Sophisticated 'Turla' hackers spying on European governments, say researchers

theguardian.com/technology/2014/aug/07/turla-hackers-spying-governments-researcher-kaspersky-symantec

August 7, 2014

This article is more than **7 years old**
This article is more than 7 years old

For six years, a mysterious and highly skilled group of hackers have been targeted governments across Europe and the US - and are still at large, say experts at Black Hat

Researchers at the Black Hat hackers' convention in Las Vegas revealed new details about a mysterious and powerful group of hackers known as Turla Photograph: Steve Marcus/Reuters Photograph: STEVE MARCUS/REUTERS
Researchers at the Black Hat hackers' convention in Las Vegas revealed new details about a mysterious and powerful group of hackers known as Turla Photograph: Steve Marcus/Reuters Photograph: STEVE MARCUS/REUTERS
One of the most sophisticated and prolonged cyber espionage campaigns ever seen has been targeting major governments and militaries for more than six years, researchers have revealed.

Dubbed the ‘Turla’ hackers, initial intelligence had indicated western powers were key targets, but it was later determined embassies for Eastern Bloc nations were of more interest.

Embassies in Belgium, Ukraine, China, Jordan, Greece, Kazakhstan, Armenia, Poland, and Germany were all attacked, though researchers from Kaspersky Lab and Symantec could not confirm which countries were the true targets.

In one case from May 2012, the office of the prime minister of a former Soviet Union member country was infected, leading to 60 further computers being affected, Symantec researchers said.

There were some other victims, including the ministry for health of a Western European country, the ministry for education of a Central American country, a state electricity provider in the Middle East and a medical organisation in the US, according to Symantec.

It is believed the group was also responsible for a much-documented 2008 attack on the US Central Command.

The attackers - who continue to operate - have ostensibly sought to carry out surveillance on targets and pilfer data, though their use of encryption across their networks has made it difficult to ascertain exactly what the hackers took. Kaspersky Lab, however, picked up a number of the attackers’ searches through their victims’ emails, which included terms such as “Nato” and “EU energy dialogue”.

Though attribution is difficult to substantiate, Russia has previously been suspected of carrying out the attacks and Symantec’s Gavin O’Gorman told the Guardian a number of the hackers appeared to be using Russian names and language in their notes for their malicious code. Cyrillic was also seen in use.

Whether the attackers are Russian or using Russian identities, their target list and the quality of their code indicated they were almost certainly nation state sponsored, the researchers said.

As a sign of the high technical capability of the hackers, O’Gorman said they were able to spread across company networks very quickly as soon as they had infected one employee. In one case they were able to spread to approximately 40 machines in one organisation within a day.

They have also used zero-day vulnerabilities, previously undiscovered software flaws that have not yet been repaired - flaws that require considerable skill, time and resource to identify.

Turla has also been developing its own malware for years, eventually adding rootkit capabilities, which run malicious code before the operating system loads. This kind of malware is rare, complex and very useful for spying on systems without being detected.

The hackers used two techniques to infect victims with the Turla malware, also known as Uroboros. Either they would hack into sites they believed their targets would visit and launch malware from there, known as “watering hole” attacks, or they would send emails containing malicious links and attachments directly to individuals.

One set of attacks used fake emails claiming to have come from a military attaché at a Middle Eastern embassy, containing an attachment masquerading as the minutes of meetings. When clicked on the Turla malware would be thrust on to the user’s computer.

Kaspersky said it had seen more than 100 websites hacked by the Turla crew, including the Palestinian Authority Ministry of Foreign Affairs.

The attacks were multi-staged. Often malware called Wipbot was initially downloaded, which would do reconnaissance to determine whether the target was worth surveilling. Wipbot would then be used to download the Turla spy tool, which has far greater capability. That would then give the attackers remote access to the infected computer, meaning they could siphon off the relevant data and install further malware.

“The current campaign is the work of a well-resourced and technically competent attack group that is capable of penetrating many network defenses,” Symantec added in its blog post.

Hacker makes $84k hijacking Bitcoin mining pool

Topics

Hacking