WannaCry **Remediation Advisory**

HOW TO DETECT AND REMEDIATE WANNACRY WITH SKYBOX SECURITY

A GLOBAL OUTBREAK

WannaCry (also known as WanaCrypt, WanaCryptor 2.0 and Wanna Decryptor) is a new ransomware variant that exploits a group of Microsoft Windows vulnerabilities collectively known as MS17-010. They are identified in the Skybox™ Intelligence Feed by the following CVE numbers: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 and CVE-2017-0148.

WannaCry spreads quickly throughout networks by using an exploit called EternalBlue as a distribution mechanism. EternalBlue targets MS17–010 vulnerabilities and uses a worm component to propagate. In most cases, ransomware needs to be actively downloaded to each machine through a phishing email or browser vulnerability. However, WannaCry only needs to be downloaded to one machine, after which it continues to spread throughout a network via Windows Server Message Block (SMB).

Microsoft delivered a patch for supported systems affected by MS17-010 on March 14, 2017. Skybox published the vulnerabilities in the Skybox Intelligence Feed on March 15, 2017.

After assessment of real–time threat intelligence by the Skybox™ Research Lab, MS17-010 vulnerabilities were marked as “exploited in the wild” on April 18, 2017, in Skybox™ Vulnerability Control.

Some systems affected by the MS17-010 are no longer supported by Microsoft, and there were no patches available for Microsoft Windows XP, Windows Server 2003 and Windows 8 in Microsoft’s March 14, 2017, update. After the WannaCry outbreak, however, Microsoft issued patches for these systems on May 13, 2017.

Recommendations

PROTECT AND RESPOND: THE SKYBOX SECURITY SUITE

Skybox solutions for vulnerability and threat management, firewall management and security policy management can assist in the remediation of MS17-010 vulnerabilities and access rules exploited by the WannaCry ransomware variant. These solutions can also help protect against similar attacks in the future.

VULNERABILITY AND THREAT MANAGEMENT

Use Skybox Vulnerability Control to identify and remediate vulnerabilities exploited by WannaCry.

Step 1: Discovery

Skybox Vulnerability Control can identify all devices that contain the MS17-010 vulnerabilities. This identification can be performed within minutes by the vulnerability detection feature.

After remediation steps are complete, Skybox recommends repeating vulnerability detection to ensure all vulnerable devices have been addressed.

Vulnerability Control can also be used to quickly track remediation efforts by running it every few hours (this is not possible with a traditional scan).

Step 2: Prioritization

Vulnerability Control’s Prioritization Center identifies the MS17-010 vulnerabilities as being “exploited in the wild” and tags them as a critical severity.

Skybox™ Horizon also identifies high–density vulnerability hot spots throughout organizational units and across geographies, marking them for immediate triage and remediation.

Skybox’s attack simulation identifies exposure to attack from third–party and other external connections. You may wish to close off these connections to protect against future infections.

Step 3: Remediation

Apply patches and use IPS signatures, access rules and network segmentation to block attack paths.

Use the Remediation Center feature in Vulnerability Control to track the remediation status of MS17-010, ensuring that all proper procedures were carried out and no devices were omitted.

Skybox recommends adopting an approach of using Vulnerability Control to continuously monitor for new vulnerabilities and identify changes in asset exposure, as well as the emergence of new threats circulating in the wild.

FIREWALL AND SECURITY POLICY MANAGEMENT

Use Skybox™ Firewall Assurance, Skybox™ Network Assurance and Skybox™ Change Manager to change firewall or network device rules and block the propagation of the exploit.

- Identify all routes and firewall rules that are using the infected services — Server Message Block (SMB): 135, 139, 445
- Review and consider their requirement as part of network segmentation to minimize the spread of infection
- Create change requests to remove these rules and prevent further infection
- Review network topology, third-party connections and access routes
- Ensure these routes block any potential attack paths

ADDITIONAL RESOURCES

Skybox's Threat-Centric Vulnerability Management (TCVM) page has a wealth of information, including: a solution brief, technology brief on our intelligence gathering, whitepaper, Gartner report and more.

PREVENTING A SIMILAR ATTACK IN THE FUTURE

- Address underlying issues around poor cyber hygiene immediately
- Conduct a comprehensive risk assessment of all vulnerabilities in your network, including cloud and virtual environments, using Vulnerability Control
- Prioritize vulnerability remediation by "imminent" and "potential" threats using Vulnerability Control; develop a plan to remediate imminent threats immediately and track through to completion; deal with potential threats over time
- Change your approach from simple vulnerability management to threat-centric vulnerability mangement, TCVM (see Skybox TCVM)
- Identify and audit your network perimeter to ensure ingress/egress is properly identified; understand the extent of access that all third parties have into your network using Network Assurance and Firewall Assurance
- Audit network and firewall infrastructure regularly for misconfigurations using Firewall Assurance and Network Assurance
- Build compliance and risk assessments into firewall change processes using Change Manager
- Develop fit-for-purpose organizational access policies and configuration standards using Firewall Assurance and Network Assurance
- Build and maintain a detailed understanding of the assets within your network, including cloud and virtual networks, aligned to business criticality using the Skybox Security Suite platform

If you have additional questions or would like a product demonstration to guide you through any of the steps we've recommended, contact us.

About Skybox Security

Skybox arms security leaders with the broadest set of solutions for security operations, analytics and reporting. The Skybox Security Suite integrates with 100+ technologies and uses network modeling, attack vector analytics and multi-factor vulnerability assessment to give unprecedented visibility of the attack surface and key indicators of exposure (IOEs). This gives security leaders the insight needed for effective, threat-centric vulnerability management and automated firewall and security policy management across physical, virtual and cloud networks.

REQUEST A DEMO!

SKYBOX™ SECURITY

www.skyboxsecurity.com | info@skyboxsecurity.com | +1 408 441 8060