Endpoint Protection

symantec.com/connect/blogs/sowbug-cyber-espionage-group-targets-south-american-and-southeast-asian-governments

Nov 07, 2017 09:00 AM

A L Johnson

Symantec has identified a previously unknown group called Sowbug that has been conducting highly targeted cyber attacks against organizations in South America and Southeast Asia and appears to be heavily focused on foreign policy institutions and diplomatic targets. Sowbug has been seen mounting classic espionage attacks by stealing documents from the organizations it infiltrates.

Symantec saw the first evidence of Sowbug-related activity with the discovery in March 2017 of an entirely new piece of malware called Felismus used against a target in Southeast Asia. We have subsequently identified further victims on both sides of the Pacific Ocean. While the Felismus tool was first identified in March of this year, its association with Sowbug was unknown until now. Symantec has also been able to connect earlier attack campaigns with Sowbug, demonstrating that it has been active since at least early-2015 and may have been operating even earlier.

To date, Sowbug appears to be focused mainly on government entities in South America and Southeast Asia and has infiltrated organizations in Argentina, Brazil, Ecuador, Peru, Brunei and Malaysia. The group is well resourced, capable of infiltrating multiple targets simultaneously and will often operate outside the working hours of targeted organizations in order to maintain a low profile.

[click_to_tweet:1]

Highly targeted intrusions

Some clues about the motivation and interests of the attackers can be found in their activities after compromising victims. For example, in a 2015 attack on one South American foreign ministry, the group appeared to be searching for very specific information.

The first evidence of its intrusion dated from May 6, 2015 but activity appeared to have begun in earnest on May 12. The attackers appeared to be interested in one division of the ministry that is responsible for relations with the Asia-Pacific region. They attempted to extract all Word documents stored on a file server belonging to this division by bundling them into a RAR archive by running the following command:

cmd.exe /c c:\windows\rar.exe a -m5 -r -ta20150511000000 -v3072 c:\recycler\[REDACTED].rar "\\[REDACTED]*.docx" \\[REDACTED]*.doc.

Interestingly, the command specified that only files modified from May 11, 2015 onwards should be archived.

The attackers appear to have successfully extracted the archive because an hour later they returned, this time attempting to extract all documents modified from May 7, 2015, an extra four days' worth of data. Presumably they either didn't find what they were looking for in the initial incursion, or else noticed something in the documents they stole earlier that prompted them to hunt for more information.

The attackers didn't stop there. Their next move was to list any remote shared drives and then attempt to access remote shares owned by the specific government office they were targeting, again attempting to extract all Word documents. In this case, they searched for any documents modified from May 9 onwards. The attackers then seemed to broaden their interest, listing the contents of various directories on remote shares, including one belonging to another division of the South American foreign ministry, this one responsible for relations with international organizations. They also deployed two unknown payloads to the infected server. In total, the attackers maintained a presence on the target's network for four months between May and September 2015.

Network traversal: Keeping a low profile

Sowbug frequently maintains a long-term presence on the networks of targeted organizations, sometimes remaining inside a victim environment for up to six months. One of the tactics it uses to avoid drawing attention to itself is impersonating commonly used software packages such as Windows or Adobe Reader. It has never attempted to compromise the software itself. Rather, it gives its tools file names similar to those used by

the software and places them in directory trees that could be mistaken for those used by the legitimate software. This allows the attackers to hide in plain sight, as their appearance in process listings is unlikely to arouse suspicion.

For example, in September 2016, Sowbug infiltrated an organization in Asia, deploying the Felismus backdoor on one of its computers, Computer A, using the file name adobecms.exe in CSIDL_WINDOWS\debug. From there, it installed additional components and tools to a directory named CSIDL_APPDATA\microsoft\security.

The attackers then began to perform reconnaissance activities on Computer A via cmd.exe, collecting system-related information, such as the OS version, hardware configuration, and network information. They then performed some further reconnaissance, attempting to identify all installed applications on the computer. They returned four days later, creating a sub-directory called “common” in the Adobe directory of the Program Files folder, i.e. c:\Program Files\Adobe\common, and installed another tool in this sub-directory, again named adobecms.exe. This was possibly an updated version of the backdoor.

The attackers’ network reconnaissance appeared to be successful because a second computer of interest in the organization was identified and compromised. The attackers then returned to Computer A, installing another executable called fb.exe. This file appears to be used to copy Felismus across the network to other computers and there is evidence that the attackers used it to attempt to infect at least two more computers.

The attackers took further measures to remain under the radar by carrying out their operations outside of standard office hours. In this case, the attackers maintained a presence on the target’s network for nearly six months between September 2016 and March 2017.

Infection vectors

How Sowbug performs its initial infiltration of a target’s network remains unknown. In some cases, there was no trace of how Felismus made its way onto compromised computers, meaning it was likely deployed from other compromised computers on the network. In other attacks, there was evidence that Felismus was installed using a tool known as Starloader (detected by Symantec as Trojan.Starloader). This is a loader that installs and decrypts data from a file called Stars.jpg. Additionally, Starloader was also observed deploying additional tools used by the attackers, such as credential dumpers and keyloggers.

It is still unknown how Starloader is installed on the compromised computer. One possibility is that the attackers use fake software updates to install files. Symantec has found evidence of Starloader files being named AdobeUpdate.exe, AcrobatUpdate.exe, and INTELUPDATE.EXE among others. These were used to create versions of the Felismus backdoor as well as other tools.

Global threat

While cyber espionage attacks are often seen against targets in the U.S., Europe, and Asia, it is much less common to see South American countries targeted. However, the number of active cyber espionage operations has increased steadily in recent years and the emergence of Sowbug is a reminder that no region is immune to this kind of threat.

Protection

Symantec customers are protected against Sowbug and Symantec has also made efforts to notify identified targets of its operations.

Customers with Intelligence Services or WebFilter-enabled products are protected against activity associated with the Sowbug group. These products include:

- Web Security Service (WSS)
- ProxySG
- Advanced Secure Gateway (ASG)
- Security Analytics
- Content Analysis
- Malware Analysis
- SSL Visibility
- PacketShaper

Symantec has the following specific detections in place for the threats called out in this blog:

AV

- Backdoor.Felismus
- Trojan.Starloader

IPS

Indicators of compromise

Backdoor.Felismus samples

MD5	Detection
514f85ebb05cad9e004eee89dde2ed07	Backdoor.Felismus
00d356a7cf9f67dd5bb8b2a88e289bc8	Backdoor.Felismus
c1f65ddabcc1f23d9ba1600789eb581b	Backdoor.Felismus
967d60c417d70a02030938a2ee8a0b74	Backdoor.Felismus

Trojan.Starloader samples

MD5	Detection
4984e9e1a5d595c079cc490a22d67490	Trojan.Starloader

Hacktools

MD5	Detection
e4e1c98feac9356dbfcac1d8c362ab22	Hacktool.Mimikatz

Installation directory

- %WINDOWS%\debug
- %APPDATA%\microsoft\security

Command and control infrastructure

- nasomember[DOT]com
- cosecman[DOT]com
- unifoxs[DOT]com