NEXT GENERATION ZERO-DAY PROTECTION: THE BEST PROTECTION AT EVERY LEVEL

THE RISE OF KNOWN AND UNKNOWN MALWARE

The term 'malware' has become so much a part of the news landscape in the last few years that many forget that it describes a series of techniques to produce undesired behaviors. Most malware falls into one of these categories: Adware, Spyware, Virus, Worm, Trojan, Rootkit, backdoors, Keyloggers, Rogue Security Software, Ransomware and Browser Hijackers. While each malware type affects computer systems differently, they all have a common set of objectives: To steal data, to perform unsolicited business transactions and/or disrupt business.

In early 2014, many news organizations around the world hailed 2013 as the Year of the Breach. That was until 2014 came to a close. According to a January 2015 report from AV-Test, an independent IT security research firm, malware incidents increased 72% from 2013 to 2014. There was more malware found in the past two years than in the previous 10 years combined. Readily available crimeware 'kits' on the Internet automate identity theft activities through social engineering. They are simple to deploy and simple to launch in large scale.

On December 18, 2014, cyber security firm CYREN observed 10.7 billion malware-infected emails sent, followed by another 10.7 billion on December 23 according to an article in IBTimes. The December attacks represent the largest-ever email-attached malware outbreak seen by CYREN, which monitors 17 billion transactions each day. These types of statistics highlight that the number of malware attacks are increasing at nearly exponential rates.

Malware complexity is also increasing as cybercriminals get better at combining techniques, masking their malware signatures and varying their attack methods. Zero-day (also called zero-hour or day zero) attacks exploit previously unknown vulnerabilities that developers have not addressed or patched. A zero-day attack is one that uses a zero-day vulnerability. Zero-day vulnerabilities are not so readily available to the novice hacker, and sell on the black market for thousands to millions of dollars. Unknown malware is malware typically not recognized or known by antivirus systems. Each new unknown malware variant, unique perhaps in only small ways, is potentially capable of bypassing even the most up-to-date anti-virus and virtual sandbox protections. According to Check Point's Annual Security Report, the rate of unknown malware downloads jumped from 2.2 per hour in 2013 to 106 per hour in 2014.

SECURITY APPROACHES TO ZERO-DAY ATTACKS

According to the site Internet Live Stats, more than 2.3 million emails are sent every second, and about 67% of those are spam. At the same time, email attachments have become the preferred method to transfer files in business. Most employees believe that once an email hits their inbox, it is safe to open.

Like changing your automobile oil every 3,000 miles, the maintenance prescription for scanning all this email used to be to install a good anti-virus program, keep it up to date, and avoid suspicious-looking files and sites. Unfortunately, that sage advice in today's world would be considered 'necessary but not sufficient' to protect against modern malware.

Malware attacks hide in executables or in regular documents (PDF, DOC etc.) and web pages. Attacks embedded in an executable are typically harder to detect. Once the end-user runs a malicious executable the attacker has full access to his system, making it easier for him to hide his true malicious intentions.

Sandboxes can be very effective for pre-screening files before they enter your network. These emulate a standard operating system (OS) in a restricted environment hosted outside your network. The sandbox stimulates an untested file in various ways as if it were opened by an actual user, then observed to see if it activates anything beyond what is normally expected. A combination of up-to-date anti-virus, along with Behavioral Analysis and Static Analysis provide reasonable protection against potentially malicious executables. An OS-level sandbox performs the Behavioral Analysis as a run-time test. The Static Analysis performs the deep scan of the code constructs within the executable. A security best practice is to block any executable not stamped by a recognized application manufacturer, e.g. Oracle, Microsoft, etc. In many cases, organizations overlook this simple protection means.

Key factors to consider in selecting a good sandbox include:

- Ability to avoid evasions
- Fast accurate detection
- Ability to block attacks, not just detect them
- Ability to decrypt SSL
- Ability to support common file-types
- Ability to support web objects such as Flash

Scanning the widest array of file types (.doc, .xls, .ppt, .pdf, .exe, .zip, .rar, etc.) including archive files is important to increasing a security layer's 'catch rate' of malicious content. If your current sandbox solution only addresses a portion of file types, you should consider upgrading, as cybercriminals embed malware into a wide array of transport files. When complemented with a mail transfer agent (MTA), the inspection process of the security system is able to avoid timeout and modify the mail in transit.

While it should be standard practice to inspect files and clear them before they enter into a network, this practice is relatively recent. In fact, due to the ease of use of implementing sandbox technologies, it is surprising that not all companies are implementing it. Those that do, find it easy to configure and not disruptive to existing deployments. Cybercriminals recognize these safeguards exist on some percentage of networks and are implementing sometimes simple and other times exotic evasion techniques. Today, the most popular sandbox bypassing techniques include:

- **Delayed launch** where the payload has a timer that delays launch after initial inspection on specific days or after few minutes/hours from initial opening
- **Identifying the sandbox** by looking for virtual machine indicators such as scanning registry keys, disk size or remote communications and not deploying if conditions are met
- **Checking for human pulse** activities such as page scrolling, mouse clicks, mouse movement that are difficult to replicate in a virtual environment

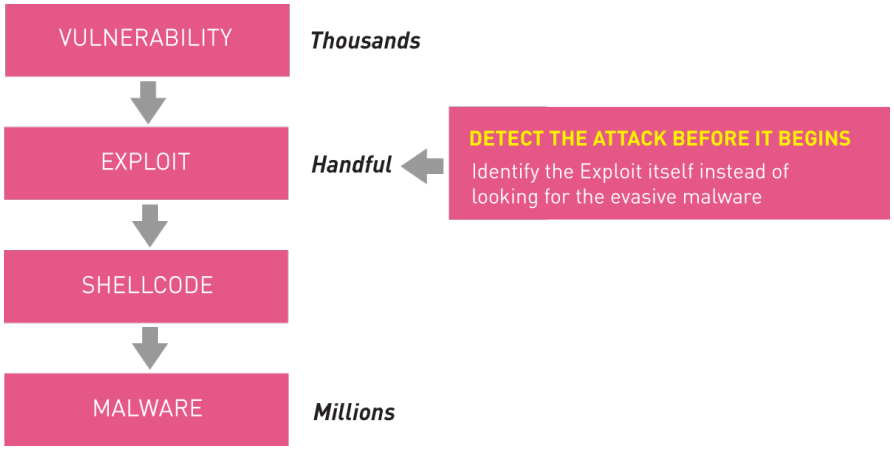
It is possible to combat many of these advanced malware techniques using dynamic OS-level sandboxing anti-evasion techniques. These include stimulating the file in different ways, multiple times, accelerating the system clock, and even emulating the CPU in software, a time-consuming tactic that often defeats its purpose, as the use of an emulator is fairly easy to detect by the malware. These approaches take time to create protections and to block the malware from entry. They are often detectable by the malware, and serve as indicators: Once the cybercriminals know you are watching, they can figure out how to avoid detection. No matter how good the OS-level sandboxing technology is, a smart cybercriminal will find some innovative way to spoof it. This requires taking a broader view and a more radical approach to threat elimination.

ANATOMY OF A NON-EXECUTABLE MALWARE ATTACK

Non-executable malware attacks are the most effective attack vector available to cybercriminals since many companies prevent the download of executable files or in allowing executables in email attachments. However, documents such as those in Microsoft Word, PowerPoint or Adobe PDF, are essential to business and are constantly entering and leaving organizations. Tricking a user into opening a document is often a simple social engineering task. Many targeted and advanced attacks begin with a spear phishing attack to trick the victim into opening a seemingly legitimate document, crafted to exploit some vulnerability and infect the system. As a result, defending against non-executable malware attacks is very critical and likely the most important defense to implement.

In looking at the anatomy of a malware attack, the millions of malware variants are activated from thousands of vulnerabilities found in computer system software. The U.S. Air Force may have defined vulnerabilities best in their 'Three Tenants of Cyber Security' analysis as the 'intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.' With this definition in mind, a malware attack typically involves four stages:

1. **Find a Vulnerability:** Every attack begins by finding one or more vulnerabilities, either in the operating system code or in a popular application such as a browser, a PDF reader etc. The attacker then uses those vulnerabilities to inject their logic into the system and trigger an attack.
2. **Use an Exploit method:** An exploit allows the attacker to use their injected logic to manipulate the target system to run malicious code. This requires overcoming built-in security controls implemented by the OS and the CPU such as DEP and ASLR. There are only a handful of exploitation methods, and new ones are very rare to surface.
3. **Run a Shellcode:** A shellcode is a small payload, typically embedded into a file or web page. By chaining one or more exploit methods, the attacker plants the shellcode into executable memory and gets the system to run it. The shellcode retrieves the actual malware and places it on the infected system.
4. **Run the Malware:** Complete the infection by running the malware.



While there are countless vulnerabilities and millions of malware, there is only a very short list of exploit methods. CPU-level sandboxing allows you to detect the use of these methods by carefully examining the CPU activity and the execution flow at the assembly code level while the exploit occurs. Not only is this OS-agnostic detection, but it makes it virtually impossible for hackers to evade detection. The detection occurs before they have a chance to employ any evasion tactic. The speed and accuracy of detection make CPU-level sandboxing the best technology in detecting both zero-day attacks as well as known and unknown attacks.

DOCUMENTS POSE GREATEST RISKS

As noted earlier, documents pose one of the greatest risks to organizations today. Last year, 84% of companies downloaded a malicious document[1]. In business functions, from human resources to purchasing and beyond, employees must routinely open documents from job applicants, customers, and vendors as part of their job responsibilities. While researching markets, competitors, and new technologies, employees regularly open documents downloaded from the web. Most employees open these documents without considering the implications, and risk exposing their companies to malware embedded inside them.

Organizations need to implement protections against the risks posed by malicious content in documents. Hackers often use macros in Microsoft Office documents to spread malicious code. In fact, the Microsoft Malware Protection Center (MMPC) has recently seen an increasing number of threats using macros to spread their malicious code. This technique uses spam emails and social engineering to infect a system. As a result, Microsoft set the default setting to "Disable all macros with notification". Even with this change, MMPC has seen new threats emerging that include some form of social engineering to convince users to manually enable macros and allow the malicious code to run once this.

Sandboxing, with its ease of deployment and use, is the preferred solution to protect against unknown malware. However, despite the ease of use of sandbox technology, its utilization in many companies is still nascent. Users want and need to see the content in a safe environment. There is a need for a complementary method of protection against threats with a simple, fast and seamless process—one that eliminates all chance of malware, before it ever has the opportunity to reach employees.

FOR MORE INFORMATION ON CPU-LEVEL SANDBOXING, PLEASE REVIEW THE WHITEPAPER CPU-LEVEL SANDBOX TECHNOLOGY.

[1] Check Point 2014 Security Report

NEXT GENERATION ZERO-DAY PROTECTION

A radical approach of threat prevention is needed—Next-Generation Zero-Day Protection. This combines innovative technologies to eliminate threats:

- Deep CPU-level and OS-level sandbox capabilities to detect and block malware
- Threat extraction to reconstruct incoming documents with zero malware in zero seconds

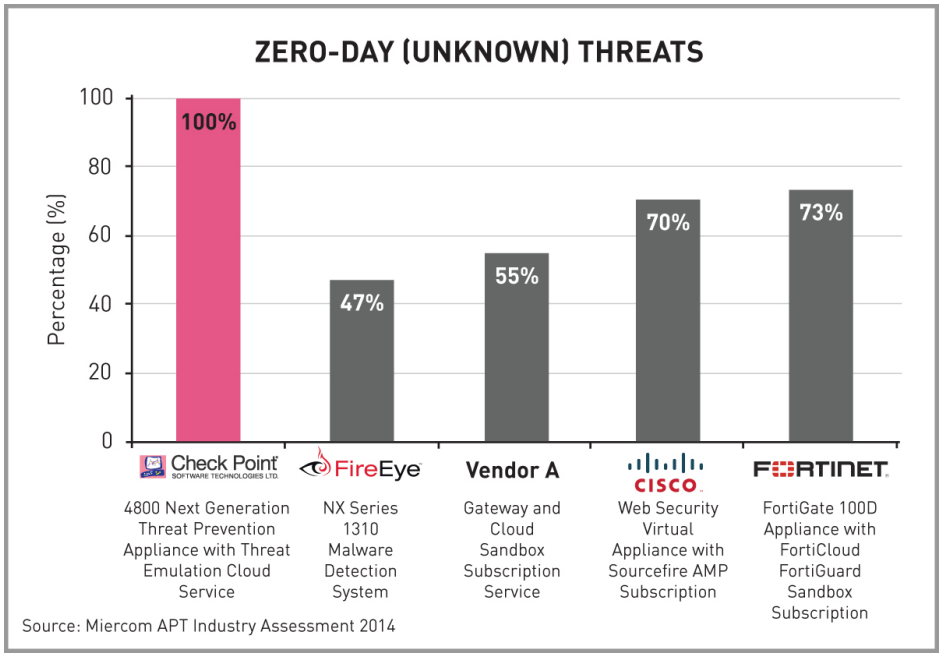
Deep CPU-level sandboxing detects an infection in data files at the exploit phase while the OS-level is used to detect attacks in both executable and data files alike. Together, they create a next generation technology that delivers the best possible catch rate for threats. Threat extraction on the other hand, delivers malware-free documents providing complete protection against any zero-day attack. Next-Generation Zero-Day Protection is the one solution that provides complete detection, inspection and protection.

THE BEST AND FASTEST CATCH RATE

When implementing Next Generation Zero-Day Protection, you get the best and fastest catch rate of malware. To evaluate efficacy and speed, Check Point conducted two tests, Zero Second and Unknown 300 Comparison Tests, which stacked Next Generation Zero-Day Protection against offerings from other vendors. The test determined (a) what percentage of unknown malware each vendor could detect and (b) how long each vendor took with its OS-level sandbox. The results of those two comparisons were the following:

- Check Point's Threat Emulation completed in four minutes and had the best catch rate of unknown malware
- Other vendors ranged from double the time at eight minutes up to 19 minutes to complete sandboxing. Their catch rate ranged from 27% to 70% of the unknown malware samples.

Definitely, a wide range of performance, but an industry assessment from Miercom on Advanced Persistent Threats (APTs) in 2014 found similar results.



Although the conclusion of the evaluations showed that Check Point OS-level sandbox techniques were the best, this is a cat-and-mouse game with cybercriminals. No matter how good the OS-level sandboxing technology is, a smart cybercriminal will find some innovative way to spoof it. To minimize that, the best sandbox technology takes both an OS-level and CPU-level approach to sandboxing.

Next Generation Zero-Day Protection elevates threat defense to a completely new level. It is the first true zero-day detection engine. It looks for malicious activities at the OS-level and exploits at the CPU-level preventing attacks before they occur. By detecting exploit attempts during the pre-infection stage, Check Point Next Generation Zero-Day Protection avoids evasion techniques. It also uses the threat extraction capability to provide protection out of the “sandbox” by eliminating the potential of threats. For the web, it delivers first pass protection that no sandboxing solution can provide today against macros. It eliminates threats from Microsoft Office and PDF documents by removing exploitable content, such as macros, embedded objects and files, and external links. Employees receive documents reconstructed with known safe elements. Providing complete protection from threats by removing potentially exploitable content, Next Generation Zero-Day Protection delivers malware-free documents to your employees with zero delay.

SUMMARY: THE BEST PROTECTION AT EVERY LEVEL

Anti-virus is necessary but not sufficient for total protection. Addressing crafty, modern zero-day cyber threats requires identifying known as well as unknown and zero-day threats both within and beyond the operating system, and delivering safe documents with zero malware in zero seconds.

In this area, Check Point innovates again with Next-Generation Zero-Day Protection technology bringing together CPU-level and OS-level sandboxing with threat extraction all in one solution. Most importantly, this complete protection approach is capable of delivering safe, secure data even faster than before. Here is how it works:

Check Point’s Next Generation Zero-Day Protection stops attacks before they have a chance to launch. Check Point’s threat prevention engine now monitors CPU-based instruction flow for exploits attempting to bypass OS security controls, adding significantly greater protection with no added latency. It also offers complete OS-level suspicious file analysis in a protected setting. The OS-level sandbox examines threats that do not use an exploit such as executables, embedded macros, JavaScript, etc., for complete coverage of all file types. You can use this capability either via the cloud-based service or locally as an appliance. It also supports web, email and file sharing in a single appliance. It comes with a suite of attack visibility tools like SmartView Tracker, Smart Log and Smart Event. This is helpful for forensics and to see what the malware detected by the CPU-level sandbox would have done, had it been allowed to run. Through the unique capability of threat extraction, you eliminate potentially malicious content from documents and files before letting them onto your network.

The best protection is a combination of the fastest operating solution that offers the top catch rate and protects your business from attack. The ultimate performance measure is productivity. With Check Point’s Next-Generation Zero-Day Protection Solution, your business receives maximum protection in zero seconds—with no disruption to productivity. Only one company keeps innovating to deliver the best security—Check Point.