CitiusTech Whitepaper

WannaCry Ransomware:

Time to Power up your Infrastructure and Bolster your Security

What is WannaCry ransomware?

WannaCry ransomware outbreak brought over 200,000 systems to halt across 150 countries including a major hit on the National Health Service (UK), posing grave threat to confidential healthcare information.[1] There is a possibility of such global attacks striking again which could be more advance in nature, making it crucial for healthcare organizations to now have more sophisticated security solutions in place and be well prepared to protect their systems and data.

WannaCry ransomware is a type of malicious software designed to block access to computer systems until a sum of money is paid. WannaCry ransomware just needs a single Windows operating machine in a network to begin the exploit and it further propagates to other vulnerable systems in the network. It then encrypts the computer's data and warns users that the files are encrypted and can be decrypted only by paying that sum of money in bitcoins or it will delete all the files.

Fig 1: WannaCry Ransom Note

Impact of WannaCry on healthcare

Healthcare companies are the best targets for popular ransomware because they have an urgent need to restore service for their patients. They may therefore be more likely to pay criminals to reinstate systems making them relatively easy targets. We have listed below a few relevant cases which involved healthcare firms:

- Multiple emergency rooms across England spread the word that patients should avoid coming.
- Activities around hospitals were halted as the ransomware made the data unavailable until the time ransom was paid.
- Many hospital workflows like patient admission, scheduling and discharging were shifted to paper as the systems were locked down, while few hospitals had to cancel patient schedules due to the lockdown.
- Surgeries were delayed, cancelled or were shifted to other hospitals due to unavailability of the systems.
- As a precautionary measure, many hospitals had shut down their IT systems to prevent the attack.

How does WannaCry work?

The ransomware exploits an old vulnerability in Server Message Block (SMB) protocol of Windows for which Microsoft had released a security Patch (Microsoft Security Bulletin MS17-010) in March 2017. However, this attack was still widespread as many systems have not been updated with the latest patches and few organizations still use outdated operating systems like Windows Vista or XP.

For this attack to successfully work, phishing is used as an initial vector. It starts with an email with malicious attachment, where a person is required to open the attachment. It then infects the system and starts transmitting the malware to other unpatched systems on port 445. The malware will then install the code on other target machines and begin the encryption.

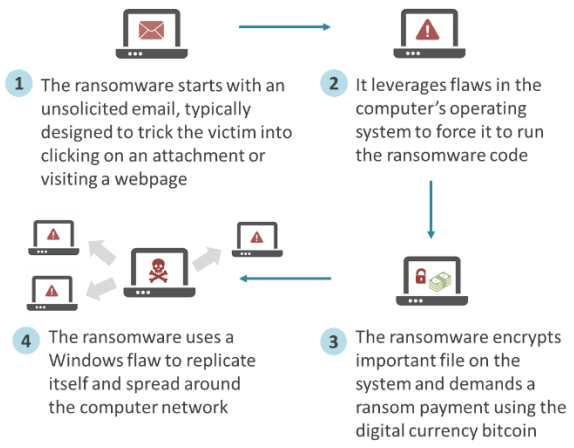

Fig 2: How WannaCry ransomware works

WannaCry is different from other ransomware as it can self-propagate over the network, can be installed on other machines in the network without any external help, and can start encrypting the vulnerable machines. In addition, even if the scale of ransoms is small while the numbers of systems impacted is large, the income of the attackers may go up over the period. Other ransomware generally sends emails to as many people as possible and only those users who click on the email are required to pay the ransom.

Kill switch for WannaCry

A 22-year-old cybersecurity researcher, identified by his online blog called MalwareTech, analyzed and identified that the WannaCry ransomware tries to connect to an unregistered domain. This led him to register the domain that prevented the spread of ransomware.

While analyzing the malware code by reverse engineering technique, it was observed that the malware was being executed only if domain name was unregistered. If domain name is found to be registered, then code execution will be terminated. In the malware code, domain name was hardcoded and so once he registered the domain name, the infections stopped.

An important point to be noted here is that this kill switch was used only to stop this sample. Hence once the attackers remove the domain check from the code and release the new variant; it will again start infecting the unpatched systems.

Recovery and prevention

Non-infected machine

- Install MS17-010 patch published by Microsoft. [2]
- Install emergency Windows patch for Windows XP that Microsoft no longer supports.[3]
- If the patches cannot be installed then disable SMBv1 and alternately, or in addition, block SMBv1. Follow the Microsoft advisory on how to disable SMB service.[4]
- If none of the above options are available, then it is recommended to either shutdown the machine or disconnect it from any form of network.

Infected machine

- Quarantine the machine by physically removing the network access by either removing the Ethernet cable or disabling the Wi-Fi button.
- Perform a full anti-malware scan on the system(s) by using any of the following:
  - F-SECURE: http://www.f-secure.com/en/web/home_global/online-scanner
  - MCAFEE- http://www.mcafee.com/uk/downloads/free-tools/stinger.aspx
  - MICROSOFT - http://www.microsoft.com/security/scanner/en-us/default.aspx
  - SOPHOS - http://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx
  - TREND MICRO - http://housecall.trendmicro.com/
- If the machine is already infected, then extent of encryption can be found out by simply searching for files with extensions .wnry, .wcry, .wncry, and .wncryt.
- If the machine is already infected, then decryption of encrypted files is not possible at present. If backup copies of affected files are available, then it is possible to restore them. CitiusTech does not recommend paying the ransom.
- In some cases, files may be recovered without backups. Files saved on the Desktop, My Documents, or on a removable drive are encrypted and their original copies are wiped-out. These are not recoverable. Files stored elsewhere on a computer are encrypted and their original copies are simply deleted. This means they could be recovered using an undelete tool.

Network-level security

Antivirus/ anti-malware solutions: Update engine and database signatures with latest updates. All reputed vendors have released the signatures to detect and block the WannaCry ransomware. The vendor list includes McAfee, Symantec, Norton, Kaspersky, Trend Micro, Microsoft Windows Defender, and many more.

Firewall protection: Block SMB ports (UDP 137, 138 and TCP 139, 445) from WAN connections at perimeter firewall. Update the operating system of the firewall with latest patches. In addition, block malicious IP addresses and domain names mentioned in the Annexure – Supporting Data. Whitelist the below two domain names:

- www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

Intrusion prevention system (IPS): Update the IPS with latest updates/ signatures and apply rules specific to WannaCry ransomware.

- Snort Rules: 42329-42332, 42340, 41978
- Trend Micro Deep Security and Vulnerability Protection Rules: 1008224, 1008228, 1008225, 1008227

Anti-spam solutions: Update the anti-spam solution with latest updates. It's a great idea to configure your webmail server to block dubious attachments with extensions like .exe, .vbs, or .scr. It is recommended to add filters for known subject lines associated with the WannaCry phishing emails as mentioned in the Annexure – Supporting Data.

Consideration for cloud-based systems

Considerations for cloud-based systems are like the one for on-premise systems – not keeping unnecessary ports open, ensuring regular backup, keeping the servers/ instances updated, and having a strong firewall, antivirus/ anti-spamware solution in place.

For peer systems (where multiple VPCs are connected and are sharing resources), set strong inbound and outbound rules for VPC to restrict connections from the ports which are not required. Do not set any rule to 0.0.0.0/0 – All. It is also applicable to non-peer connections.

Strategic steps for a long-term approach

Since the propagation of the ransomware has slowed down and is now under control, does that mean that it will not happen again? Apparently, since ransomware are large in number, they can affect the systems and lead to huge business loss. Below are strategic steps, which would help prevent a similar kind of attack affecting your systems:

Regular and early security patch updates: Keep system software up-to-date by scheduling regular updates. Solutions like Microsoft Windows Server Update Services (WSUS), IBM BigFix can be used to automate and streamline the patch management process.

A multi-layered security solution: A multi-layered security solution will include an intrusion prevention/ detection system (IPS/ IDS) with behavior-blocking components that monitor devices and look for actions typically initiated by malware. It would be accompanied by firewalls, antivirus solutions, and anti-spam solutions. It is crucial that all the components are kept updated.

Data backup on regular basis: Encrypting data is the equivalent of destroying it; protection against the destruction of data is to make copies. One of the best ways to battle ransomware that locks down servers or other systems is to maintain offsite backups.

If the file system can access the offsite or cloud-based backup, so can ransomware. Even though most enterprises already back up corporate data to an offsite location, too often these backups can be directly accessed from the system where the data originated. Many cloud-based services, for example Dropbox, allow access to storage directly from a user's file system. Instead, offsite or cloud-based backups must be stored offline and should not be directly accessible from the originating system.

Business continuity planning and disaster recovery: Rather than having a rudimentary backup policy, it is highly recommended to have either a business continuity plan (BCP) or a disaster recovery (DR) plan in place.

BCP refers to maintaining business functions or quickly resuming them in the event of a major disruption, whether caused by a fire, flood, epidemic illness or a malicious attack across the internet. A business continuity plan will outline procedures and instructions

an organization must follow in the face of disasters such as a ransomware attack; it covers business processes, assets, human resources, business partners and more. During the business continuity planning, the ransomware threat should be identified and considered and a solution around the recovery strategy from such threat should be designed.

DR plan focuses mainly on restoring IT infrastructure and operations after a crisis. It's just one part of a complete BCP, as a BCP looks at the continuity of the entire organization.

User education/ user awareness: Organizations should focus more on educating employees about good computer practices and identifying social engineering attempts and spear-phishing emails. Downloading attachments from unsolicited emails and accessing compromised sites after clicking pop-up ads are two of the most frequent vectors of infection with ransomware. Newer variants of ransomware have also been seen to spread through removable USB drives or IM clients, with the payload disguised as an image.

Establish security awareness campaigns that stress the avoidance of clicking on links and attachments in email. Users should ask themselves these questions when receiving an email message with a link or an attached file: 1) Do I know the sender? 2) Do I really need to open that file or go to that link? 3) Did I really order something from the sender?

Red teaming for readiness assessment: A full-scope, multi-layered attack simulation designed to measure how well your people, networks, applications and physical security controls can withstand an attack from a real-life adversary should be conducted at least once a year. The CitiusTech Security Practice team can help you perform the red team attacks and test your organization's readiness against cyber-attacks and ransomware attacks.

Restrict administrative rights on endpoints: Organizations should remove administrative rights from all users. Administrative rights on enterprise endpoints provide users with complete control over the device. These rights allow users to install software, change the Windows Registry settings, change a wide variety of configuration files and generally do whatever they want on the device.

So, why are administrative rights a problem? Mainly because users might change the endpoint configuration or install unauthorized software. If a user installs benign unauthorized software, at most, it will become a nuisance. However, if unauthorized software is malicious and installed under administrative rights, its impact can be devastating. Additionally, since many Windows vulnerabilities that enable code execution do so in the context of the logged-in user, exploits might be able to execute without any restrictions on the endpoint. Therefore, limiting administrative privileges for corporate end users improves the organization's security posture by reducing the attack surface significantly.

Security information and event management (SIEM) software: With an updated antivirus or firewall configured with a proper consideration of a company's rules of network traffic control, it is still impossible to guarantee that a security system can resist a ransomware attack. Since no security solution provides iron-clad protection against ransomware, the more security layers an IT network has, the higher its potential would be to catch ransomware infection before it starts running. A comprehensive SIEM-based approach to detecting ransomware in a network is recommended; as such an approach ensures a holistic overview of a company's IT environment from a single point of view in terms of its specific security events.

SIEM will help in monitoring of network traffic, behavioral analysis, operating system logs monitoring and correlating inputs from all these to further pinpoint any specific threats.

Using software as a service (SaaS) products: Using the applications from SaaS-based model paired with protected user data can be a winning model; however, if the user data is not protected, then it is as unsafe as on-premise deployment model.

Using virtual desktops: Historically, non-persistent virtual desktops have provided a degree of immunity to malware. If the virtual desktop operating system gets infected with a more traditional form of malware; at the end of the user's session the virtual desktop would be rolled back to a pristine state, thereby eliminating the infection. Depending on which form of ransomware the user has contracted, it may attack the contents of the user's profile folder i.e. documents, photos and so on, or it could end up encrypting any data found on mapped network drives. In either case, the user's data has been encrypted, and the virtual desktop operating system is infected with a ransomware.

Virtual Desktop Environment can be made safer by configuring it securely by protecting the network drives, using private VLANs to isolate VMs from one another, removing local admin rights from users, prohibiting execution of unsolicited programs, etc.

References

[1] The Telegraph
[2] Microsoft Security TechCenter
[3] Microsoft Download Center
[4] Microsoft Support

Other References

- Microsoft Customer Guidance
- Malware Tech Kill Switch Analysis
- Symantec Information
- Sophos Knowledge Base
- McAfee in detail analysis
- Kaspersky Blog
- VMWare Blog
- Trapx

Authors

Mahesh Gharat
Senior Manager & Security Practice Lead, CitiusTech
mahesh.gharat@citiustech.com

Mahesh has more than 16 years of strong information security experience, with a focus on vulnerability assessment, penetration testing, web application security testing, mobile application security testing, and network architecture reviews. He is a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Ethical Hacker (CEH), ISO 27001 Lead Auditor, BS 25999 Lead Auditor, and Information Technology Infrastructure Library (ITIL) certified.

Adarsh Dharmavarapu
Technical Lead, CitiusTech
adarsh.dharmavarapu@citiustech.com

Adarsh has more than 5 years of strong healthcare IT experience and is part of the CitiusTech Security Test Practice. He is HL7 V2.6 and CDA certified and is also a certified Ethical Hacker. Adarsh has a rich healthcare domain experience including having worked on implementation of EHRs, dialysis workflows and patient health population workflows.

Annexure: Supporting data

Type	Details
Phishing mail subjects	Aviso – depósito a Cuenta Interbancaria PAGO DE SERVICIO CIE RETIRO DE EFECTIVO EN ATM AJENO Alertas Bancomer Móvil FISCAL CREDIT TAX COLLECTION TRASPASO DE TERCEROS BANCOMER (TDC) TRASP CTAS BANCOMER(CON O SIN CHEQUERA) TRASPASO CUENTAS PROPIAS (TDC) TRASPASO INTERBANCARIO Activacion de TOKEN Alertas Bancomer.com Comprobante / Notificación – Retiro de Efectivo ULTIMOS DíAS PARA ACTUALIZAR TUS DATOS Transferencia Banca en Lnea ACTIVACION TDC ACTUALIZA TUS DATOS Y USA TU TARJETA ACTIVACION TDD BLOQUEO TDD RECEIVED TRANSACTION FILE
Malicious domains	ofdwcjnko.us peuwdchnvn.us pvbeqjbqrslnkmashlsxb.us pxyhybnyv.us qkkftmpy.us rkhlkmpfpoqxmlqmkf.us ryitsfeogisr.us srwcjdfrtnhnjekjerl.us bqkv73uv72t.com wwld4ztvwurz4.com bqmvdaew.net thstlufnunxaksr.us udrgtaxgdyv.us w5q7spejg96n.com xmqlcikldft.us yobvyjmjbsgdfqnh.us yrwgugricfklb.us ywpvqhlqnssecpdemq.us 43bwabxrduicndiocpo.net dyc5m6xx36kxj.net 76jdd2ir2embyv47.onion gurj5i6cvyi.net bcbnprjwry2.net quvdaew.net sxdcmuaSae7saa2.net rbacrbyq2czpwn15net ow24dthuhwx6uj.net fa3e7yyp7slwb2.com ww|d4ztkurz4.com bqu73uv72t.com xanznp2kq.com chy4j2eqieccuk.com

Type	Details
	lkry2vwbd.com ju2ymymh4zlsk.com graficagbin.com.br iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com sdhjjekfp4k.com cwwnhwhlz52ma.onion gx7ekbenv2riucmf.onion xxlvbrloxvriy2c5.onion 57g7spgrzlojinas.onion
Malicious IPs	188.166.23.127:443 193.23.244.244:443 2.3.69.209:9001 146.0.32.144:9001 50.7.161.218:9001 87.7.10.93 192.42.115.101 178.62.197.82 212.47.244.98 5.35.251.247 128.31.0.39 91.219.236.222 128.310.39 144.76.92.176 148.244.38.101 149.202.160.69 163.172.149.155 171.25.193.9 195.22.26.248 197.231.221.221 198.96.155.3 213.61.66.117 46.101.166.19 62.210.124.124 91.121.65.179 91.219.237.229 217.79.179.177 212.47.232.237:9001 81.30.158.223:9001 79.172.193.32:443 38.229.72.16:443 46.101.166.19 23.254.167.231

About CitiusTech

CitiusTech is a specialist provider of healthcare technology services and solutions to medical technology companies, providers, payers and life sciences organizations. CitiusTech's services and solutions include healthcare software development, healthcare interoperability, regulatory compliance, BI/analytics, consumer engagement, care coordination and population health management. CitiusTech helps customers accelerate innovation in healthcare through a number of solutions and accelerators for clinical quality reporting, big data, cloud computing, mobile health and predictive analytics. With cutting-edge technology expertise, world-class service quality and a global resource base, CitiusTech consistently delivers best-in-class solutions and an unmatched cost advantage to healthcare clients