Linux Modules Connected to Turla APT Discovered

By Michael Mimoso

Published: 2014-12-09 · Archived: 2026-04-02 10:37:20 UTC

Researchers at Kaspersky Lab have found two Linux modules connected to the Turla APT campaigns.

The Turla APT campaigns have a broader reach than initially anticipated after the recent discovery of two modules built to infect servers running Linux. Until now, every Turla sample in captivity was designed for either 32- or 64-bit Windows systems, but researchers at Kaspersky Lab have discovered otherwise.

“The attack tool takes us further into the set alongside the Snake rootkit and components first associated with this actor a couple years ago,” wrote Kurt Baumgartner and Costin Raiu, researchers with Kasperky’s Global Research and Analysis Team. “We suspect that this component was running for years at a victim site, but do not have concrete data to support that statement just yet.”

Like its Windows brethren, this version of Turla is a backdoor used to open communication to a command and control server—Kaspersky said it has sink-holed one such domain, which is based on UDP packets, used by one of the Linux modules—for file exfiltration, remote management and remote code execution.

Turla has been used in espionage campaigns against municipal governments, embassies, militaries and other industrial targets, primarily in the Middle East and Europe. In August, another component to these stealthy attacks called Epic Turla was disclosed; Epic is a multistage attack in which victims are compromised via spearphishing emails and other social engineering scams, or watering hole attacks.

The Epic Turla campaigns combined commodity exploits with zero-day attacks against Windows XP and Windows Server 2003 machines, as well as an Adobe Reader zero day.

The Epic Turla campaigns combined commodity exploits with zero-day attacks against Windows XP and Windows Server 2003 machines, as well as an Adobe Reader zero day have been used to elevate an attacker’s privileges on the underlying system.

More than 100 websites were reported to be infected in Epic Turla attacks, including the website for City Hall in Pinor, Spain, an entrepreneurial site in Romania and the Palestinian Authority Ministry of Foreign Affairs.

All of the sites were built using the TYPO3 content management system, indicating the attackers had access to a vulnerability on that platform.

Once compromised, the websites then loaded remote JavaScript that performs a number of tasks, including dropping exploits for flaws in Internet Explorer 6-8, recent Java or Flash bugs, or a phony Microsoft Security Essentials application signed with a legitimate certificate from Sysprint AG.

Kaspersky’s Raiu and Baumgartner said most of the code in the Linux version of Turla comes from public sources. The backdoor, for example, is based on cd00r, Baumgartner and Raiu wrote. It includes an ELF

executable that is statically linked against the GNU C library, an older version of OpenSSL and libpcap, the tcpdump network capture library.

The use of the cd00r backdoor enables the attack to go undetected, researchers said, because it does not require elevated privileges while running remote commands.

“It can’t be discovered via netstat, a commonly used administrative tool. It uses techniques that don’t require root access, which allows it to be more freely run on more victim hosts,” the researchers wrote. “Even if a regular user with limited privileges launches it, it can continue to intercept incoming packets and run incoming commands on the system.”

Turla was uncovered early this year and researchers also found a connection to the Agent.btz worm which infected U.S. military networks and led to a government mandate banning the use of USB drives. While Agent.btz and Turla share characteristics, no one has linked the authors. Turla uses the same XOR key and log file names as Agent.btz, for example. Kaspersky’s Baumgartner and Raiu said that Linux variants were known to exist, but this is the first sample caught in the wild.

“Some of the malicious code appears to be inactive, perhaps leftovers from older versions of the implant,” the said. “Perhaps the most interesting part here is the unusual command and control mechanism based on TCP/UDP packets, as well as the C&C hostname which fits previously known Turla activity.”
