happiest minds
The Mindful IT Company

WANNACRY RANSOMWARE

How to Defend Against It

www.happiestminds.com

WHAT HAPPENED?

An unprecedented wave of ransomware infections is hitting organizations in all industries around the world popularly known as **WannaCry Ransomware.**

Multiple companies and organizations around the world were hit by variations of a crypto-ransomware dubbed WannaCry / WannaCrypt / WanaCrypt0r / WCrypt / WCRY (here on called WannaCry for simplicity). The ransomware also acts as a worm and once it infects a system, it then self-propagates throughout the rest of the network. The ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 190,000 systems. Interestingly the attack was mounted on Friday 12th May 2017, just before the weekend, making it very difficult for companies and organizations to quickly react and resolve the crisis.

Background and Attack Vector

According to numerous open-source reports, a widespread ransomware campaign is affecting various organizations with reports of tens of thousands of infections in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, India and Japan. The software can run in as many as 27 different languages.

The latest version of this ransomware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered the morning of May 12, 2017, by an independent security researcher and has spread rapidly over several hours. Open-source reporting indicates a requested ransom of .1781 bitcoins, roughly $300 U.S.

Infection & Propagation

What's particularly interesting about the WannaCry ransomware variant is its successful worm-spreading functionality. It exploits an known SMB vulnerability (Server Message Block is a Microsoft Windows protocol for file-sharing over a network) and once a system becomes infected the ransomware propagates to the rest systems of a network and infects them if they are vulnerable. Moreover, it also scans for public IPs in its attempt to infect external networks as well. WannaCry ransomware exploits an SMB vulnerability (EternalBlue/DoublePulsar) that was revealed in the recent "Shadow Brokers" leak in April 2017. The leak contains hacking tools/cyber weapons allegedly owned or developed by the NSA.

Initial reports indicate the hacker or hacking group behind the WannaCry campaign is gaining access to enterprise servers through the exploitation of a critical Windows SMB vulnerability. Microsoft released a security update for the MS17-010(link is external) vulnerability on March 14, 2017. Additionally, Microsoft released patches for Windows XP, Windows 8, and Windows Server 2003(link is external) operating systems on May 13, 2017. As per open sources, one possible infection vector may be through phishing.

Impact

Ransomware not only targets home users; businesses can also become infected with ransomware, leading to negative consequences, including

- Temporary or permanent loss of sensitive or proprietary information,
- Disruption to regular operations,
- Financial losses incurred to restore systems and files, and
- Potential harm to an organization's reputation.

Recommended Steps for Prevention

1
Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.

2
Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate in-bound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain-Keys Identified Mail (DKIM) to prevent email spoofing.

3
Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.

4
Ensure anti-virus and anti-malware solutions are set to automatically conduct regular scans.

5
Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary.

6
Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.

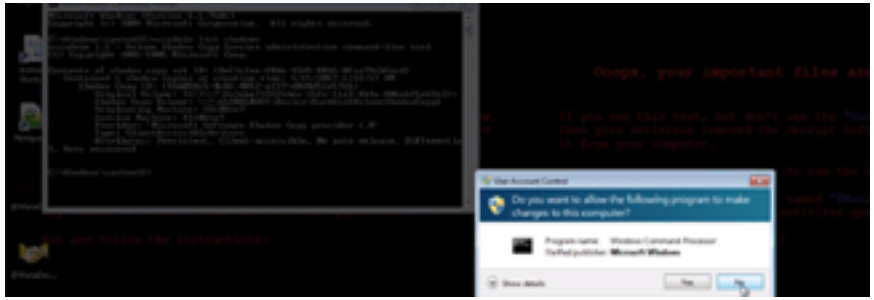
7
Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office suite applications.

8
Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.

9
Run regular penetration tests against the network, no less than once a year. Ideally, run these as often as possible and practical.

10
Test your backups to ensure they work correctly upon use.

11
DO NOT click YES on the UAC prompt window appearing during infection.



Recommendations for Network Protection

Apply the patch (MS17-010). If the patch cannot be applied, consider:

- Disabling SMBv1 and blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.
- Segregate networks and functions.
- Limit unnecessary lateral communications.
- Harden network devices.
- Secure access to infrastructure devices.
- Perform out-of-band network management.
- Validate integrity of hardware and software.

Note: disabling or blocking SMB may create problems by obstructing access to shared files, data, or devices. The benefits of mitigation should be weighed against potential disruptions to users.

Recommended Steps for Remediation

Implement your security incident response and business continuity plan. Ideally, organizations should ensure they have appropriate backups so their response is simply to restore the data from a known clean backup.

Defending Against Ransomware In General

Precautionary measures to mitigate ransomware threats include:

- Ensure anti-virus software is up-to-date.
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in emails, and do not open attachments included in unsolicited emails.
- Only download software—especially free software—from sites you know and trust.
- Enable automated patches for your operating system and Web browser.
- End user awareness and trainings
- Early identification through next gen network security and anti-malware solutions
- Capability to stop spread and lateral movement at end points leveraging advanced end-point threat detection and response
- An integrated, advanced SOC and analytics capability for early detection and faster incident response.
- Prepare ,Practice an incident response play book which can be followed in case of such major infection.

References

- Malwarebytes LABS: WanaCrypt0r ransomware hits it big just before the weekend
- Malwarebytes LABS: The worm that spreads WanaCrypt0r
- Microsoft: Microsoft Security Bulletin MS17-010
- Forbes: An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak
- Reuters: Factbox: Don't click - What is the 'ransomware' WannaCry worm?
- GitHubGist: WannaCry|WannaDecrypt0r NSA-Cyberweapon-Powered Ransomware Worm
- Microsoft: Microsoft Update Catalog: Patches for Windows XP, Windows 8, and Windows Server 2003, (KB4012598)
- Cisco: Player 3 Has Entered the Game: Say Hello to 'WannaCry'
- Washington Post: More than 150 countries affected by massive cyberattack, Europol says

About Happiest Minds

Happiest Minds enables Digital Transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights through an integrated set of disruptive technologies: big data analytics, internet of things, mobility, cloud, security, unified communications, etc. Happiest Minds offers domain centric solutions, IPs in IT Services, Product Engineering, Infrastructure Management and Security. These services have applicability across industry sectors such as retail, CPG, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality. As a Mindful IT Company, the focus is on 'Being Mindful' and 'Doing Mindful' which involves perceiving immersively, processing non-judgmentally and performing empathetically. 60 minutes in a week is committed towards inculcating a mindful approach within the organization, using a select set of tools and techniques. Headquartered in Bangalore, India, Happiest Minds has operations in the US, UK, The Netherlands, Australia, Middle East and Turkey.

happiest minds
The Mindful IT Company

www.happiestminds.com