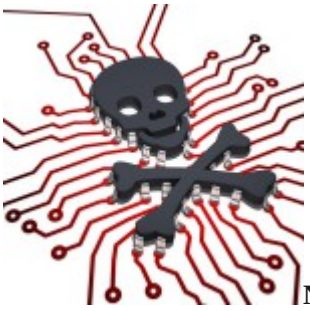
Trochilus, PlugX RATs in Targeted Attacks on Governments

By Milena Dimitrova

Published: 2016-01-12 · Archived: 2026-04-06 03:17:31 UTC



New types of RATs, or remote access Trojans, appear more often than ever before. Such Trojans are typically employed in targeted attacks against corporations, organisations and governments. One of the latest RATs, discovered by the Arbor Security Engineering & Response Team (ASERT) at Arbor Networks, has started malicious campaigns in South-East Asia. A similar RAT previously was detected in an attack against the government of Myanmar. The hacking team behind those attacks has been identified by Cisco's Talos Group as Group 27.

Learn More about RATs, Corporate Attacks and Incident Response:

- How Moker RAT Evades Detections
- Common Vulnerabilities and Exposures
- Exploit Kit Attacks

How was the attack carried out?

Watering hole attacks were performed on the government's official websites. As a result, users visiting the pages to access information on upcoming elections were infected with PlugX – a well-known RAT used in multiple attacks throughout 2015.

The fact that the attacks against Myanmar's government were disclosed hasn't stopped Group 27. According to latest reports by Arbor's Response Team (ASERT) a new remote access Trojan, associated with the group's activities has been released. During the time of analysis, the new RAT remained undetected by most antivirus vendors. This proves that this new piece crafted for cyber espionage is quite sophisticated. It has been dubbed Trochilus.

What is specific about Trochilus?

The latest Group 27's RAT includes a total of six malware strains, combined in different variations in accordance with the data targeted by the criminals.

ASERT experts named the whole collection of malware the Seven Pointed Dagger. It consists of:

- Two Trochilus RAT versions;
- A version of the 3012 variant of the 9002 RAT;
- An EvilGrab RAT version;
- One unknown piece of malware yet to be identified.

Security analysts believe that Group 27 didn't care much about the fact that their initial cyber espionage campaign was detected. Furthermore, the group continued infecting victims via the very same entrance – the Myanmar Election Commission website.

Trochilus RAT source code uploaded on GitHub

Despite that the RAT was designed to execute in the memory of the machine (thus evading detection by AV software), ASERT researchers obtained the RAT's source code and connected it to a GitHub profile of a user named 5loyd.

On the GitHub page, the RAT has been advertised as a fast and free Windows remote administration tool. **Other details include:**

- Written in CC+;
- Supports various communication protocols;
- Has a file manager module, a remote shell, a non-UAC mode;
- Able to uninstall itself;
- Able to upload information from remote machines;
- Able to download an execute files.

Researchers believe that 5loys is not a part of Group 27. More likely, the user's profile has been hijacked by the group and used for their own purposes.

Spy Hunter scanner will only detect the threat. If you want the threat to be automatically removed, you need to purchase the full version of the anti-malware tool.Find Out More About SpyHunter Anti-Malware Tool / How to Uninstall SpyHunter

Milena Dimitrova

An inspired writer and content manager who has been with SensorsTechForum since the project started. A professional with 10+ years of experience in creating engaging content. Focused on user privacy and malware development, she strongly believes in a world where cybersecurity plays a central role. If common sense makes no sense, she will be there to take notes. Those notes may later turn into articles! Follow Milena @Milenyim

More Posts

Follow Me: