WannaCry Ransomware and SMB Vulnerability - Update

This is an update on the SMB (Server Message Block) vulnerability and WannaCry ransomware outbreak. Article CC-1411 on the Information Sharing Portal contains all the latest information:

https://nww.carecertisp.digital.nhs.uk/pages/viewpage.action?pageId=4685842

Further details of NHS Digital guidance and publication can be found at:

https://digital.nhs.uk/article/1495/Latest-guidance-for-NHS-on-protecting-against-cyber-attack

Update your Anti-Virus – important

As is usual with malware, it is likely that variations will continue trying to take advantage of vulnerabilities. It is therefore imperative that organisations continue to take action to avoid infection.

It is absolutely vital that all organisations ensure their Anti-Virus software has been updated with the latest definitions as a matter of urgency – and that the latest updates are regularly rolled out across the estate.

National Services Information

None of the national services provided by NHS Digital to England's health and care system have been impacted on by Friday's cyber-attack.

All systems and services we run have continued to operate as expected whilst our Data Security Centre has continued to work round the clock to support NHS organisations which were affected.

Guidance on NHSmail and 'reconnecting to the national network' for organisations which disconnected as a preventative measure has been made available:

https://digital.nhs.uk/media/1487/Technical-guidance-on-reconnecting-to-networks-following-precautionary-disconnection/pdf/Reconnecting_to_networks_guidance_150517

https://digital.nhs.uk/media/1486/NHSmail-confirmation-it-is-safe-to-connect/pdf/NHSmail_150517

Any issues at local NHS organisations regarding connectivity to NHS Digital's services; PDS, MESH, EPS and e-RS should be logged as an incident through their usual local support channel.

If you're an IT manager and you believe your organisation has been affected by Friday's cyber-attack and require support or further information, please contact NHS Digital on carecert@nhsdigital.nhs.uk or by calling 0800 085 6653.

Latest Developments

The malware may spread via the Internet or other networks: such as N3 (Transition Network), HSCN or the PSN networks if NetBIOS ports are allowed through your organisation's perimeter firewalls.

CareCERT has already advised NHS organisations to block NetBIOS related ports at their perimeter firewalls including NetBIOS UDP ports 137 and 138, NetBIOS TCP port 139 and SMB port TCP 445 - Organisations are additionally recommended to block port TCP 137 which is also associated with NetBIOS but uncommonly used.

The malware uses two hardcoded IP addresses: (192.168.56.20, 172.16.99.5) which may be used to identify and quarantine infected hosts and to block the exploit via Network IPS (Intrusion Prevention Systems) with updated detection signatures.

The malware may attempt to connect to a kill switch domain following each system reboot and each system logon: when this connection attempt fails then the malware is executed.

Description:

The SMB vulnerabilities within security bulletin MS17-010 are critical vulnerabilities that are highly likely to be used by future malware variants to achieve worm-like local network propagation. The patching of all affected versions should be aggressively prioritised.

This attack was not specifically targeted at the NHS and is affecting many organisations around the world from a range of sectors.

The ransomware is called WannaCry, Wanna Decryptor, Wanna Cryptor, WanaCrypt0r or WCry version 2.0 and spread quickly around the world after it was first detected on 12th May.

The malware encrypts files and provides the user with a prompt which includes a ransom demand, a countdown timer and Bitcoin wallet to pay the ransom into. It uses strong encryption and targets specific often-used files such as documents, videos and pictures. At the time of publication there is no known decryption method.

The ransomware delivery campaign leverages exploits from the ShadowBrokers release which uses vulnerabilities in Microsoft SMB (Server Message Block) - this is a legacy protocol used to share files and printers across local networks. The SMB vulnerabilities are used to propagate through a network, spreading similar to a worm, compromising hosts on the same network, encrypting files stored on them then demanding a ransom payment in the form of Bitcoin.

The malware also uses the DoublePulsar (CC-1354) attack, a backdoor also released by the ShadowBrokers group to deliver the payload and provide remote code execution.

The ShadowBrokers release contained exploits which use a range of SMB vulnerabilities which have all been patched by Microsoft within security bulletin MS17-010 including:

- *EternalRomance* - SMBv1 exploit over TCP port 445 which targets Windows XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2 and gives SYSTEM privileges.
- *EternalBlue (CC-1353)* - SMBv2 exploitation tool which leads to remote code execution.
- *EternalSynergy* - SMBv3 remote code execution flaw for Windows 8 and Server 2012 SP0.

WannaCry uses the MS17-010 exploit to spread to other machines through NetBIOS. The malware targets the following specific MS17-010 vulnerabilities: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147 and CVE-2017-0148.

The malware may spread not only to other machines in same network, but via Internet or other networks: such as N3 (Transition Network), HSCN or the PSN networks if NetBIOS ports are allowed through your organisation's perimeter firewalls. It randomly generates internal and external IP addresses which the malware attempts to initiate communications with. When an open NetBIOS port is found, three NetBIOS session setup packets are sent along with SMB packets containing the exploit shell code and an encrypted payload.

During these communications the malware includes two hardcoded IP addresses (192.168.56.20, 172.16.99.5) - these IP addresses may be used by network monitoring tools to identify infected hosts which can then be quarantined. Intrusion Prevention Systems (IPS) can use this information block the exploit with updated detection signatures.

Kill switch domain:

The outbreak of WannaCry 2.0 was dramatically slowed by the registration of these domains, however new versions of this ransomware may have been released without this dependency.

Once a system is infected, the malware first checks whether a specific internet domain is present, www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com or www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.] com:

- If the domain is found then the malware stops running.
- If the domain is not found then the malware executes.

The malware may attempt to connect to a kill switch domain following each system reboot and each system logon.

Organisations need to ensure connections to the kill switch domains are consistently achieved. Organisations which have disconnected themselves from the internet may inadvertently allowed the malware to spread within their organisation.

Further analysis has identified that the malware is not proxy aware, which poses a significant threat to environments that likely route outbound traffic through a proxy. When attempting to connect to the kill switch domains, if a well configured proxy is used, the malware may be unable to connect

and will therefore execute and continue to propagate.

See the Kill switch domain remediation for further information.

Remediation

SMB Vulnerability Remediation:

Note: Remediating the vulnerability does not remove an existing infection - any infected system requires quarantining, rebuilding to patched standard and redeploying.

- Monitor connections attempts to the two hardcoded IP addresses within the malware: 192.168.56.20 & 172.16.99.5
- Update IDS signatures to identify and block connections to the two hardcoded IP Addresses: 192.168.56.20 & 172.16.99.5
- If your network becomes infected immediately report it to your AV provider for investigation and patching
- Block SMB related ports (UDP 137, 138 and TCP 137, 139, 445) at your organisation's external firewall https://support.microsoft.com/en-us/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic-from-leaving-the-corporate-environment
- Ensure your AV software is updated with the very latest security patches, vendors are increasingly becoming able to detect and remediate this malware.
- Ensure all affected platforms are updated in line with the Microsoft security bulletin **MS17-010** Microsoft has additionally advised to prioritise the updating of all security patches released within the last 60 days - internet and N3 facing systems should be prioritised. Because of the high severity of this vulnerability Microsoft has taken the highly unusual step of releasing a patch for out of support operating systems including Windows XP, Windows 8, and Windows Server 2003. (Please be aware though that your AV provider is unlikely to release AV definitions to protect out of support operating systems.)
- Use a vulnerability scanner (such as Nessus, OpenVas or Microsoft Baseline Security Analyser) to identify any unpatched systems.
- If it is not possible to apply this patch then block SMB related ports (UDP 137, 138 and TCP 139, 445) across your organisation's network or disable SMB
- If your organisation has SMB port 445 exposed on any system then review if this is operationally necessary (including the use of NetBIOS ports UDP 137 & 138 and NetBIOS over TCP/IP TCP Ports 137 & 139) as SMB and NetBIOS are both legacy protocols that may no longer be required within your environment.

Securing RDP

If RDP is not used then ensure:

- Port 3389 is blocked at your internet firewall

If RDP is used:

- Ensure only authorised users are granted RDP permissions.
- Authorised users have a strong password.
- RDP connections are protected with multifactor authentication.
- For additional security only allow RDP to run through VPN connections.

Kill switch domain Remediation

Ensure that the two kill switch domains are not blocked by firewalls because they stop some variants of the malware from running:

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

Organisations who have disconnected from the internet or who maintain a proxy server are recommended to implement a local webserver which resolves via local DNS servers (or via configuration of local host files) to the kill switch domains. This will prevent WannaCry 2.0 from spreading within your organisation regardless of any connectivity issues.

Ransomware Remediation

For full ransomware remediation please see the Best Practice Guide **Ransomware - Controls to avoid infection**.

It is not recommended to pay any ransom; there is no guarantee that paying a ransom will unlock the encrypted files or that the integrity of the files will be maintained. It could additionally increase the likelihood of your organisation being targeted in future campaigns.

Examine network connections for attempts to access the kill switch domains - this is a sign of an infection which is effectively dormant and still needs to be removed.

Responding to an Outbreak

1) Containment and Eradication

Because this threat uses an SMB vulnerability to propagate like a worm across a local network, the following containment activities should be performed. These actions can be broken down into a

number of work streams which can be performed across different teams:

Stream 1 - Identify and quarantine all systems infected with the malware.

- Monitor connections attempts to the two hardcoded IP addresses within the malware: 192.168.56.20 & 172.16.99.5
- Update IDS signatures to identify and block connections to the two hardcoded IP Addresses: 192.168.56.20 & 172.16.99.5
- Immediately quarantine all newly identified infected systems.
- Identify basic file IOC's on quarantined machines - are files encrypted with .wncry and .uiwix or this a different extension?
- Ensure users report all infections to the IT helpdesk. Infected devices should be immediately disconnected from the network and investigated by an IT analyst.
- Clearly label all quarantined devices and do not reconnect them to the network until they have been reimaged, patched and updated with the latest AV definitions.
- Identify all shared network storage the logged in user of the infected machine has access to and search these file shares for IOC (Indicator of Compromise) files:
    - File extension: .wncry and .uiwix
    - Ransom note name: @Please_Read_Me@.txt
- If IOC files are found on shared network storage:
    - If file auditing is enabled: identify users that wrote IOC files to the share. More info
    - If file auditing is not enabled: attempt to manually identify users that wrote IOC files to the share. More info
- Set up a file screening rule and alert on shared network storage to identify system administrators whenever an IOC file is written to a network share.
    - File extension: .wncry and .uiwix
    - Ransom note name: @Please_Read_Me@.txt
    - By using Windows File Server Resource Manager FSRM (or the equivalent for your file storage servers or SAN's operating system) you can identify IOC files as they're written and capture the name of the logged in user and computer the IOC file was written by. Immediately quarantine all newly identified infected computers
- Examine network connections for attempts to access the kill switch domains **www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com** and **www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.] com** - this is a sign of an infection on your network.

Stream 2 – Patch the vulnerability that enables malware to propagate throughout a network.

- Ensure all affected platforms are updated in line with the Microsoft security bulletin MS17-010:
- https://technet.microsoft.com/en-us/library/security/ms17-010.aspx (internet facing systems should be prioritised).
- Because the vulnerability MS17-010 allows the malware to propagate like a worm, patching this vulnerability needs to be aggressively prioritised.
- Use a vulnerability scanner (such as Nessus, OpenVas or Microsoft Baseline Security Analyser) to identify any unpatched systems.
- If it is not possible to apply this patch then block SMB related ports (UDP 137, 138 and TCP 137,139, 445) across your organisation's network or disable SMB - Advice on disabling SMBv1 can be found at MS17-010

Stream 3 – Ensure all systems are updated with the latest AV (Anti-Virus) definitions

- Update your AV software with the latest security definitions.
- Confirm with your AV provider that they have rolled out virus definition to protect you from the spread of this malware, which are supported by your organisation's operating systems.

Stream 4 - Implement additional technical controls to prevent the malware from propagating

- Block SMB related ports (UDP 137, 138 and TCP 139, 445) at your organisation's external firewall https://support.microsoft.com/en-us/help/3185535/guidelines-for-blocking-specific-firewall-ports-to-prevent-smb-traffic-from-leaving-the-corporate-environment.
- Ensure connectivity is maintained to the kill switch domain.
- Organisations that have disconnected from the internet or maintain a proxy solution are advised to implement a local webserver which resolves via local DNS servers (or via configuration of local host files) to the kill switch domain. Some variants of the malware will stop spreading further if this domain appears to exist.

Further information see the Best Practice Guide: Ransomware - Controls to avoid infection

2) Recovery

Remediating the vulnerability does not remove an existing infection - any infected system requires quarantining, reimaging/rebuilding to patched standard, protecting with the latest AV definitions and re-deploying.

Indicators of Compromise:

File extension: .wncry

Ransom note name: @Please_Read_Me@.txt

Possible malicious and associated files:

- WanaDecryptor.exe
- WanaDecryptor.exe.lnk
- !WannaDecryptor!.exe
- !WannaDecryptor!.exe.lnk
- !WannaCryptor!.bmp
- Please_Read_Me@.txt
- !Please Read Me!.txt
- Please Read Me!.txt
- C:\WINDOWS\tasksche.exe
- C:\WINDOWS\MSSECSVC.exe
- C:\WINDOWS\qeriuwjhrf
- C:\WINDOWS\system32\taskdl.exe
- 131181494299235.bat
- 176641494574290.bat
- 217201494590800.bat
- [0-9]{15}.bat #regex
- 00000000.pky
- 00000000.eky
- 00000000.res
- \TaskData\Data
- \TaskData\Tor
- \TaskData\Data\Tor
- \TaskData\Tor\libeay32.dll
- \TaskData\Tor\libevent-2-0-5.dll

- \TaskData\Tor\libevent_core-2-0-5.dll
- \TaskData\Tor\libevent_extra-2-0-5.dll
- \TaskData\Tor\libgcc_s_sjlj-1.dll
- \TaskData\Tor\libssp-0.dll
- \TaskData\Tor\ssleay32.dll
- \TaskData\Tor\taskhsvc.exe
- \TaskData\Tor\tor.exe
- \TaskData\Tor\zlib1.dll

Kill switch domains

- **iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com**
- **ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.] com**

Note: These kill-switch domains **MUST NOT BE BLOCKED** by firewalls because they stop some variants of the malware from running.

Tor client download location: https[:]//dist[.]torproject[.]org/torbrowser/6.5.1/tor-win32-0.2.9.10.zip

Malicious domains:

- rphjmrpwmfv6v2e[.]onion
- gx7ekbenv2riucmf[.]onion
- 57g7spgrzlojinas[.]onion
- xxlvbrloxvriy2c5[.]onion
- 76jdd2ir2embyv47[.]onion
- cwwnhwhlz52maqm7[.]onion

IP Addresses:

- 2.3.69.209
- 38.229.72.16
- 46.101.166.19
- 47.91.107.213

- 50.7.151.47
- 50.7.161.218
- 51.15.36.164
- 51.255.41.65
- 62.138.7.231
- 62.138.10.60
- 79.172.193.32
- 81.19.88.103
- 81.30.158.223
- 82.165.142.107
- 82.94.251.227
- 83.162.202.182
- 83.169.6.12
- 86.59.21.38
- 89.40.71.149
- 89.45.235.21
- 91.121.65.179
- 94.23.173.93
- 104.131.84.119
- 128.31.0.39
- 128.31.0.39
- 136.243.176.148
- 146.0.32.144
- 149.202.160.69
- 158.69.92.127
- 163.172.25.118
- 163.172.35.247

- 163.172.149.155
- 163.172.153.12
- 163.172.185.132
- 167.114.35.28
- 171.25.193.9
- 176.9.39.218
- 176.9.80.202
- 178.62.173.203
- 178.208.83.16
- 178.254.44.135
- 185.97.32.18
- 188.138.33.220
- 188.166.23.127
- 192.42.113.102
- 192.42.115.102
- 193.11.114.43
- 193.23.244.244
- 197.231.221.221
- 198.199.64.217
- 199.254.238.52
- 212.47.232.237
- 213.239.216.222
- 213.61.66.116
- 217.69.133.148
- 217.79.179.177
- 217.172.190.251

SHA-256 Hashes:

- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa
- c365ddaa345cfcaff3d629505572a484cff5221933d68e4a52130b8bb7badaf9
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- 0a73291ab5607aef7db23863cf8e72f55bcb3c273bb47f00edf011515aeb5894
- 428f22a9afd2797ede7c0583d34a052c32693cbb55f567a60298587b6e675c6f
- 5c1f4f69c45cff9725d9969f9ffcf79d07bd0f624e06cfa5bcbacd2211046ed6
- 62d828ee000e44f670ba322644c2351fe31af5b88a98f2b2ce27e423dcf1d1b1
- 72af12d8139a80f317e851a60027fdf208871ed334c12637f49d819ab4b033dd
- 85ce324b8f78021ecfc9b811c748f19b82e61bb093ff64f2eab457f9ef19b186
- a1d9cd6f189beff28a0a49b10f8fe4510128471f004b3e4283ddc7f78594906b
- a93ee7ea13238bd038bcbec635f39619db566145498fe6e0ea60e6e76d614bd3
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- eb47cd6a937221411bb8daf35900a9897fb234160087089a064066a65f42bcd4
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
- 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
- 2c2d8bc91564050cf073745f1b117f4ffdd6470e87166abdfcd10ecdff040a2e
- 7a828afd2abf153d840938090d498072b7e507c7021e4cdd8c6baf727cafc545
- a897345b68191fd36f8cefb52e6a77acb2367432abb648b9ae0a9d708406de5b
- fb0b6044347e972e21b6c376e37e1115dab494a2c6b9fb28b92b1e45b45d0ebc
- 9588f2ef06b7e1c8509f32d8eddfa18041a9cc15b1c90d6da484a39f8dcdf967
- b43b234012b8233b3df6adb7c0a3b2b13cc2354dd6de27e092873bf58af2693c
- 4186675cb6706f9d51167fb0f14cd3f8fcfb0065093f62b10a15f7d9a6c8d982
- 09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa
- dff26a9a44baa3ce109b8df41ae0a301d9e4a28ad7bd7721bbb7ccd137bfd696
- 201f42080e1c989774d05d5b127a8cd4b4781f1956b78df7c01112436c89b2c9
- b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
- aae9536875784fe6e55357900519f97fee0a56d6780860779a36f06765243d56

- 21ed253b796f63b9e95b4e426a82303dfac5bf8062bfe669995bde2208b360fd
- 2372862afaa8e8720bc46f93cb27a9b12646a7cbc952cc732b8f5df7aebb2450
- f8812f1deb8001f3b7672b6fc85640ecb123bc2304b563728e6235ccbe782d85
- 4a468603fdcb7a2eb5770705898cf9ef37aade532a7964642ecd705a74794b79
- 4b76e54de0243274f97430b26624c44694fbde3289ed81a160e0754ab9f56f32
- 9cc32c94ce7dc6e48f86704625b6cdc0fda0d2cd7ad769e4d0bb1776903e5a13
- 78e3f87f31688355c0f398317b2d87d803bd87ee3656c5a7c80f0561ec8606df
- be22645c61949ad6a077373a7d6cd85e3fae44315632f161adc4c99d5a8e6844
- 5d26835be2cf4f08f2beeff301c06d05035d0a9ec3afacc71dff22813595c0b9
- 76a3666ce9119295104bb69ee7af3f2845d23f40ba48ace7987f79b06312bbdf
- fc626fe1e0f4d77b34851a8c60cdd11172472da3b9325bfe288ac8342f6c710a
- eeb9cd6a1c4b3949b2ff3134a77d6736b35977f951b9c7c911483b5caeb1c1fb
- 043e0d0d8b8cda56851f5b853f244f677bd1fd50f869075ef7ba1110771f70c2
- 57c12d8573d2f3883a8a0ba14e3eec02ac1c61dee6b675b6c0d16e221c3777f4
- ca29de1dc8817868c93e54b09f557fe14e40083c0955294df5bd91f52ba469c8
- f7c7b5e4b051ea5bd0017803f40af13bed224c4b0fd60b890b6784df5bd63494
- 3e6de9e2baacf930949647c399818e7a2caea2626df6a468407854aaa515eed9
- 9b60c622546dc45cca64df935b71c26dcf4886d6fa811944dbc4e23db9335640
- 5ad4efd90dcde01d26cc6f32f7ce3ce0b4d4951d4b94a19aa097341aff2acaec
- 12d67c587e114d8dde56324741a8f04fb50cc3160653769b8015bc5aec64d20b
- 3f3a9dde96ec4107f67b0559b4e95f5f1bca1ec6cb204bfe5fea0230845e8301

Further analysis is being performed and CareCERT will keep updating this article as new IOCs and more information becomes available.

For further information about CareCERT services, including previous advisories and guidance in cyber security matters, please visit the Information Sharing Portal https://nww.carecertisp.digital.nhs.uk/