Cyberespionage the Gamaredon way: Analysis of toolset used to spy on Ukraine in 2022 and 2023

welivesecurity.com/en/eset-research/cyberespionage-gamaredon-way-analysis-toolset-used-spy-ukraine-2022-2023/

ESET RESEARCH

ESET Research has conducted a comprehensive technical analysis of Gamaredon's toolset used to conduct its cyberespionage activities focused in Ukraine

Zoltán Rusnák

26 Sep 2024 , 5 min. read

The war in Ukraine, which started in February 2014 and intensified with Russia's invasion of the country on February 24th, 2022, exemplifies a multifaceted war, rife with disinformation campaigns and cyberwarfare. Throughout these years, ESET Research has revealed several high-profile cyberattacks conducted by Russia-aligned advanced persistent threat (APT) groups targeting Ukrainian entities and Ukrainian speakers, analyzed various operations, and kept track of multiple APT groups focusing on this region because of the war.

In this research, we decided to examine the operations of Gamaredon, the Russia-aligned group that has been active since at least 2013 and is currently the most engaged APT group in Ukraine. The intensity of the physical conflict has noticeably increased since 2022, but it's worth noting that the level of activity from Gamaredon has remained consistent – the group has been methodically deploying its malicious tools against its targets since well before the invasion began.

We have analyzed thousands of samples while conducting a comprehensive technical analysis of Gamaredon's toolset used to conduct its cyberespionage activities in 2022 and 2023; we reveal the results of our analysis in our white paper, which you can read in full here:

Cyberespionage the Gamaredon way: Analysis of toolset used to spy on Ukraine in 2022 and 2023

Read full report

In the white paper, we share details about Gamaredon's ever-changing obfuscation tricks and numerous techniques used for bypassing domain-based blocking. These tactics pose a significant challenge to tracking efforts, as they make it harder for systems to automatically detect and block the group's tools. Nevertheless, during our research, we managed to identify and understand these tactics, and keep track of Gamaredon's activities. We also describe the tools that are most prevalent or interesting in some other way in order to shed more light on the relationships that exist among the tools and to help create a bigger picture of the tools' ecosystem.

Victimology and group background

Gamaredon has been attributed by the Security Service of Ukraine (SSU) to the 18th Center of Information Security of the FSB, operating out of occupied Crimea. We believe this group to be collaborating with another threat actor that we discovered and named InvisiMole.

As evidenced over time by ESET telemetry, in several reports from CERT-UA, and from other official Ukrainian bodies, the majority of Gamaredon's attacks are directed against Ukrainian governmental institutions. To our surprise, in April 2022 and February 2023, we saw a few attempts to compromise targets in several NATO countries, namely Bulgaria, Latvia, Lithuania, and Poland, but no successful breaches were observed.

Between November 1st, 2022 and December 31st 2023, we observed more than a thousand unique machines in Ukraine that were attacked by Gamaredon. The seven-day moving average of daily additions is visualized in Figure 1.

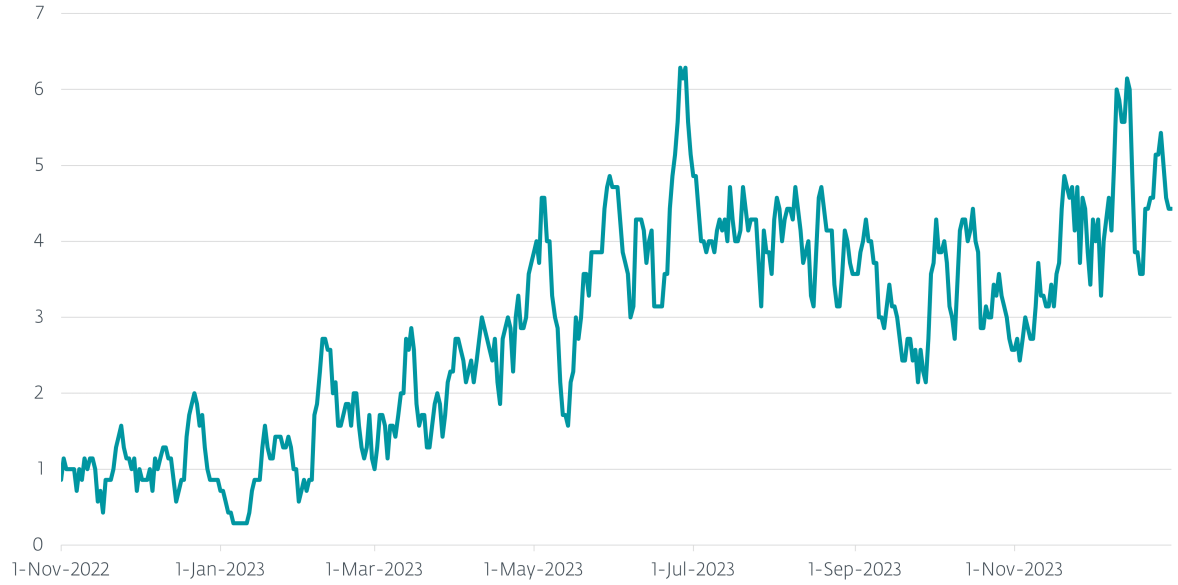

Figure 1. Seven-day moving average of unique machines attacked in Ukraine

Noisy and reckless, but still dangerous

To compromise new victims, Gamaredon conducts spearphishing campaigns and then uses its custom malware to weaponize Word documents and USB drives accessible to the initial victim and that are expected to be shared with further potential victims.

According to our long-term observations, Gamaredon, unlike most APT groups, does not try to be stealthy and remain hidden as long as possible by using novel techniques when conducting cyberespionage operations, but rather the operators are reckless and do not mind being discovered by defenders during their operations. Even though they do not care so much about being noisy, they apparently put in a lot of effort to avoid being blocked by security products and try very hard to maintain access to compromised systems.

Typically, Gamaredon attempts to preserve its access by deploying multiple simple downloaders or backdoors simultaneously. The lack of sophistication of Gamaredon tools is compensated by frequent updates and use of regularly changing obfuscation.

A shift towards VBScript and PowerShell

Gamaredon's toolset has undergone several changes over time. In 2022, the group slowly started to shift toward the use of VBScript and PowerShell in tandem, and Gamaredon almost completely ditched the use of SFX archives, which had been its primary tactic previously. During 2023, Gamaredon notably improved its cyberespionage capabilities and

developed several new tools in PowerShell, with the focus on stealing valuable data, for example from web applications running inside internet browsers, email clients, and instant messaging applications such as Signal and Telegram.

However, PteroBleed, an infostealer we discovered in August 2023, also focuses on stealing data related to a Ukrainian military system and from a webmail service used by a Ukrainian governmental institution. The timeline of new tools released in 2022 and 2023 is shown in Figure 2; except for PteroScreen, all of them were discovered by ESET Research.

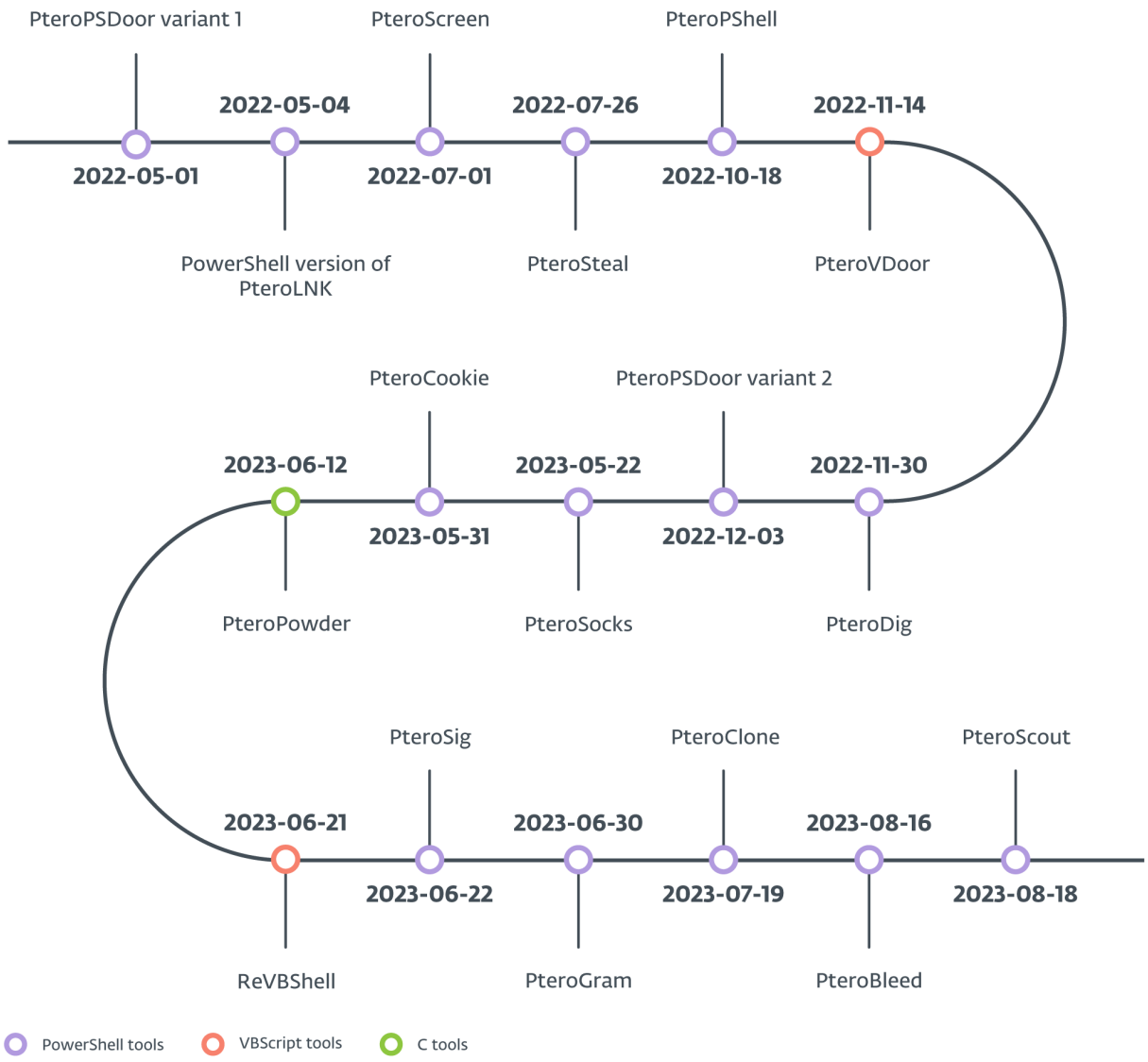

Figure 2. Timeline of new tools added to Gamaredon's arsenal

In general, we can categorize Gamaredon's toolset into downloaders, droppers, weaponizers, stealers, backdoors, and ad hoc tools. The group uses a combination of general-purpose and dedicated downloaders to deliver payloads. Droppers are used to deliver various VBScript payloads; weaponizers alter properties of existing files or create new files on connected USB drives, and stealers exfiltrate specific files from the file system.

Additionally, backdoors serve as remote shells, and ad hoc tools perform specific functions, like a reverse SOCKS proxy or payload delivery using the legitimate command line program rclone.

Fast switching of C&C IP addresses and domains

Our analysis also sheds light on the group's network infrastructure. Gamaredon uses a technique known as fast flux DNS – frequently changing its command and control (C&C) servers' IP addresses, usually several times per day, to avoid IP-based blocking. The group also frequently registers and updates many new C&C domains to avoid domain-based blocking, mainly using .ru as the top-level domain (TLD).

Gamaredon has also demonstrated resourcefulness by employing various techniques to evade network-based detections, leveraging third-party services such as Telegram, Cloudflare, and ngrok.

Despite the relative simplicity of its tools, Gamaredon's aggressive approach and persistence make it a significant threat. Given the ongoing war in the region, we expect Gamaredon to continue in its focus on Ukraine.

For a more detailed analysis and technical breakdown of Gamaredon's tools and activities, you can access the full ESET Research white paper here.

A comprehensive list of indicators of compromise (IoCs) can be found in our GitHub repository and the Gamaredon white paper.

Let us keep you up to date

Sign up for our newsletters