Perkiler malware turns to SMB brute force to spread

blog.malwarebytes.com/trojans/2021/03/perkiler-malware-turns-to-smb-brute-force-to-spread/

Malwarebytes Labs

March 25, 2021

Researchers at Guardicore have identified a new infection vector being used by the Perkiler malware where internet-facing Windows machines are breached through SMB password brute force.

Perkiler is a complex Windows malware with rootkit components that is dropped by the Purple Fox exploit kit (EK) and was spread by phishing campaigns.

What is SMB?

Server Message Block (SMB), aka Common Internet File System (CIFS), is the network-protocol that enables file exchanges between Microsoft Windows computers. You will find it wherever Windows computers are sharing printers, files, and sometimes remote control. By default, SMB is configured to use the ports 139 and 445.

SMB vulnerability history

SMB has a history of being used by malware (coupled with a history of being enabled by mistake and exposed to the Internet by accident). The most famous example of SMB-exploiting malware is WannaCry. This worm-like outbreak spread via an operation that hunted down vulnerable public facing SMB ports and then used the EternalBlue exploit to get on the network, chained with the DoublePulsar exploit to establish persistence, and allow for the installation of the WannaCry ransomware.

What are brute force attacks?

A brute-force password attack is a relentless attempt to guess the username and password of one or more systems. As it sounds, a brute-force attack relies on force rather than cunning or skill: It is the digital equivalent of throwing everything and the kitchen sink at something. Some attacks will try endless combinations of usernames and passwords until finding a combination that works, others will try a small number of usernames and passwords on as many systems as possible.

Brute force attacks are usually automated, so they don’t cost the attacker a lot of time or energy. Certainly not as much as individually trying to figure out how to access a remote system. Based on a port number or another system-specific property, an attacker picks the target and the method and then sets his brute force application in motion. He can then move on to the next target and wait to get notified when one of the systems has swallowed the hook.

Not a new infection method

The fact that the researchers found the Perkiler malware attacking Windows machines through SMB password brute force came as something of a surprise. Not because of the SMB brute force per se. SMB has always been brute forced, but why would you bother when you have:

- EternalBlue that allows you to own every single unpatched SMB server without going through the brute force routine.
- A few million RDP ports you can brute force with a potentially bigger gain. Remote desktop is exactly what the name implies, an option to remotely control a computer system. Which is much more interesting to an attacker than just being able to drop a file on an SMB server.

The answer to this question remains a mystery for now. Maybe they are planning ahead for when the number of vulnerable RDP servers dries up.

Using compromised machines

Perkiler uses a large network of compromised servers to host its dropper and the payloads. These servers appear to be compromised Microsoft IIS 7.5 servers. Most of these Windows Servers are running IIS version 7.5 and Microsoft FTP, which are known to have multiple vulnerabilities with varying severity levels.

The rootkit

Once a machine is infected with the new variant of Perkiler, it reboots to load the rootkit that's hidden inside the encrypted payload. The purpose of this rootkit is to hide various registry keys and values, files, etc. Ironically enough, the hidden rootkit was developed by a security researcher to conduct various malware analysis tasks and to keep the research tasks hidden from the malware.

Infected machines

Once the machine is restarted, the malware will be executed as well. After its execution, the malware will start its propagation process: the malware will generate IP ranges and start scanning them on port 445. When a machine responds to the SMB probe on port 445, it will try to authenticate to SMB by brute-forcing usernames and passwords, or by trying to establish a null session.

One interesting detail is that the malware will install an IPv6 interface on the infected machine to allow the malware to port scan IPv6 addresses as well as to maximize the efficiency of the spread over (usually unmonitored) IPv6 subnets.

Mitigation

In theory, brute force password attacks conducted over the Internet can be defeated by even moderately strong passwords (six characters should be enough). However, even the threat of big-game ransomware using RDP brute force attacks hasn't been enough to get people using stronger passwords. And if the prospect of facing a $50 million ransom isn't enough motivation, it's hard to see anything else working.

Luckily there are other, easier ways to blunt brute force attacks. The best defence of all is to remove the SMB (or RDP, or anything else) service from the Internet entirely, if possible, or to put it behind a VPN protected by two-factor authentication if it isn't possible.