Analysis of Ragnar Locker Ransomware

By Acronis

Published: 2021-06-04 · Archived: 2026-04-05 21:29:28 UTC

Analysis of Ragnar Locker Ransomware

Summary

- First discovered in April 2020.
- Uses the increasingly popular “double extortion” tactic, in which the attacker first exfiltrates sensitive data, then triggers the encryption attack, threatening to leak the stolen data if the target refuses to pay the ransom.
- Has 10 known victims to date whose data have been published on the data leak site.
- Uses a specially-crafted virtual machine image for its payload execution in order to evade anti-malware detection.
- Uses the Salsa20 encryption algorithm (which to strong to decrypt using brute-force methods) for file encryption and RSA-2048 to encrypt file keys.
- Uses CVE-2017-0213 vulnerability to elevate privileges via COM objects

Delivery of Ragnar Locker

The threat actor begin the attack by compromising the company’s network via RDP service, using brute force to guess weak passwords or with stolen credentials bought on the Dark Web. Next, the attacker performs second-stage reconnaissance. To elevate privileges, the attacker exploits the CVE-2017-0213 vulnerability in the Windows COM Aggregate Marshaler to run arbitrary code with elevated privileges. Having achieved privilege escalation, the attacker sometimes deploys a VirtualBox virtual machine (VM) with a Windows XP image to evade detection: an early use of a virtual machine image in this manner to run the ransomware encryption attack. The technique has been adopted since by the Maze family of ransomware operators.

The specially-crafted VM image is loaded to the VirtualBox VM, mapping all local drives as read/writable into the virtual machine. This allows the ransomware process running inside the VM to encrypt all files. To the host files, the encryption appears to be a trusted VirtualBox process and thus will be ignored by many security products.

Next, the Ragnar Locker operator deletes any extant shadow copies, disables any detected antivirus countermeasures, and uses a PowerShell script to move from one company network asset to another one. Finally, before launching Ragnar Locker ransomware, the attacker steals sensitive files and uploads them to one or more servers to publish them if the victim refuses to pay the ransom.

Obfuscation

The ransomware code is protected with obfuscation techniques that include adding junk code as well as encryption. The sample code snippet below shows such junk arithmetic instructions, the results of which are not used:

After performing its most resource-intensive operations, Ragnar Locker allocates 7680 (1E00) bytes of free memory space in the current process via VirtualAllocEx().

It then fills the memory space with shellcode to run it.

The shellcode’s main goal is to allocate the ransomware executable in memory and call it.

The first call of VirtualAlloc() allocates 9218 bytes of memory to store the encrypted payload.

The second call of VirtualAlloc() allocates 48640 (BE00) bytes of memory to store the decrypted payload (PE file).

The hashes of the decrypted payload are as follows:

MD5: 6360B252B21FE015D667B093F6497E33

SHA256: 1DE475E958D7A49EBF4DC342F772781A97AE49C834D9D7235546737150C56A9C

After resolving the address of the .text section, the ransomware jumps to the original entry point (OEP) of the unpacked sample.

Locale check

Ragnar Locker checks the locale info to avoid CIS countries from being infected. It identifies the following languages for exclusion:

It uses GetLocaleInfoW() with LANG_SYSTEM_DEFAULT and LOCALE_SENGLISHLANGUAGENAME to retrieve the operating system default language of the victim's machine.

If the machine's default language matches one on the CIS list, the ransomware process is terminated with the "666" exit code.

Command-line arguments

Ragnar Locker can be run with '-list' or '-force' command-line options. The "-list" argument is passed with a file containing the list of files to be encrypted.

The '-force' argument is passed with a path pointing to where the encryption should start.

By default, the ransomware is run without any command-line options, thereby encrypting the whole system.

Ragnar Locker encryption

The payload PE file contains a section with the name ".keys" in which the crypto keys and obfuscated configuration strings are stored.

The ransomware uses hardcoded obfuscated strings, decrypted in runtime.

The first decrypted value is a unique sample ID.

Next, it references a list of services to be terminated by Ragnar Locker that include strings related to backup and antivirus solutions (such as 'sophos' and 'veeam'), as well as remote management software (RMM) tools like ConnectWise and Kaseya that are typically used by managed service providers (MSPs).

The blacklist of processes includes text, database, and email processors. As a result, after terminating the processes, valuable target files such as documents, documents, and emails are released and available for encryption.

The embedded master RSA-2048 public key uses the PEM format.

The hardcoded ransom note includes the name of the target organization.

Ragnar Locker generates two key data arrays of 40 bytes and 32 bytes for use by Salsa20 cipher.

A custom-named GenKey function uses CryptGenRandom(), then manually initializes a SHA-512 hash with corresponding constants and effects some permutation to encrypt using randomly-generated keys.

These keys are encrypted by the master RSA-2048 public key and added to the footer of a file.

To import a RSA-2048 key, the ransomware decodes it from Base64, then executes CryptDecodeObjectEx() to decode the structure of the RSA-2048 key.

After getting the value '1.2.840.113549.1.1.1' -- which stands for RSAES-PKCS1-v1_5 encryption scheme -- Ragnar Locker imports the public key by using CryptImportPublicKeyInfo().

With the keys for encryption in hand, the malware next deletes any extant shadow copies by running processes with the following commands:

Wmic.exe shadowcopy delete

Vssadmin delete shadows /all /quiet

Ragnar Locker then commences the encryption process in 64 simultaneous threads.

A whitelist includes the following folders, files and extensions to skip during encryption:

The file names:

The file extensions:

Ragnar Locker uses the Salsa20 encryption algorithm with a custom matrix, which is filled in with generated keys placed in rearranged order. The matrix used for Salsa20 is 64 bytes in size, where 8 bytes defines the stream position, so the ransomware removes 16 bytes from the second key to be matched with the matrix size, and leaves the stream position values with zero bytes.

Ragnar Locker randomizes file extensions per user by retrieving the computername value and passing it to the next piece of code.

As output from the code above, ransomware gets 8 bytes and creates the ‘ragnar_{computer_id}’ string to append it to the filename.

The encrypted file contains the encrypted Salsa20 key data (40+32 bytes) with the signature ‘_RAGNAR_’ added to the footer at the very end.

To complete the ransom note, Ragnar Locker adds a hardcoded company_id encoded with Base64.

The ransom note file is named RGNR_{computer_id}.txt:

****

HELLO EDP.com !

If you reading this message, then your network was PENETRATED and all of your files and data has been ENCRYPTED

by RAGNAR_LOCKER !

****

!!!!! WARNING !!!!!

DO NOT Modify, rename, copy or move any files or you can DAMAGE them and decryption will be impossible.

DO NOT use any third party or public decryption software, it also may damage files.

DO NOT Shutdown or reset your system

There is ONLY ONE possible way to get back your files - contact us and pay for our special decryption key !

For your GUARANTEE we will decrypt 2 of your files FOR FREE, as a proof of our capabilities

Don't waste your TIME, the link for contacting us will be deleted if there is no contact made in closest future and you will never restore your DATA.

HOWEVER if you will contact us within 2 day since get penetrated - you can get a very SPECIAL PRICE.

ATTENTION !

We had downloaded more than 10TB of data from your fileservers and if you don't contact us for payment, we will publish it or sell to interested parties.

Here is just a small part of your files that we have, for a proof (use Tor Browser for open the link) : http://p6o7m73ujalhgkiv.onion/?p=171

We gathered the most sensitive and confidential information about your transactions, billing, contracts, clients and partners. And be assure that if you wouldn't pay,

all files and documents would be publicated for everyones view and also we would notify all your clients and partners about this leakage with direct links.

So if you want to avoid such a harm for your reputation, better pay the amount that we asking for.

==========

! HERE IS THE SIMPLE MANUAL HOW TO GET CONTACT WITH US VIA LIVE CHAT !

!!!

a) Download and install TOR browser from this site : https://torproject.org

b) For contact us via LIVE CHAT open our website : http://mykgoj7uvqtgl367.onion/client/?6bECA2b2AFFfBC1Dff0aa0EaaAd468bec0903b5e4Ea58ecde3C264bC55c7389E

c) For visit our NEWS PORTAL with your data, open this website : http://p6o7m73ujalhgkiv.onion/?page_id=171

d) If Tor is restricted in your area, use VPN

When you open LIVE CHAT website follow rules :

Follow the instructions on the website.

At the top you will find CHAT tab.

Send your message there and wait for response (we are not online 24/7, So you have to wait for your turn).

****

---RAGNAR SECRET---

NmJFQ0EyYjJBRkZmQkMxRGZmMGFhMEVhYUFkNDY4YmVjMDkwM2I1ZTRFYTU4ZWNkZTNDMjY0YkM1NWM3Mzg5RQ==

---RAGNAR SECRET---

****

Ragnar Locker decryption service

It is not possible to decrypt files without having the master key or decrypter.

The ransom note provides the address of the leak site, live chat and Ragnar Secret. The Ragnar Secret described above as ‘company_id’ encoded with Base64.

The data leak site is created to publish sensitive data stolen from the corporate network before running Ragnar Locker, because the ransomware has no network communication.

The mirrors of the data leak site: http://p6o7m73ujalhgkiv.onion/?page_id=171

http://rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd.onion/ http://rgleak7op734elep.onion/

The Live chat no longer works once the negotiation phase between the Ragnar Locker operators and attacked organization has been finished.

http://mykgoj7uvqtgl367.onion/client/?6bECA2b2AFFfBC1Dff0aa0EaaAd468bec0903b5e4Ea58ecde3C264bC55c7389E

Detection of Ragnar Locker by Acronis Cyber Protect

Ragnar Locker ransomware is detected and blocked by Acronis Cyber Protection products in multiple layers, for example by signatures as well as by behavior detection.

Conclusion

Ragnar Locker employs advanced defense-evasion techniques to bypass antivirus protection. It uses a small Windows XP virtual machine image to launch its payload and encrypt the files on a user's drive connected as a network drive. It poses a significant risk to organizations even with anti-malware solutions installed.

IoCs

MD5(packed): 6d122b4bfab5e75f3ae903805cbbc641

SHA256(packed): 68eb2d2d7866775d6bf106a914281491d23769a9eda88fc078328150b8432bb3

MD5: 6360b252b21fe015d667b093f6497e33

SHA256: 1de475e958d7a49ebf4dc342f772781a97ae49c834d9d7235546737150c56a9c

ragnar_{computer_id}

.keys

RGNR_{computer_id}.txt

http://mykgoj7uvqtgl367.onion/client/?6bECA2b2AFFfBC1Dff0aa0EaaAd468bec0903b5e4Ea58ecde3C264bC55c7389E

http://p6o7m73ujalhgkiv.onion/?page_id=171

http://rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd.onion/ http://rgleak7op734elep.onion/
