National Cyber Security Centre
a part of GCHQ

Advisory: Ryuk ransomware targeting organisations globally

Reference: NCSC-Ops/17-19

22 June 2019

Introduction

The NCSC is investigating current Ryuk ransomware campaigns targeting organisations globally, including in the UK. In some cases, Emotet and Trickbot infections have also been identified on networks targeted by Ryuk.

Details

Ryuk was first seen in August 2018 and has been responsible for multiple attacks globally. Ryuk is a targeted ransomware where demands are set according to the victim's perceived ability to pay.

The Ryuk ransomware is often not observed until a period of time after the initial infection – ranging from days to months – which allows the actor time to carry out reconnaissance inside an infected network, identifying and targeting critical network systems and therefore maximising the impact of the attack.[1] But it may also offer the potential to mitigate against a ransomware attack before it occurs, if the initial infection is detected and remedied.

Links to other malware

Ryuk ransomware has been linked to other malware families, in particular the Emotet and Trickbot banking trojans, although it could also be dropped by other malware.

Emotet is a modular banking trojan first detected in 2014, and while it has its own capability, has been increasingly used as a dropper for other trojans, facilitating the deployment of other threats.[2]

Trickbot, which has been targeting victims since late 2016, employs browser manipulation techniques to facilitate data theft with the aim of accessing the victims' various online accounts in order to enable further fraud and generate financial revenue for the operators.

According to industry reporting, when a Ryuk infection occurs, Emotet is commonly observed distributing Trickbot as part of the infection chain. Trickbot subsequently deploys additional post-exploitation tooling to enable their operations, including Mimikatz and PowerShell Empire modules. These facilitate credential harvesting, remotely monitoring of the victim's workstation, and performing lateral movement to other machines within a network.

This initial infection enables the attacker to assess whether the machine presents a ransomware opportunity, and if so, to deploy Ryuk.[3]

The relationship between these threats is modular in nature: Emotet drops other implants; Trickbot has been distributed by other methods. It is however possible that Ryuk could be deployed through an infection chain other than that detailed here.

---

[1] https://www.techradar.com/uk/news/ryuk-ransomware-targets-big-businesses
[2] https://www.us-cert.gov/ncas/alerts/TA18-201A
[3] https://blog.kryptoslogic.com/malware/2019/01/10/dprk-emotet.html, https://www.cybereason.com/blog/one-two-punch-emotet-trickbot-and-ryuk-steal-then-ransom-data

Access to compromised machines can be sold to other criminal operators at any stage in this process, either as a facilitated deployment, or through the sale of credentials for the compromised network (e.g. for RDP access).

Ryuk functionality

Ryuk is a persistent infection. The malware's installer will attempt to stop certain anti-malware software and install the appropriate version of Ryuk depending on a system's architecture.

The Ryuk ransomware itself does not contain the ability to move laterally within a network, hence the reliance on access via a primary infection, but it does however have the ability to enumerate network shares and encrypt those it can access. This, coupled with the ransomware's use of anti-forensic recovery techniques (such as manipulating the virtual shadow copy), is a technique to make recovering from backups difficult.

All non-executable files across the system will be encrypted and will be renamed with the .ryk file extension. A ransom note will be dropped in each processed folder with the name RyukReadMe (.html or .txt).

Indicators of compromise

Indicators of compromise (IOCs) for threats associated with Ryuk ransomware deployments can be found in the Appendix.

Mitigation

The NCSC publishes guidance that explains how to **defend your organisation from ransomware.** You should prioritise:

- keeping safe backups of important files
- defending your systems from malware and

remembering that paying the ransom may not get your data back.

See NCSC Guidance:
https://www.ncsc.gov.uk/guidance/protecting-your-organisation-ransomware
https://www.ncsc.gov.uk/guidance/mitigating-malware
https://www.ncsc.gov.uk/guidance/backing-your-data

The most effective mitigations for ransomware and other malware will include a defence-in-depth approach that makes it more difficult to successfully deploy malware, and reduce the impact and spread of a successful infection. We therefore recommend that longer-term, you should seek to:

- **Protect your devices and networks by keeping them up to date**: use the latest supported versions, apply security patches promptly, use anti-virus and scan regularly to guard against known malware threats. This should include your operating system and productivity apps. Users with Office 365 licensing can use 'click to run' to keep their office applications seamlessly updated. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware. If you cannot move off out-of-date platforms and applications straight away, there are short term steps you can take to improve your position. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/obsolete-platforms-security
- **Whitelist applications**. If supported by your operating environment, consider whitelisting of permitted applications. This will help prevent malicious applications from running. See NCSC Guidance: https://www.ncsc.gov.uk/collection/end-user-device-security/platform-specific-guidance/eud-security-guidance-windows-10-1809#whitelist
- **Use antivirus**. Keep any antivirus software up to date and consider use of a cloud-backed antivirus product. These provide better threat intelligence and more advanced analysis. Ensure that it is also capable of scanning MS Office macros if you have not disabled them. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/macro-security-microsoft-office
- **Use URI reputation services:** These are included with web browsers and antivirus to help detect malicious websites that distribute malware. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware
- **Implement architectural controls for network segregation and limit opportunity for lateral movement**. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-network-security https://www.ncsc.gov.uk/collection/cyber-security-design-principles https://www.ncsc.gov.uk/guidance/preventing-lateral-movement
- **Protect the management interfaces of your critical operational systems**. In particular, use browse-down architecture to prevent attackers easily gaining privileged access to your most vital assets. Remote management interfaces that use RDP should only be accessible from within a private network, using a VPN to access the network remotely. See NCSC blog post: https://www.ncsc.gov.uk/blog-post/protect-your-management-interfaces.

- **Set up a security monitoring capability** so you are collecting the data that will be needed to analyse network intrusions. See NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.
- **Review and refresh your incident management processes.** See NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-incident-management.
- **Use multi-factor authentication (/2-factor authentication/two-step authentication) to reduce the impact of password compromises**. See NCSC guidance: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa
- **Layer phishing defences.** Detect and quarantine as many malicious email attachments and spam as possible, before they reach your end users. Multiple layers of defence will greatly cut the chances of a compromise. Your approach should **treat people as your first line of defence**. Tell staff how to report suspected phishing emails, and ensure they feel confident to do so. Investigate their reports promptly and thoroughly. Never punish users for clicking phishing links or opening attachments. See NCSC Guidance: https://www.ncsc.gov.uk/phishing

Appendix

PowerShell Empire

Network traffic associated with PowerShell Empire beacons are observed as an HTTP request with the characteristics below. It is possible to use this to form log or IDS signatures for a platform. (Note that variations in the User Agent have been noted, but only in alterations to the white-space between the 'tokens').

```
GET <URI> HTTP/1.1
Cookie: session=<base64 string>
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0;
rv:11.0) like Gecko
Host: <IP address>
```

The URI may be one of:

- `/login/process.php`
- `/admin/get.php`
- `/news.php`

The IOCs below are associated with recent PowerShell Empire activity. While the presence of these does not confirm Ryuk has also been deployed, they may help identify lateral movement, and should be investigated further:

dcb432c5d056cc3bd3178cea44913b84	MD5 hash
c512e140f8f884af26ab59c0b184dcef	MD5 hash
ca3f48cc8221830ed6b433fc7d776f9a	MD5 hash

TrickBot

The following IOCs are associated with recent Trickbot activity. While the presence of these does not confirm Ryuk has also been deployed, they may help identify precursor infections and lateral movement, and should be investigated further:

0146EAC3AEDCA01C0095A50BCE1B316D	MD5 hash
0146eac3aedca01c0095a50bce1b316d	MD5 hash
200[.]107[.]59[.]130:449	Attacker IP
5[.]196[.]154[.]93	Attacker IP
94[.]103[.]94[.]154	Attacker IP
186[.]42[.]186[.]202:449	Attacker IP
177[.]52[.]79[.]29:449	Attacker IP
187[.]8[.]169[.]10:449	Attacker IP
187[.]65[.]49[.]88:449	Attacker IP
200[.]83[.]49[.]141:449	Attacker IP
200[.]35[.]56[.]81:449	Attacker IP
177[.]183[.]194[.]194:449	Attacker IP
200[.]110[.]72[.]134:449	Attacker IP
186[.]248[.]163[.]198:449	Attacker IP
191[.]241[.]233[.]195:449	Attacker IP
187[.]95[.]32[.]18:449	Attacker IP
187[.]95[.]123[.]179:449	Attacker IP

177[.]52[.]28[.]238:449	Attacker IP

The file paths below may indicate the presence of malware related to this activity on a system:

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

Yara rules for Ryuk

The following Yara rules are associated with recent Ryuk activity. Any results should be further checked to identify false positives:

```
rule ryuk_custom_packer
{
  meta:
    description = "Rule for detecting the packed Ryuk binary"
    author = "NCSC"
    hash =
"b895399bdd8b07b14e1e613329b76911ebe37ab038e4b760f41e237f863b4964"

  strings:
    $ = { 55 8b ec 8b 45 08 8d 04 c5 4d 01 00 00 5d c3 }
    $ = { 83 c4 04 ba ed 6e 46 00 81 ea 1d 4e 06 00 ff e2 8b e5 5d c3 }
    $ = { ba 01 00 00 00 85 d2 74 02 eb f5 8b e5 5d c3 }
    $ = { 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 all of
them
}
```

```
rule ryuk_afx_packer
{
  meta:
    description = "Rule for detecting the packed Ryuk binary"
    author = "NCSC"
    hash                                                                    =
"fe55650d8b1b78d5cdb4ad94c0d7ba7052351630be9e8c273cc135ad3fa81a75"

  strings:
    $ = { 3C EB AB AD 17 E5 B3 50 80 18 F1 2A 1C 30 CB 82 }
    $                                                                       =
"KQAAADFZc3EAAAAAs8ws/pW8/pa4/pa8AWm8/i68/pa8/pa8vpa8/pa8/pa8/pa8/pa8/pa8
/pa8/pa8/pa8/pa8/pa8/pa8/pe8/pijRJi8Sp9x3y69sludqv7VjbbM" ascii
    $ = { 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 all of
them
}
```

```
rule ryuk_main_artefacts
{
  meta:
    description = "Rule for detecting the main Ryuk payload"
    author = "NCSC"

  strings:
    $ = ".RYK" wide
    $ = "RyukReadMe.html" wide
    $ = "UNIQUE_ID_DO_NOT_REMOVE" wide
    $ = "\\users\\Public\\finish" wide
    $ = "\\users\\Public\\sys" 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 all of
them
}
```

```
rule ryuk_decryptor_strings
{
  meta:
    description = "Rule for detecting the Ryuk decryptor binary"
    author = "NCSC"
    hash                                                                    =
"85e5aff9b169657ba912f4edc019e2d38dd3c3fb2be187309dd65d4ae8732529"

  strings:
    $     =     "write     full     address     of     file,     example
\"C:\\mypath\\somepath\\somefile.xls\"" ascii
    $ = "choose next file, 0 for exit" ascii
    $ = "DECRYPT START FOR 30 SECONDS, TURN OFF ALL ANTIVIRUS SOFTWARE"
ascii
    $ = "NOTE: don't do anything, just wait, after decrypt has been finished
u see the message" ascii
    $ = "rename *.RYK *." ascii
    $ = "System need to reboot, after reboot run decryptor" ascii
    $ = "Ryuk decryptor software" ascii

  condition:
    uint16(0) == 0x5a4d and uint32(uint32(0x3c)) == 0x00004550 and all of
them
}
```