THE NEXT CYBER ATTACK CAN BE PREVENTED

THE LATEST ATTACKS COULD HAVE BEEN AVOIDED

SandBlast™ prevented both the WannaCry and the Petya outbreaks **from the moment they started**.

Several of SandBlast technologies were key in preventing these outbreaks:

Threat Emulation
Threat Emulation blocked the infectious payloads of both Petya and WannaCry.

IPS
Check Point's IPS had protections for the exploit used by WannaCry and Petya long before the attacks erupted, effectively preventing both the initial infection and the lateral movement of these attacks. The IPS protection covered also XP systems for which a security patch did not exist at the time.

Anti-Ransomware
As the last line of defense on the endpoint, our Anti-Ransomware effectively prevented both the attacks. Check out the SandBlast prevention videos for WannaCry and for Petya.

ABSTRACT

In the wake of the recent outbreaks of WannaCry and Petya, and large breaches such as the HBO leak and Equifax, organizations are increasingly worried about their business vulnerability to cyber threats. This is for good reason – these two incidents illustrate the huge global impact and devastation that may be caused by modern cyber-attacks. Today's threat actors have more powerful and destructive tools at their disposal than ever before.

This document discusses the growing threats and potential damages posed by cyberattacks, and provides guidelines to the approaches organizations should take and technologies they should use in order to prevent the next attack.

A WAKEUP CALL

The future is here – in today's world everything and everyone is constantly connected, and people's information and transactions are completely digitized. This incredible technological era holds huge opportunities for mankind, but at the same time it means that organizations are more vulnerable and more exposed than ever before.

In May and June of 2017, the world witnessed two massive cyberattacks that demonstrated the world's fragility. The outbreaks, dubbed WannaCry and Petya, rapidly propagated by exploiting Windows vulnerability and caused tremendous damage worldwide.

The Petya attack (sometimes referred to as NotPetya) was reportedly spread through updates of a compromised Ukrainian accounting software. Once a system was infected, the attack moved laterally, exploiting vulnerabilities in the Windows operating system to infect other hosts on the network. Ukrainian banks, ministries, media, and energy companies were shut down and Ukrainian infrastructure was crippled. Although seemingly focused on Ukrainian targets, in actuality Petya generated global damage, paralyzing companies across the world and causing huge financial losses.

The WannaCry outbreak from a month earlier was even larger in scale and impact. Within a day it had infected over 230,000 computers across 150 countries. Similar to Petya, WannaCry severely impacted many companies globally. Among its victims were hospitals in the UK, carmaker Renault, Russian and German Railways, Telefónica, O2, Hitachi, LATAM Airlines and FedEx. Estimates of the total damage range from hundreds of millions of dollars to up to $4 billion. These attacks, along with others targeting health care institutions, TV productions (HBO leak) and financial services such as the Equifax breach, all present to us, in a very clear voice, the overwhelming, growing threat that cyber based attacks impose on our society and our daily lives.

Cyberattacks continue to grow at an alarming rate – in volume, sophistication and impact. As of May 2017, Check Point products detect over 17 million attacks each week, more than half of these attacks include payloads which are unknown at the time of detection and cannot be detected by conventional signature-based technology.

In this age of super powered cybercrime, the need to protect from advanced attacks is more essential than ever before. Companies must utilize cutting-edge technologies in order to remain protected.

HOW TO PREVENT THE NEXT ATTACK

The impacts of the Petya and WannaCry attacks were not inevitable. With the correct measures and technologies in place, many organizations were able to avoid these attacks.

In order to truly combat the next threats, organizations must take a proactive approach, utilizing advanced technologies that can prevent even the most evasive zero-day attacks.

The next attack can be prevented, if companies will change their view on security, and follow a few principles:

1. Maintain Security Hygiene

Maintaining solid security hygiene across all IT systems will reduce the attack surface and can help prevent or contain many attacks. The top measures and best practices that should be followed include:

- **Patching:** All too often, attacks penetrate by leveraging known vulnerabilities for which a patch exists but has not been applied. Organizations should strive to make sure up-to-date security patches are maintained across all systems and software.
- **Segmentation:** Networks should be segmented, applying strong firewall and IPS safeguards between the network segments in order to contain infections from propagating across the entire network.
- **Review:** Security products' policies must be carefully reviewed, and incident logs and alerts should be continuously monitored.
- **Audit:** Routine audits and penetration testing should be conducted across all systems.
- **Principle of Least Privilege:** User and software privileges should be kept to a minimum – is there really a need for all users to have local admin rights on their PCs?

2. Choosing Prevention Over Detection

Companies and other players in the industry often claim that attacks will happen either way, there is no way to avoid them, and therefore the only thing left to do is to invest in technologies that detect the attack once it has already breached the network, and mitigate the damages as soon as possible.

This is simply not true! Not only can attacks be blocked, Zero-Day attacks and unknown malware are also preventable. With the right technologies in place, the majority of attacks, even the most advanced ones can be prevented without disrupting the normal business flow.

3. Leveraging a Complete Unified Architecture

Many companies attempt to build their security using a patchwork of point products from multiple vendors. This approach almost always fails: it results in disjoint technologies that don't collaborate – creating security gaps, and it introduces a huge overhead of working with multiple systems and vendors. As a result of this inefficient approach many attacks are not prevented, forcing organizations to invest more on post-infection and breach mitigation.

In order to achieve comprehensive security, companies should adopt a unified multi-layer approach that protects all IT elements – networks, endpoint, cloud and mobile, all sharing the same prevention architecture and the same threat intelligence.

4. Covering All Attack Vectors

Attackers use many malicious tricks to penetrate. The top vectors include:

- **Mail or Message**
  Send a mail or text message with a malicious attachment or a malicious link
- **Web Browsing**
  Compromise the user's browser (typically through exploit kits) or trick a user to download and open a malicious file
- **Server and Systems Exploitation**
  Infect by exploiting unpatched vulnerabilities in any online host
- **Mobile Apps**
  One of the most common sources for compromising mobile devices is through mobile apps
- **External Storage**
  Physically mounted drives allow malicious files to enter without even traversing the network

THE AGE OF SUPER POWERED CYBERCRIME

The WannaCry and Petya attacks both encrypted victims' files and demanded ransom. However, these two attacks have something much more fundamental in common: both leveraged cyber-weapons which were developed by the National Security Agency of the United States and leaked to the public in April 2017.

The US is hardly the only country developing sophisticated offensive cyberwarfare capabilities. Nation-states across the globe are investing billions and employing top talent to create advanced hacking tools and cyber weaponry.

Was the NSA leak from April the last of its kind? It would be naïve to believe so. In all likelihood, we will see more military-grade cyber tools exposed in the future. The WannaCry and Petya attacks illustrate how leaked tools and knowledge from powerful threat actors put incredible firepower in the hands of common cyber criminals.

To achieve effective coverage, organizations should seek a single solution that can cover all bases, one that provides a broad prevention across all surfaces of attack, including mail, web browsing, systems exploitation, external storage, mobile apps and more.

5. Implementing the Most Advanced Technologies

Attack techniques are diverse and constantly evolving. IT systems are complex. There is no silver-bullet single technology that can protect from all threats and all threat vectors.

There are many great technologies and ideas available – machine learning, sandbox, anomaly detection, content disarmament, and numerous more. Each of these technologies can be highly effective in specific scenarios, covering specific file types or attack vectors. Strong solutions integrate a wide range of technologies and innovations in order to effectively combat modern attacks in IT environments.

The Bottom Line

Today's cyber threat landscape is overwhelming and includes various methods of growing concerns, including cyber threats that threaten our daily lives and society's welfare. The good news is that getting hit is not predetermined and can be avoided.

CONCLUSION

Even with numerous daily cyberattacks, the WannaCry and Petya outbreaks stand-out due to their rapid propagation, their devastating impact, and above all their use of leaked superpower cyber weapons. Many look upon these attacks as a wakeup call, a call to reduce business vulnerability to cyberattacks and to the disastrous potential they pose to day to day business operations.

Relying on post-infection breach detection and mitigation as the sole security strategy is a risky and dangerous paradigm.

Prevention is possible – **the next attack can be prevented!**

In order to truly combat the next threats, organizations must take a proactive approach, utilizing advanced technologies that can prevent even the most evasive zero-day attacks. Companies should seek to adopt a proven unified solution, which offers a broad multi-layered cyber protection architecture, implemented across their entire IT infrastructure and covering all attack vectors.

SandBlast, Check Point's zero-day protection suite and part of the Infinity architecture, is proven daily by protecting thousands of customers. Built to block advanced and unknown attacks, SandBlast is designed to effectively prevent the cyber-attacks that the world has yet to see.

Learn how to prevent the next attack with Check Point Infinity and the SandBlast product family.

PREVENT THE NEXT ATTACK WITH CHECK POINT INFINITY

Check Point Infinity is the only fully consolidated cyber security platform that future-proofs business and IT infrastructure across all networks, cloud and mobile. Check Point Infinity offers a multi layered set of capabilities, to preemptively block the most sophisticated known and unknown threats.

At the forefront of Check Point Infinity's focused threat-prevention, stands **SandBlast** – a family of products incorporating the most advanced zero-day prevention technologies, all sharing the same threat intelligence – based on Check Point ThreatCloud. With over 30 different innovative technologies, SandBlast focuses on prevention rather than detection, addresses all common attack vectors, and covers all IT elements – network, mobile endpoint and cloud.

SANDBLAST TECHNOLOGIES

SandBlast's technology portfolio includes:
Threat Emulation (Sandboxing) – a unique evasion-resistant sandbox technology. Threat Emulation detects and blocks unknown and zero-day malware in files and objects entering a network – through mail and web, or delivered directly to endpoints. It blends a dozens of underlying innovative technologies to facilitate the best detection rates and fastest verdict speeds in the industry.

Threat Extraction delivers sanitized threat-free files to users – in real-time, providing a high security posture while maintaining business flow. Email attachments and web downloads are sanitized on the fly, delivering safe content to users without exposing them to risks that may lurk in the original file. The original files are sent in parallel to the Threat Emulation sandbox, and can easily be retrieved by the user – if they aren't malicious.

Anti-Ransomware is an endpoint protection designed specifically to combat ransomware. Its signature-less technology is designed to detect unknown and zero-day ransomware attacks through advanced behavioral analysis and by detecting attempts to illegitimately encrypt files. Moreover, ransomware infections are automatically quarantined and if any data was encrypted then it is automatically restored.

Zero Phishing protects user credentials using signature-less identification of unknown phishing sites. The technology further protects company credentials by alerting when users reuse their corporate credentials on personal internet accounts.

Mobile Threat Defense delivers a comprehensive protection against cyberattacks for Android and IOS. The technology identifies and blocks malicious apps, and prevents network and OS attacks from compromising mobile devices.

Forensic Analysis and Incident Quarantine provides automated attack quarantine and instant actionable insight to attacks. Taking a unique approach, SandBlast's Forensic analysis makes attack information useful to any security administrator – not just forensics experts. Based on the automated forensic analysis, SandBlast automatically quarantines infections.

Intrusion Prevention (IPS) blocks attacks and exploitation attempts on networks and systems. Check Point IPS leads the industry in terms of vulnerability coverage and in the timeliness of delivering protections for new vulnerabilities – as they surface.

Anti-Bot using the unique Multi-Tier ThreatSpect™ engine, Check Point Anti-Bot technology identifies infected hosts and blocks command-and control communications, thus containing the infection and preventing data exfiltration.

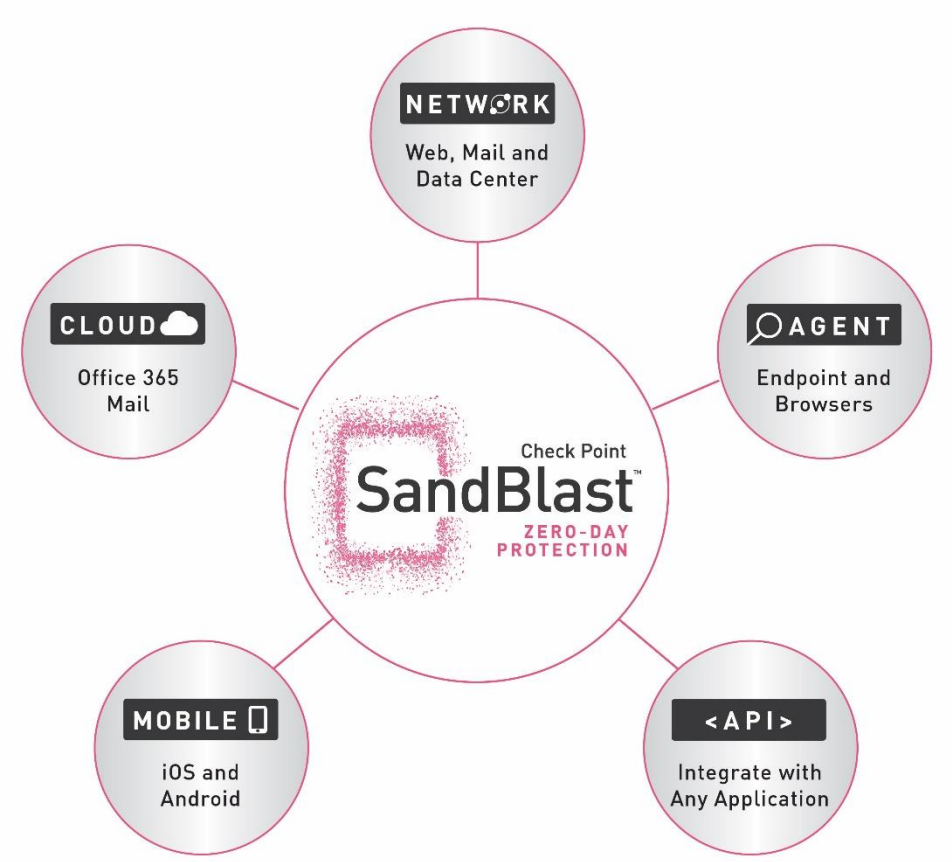
THE SANDBLAST PRODUCT FAMILY

The SandBlast solution is built upon a unified family of products, providing comprehensive multilayer protection from all attack vectors and covering all IT assets.

SandBlast Network

SandBlast for Networks offers complete protection with a unique combination of advanced threat prevention technologies – starting with the baseline IPS and AV and adding SandBlast's unique combination of Threat Emulation and Threat Extraction for proactive prevention of unknown and zero-day attacks. The solution is tuned to provide maximum security without disrupting the business flow.

The Anti-Bot protection brings networks an additional advanced defense layer by identifying compromised hosts and cutting off their command and control communications.



Check Point customers can add SandBlast protection to their existing security gateways, thus leveraging their investment in Check Point security gateways, as well as the skill-set of their existing staff.

Flexible deployment options allow for inline or SPAN-port deployment. Mail integration can be achieved via MTA and web browsing can be protected either inline or through integration with an HTTP proxy integration using the ICAP protocol.

The SandBlast network solution is fully integrated with Check Point's SSL inspection and Identity Awareness technologies providing maximum visibility and attack coverage.

SandBlast Agent

SandBlast Agent offers advanced protections to the endpoint layer, covering Web Downloads, the File System, applications and the operating systems. The direct endpoint protection adds an additional defense layer over network protections, and additional coverage for roaming users and files entering through external storage.

SandBlast Agent implements a comprehensive set of SandBlast's advanced technologies including Threat Emulation, Threat Extraction, Zero Phishing and Anti-ransomware. Incident analysis and remediation are automated through SandBlast's advanced forensics capabilities.

SandBlast Mobile

SandBlast Mobile protects organizations' iOS and Android devices, utilizing a wide range of unique technologies to protect from advanced mobile threats.

The solution integrates with existing mobile device management systems to provide improved manageability and protection.

SandBlast Cloud

SandBlast Cloud provides industry-leading security for Microsoft Office 365™ email, to prevent known threats and unknown malware from reaching end-users.

SandBlast Cloud enables organizations with cloud-hosted mail to achieve an excellent protection level by utilizing Threat Emulation and Threat Extraction to proactively prevent new, unknown and zero-day threats delivered via emails and file attachments. Antivirus and URL Reputation leverage information from ThreatCloud™ intelligence ecosystem to block the latest signature-based threats.

SandBlast Cloud is a pure cloud solution, Check Point's cloud integrates directly with Microsoft's Office 365™ cloud, customers are not required not need to deploy hardware or install any software to utilize this solution.