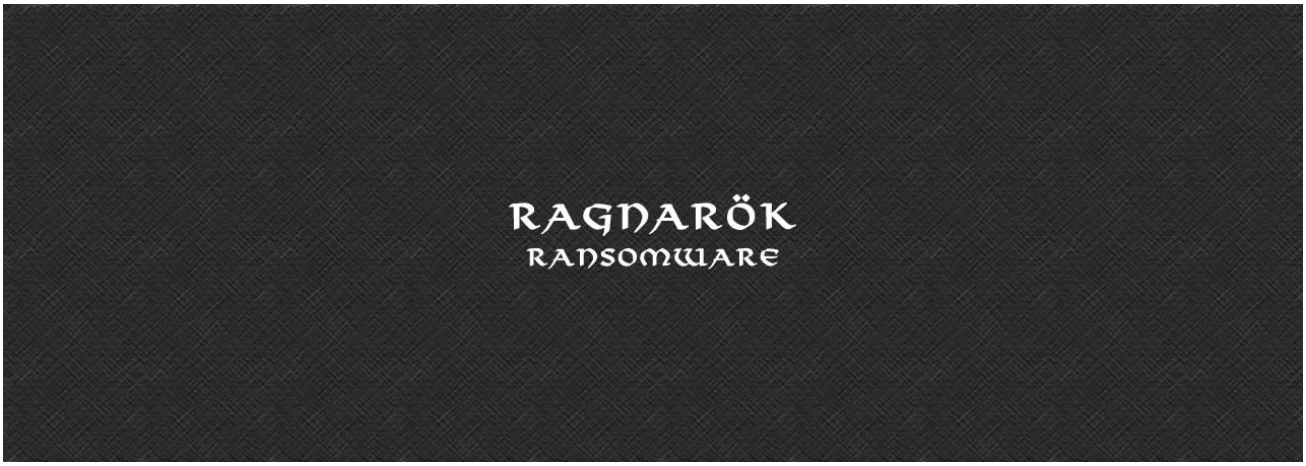
Ragnarok Ransomware Targets Citrix ADC, Disables Windows Defender

bleepingcomputer.com/news/security/ragnarok-ransomware-targets-citrix-adc-disables-windows-defender/

Lawrence Abrams

By
Lawrence Abrams

- January 28, 2020
- 03:30 AM
- 0



A new ransomware called Ragnarok has been detected being used in targeted attacks against unpatched Citrix ADC servers vulnerable to the CVE-2019-19781 exploit.

Last week, FireEye released a report about new attacks exploiting the now patched Citrix ADC vulnerability to install the new Ragnarok Ransomware on vulnerable networks.

When attackers can compromise a Citrix ADC device, various scripts would be downloaded and executed that scan for Windows computers vulnerable to the EternalBlue vulnerability.

If detected, the scripts would attempt to exploit the Windows devices, and if successful, inject a DLL that downloads and installs the Ragnarok ransomware onto the exploited device.

After Head of SentinelLabs Vitali Kremez extracted the ransomware's configuration file, we were able to discover some interesting behavior not commonly seen in other ransomware, which we detail below.

Excludes both Russia and China from encryption

Many ransomware operations are created by developers based out of Russia or other CIS countries.

To fly under the authority's radar, it is common for ransomware developers to exclude users in Russia and other former Soviet Union countries from being encrypted if they become infected.

Ragnarok operates similarly by checking the installed Windows language ID and if it matches one of the following will not perform an encryption of the computer.

```
0419 = Russia
0423 = Belarus
0444 = Russia
0442 = Turkmenistan
0422 = Ukraine
0426 = Latvia
043f = Kazakhstan
042c = Azerbaijan
```

Strangely, in addition to the CIS countries, Ragnarok will also avoid encrypting victims who have the 0804 language ID for China installed.

Ransomware excluding both Russia and China at the same time is rare and it is not known if this being done as a decoy for law enforcement or if the ransomware operates out of both countries.

Attempts to disable Windows Defender

As Microsoft's Windows Defender has become a solid and reliable antivirus and security program, we are finding that numerous malware programs are attempting to disable or bypass it to more easily conduct malicious operations.

For example, we have seen GootKit, TrickBot, and the Novter infections all utilizing some sort of Windows Defender bypass.

It is rare, though, to see ransomware infections themselves attempt to disable the functionality of Windows Defender, which is what Ragnarok attempts.

It does this by adding the following Windows group policies that disable various protection options in Windows Defender:

```
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender "DisableAntiSpyware" = 1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
"DisableRealtimeMonitoring" = 1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
"DisableBehaviorMonitoring" = 1
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection
"DisableOnAccessProtection" = 1
```

The good news is that if you have Windows 10's Tamper Protection feature enabled, these methods will not work and Windows will simply ignore any attempts to bypass Windows Defender.

In addition to Windows Defender, Ragnarok will also attempt to clear Shadow Volume Copies, disable Windows automatic startup repair, and turn off the Windows Firewall with the following commands:

```
cmd.exe /c vssadmin delete shadows /all /quiet
cmd.exe /c bcdedit /set {current} bootstatuspolicy ignoreallfailures
cmd.exe /c bcdedit /set {current} recoveryenabled no
cmd.exe /c netsh advfirewall set allprofiles state off
```

Strange Unix file references

Another strange aspect of this ransomware is the numerous references in the Windows executable to various Unix/Linux file paths such as:

```
    "no_name4": "/proc",
    "no_name5": "/proc/%s/status",
    "no_name8": "/tmp/crypt.txt",
    "no_name9": "/proc/%s",
    "rand_path": "/dev/random",
    "home_path": "/home/",
```

It is not clear as of yet why these paths are included and what they are used for, but Kremez believes it could be a possible in-development cross-platform targeting being used by the attackers.

"I believe "no_name5": "/proc/%s/status" specifically demonstrates that the actors are checking if the malware is running on the system via Unix command "/proc/[proccess_id]/status." Given that Citrix is exploited cross-platform and might be running on both Unix and Windows systems. This specific "no_name" setup allows the cross-platform targeting and checks for both Windows and Unix systems in mind. By and large, this targeting and any Unix payloads might be still in development; however, criminals behind Ragnarok appear to be as modular and adaptive as possible given this configuration setup to affect more systems," Kremez told BleepingComputer in a conversation.

A standard encryption routine

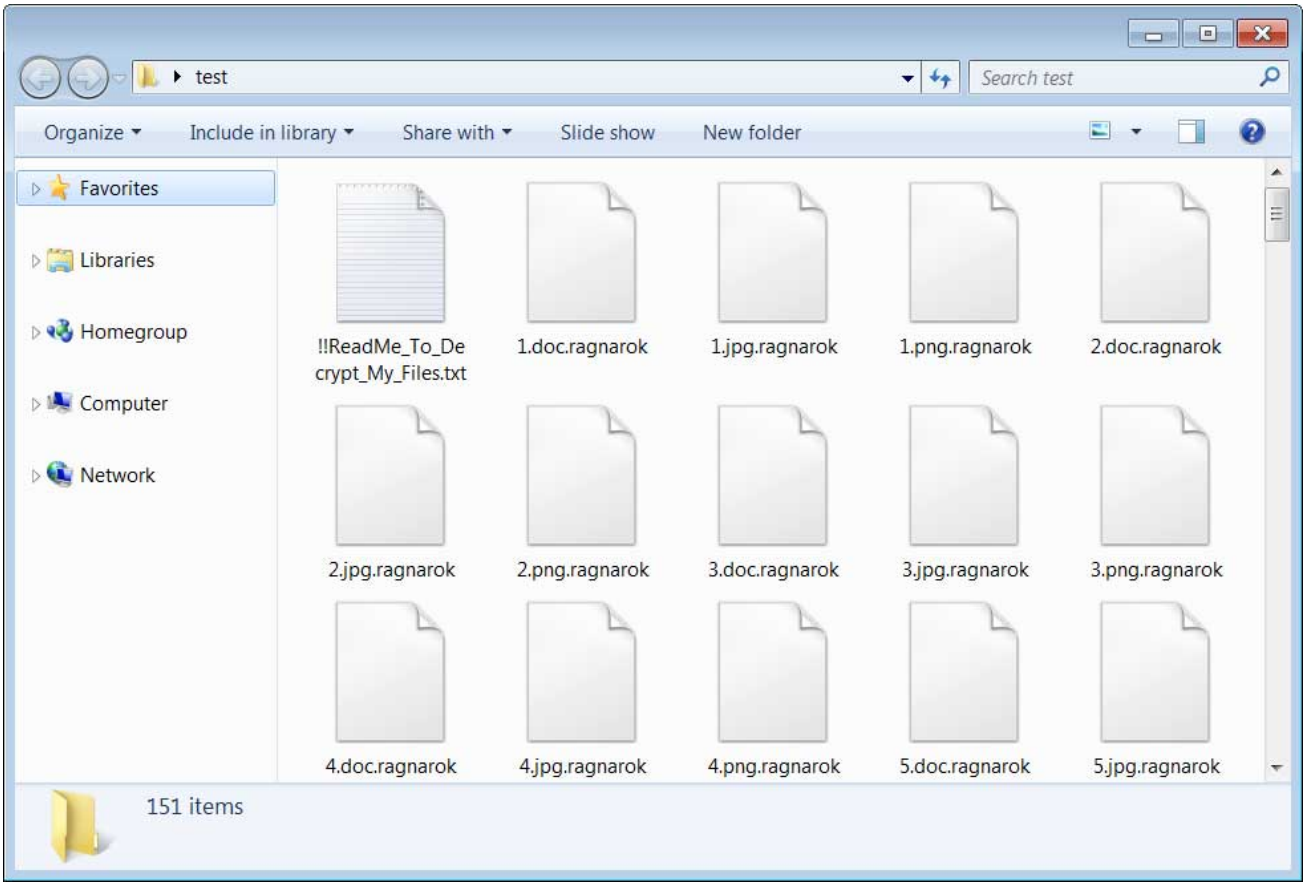
The rest of the Ragnarok encryption process is similar to what we see in other ransomware infections.

When encrypting files it will use AES encryption and the generated key will be encrypted with a bundled RSA encryption key. This makes it so only the ransomware developers can decrypt the victim's encryption key.

When scanning for files to encrypt, Ragnarok will skip any files that have the ".exe", ".dll", ".sys", and ".ragnarok" extensions. It will also skip any files whose path contains the following strings:

```
content.ie5
\temporary internet files
\local settings\temp
\appdata\local\temp
\program files
\windows
\programdata
$
```

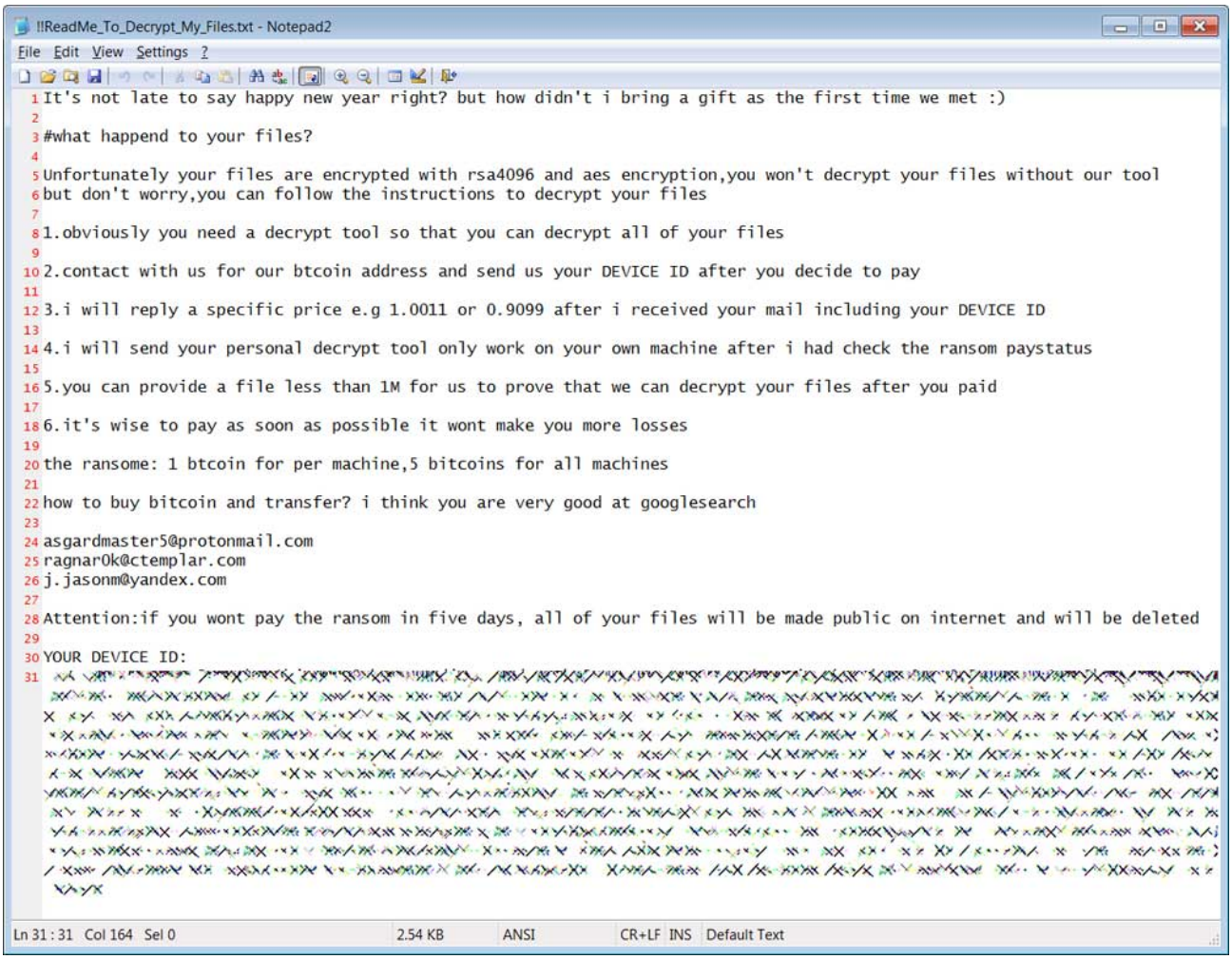
Each encrypted file will have the **.ragnarok** extension appended to the file name. For example, 1.doc would be encrypted and renamed to 1.doc.ragnarok.



Folder encrypted by Ragnarok

While encrypting the computer, it will create a ransom note in every traversed folder called **!!ReadMe_To_Decrypt_My_Files.txt**.

This ransom note contains instructions on what happened to a victim's files, their encrypted decryption key, and three email addresses to contact for payment instructions. It is not known how many bitcoins the attackers are demanding for a decryptor.



Ragnarok Ransom Note

At this time, it appears that the Ragnarok's encryption can't be broken, but will be further researched for any weaknesses.

Related Articles:

Magniber ransomware gang now exploits Internet Explorer flaws in attacks

Darknet market Versus shuts down after hacker leaks security flaw

The Week in Ransomware - May 20th 2022 - Another one bites the dust

Zyxel fixes firewall flaws that could lead to hacked networks

Critical F5 BIG-IP vulnerability exploited to wipe devices

IOCs

Hashes:

`b7319f3e21c3941fc2a960b67a150b02f1f3389825164140e75dfa023a73d34c`

Files:

```
!!ReadMe_To_Decrypt_My_Files.txt
C:\Users\public\Files\rgnk.dvi
```

Email addresses:

```
asgardmaster5@protonmail.com
ragnar0k@ctemplar.com
j.jasonm@yandex.com
```

Ransom note text:

```
It's not late to say happy new year right? but how didn't i bring a gift as the
first time we met :)

#what happend to your files?

Unfortunately your files are encrypted with rsa4096 and aes encryption,you won't
decrypt your files without our tool
but don't worry,you can follow the instructions to decrypt your files

1.obviously you need a decrypt tool so that you can decrypt all of your files

2.contact with us for our btcoin address and send us your DEVICE ID after you decide
to pay

3.i will reply a specific price e.g 1.0011 or 0.9099 after i received your mail
including your DEVICE ID

4.i will send your personal decrypt tool only work on your own machine after i had
check the ransom paystatus

5.you can provide a file less than 1M for us to prove that we can decrypt your files
after you paid

6.it's wise to pay as soon as possible it wont make you more losses

the ransome: 1 btcoin for per machine,5 bitcoins for all machines

how to buy bitcoin and transfer? i think you are very good at googlesearch

asgardmaster5@protonmail.com
ragnar0k@ctemplar.com
j.jasonm@yandex.com

Attention:if you wont pay the ransom in five days, all of your files will be made
public on internet and will be deleted

YOUR DEVICE ID:
xx
```

- Citrix ADC

- ETERNALBLUE
- Exploit
- Ragnarok
- Ransomware
- Vulnerability
- Windows Defender

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: