Check Point
SOFTWARE TECHNOLOGIES LTD.

CLOUD • MOBILE • THREAT PREVENTION

WELCOME TO THE FUTURE OF CYBER SECURITY

PREVENTING WANNACRY RANSOMWARE AND ZERO DAY ATTACKS

The WannaCry Attack

As ransomware attacks continue to rise both in frequency and intensity, their impact on business grows exponentially. WannaCry, the latest global outbreak, is particularly devastating due to its ability to spread, infect and paralyze thousands of computers beyond the initial infection point. It encrypts the data and locks out the owner demanding a minimum of $300 in bitcoin. In order to rapidly spread across networks WannaCry utilizes a Windows OS vulnerability that was recently exposed as part of the leaked NSA hacker tools.

WannaCry implements several advanced malware techniques. For example, it attempts to evade sandbox detection by resolving a non-existing DNS address. It also utilizes and encrypts its command and control communications using TOR. Some samples we have seen use an Excel-like icon, pretending to be a harmless Excel file.

WannaCry may penetrate via web or mail, or even directly through a computer with an SMB connection open to the internet. Once the initial penetration was successful it spreads laterally using vulnerabilities in unpatched Windows SMB.

Protecting with SandBlast

SandBlast advanced technologies prevented the recent WannaCry ransomware attack, even when it was still a new and completely unknown threat. SandBlast technologies are designed to be future-proof, capable of mitigating and preventing virtually all forms of ransomware and other malware – known and unknown, current and future.

Threat Emulation and Threat Extraction have been preventing WannaCry from the moment the attack campaign began. By offering evasion-resistant defense, these technologies block the initial entry over the network via mail or web, as well as protecting the endpoint from introduction of malicious files.

SandBlast Agent provides an additional defense layer directly on the endpoint. The Anti-Ransomware technology, which is part of SandBlast Agent, has prevented all WannaCry infections that reached customer endpoints and all the samples we tested in our labs, and ensured no files were lost to encryption.

How SandBlast Prevents WannaCry

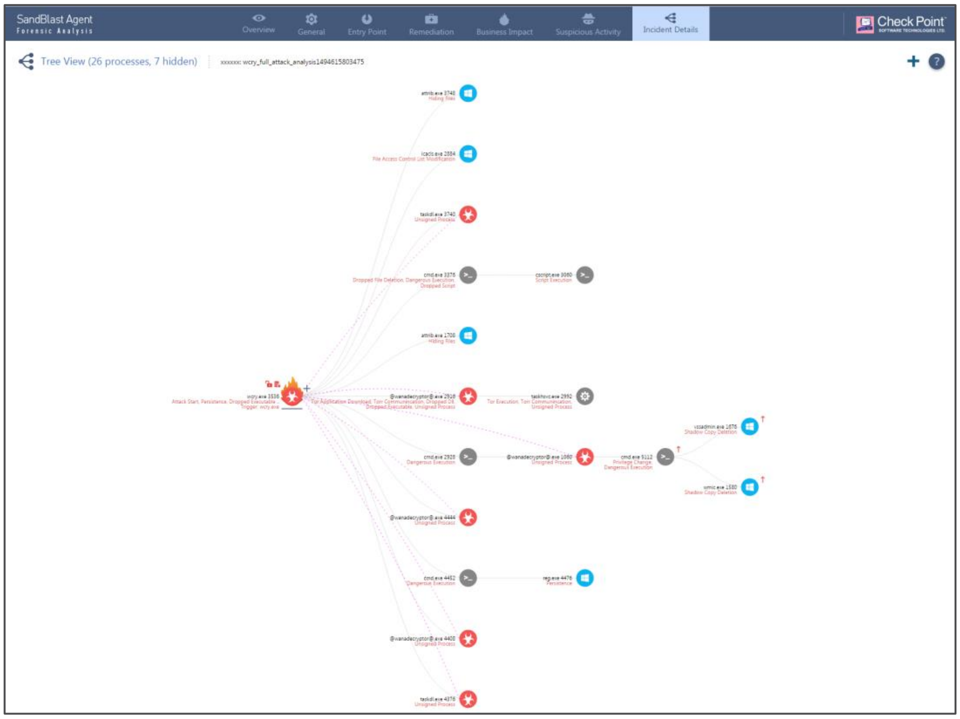
Anti-Ransomware

Check Point's Anti-Ransomware provides ransomware defense directly on the endpoint – as part of SandBlast Agent.

Anti-Ransomware prevents WannaCry by using a purpose-built behavioral analysis engine capable of detecting and remediating ransomware infections on endpoints.

WannaCry was prevented by Anti-Ransomware even when it was a completely new and unknown threat. SandBlast Agent's behavioral analysis picks up several of the ransomware's actions including shadow copy deletion and attempts to systematically encrypt files, quickly categorizing it as malicious.

WannaCry infections are automatically and fully quarantined based on SandBlast Agent's forensic analysis. Files that were encrypted are automatically restores to their original state prior to the attack containment.



Anti-Ransomware analysis of WannaCry

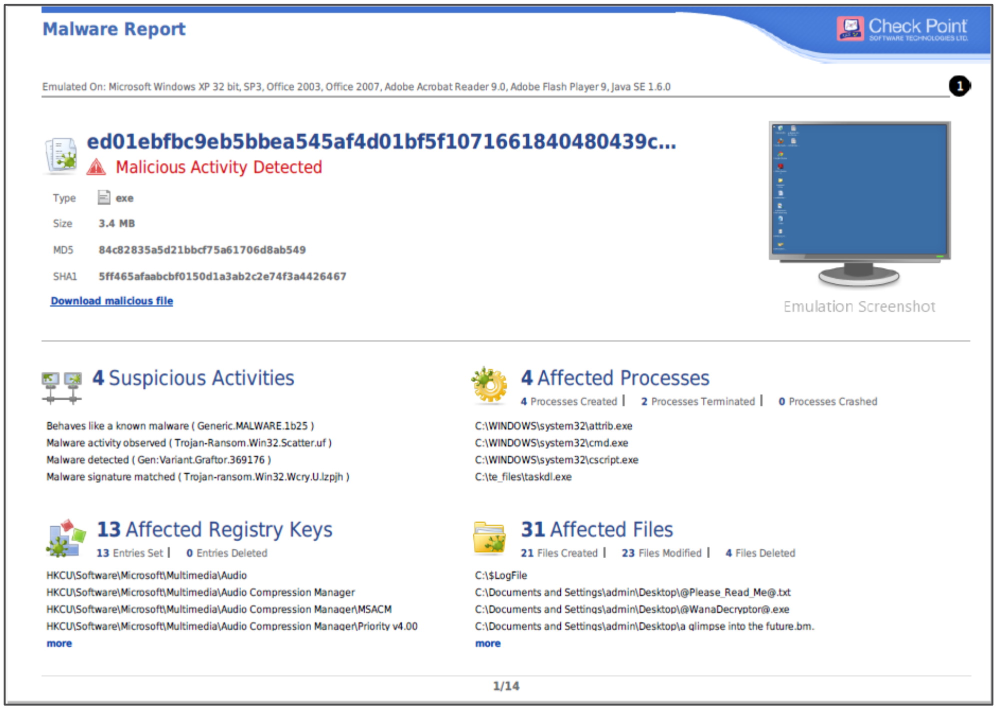
Threat Emulation

The Threat Emulation sandbox technology can be applied to both network and endpoints. It prevents entry of WannaCry via incoming mail, web browsing, web downloads and any file copied to the endpoint (e.g. from external storage).

©2017 Check Point Software Technologies Ltd. All rights reserved.

Threat Emulation identifies and prevents all known WannaCry variants and has done so from the moment the attack started.

Threat Emulation's evasion-resistant technology has proven its ability to overcome WannaCry's various sandbox evasion techniques.



Malware Report

Emulated On: Microsoft Windows XP 32 bit, SP3, Office 2003, Office 2007, Adobe Acrobat Reader 9.0, Adobe Flash Player 9, Java SE 1.6.0

ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c...

Malicious Activity Detected

Type	exe
Size	3.4 MB
MD5	84c82835a5d21bbcf75a61706d8ab549
SHA1	5ff465afaabcbf0150d1a3ab2c2e74f3a4426467

4 Suspicious Activities

Behaves like a known malware (Generic.MALWARE.1b25)
Malware activity observed (Trojan-Ransom.Win32.Scatter.uf)
Malware detected (Gen:Variant.Graftor.369176)
Malware signature matched (Trojan-ransom.Win32.Wcry.U.lzpjh)

4 Affected Processes

4 Processes Created | 2 Processes Terminated | 0 Processes Crashed

C:\WINDOWS\system32\attrib.exe
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32\cscript.exe
C:\te_files\taskdl.exe

13 Affected Registry Keys

13 Entries Set | 0 Entries Deleted

HKCU\Software\Microsoft\Multimedia\Audio
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\MSACM
HKCU\Software\Microsoft\Multimedia\Audio Compression Manager\Priority v4.00

31 Affected Files

21 Files Created | 23 Files Modified | 4 Files Deleted

C:\$LogFile
C:\Documents and Settings\admin\Desktop\@Please_Read_Me@.txt
C:\Documents and Settings\admin\Desktop\@WanaDecryptor@.exe
C:\Documents and Settings\admin\Desktop\a glimpse into the future.bm.

Threat Emulation report of WannaCry

Threat Extraction

A common delivery mechanism for Ransomware is through documents with macros, or by exploiting the document reader application. Threat Extraction provides proactive protection by delivering sanitized files to users. It ensures users are not exposed to threats such as WannaCry, which may be hidden within the original document, while still maintaining the integrity of the visual content in the document.

Threat Extraction can be applied to incoming mail and to web downloads.

Consuming the SandBlast Protections

SandBlast protections are available across all IT assets, including networks, endpoints, cloud and mobile. Protecting against WannaCry and other unknown threats requires protection in layers, addressing both the potential entry points and the potential infection points.

SandBlast Network Protection

Check Point NGTX gateways provide a wide array of advanced SandBlast zero day protections to email, web browsing and server farms.

©2017 Check Point Software Technologies Ltd. All rights reserved.

Protection technologies include Threat Emulation, Threat Extraction, IPS, Anti-Virus and Anti-Bot.

Implementing SandBlast Network protection is highly effective in preventing WannaCry initial infection and subsequent lateral movement. It also prevents numerous other advanced threats using over 30 innovative engines that offer the broadest available coverage against the modern threats landscape.

SandBlast Agent Endpoint Protection

SandBlast Agent provides comprehensive advanced protection to endpoints.

Protection technologies include Anti-Ransomware, Threat Emulation, Threat Extraction, Anti-Bot, Zero-Phishing and Forensics.

SandBlast Agent can be deployed alongside an existing 3rd party endpoint suite, or as a comprehensive solution with the **Endpoint Complete** suite.

Implementing SandBlast Agent on endpoints is highly effective in preventing WannaCry infection. It also prevents numerous other advanced threats and provides advanced forensic analysis for automated incident containment and speedy response.

Check Point
SandBlast™
ZERO-DAY
PROTECTION

THE ULTIMATE PROTECTION FROM MODERN CYBER THREATS

©2017 Check Point Software Technologies Ltd. All rights reserved.
May 14, 2017