ESET APT Activity Report Q4 2024-Q1 2025: Malware sharing, data wiping and exploits

By ESET Research

Podcasts

ESET experts discuss Sandworm’s new data wiper, relentless campaigns by UnsolicitedBooker, attribution challenges amid tool-sharing, and other key findings from the latest APT Activity Report

01 Jul 2025 • , 2 min. read

In the latest episode of the *ESET Research Podcast*, ESET Distinguished Researcher Aryeh Goretsky is joined by ESET Security Awareness Specialist Rene Holt to dissect the key findings from ESET’s APT Activity Report.

The first actor that steps into the limelight is UnsolicitedBooker, a China-aligned APT group that has demonstrated a level of persistence that truly puts the "P" in APT. This group targeted the same organization three times over several years, attempting to deploy its signature backdoor, MarsSnake. This example highlights the relentless focus of certain groups that will stop at nothing to achieve their objectives.

The conversation then shifts to the challenges of attribution, particularly with the increasing trend of tool-sharing, primarily among China-aligned actors such as Worok. Their tactic is to muddy the waters by using overlapping

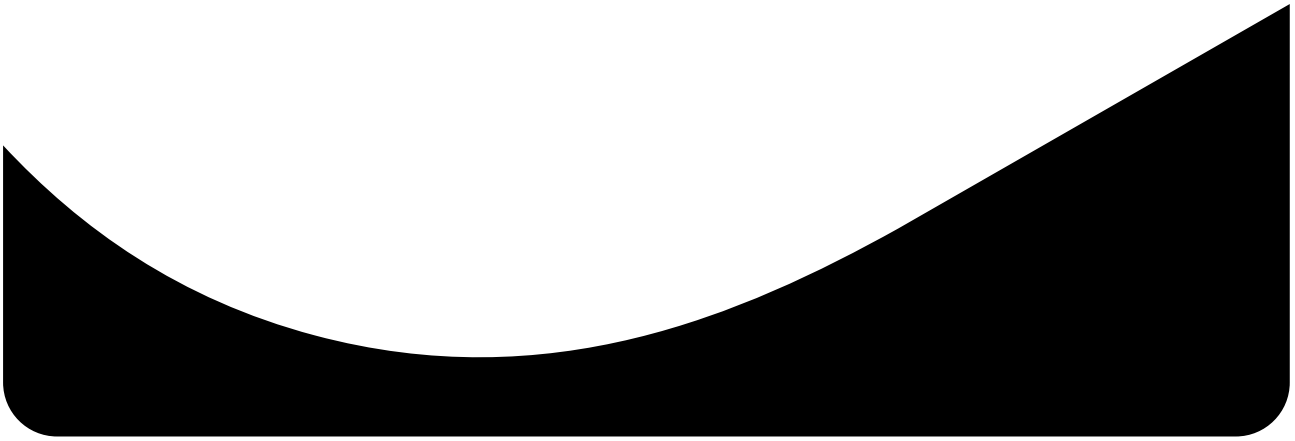
toolsets sourced from digital quartermasters, intertwining their activities with those of other groups such as LuckyMouse and TA428.

Turning to Russia-aligned actors, the discussion focuses on groups like Sednit, Gamaredon, and Sandworm. Sednit's latest activity revolves around Operation RoundPress, which originally targeted the popular webmail service Roundcube but has recently expanded to other platforms such as Horde, MDaemon, and Zimbra. Sednit has been using targeted emails, exploiting flaws in these services, and employing cross-site scripting to attack defense companies located in Bulgaria and Ukraine.

Gamaredon remains one of the most active APTs in Ukraine, constantly tweaking its obfuscation techniques to stay ahead of detection. Meanwhile, Sandworm has intensified its use of data-wiping malware, deploying a new wiper called ZEROLOT multiple times in the past six months. This wiper operates with surgical precision, erasing specific files and directories without immediately taking down the entire system—an approach that ensures the malware can complete its destructive mission.

Aryeh and Rene also delve into the activities of North Korea-aligned and Iran-aligned groups. If you're interested in more details, be sure to listen to this episode of the ESET Research Podcast or download the latest ESET APT Activity Report.

> *Discussed topics:*
>
> *UnsolicitedBooker (MarsSnake) 1:45*
>
> *Worok (and its digital quartermasters) 4:50*
>
> *Sednit (Operation RoundCube) 9:55*
>
> *Gamaredon 13:55*
>
> *Sandworm (ZEROLOT wiper) 16:15*
>
> *DeceptiveDevelopment (WeaselStore, ClickFix) 24:10*
>
> *MuddyWater vs Lyceum 29:40*



Source: https://www.welivesecurity.com/en/podcasts/eset-apt-activity-report-q4-2024q1-2025-malware-sharing-wipers-exploits/