A new widespread ransomware worm, known as “Bad Rabbit,” that hit over 200 major organisations, primarily in Russia and Ukraine this week leverages a stolen NSA exploit released by the Shadow Brokers this April to spread across victims’ networks.

Earlier it was reported that this week’s crypto-ransomware outbreak did not use any National Security Agency-developed exploits, neither EternalRomance nor EternalBlue, but a recent report from Cisco’s Talos Security Intelligence revealed that the Bad Rabbit ransomware did use EternalRomance exploit.

NotPetya ransomware (also known as ExPetr and Nyetya) that infected tens of thousands of systems back in June also leveraged the EternalRomance exploit, along with another NSA’s leaked Windows hacking exploit EternalBlue, which was used in the WannaCry ransomware outbreak.

Bad Rabbit Uses EternalRomance SMB RCE Exploit
Bad Rabbit does not use EternalBlue but does leverage EternalRomance RCE exploit to spread across victims’ networks.

Microsoft and F-Secure have also confirmed the presence of the exploit in the Bad Rabbit ransomware.
EternalRomance is one of many hacking tools allegedly belonged to the NSA’s elite hacking team called Equation Group that were leaked by the infamous hacking group calling itself Shadow Brokers in April this year.

EternalRomance is a remote code execution exploit that takes advantage of a flaw (CVE-2017-0145) in Microsoft’s Windows Server Message Block (SMB), a protocol for transferring data between connected Windows computers, to bypass security over file-sharing connections, thereby enabling remote code execution on Windows clients and servers.

Along with EternalChampion, EternalBlue, EternalSynergy and other NSA exploits released by the Shadow Brokers, the EternalRomance vulnerability was also patched by Microsoft this March with the release of a security bulletin (MS17-010).
Bad Rabbit was reportedly distributed via drive-by download attacks via compromised Russian media sites, using fake Adobe Flash players installer to lure victims' into install malware unwittingly and demanding 0.05 bitcoin (~ $285) from victims to unlock their systems.

**How Bad Rabbit Ransomware Spreads In a Network**

According to the researchers, Bad Rabbit first scans the internal network for open SMB shares, tries a hardcoded list of commonly used credentials to drop malware, and also uses Mimikatz post-exploitation tool to extract credentials from the affected systems.
Bad Rabbit can also exploit the Windows Management Instrumentation Command-line (WMIC) scripting interface in an attempt to execute code on other Windows systems on the network remotely, noted EndGame.

However, according to Cisco's Talos, Bad Rabbit also carries a code that uses eternal romance, which allows remote hackers to propagate from an infected computer to other targets more efficiently.
"We can be fairly confident that BadRabbit includes an EternalRomance implementation used to overwrite a kernel's session security context to enable it to launch remote services, while in Nyetya it was used to install the DoublePulsar backdoor," Talos researchers wrote.
"Both actions are possible due to the fact that EternalRomance allows the attacker to read/write arbitrary data into the kernel memory space."

Is Same Hacking Group Behind Bad Rabbit and NotPetya?
Since both Bad Rabbit and NotPetya uses the commercial DiskCryptor code to encrypt the victim's hard drive and "wiper" code that could erase hard drives attached to the infected system, the researchers believe it is "highly likely" the attackers behind both the ransomware outbreaks are same.

“It is highly likely that the same group of hackers was behind BadRabbit ransomware attack on October the 25th, 2017 and the epidemic of the NotPetya virus, which attacked the energy, telecommunications and financial sectors in Ukraine in June 2017,” Russian security firm Group IB noted.

“Research revealed that the BadRabbit code was compiled from NotPetya sources. BadRabbit has same functions for computing hashes, network distribution logic and logs removal process, etc.”
NotPetya has previously been linked to the Russian hacking group known as BlackEnergy and Sandworm Team, but since Bad Rabbit is primarily targeting Russia as well, not everyone seems convinced with the above assumptions.

How to Protect Yourself from Ransomware Attacks?
In order to protect yourself from Bad Rabbit, users are advised to disable WMI service to prevent the malware from spreading over your network.

Also, make sure to update your systems regularly and keep a good and effective anti-virus security suite on your system.

Since most ransomware spread through phishing emails, malicious adverts on websites, and third-party apps and programs, you should always exercise caution before falling for any of these.
Most importantly, to always have a tight grip on your valuable data, keep a good backup routine in place that makes and saves copies of your files to an external storage device that isn’t always connected to your PC.

Action Point

**PS:** Click on the link below to sign up for my Online E-Course CRM Training. Make sure you confirm your subscription by clicking on the link sent to you. Thanks