This stealthy cat-and-mouse hacking campaign aims to steal diplomatic secrets

By Written by Danny Palmer, Senior WriterSenior Writer Nov. 7, 2017 at 6:00 a.m. PT

Archived: 2026-04-05 12:39:20 UTC

Video: Ransomware using trojan trick to expand threat

A previously unknown hacking and espionage operation is using malware to infiltrate governments in an attempt to steal sensitive data in a series of highly targeted attacks.

Dubbed Sowbug, the group behind the attacks is apparently focused on foreign policy institutions and diplomatic targets in South America and South East Asia and is thought to have been active since at least early 2015.

A low-profile, under-the-radar operation has helped the operation avoid detection, even as it carried out campaigns which remained undetected by governments for up to six months.

Governments in Brazil, Argentina, Peru, Ecuador, Malaysia, and Brunei have all fallen victim to the Sowbug campaign, which has been detailed by researchers at Symantec.

The group uses Felismus, a backdoor trojan, in all of its attacks. The malware was first identified in March and among other things allows attackers to conduct espionage, key-logging, traffic analysis, further malware deployment, the ability to evade detection and more.

The group behind the attacks is described as well resourced and capable of infiltrating multiple targets simultaneously via campaigns which operate outside the working hours of targeted organisations in order to ensure the attacks keep a low profile.

While it's unknown where in the world the Sowbug is based, or who they ultimately are -- or work on behalf of -- it's possible it could be a state-backed operation.

"They bear some hallmarks of a group potentially backed by a nation-state -- the malware used in those attacks appear to be sophisticated. The group is likely to be well resourced, which has enabled it to remain under the radar

and steal information from these foreign policy and diplomatic targets since early 2015," Alan Neville, threat researcher at Symantec, told ZDNet.

Analysis of compromised victims has shone light on Sowbug's activities, as well as clues to the group's potential motivations -- which appear to be based around the theft of specific information.

See also: Cyberwar: A guide to the frightening future of online conflict

One attack against a South American foreign ministry - dated to have taken place in May 2015 - appeared to focus specifically on the division responsible for relations with the Asia-Pacific region. The attack resulted in all Word documents modified after May 11 stored within the target's file server being extracted.

The attackers later returned to extract all documents modified from May 7, 2015. Additional attacks continued - with more and more documents being removed and the deployment of two unknown payloads to the infected server - for another four months, before those behind the campaign wiped their presence from the server in September 2015.

One method attackers use to maintain long-term presence on infected networks is by disguising the malicious files as commonly used software such as Windows or Adobe Reader. The malicious tools are given file names similar to those used by legitimate software and hidden in directory trees, allowing them to remain present without arising suspicion.

The stealthy nature of the Sowbug operation and its Felismus distribution campaign means it's still isn't known how attackers initially infiltrate a target's network.

In some cases, there's no trace of how Felismus made its way onto compromised computers - pointing to the possibility it was deployed from an already-compromised system on the network. In other instances, there's some evidence that the Felismus is installed using a malware loader called Starloader, but it's unknown how Starloader itself invades a computer.

One theory is that Starloader is deployed as fake software updates, as researchers found evidence of Starloader files AdobeUpdate.exe, AcrobatUpdate.exe, and INTELUPDATE.EXE among others.

Sowbug also serves as a reminder that no matter where a target is in the world, they could become the victim of cyber attacks and espionage.

"While we're not at the stage where no region is untouched by cyber espionage, it was previously unusual to see countries in South America targeted by groups such as Sowbug," said Neville.

Felismus acquired its named upon its initial discovery in March because of a reference to *Tom & Jerry* in its only human-readable encryption key - Felis is Latin for 'cat' and Mus is Latin for 'mouse'.

Felismus malware has acquired its name from references to a cat and mouse in the code.

Image: iStock

Previous and related coverage

What is phishing?

Everything you need to know to protect yourself from scam emails and more

IT leader's guide to the threat of cyberwarfare [Tech Pro Research]

As we become increasingly reliant on digital infrastructure, the possibility of a crippling cyberattack continues to mount. Communications and banking systems, power grids and factories--all face an increased risk of attack.

Cybercrime Inc: How hacking gangs are modeling themselves on big business

Franchises, resellers, customer service, collaboration tools, and training -- professional hacking organizations are now operating like any other business.

Read more on cybercrime

- Hackers are using hotel Wi-Fi to spy on guests, steal data
- Chinese hacking group returns with new tactics for espionage campaign
- Hackers gain access to hundreds of global electric systems [CNET]
- CIA tools exposed by Wikileaks linked to hacking across 16 countries
- The new art of war: How trolls, hackers and spies are rewriting the rules of conflict [TechRepublic]
