A PRACTICAL GUIDE TO COMBATING ADVANCED MALWARE

What small, midsize and distributed enterprises need to know about next-generation network threats

PUBLISHED JUNE 2016
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 conventional defenses. Attackers have evolved over time and gotten smarter.

In this eBook, we’ll explain how that happened – and more importantly, what you can do about it.
DEFENSES THAT DON’T GO FAR ENOUGH

Way back in 2003, the “SQL Slammer” worm brought Internet traffic to a standstill in many parts of the world for several hours. This notorious worm targeted a known vulnerability in the Microsoft SQL database. The keys to its success and proliferation were 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. Each month Microsoft releases a series of updates to address vulnerabilities that have been found in its 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 routinely encouraged to patch their systems frequently to stay current.

Other defenses include:

**Intrusion prevention systems** (IPSs) that inspect traffic to look for known patterns of vulnerability exploits.

**Antivirus systems** to block and quarantine malware.

**Regulations like PCI DSS**, which mandate that companies keep their antivirus software updated to the latest signatures.

**Central management solutions** 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.

PATCHES, SIGNATURES, AND MORE
WHAT IS AN ADVANCED PERSISTENT THREAT?

To understand why current technologies aren’t enough to protect today’s network, we need to understand what’s different about new **Advanced Persistent Threats (APTs).**

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 is stealthy and carefully hides its communications. 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 very well-funded attackers represent significant **Threats** because they have very specific goals in mind – often financial gain from theft of credit cards and other valuable personal information.
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.

Threats
Sophisticated, difficult-to-detect threats are launched daily at targets ranging from major organizations to small and midsize businesses.
THE EVOLUTION OF ADVANCED PERSISTENT THREATS

NATION-STATE TECHNIQUES NOW USED FOR FINANCIAL GAIN

Consequences of breaches are significant for any company. *Forbes* reported that profits at large U.S. retailer Target – arguably the most notorious retail breach of all time – were down almost 50% in Q4 of 2013, and the main reason was negative publicity around their major data security breach in the 2013 holiday season. 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.

This chronology of highly publicized attacks shows how advanced techniques used by nation-states for cyber warfare became standard tools for hackers targeting government, retail, hospitality, education, and more.
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 (AV) companies employ engineers and signature writers who 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 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.

Lastline Labs published research based on hundreds of thousands of pieces of malware they detected in 2014. Each malware sample was tested against the 47 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.
• **On Day 0**, only 51% of AV scanners detected new malware samples.

• **After 2 weeks**, there was a notable bump in detection rates (up to 61%), indicating a common lag time for AV vendors.

• **Malware in the one percentile** “least likely to be detected” category (red line) went undetected by the majority of AV scanners for months and, in some cases, was never detected at all.
DEFENSES ARE EVOLVING

STEP 1: BEYOND THE SANDBOX

Today, sandbox solutions are used as part of the detection process. Code is run and analyzed in the sandbox environment. But malware authors now use evasive techniques to ensure that their programs do not reveal any malicious activity when executed in such a basic analysis environment.

Common evasive techniques used by malware include:

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

Some security vendors have reacted by adding counter-intelligence of their own to their systems. They can check for malware queries for well-known keys, and force a program to wake up after it calls sleep. But this approach is still reactive. Unfortunately, these malware analysis systems need to be manually updated to handle each new, evasive trick. Malware authors who create zero day evasions can still bypass detection until the sandbox is upgraded.
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, the stalling code is code that runs between the system calls.

LIMITATIONS OF SANDBOXES BASED ON VIRTUALIZATION
STEP 2: FULL SYSTEM EMULATION

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.
APT Blocker, a new 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, 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.4

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 right away.

**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

**LASTLINE TECHNOLOGY**

WatchGuard selected a best-in-class 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.5
MALWARE DETECTION EVASION DIFFICULTY

Full system emulation has the strongest malware detection.
STEP 3: SYSTEM VISIBILITY

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

APT REPORT SHOWS MALICIOUS ACTIVITY

The example above shows several characteristics that are typical of malware. The two evasions at the top demonstrate how the solution has been able to detect malicious activity that may have fooled other sandbox solutions.
APT BLOCKER ACTIVITIES VIEWED THROUGH WATCHGUARD DIMENSION
STEP 4: ACTIONABLE INFORMATION

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, but did not act. Target had log files a couple of days after the first breach indicating there was a problem but they were ignored.

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 that is included at no charge with all WatchGuard Firebox 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.
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. 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. **Go beyond the sandbox** to detect different forms of advanced evasions
3. **Visibility with clear alerts** of all detected malware and explanations of why each file is considered malicious
4. **Ability to proactively respond** 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, and other best-in-class security services WatchGuard delivers on its security platforms, visit www.watchguard.com/apt.**
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-grade 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.

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. ©2016 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and WatchGuard Dimension are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners.

END NOTES

1http://en.wikipedia.org/wiki/SQL_Slammer
5http://info.lastline.com/blog/different-sandboxing-techniques-to-detect-advanced-malware
6http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data