Australian Government
Australian Digital Health Agency

Digital Health Cyber Security Centre - Security Alert

Victorian healthcare providers infected with ransomware

1 October 2019

Document identifier: SEC-011019-01

Threat Level: Guarded

Summary

The Victorian government reported a ransomware incident affecting several health service providers and hospitals from South West Alliance of Rural Health. Media report that the malware blocked access to several systems, including financial management systems. [1]

The My Health Record System is secure and there is no indication of any impact to the security and privacy of patient information on the My Health Record (MyHR) system. The Agency is undertaking increased monitoring of the MyHR system to ensure there is no impact on the MyHR system or any other connected systems.

Technical Details

While investigations are continuing, the initial access vector is likely to be via Remote Desktop Protocol (RDP) services used for remote access management or spam email. Ransomware can also be distributed by Emotet malware, which acts as a downloader for other malware, such as Ryuk ransomware. [2] [3]

The most recent versions of Emotet use spam email that addresses recipients by name [4] and includes quotes from legitimate emails they sent or received in the past, making them appear less suspicious. [5] Media reports state, however, that no ransom demands have been made. [1] Emotet has previously compromised Australian healthcare organisations.

Potential impacts

The main impact of ransomware is the inability to use systems with encrypted data; the cost and time it takes to recover data from back ups; and the inability to deliver services that depend on affected systems. Attackers with access to personal health records may potentially access or attempt to exfiltrate data for ransom purposes.

Media reports indicate that it was too early to determine if patient records had been compromised yet. [1] [6]

TLP: WHITE

Recommended actions

1. Review and implement recommendations outlined in the Preventing and recovering from ransomware for senior managers [7] and IT professionals [8] and the UK [9] and US [10] government.
2. Advise users that malicious email may appear to come from senders known to them whose email accounts have been compromised and used to spread malware to your organisation.
3. Be aware of the risks posed by insecure RDP services that provide remote access to your network, including by ransomware. Ask your IT service provider if they use RDP services to access your network via the Internet.
    a. Restrict access to RDP services to authorised networks only. If RDP is not needed, configure firewall rules to block access to RDP ports from the Internet and other untrusted networks.
    b. Where RDP is required, ensure external access is made over secure VPN connections (firewall / gateway device) using two factor authentication, then establish an RDP link to the computing resource.
    c. Ensure RDP vulnerabilities are patched as a high priority. [11]

Indicators of compromise

Refer to the attached list of IOCs. Additional IOCs are included in the UK report. [9]

Further information

1. The Age. *Regional Victorian hospitals hit by cyber attack*. Available from: https://www.theage.com.au/national/victoria/regional-victorian-hospitals-hit-by-cyber-attack-20191001-p52whl.html.
2. Crowdstrike. *Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware*. 2019. Available from: https://www.crowdstrike.com/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/.
3. Cylance. *2019 Threat Report*. Available from: https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/Cylance-2019-Threat-Report.pdf.
4. Malwarebytes Labs. *Emotet is back: botnet springs back to life with new spam campaign*. 2019. Available from: https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/.
5. Ars Technica. *World's most destructive botnet returns with stolen passwords and email in tow*. 2019. Available from: https://arstechnica.com/information-technology/2019/09/worlds-most-destructive-botnet-returns-with-stolen-passwords-and-email-in-tow/.
6. ABC. *Victorian hospitals across Gippsland, Geelong and Warrnambool hit by ransomware attack*. Available from: https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988.
7. Australian Digital Health Agency. *Preventing and recovering from ransomware - a briefing for senior managers*. 2019. Available from:

https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/Ransomware%20-%20Senior%20Managers_300519.pdf.

8. Australian Digital Health Agency. *Preventing and recovering from ransomware - a briefing for IT professionals*. 2019. Available from: https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/Ransomware%20-%20Senior%20Managers_300519.pdf.
9. UK National Cyber Security Centre. *Ryuk ransomware targeting organisations globally*. 2019. Available from: https://www.ncsc.gov.uk/news/ryuk-advisory.
10. US-CERT. *Ransomware*. Available from: https://www.us-cert.gov/Ransomware.
11. Australian Digital Health Agency. *Patching: Protecting healthcare information by updating systems and software*. Available from: https://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/Patching-Senior-Managers-December2017.pdf.
12. *No More Ransom*. Available from: https://www.nomoreransom.org/en/ransomware-qa.html.

Contact us

If you have feedback, or information you wish to share about this matter, please contact the Digital Health Cyber Security Centre at cyber-incidents@digitalhealth.gov.au.

TLP: WHITE

Handling

TLP:WHITE This information is not confidential. It is suitable for public, unrestricted dissemination, publication, web-posting or broadcast. However, it is still subject to copyright and any restrictions or rights noted in the information.

Indicators of Compromise

Yara Rules

1. rule general_ryuk{ strings: $ryuk1 = ".RYK" wide $ryuk2 = "RyukReadMe.html" wide $unique = "UNIQUE_ID_DO_NOT_REMOVE" wide $proc1 = "csrss.exe" wide $proc2 = "explorer.exe" wide $proc3 = "lsaas.exe" wide $proc4 = "\\System32\\cmd.exe" wide $av1 = "SAVAdmin" wide $av2 = "McShield" wide $av3 = "SepMaster" wide $av4 = "KAVF" wide $av5 = "Antivirus" wide $av6 = "Sophos" wide $av7 = "EPSecurity" wide $av8 = "mfefire" wide $priv1 = "LookupPrivilegeValue error: %u" $priv2 = "AdjustTokenPrivileges error: %u" $func1 = "GetSystemDefaultLangID" condition: uint16(0) == 0x5A4D and #unique > 1 and all of ($ryuk*,$proc*,$av*,$priv*,$func*) }

2. rule unique_hardcoded_strings_ransomware { strings: $a = "/C REG ADD \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"svchos\" /t REG_SZ /d \"" wide ascii $b = "/reg:64" wide ascii $c = "No system is safe" wide

3. rule codedatastrings_2019 { strings: $ = "<htr<jtb<lt6<tt&<wt" ascii $ = "!\"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\\]^_`abcdefghijklmnopqrstuvwxyz{|}~" ascii $ = "ocautoupds" wide ascii $ = "firefoxconfig" wide ascii $ = "sqbcoreservice" wide ascii $ = "tbirdconfig" wide ascii $ = "klnagent" wide ascii $ = "\\Documents and Settings\\Default User\\finish" wide ascii $ = "UNIQUE_ID_DO_NOT_REMOVE" wide ascii $ = "taskkill" wide ascii condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 7 of them }

4. rule ransom_string_xor_deobfuscation_instructions { strings: $ = {99 F7 3D ?? ?? ?? ?? 8B C2 48 98 48 8D 0D ?? ?? ?? ?? 0F BE 04 01 8B ?? ?? ?? ?? ?? ?? 33 C8 8B C1} condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them }

5. rule packer_function { strings: $ = { 55 8b ec 8b 45 08 8d 04 c5 4d 01 00 00 5d c3 } condition: uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and any of them }

6. rule calculate_offset_jmp_edx { strings: $ = { 83 c4 04 ba ed 6e 46 00 81 ea 1d 4e 06 00 ff e2 8b e5 5d c3 } condition: uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and any of them }

7. rule infinite_loop { strings: $ = { ba 01 00 00 00 85 d2 74 02 eb f5 8b e5 5d c3 } condition: uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and any of them }

8. rule stall_execution_loop { strings: $ = { 8b 45 fc 83 c0 02 89 45 fc 81 7d fc 7b a1 c2 00 73 02 eb ec } condition: uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and any of them }

9. rule ryuk_artefacts { strings: $ = ".RYK" wide $ = "RyukReadMe.html" wide $ = "UNIQUE_ID_DO_NOT_REMOVE" wide $ = "\\users\\Public\\finish\\users\\Public\\sys" wide $ = "" wide $ = "\\Documents and Settings\\Default User\\finish" wide $ = "\\Documents and Settings\\Default User\\sys" wide condition: uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and 3 of them }

10. rule decryptor_strings{ strings: $a = "write full address of file, example \"C:\\mypath\\somepath\\somefile.xls\"" $b = "choose next file, 0 for exit" $c = "DECRYPT START FOR 30 SECONDS, TURN OFF ALL ANTIVIRUS SOFTWARE" $d = "NOTE: don't do anything, just wait, after decrypt has been finished u see the message" $e = "rename *.RYK *." $f = "System need to reboot, after reboot run decryptor" $g = "Ryuk decryptor software" condition: 4 of them }

11. rule taskkill_proc_list { strings: $ = "veeam" wide $ = "backup" wide $ = "Backup" wide $ = "xchange" wide $ = "sql" wide $ = "dbeng" wide $ = "sofos" wide $ = "calc" wide $ = "ekrn" wide $ = "zoolz" wide $ = "encsvc" wide $ = "excel" wide $ = "firefoxconfig" wide $ = "infopath" wide $ = "msaccess" wide $ = "mspub" wide $ = "mydesktop" wide $ = "ocautoupds" wide $ = "ocomm" wide $ = "ocssd" wide $ = "onenote" wide $ = "oracle" wide $ = "outlook" wide $ =

12. rule av_service_list { strings: $ = "veeam" wide $ = "Back" wide $ = "xchange" wide $ = "ackup" wide $ = "acronis" wide $ = "sql" wide $ = "Enterprise" wide $ = "Sophos" wide $ = "Veeam" wide $ = "AcrSch" wide $ = "Antivirus" wide $ = "Antivirus" wide $ = "bedbg" wide $ = "DCAgent" wide $ = "EPSecurity" wide $ = "EPUpdate" wide $ = "Eraser" wide $ = "EsgShKernel" wide $ = "FA_Scheduler" wide $ = "IISAdmin" wide $ = "IMAP4" wide $ = "MBAM" wide $ = "Endpoint" wide $ = "Afee" wide $ = "McShield" wide $ = "Task" wide $ = "mfemms" wide $ = "mfevtp" wide $ = "mms" wide $ = "MsDts" wide $ = "Exchange" wide $ = "ntrt" wide $ = "PDVF" wide $ = "POP3" wide $ = "Report" wide $ = "RESvc" wide $ = "sacsvr" wide $ = "SAVAdmin" wide $ = "SamS" wide $ = "SDRSVC" wide $ = "SepMaster" wide $ = "Monitor" wide $ = "Smcinst" wide $ = "SmcService" wide $ = "SMTP" wide $ = "SNAC" wide $ = "swi_" wide $ = "CCSF" wide $ = "TrueKey" wide $ = "tmlisten" wide $ = "UI0Detect" wide $ = "W3S" wide $ = "WRSVC" wide $ = "NetMsmq" wide $ = "ekrn" wide $ = "EhttpSrv" wide $ = "ESHASRV" wide $ = "AVP" wide $ = "klnagent" wide $ = "wbengine" wide $ = "KAVF" wide $ = "Mfefire" wide condition: uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and 10 of them }

13. rule afx_packer_function { strings: $start_obfus_code = { 3C EB AB AD 17 E5 B3 50 80 18 F1 2A 1C 30 CB 82 } $start_obfus_payload = "KQAAADFZc3EAAAAAs8ws/pW8/pa4/pa8AWm8/i68/pa8/pa8vpa8/pa8/pa8/pa8/pa8/pa8 /pa8/pa8/pa8/pa8/pa8/pa8/pe8/pijRJi8Sp9x3y69sludqv7VjbbM" ascii nocase $version_copyright = "Copyright (C) 20017" wide nocase $rich_header = {52 2F 43 34 16 4E 2D 67 16 4E 2D 67 16 4E 2D 67 40 51 3E 67 36 4E 2D 67 16 4E 2D 67 0D

4E 2D 67 74 51 3E 67 07 4E 2D 67 16 4E 2C 67 C3 4F 2D 67 95 52 23 67 0A 4E 2D 67 FE 51 27 67 98 4E 2D 67 FE 51 26 67 4E 4E 2D 67 AE 48 2B 67 17 4E 2D 67 52 69 63 68 16 4E 2D 67 } condition: uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and any of them }

Attacker IPs

Powershell Empire	198[.]12[.]71[.]157
Emotet	144[.]217[.]246[.]57
Emotet	54[.]39[.]180[.]109
Emotet	173[.]248[.]147[.]186
Trickbot	181[.]129[.]49[.]98:449
Trickbot	37[.]255[.]200[.]157:449
Trickbot	190[.]146[.]112[.]216
Trickbot	5[.]188[.]108 [.]14
Trickbot	94[.]250 [.]255 [.]16
Trickbot	181[.]112[.]145 [.]222
Trickbot	186[.]10[.]243 [.]70
Trickbot	5[.]160[.]77[.]180
Trickbot	217[.]106 [.]238 [.]132
Trickbot	31[.]47[.]55[.]106
Trickbot	85[.]133[.]183[.]174

Registry Keys

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

File names

RyukReadMe.txt, RyukReadMe.html, *.ryk

File paths

c:\Windows\System32\setup.exe
c:\Users\Default\AppData\Roaming\msnet\uetur.exe

c:\Users*\AppData\Roaming\msnet\uetur.exe

c:\Users*\AppData\Roaming\msnet

c:\Windows\System32\config\systemprofile\AppData\Roaming\msnet\uetut.exe

c:\Windows\System32\config\systemprofile\AppData\Roaming\msnet

c:\Windows\System32\Tasks\Ms net

C:\users\Public\sys

C:\Documents and Settings\Default User\sys