



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 / WanaCryptOr / 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.

Wana Decrypt0r 2.0	English				
1	What Happened to My Computer? Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.				
Payment will be raised on	Can I Recover My Files?				
5152017 163252 Time Left Ø2: 23: 59: 49	Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.</decrypt>				
Your files will be lost on 5/19/2017 16:32:52 Time Left Ø 5 # 23 # 59 # 49	We will have free events for users who are so poor that they couldn't pay in 6 months. How Do I Pay? Payment is accepted in Bitcoin only. For more information, click <about bitcoin="">. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <how bitcoins="" buy="" to="">. And send the correct amount to the address specified in this window. After your payment, click <check payment="">. Best time to check: 9:00am - 11:00am Chr. form Mondaute Diday.</check></how></about>				
About bitcoin How to bace bitcoins?	Ditcoin      Send \$300 worth of bitcoin to this address:        12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw      Cop				
Contact Us	Check Payment Decrypt				

### 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**

<b>1</b> 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.						
<b>4</b> 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.						
<b>7</b> 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.		<b>8</b> Develop, institute, and practice employee education programs for identifying scams, malicious links, and attempted social engineering.	pe ag no ye as	in regular netration tests ainst the network, less than once a ar. Ideally, run thes often as possible d practical.	<b>10</b> Test your backups to ensure they work correctly upon use. e		
<b>11</b> DO NOT click YES of prompt window appe infection.		A second	A Province of the second secon	and them and a second for the second to be card, for the second to the second to the second to	Cooper, your taper tast files are realized to the second second second second second realized to the second		

### 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.

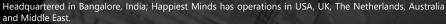
- Implement a data back-up and recovery plan to maintain copies of sensitive or proprietary data in a separate and secure location. Backup copies of sensitive data should not be readily accessible from local networks.
- Scrutinize links contained in emails, and do not open attachments included in unsolicited 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: WanaCryptOr ransomware hits it big just before the weekend
- Malwarebytes LABS: The worm that spreads WanaCryptOr
- 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|WannaDecryptOr 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, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.



Write to us at business@happiestminds.com



www.happiestminds.com