New Nation-State Attacker Revealed as Targeting Specific Individuals

Looks like it's time to call in Gandalf and the hobbits for an adventure to malware earth.

An extremely stealthy nation-state cyberespionage group, dubbed as Project Sauron, has recently been uncovered. Adeptly named, this ever-seeing information exfiltration malware has been spying on state organizations across the world for the past five years. Much like J. R. R. Tolkien's 'Lord of the Rings' main antagonist referenced in the source code, the group is fierce and highly sophisticated.

Threat actor alerts were issued following proof of malware on multiple company networks. To keep you safe, we've drilled down the releases to the most pertinent information you need to know about this covert operation.

Alternate Alias
You may also hear the attackers referred to as Strider Group.

Project Sauron is Highly Selective
At least 30 organizations including government, military, scientific research centers, telecommunications companies, and financial service providers have been targeted. While some security professionals have traced the malware to areas including Russia, Iran, and Rwanda, further research also found it lurking on devices in Belgium, Sweden, and China.

It would be remiss to leave out that these places aren't high on the United States' list of friends. We're not the only ones to notice and speculate that the U.S. could be behind such an advanced group. In fact, this isn't the first time the U.S. has been linked to a large-scale cyber weapon. The infamous Stuxnet virus designed to sabotage the Iranian nuclear program was rumored to be jointly built by the U.S. and Israel.

Core Payloads Are a One-Time Use
Each victim is attacked using an individualized file name and size, creating a perfect storm for those trying to identify the threat actor with basic indicators. Core implants piggyback on legitimate update scripts, providing the opportunity to download new modules and run commands in memory. This sophistication has provided an abiding way to spy while remaining elusive.

Using a high level of detail, it appears operators have chosen to target systems and infrastructures used for encryption of communications, voice, email, and document transfers. The malware is used to capture passwords, encryption keys, configuration files and log stores. Once deployed, it opens up a backdoor for complete control of the network or system.

Infects Air-Gapped Systems
After penetrating through some of the most extensive firewalls, the malware can infect air-gapped systems. Specially modified USB drives are utilized to transfer data in systems that are

not directly connected to the Internet. Masquerading as a common mass storage device, these are anything but. Using a secret partition, the USB drive conceals an entire virtual file system to be accessed by the actors.

Protecting Organizations from Advanced Cyberespionage

Security experts agree that the first step to protection is a complete audit of IT networks and endpoints, followed by:

- Implementing an anti-targeted attack solution paired with new/existing endpoints.
- Reaching out to experts when your security technology flags a problem to analyze, mitigate, and thwart the threat.
- Educating employees on spear-phishing and other approaches to promote responsible online behavior.

It's important to consistently review your company's security measures in preparation for new and more sophisticated attacks. Project Sauron's activities are just one example of un-traditional cyberespionage that break through security barriers. Prior to this threat discovery, the only other similar tool was Flamer, so it's critical to be aware and adjust systems accordingly.

If you want to learn more about malware and how to safeguard against it, download our free white paper, *The Wicked Truth About Malware & Exploits*.