Turla Hiding in the Sky: Russian Speaking Cyberespionage Group Exploits Satellites to Reach the Ultimate Level of Anonymity

9 September 2015

While investigating the infamous Russian-speaking cyberespionage actor Turla, Kaspersky Lab researchers have discovered how it's evading detection of its activity and physical location. As a solution for anonymity, the group uses security weaknesses in global satellite networks.

Turla is a sophisticated cyberespionage group that has been active for more than 10 years. The attackers behind Turla have infected hundreds of computers in more than 45 countries, including government institutions and embassies, as well as military, education, research and pharmaceutical companies. At the initial stage, the Epic backdoor performs victim profiling. For only the most high profile targets, the attackers then use an extensive satellite-based communication mechanism in the final stages of the attack, which helps them to hide their traces.

Satellite communications are known mostly as a tool for TV broadcasting and secure communications; however, they are also used to provide access to the Internet. Such services are mostly used in remote locations where all other types of Internet access are either unstable and slow, or not available at all. One of the most widespread and inexpensive types of satellite-based Internet connection is a so-called downstream-only connection.

In this case, outgoing requests from a user's PC are communicated through conventional lines (a wired or GPRS connection), with all the incoming traffic coming from the satellite. This technology allows the user to get a relatively fast download speed. However, it has one big disadvantage: all the downstream traffic comes back to the PC unencrypted. Any rogue user with the right set of inexpensive equipment and software could simply intercept the traffic and get access to all the data that users of these links are downloading.

The Turla group takes advantage of this weakness in a different way: by using it to hide the location of its Command and Control servers (C&C), one of the most important parts of the malicious infrastructure. The C&C server is essentially a "homebase" for the malware deployed on targeted machines. Discovering the location of such a server can lead investigators to uncover details about the actor behind an operation, so here's how the Turla group is avoiding such risks:

1. The group first "listens" to the downstream from the satellite to identify active IP addresses of satellite-based Internet users who are online at that moment.

2. They then choose an online IP address to be used to mask a C&C server, without the legitimate user's knowledge.

3. The machines infected by Turla are then instructed to exfiltrate data towards the chosen IPs of regular satellite-based Internet users. The data travels through conventional lines to the satellite Internet provider's teleports, then up to the satellite, and finally down from the satellite to the users with the chosen IPs.

Interestingly, the legitimate user whose IP address has been used by the attackers to receive data from an infected machine, will also receive these packets of data but will barely notice them. This is because the Turla attackers instruct infected machines to send data to ports that, in the majority of cases, are closed by default. So the PC of a legitimate user will simply drop these packets, while the Turla C&C server, which keeps those ports open, will receive and process the exfiltrated data.

Another interesting thing with the Turla actor tactics is that they tend to use satellite Internet connection providers located in Middle Eastern and African countries. In their research, Kaspersky Lab experts have spotted the Turla group using IPs of providers located in Afghanistan, Congo, Lebanon, Lybia, Niger, Nigeria, Somalia and Zambia.

Satellites that are used by operators in these countries usually do not cover European and North American territories, making it very hard for most of security researchers to investigate such attacks.

"In the past, we've seen at least three different actors using satellite-based Internet links to mask their operations. Of these, the solution developed by the Turla group is the most interesting and unusual. They are able to reach the ultimate level of anonymity by exploiting a widely used technology – one-way satellite Internet. The attackers can be anywhere within range of their chosen satellite, an area that can exceed thousands of square kilometers," said Stefan Tanase, Senior Security Researcher at Kaspersky Lab. "This makes it almost impossible to track down the attacker. As the use of such methods becomes more popular, it's important for system administrators to deploy the correct defense strategies to mitigate such attacks."

Kaspersky Lab products successfully detect and block the malware used by the Turla threat actor.

Read more about the mechanisms for abusing of satellite-based Internet links used by the Turla cyberespionage group, and find Indicators of Compromise, on Securelist.com

About Kaspersky Lab

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997 Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.
Learn more at www.kaspersky.com.