Bad Rabbit Ransomware

Rob Sobers Rob Sobers |

Clock for time it takes to read article 3 min read

|

Last updated May 6, 2022

Bad Rabbit Ransomware

What is Bad Rabbit ransomware?

Bad Rabbit is ransomware belonging to the Petya family of ransomware that hit over 200 organizations throughout Eastern Europe in October of 2017. Targets were primarily Russian media agencies however various corporate networks throughout Russia, Eastern Europe, and Japan were hit due to the method that ransomware used to spread through networks.

Bad Rabbit was spread through a drive-by attack where compromised websites spread a fake Adobe Flash update which, once run, would encrypt system files with RSA 2048 bit keys and demand .05 Bitcoin.

Who created Bad Rabbit?

The Bad Rabbit ransomware is not currently attributed to any threat group. However, the code and list of domains used for the drive-by attack share enough similarities with NotPetya (also referred to as ExPetr or Nyetya) to lead researchers to believe the same group is responsible for both. NotPetya has links to BlackEnergy and Sandworm Team yet those teams are Russian and Bad Rabbit is primarily targeting Russia which complicates attribution. Some researchers and commentators have proposed Bad Rabbit was a state-funded group targeting dissonant media organizations. However, other than the primary watering hole websites being media related there is no conclusive evidence to support that suggestion.

What systems are vulnerable to Bad Rabbit?

Only unpatched Windows 7 and later Windows operating systems are affected by Bad Rabbit. Initial reports indicated the ransomware did not use any NSA-developed exploits. However, follow-up research by Cisco's Talos Security Intelligence showed Bad Rabbit did in fact use the EternalRomance exploit CVE-2017-0145 to bypass Windows Server Message Block (SMB) file-sharing security and enable remote code execution on Windows systems. That is the same exploit leaked by the Shadow Brokers in April and used by NotPetya in June.

Bad Rabbit Timeline

1. March 2016 Petya First Spotted
2. April 2017 Shadow Brokers Leak EternalRomance
3. June 2017 NotPetya First Spotted
4. Oct 12th Ukraine’s SBU Warns of imminent attack similar to the NotPetya
5. Oct 24th 2017 BadRabbit First Spotted

How is Bad Rabbit spread?

The initial attack vectors for Bad Rabbit were compromised Russian media sites. The attackers uploaded fake Adobe Flash Player installers to these websites, which once downloaded and run manually by a user would initiate the Bad Rabbit ransomware.

The compromised websites hosted a redirect to 1dnscontrol[.]com for 6 hours. Once redirected a post request was sent to 185.149.120[.]3 providing the attackers with the user agent and other identifying information. From there the dropper was downloaded from two sources: 1dnscontrol[.]com/index.php and /flash_install.php.

Once a user runs the malicious Adobe Flash Player Executable, Bad Rabbit scans for SMB shares which it then brute forces with a hard-coded list of common credentials. Mimikatz post-exploitation tools are also used to harvest usernames and passwords and gain access to yet more SMB shares.

From there Bad Rabbit would attempt to exploit Windows Management Instrumentation Command-line (WMIC) in order to execute code on networked Windows systems.

Lastly, it uses an EternalRomance implementation, very similar to this publicly available python one, to read and write arbitrary data in the kernel memory space overwriting the session security. Then Bad Rabbit would use the access to run full disk encryption with DiskCryptor an open-source encryption application.

Indicators of Compromise

Bad Rabbit Ransomware Note

```
Oops! Your files have been encrypted. If you see this text, your files are no longer accessible. You might have been looking for a way to recover your files. Don't waste your time. Ho one will be able to recover them without our decryption service. We guarantee that you can recover all your files safely. All you need to do is submit the payment and get the decryption password. Visit our web service at caforssztxqzf2nm.onion Your personal installation key#1: If you have already got the password, please enter it below. Password#1:
```

Known Compromised Websites

The following sites were hacked and visitors to them were forced to download the Bad Rabbit installer.

- hxxp://www.fontanka[.]ru
- hxxp://www.otbrana[.]com
- hxxp://grupovo[.]bg
- hxxp://i24.com[.]ua
- hxxp://spbvoditel[.]ru
- hxxp://blog.fontanka[.]ru
- hxxp://www.pensionhotel[.]cz
- hxxp://www.sinematurk[.]com
- hxxp://most-dnepr[.]info
- hxxp://www.imer[.]ro
- hxxp://calendar.fontanka[.]ru
- hxxp://an-crimea[.]ru
- hxxp://www.online812[.]ru
- hxxp://www.aica.co[.]jp
- hxxp://www.mediaport[.]ua
- hxxp://ankerch-crimea[.]ru
- hxxp://novayagazeta.spb[.]ru
- hxxp://osvitaportal.com[.]ua
- hxxp://www.grupovo[.]bg
- hxxp://argumenti[.]ru
- hxxp://bg.pensionhotel[.]com
- hxxp://argumentiru[.]com
- hxxp://www.t.ks[.]ua

Command and Control Domains

- http://caforssztxqzf2nm[.]onion
- http://185.149.120[.]3/scholargoogle/
- hxxp://1dnscontrol[.]com/flash_install.php

Extensions Targeted for Encryption by Bad Rabbit

.3ds .7z

.accdb .ai .asm .asp .aspx .avhd .back .bak .bmp .brw .c .cab .cc .cer .cfg .conf .cpp .crt .cs .ctl .cxx .dbf .der .dib .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .h

SHA 256 Hash of files

- 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da

Payload Files SHA 256 Hashes

- 579fd8a0385482fb4c789561a30b09f25671e86422f40ef5cca2036b28f99648
- 0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6
- 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93
- 301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c
- 2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035