Espionage campaign linked to Russian intelligence services

13.04.2023

The Military Counterintelligence Service and the CERT Polska team (CERT.PL) observed a widespread espionage campaign **linked to Russian intelligence services**, aimed at collecting information from foreign ministries and diplomatic entities. Most of the identified targets of the campaign are located in NATO member states, the European Union and, to a lesser extent, in Africa.

Many elements of the observed campaign – the infrastructure, the techniques used and the tools - overlap, in part or in full, with activity described in the past, referred to by Microsoft as “NOBELIUM” and by Mandiant as “APT29”. The actor behind them has been linked to, among other things, a campaign called “SOLARWINDS”[1] and the tools “SUNBURST”, “ENVYSCOUT”[2, 3,] and “BOOMBOX”[4], as well as numerous other espionage campaigns[5].

The activities described here differ from the previous ones in the use of software unique to this campaign and not previously described publicly. New tools[6] were used at the same time and independently of each other, or replacing those whose effectiveness had declined, allowing the actor to maintain continues, high operational tempo.

At the time of publication of the report, the campaign is still ongoing and in development. The Military Counterintelligence Service and CERT.PL recommend all entities which may be in the area of interest of the actor to implement mechanisms aimed at improving the security of IT Security systems in use and increasing the detection of attacks. Examples of configuration changes and detection mechanisms are proposed in the recommendations.

The aim of publishing the advisory is to disrupt the ongoing espionage campaign, impose additional cost of operations against allied nations and enable the detection, analysis and tracking of the activity by affected parties and the wider cyber security industry.

The course of the observed campaigns

In all observed cases, the actor utilised spear phishing techniques. Emails impersonating embassies of European countries were sent to selected personnel at diplomatic posts. The correspondence contained an invitation to a meeting or to work together on documents. In the body of the message or in an attached PDF document, a link was included purportedly directing to the ambassador's calendar, meeting details or a downloadable file.

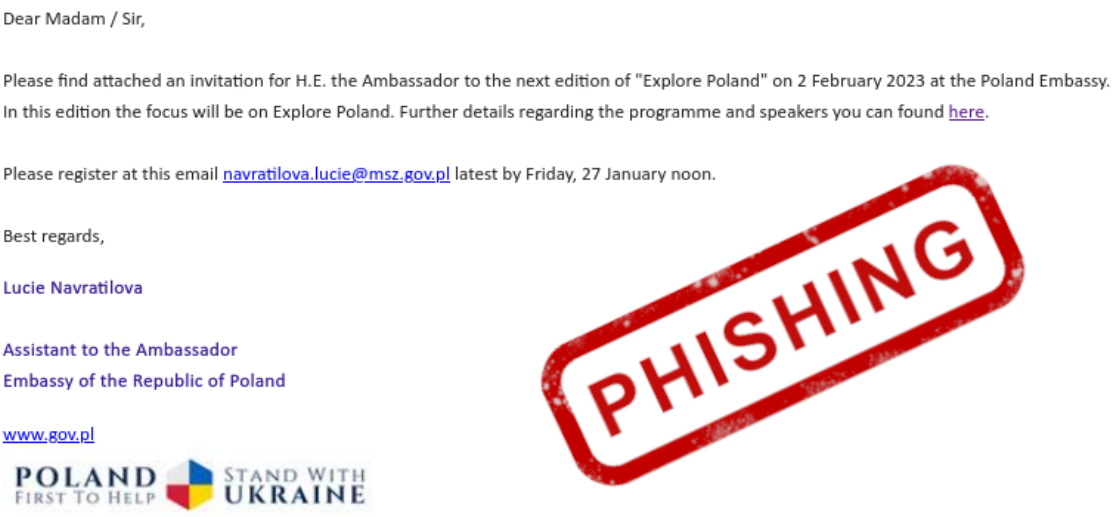

Figure 1. Example of an email impersonating the Polish embassy and urging the addressee to click on a malicious link.

The link directed to a compromised website that contained the actor's signature script, publicly referred to as “ENVYSCOUT”. It utilises the HTML Smuggling technique – whereby a malicious file placed on the page is decoded using JavaScript when the page is opened and then downloaded on the victim's device. This makes the malicious file

more difficult to detect on the server side where it is stored. The web page also displayed an information intended to reassure the victim that they had downloaded the correct attachment.

In the course of the described campaign, three different versions of the ENVYSCOUT tool were observed, progressively adding new mechanisms to hinder analysis.

Figure 2. A website impersonating the Polish embassy suggesting a downloadable calendar

Campaigns observed in the past linked to “NOBELIUM” and “APT29” used .ZIP or .ISO files to deliver the malware. During the campaign described above, .IMG files were also used in addition to the aforementioned file formats. ISO and IMG disk images, on Windows computers, are automatically mounted in the file system when opened, which causes their contents to be displayed in Windows Explorer. In addition, they do not carry the so-called *mark-of-the-web*, i.e. the user will not be warned that the files were downloaded from the Internet.
The actor used various techniques to get the user to launch the malware. One of them was a Windows shortcut (LNK) file pretending to be a document but actually running a hidden DLL library with the actor's tools. The *DLL Sideloading* technique was also observed, using a signed executable file to load and execute code contained in a hidden DLL library by placing it in the same directory, under a name chosen according to the entries in the import table. At a later stage of the campaign, the name of the executable file contained many spaces to make the exe extension difficult to spot.

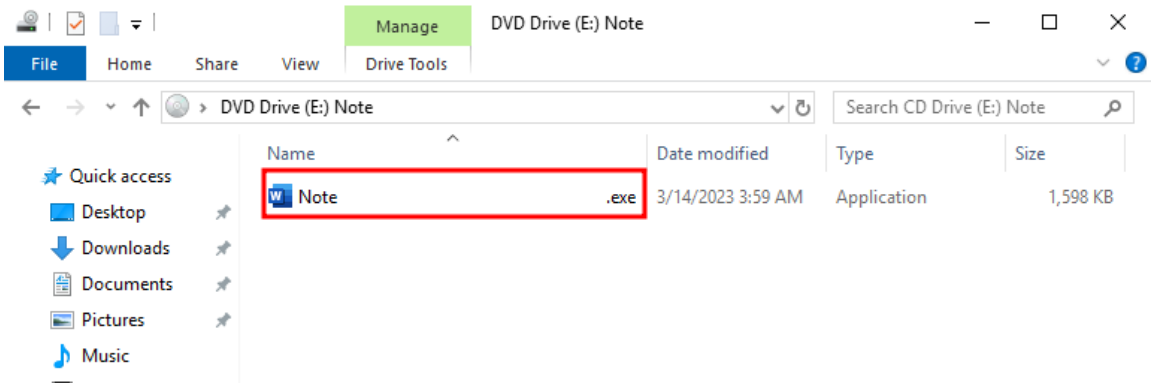

Figure 3. View after the victim starts-up an image file with the default Windows Explorer settings.

Tools used during the campaign

The actor used various tools at different stages of the described campaign. All those listed below are unique to the set of activities described. A detailed technical analysis of each is included in separate documents:

1. SNOWYAMBER – a tool first used in October 2022, abusing the Notion[7] service to communicate and download further malicious files. Two versions of this tool have been observed.
2. HALFRIG – used for the first time in February 2023. This tool is distinguished from the others by the embedded code that runs the COBALT STRIKE tool.
3. QUARTERRIG – a tool first used in March 2023, sharing part of the code with HALFRIG. Two versions of this tool were observed.

The first version of the SNOWYAMBER tool was publicly described by Recorded Future, among others[8]. **A modified version of the SNOWYAMBER tool, the HALFRIG tool and the QUATERRIG tool have not previously been described publicly.**

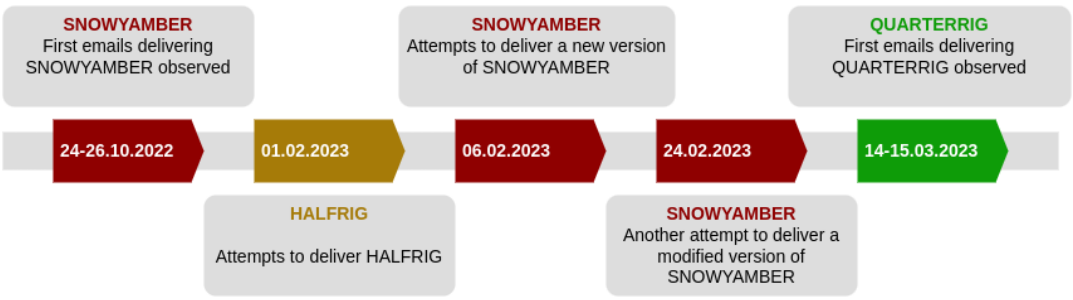

Figure 4. Timeline illustrating the observed actions of the actor

The SNOWYAMBER and QUARTERRIG tools were used as so-called downloaders. Both tools sent the IP address as well as the computer and user name to the actor. They were used to assess whether the victim was of interest to the actor and whether it was a malware analysis environment. If the infected workstation passed manual verification, the aforementioned downloaders were used to deliver and start-up the commercial tools COBALT STRIKE or BRUTE RATEL. HALFRIG, on the other hand, works as a so-called loader – it contains the COBALT STRIKE payload and runs it automatically.

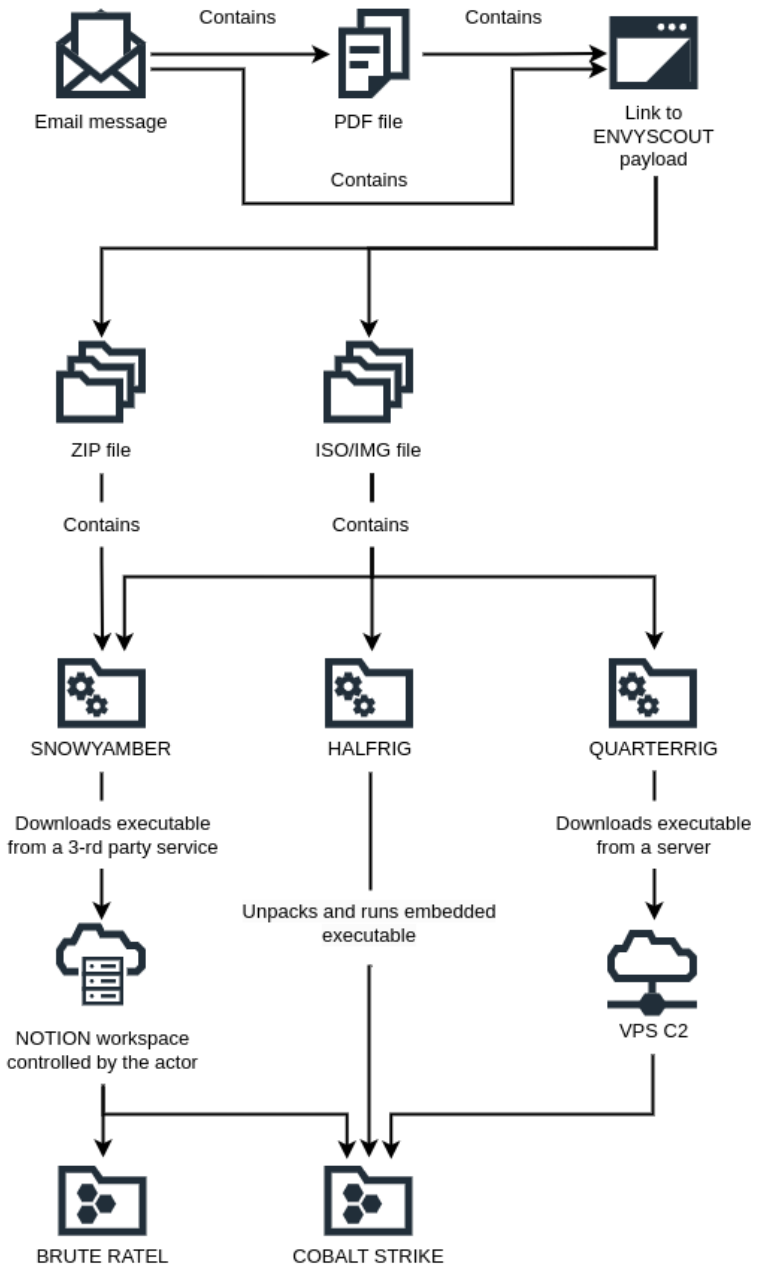

Figure 5. Illustration of the actor's tool delivery course

Despite the observed changes in tools, many of the elements of the campaign are repeatable. These include:

1. The way the infrastructure is built. The actor behind the espionage campaign prefers to use vulnerable websites belonging to random entities.
2. Email theme. All acquired emails used in the campaigns used the theme of correspondence between diplomatic entities.
3. The use of a tool publicly referred to as ENVYSCOUT. This script has been used by the actor since at least 2021[9]. Modifications to the tool's code were observed during the campaign, but they did not significantly affect its functionality.
4. A link to the ENVYSCOUT tool was provided to the victim in the form of a link embedded in the body of the email or in the body of an attached PDF file.
5. Use of ISO and IMG disc images.
6. Use of a technique called “DLL Sideloading” that uses a non-malicious, digitally signed executable file to start-up the actor’s tools.
7. Use of commercial tools COBALT STRIKE and BRUTE RATEL.

Recommendations

The Military Counterintelligence Service and CERT.PL **strongly** recommend that all entities that may be in the actor's area of interest implement configuration changes to disrupt the delivery mechanism that was used in the described campaign. Sectors that should **particularly** consider implementing the recommendations are:

1. Government entities;
2. Diplomatic entities, foreign ministries, embassies, diplomatic staff and those working in international entities;
3. International organisations;
4. Non-Governmental organisations.

The following configuration changes can be used to disrupt the malware delivery mechanism used in the described campaign:

1. Blocking the ability to mount disk images on the file system. Most users doing office work have no need to download and use ISO or IMG files.
2. Monitoring of the mounting of disk image files by users with administrator roles.
3. Enabling and configuring *Attack Surface Reduction Rules*[10].
4. Configuring Software Restriction Policy and blocking the possibility of starting-up executable files from unusual locations (in particular: temporary directories, %localappdata% and subdirectories, external media[11]).

We also include a collection of all observed indicators of compromise (IoCs) related to the campaign described, and we recommend to verify the system and network logs collected for their occurrence.

Attachments

---

[1] https://www.mandiant.com/resources/blog/unc2452-merged-into-apt29

[2] https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/, https://www.microsoft.com/en-us/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

[3] https://www.mandiant.com/resources/blog/tracking-apt29-phishing-campaigns

[4] Terminology taken from the Microsoft MSTIC team's publicly available analysis: https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/.

[5] https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF, https://www.ncsc.gov.uk/files/Advisory%20Further%20TTPs%20associated%20with%20SVR%20cyber%20actors.pdf, https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services, https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

[6] The term “tools” is used in a broad sense and includes file delivery scripts, “loader”, “stager” and “dropper” software

[7] https://www.notion.so/

[8] https://go.recordedfuture.com/hubfs/reports/cta-2023-0127.pdf

[9] https://microsoft.com/en-us/security/blog/2021/05/28/breaking-down-nobeliums-latest-early-stage-toolset/

[10] https://docs.microsoft.com/windows/security/threat-protection/microsoft-defender-atp/attack-surface-reduction

[11] For example:
C:\Windows\Temp*.exe
C:\Windows\Temp**.exe
%USERPROFILE%\AppData\Local*.exe
%USERPROFILE%\AppData\Local**.exe
%USERPROFILE%\AppData\Roaming*.exe
%USERPROFILE%\AppData\Roaming**.exe