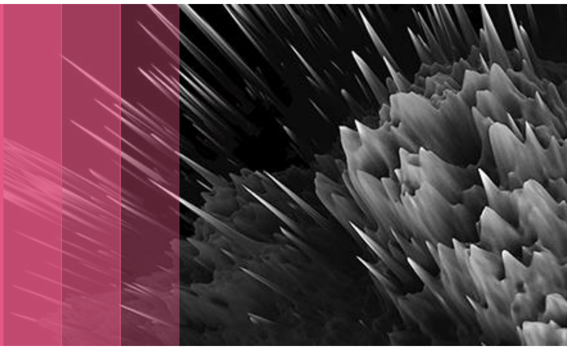
EXPOSING THE UNKNOWN:
HOW SANDBOXING TECHNOLOGY FIGHTS MODERN THREATS



EXECUTIVE SUMMARY

Increasingly skillful at stealing data and disrupting network operations, cyber criminals wreak havoc with numerous, large-scale data breaches. As these attacks happen more frequently, it's only a matter of time before your company becomes a target. Some organizations will be aware of those breaches (or even prevent them) and take corrective action, but most will not even know they happened. With the "hacking industry" approximately three to five times the size of the security industry[1], the global hacking economy is real. But what does this mean? It means that threats are imminent, multi-faceted, and evolved beyond imagination. It means your company is vulnerable.

Cybercrime is extremely advanced. Over the decades, it has caused vast destruction to both large and small companies around the world. Attackers hide malware inside documents, websites, servers, and networks. A sophisticated hacker ecosystem has evolved, with tools to share known vulnerabilities and disguise known malware to avoid detection, essentially turning old exploits into unknown threats. Typically, they focus on stealing data, sabotaging business continuity, or damaging a company's reputation.

A data breach happens when unauthorized individuals access (or steal) confidential, sensitive information. Breaches include exfiltration of confidential corporate information, personal financial details, medical information (PHI), intellectual property, and other personally identifiable information (PII). Among the types of threats, data breaches are both the most frequent and expensive security failures. With today's data moving freely between multiple internal and external networks, mobile devices, the Internet, and the cloud, without a concerted effort these breaches will continue to happen.

Learn how to better protect your business assets and deepen your understanding of the threat landscape with this white paper. Explaining the challenges enterprises face, it highlights the increasing need for comprehensive solutions to protect against advanced persistent threats and zero-day threats.

> “
>
> **WE ARE CALLED TO BE ARCHITECTS OF THE FUTURE, NOT ITS VICTIMS.**
>
> R. BUCKMINSTER FULLER
>
> ”

[1] RSA Conference San Francisco | Keynote of Martin Roesch, VP of Cisco

June 2015

THE MODERN THREAT LANDSCAPE

The threat environment of 2015 is one of relentless change. Everything is changing before our eyes – the way we work, our perceptions, the types of security threats we face, and the methods cybercriminals use to infiltrate networks and confiscate data. These new, ever-changing threats have become very complex, bringing new risks and uncertainties.

Cybercriminals skillfully use custom malware, social engineering, and spear-phishing techniques to evade detection from traditional security technology. Sophisticated hacking tools keep them one step ahead, constantly changing the threat vector – leaving many organizations struggling to keep up. New threats need new protections, making unknown malware the fulcrum of advanced attacks.... Typically, signature-based protection like antivirus (AV) and intrusion prevention systems (IPS) detect and block *known* malware from infecting the organization. However, knowing that most organizations have deployed these technologies, hackers have turned their focus towards creating *unknown* malware – often just variants of earlier code – in order to bypass these systems more readily. Threat prevention solutions must protect against both known and unknown threats in order to be effective.

Though often used loosely in the media, it's important to truly understand the terms "Zero-Day Attacks" and "Advanced Persistent Threat" (APT), how these threats behave, and the proper techniques to effectively deal with them.

> "CYBERCRIMINALS DON'T DISCRIMINATE. ADVANCED PERSISTENT THREATS HAVE TARGETED BOTH LARGE AND SMALL ORGANIZATIONS ALIKE."

ZERO-DAY ATTACKS

Zero-day vulnerabilities are previously undetected flaws in the software that do not have a current patch or fix. Attacks typically aim to compromise an operating system, a database management system or other platform technology, or a specific application. The vulnerability period can last from a few hours to several years, depending on how quickly the compromise is noticed, as well as how long it takes the vendor of the exploitable code to issue a patch. Some zero-day attacks carefully execute over a long period of time to avoid discovery, while stealing highly valuable information. For example, at Sony, hackers used spear-phishing techniques in email attachments that installed malicious code. This weakened the corporate network, and exposed sensitive corporate data, contracts, business plans, even the personal email addresses of Sony executives.[2]

Discovering a new vulnerability or creating a new zero-day threat is very difficult, but potentially very valuable to a hacker. Zero-day attacks do not have a *known* signature, and therefore can pass through antivirus, Intrusion Prevention Systems and other analysis technologies, allowing a window of time for malicious activity before it is detected. By modifying, encrypting, or otherwise disguising existing exploits, hackers can easily turn known malware into the unknown, gaining the same advantages with much less effort or skill needed.

ADVANCED PERSISTENT THREATS (APT)

Typically launched by organizations or nation-states with significant funding, APTs employ multiple attack techniques in numerous stages. APTs are extremely difficult to detect because they occur over days, weeks, months, or years. They are composed of multiple small events, which individually may seem harmless. When finally detected, it is often too late. Advanced persistent threats (APTs) are highly dangerous to an organization. Designed to infiltrate systems while evading detection, APTs allow attackers to target a company and gain access to particular assets over a period of time.

[2] Hesseldahl, Arik. "Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability." Recode. N.p., 20 Jan. 2015. Web. 04 June 2015. <http://recode.net/2015/01/20/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability/

Cybercriminals don't discriminate. Advanced persistent threats have targeted both large and small organizations alike. You don't have to be a government agency, a massive financial institution, or an energy company to become a victim. It's all about the information. Virtually all companies have information that is damaging in the wrong hands and must mitigate these threats.

THE CONSEQUENCES

The consequences of not protecting your company's data and networks are dramatic and severely damaging to all those involved. We don't have to look very far to find evidence of data and network breach catastrophes – Anthem, Target, Home Depot, and Sony, just to name a few.

There can be downtime from compromised systems, loss of intellectual property and the burden of remediation such as restoring systems from backups. With the average cost of a data breach at $154 **per record** according to Ponemon research, and many incidents involving thousands, or even millions of records, the average total cost of a single data breach rose 23 percent to $3.79 million in 2015.[3]

Reputation and Customer Trust

Data breaches cause potentially long-lasting damage to your brand and reputation. Brand value on average decreases 21% as a direct result of a security breach. Recovering and restoring your reputation takes time. Ultimately, a data breach leads to decreases in customer trust because your company wasn't able to protect their personal information.

Drained Resources

The 2013 Target breach is perhaps one of the biggest examples of the extreme financial loss for companies that fall victim to a security breach. Total reported losses to date exceed $248 million. This figure includes insurance payments, card reissuance costs for customers, liabilities to payment card networks, and expenses for legal, investigative, and consulting fees. Some sources estimate that the costs will ultimately reach more than $2.2 billion when including losses from fraudulent charges[4]. This does not include the potential costs to their customers who are concerned about identify theft and credit reputation.

Financial institutions usually have the burden of paying the costs of reissuing cards, as well as initial responsibility for fraudulent charges made on compromised credit cards. In some cases, issuers may attempt to recover these costs from retailers for not properly securing their networks and data according to industry standards such as PCI/DSS. Financial institutions can claim a vast array of damages – for costs associated with notifying customers, closing accounts and opening new ones, reissuing credit cards, and refunding any customer losses.

It's also important to note that large companies like Target and Sony are not the only ones being hacked. As described earlier, it's about the information. Cybercriminals seek opportunities in organizations of any size. They are drawn to the low hanging fruit, which make small businesses a big target. According to Trustwave research, 90% of data breaches impact small businesses.[5] They are consistently hit with social engineering and spear-phishing techniques. And the financial losses can be huge.

CONSIDER THE STATISTICS

- Every 24 seconds, a host accessed a malicious website.
- Every 34 seconds, an unknown malware is downloaded.
- Every minute, a bot communicated with its command and control center.
- Every 5 minutes, a high-risk application is used.
- Every 6 minutes, known malware is downloaded.
- Every 36 minutes, sensitive data are sent outside of the organization.

[3] Korolov, Maria. "Ponemon: Data Breach Costs Now Average $154 per Record." Ponemon: Data Breach Costs Now Average $154 per Record. CSO, 27 Mar. 2015. Web. 16 June 2015.
[4] Weiss, N. Eric, and Rena S. Miller. "The Target and Other Financial Data Breaches:." (2004): n. pag. *The Target and Other Financial Data Breaches:*. Congressional Research Service, 4 Feb. 2015. Web. 20 June 2015. <https://fas.org/sgp/crs/misc/R43496.pdf>.
[5] Trustwave. "2015 Trustwave Global Security Report." (2015): *Trustwave Global Security Report*. Trustwave, 2015. Web. 1 June 2015. <https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf>.

The Ultimate Lesson

Breaches can bring your business to its knees. They impede normal business activity and cause your business to cease functioning properly. You have the ultimate responsibility of making sure your company's information is secure. So, how do you protect your company in the digital age? You need intelligent technology that keeps up with the threat landscape – technology that can detect and block unknown threats.

THE SANDBOX SOLUTION

The word "sandbox" brings images of a child's sandpit in a backyard or on a school playground to our minds. In the software world, it's actually quite similar. Just like a sandbox is a safe environment for children to play (without destroying other parts of the backyard), a sandbox is a safe environment to evaluate suspicious files, so they don't wreak havoc on your networks and data. Sandboxing has emerged as a powerful weapon in cyber security – and rightfully so. It is extremely effective at spotting malicious files and targeted attacks that evade traditional signature-based defenses, such as antivirus technology.

Here's how it works:

Sandboxing captures an executable file or document and activates that file in a virtual machine or "emulator" that provides a deep analysis that antivirus or firewalls simply can't deliver. In this controlled environment, potential threats are unpacked and run to see exactly how the executing software behaves, without accessing production systems or the network. If executing files and/or software prove to be malicious, they are dealt with accordingly. This important security technique prevents malicious files or programs from damaging your network or confiscating your information.

For detecting unknown threats, sandboxing is very effective and absolutely necessary. As the modern threat landscape continues to evolve, sandboxing will become an integral part of every organization's overall security arsenal.

> "SANDBOXING HAS EMERGED AS A POWERFUL WEAPON IN CYBER SECURITY."

TRADITIONAL SANDBOXING

Several cyber security companies offer sandboxing technology to analyze potential malware. However, not all sandboxes are equal. Some sandboxes detect unknown malware, but do not actually *block* malware. More advanced sandboxes share information on newly identified malware with cloud intelligence networks. This expedites the circulation of new attack data, enabling connected organizations to rapidly protect themselves. With a plethora of new attack methods, understanding the difference between traditional and advanced sandboxing is important.

The traditional approach to improving unknown and zero-day malware catch rates runs suspicious files in a sandbox outside the network, 'imitating' a standard operating system (OS) for safe observation. Using sandbox tools, you activate files in various ways to simulate an actual user opening the file. Then you watch to see if it triggers anything beyond what was normally expected.

Cybercriminals are smart. They recognize these safeguards exist on some networks and implement evasion techniques. They can actually write malware that knows when it's inside a sandbox and instruct the malware not to install until it knows it's outside of the sandbox and on an actual end point device. Another common approach hacker's use is to build sleep timers into the malware, allowing it to open minutes – or even days – after infection, long after the file has been marked safe. Other common techniques include malware that notices mouse movements, or that encrypts threats in email attachments. These evolved evasions show us that the current technology in place isn't enough. Security solutions must evolve faster in order to stay ahead of hackers.

THE ADVANCED SANDBOX

Traditional (operating system-level, or *OS-level*) sandboxing solutions are a critical component for preventing zero-day attacks and can detect malware once it is running. However, using some of the techniques above, malware can still avoid detection. For that reason, advanced protection is needed: Traditional sandboxes detect attacks in both executable files and data files alike. Advanced sandboxes take these capabilities, but also add the capability to detect malware in data files before it is fully deployed, by watching activity at the processor instruction level during the exploit phase, when the attack is trying to obtain unlawful execution privileges from the operating system. Traditional sandboxing, combined with the power of exploit-focused sandboxing delivers an advanced sandbox with powerful, evasion-resistant protection that detects AND blocks unknown malware.

The goal is clear: proactively find threats and address evasion techniques. While there are still numerous vulnerabilities, there are only a handful of exploitation methods that can be used to execute the malicious payload, download the malware and activate it. Advanced sandboxing detects the use of exploitation techniques by carefully examining activity in the CPU of the sandbox host, and its execution flow at the assembly code level before the malicious payload has a chance to run. As a result, it preempts most, if not all, possibilities of hackers evading detection. The speed and accuracy of detection, and the fact that the attack is detected before the malware is even downloaded to the end point device, make advanced sandboxing the best technology in detecting unknown threats. When you combine deep OS-level and CPU-level sandbox capabilities, you get powerful next generation sandbox threat elimination.

With new advanced technology, you can now address this security gap by enabling the detection of threats at the *pre*-infection stage. Once the threat has been caught, the new (previously *unknown*) malware is then turned into a *known* and documented malware by creating a signature. Future attempts to use the same attack, will be blocked at the IPS or Antivirus stage, and will not need to be run in the sandbox again.

Advanced sandboxing contains all the capabilities of traditional sandboxing, and includes CPU-level protection, focusing on the exploitation stage of the attack. This allows you to detect and block advanced persistent threats and zero-day threats, as well as advanced malware that can evade detection by traditional sandbox technology alone.

Key Factors to Consider in Selecting a Good Sandbox Include:

- ***Detection** and **blocking of** attacks*
- *Evasion resistance*
- *Fast and accurate detection*
- *Support common file types*
- *Support web objects such as Flash*

WHY IT MATTERS

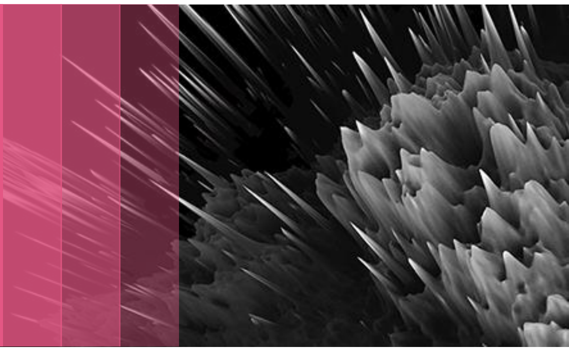
As evasion techniques evolve and get smarter, so must the technology to keep your business secure. Sandboxes address the growing and serious problems of unknown malware, advanced persistent threats and zero-day attacks. These kinds of challenges bypass antivirus technologies. Unknown malware penetrates traditional security solutions with ostensible ease. Sandboxes can detect and block these kinds of attacks before they have a chance to infiltrate your company.

Essentially, sandbox solution allows you to be *proactive* in your approach to security, rather than *reactive*. When you are constantly reacting to problems *after* they occur, rather than preventing them, it wastes time, energy, and money that your company may not have to spend.

SANDBOXING SOLUTION CONSIDERATIONS

- ✓ *Protect against the latest cyber threats:* Choose a solution with multiple layers of protection to deal with the latest cyber threats – both known and unknown. A solution that is evasion-resistant will catch more malware.
- ✓ *Prevent malicious files from entering your network:* Many solutions can only detect malware but not prevent it from infecting the network in the first place. This increases risk and compromises the security posture of the organization.
- ✓ *Inspect a wide range of file types, including all archive types:* Malware that compressed in an archive file (zip, rar, etc.) bypasses some solutions, making this attack a very common vehicle for hackers.

THE BOTTOM LINE



Every day you send and receive hundreds of files to and from organizations and individuals you trust. However, some of those documents you receive include threats against your security. Every time you open an attachment, you're taking a risk.

Many organizations have protected their systems and data by implementing antivirus software, firewalls, or further segmenting networks. As recent breaches of organizations with reasonable basic security implemented, this is no longer enough. These methods, while essential and very useful for specific types of threats, are defenseless against zero-day and advanced persistent threats. You need to evaluate and analyze potential threats before they enter your network. With sandboxing, you can prevent malicious files from infecting your company's networks by promptly putting them on lockdown. Safe files move out of the sandbox and into the public environment. Protect your company at all points.

IT'S NO LONGER AN OPTION

Even the most responsive antivirus, anti-bot, and IPS solutions cannot protect against unknown malware. Even once a new vulnerability is identified, organizations will face a window during which newly identified malware remains undetected in their networks because a patch does not exist to address the vulnerability, or has not yet been implemented within their IT infrastructure. This interval provides more than ample time for attackers to gain significant traction within your organization. Advanced sandboxing that combines both OS level and CPU level detection capabilities addresses that gap, proactively protecting your valuable assets from zero-day and advanced persistent threats.

> “
>
> WHEN YOU ARE CONSTANTLY ON THE DEFENSIVE, REACTING TO PROBLEMS AFTER THEY OCCUR, RATHER THAN PREVENTING THEM, YOU WASTE TIME, ENERGY AND RESOURCES THAT YOUR COMPANY MAY NOT HAVE.
>
> ”

These threats are real. How many more breaches must happen before companies take the correct preventative action? How long before it's realized that yesterday's security technology is not keeping pace with modern threats, and sophisticated hackers? How long before we take network and data security seriously? Perhaps one of the biggest lessons we can learn is that many of the devastating security breaches that occurred in 2014 and 2015 were preventable, had the right technology and solutions been in place.

To learn more about threat prevention and how next-generation sandboxing can help secure your company, please sign up for a free Check Point Security Checkup at www.checkpoint.com/resources/securitycheckup.

June 2015