Turla APT Group Abusing Satellite Internet Links

By Michael Mimoso

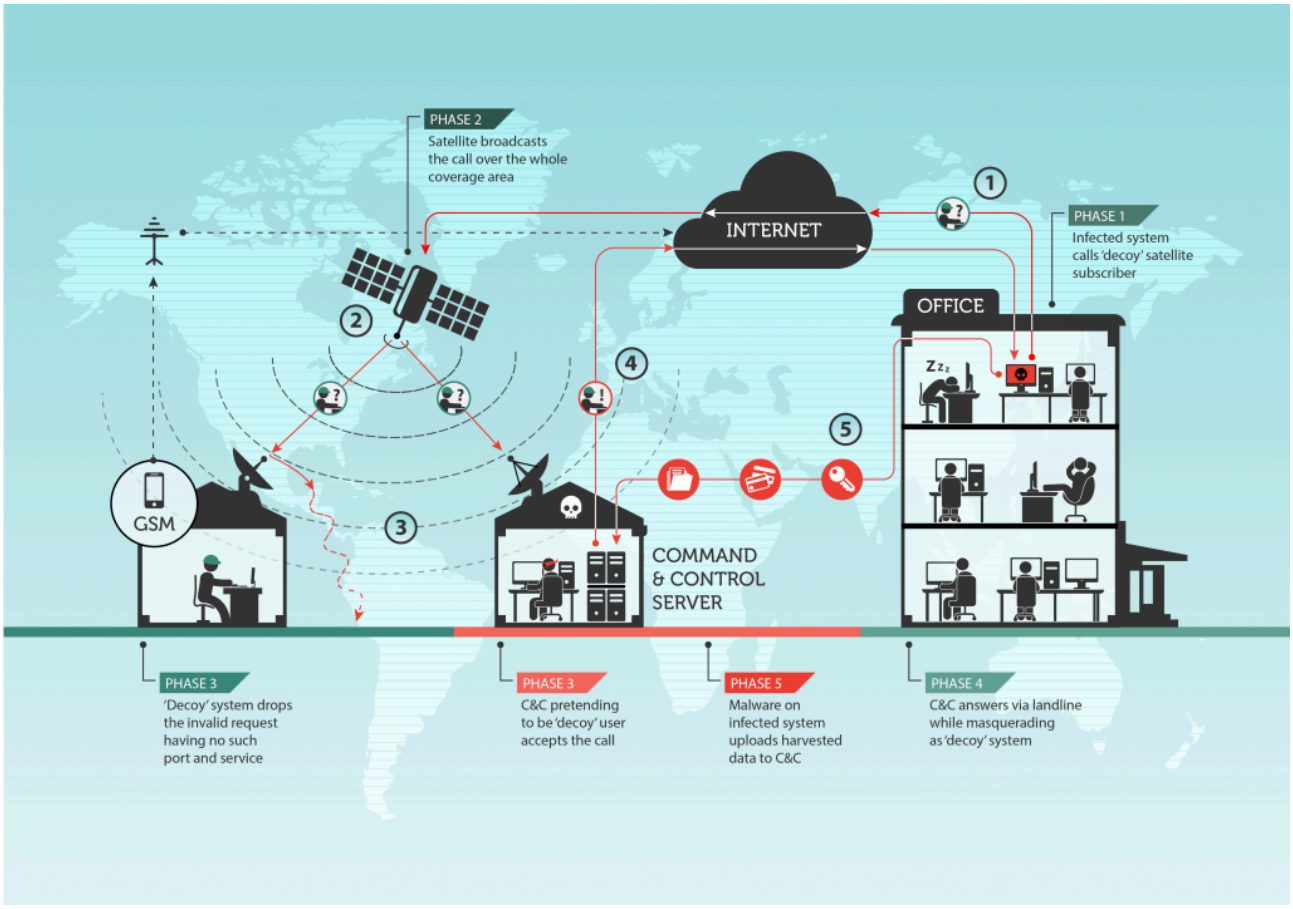
Published: 2015-09-09 · Archived: 2026-04-05 14:20:56 UTC

Researchers at Kaspersky Lab have revealed that the Turla APT gang is using satellite-based Internet links to hide command-and-control activities.

Poorly secured satellite-based Internet links are being abused by nation-state hackers, most notably by the Turla APT group, to hide command-and-control operations, researchers at Kaspersky Lab said today.

Active for close to a decade, Turla's activities were exposed last year; the Russian-speaking gang has carried out espionage campaigns against more than 500 victims in 45 countries, most of those victims in critical areas such as government agencies, diplomatic and military targets, and others.

Its use of hijacked downstream-only links is a cheap ($1,000 a year to maintain) and simple means of moving malware and communicating with compromised machines, Kaspersky researchers wrote in a report. Those connections, albeit slow, are a beacon for hackers because links are not encrypted and ripe for abuse.



"Once an IP address that is routed through the satellite's downstream link is identified, the attackers start listening for packets coming from the internet to this specific IP," the researchers wrote. "When such a packet is identified,

for instance a TCP/IP SYN packet, they identify the source and spoof a reply packet (e.g. SYN ACK) back to the source using a conventional Internet line."

The victim, meanwhile, is none the wiser because the link ignores the packet because it's going to an unconventional port.

"There is an important observation to make here," the researchers wrote. "Normally, if a packet hits a closed port, a RST or FIN packet will be sent back to the source to indicate that there is nothing expecting the packet. However, for slow links, firewalls are recommended and used to simply DROP packets to closed ports. This creates an opportunity for abuse."

Abuse of satellite links is not solely the domain of Turla. HackingTeam command and control servers, for example, were found to be using such links to mask operations, as were links traced to Rocket Kitten and Xumuxu, two APT groups that are government-backed or have governments as customers, Kaspersky said.

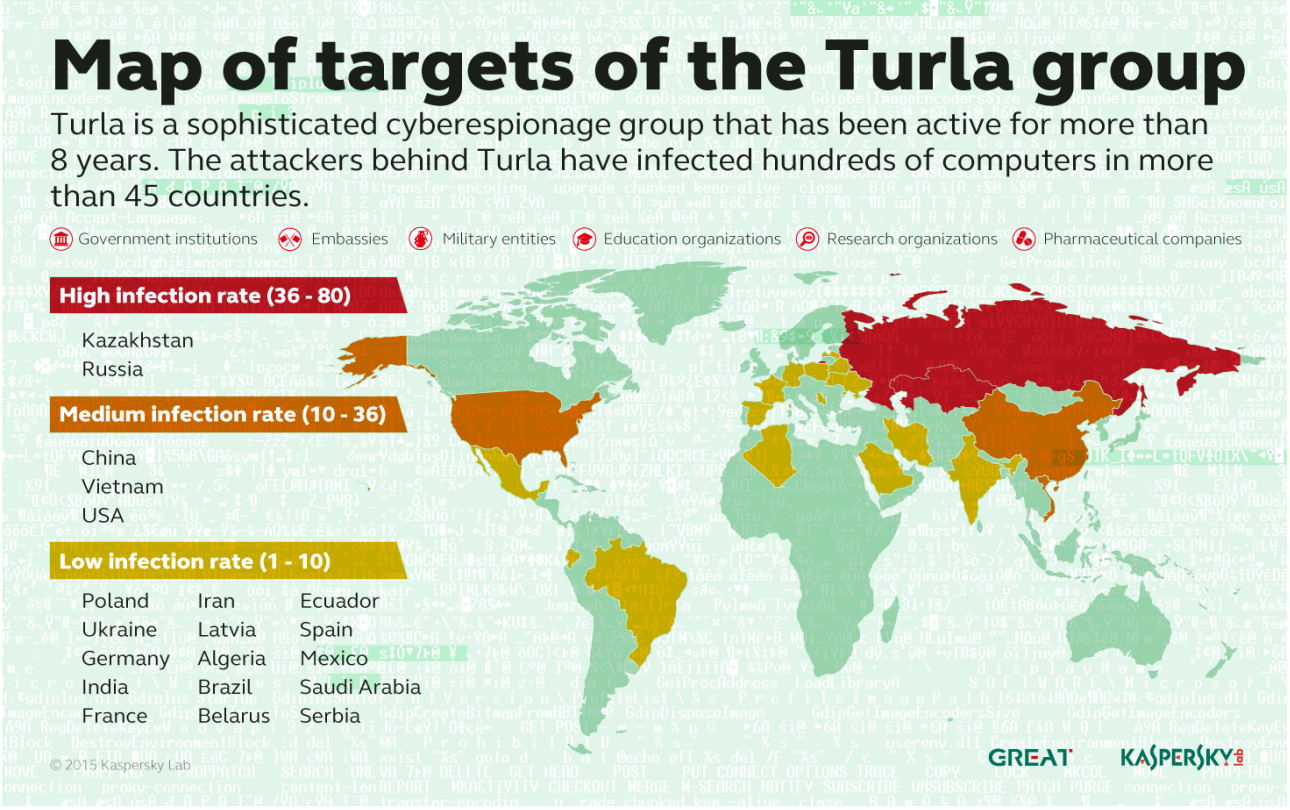
Kaspersky speculates that APT groups turn to satellite-based Internet links for C&C for a number of reasons, including as a countermeasure against botnet takedowns by law enforcement and ISPs, which open an avenue for researchers to determine who is behind an operation. Using these satellite links, however, is not without its risks to the attacker.

"On the one hand, it's valuable because the true location and hardware of the C&C server cannot be easily determined or physically seized. Satellite-based Internet receivers can be located anywhere within the area covered by a satellite, and this is generally quite large," the researchers wrote. "The method used by the Turla group to hijack the downstream links is highly anonymous and does not require a valid satellite Internet subscription. On the other hand, the disadvantage comes from the fact that satellite-based Internet is slow and can be unstable."

Rather than buy expensive subscriptions to the satellite-based links or hack an ISP with a man-in-the-middle attack at the router level in order to hijack streams, Turla's approach is much cheaper and keeps the attackers anonymous, Kaspersky said. They instead hijack satellite DVB-S links—similar research was presented at Black

Hat in 2010—that requires minimal equipment including a satellite dish, a low-noise block downconverter, a dedicated DVB-S tuner on a PCIe card made by TBS Technologies, and a Linux PC.

"The TBS card is particularly well-suited to this task because it has dedicated Linux kernel drivers and supports a function known as a brute-force scan which allows wide-frequency ranges to be tested for interesting signals," the researchers wrote. "Of course, other PCI or PCIe cards might work as well, while, in general the USB-based cards are relatively poor and should be avoided."



The group behind Turla has been abusing DVB-S (digital video broadcasting-satellite) Internet providers in the Middle East and Africa, locations where their satellite beams do not cover Europe or Asia, steering them clear of many security researchers. Kaspersky published a long list of command and control servers resolving to satellite-based ISPs in its report, calling out one in particular falling into the range of Germany's IABG mbH. The IP address is encrypted in the C&C server, which is a Turla backdoor called Agent.DNE compiled in 2007.

"Of course, for logistical reasons it is more straightforward to rely on bullet-proof hosting, multiple proxy levels or hacked websites, but this method provides an unmatched level of anonymity," the researchers wrote. "In truth, the Turla group has been known to use all these other techniques as well, making it for a very versatile, dynamic and flexible cyber-espionage operations."

Last August, researchers at Kaspersky exposed many of Turla's traditional hacking activities, including the use of watering hole attacks and spear phishing to initially compromise victims with the Snake or Uroburos backdoor. The Epic Turla campaign also used at least two zero-day exploits at the time, giving the hackers privilege escalation on Windows machines and code execution via an Adobe Reader vulnerability. There were also exploits against a number of patched vulnerabilities.
