The Garden of Forking Paths: Sophisticated APTs diversify toolsets

By Kaspersky

Published: 2019-10-16 · Archived: 2026-04-05 18:41:01 UTC

Advanced persistent threat (APT) activity in the third quarter of 2019 has indicated an increase in the usage and number of new and previously unknown malicious toolsets.

This is a sign of a consistent trend of the threat actor exodus into deeper waters, to evade detection. These and other APT trends across the world are covered in Kaspersky's latest quarterly threat intelligence summary.

A three-month APT trends summary for the last quarter came from Kaspersky's private threat intelligence research, as well as other sources that cover the major developments that researchers believe everyone should be aware of.

In Q3 2019, Kaspersky researchers observed a tendency of APT toolsets' diversification across the world. The most significant changes were performed by:

- Turla (aka Venomous Bear, Uroburos and Waterbug) has made significant changes to its toolset. While investigating malicious activity in Central Asia, Kaspersky identified a new backdoor that was attributed with some degree of confidence to this APT group. The malware, named "Tunnus" is a .NET-based backdoor with the ability to run commands or perform file actions on an infected system and send the results to its command-and-control servers. So far, the infrastructure has been built using compromised sites with vulnerable Wordpress installations. According to the company's telemetry, Tunnus activity started in March and remained active.
- Turla has also wrapped its famous JavaScript KopiLuwak malware in a new dropper called "Topinambour." This is a new .NET file that the group is using to distribute and drop its JavaScript KopiLuwak through infected installation packages for legitimate software programs such as VPNs. Some of the changes are to help Turla dodge detection. The two KopiLuwak analogues – the .NET "RocketMan" Trojan and the PowerShell "MiamiBeach Trojan" – are used for cyber-espionage. It is possible that a threat actor deploys these versions when their targets are protected with security software that is able to detect KopiLuwak. All three implants are able to fingerprint targets, gather information on system and network adapters, steal files, and download and execute additional malware.
- HoneyMyte (aka Temp.Hex and Mustang Panda), which has been active for several years, has adopted different techniques to perform its attacks over the past couple of years, and has focused on various targeting profiles. That campaign targeted government entities in Myanmar, Mongolia, Ethiopia, Vietnam and Bangladesh. The actor's attacks relied on a diversified number of tools: (a) PlugX implants; (b) a multi-stage package resembling the CobaltStrike stager and stageless droppers with PowerShell and VB scripts, .NET executables, cookie-stealers and more; (c) ARP poisoning with DNS hijacking malware, to

deliver poisoned Flash and Microsoft updates over http for lateral movement; (d) various system and network utilities. Based on the targeting of government organizations related to natural resource management in Myanmar and a major continental African organization, it is possible that one of the main motivations of HoneyMyte is gathering geo-political and economic intelligence.

- In August, Dragos published an overview of attacks called "Oil and Gas Threat Perspective Summary", which references an alleged new threat actor they call "Hexane". Dragos claims to have identified the group in May 2019, associating it with OilRig and CHRYSENE. Kaspersky analysis reveals some low-confidence similarities with OilRig based on TTPs, which is something that Dragos also mentions in its research.

"Just as we predicted last year, in seeking to evade detection, threat actors refresh their toolsets and go into deep waters. This quarter, we have seen this clearly in the developments by a number of APT actors and campaigns across the globe. This is a challenge for researchers – when a new campaign is observed, it's not always immediately clear whether the tools used are the result of an established threat actor revamping its tools, or a completely new threat actor making use of the tools developed by an existing APT group. Still, it highlighted the importance of investing in threat landscape intelligence. Knowledge is power, and you can only know where the danger might come from only informing yourself in advance," said Vicente Diaz, security researcher, Global Research and Analysis Team, Kaspersky.

The APT trends report for Q3 summarizes the findings of Kaspersky's subscriber-only threat intelligence reports, which also include Indicators of Compromise (IOC) data and YARA rules to assist in forensics and malware-hunting. For more information, please contact: intelreports@kaspersky.com

In order to avoid falling victim to a targeted attack by a known or unknown threat actor, Kaspersky researchers recommend implementing the following measures:

- Provide your Security Operations Center (SOC) team with access to the latest threat intelligence, to keep up to date with the new and emerging tools, techniques and tactics used by threat actors and cybercriminals.
- For endpoint level detection, investigation and timely remediation of incidents, implement EDR solutions such as Kaspersky Endpoint Detection and Response.
- In addition to adopting essential endpoint protection, implement a corporate-grade security solution that detects advanced threats on the network level at an early stage, such as Kaspersky Anti Targeted Attack Platform.

Read the full APT Q3 2019 trends report on Securelist.
