WatchGuard

Smart Security

Combating the Next Generation of Advanced Malware

White Paper

WatchGuard® Technologies, Inc.
Published: April 2014

Patches, Signatures, and the Security Treadmill

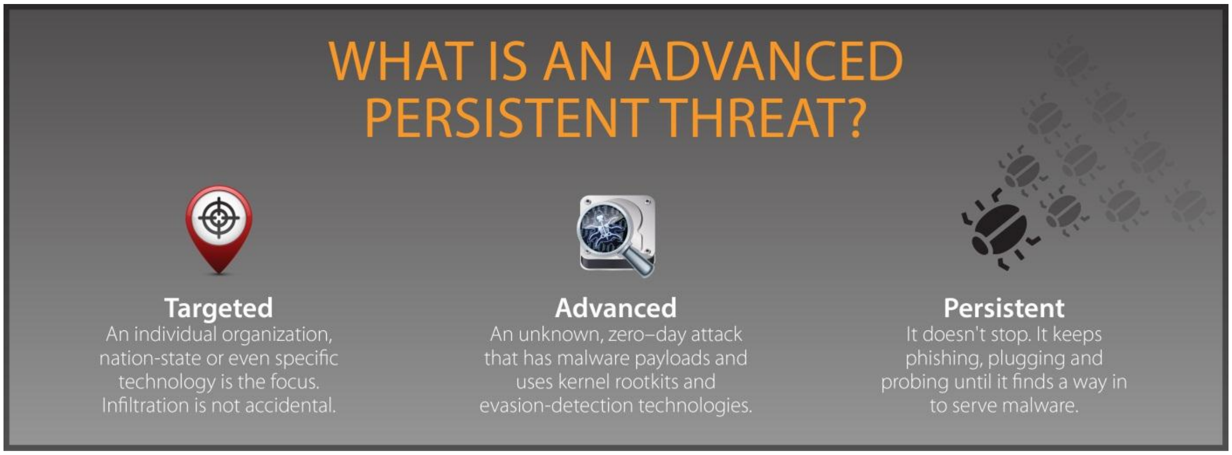
In 2003, the “SQL Slammer” worm brought Internet traffic to a standstill in many parts of the world for several hours.[1] This notorious worm targeted a known vulnerability in the Microsoft SQL database for which a patch was available six months earlier. Key to its success and proliferation was its small 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 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. Attackers have evolved over time and gotten smarter.



Targeted: An individual organization, nation-state or even specific technology is the focus. Infiltration is not accidental.

Advanced: An unknown, zero–day attack that has malware payloads and uses kernel rootkits and evasion-detection technologies.

Persistent: It doesn't stop. It keeps phishing, plugging and probing until it finds a way in to serve malware.

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 LiveSecurity® 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 the Duqu highlights how advanced techniques used by nation states are now used by hackers for financial gain, targeting Fortune 500 companies, small and medium businesses, government-related infrastructure, and the industrial sector.

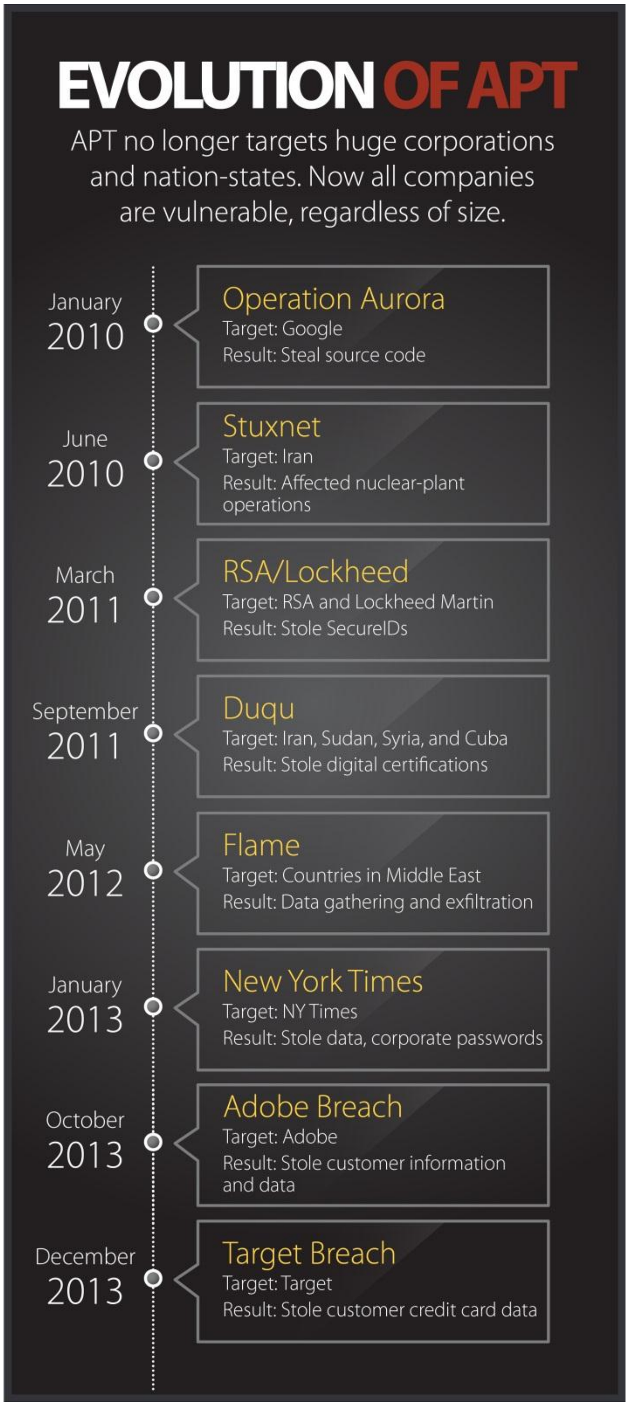

EVOLUTION OF APT
APT no longer targets huge corporations and nation-states. Now all companies are vulnerable, regardless of size.
January 2010
Operation Aurora
Target: Google
Result: Steal source code
June 2010
Stuxnet
Target: Iran
Result: Affected nuclear-plant operations
March 2011
RSA/Lockheed
Target: RSA and Lockheed Martin
Result: Stole SecureIDs
September 2011
Duqu
Target: Iran, Sudan, Syria, and Cuba
Result: Stole digital certifications
May 2012
Flame
Target: Countries in Middle East
Result: Data gathering and exfiltration
January 2013
New York Times
Target: NY Times
Result: Stole data, corporate passwords
October 2013
Adobe Breach
Target: Adobe
Result: Stole customer information and data
December 2013
Target Breach
Target: Target
Result: Stole customer credit card data

Figure 2: Evolution of APTs from 2010 through 2013

[2] http://watchguardsecuritycenter.com

Consequences of breaches are significant for any company. Forbes reported that sales at large U.S. retailer Target were down almost 50% in Q4 of 2013,[3] and the publicity around their data security breach was the main reason. The stock price dropped 9%. The CIO is no longer at the company, and 5%-10% of shoppers at Target have reported that they will never shop at the store again.[4]

Defenses Are Evolving: Sandboxes

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% probability that new malware has been created as a variant of existing malware to avoid detection by classic techniques.

Writing signatures is a losing proposition. 88% of malware detected is a variant of existing malware.

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.

[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/

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

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.

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.

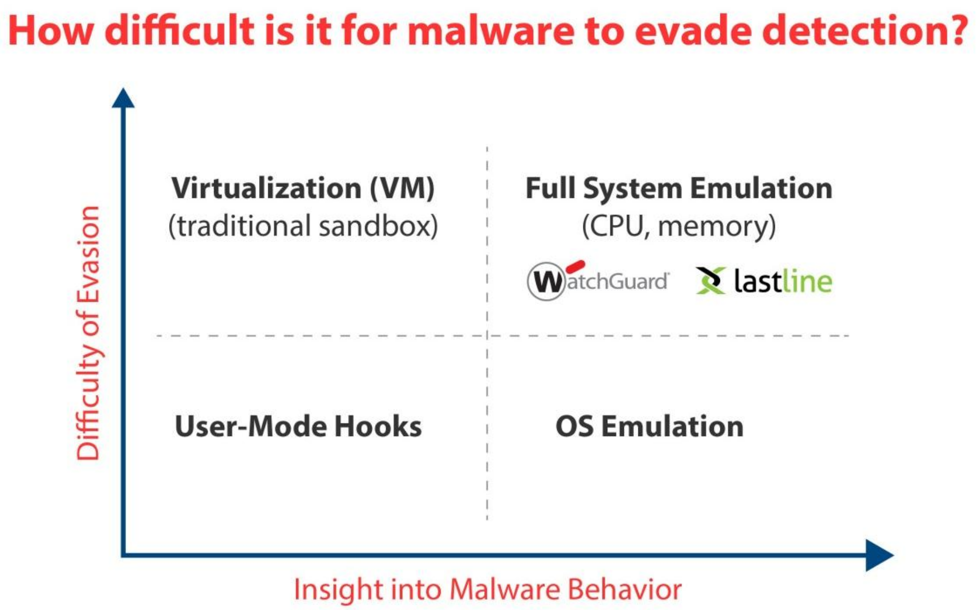


Figure 3: Full system emulation has the strongest malware detection

WatchGuard APT Blocker

APT Blocker, a new 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, 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.[5] A comprehensive set of file types is reviewed (sidebar).

File types analyzed by APT Blocker:

- **All Windows executable files**
- **Adobe PDF**
- **Microsoft Office**
- **Android Application Installer (.apk) files**
- **Packed files like Windows .zip files are decompressed**

WatchGuard selected a best-of-breed partner for the development of the APT Blocker service. 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 eight years to analyze files for potential malware.[6]

When malware is detected it can immediately get 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 alerts within minutes 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 information. 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, another U.S. retail chain that was recently breached, had over 60,000 log incidents that showed there was malware on their network.[7] Target had log files a couple of days after the first breach indicating there was a problem but they were ignored.[8]

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

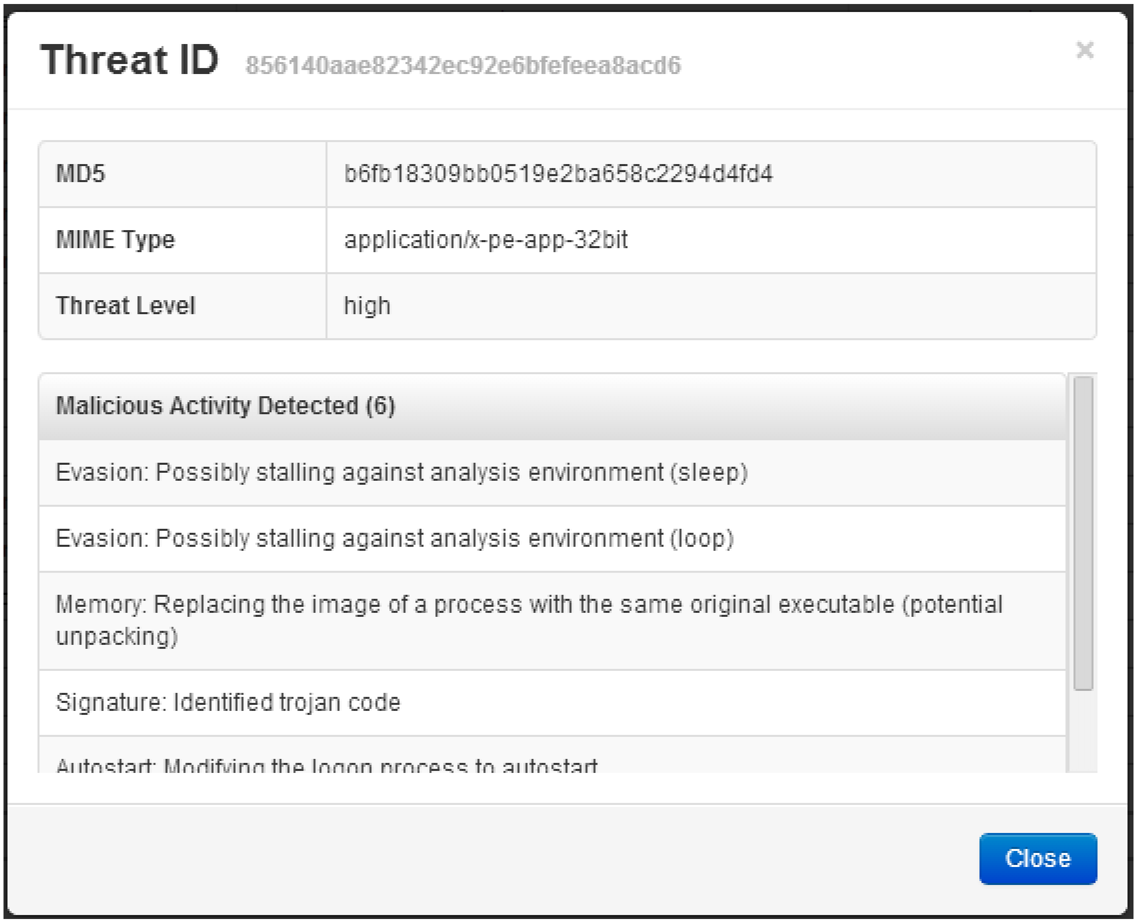
[5] http://info.lastline.com/blog/next-generation-sandbox-offers-comprehensive-detection-of-advanced-malware

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

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

[8] 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[9] that is included at no charge with all WatchGuard UTM solutions. It goes beyond a simple alert saying that is a file is suspicious. Instead, a detailed malicious activity report is provided for each file that is scored as malware.



Threat ID 856140aae82342ec92e6bfefeea8acd6

MD5	b6fb18309bb0519e2ba658c2294d4fd4
MIME Type	application/x-pe-app-32bit
Threat Level	high

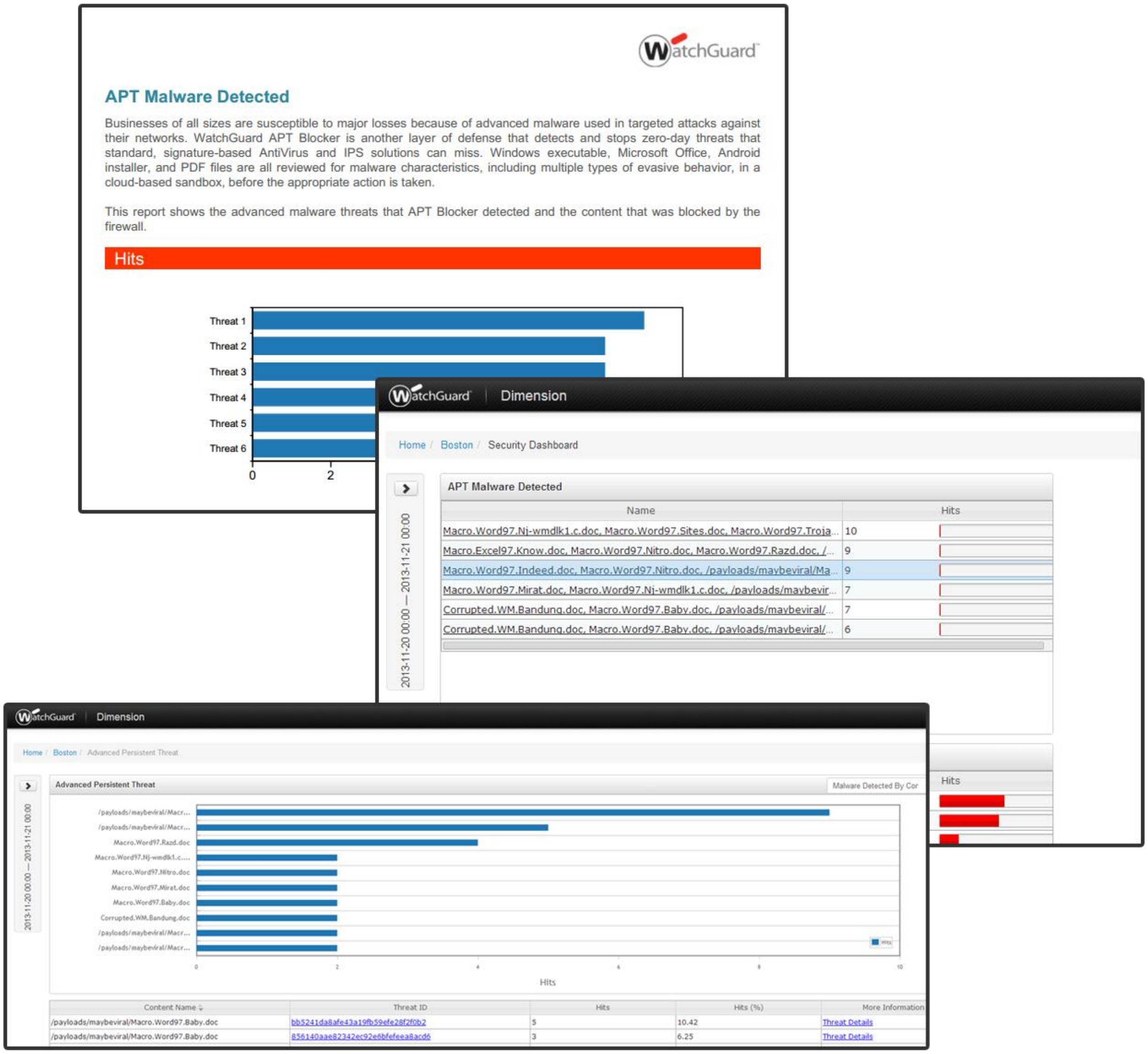
Malicious Activity Detected (6)

- Evasion: Possibly stalling against analysis environment (sleep)
- Evasion: Possibly stalling against analysis environment (loop)
- Memory: Replacing the image of a process with the same original executable (potential unpacking)
- Signature: Identified trojan code
- Autostart: Modifying the logon process to autostart

Figure 4: An APT report shows detail Malicious Activity explaining why a file is marked as malware

The example above highlights a file that shows several characteristics that are typical of malware. The two evasions demonstrate how the solution has been able to detect malicious activity that may have fooled other sandbox solutions.

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



WatchGuard

APT Malware Detected

Businesses of all sizes are susceptible to major losses because of advanced malware used in targeted attacks against their networks. WatchGuard APT Blocker is another layer of defense that detects and stops zero-day threats that standard, signature-based AntiVirus and IPS solutions can miss. Windows executable, Microsoft Office, Android installer, and PDF files are all reviewed for malware characteristics, including multiple types of evasive behavior, in a cloud-based sandbox, before the appropriate action is taken.

This report shows the advanced malware threats that APT Blocker detected and the content that was blocked by the firewall.

Hits

WatchGuard | Dimension

Home / Boston / Security Dashboard

2013-11-20 00:00 — 2013-11-21 00:00

APT Malware Detected

Name	Hits
Macro.Word97.Nj-wmdlk1.c.doc, Macro.Word97.Sites.doc, Macro.Word97.Troja...	10
Macro.Excel97.Know.doc, Macro.Word97.Nitro.doc, Macro.Word97.Razd.doc, /...	9
Macro.Word97.Indeed.doc, Macro.Word97.Nitro.doc, /payloads/maybeviral/Ma...	9
Macro.Word97.Mirat.doc, Macro.Word97.Nj-wmdlk1.c.doc, /payloads/maybevir...	7
Corrupted.WM.Bandung.doc, Macro.Word97.Baby.doc, /payloads/maybeviral/...	7
Corrupted.WM.Bandung.doc, Macro.Word97.Baby.doc, /payloads/maybeviral/...	6

WatchGuard | Dimension

Home / Boston / Advanced Persistent Threat

2013-11-20 00:00 — 2013-11-21 00:00

Advanced Persistent Threat

Malware Detected By Cor

/payloads/maybeviral/Macr...
/payloads/maybeviral/Macr...
Macro.Word97.Razd.doc
Macro.Word97.Nj-wmdlk1.c....
Macro.Word97.Nitro.doc
Macro.Word97.Mirat.doc
Macro.Word97.Baby.doc
Corrupted.WM.Bandung.doc
/payloads/maybeviral/Macr...
/payloads/maybeviral/Macr...
Hits
0
2
4
6
8
10
Hits

Content Name	Threat ID	Hits	Hits (%)	More Information
/payloads/maybeviral/Macro.Word97.Baby.doc	bb5241da8afe43a19fb59efe28f2f0b2	5	10.42	Threat Details
/payloads/maybeviral/Macro.Word97.Baby.doc	856140aae82342ec92e6bfefeea8acd6	3	6.25	Threat Details

Figure 4: APT Blocker activities viewed through WatchGuard Dimension, along with other UTM services

WatchGuard Dimension makes network security activities, such as those captured by APT Blocker, transparent and allows administrators to drill down for detailed data. Dimension includes more than 70 comprehensive reports, with the ability to pre-schedule reports for email delivery to key stakeholders in your organization. Options include summary and detail views, and special reports for HIPAA and PCI compliance. The Executive Report is a high-level summary tailored for C-level executives, IT directors, compliance officers, and small business owners.

Summary: Keep Your Data Safe with Advanced Malware Detection

Threats have evolved. Hackers today use the same advanced techniques that were previously used in attacks on nation states in past years.

Security Solutions need to evolve to stay ahead of these threats and to keep your network safe. Signatures 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. **Not just detection,** but 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 WatchGuard APT Blocker, visit www.watchguard.com/apt.

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

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. Part.No. WGCE66833_040214