Advanced Zero Day Protection with APT Blocker

White Paper

WatchGuard® Technologies, Inc.
Published: June 2016

Patches, Signatures and More

Way back in 2003, the SQL Slammer worm brought Internet traffic to a standstill in many parts of the world for several hours.[1] This notorious worm targeted a known vulnerability in the Microsoft SQL database. Key to its success and proliferation was its small size and the way it quickly replicated itself and randomly looked for new targets to infect.

IT vendors have been responding to threats like this ever since. Every month Microsoft releases a series of updates to address vulnerabilities that have been found in their software. Adobe follows their lead and releases security hotfixes on the same "Patch Tuesday." Cisco also provides a major set of security-related fixes once per quarter. And IT administrators are routinely encouraged to patch their systems frequently to stay current.

Other defenses include intrusion prevention systems (IPSs) that inspect traffic for known patterns of vulnerability exploits. Antivirus systems block and quarantine malware. Regulations like PCI DSS mandate that companies keep their antivirus software updated to the latest signatures. Central management solutions are deployed to ensure that all users are running the latest AV solutions on their desktop, laptop, and now even on mobile devices running Android. But it's not enough, and in this paper we'll explain why.

Zero Day Is the New Battleground

In the biomedical field, researchers and doctors have long understood that microbes and bacteria evolve over time and become more resistant to antibiotics. They need to develop new and stronger medicines to stay current. Likewise, in the information security world, new breeds of malware continually emerge that are more advanced and resistant to the conventional defenses. Hackers have traditionally targeted large corporations, but today small to midsize businesses are being attacked with the same type of highly sophisticated malware. These new strains of advanced malware are often referred to as **Advanced Persistent Threats (APTs).**

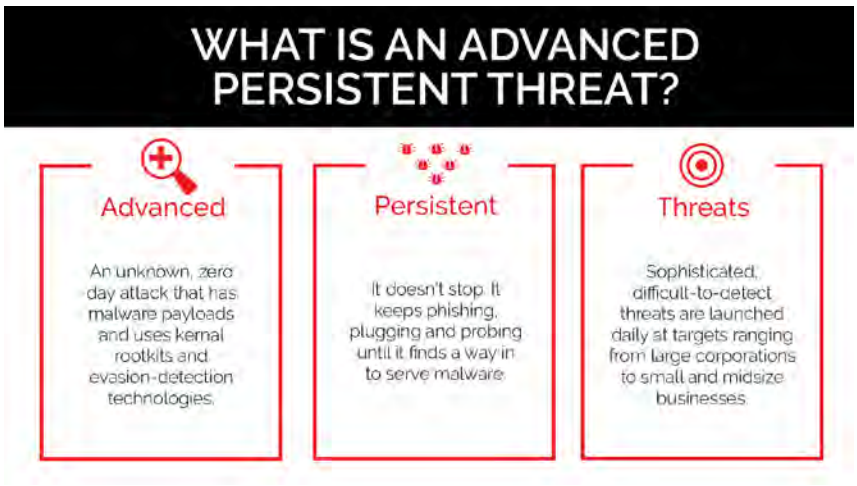

Figure 1: Characteristics of an Advanced Persistent Threat

[1] http://en.wikipedia.org/wiki/SQL_Slammer

Modern malware uses **Advanced** techniques such as encrypted communication channels, kernel-level rootkits, and sophisticated evasion capabilities to get past a network's defenses. More importantly, they often leverage zero day vulnerabilities – flaws for which no patch is available yet and no signature has been written.

Modern malware is often **Persistent** and designed to stick around. It stealthy and carefully hides its communications. It lives in a victim's network for as long as possible, often cleaning up after itself by deleting logs, using strong encryption, and only reporting back to its controller in small, obfuscated bursts of communication.

Many attacks are now blended combinations of different techniques. A common tactic for hackers is to initiate an APT with spear phishing. This involves sending a carefully crafted email that appears to be from a known individual or business with a link to a malicious website or an infected download. Once the initial breach is successful, attackers can further damage defenses by disabling security protocols, changing security settings or stealing passwords.

Groups of highly skilled, motivated, and very well-funded attackers represent significant **Threats** because they have very specific targets and goals in mind – often financial gain from theft of credit cards and other valuable account information.

Figure 2 shows a chronology of some of the most publicized attacks going back to the beginning of the decade. The evolution of Stuxnet to Duqu highlights how advanced techniques used by nation-states for cyber warfare became standard tools for hackers seeking financial gain by targeting government, retail, hospitality, education, and more.

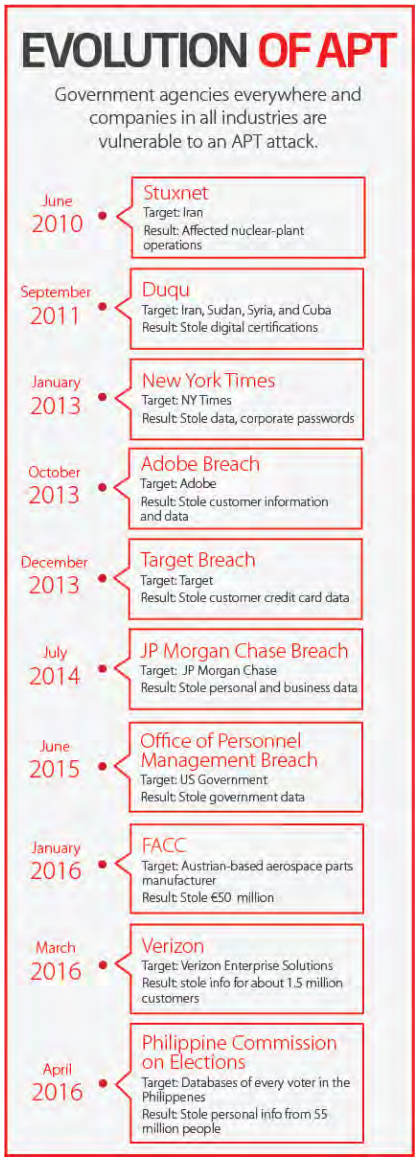

Figure 2: A sampling of successful attacks over that last seven years.

The consequences of a breach are significant for any organization. Forbes reported that sales at major US retailer Target – arguably the most notorious retail breach of all time – were down almost 50% the quarter of the attack[2] and the main reason was negative publicity around stolen customer data. The stock price dropped 9%. The CIO left the company, and 5-10% of shoppers at Target reported that they would never shop at the store again.[3]

[2] http://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/

[3] http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/

The number of cyber attacks per year continues to climb, and according to the Ponemon Institute, the average cost of a data breach today is $4 million, representing a 29 percent increase since 2013.[4]

- Premera discovered that hackers broke into their IT systems and stole applicant and member information including Social Security numbers, member ID numbers, claims information, bank account information, and more. About 11 million customers were affected. The investigation revealed the initial attack occurred in May 2014 but it was not discovered until January 2015.

- In 2016, a 2012 data breach came back to haunt LinkedIn, the giant social networking site designed specifically for the business community, when 117 million email and password combinations stolen by hackers four years ago popped up online.

- The financial data of more than 80,000 students, alumni, employees, and school officials of the University of California, Berkeley was compromised around December 2015 and announced to the public in February 2016.

- The Philippe Commission on Elections (COMELEC) database was breached in April 2016. It is believed that the personal information of every single voter in the Philippines – approximately 55 million people – was compromised.

- In May of 2016, Wendy's fast-food chain reported malware infiltrated the point of sale (POS) system at approximately five percent of their locations. One month later they began revising the estimated number of compromised sites, saying that the number was considerably higher – an indication of the stealth by which the malware is able to hide itself.

Antivirus Can't Keep Up

The fight against malicious code is an arms race. Whenever new detection techniques are introduced, attackers look for new ways to bypass them. Traditional antivirus companies employ engineers and signature writers to analyze files. They monitor unknown programs in a lab environment, or they may submit files to tools like Anubis, which run a file and report on any suspicious activity or behavior that indicates a virus. But relying on signatures alone is dangerous because there is an 88 percent probability that a variant of existing malware has been created to avoid detection by classic techniques.

Lastline Labs studied the growth of evasive malware through 2015. Their research found the number of evasive techniques dropped significantly in Q2, only to rise even more dramatically in Q3. The arms race continues.

[4] https://www.helpnetsecurity.com/2016/06/16/data-breach-cost-4-million/

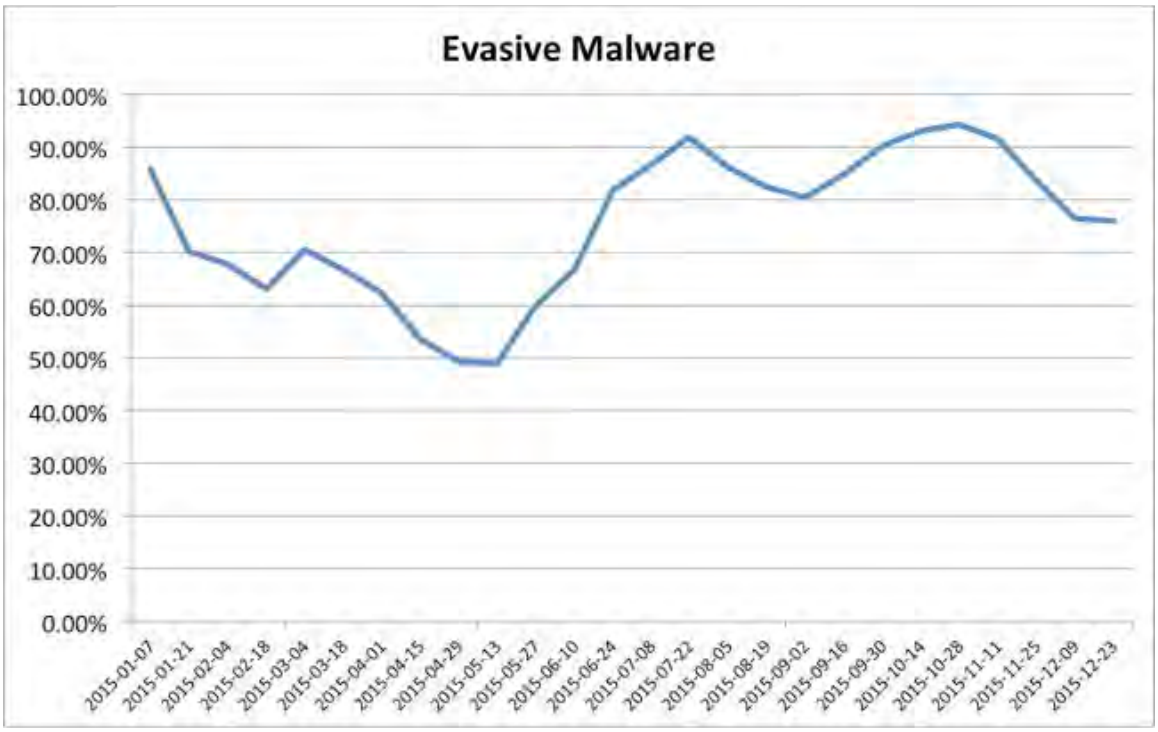

Figure 3: Evasive malware growth through 2015

Lastline also published research based on hundreds of thousands of pieces of malware they detected throughout 2015. Each malware sample was tested against dozens of antivirus vendors featured in VirusTotal, a third-party site that aggregates and compares different AV solutions. The goal was to determine how effective AV is, which engines caught the malware samples, and how quickly they detect new malware. The results were astonishing.

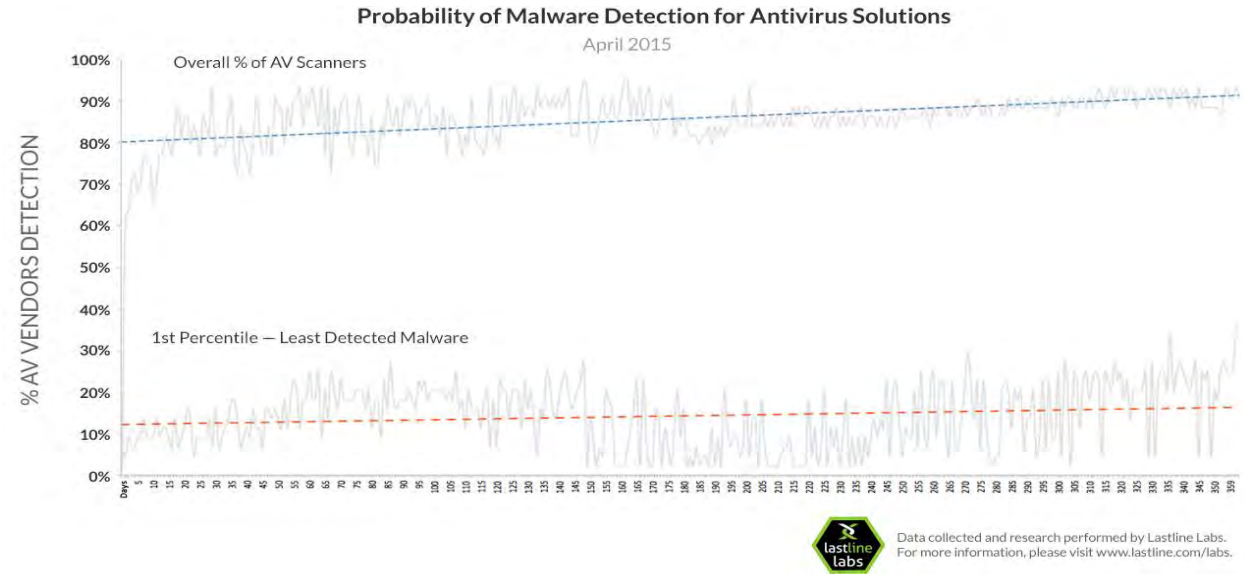

Figure 4: Antivirus malware detection probability

The graph shows two lines: the blue represents common malware and the red represents the least detected malware. Malware in the one percentile of "least likely to be detected" category has gone undetected by the majority of antivirus scanners.

A particularly prevalent form of malware today is ransomware. It works by encrypting a victim's files and then convincing the victim that the only way to retrieve the files is to pay a ransom. The evolved, kidnapping-style tactics are designed to increase anxiety and stress in the hopes that the victim hastily concedes to the criminal's demands. In early 2016, Hollywood Presbyterian Hospital paid a ransom of $17,000 to retrieve their data.[5] The University of Calgary transferred 20,000 Canadian dollars-worth of bitcoins after it was unable to undo damage caused by the ransomware attack.[6]

Trend-watchers at the National Cybersecurity Institute see volume rather than specific targets as a common attack strategy.[7] A virulent strain of ransomware called Locky is reportedly infecting at least 90,000 machines a day.[8] Ransom demands are frequently under $1,000 – an amount that many small to midsize businesses might be willing to pay. The logic is if the ransom can be seen as a nuisance expense, it will be more readily paid and paying ransom will be thought of as an unfortunate consequence of doing business today.

Defenses Are Evolving: Sandboxes

Malware authors use devious evasive techniques to ensure their programs do not reveal any malicious activity that can be detected in an automated analysis environment. Common evasion techniques include:

- Determining the presence of a virtual machine
- Querying for well-known Windows registry keys that will indicate a particular type of sandbox
- Sleeping for a while, waiting for the sandbox to timeout the analysis

Security vendors have reacted by adding some counter-intelligence of their own to their systems. For example, they can check for malware queries for well-known keys, and force programs to wake up after they call sleep. But this approach is still reactive. Unfortunately, malware analysis systems like these need to be manually updated to handle each new, evasive trick. Malware authors who create zero day evasions are able to bypass detection until the sandbox is upgraded.

Beyond the Sandbox - Full System Emulation

The most common sandbox implementations today typically rely on a virtual environment that contains the guest operating system. Sometimes, a sandbox runs the operating system directly on a real machine. The key problem, and the fundamental limitation of modern sandboxes based on virtualization, is their lack of visibility and insight into the execution of a malware program. The sandbox needs to see as much of the malware behavior as it possibly can, but it needs to do it in a way that hides itself from the malware. If malware can detect the presence of a sandbox it will alter its behavior.

[5] http://www.darkreading.com/operations/two-biggest-reasons-ransomware-keeps-winning/d/d-id/1324631
[6] http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979
[7] http://www.nationalcybersecurityinstitute.org/small-business/trends-in-ransomware-affecting-small-business/
[8] http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#5ec17f1c75b0

For example, instead of simply sleeping, sophisticated programs perform some useless computation that gives the appearance of activity. Hence, there is no way for the sandbox to wake the program up. The program simply executes, and to the malware analysis system everything is normal.

Most malware runs in user mode (either as a regular user or administrator). Sandboxes based on virtualization look at Windows API calls and system calls from the user mode programs. System calls or function calls capture all interactions between a program and its environment (e.g., when files are read, registry keys are written, and network traffic is produced). But the sandbox is blind to everything that happens between these calls. Malware authors can target this blind spot.

A smarter approach is required. An emulator is a software program that simulates the functionality of another program or a piece of hardware. Since an emulator implements functionality in software, it provides great flexibility. OS emulation of the operating system provides a high level of visibility into malware behaviors. But OS-level emulators cannot replicate every call in an operating system. They typically focus on a popular subset of functionality. Unfortunately, this approach is the easiest for advanced malware to detect and evade.

Dormant functionality is another way hackers can get around traditional sandbox-based systems. This is when a piece of malware remains dormant during analysis and executes only when certain conditions have been met.

Full System Emulation, where the emulator simulates the physical hardware (including CPU and memory), provides the deepest level of visibility into malware behavior, and it is also the hardest for advanced malware to detect and evade.

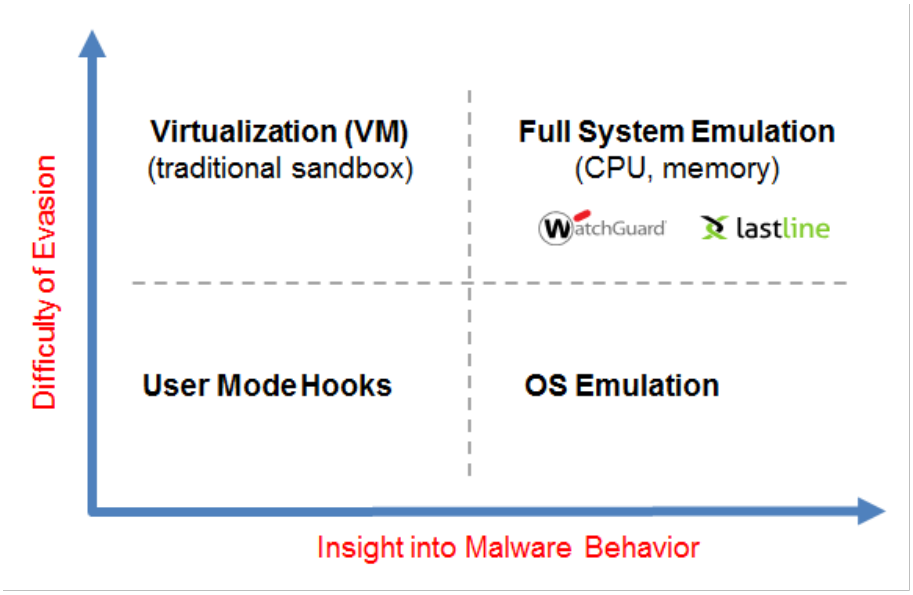

Figure 5: Full system emulation has the strongest malware detection

WatchGuard APT Blocker

APT Blocker, a subscription-based service available for all WatchGuard Firebox appliances, uses full system emulation (CPU and memory) to get detailed views into the execution of a malware program. After first running through other security services such as gateway antivirus and intrusion prevention, files are fingerprinted and checked against an existing database – first on the appliance and then in the cloud. If the file has never been seen before, it is analyzed using the system emulator, which monitors the execution of all instructions. It can spot the evasion techniques that other sandboxes miss.[9] A comprehensive set of file types are reviewed in the sidebar below.

WatchGuard selected a best-in-class technology partner for the next-gen sandbox used by APT Blocker. Lastline Technology was founded by the technical team that developed Anubis, the tool that has been used by researchers around the world for the last nine years to analyze files for potential malware.[10]

When malware is detected it can immediately be blocked at the firewall. In some cases, a true zero day file may pass through while analysis takes place in the cloud. In such cases, the WatchGuard system can provide immediate alerts that a suspect piece of code is on the network so IT can follow up immediately.

File types analyzed by APT Blocker:

- HTTP proxy
- FTP proxy
- SMTP proxy
- POP3 proxy
- All Windows executable files
- Adobe PDF
- Microsoft Office
- Rich Text Format
- Android executable files (.apk) files
- Files within compressed archives

Visibility

But detecting malware is not enough. IT staff need to get clear, actionable information that is not lost in an ocean of log data. IT departments are tasked with keeping a business running and helping the bottom line. Despite the tremendous impact that security incidents can have on a business, many IT departments are suspicious of suspected security alerts. Neiman Marcus, the victim of another infamous retail breach, had over 60,000 log incidents that showed there was malware on their network.[11] Target had log files a few days after the first breach indicating there was a problem but they were ignored.[12]

An effective advanced malware solution needs to provide the following:

- **Email alerts** when a harmful file is detected
- **Log and report capabilities** that are closely integrated with other security capabilities on the network
- **Clear indication** of why any file has been detected as malware, so it is not immediately dismissed as a potential false positive

[9] http://info.lastline.com/blog/different-sandboxing-techniques-to-detect-advanced-malware

[10] http://info.lastline.com/blog/next-generation-sandbox-offers-comprehensive-detection-of-advanced-malware

[11] http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

[12] http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1

The WatchGuard APT Blocker solution meets all the visibility requirements with email alerts, real-time log analysis, and the ability to drill deeper to find more information. The service is fully integrated into WatchGuard Dimension™, the award-winning security intelligence and visibility solution[13] that is included at no charge with all WatchGuard Firebox security solutions. It goes beyond a simple alert saying that a file is suspicious. A detailed malicious activity report is provided for each file that is scored as malware.

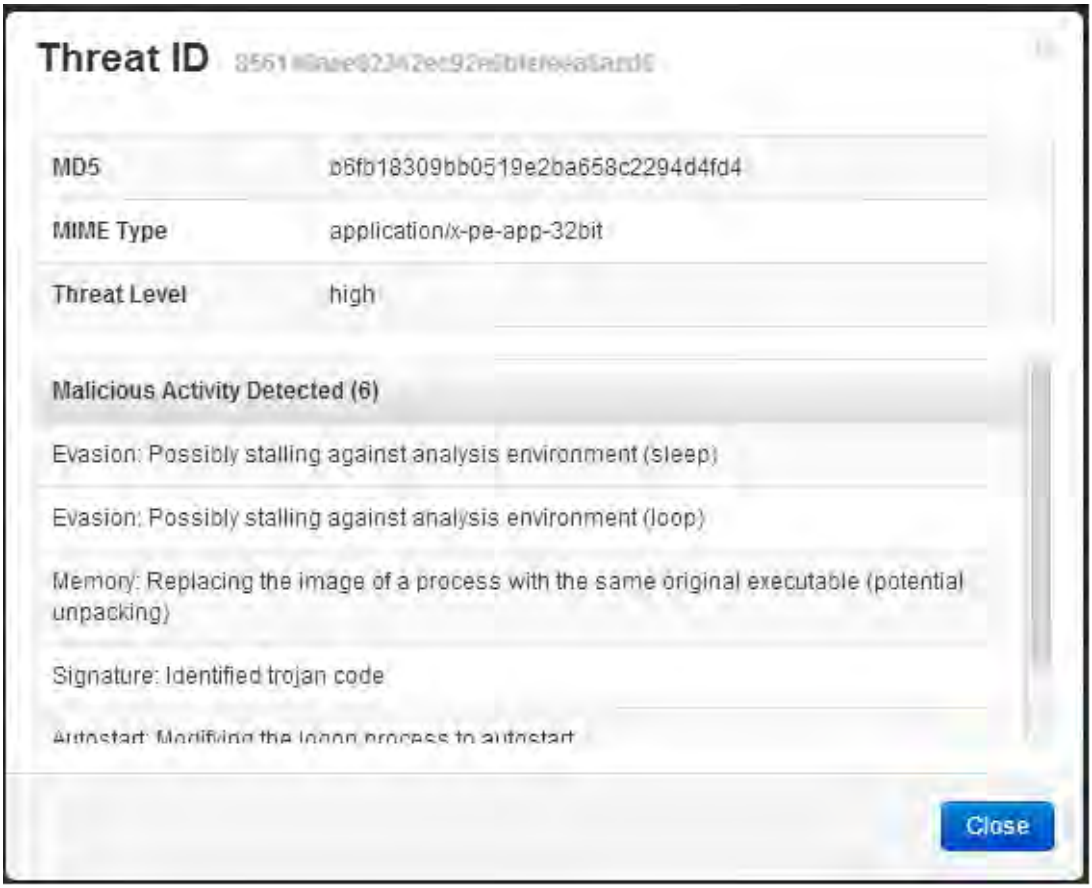

Figure 6: An APT report shows detailed Malicious Activity, explaining why a file is marked as malware

The example above highlights a file that showed several characteristics that are typical of malware. The two evasion techniques detected show how the WatchGuard solution has been able to recognize malicious activity that may have fooled other sandbox products.

WatchGuard Dimension reveals APT activity in its top level security dashboards, along with detailed security reporting from all of the other security services. APT activity is also included in the top level executive summary reports, and there are ten predefined reports for the administrator to choose from.

[13] http://www.watchguard.com/news/press-releases/network-computing-awards-names-watchguard-dimension-best-new-product-of-the-year.asp

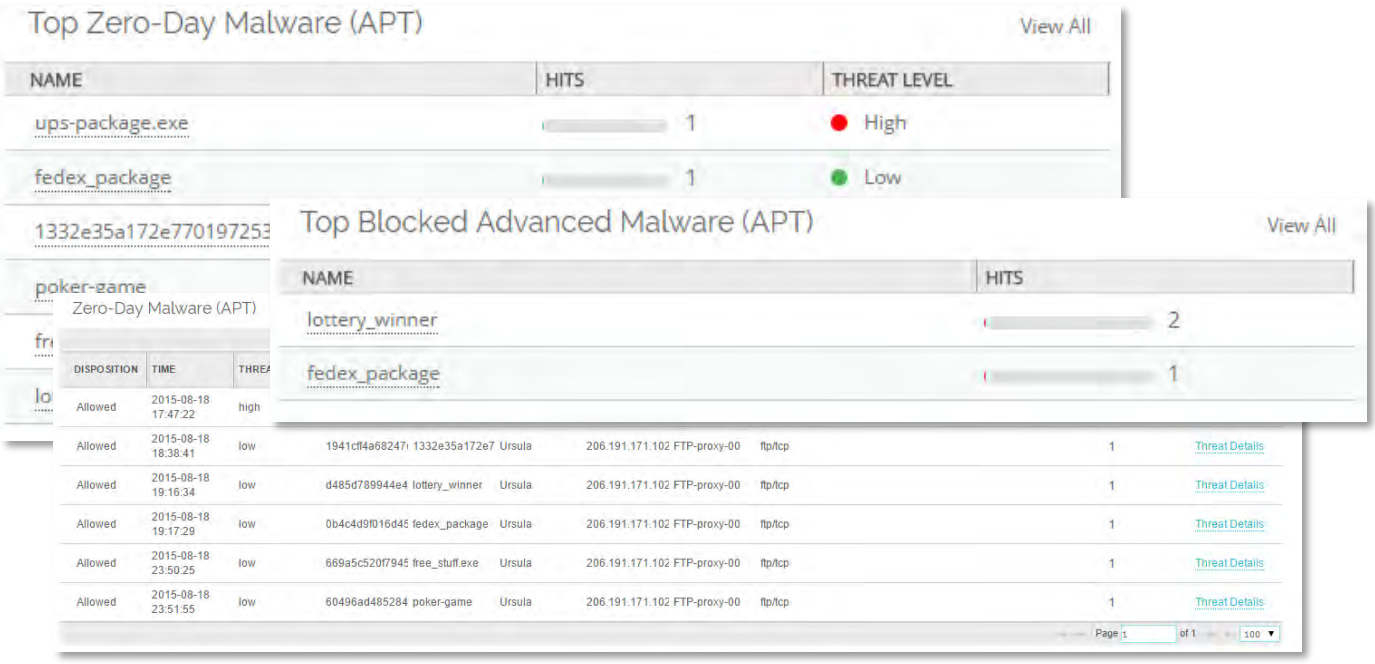

Figure 6: APT Blocker activities viewed through WatchGuard Dimension, along with other UTM services

Conclusion: Keep Your Data Safe with Advanced Malware Detection

Hacking techniques have evolved and threats to your network are becoming more sophisticated. Cyber criminals today use the same advanced techniques that were formerly reserved for high-profile nation-state attacks to target small and midsize organizations, and even tablets and mobile devices.

Security solutions need to evolve to stay ahead of threats and to keep networks safe. Signature-based malware detection is no longer sufficient. Antivirus and intrusion prevention systems are still a necessary part of any company's defense profile, but they need to be supplemented with new advanced detection capabilities with four key characteristics.

1. **Sandbox in the cloud** with full system emulation – with the ability to analyze multiple file types
2. **The ability to go beyond the sandbox** to detect different forms of advanced evasions
3. **Visibility so that network operations** staff and IT teams get clear alerts of all detected malware and explanations of why each file is considered malicious
4. **The ability to proactively take action** and block bad files

WatchGuard APT Blocker goes beyond signature-based antivirus detection, using a cloud-based sandbox with full system emulation to detect and block advanced malware and zero day attacks.

To learn more about APT Blocker and other best-in-class security services WatchGuard delivers on its Firebox security platforms, visit http://www.watchguard.com/aptblocker.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

WatchGuard® Technologies, Inc. is a global leader of integrated, multi-function business security solutions that intelligently combine industry-standard hardware, best-in-class security features, and policy-based management tools. WatchGuard provides easy-to-use, but enterprise-powerful protection to hundreds of thousands of businesses worldwide. WatchGuard is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.