Strider: Cyberespionage group turns eye of Sauron on targets

symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets

August 6, 2016

Symantec Official Blog

Low-profile group uses Remsec malware to spy on targets in Russia, China, and Europe.

By: Symantec Security ResponseSymantec Employee

- Created 07 Aug 2016
- : 简体中文, 日本語

A previously unknown group called Strider has been conducting cyberespionage-style attacks against selected targets in Russia, China, Sweden, and Belgium. The group uses an advanced piece of malware known as Remsec (Backdoor.Remsec) to conduct its attacks. Remsec is a stealthy tool that appears to be primarily designed for spying purposes. Its code contains a reference to Sauron, the all-seeing antagonist in Lord of the Rings.

Strider's attacks have tentative links with a previously uncovered group, Flamer. The use of Lua modules, which we'll discuss later, is a technique that has previously been used by Flamer. One of Strider's targets had also previously been infected by Regin.

Background

Strider has been active since at least October 2011. The group has maintained a low profile until now and its targets have been mainly organizations 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 our behavioral engine.

Remsec is primarily designed to spy on targets. It opens a back door on an infected computer, can log keystrokes, and steal files.

Targets

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

Figure 1. Only a small number of organizations in four countries are impacted by Strider

Stealthy back door

The Remsec malware used by Strider has a modular design. Its modules work together as a framework that provides the attackers with complete control over an infected computer, allowing them to move across a network, exfiltrate data, and deploy custom modules as required.

Remsec contains a number of stealth features that help it to avoid detection. Several of its components are in the form of executable blobs (Binary Large Objects), which are more difficult for traditional antivirus software to detect. In addition to this, much of the malware's functionality is deployed over the network, meaning it resides only in a computer's memory and is never stored on disk. This also makes the malware more difficult to detect and indicates that the Strider group are technically competent attackers.

Remsec modules seen by Symantec to date include:

- **Loader:** Named MSAOSSPC.DLL, this module is responsible for loading files from disk and executing them. The files on disk contain the payload in an executable blob format. The loader also logs data. Executable blobs and data are encrypted and decrypted with a repeating key of 0xBAADF00D. The loader maintains persistence by being implemented as a fake Security Support Provider.
- **Lua 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. These Lua modules are stored in the same executable blob format as the loader. Lua modules include:
    - **Network loader** – This loads an executable over the network for execution. It may use RSA/RC6 encryption.
    - **Host loader** – This is used to decrypt and load at least three other Lua modules into running processes. It references three named modules: ilpsend, updater (neither of which has been discovered to date), and, kblog (likely the Keylogger module detailed below).
    - **Keylogger** – This logs keystrokes and exfiltrates this data to a server under the attackers' control. This is the module that contains a string named "Sauron" in its code. Given its capabilities, it is possible the attackers have nicknamed the module after the all-seeing villain in Lord of the Rings.

Figure 2. String referencing Sauron in Remsec keylogger module

- **Network listener:** A number of examples of Remsec implement different techniques for opening a network connection based on monitoring for specific types of traffic. These include ICMP, PCAP, and RAW network sockets.
- **Basic pipe back door:** This is a minimal back door module, controlled over named pipes. It can execute data in the format of the executable blob or a standard executable.
- **Advanced pipe back door:** This offers several more commands than the basic version, including sending the executable blob, listing files, and reading/writing/deleting files.
- **HTTP back door:** This module includes several URLs for a command and control (C&C) server.

Strider is capable of creating custom malware tools and has operated below the radar for at least five years. Based on the espionage capabilities of its malware and the nature of its known targets, it is possible that the group is a nation-state level attacker. Symantec will continue to search for more Remsec modules and targets in order to build upon our understanding of Strider and better protect our customers.

Protection

Symantec and Norton products detect this threat as Backdoor.Remsec.

Indicators of compromise

We have also compiled an indicators-of-compromise document containing further details which can be used to help identify the threats if they are present in your environment.

- Tags: Products, Endpoint Protection, Security Response, Backdoor.Remsec, Belgium, China, Cyberespionage, Flamer, LOTR, Malware, Russia, Strider, Sweden
- Subscriptions (0)