Scam of The Week: Worldwide Bad Rabbit Ransomware Outbreak Starts with Social Engineering

The outbreak appears to have started via files on hacked Russian media websites, using the popular social engineering trick of pretending to be an Adobe Flash installer. The ransomware demands a payment of 0.05 bitcoin, or about $275, from its victim, though it isn't clear whether paying the ransom unlocks a computer's files. You have just 40 hours to pay.

Bad Rabbit shares some of the same code as the Petya virus that caused major disruptions to global corporations in June this year, said Liam O'Murchu, a researcher with the antivirus vendor Symantec Corp.

Based on analysis by ESET, Emsisoft, and Fox-IT, Bad Rabbit uses Mimikatz to extract credentials from the local computer's memory, and along with a list of hard-coded credentials, it tries to access servers and workstations on the same network via SMB and WebDAV.

The hardcoded creds are hidden inside the code and include predictable usernames such as `root`, `guest` and `administrator`, and passwords straight out of a worst passwords list. (Note To Self: all user passwords need to be strong!)

As for Bad Rabbit, the ransomware is a so-called disk coder, similar to Petya and NotPetya. Bad Rabbit first encrypts files on the user's computer and then replaces the MBR (Master Boot Record).

What Should You Do?

Be certain that all your passwords are strong. Stay away from using dictionary words. Use alpha and numeric methods. To take it a step further, add symbols. The longer the password with a variation of numbers, letters, and symbols, the stronger it will be.