST ADVANCED PERSISTENT THREATS EFFECTIVELY, SECURITY SOLUTIONS NEED TO PROVIDE THE FOLLOWING FIVE KEY ESSENTIALS:

1. **Real-time Threat Analysis**

   Traditional defenses rely on signatures, rendering them largely ineffective to combat today's advanced threats. In order to protect against spear-phishing, exploit kits, dynamic redirects, or similar components of an APT attack, additional real-time analysis needs to be conducted, and risk scores need to be assigned for traffic.

2. **Global Threat Awareness**

   Any security solution can benefit greatly from a large threat detection network. The larger the network, the greater the threat awareness and protection capabilities of the solution.

3. **DLP Capabilities**

   The ultimate goal of an APT is data theft. Considering an APT's complexity, it is crucial to not just rely on inbound defenses, but also have cutting-edge outbound data theft technology in place. Pattern-matching alone is not enough; rather, a fully contextually aware DLP solution must be deployed to protect your sensitive data against exfiltration.

4. **Sandboxing**

   Cybersecurity has become a hand-on business for IT and security professionals. Effective reporting and analysis done on malware and advanced threats has become crucial. Security professionals need insights into how malware would behave and how it would impact their networks to better protect their companies' assets. A good sandboxing solution provides this capability.

5. **Forensic and Behavioral Reporting**

   Hand-in-hand with any security deployment goes the need for excellent forensic and behavioral reporting. Actionable reports providing valuable insight into threat behavior, impact and forensic details are a key component of any security deployment. The more actionable a report is, the more value it has to an IT or security professional.

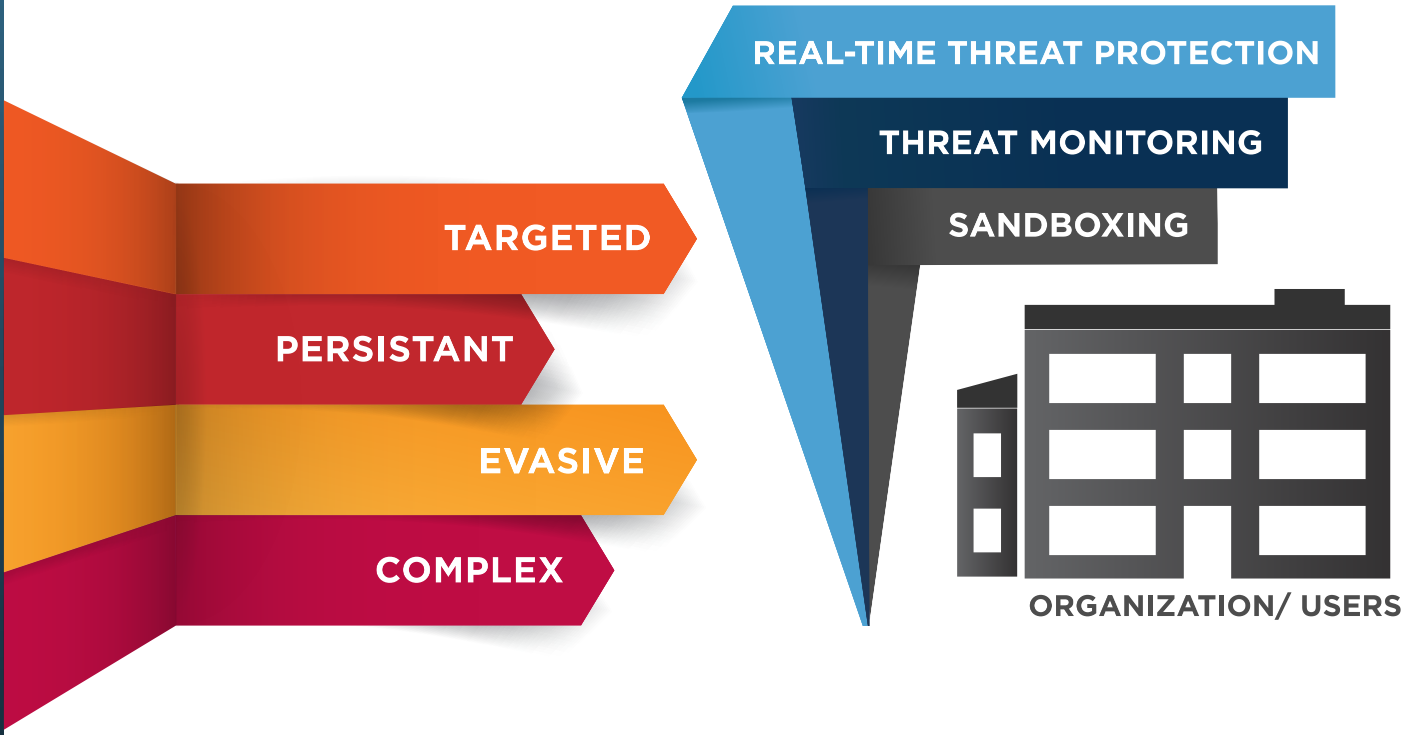
WEBSENSE SOLUTIONS FOR PROTECTING AGAINST APTS

Websense offers a full suite of products that provide thorough protection against APTs and other advanced threats. The product portfolio consists of the following product groups:

- **Protection Products:** Websense TRITON® products include proxy gateway solutions for web, email, data and mobile security. All provide:
  - **Real-Time Advanced Threat Detection and Protection.** Websense ACE (Advanced Classification Engine) uses eight defense assessment areas with over 10,000 analytics to provide real-time threat analysis of web traffic.
  - **Global Threat Awareness.** Websense ThreatSeeker® Intelligence Cloud unites over 900 million end-points and analyzes up to 3-5 billion requests per day, providing global threat awareness and vital defense analytics to ACE.
  - **Data Theft and Loss Detection.** Websense DLP defenses detect and block data exfiltration for registered and described data. Industry leading features within Websense DLP include OCR of text within images, geolocation destination awareness, detection of criminal-encrypted uploads and password file data theft, and slow data leak protection.

- **Sandboxing Solution:** Websense TRITON ThreatScope™ offers unparalleled sandboxing and analytics functionality, providing security professionals with valuable behavioral and forensic insights about malware contained in files and URLs. (Please refer to Appendix A.)

- **Threat Monitoring Solutions:** Websense TRITON RiskVision™ is a complete threat monitoring solution offering effective detection of the most advanced threats including APTs and data exfiltration attempts. Behavioral and forensic reporting provides actionable data empowering security professionals to decrease the risk exposure.



APPENDIX A: BEHAVIORAL SANDBOXING

Websense Behavioral Sandboxing Offers Unmatched Real-Time Analysis

Protecting against today's advanced targeted attacks requires a far more comprehensive approach to security than even a couple of years ago. Gartner Inc. recommends to "Use a comprehensive approach; no single technology will stop advanced targeted attacks."[1] Such an approach includes protecting both web and email traffic with a variety of proven and newer technologies, including sandboxing.

Sandboxing is increasingly entering the conversation for security professionals due to its ability to monitor malware activity in a virtualized environment kept completely separate from customers' networks. By allowing security professionals to view malware changes in a virtual environment, sandboxing provides the information needed to better understand the nature of the threat.

However, not all sandbox solutions are created equal. Many continue to use signature-based or static lists of known malicious system activity and communications. The problem is, malware continues to change and adapt to the security put in place to prevent it. Even a slight variant of existing malware will be different enough to evade many traditional defenses.

This raises the question: how do you defend against something that's never been seen before?

Behavioral sandboxing is how. It uses real-time correlation of malware activity with global threat intelligence to provide unrivalled protection from even the most advanced threats.

How Sandboxing Works

Whether a file is delivered via web or email, sandboxing runs it in a virtual environment that is completely separated from all other environments and networks. This allows the file to fully execute and the sandbox to monitor the entire infection lifecycle. A typical sandbox environment includes not only a standard operating system but also today's most commonly used business applications. From Microsoft Windows to Microsoft Office and Adobe Acrobat reader, any sandbox environment emulates the most common business environment to present the largest possible target for the malware, thereby increasing the chances of catching the malware "in the act."

Monitoring the malware infection lifecycle requires analysis of both system activity and the subsequent communication. System activity includes everything from process and file system modifications to registry changes. By using a new virtual environment for each analysis, sandboxing always starts from the same point, allowing the subsequent analysis to be very specific about what changes are being made. Knowing this specific list of system changes is crucial for security professionals to understand the nature of the malware and to remediate the infection.

Equally important to understanding system activity is monitoring malware communication. System activity lays the foundation for the actual damage, generally by downloading additional components or exfiltrating data. In both scenarios it is imperative that all communication protocols, destination IP or hosts, DNS requests, and types of transferred data be analyzed.

Tracking both system activity and communication is required to understand the full infection lifecycle — but it is only the starting point.

[1] Gartner, Inc. "Best Practices for Mitigating Advanced Persistent Threats" by Lawrence Pingree, Neil MacDonald, Peter Firstbrook, Sept. 12, 2013.

Behavioral Sandboxing Adds Real-Time Intelligence

Moving beyond basic sandboxing to behavioral sandboxing requires the correlation of malware activity against known and suspicious actions in real time. Maintaining a static list of known malicious activity is still valuable in providing immediate feedback to malware actions, but the most advanced malware, resulting in the most dangerous advanced persistent threats (APTs), will most likely not be found in a static list.

Understanding the malware behind advanced targeted attacks and APTs can be best achieved through the combined analysis generated by two core Websense® technologies: Websense ACE (Advanced Classification Engine) and Websense ThreatSeeker® Intelligence Cloud. By analyzing up to 5 billion daily requests from 900 million endpoints across over 10,000 analytics, Websense is able to correlate activity from the largest global threat intelligence network and apply this information to the malware activity being monitored in the sandbox environment. And even while the malware is running in the sandbox, Websense technologies continue to collect new information and make it available for comparing against the current malware's activity.

The Advantages of Cloud-Based Sandbox Deployments

Many sandbox solutions are delivered via an on-premise appliance, a deployment that creates two challenges. First, the sandbox capacity is self-limiting to the available resources on the sandbox appliance. Appliance sandbox solutions in high-traffic environments are unable to analyze all suspicious activity and therefore must prioritize only the highest priority threats the busier they get. Cloud-based sandboxing, on the other hand, has no capacity issues and can scale easily to monitor all suspicious threats regardless of traffic volume.

Second, but equally important, is the sharing of information across multiple appliances. Even within a small appliance population, threat intelligence updates can be delayed, and even the shortest delay can result in the mis-classification of zero-day malware that can potentially lead to infection. Websense solves this problem with real-time global threat intelligence that automatically updates across all Websense sandbox solutions, creating the fastest learning and most up-to-date intelligence available and providing true real-time protection against advanced targeted attacks and APTs.

The Need for Forensic Reporting

To assist security professionals with awareness and remediation, behavioral sandboxing must include forensic reporting. And the forensic reporting must be easy to read while providing detailed information on malware activity and communication — in other words, it must be an actionable report. Websense behavioral sandbox forensic reports provide detailed information on observed activity, system changes and malware communications, and are automatically delivered for all malicious files identified by sandboxing.

Websense Sandboxing Solutions

Websense behavioral sandboxing is available in two innovative solutions:

- TRITON® ThreatScope™, an add-on service to provide additional defenses for the most advanced, targeted zero-day threats and APTs that may attack through email or web channels.
- TRITON® RiskVision™, an unmatched threat monitoring solution that provides immediate visibility into advanced threats, data exfiltration and infected systems by unifying four key defenses into a single appliance.

ABOUT WEBSENSE, INC.

Websense, Inc. is a global leader in protecting organizations from the latest cyber attacks and data theft. Websense TRITON comprehensive security solutions unify web security, email security, mobile security and data loss prevention (DLP) at the lowest total cost of ownership. Tens of thousands of enterprises rely on Websense TRITON security intelligence to stop advanced persistent threats, targeted attacks and evolving malware. Websense prevents data breaches, intellectual property theft and enforces security compliance and best practices. A global network of channel partners distributes scalable, unified appliance- and cloud-based Websense TRITON solutions.

Websense TRITON stops more threats. Visit www.websense.com/proveit to see proof.

Learn more at **www.websense.com | +1 800-723-1166 | info@websense.com**

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense
TRITON®

© 2013 Websense, Inc. All rights reserved. Websense, TRITON and the Websense logo are registered trademarks of Websense, Inc. in the United States and various countries. All other trademarks are the properties of their respective owners. EN 10-4-13.