SideWinder Hackers Launched Over a 1,000 Cyber Attacks Over the Past 2 Years

By The Hacker News

Published: 2022-05-31 · Archived: 2026-04-05 15:29:03 UTC

An "aggressive" advanced persistent threat (APT) group known as **SideWinder** has been linked to over 1,000 new attacks since April 2020.

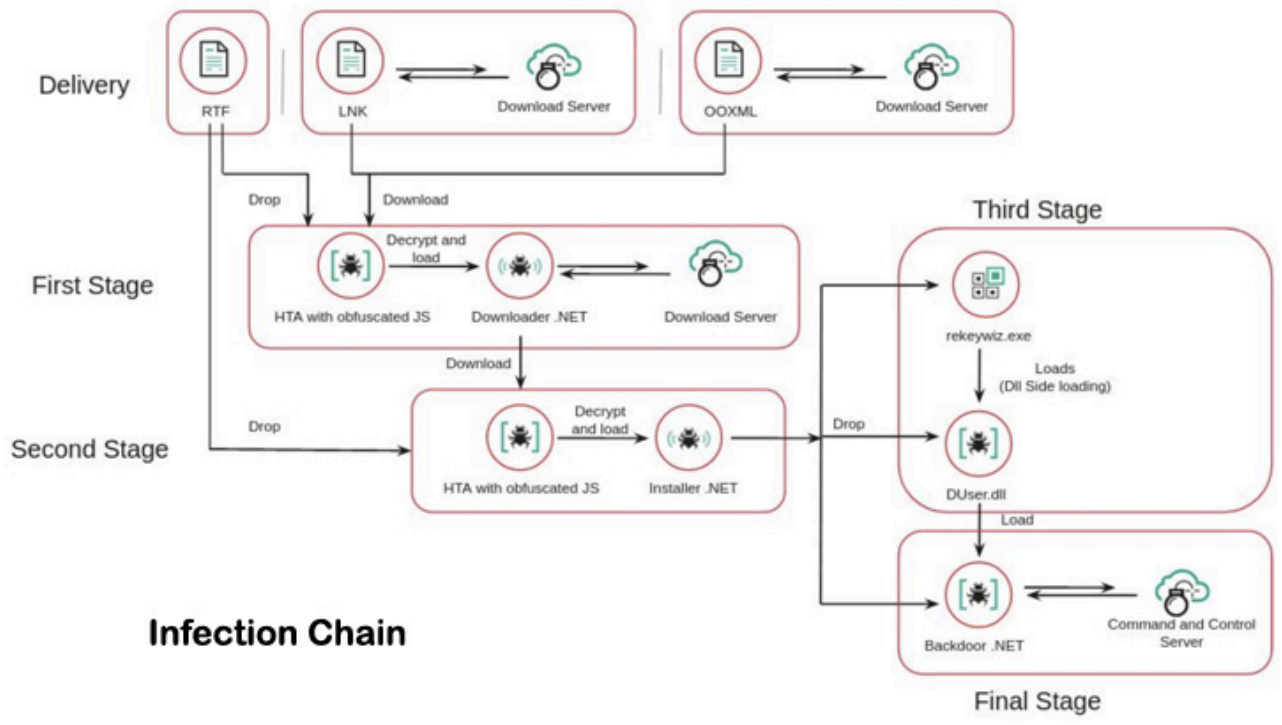
"Some of the main characteristics of this threat actor that make it stand out among the others, are the sheer number, high frequency and persistence of their attacks and the large collection of encrypted and obfuscated malicious components used in their operations," cybersecurity firm Kaspersky said in a report that was presented at Black Hat Asia this month.

SideWinder, also called Rattlesnake or T-APT-04, is said to have been active since at least 2012 with a track record of targeting military, defense, aviation, IT companies, and legal firms in Central Asian countries such as Afghanistan, Bangladesh, Nepal, and Pakistan.

Kaspersky's APT trends report for Q1 2022 published late last month revealed that the threat actor is actively expanding the geography of its targets beyond its traditional victim profile to other countries and regions,

including Singapore.

SideWinder has also been observed capitalizing on the ongoing Russo-Ukrainian war as a lure in its phishing campaigns to distribute malware and steal sensitive information.



The adversarial collective's infection chains are notable for incorporating malware-rigged documents that take advantage of a remote code vulnerability in the Equation Editor component of Microsoft Office (CVE-2017-11882) to deploy malicious payloads on compromised systems.

Furthermore, SideWinder's toolset employs several sophisticated obfuscation routines, encryption with unique keys for each malicious file, multi-layer malware, and splitting command-and-control (C2) infrastructure strings into different malware components.

The three-stage infection sequence commences with the rogue documents dropping a HTML Application (HTA) payload, which subsequently loads a .NET-based module to install a second-stage HTA component that's designed to deploy a .NET-based installer.

This installer, in the next phase, is both responsible for establishing persistence on the host and loading the final backdoor in memory. The implant, for its part, is capable of harvesting files of interest as well as system information, among others.

No fewer than 400 domains and subdomains have been put to use by the threat actor over the past two years. To add an additional layer of stealth, the URLs used for C2 domains are sliced into two parts, the first portion of

which is included in the .NET installer and the latter half is encrypted inside the second stage HTA module.

"This threat actor has a relatively high level of sophistication using various infection vectors and advanced attack techniques," Noushin Shabab of Kaspersky said, urging that organizations use up-to-date versions of Microsoft Office to mitigate such attacks.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
