## A Websense® Brief

*By Patrick Murray, Senior Director of Product Management*

# ADVANCED PERSISTENT THREATS:

## FROM "FUD" TO FACTS

**With Websense**, you can stay a step ahead of the threats. From our roots in web filtering, we've been analyzing and classifying content for more than 15 years, and we now offer must-have web, email, and DLP security that closes the gaping holes left by traditional security products.

websense®
ESSENTIAL INFORMATION PROTECTION™

"APT" (Advanced Persistent Threat) is this year's hot-button term, but what exactly does it mean? Too much marketing hype and FUD (fear, uncertainty, and doubt) have clouded the facts about a very real danger to organizations of all sizes. This overview will:

1. Explain how APT methods are now being applied by common cybercriminals
2. Explore the anatomy of a targeted attack and
3. Offer solutions for defending yourself.

## Why you should care about APTs

Large organizations with a treasure chest of intellectual property (like source code) know very well that they're high-value targets for cybercrime. But smaller organizations aren't as worried: "I'm a $10M manufacturing company in Ohio. I don't think Chinese or North Korean hackers will be knocking on my door anytime soon." That's right; they won't. But other attackers probably will.

For many companies, APTs aren't a primary concern because APTs (by definition) are usually used by governments to cause trouble for other governments or large corporations. But APTs are also a prototype for other targeted attacks that are now victimizing companies of all shapes and sizes. It's a fact: The same APT technology used by China to hack Google is now being used by cybercriminals to steal data from organizations like yours.

## How APTs get into the open marketplace

Imagine a government putting on a bullet-proof vest. To pierce that vest, other governments and state-sponsored agents spend huge resources coming up with specialized ammunition that eventually succeeds in penetrating the armor. Soon, that ammo becomes available on the open market, and criminals use it in all kinds of crimes. This same adoption cycle occurs with malware technology.

Let's look at a classic APT, and how quickly the techniques got into the hands of others.

**Websense® Security Labs™ has led the way in examining APTs in the wild and charting the emergence of these exploits. Learn more about the Security Labs.**

## The malware technology lifecycle

The Aurora attacks of 2009 were among the first widely publicized uses of APTs. Companies like Google, Adobe and Rackspace were targeted by a state-sponsored APT in November and December of that year. On January 12, 2009, Google announced they were attacked. Two days later, the zero-day exploit was revealed publicly. Nine days went by before Microsoft patched the primary vulnerability. During that time, only 26% of antivirus vendors detected the exploit because it was so new. Yet within a month, the Websense® ThreatSeeker® Network detected more than 200 new websites using the same exploit to deliver other malware. The APT spread like wildfire, fanned by organized criminal gangs who had a new round of ammunition to use against their primary targets – companies with customer information or credit card numbers they could quickly turn into cash.

## Anatomy of a targeted attack

Just how do APTs and targeted attacks work? Let's step through one example.

**Advanced**: Attackers use a spectrum of sophisticated intelligence-gathering technologies. The action usually begins months prior to the actual data-stealing attack on an organization.

*For example:*

- *The attackers infiltrate and take control of another (not the target's) company server. Often this is done through SQL injection of an old table on a neglected web page, or an insecure web application. This will be used as a dead drop for data later on, and the data trail will end there.*
- *A custom piece of malware is sent to an employee's personal email account (with the knowledge that the employee checks their personal email at work). That malware then begins to travel through the network, mapping it and checking for security measures in place. Note: Surveillance of the individual target started before surveillance of the network. Frequently the target of this email is identified through a search of the social web or LinkedIn or Facebook profiles, simple search queries for executive officers on corporate sites, etc. In a social society, there is an abundance of information available about any target, making it that much easier to social engineer a very compelling email to the subject in their native language, using their own likes and information to motivate them to open the email. The attackers may have already "friended" and conversed with the subject over social sites to gather information.*

**Persistent:** The attackers are absolutely determined to succeed. They will conduct patient, steady, ongoing monitoring to find vulnerabilities. They repeat attempts and change tactics if detected.

- *In our example, the malware has now mapped the network and has sent information to the attackers about the security protocols in place, including the AV and the proxy firewall address in place. At this point the attackers know how to get in, and more importantly, where their prize probably resides.*

**Threat:** Attackers also tend to use multiple vectors of attack, including specifically crafted malware and previously unknown zero-day vulnerabilities.

- *In our example, we've already seen one custom piece of malware used to conduct surveillance. Now comes the killer code.*
- *A new email is sent to a personal email account of a different employee – one with access to the valuable data. It carries a payload of highly refined malware that knows which systems to evade, where to find the desired data and how to steal it without immediate detection. The code is also polymorphic, updating itself frequently to remain undetected by AV and other security measures. (Remember, this isn't just a botnet looking for online banking credentials to clear your account. These attackers are thinking bigger. They want the intellectual property, trade secrets, and other sensitive data they can use to embarrass or exploit you).*
- *The data is often exfiltrated slowly, without the IT or security team noticing. Only after a separate incident will the security teams see something fishy in the logs – which is often the first time the connection with suspicious IP addresses (remember step 1?) is noticed.*

## How does Websense defend against APTs and targeted threats?

These attacks use sophisticated, blended techniques that leverage both web and email channels to deliver malware -- and those same channels for the extrusion of sensitive data. Often, the malware has never been seen before, and is designed to elude traditional defenses.

The Websense® TRITON™ solution unifies web, email, and data security to provide a blended security service for a blended style of attack. The combined security analytics in the Websense® Advanced Classification Engine (ACE) – the heart of the TRITON solution – look at content entering and exiting an organization. TRITON analyzes both the context and the content (including code) of web pages and emails, in real-time. It also analyzes content that's communicated externally to ensure sensitive data is not sent inappropriately. Unlike narrowly focused defenses like antivirus, URL filters, firewalls, and reputation-based systems, this blended TRITON security identifies and protects against both known and unknown threats.

## How does the Websense® TRITON™ solution address APTs and blended threats better than other security technologies?

Websense TRITON security is the only truly unified solution with all of these important features:

1. **Shared security awareness:** The blended security analytics in the Websense® Advanced Classification Engine (ACE) combine malware identification and protection services (including baseline antivirus and URL filters) with advanced code inspection and behavioral, heuristic, exploit, reputation, and other scanning analytics to address known and unknown threats (i.e., anything from a standard virus to a purchased Bot or Trojan, to an advanced and custom-built script that targets a vulnerability in an application or browser). ACE combines the results from the individual scanning components (e.g., reputation services + antivirus + exploit analysis, etc.) and makes a voted, intelligent decision whether the traffic should be allowed or dropped. The power of ACE enables the TRITON solution to combine intelligence from our email, web, and data security technologies to help prevent intrusion by targeted attacks that are typically missed by legacy security technologies.

2. **Outbound inspection:** Most traditional security technologies inspect only inbound threats and ignore outbound communications. However, APTs and targeted attacks are more sophisticated than traditional attacks -- and typically more successful in penetrating defenses. If and when these attacks infiltrate your network, it's critical to inspect and protect outbound data transmissions to stop the attacks from successfully exfiltrating your data.

   That's why Websense provides outbound content scanning to ensure an infected machine doesn't communicate sensitive data externally. Websense applies enterprise-class data loss prevention (DLP) technology to identify and monitor sensitive data communicated over web, email, and other channels to ensure it goes only to authorized locations, and not into an attacker's hands.

   The Websense TRITON solution also analyzes encrypted communications, which are often used in blended attacks to disguise the outbound transmission of sensitive data, and it blocks those with non-standard SSL patterns. The Websense® TRITON Web Security Gateway also scans for outbound traffic patterns indicative of botnet command and control centers that may be trying to "phone home" traffic.

3. **Comprehensive coverage, flexibility, and ease of use:** Even if a security system provides scanning for known malware, heuristics for unknown malware, and backchannel communication controls to prevent data theft, there may still be gaps in the defense. Unless the coverage extends to mobile devices

and branch offices, these "weak links" may break the security chain. Unless the solution provides for deployment flexibility (with on-premise, hosted and/or hybrid solutions) it may not grow or adapt to the needs of an organization. And unless it's easy to manage – with both the granularity and simplicity of a unified management console – it may not be used effectively.

Websense TRITON security is the only truly unified solution that meets all of these criteria.

## Conclusion: New threats demand new security solutions

While APTs don't target everyone, everyone should understand how APTs work — because these same techniques are now being used by cybercriminals in targeted attacks designed to steal sensitive data from all kinds of organizations.

Defending against these targeted attacks requires a new approach. Learn how to protect yourself now with Websense® security solutions.