Microsoft Exchange servers hacked by new ToddyCat APT gang

By Sergiu Gatlan

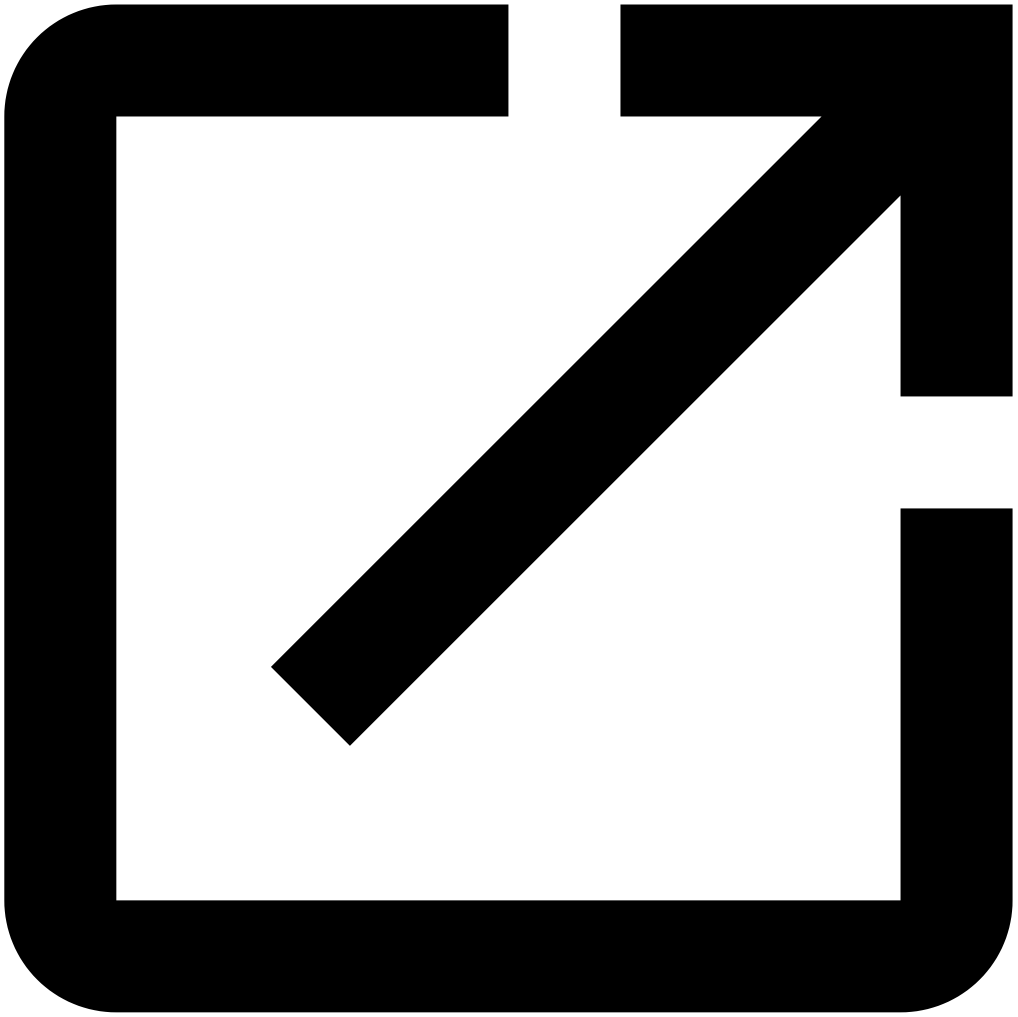
Published: 2022-06-21 · Archived: 2026-04-05 13:26:23 UTC

An advanced persistent threat (APT) group dubbed ToddyCat has been targeting Microsoft Exchange servers throughout Asia and Europe for more than a year, since at least December 2020.

While tracking the group's activity, security researchers with Kaspersky's Global Research & Analysis Team (GReAT) have also found a previously unknown passive backdoor they named Samurai and new trojan malware dubbed Ninja Trojan.

Both malware strains allow the attackers to take control of infected systems and move laterally within the victims' networks.

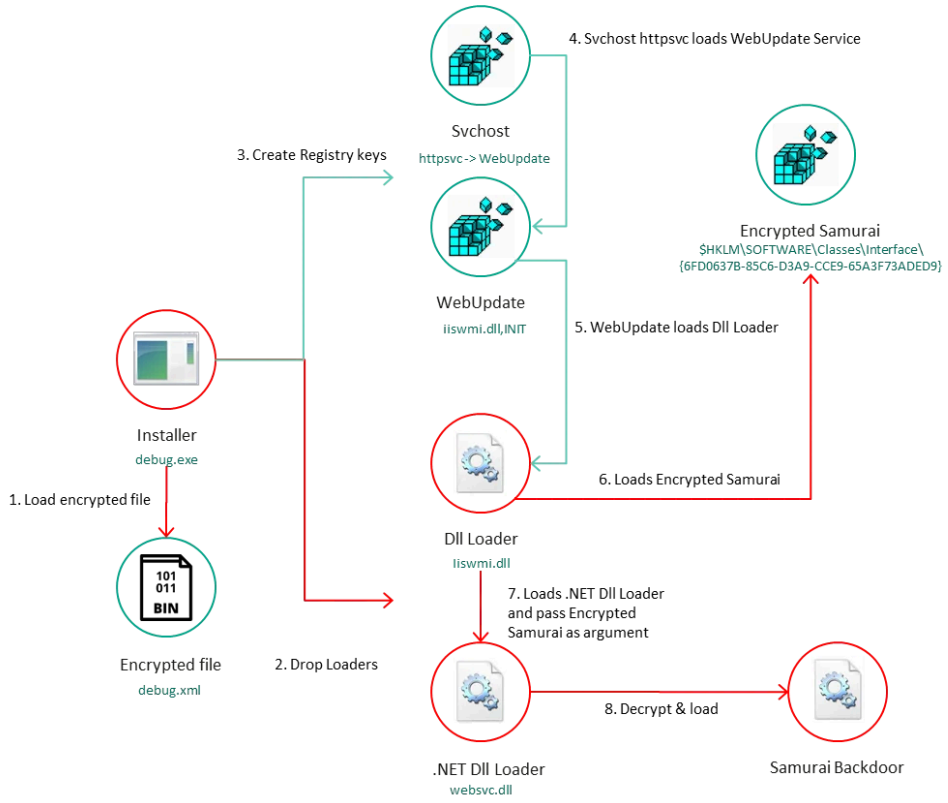

DIE LINKE.
0:00



ToddyCat's attacks have also been spotted in the past by Slovak cybersecurity firm ESET, who has been tracking them as a cluster of activity they dubbed Websiic starting with March 2021.

At the time, the hacking group exploited the ProxyLogon Exchange flaws that allowed them to gain remote code execution on vulnerable servers to deploy China Chopper web shells.

Although not very active until February 2021, they quickly escalated their attacks after starting to scan for and target unpatched Microsoft Exchange servers across Europe and Asia with ProxyLogon exploits.



ToddyCat attack flow (Kaspersky)

Waves of attacks against Exchange servers and desktop systems

"We suspect that this group started exploiting the Microsoft Exchange vulnerability in December 2020, but unfortunately, we don't have sufficient information to confirm the hypothesis," Kaspersky security researcher Giampaolo Dedola said.

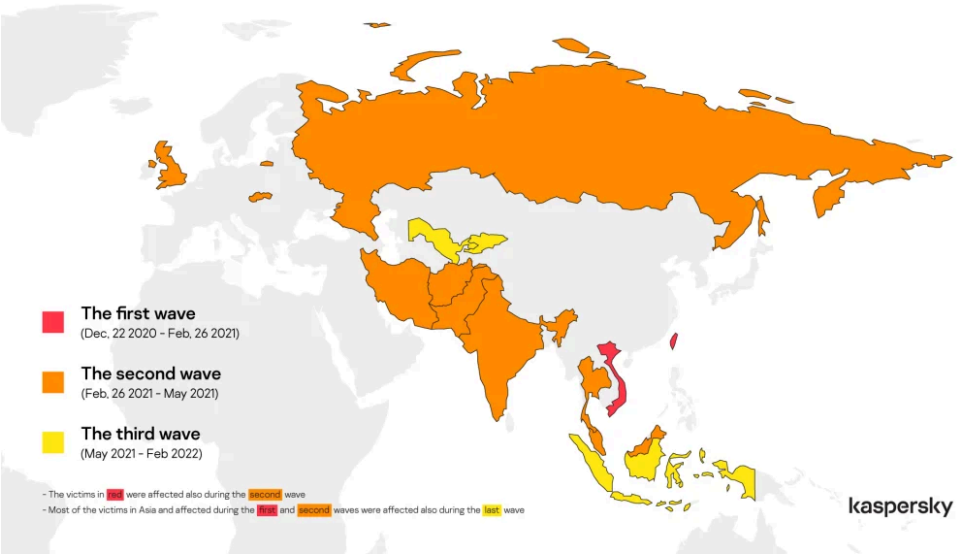
"In any case, it's worth noting that all the targeted machines infected between December and February were Microsoft Windows Exchange servers; the attackers compromised the servers with an unknown exploit, with the rest of the attack chain the same as that used in March."

The group's favorite targets are high-profile organizations, including government and military entities, as well as military contractors.

While the first attacks wave of attacks (between December 2020 and February 2021) only targeted a small number of government organizations in Vietnam and Taiwan, the next wave (between February 2021 and May 2021) quickly expanded to entities from a long list of countries worldwide, including Russia, India, Iran, and the United Kingdom.

In the next phase (until February 2022), ToddyCat targeted the same cluster of countries but also added organizations from Indonesia, Uzbekistan, and Kyrgyzstan to the list.

In this third wave of attacks, the APT group also expanded their focus to include desktop systems, while before, they were exclusively targeting Microsoft Exchange servers.



ToddyCat attack waves (Kaspersky)

Activity overlap with some Chinese-speaking APTs

Kaspersky says ToddyCat's victims are linked to industry sectors and countries also targeted by multiple Chinese-speaking groups.

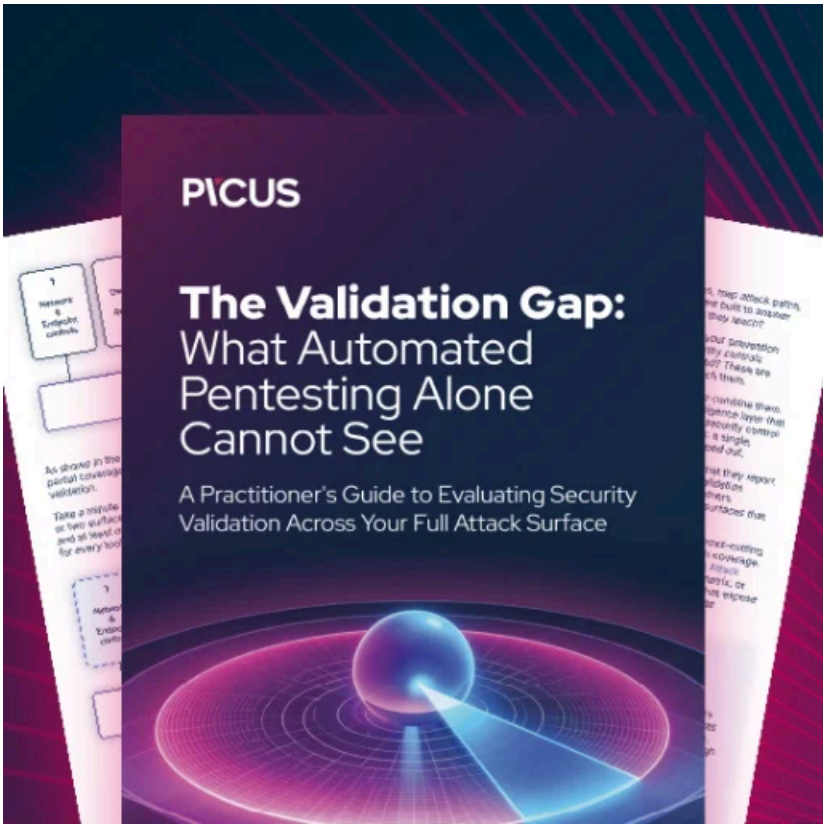
However, some of the entities they breached (in three different countries) were also hacked around the same time by Chinese-backed hackers using the FunnyDream backdoor.

"Despite the overlap, we do not feel confident merging ToddyCat with the FunnyDream cluster at the moment. Considering the high-profile nature of all the victims we discovered, it is likely they were of interest to several APT groups," Dedola added.

"Moreover, despite the occasional proximity in staging locations, we have no concrete evidence of the two malware families directly interacting (for instance, one deploying the other), and the specific directories are frequently used by multiple attackers.

"The affected organizations, both governmental and military, show that this group is focused on very high-profile targets and is probably used to achieve critical goals, likely related to geopolitical interests."

Additional technical details on the malware used by and indicators of compromise (IOCs) linked to ToddyCat can be found in Kaspersky's report.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/new-toddycat-apt-group-targets-exchange-servers-in-asia-europe/