Advanced Zero Day Protection with APT Blocker

White Paper

WatchGuard® Technologies, Inc.
Published: February 2016

Patches, Signatures and More

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 for which a patch was available six months earlier. 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.

Over the next several years, IT vendors responded to threats like this. Each 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. IT administrators are encouraged to patch their systems frequently to stay current.

Other defenses include Intrusion Prevention Systems **(IPS)** that use deep packet inspection to look 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 used 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 have emerged that are more advanced and resistant to the conventional defenses. Hackers have traditionally targeted large corporations but small to midsize businesses today are being attacked with the same type of malware. A common tactic for hackers to deploy an APT (advanced persistent threat) is the use of spear phishing. This is an email that appears to be from an individual or business that you know that asks for credit card, bank and other sensitive information.

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. In 2012, the WatchGuard's security research team reported on four zero day vulnerabilities that were being exploited in the wild. In 2013, we wrote alerts about thirteen zero day threats that were actively being used in the wild.[2]

Modern malware is often **Persistent** and designed to stick around. It is stealthy and carefully hides its communications, and it lives in a victim's network for as long as possible, often cleaning up after itself (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. Groups of highly skilled, motivated, and financially-backed 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.

These new strains of advanced malware are often referred to as **Advanced Persistent Threats (APTs).** Figure 2 shows a chronology of major impact attacks in the last few years. The evolution of Stuxnet to Duqu highlights how advanced techniques used by nation-states are now used by hackers for financial gain, targeting Fortune 500 companies, small and midsize businesses, government-related infrastructure, and the industrial sector.

Consequences of breaches are significant for any company. Forbes reported that sales at major US retailer Target were down almost 50% in Q4 of 2013[3] and the main reason was negative publicity around their major data security breach in the holiday season in 2013. The stock price dropped 9%. The CIO is no longer at the

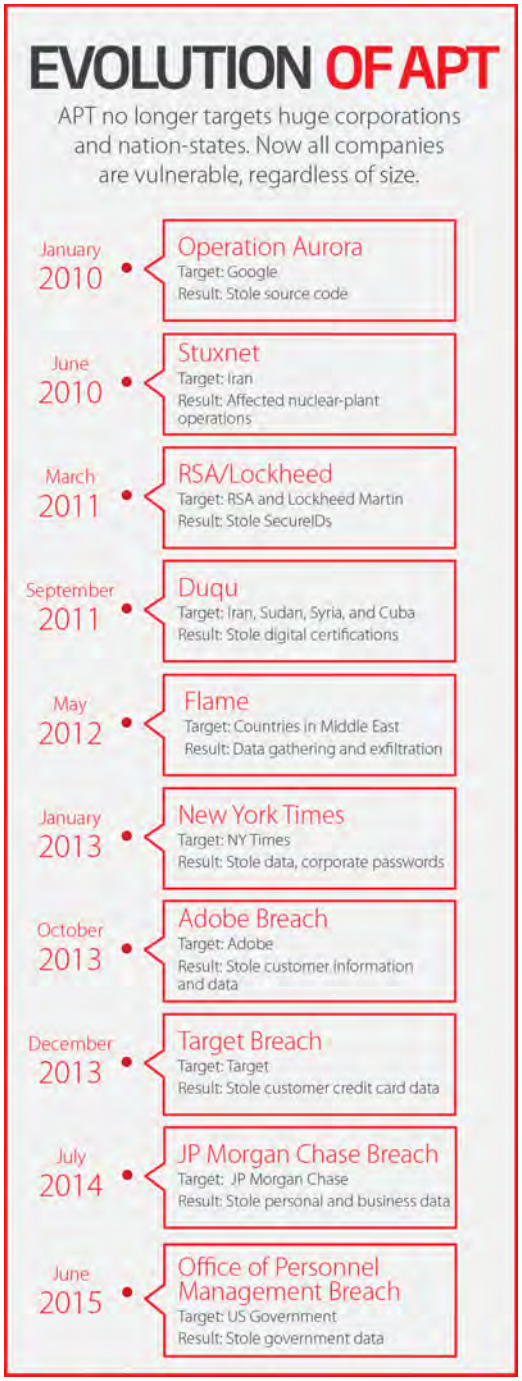

Figure 2: Evolution of APTs from 2010 through 2015

[2] Watchguardsecuritycenter.com

[3] 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/

company, and 5-10% of shoppers at Target have reported that they will never shop at the store again.[4]

In the months following the Target breach, many other large retailers revealed episodes of data loss. By the end of July 2014, the US Department of Homeland Security issued a warning that the Backoff Point-of-Sale malware and its variants had compromised 1,000+ networks. They urged companies to look for Backoff in their networks.[5]

Another company that faced public embarrassment in 2014 was Sony Pictures. A hacker group known as as the "Guardians of Peace" (GOP) not only demanded Sony to pull its film "The Interview," they claimed to have taken over 100 terabytes of the company's data. This data included unreleased films and scripts, employees' Social Security numbers, emails between employees, executive salaries, and private information.. The movie is a comedy about a plot to assassinate North Korean leader Kim Jong-un and US intelligence officials alleged the hack was sponsored by North Korea, although they have denied all responsibility.

Throughout 2014 and into 2015, the cyber attacks continued to pile up. A number of companies revealed they were hacked, which affected hundreds of millions of employees and customers in the government, financial, healthcare and transportation sectors.

- JPMorgan Chase, the largest bank in the US, was hacked in July 2014 and account information for 76 million households and 7 million small businesses was compromised. Hackers seized names, addresses, phone numbers, and emails of account holders.
- Premera discovered hackers broke into their IT systems and stole applicants' and members' information including Social Security numbers, member ID numbers, claims information, bank account information, and more. About 11 million customers were affected by this attack. The investigation revealed the initial attack occurred in May 2014 but it was not discovered until January 2015.
- The second-largest health insurer in the U.S., Anthem, estimated that personal information for around 80 million customers was compromised in the February 2015 cyber attack. The data breach extended into Blue Cross, Blue Cross and Blue Shield, Amerigroup, Caremore, and UniCare. Information such as employment information, birth dates, and more were stolen.
- Hackers attacked the Office of Personnel Management (OPM) and got sensitive information about employees who have underground background checks for security clearances. In all, about 21.5 million records were compromised in the 2015 breach.

Antivirus Can't Keep Up

The fight against malicious code is an arms race. Whenever defenders introduce new detection techniques, attackers try to find new ways to bypass them. Traditional antivirus companies employ engineers and signature writers that analyze files. They monitor the running of unknown programs in an instrumented 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 writing signatures is a losing proposition because there is an 88 percent probability that new malware has been created as a variant of existing malware to avoid detection by classic techniques.

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

[5] http://bits.blogs.nytimes.com/2014/08/22/secret-service-warns-1000-businesses-on-hack-that-affected-target/?_php=true&_type=blogs&_r=0

Lastline Labs studied the growth of evasive malware for 2014. Their research found the number of evasive techniques is growing and the percentage of evasive malware almost tripled within one year.

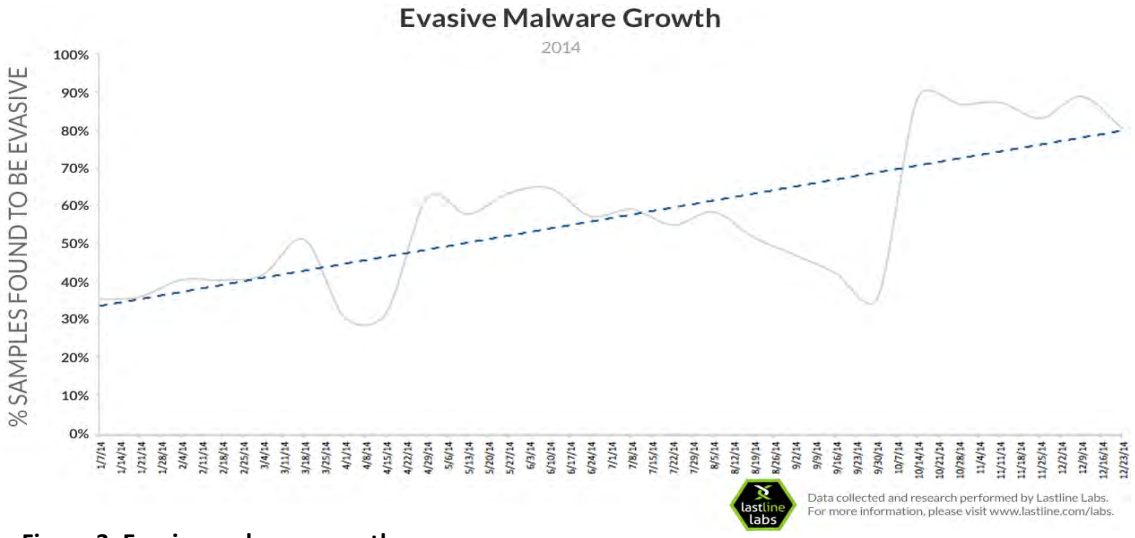

Figure 3: Evasive malware growth

Lastline also published research based on hundreds of thousands of pieces of malware they detected in one year, from April 2014 to March 2015. Each malware sample was tested against the 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.

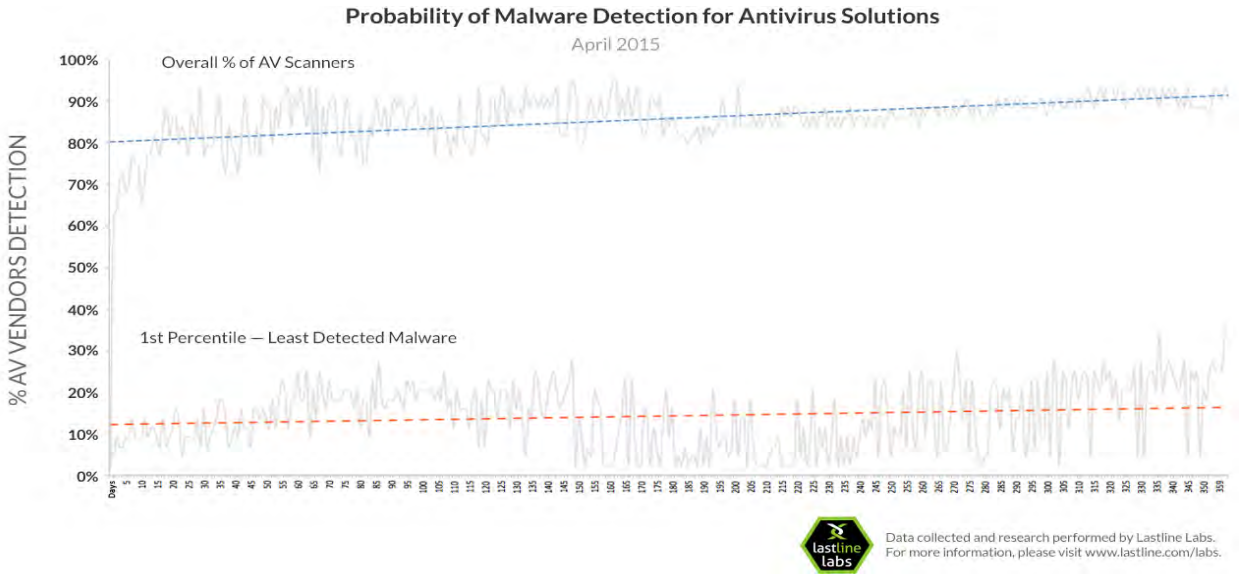

Figure 3A: Antivirus malware detection probability

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 majority of antivirus scanners.

Another type of malware that has severely impacted customers and businesses is ransomware. It commonly spreads through phishing emails containing malicious attachments or download links. Once it infects your computer, it can encrypt files making them inaccessible. And then it displays a message indicating that you have to pay a fee to obtain the encryption key to decrypt your files.

Defenses Are Evolving: Sandboxes

A new solution is required. Today sandbox solutions are used automatically as part of the detection process. Code is run and analyzed dynamically in the sandbox without any human review. But malware authors now use evasive techniques to ensure that their programs do not reveal any malicious activity when executed in such an automated analysis environment. Some common techniques used by malware are:

- Checking for the presence of a virtual machine
- Query for well-known Windows registry keys that indicate a particular sandbox
- Sleep for a while, waiting for the sandbox to timeout the analysis

Security vendors reacted by adding some counter-intelligence of their own to their systems. They check for malware queries for well-known keys, and they force a program to wake up after it calls sleep. But this approach is still reactive. Malware analysis systems need to be manually updated to handle each new, evasive trick. Malware authors who create zero day evasions can 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.

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 up the program. The program simply executes, and from the point of view of 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 the system calls. Malware authors can target this blind spot. In our example above, the stalling code is code that runs between the system calls.

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.

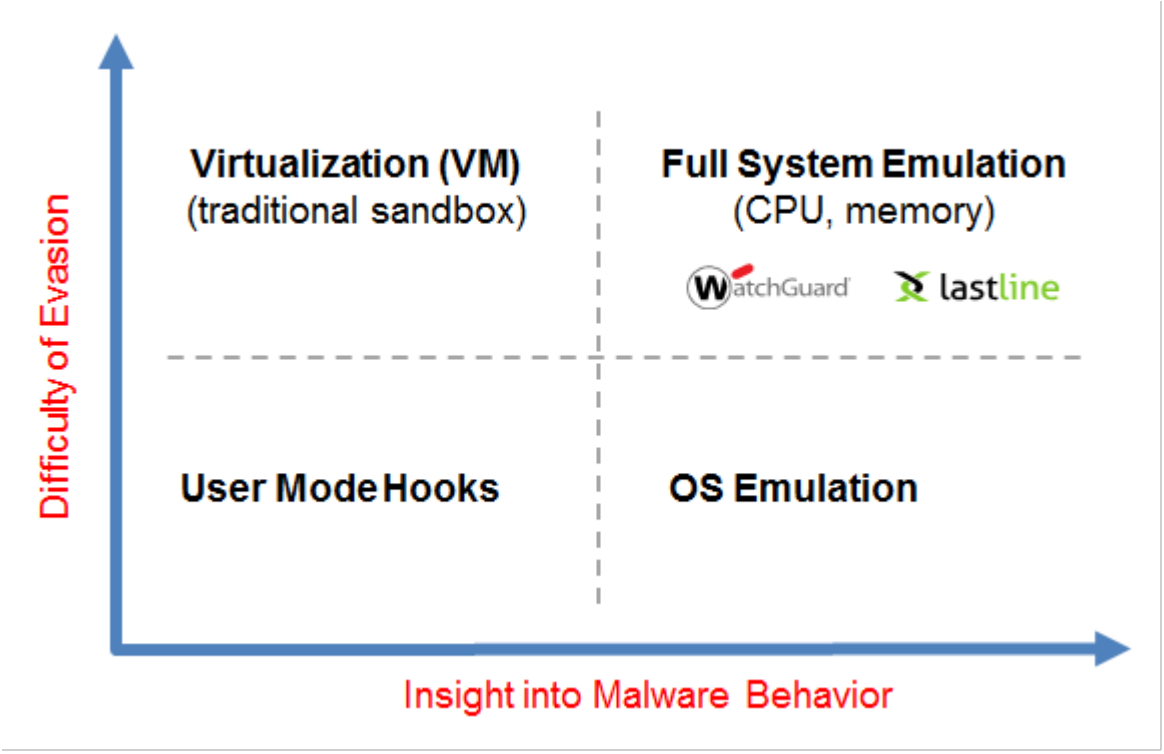

Figure 4: Full system emulation has the strongest malware detection

WatchGuard APT Blocker

APT Blocker, a service available for all WatchGuard UTM 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.[6] A comprehensive set of file types are reviewed (sidebar).

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.[7]

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.

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 had over 60,000 log incidents that showed there was malware on their network.[8] Target had log files a couple of days after the first breach indicating there was a problem but they were ignored.[9] Premera discovered the attack on January 29, 2015, but an investigation revealed that the initial attack occurred on May 5, 2014.

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

Any 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

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[10] that is included at no charge with all WatchGuard UTM and NGFW security solutions. It goes beyond a simple

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

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

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

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

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

alert saying that a file is suspicious. A detailed malicious activity report is provided for each file that is scored as malware.

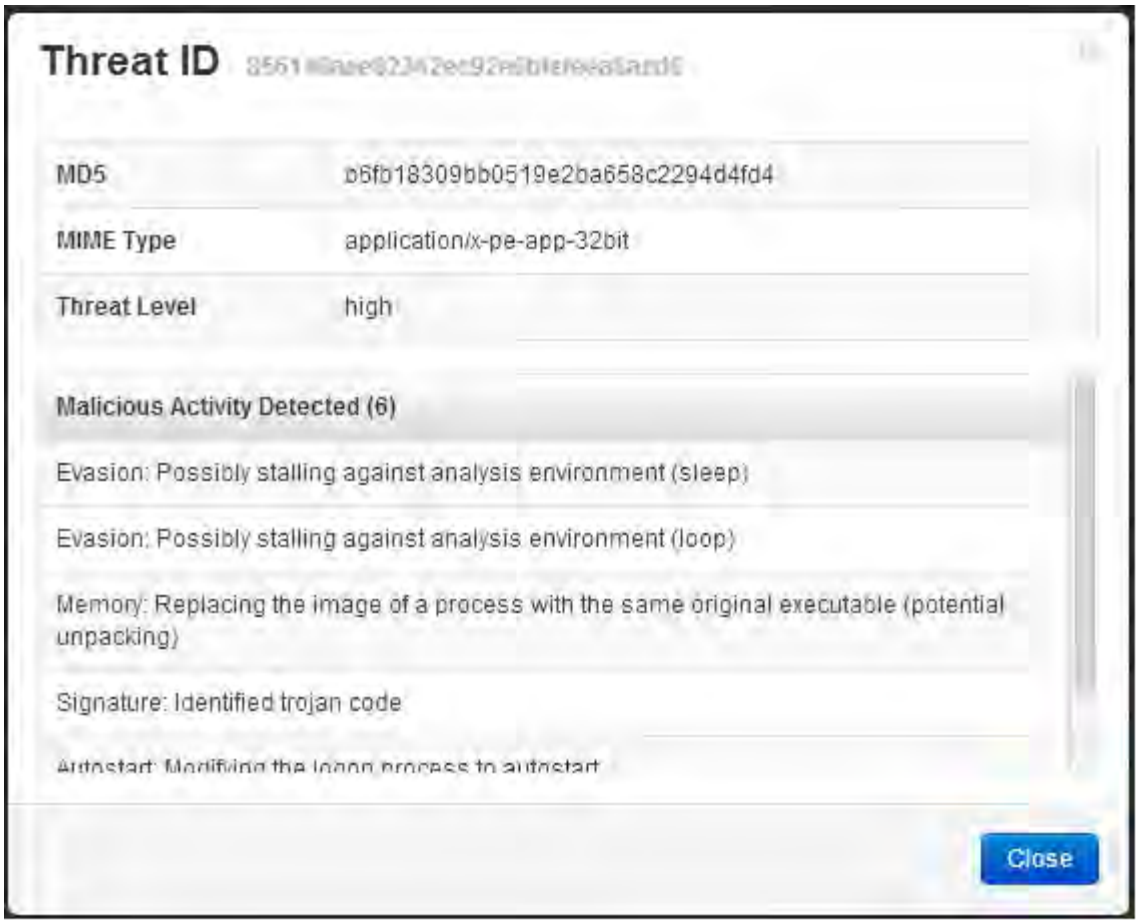

Figure 5: An APT report shows detailed Malicious Activity, explaining why a file is marked as malware

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 the 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.

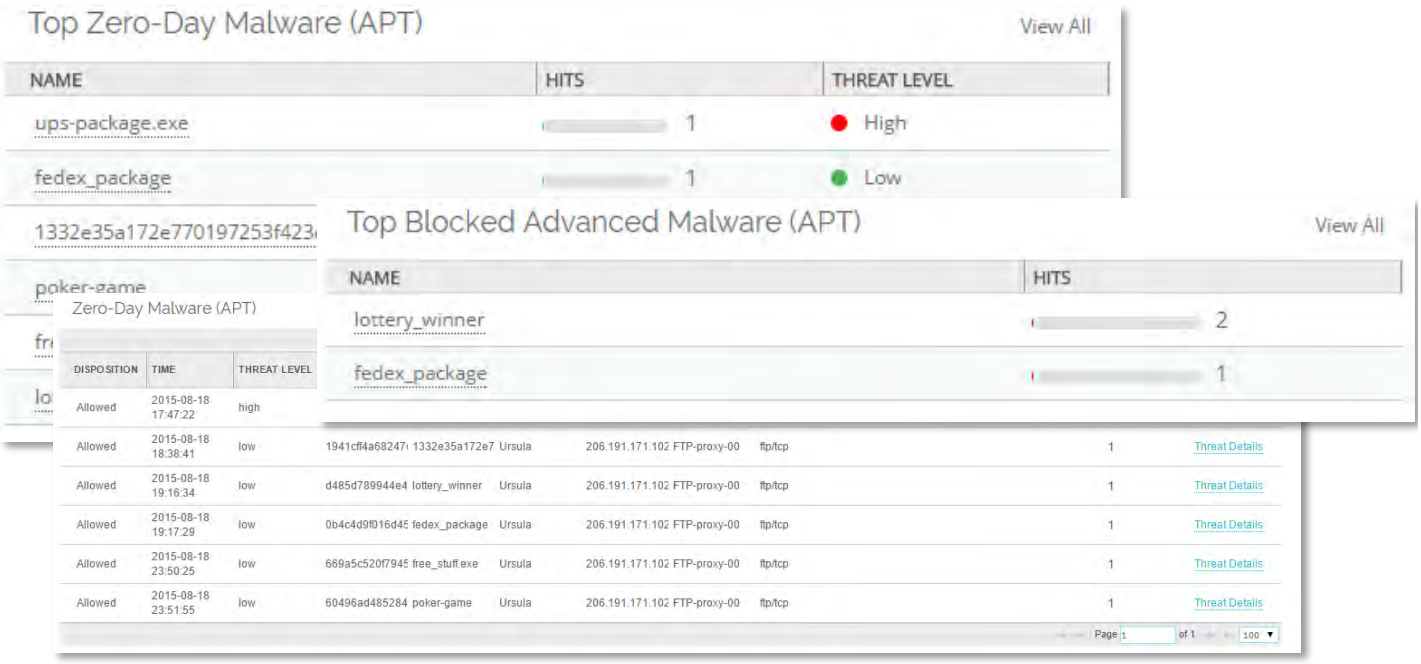

Figure 6: APT Blocker activities viewed through WatchGuard Dimension, along with other UTM services

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 used in attacks on nation states in past years to target organizations of all sizes. Experts are predicting tablets and mobile devices to be the next big targets.

Security solutions need to evolve to stay ahead of these threats and to keep your network safe. Signature-based malware detection is no longer sufficient. Antivirus and Intrusion Prevention Services are still a necessary part of any company's defense 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 your network operations** staff and IT team 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 UTM and NGFW 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, Wash. with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.