Ryuk, Software S0446 | MITRE ATT&CK®

Archived: 2026-04-05 13:31:04 UTC

Enterprise T1134 Access Token Manipulation

Ryuk has attempted to adjust its token privileges to have the `SeDebugPrivilege`.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: 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.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Ryuk has used `cmd.exe` to create a Registry entry to establish persistence.[1]

Enterprise 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.[1][4]

Enterprise T1083 File and Directory Discovery

Ryuk has enumerated files and folders on all mounted drives.[1]

Enterprise 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.[5]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Ryuk has stopped services related to anti-virus.[2]

Enterprise T1490 Inhibit System Recovery

Ryuk has used `vssadmin Delete Shadows /all /quiet` to to delete volume shadow copies and `vssadmin resize shadowstorage` to force deletion of shadow copies created by third-party applications.[1]

Enterprise T1680 Local Storage Discovery

Ryuk has called `GetLogicalDrives` to emumerate all mounted drives, and `GetDriveTypeW` to determine the drive type.[1]

Enterprise T1036 Masquerading

Ryuk can create .dll files that actually contain a Rich Text File format document.[5]

.005 Match Legitimate Resource 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`.[1]

Enterprise 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]

Enterprise T1027 Obfuscated Files or Information

Ryuk can use anti-disassembly and code transformation obfuscation techniques.[4]

Enterprise T1057 Process Discovery

Ryuk has called `CreateToolhelp32Snapshot` to enumerate all running processes.[1]

Enterprise T1055 Process Injection

Ryuk has injected itself into remote processes to encrypt files using a combination of `VirtualAlloc`, `WriteProcessMemory`, and `CreateRemoteThread`.[1]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Ryuk has used the C$ network share for lateral movement.[6]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Ryuk can remotely create a scheduled task to execute itself on a system.[5]

Enterprise T1489 Service Stop

Ryuk has called `kill.bat` for stopping services, disabling services and killing processes.[1]

Enterprise 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.[1]

Enterprise 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.[1][6]

Enterprise T1205 Traffic Signaling

Ryuk has used Wake-on-Lan to power on turned off systems for lateral movement.[6]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

Ryuk can use stolen domain admin accounts to move laterally within a victim domain.[5]

ICS T0828 Loss of Productivity and Revenue

An enterprise resource planning (ERP) manufacturing server was lost to the Ryuk attack. The manufacturing process had to rely on paper and existing orders to keep the shop floor open. [7]
