# Strider cyber attack group deploying malware for espionage

By Warwick Ashford

Published: 2016-08-08 · Archived: 2026-04-05 17:53:14 UTC

## Symantec security researchers have uncovered a spying campaign by a previously unknown group using modular malware as stealthware

- 
- 

Srtider, a previously unknown group of cyber attackers, is using stealthware for cyber espionage campaigns, security firm Symantec has revealed.

Strider is using an advanced piece of malware called Backdoor.Remsec to spy on targets in Russia, China, Sweden and Belgium.

According to Symantec researchers, Remsec appears to be designed for spying, with references in the code to Sauron, the all-seeing antagonist in *Lord of the Rings*.

Strider is capable of creating custom malware tools and has operated below the radar for at least five years, Symantec said.

Based on the espionage capabilities of the malware and the nature of its known targets, it is possible that the group is a nation-state attacker.

Other Symantec findings reveal possible links to a previously uncovered group known as Flamer because of similar techniques used.

Investigation revealed that one of Strider’s targets had also previously been infected by the Regin spyware, known for its use for systematic spying campaigns.

## Low profile

Although Strider is believed to have been active since at least October 2011, the group has maintained a low profile until now. Its targets have been mainly organisations and individuals that would be of interest to a nation state’s intelligence services.

Symantec obtained a sample of the group’s Remsec malware from a customer who submitted it following its detection by the company’s behavioural engine.

According to the researchers, Remsec typically establishes a means of enabling an attacker to bypass security mechanisms, creating a back door into computer systems so login credentials and data can be stolen.

Strider has been highly selective in its choice of targets. To date, Symantec has found evidence of infection in 36 computers across seven separate organisations. The group's targets include a number of organisations and individuals in Russia, an airline in China, an organisation in Sweden, and an embassy in Belgium.

## Modular malware

The researchers said the Remsec malware consists of modules working together as a framework that provides complete control over an infected computer, allowing the attacker to move across a network, exfiltrate data and deploy custom modules.

Several examples of Remsec use modules written in the Lua programming language. Remsec uses a Lua interpreter to run Lua modules which perform various functions, the researchers said.

Modules include a loader (to open files from disk and execute them) that masquerades as a security support provider, a host loader that decrypts and loads other Lua modules, a keylogger to record keystrokes and exfiltrate this data, a network listener for opening a network connection based on monitoring for specific types of traffic, and an HTTP back door that includes several addresses for a command and control server.

Remsec contains a number of features to help it avoid detection. Several components are in the form of executable binary large objects (blobs), which are more difficult for traditional antivirus software to detect.

In addition, much of the malware's functionality is deployed over the network, so it resides only in the computer's memory and is never stored on disk, which makes it harder to detect.

Symantec said its researchers will continue to search for more Remsec modules and targets to build their understanding of Strider. In the meantime, they have compiled an indicators-of-compromise document containing further details to help organisations identify the threats associated with Strider in their own IT environments.

**Read more on Hackers and cybercrime prevention**

- 

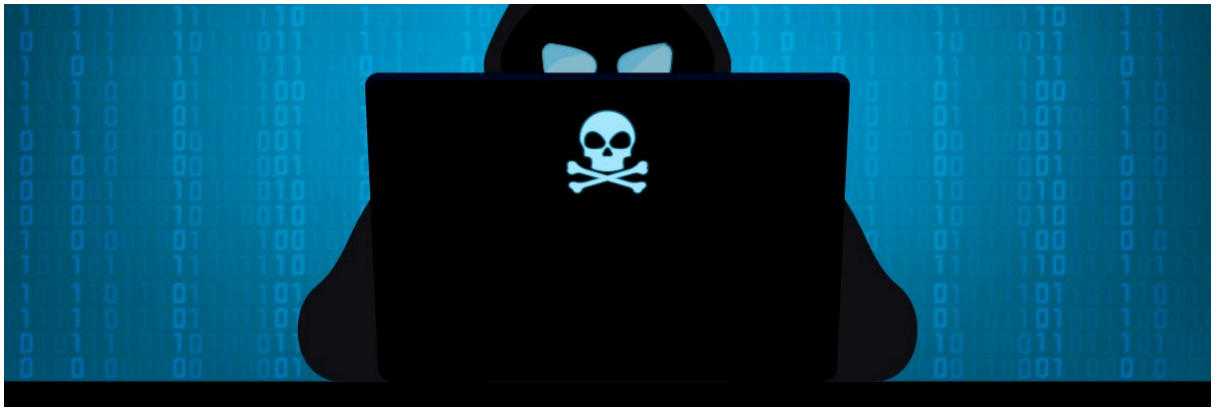
  **Black Basta might have exploited Microsoft flaw as zero-day**

By: Arielle Waldman

- 

**Exploitation of Barracuda ESG appliances linked to Chinese spies**

By: Alex Scroxton



**Barracuda zero-day bug exploited months prior to discovery**

By: Alexander Culafi

**ALPHV/BlackCat ransomware family becoming more dangerous**

By: Alex Scroxton

---