MS-ISAC®
Multi-State Information Sharing & Analysis Center®

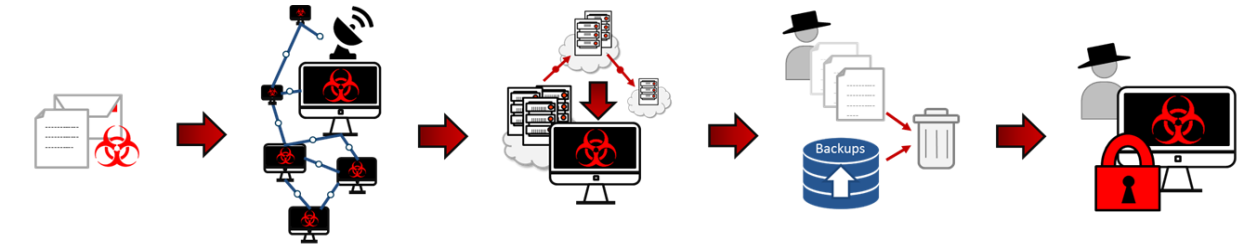
Security Primer
<December 20, 2019> • SP2020-1262

Ryuk

Overview

Ryuk is one of the most prevalent ransomware variants in the state, local, tribal, and territorial (SLTT) government threat landscape, with infections doubling from the second to the third quarter in 2019. Ransomware infections continue to increase in tandem with overall impact and monetary demands. Furthermore, Ryuk's ability to delete shadow copies and backups makes Ryuk extremely costly and almost impossible to remediate. For instance, Ryuk operators demanded nearly $600,000 from one SLTT government after successfully encrypting nearly all files on the network.

Ryuk uses encryption to block access to a system, device, or file until a ransom is paid. It is often dropped on a system by other malware (e.g., TrickBot) or delivered by cyber threat actors (CTAs) after gaining access to the system through compromising Remote Desktop Services. Once on a system, CTAs deploy Ryuk through the network using PowerShell, PsExec, or Group Policy, with aim to infect as many systems as possible. The number of infected systems depends upon how the malware is deployed as well as the CTA's access and privileges. This may be a local subnet, the list of computers in active directory, or the entire organization depending on the variability and process specific nature of spreading the malware. Once the malware is pushed out to the network, it targets backups and begins the encryption process.



The MS-ISAC observed an increase in Emotet or TrickBot infections leading to a Ryuk infection. For example, the MS-ISAC assisted in an incident where TrickBot disabled the organizations endpoint antivirus application and spread throughout the network, infecting hundreds of endpoints and multiple servers. Since TrickBot is a banking trojan, it likely harvested and exfiltrated financial and other sensitive information prior to deploying Ryuk. Once Ryuk is deployed network-wide the CTAs encrypted the organization's data and backups, and left ransom notes on the machines.

Ryuk ransom notes once contained a message and a ransom amount, but have since evolved over time. Throughout most of 2019 the ransom note did not list a ransom amount and only contained a message and email address (see Figure 1). However, now Ryuk ransom notes are very simplistic, with no price or message, only containing an email address, the ransomware's name, and the statement "balance of shadow universe" (See Figure 2). The CTAs demands payment via Bitcoin cryptocurrency and direct victims to deposit the ransom into specific Bitcoin wallets. The ransom demand is typically between $100,000-$600,000, which as of 12/19/19 is 14-84 Bitcoins. Notably the ransom demand is determined by the organizations' assessed ability to pay and the sensitivity of the data affected. It is highly likely the CTAs account for characteristics like industry, solvency, subscription to cyber insurance, and network saturation when calculating ransom demands. Furthermore, the CTAs have been known to negotiate with victims and adjust the initial ransom amount.

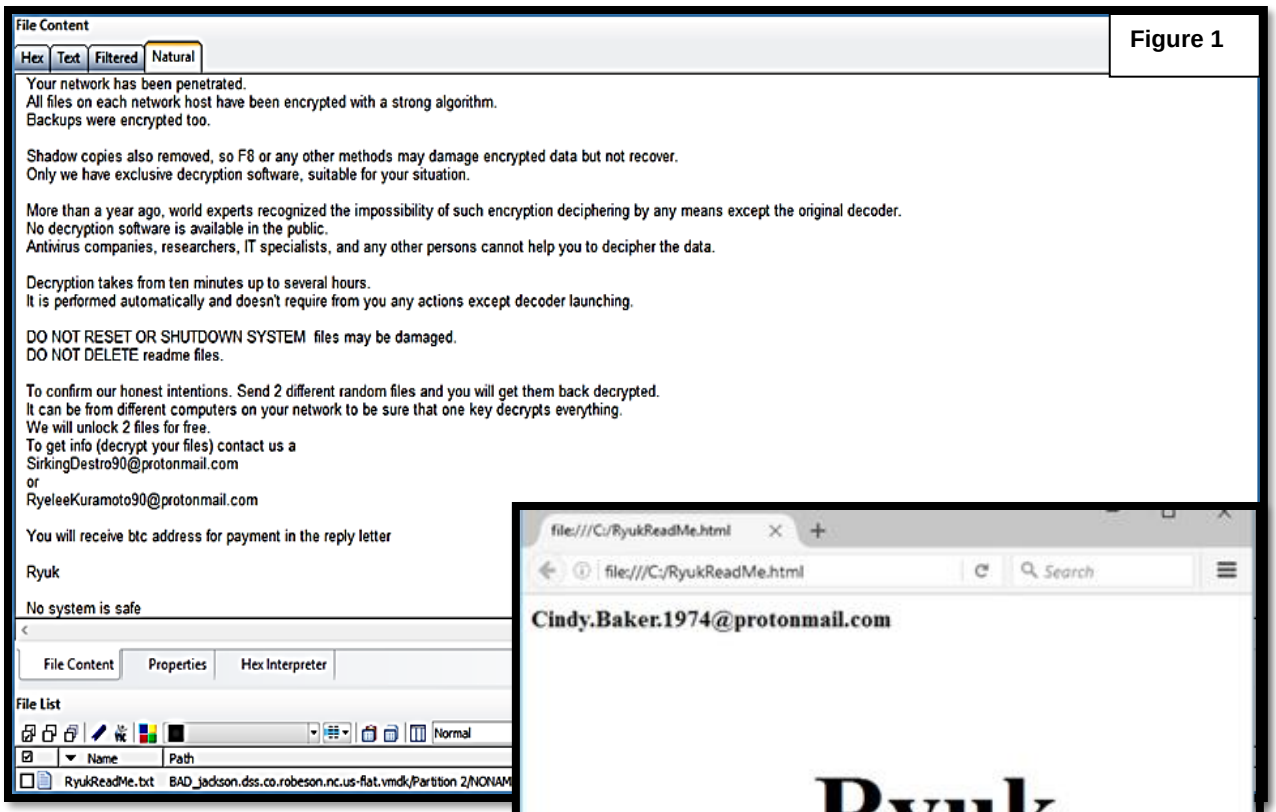


Figure 1

Figure 2

Main Module

Initial Infection: Dropped

Ryuk's main infection method is to be dropped on a system by other malware. It is difficult to recover and analyze the dropper because the main payload deletes the dropper after its initial execution. The dropper identifies a folder path to create a file for the payload. For older Windows systems, like Windows XP, the folder path would look like "*C:\Documents and Settings\Default\User*" whereas, for Vista or newer systems, the path would look like "*C:\Users\Public*". The file will have a five-letter random name that is usually generated by the *srand*[1] and *GetTickCount*[2] functions. If the file creation fails, the dropper will then try to write into its own directory. The dropper contains 32 and 64-bit modules of the ransomware. Once the file is created, the dropper then checks what system is currently running and writes the appropriate module (32 or 64-bit) to it.

Persistence

Once executed, the main payload attempts to stop antivirus related processes and services. It uses a preconfigured list to kill more than 40 specific processes and 180 services with *taskkill* and *net stop* commands. This preconfigured list includes antivirus processes, databases, backups, and document editing software. Additionally, the main payload establishes persistence in the registry and injects malicious payloads into several running processes.

To increase persistence, Ryuk makes changes to the registry allowing it to run the payload every time the user logs on. To achieve this, it creates a registry value under the Run Key using the windows command line *cmd.exe*. Ryuk then writes a Registry Run Key named *svchos* to "*HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*" with the executable as the key's target path. The naming of the Run Key is deliberate in order to look like the legitimate *svchost* process. Subsequently, Ryuk creates snapshots of all running processes via the *CreateToolhelp32Snapshot*(),duplicating this step to have two lists of running processes for comparison. The list of running processes are compared to *csrss.exe*, *explorer.exe*, and *lsass.exe*. The malware whitelists these processes to identify other running processes to inject the payload into, such as *taskhost.exe*.

Ryuk's anti-recovery techniques are more extensive and sophisticated than most types of ransomware, making recovery almost impossible without restoring from clean external offline backups. Ryuk's process injection allows the malware to gain access to the volume shadow service and delete all shadow copies, including those used by third-party applications. Ryuk starts by writing its content into a remote thread to execute its code via the *WriteProcessMemory*[3] and *CreateRemoteThread*[4] functions. Next, the malware runs a dropped *.bat* file, which contains multiple uses of *vssadmin.exe*[5]. Like other ransomware variants, Ryuk uses vssadmin.exe to delete shadow copies. However, it also uses an undocumented feature that allows it to resize the shadow copies storage, enabling it to delete third-party shadow copies. To delete the third-party shadow copies, the malware changes the size of the storage via the "*vssadmin resize shadowstorage*" command. The malware will then resize the default shadow volume size, setting

[1] Srand function sets the starting point for generating a series of pseudorandom integers in the current thread.
[2] GetTickCount function retrieves the number of elapsed milliseconds since the system was started, up to 49.7 days.
[3] WriteProcessMemory function writes data to an area of memory in a specified process.
[4] CreateRemoteThread function creates a thread that runs in the virtual address space of another process.
[5] Vssadmin Displays current volume shadow copy backups and all installed shadow copy writers and providers. Select a command name in the following table view its command syntax.

it to unbound, which grants storage use of all available disk space. Once completed, the malware will run the delete shadow command via "*delete shadows /all/quiet*" to remove the files based on extensions and folder locations for shadow copies, including those created by third-party applications. Furthermore, it will search for and delete multiple files that have backup-related extensions and any backups that are currently connected to the infected machine or network.

Encryption

Ryuk uses RSA and AES encryption algorithms with three keys. The CTAs use a private global RSA key as their *base* encryption model. The second RSA key is delivered to the system via the main payload and is encrypted with the CTA's private global RSA key. Once the malware is ready for encryption, the final key is created in their three-key encryption model. The third key is an AES key that is created for each of the victim's files via the *Win32API* function *CryptExportKey*[6]. The AES keys created for the third key are then exported via *CryptExportKey* and encrypted using the second RSA key. Additionally, it uses the second RSA key for the *HExpKey* parameter[7].

Ryuk scans the infected systems and encrypts almost every file, directory, drive, network share, and network resource. Ryuk attempts to encrypt all mounted network drives and hosts that have Address Resolution Protocol (ARP) entries. The malware also enumerates mounted drives using the *GetLogicalDrives* function and determines the drive's type via *GetDriveTypeW*. As long as the drives are not CD-ROM types, the files will be encrypted. Ryuk will also use the *GetIpNetTable* function to find ARP entries associated with IP addresses.

While Ryuk tries to encrypt almost everything, there are specific files and directories that are whitelisted and left unencrypted. For example, folders with the extensions .exe, .dll, and .hrmlog, as well as folders named AhnLab, Chrome, Microsoft, Mozilla, recycle.bin, and Windows will not be encrypted as these allow the victim to access the internet (e.g., to buy cryptocurrency for the ransom demand) or to keep the host stable. Finally, once the malware is finished with the encryption process, it will create the ransom note, "*RyukReadMe.txt*", placing it in every folder on the system.

Recommendations

SLTT governments should adhere to best practices, such as those described in the CIS Controls, which are part of CIS SecureSuite. The MS-ISAC recommends organizations adhere to the following recommendations to limit the potential compromise and impact of Ryuk ransomware.

Preparation

- Perform regular system backups. Ransomware is known to delete Volume Shadow Copies, so ensure that backups are created and stored off-site or out-of-band. Also, use a backup strategy that allows multiple iterations of the backups to be saved and stored, in case the backups include encrypted or infected files. Routinely test backups for data integrity and to ensure you can recover from them.
- Ensure that the organization's antimalware software updates its scanning engine and signature database on a regular basis.
- Keep all operating systems, applications, and essential software up to date to mitigate potential exploitation by attackers.

[6] CryptExportKey exports a cryptographic key or pair of keys from a cryptographic service provider in a secure manner.
[7] HExpKey, a CryptExportKey parameter, is a handle to a cryptographic key of a destination user.

- Perform network segmentation according to organizational functionality and apply access controls between trust zones.
- For any publicly-exposed services, such as Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), and File Transfer Protocol (FTP), assess the need for exposure to the Internet.
- Assess the need to have RDP (port 3389) and Server Message Block (SMB) (port 445) open on systems and, if required, consider limiting allowed connections to only specific, trusted hosts.
    - Enable heightened monitoring for SMB activity throughout the network. Make sure to disable SMBv1 on all systems and utilize SMBv2 or SMBv3 after appropriate testing. Also, implement more robust Windows Event logging, including centralized logging of all Windows hosts and an increase in the maximum file size for the Event Logs.
- Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.
- Provide end-user training to help users identify suspicious emails or links and ensure that users are aware of the potential dangers of opening unsolicited email attachments or links. Ensure that users are aware of any support policies and procedures in place for assistance.
- Implement filters at the email gateway to filter out emails with known malspam indicators, such as known malicious subject lines, and block suspicious IP addresses at the firewall.
    - If you do not have a policy regarding suspicious emails, consider creating one. Part of this policy should specify that all suspicious emails should be reported to the security and/or IT departments.
- Adhere to the principal of least privilege, ensuring that users have the minimum level of access required to accomplish their duties. Limit administrative credentials to designated administrators.
- Ensure all user accounts fall under (and are not exempt from) acceptable policies associated with password aging, password complexity, and account lockout.
- If remote access for the user account is required by a third-party vendor, consider developing a process that keeps the user account disabled until access is needed.
- Consider restricting PowerShell execution to signed scripts and trusted scripts used for administration.

Recovery

- Rebuild the compromised system from a fresh installation or known good backup. Due to other potential malicious files that may have yet to be identified, this is the best initial step in helping to mitigate further malicious activity on the system.
- Out of an abundance of caution, reset all local and domain account passwords, as other credentials may have been compromised.
- Review any vendor accounts and their associated passwords to ensure they have been changed from their default settings.

The *MS-ISAC* is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance is available at 866-787-4722, *SOC@cisecurity.org*. The MS-ISAC is interested in your comments - an anonymous feedback *survey* is available.