Check Point UK Summary of WannaCry

The Attack

On May 12, 2017 the Check Point Incident Response Team started tracking a wide spread outbreak of the WannaCryptor ransomware. We have reports that multiple global organizations are experiencing a large scale ransomware attack which is utilizing a known vulnerability in the Windows SMB protocol to propagate within their networks.

The attack originated in Asia and using the SMB vulnerability spread rapidly within infected networks and across the globe.

Given the wide footprint of unpatched systems within its estate the NHS was particularly hard hit by the ransomware. The attack has spread across large and small organisations across industries in over 100 countries WW.

Entry Points

1. WannaCryptor – Direct infection utilizing SMB as delivery method
2. Hostile links within an email
3. Hostile attachments that contain a hostile link within a PDF
4. Hostile attachments that are password encrypted ZIP file which contains a PDF which starts the infection chain.
5. Brute force login attacks against RDP servers which then plant ransomware

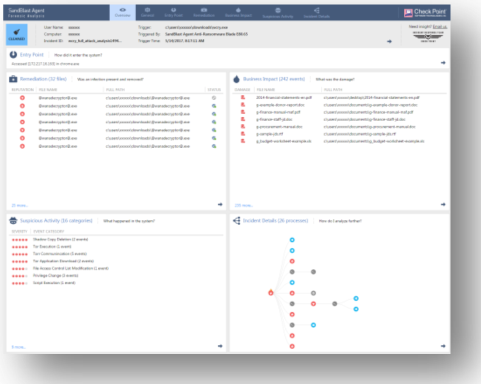
Best Practices

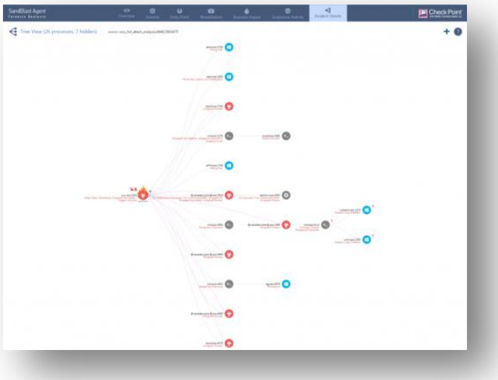
- **DO NOT PAY** – evidence suggests that WannaCry does not decrypt on payment http://blog.checkpoint.com/2017/05/14/wannacry-paid-time-off/
- **PATCH** – Windows machines should be patched for vulnerabilities discussed in Microsoft Security Bulletin MS17-010 – Critical Security Update for Microsoft Windows SMB Server (4013389) https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
- Ensure a backup is available that is not shared on the network
- Block encrypted password protected attachments from email gateways

Check Point Solutions

SandBlast

- Threat Extraction – Strips code from the e-mail attachment ensuring end user does not receive the initial malware
- Threat Emulation – detects the code in the e-mail attachment is malicious and prevents the e-mail being delivered
- Anti-Bot – detects the outbound C&C call back and blocks
- Anti-Ransomware – detects WannaCry running, blocks it and de-crypts files (see https://www.youtube.com/watch?v=5M6quttHbkI)
- Forensics – identifies all indicators of compromise and highlights machines that are vulnerable


SandBlast Agent
Forensic Analysis
Overview
Check Point
Entry Point
Remediation (32 files)
Business Impact (242 events)
Suspicious Activity (16 categories)
Incident Details (26 processes)



IPS Protections (will not work on a flat network)

- Microsoft Windows EternalBlue SMB Remote Code Execution https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0332.html
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0143) https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0177.html
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0144) https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0198.html
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0145) https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0200.html
- Microsoft Windows SMB Remote Code Execution (MS17-010: CVE-2017-0146) https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0203.html
- Microsoft Windows SMB Information Disclosure (MS17-010: CVE-2017-0147) https://www.checkpoint.com/defense/advisories/public/2017/cpai-2017-0205.html

Check Point UK Press Coverage

http://www.bbc.co.uk/news/technology-39901382
http://www.dailymail.co.uk/wires/pa/article-4500534/NHS-cyber-attack-What-Wanna-Decryptor-does-work.html
www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-hack-ransomware-world-global-security-safety-privacy-a7733236.html
https://www.thesun.co.uk/news/3549181/nhs-cyber-attack-ransomware-spreading-globe-countries-attacked/
https://www.infosecurity-magazine.com/news/nhs-ransomware-attack-goes-global/
http://www.computerweekly.com/news/450418720/NHS-hospitals-hit-by-suspected-ransomware-attack
Fri 12th May Check Point interviewed on BBC Radio 5 Live Drive Time show
Fri 12th May Check Point interviewed on BBC News (7.30pm Show)

Resources & Collateral

- Background on the attack – http://blog.checkpoint.com/2017/05/12/global-outbreak-wanacryptor/
- Why you should not pay the ransom – http://blog.checkpoint.com/2017/05/14/wannacry-paid-time-off/
- Forensics Report - http://freports.us.checkpoint.com/wannacryptor2_1/index.html
- SandBlast Agent vs WannaCry – https://www.youtube.com/watch?v=5M6quttHbkI

Useful Next Steps

Check Point's Incident Response and Threat Intelligence teams are actively working through the current outbreak at both a global and customer level. Check Point SandBlast is a range of threat prevention technologies that are proven to actively prevent both WannaCry and the various attack vectors it uses. For further information on these services and technologies please contact your partner or account manager.