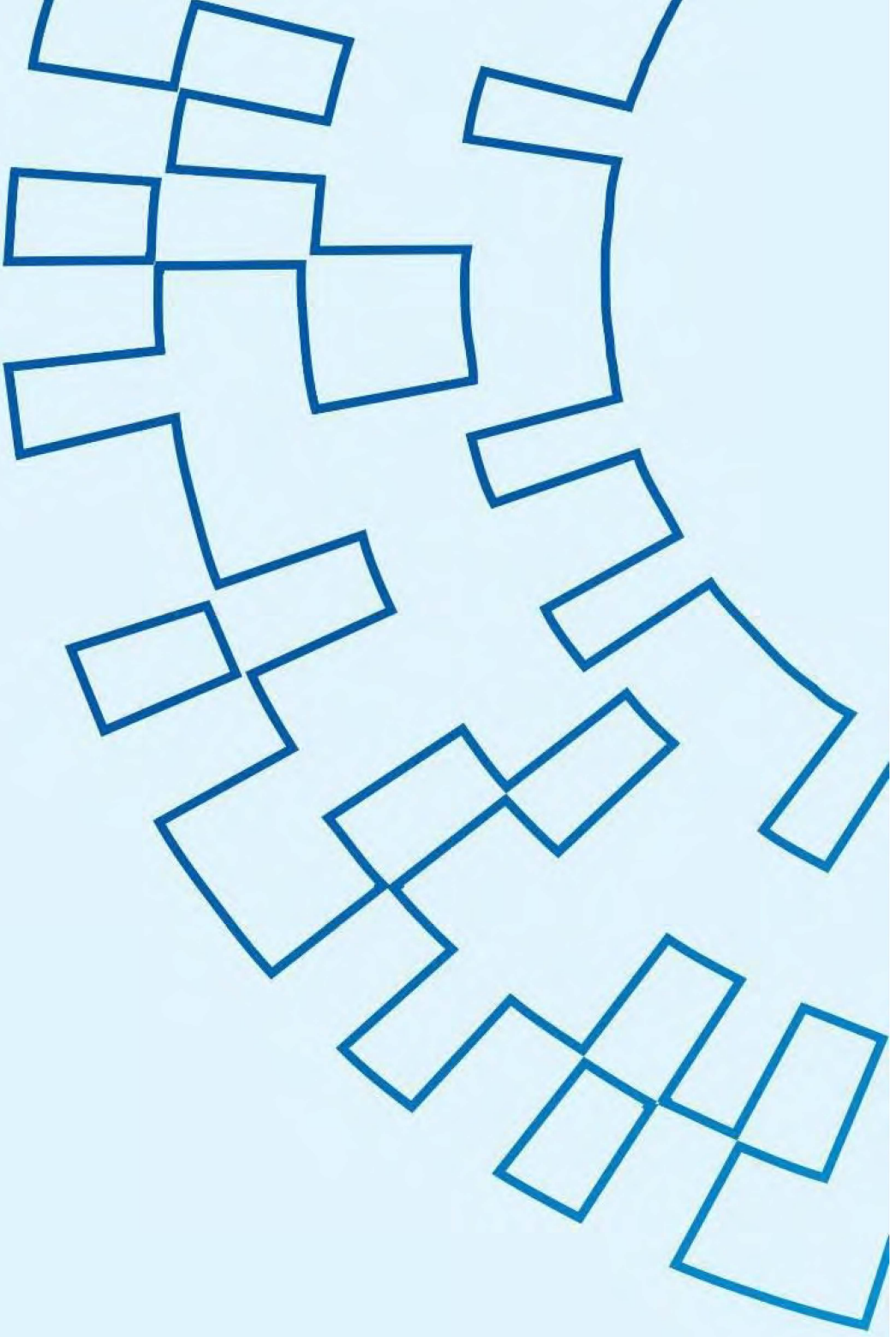
НКЦК

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ



APT29 ATTACKS EMBASSIES USING CVE-2023-38831

Executive Summary

In this report, we unveil a sophisticated cyberattack orchestrated by APT29, an advanced persistent threat group linked to Russia's Foreign Intelligence Service (SVR). The targets of this attack spanned multiple European nations, including Azerbaijan, Greece, Romania, and Italy, with the primary goal of infiltrating embassy entities. APT29 leveraged a newly discovered vulnerability in WinRAR, identified as CVE-2023-38831, to facilitate their intrusion.

This report delves into the intricate details of these cyber operations, shedding light on the attackers' tactics, techniques, and procedures. APT29 ingeniously employed benign-looking lures in the form of enticing BMW car sale photos and documents, expertly crafted to draw in unsuspecting victims. The lure documents contained hidden, malicious content that exploited the WinRAR vulnerability, granting attackers access to the compromised systems.

This campaign exemplifies the evolving nature of cyber threats and the persistent endeavors of nation-state-sponsored actors to compromise critical entities. The insights within this report aim to raise awareness about the complex threat landscape faced by diplomatic missions and organizations, ultimately fostering a proactive approach to cybersecurity defense.

Geopolitical Implications

At the outset of September 2023, the infamous APT29, affiliated with Russia's SVR, embarked on a sweeping cyber offensive that cast a wide net, targeting embassies, international organizations, and even internet service providers. Their primary focus rested on diplomatic accounts, with the Ministry of Foreign Affairs (MFA) in Azerbaijan and Italy bearing the brunt of the onslaught. Additionally, embassies situated in Greece and Romania, along with the email accounts of a prominent Greek ISP, Otenet, were also among the numerous targets. The list of victims extended to encompass major international organizations, emphasizing the audacity and scope of this campaign.

Figure.1 Map of countries with the most targeted accounts.

Domain	Organization
@gccsg.org	Secretariat General of the Gulf Cooperation Council
@ec.europa.eu	European Commission
@unhcr.org	United Nations High Commissioner for Refugees
@unicef.org	United Nations International Children's Emergency Fund
@auf.org	Agence universitaire de la Francophonie
@francophonie.org	Organisation Internationale de la Francophonie (OIF)
@iom.int	International Organization for Migration
@worldbank.org	The World Bank
@selec.org	Southeast European Law Enforcement Center
@coe.int	Council of Europe
@euro.who.int	World Health Organization European Region

Table.1 List of international organizations targeted in APT29 campaign.

The geopolitical implications are profound. Among the several conceivable motives, one of the most apparent aims of the SVR might be to gather intelligence concerning Azerbaijan's strategic activities, especially in the lead-up to the Azerbaijani invasion of Nagorno-Karabakh. It's noteworthy that the countries targeted—Azerbaijan, Greece, Romania, and Italy—maintain significant political and economic ties with Azerbaijan. In a noteworthy development, Azerbaijan had recently struck an agreement to procure military aircraft from Italy, marking a rare arms deal with a Western nation.

The attack methodology entailed the use of phishing emails equipped with enticing lures, portraying BMW car sales, which is a tactic previously employed by APT29 in attacks on embassies in Kyiv. This campaign, consisting of over 200 targeted email addresses, accentuates the evolving nature of cyber threats in the international arena.

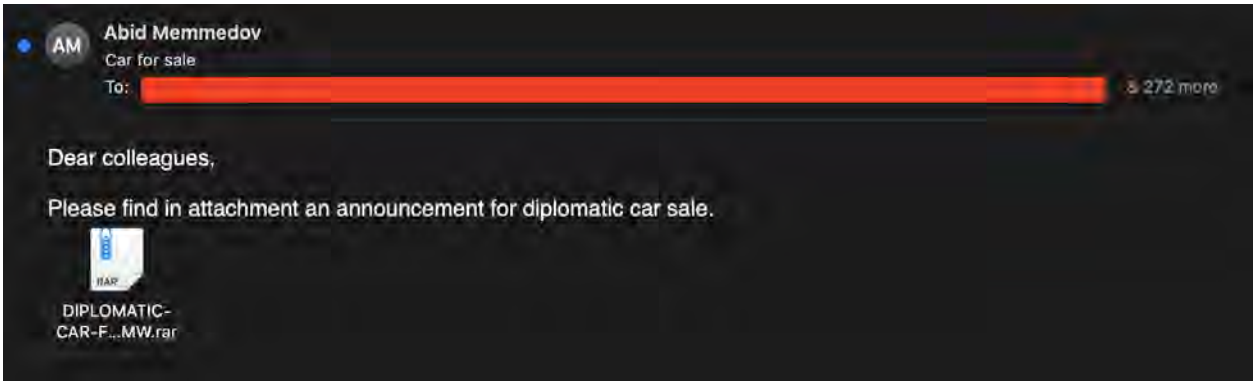


Figure.2 APT29 phishing email with BMW car for sale theme.

Old And New Tactics

APT29's persistence in using the BMW car for sale theme as a lure in their phishing attacks has taken on a new dimension with the deployment of a thematically named RAR archive, "DIPLOMATIC-CAR-FOR-SALE-BMW.rar." This archive contains a recently disclosed and exploitable vulnerability, CVE-2023-38831. This vulnerability, which came to light in April 2023, is rooted in the mishandling of ZIP archives that seemingly contain innocuous files, like standard .PDF documents, and folders sharing identical names.

The core issue lies in the archives, where threat actors can surreptitiously insert folders with matching names. When an unsuspecting user attempts to access one of the benign files, the ZIP archive may contain a similarly named folder concealing executable content, often hosting malware or other malicious code. In the course of the user's effort to open the harmless file, the system unwittingly processes the concealed malicious content within the folder with a matching name, thus enabling the execution of arbitrary code.

In the context of this particular attack, a script is executed, generating a PDF file featuring the lure theme of a BMW car for sale. Simultaneously, in the background, a PowerShell script is downloaded and executed from the next-stage payload server. Notably, the attackers introduced a novel technique for communicating with the malicious server, employing a Ngrok free static domain to access their server hosted on their Ngrok instance.

Figure.3 "DIPLOMATIC-CAR-FOR-SALE-BMW.pdf" lure document.

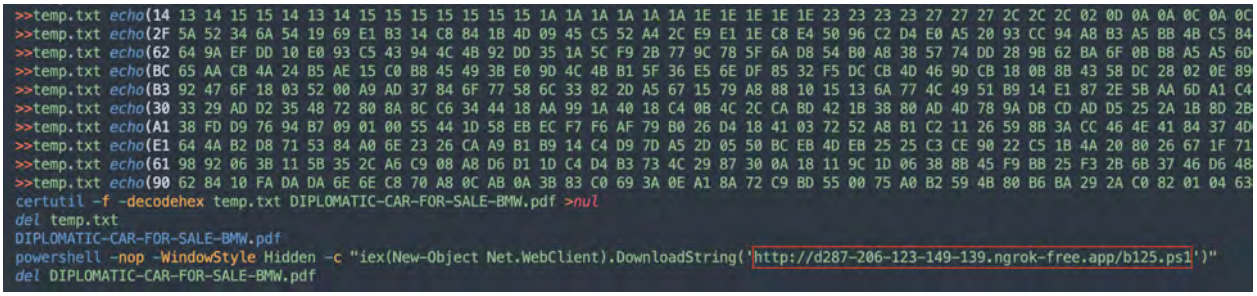


Figure.4 PowerShell script deploying .pdf lure and downloading next-stage payload from ngrok-free.app.

Ngrok, at its core, is an incredibly versatile and cross-platform tool designed to expose local network ports securely to the internet through a process known as tunneling. However, in the context of cyber adversaries, Ngrok has taken on a different role. Instead of legitimate purposes, adversaries have begun leveraging Ngrok to store their next-stage PowerShell payloads and establish covert communication channels.

In this nefarious tactic, they utilize Ngrok's services by utilizing free static domains provided by Ngrok, typically in the form of a subdomain under "ngrok-free.app." These subdomains act as discrete and inconspicuous rendezvous points for their malicious payloads. This clever adaptation allows the adversaries to obfuscate their activities and communicate with compromised systems while evading detection. By exploiting Ngrok's capabilities in this manner, threat actors can further complicate cybersecurity efforts and remain under the radar, making defense and attribution more challenging.

CVE-2023-38831

A critical security flaw, identified as CVE-2023-38831, has been discovered in earlier versions of RARLab's WinRAR software, specifically those released prior to version 6.23. This vulnerability poses a significant threat as it allows attackers to execute arbitrary code through the exploitation of a specially crafted ZIP archive.

The root cause of this vulnerability lies in the incorrect handling of ZIP archives that contain seemingly benign files, such as standard .PDF documents, alongside folders bearing identical names. The crux of the issue is that within these archives, malicious actors can insert folders with matching names. When a user attempts to access one of the harmless files, the ZIP archive may include a folder with the same name that contains executable content, often malware or other malicious code. During the user's attempt to open the benign file, the system unwittingly processes the malicious content within the similarly named folder, resulting in the execution of arbitrary code.

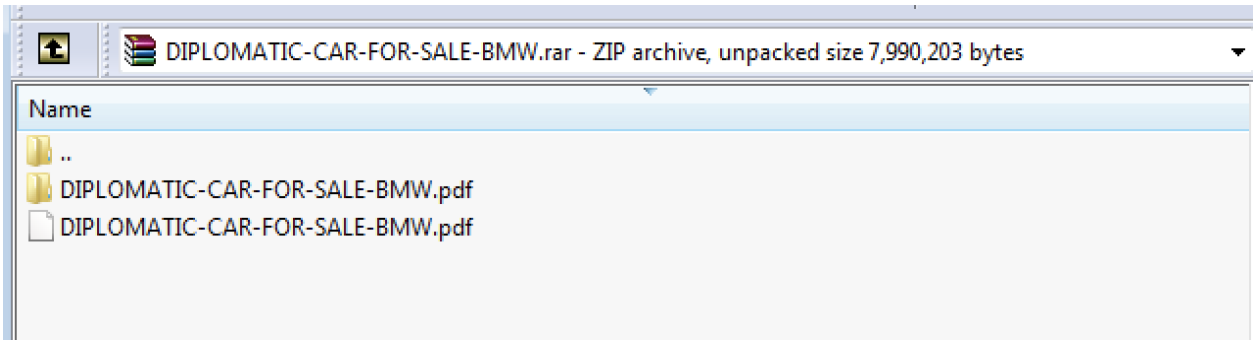


Figure.5 WinRAR archive exploiting CVE-2023-38831.

This vulnerability has not remained merely theoretical; it has been actively exploited in real-world incidents. These attacks have been observed occurring between April and October of 2023. Attackers utilize this vulnerability to craft malicious ZIP archives and distribute them via various channels, such as email attachments or compromised websites. Unsuspecting users who open these seemingly benign files can unknowingly trigger the execution of malicious code, granting attackers access to the victim's system, and potentially leading to a host of detrimental consequences, including data theft, system compromise, and more. The PoC of this vulnerability is publicly available.

In August 2023, ESET researchers discovered another spearphishing campaign attributed to **Sednit APT** exploiting the CVE-2023-38831 vulnerability in WinRAR. Sednit, also known as APT28, a threat actor group closely associated with the Russian military intelligence agency, GRU. Sednit's approach was to employ emails with lures that revolved around the agenda of the European Parliament. This was a calculated choice, as the campaign's primary targets were political entities within the European Union and Ukraine.

A concerning trend of exploiting CVE-2023-38831 vulnerability by Russian intelligence services hacking groups demonstrates its growing popularity and sophistication. It becomes increasingly essential for organizations and security professionals to remain vigilant and proactive in defending against these threats. It is of utmost important for WinRAR users to update their software to version 6.23 or later, which includes the necessary security patches to mitigate this critical vulnerability. Furthermore, practicing caution when opening files received from unknown sources or untrusted locations is an additional layer of defense against potential exploitation of this vulnerability. Cybersecurity awareness and prompt software updates are crucial in maintaining a resilient defense against such threats.

Conclusion

In this comprehensive report, we've delved into the intricate campaign orchestrated by APT29, a threat group associated with Russia's intelligence apparatus. Their targeted attack against embassies, particularly in Azerbaijan, Greece, Romania, and Italy, offers a sobering view of the evolving threat landscape.

One of the most apparent geopolitical motives behind these attacks is the quest for intelligence, especially concerning Azerbaijan's impending actions in Nagorno-Karabakh. It's a stark reminder that cyber-espionage is a tool of statecraft, and its reach extends to diverse regions and sectors.

What makes this campaign particularly noteworthy is the synthesis of old and new techniques. APT29 continues to employ the BMW car for sale lure theme, a tactic that's been seen in the past. However, the deployment of the CVE-2023-38831 WinRAR vulnerability, a novel approach, reveals their adaptability to the evolving threat landscape. Additionally, their use of Ngrok services to establish covert communications emphasizes their determination to remain concealed.

Furthermore, the prevalence of similar techniques among Russian hacking groups underscores the imperative for organizations to take robust security measures seriously. Implementing stringent cybersecurity practices, staying updated on the latest vulnerabilities, and fostering a culture of cybersecurity awareness are vital to guarding against these complex and persistent threats.

Indicators of Compromise

Type	Value
filename	NEAS.f78ee3005ca9f0e78a9dd136fc69afe7c06d69d1fc6218bc9e7eb3adec045977zip.zip
md5	3b641b7e68b671da6497d10f773dcf7c
sha-1	37c619b18ba52956c249551587b955e7b2066b73
sha-256	f78ee3005ca9f0e78a9dd136fc69afe7c06d69d1fc6218bc9e7eb3adec045977
filename	payload_1.ps1
md5	2b9812a7793c3fe0f171456acd9edf02
sha-1	448047b975175cb9c1e8b36036324835a9e9943e
sha-256	5d6bfb8fd1102273ef489060219293f8da796d07e8b2872efbda55050512b71f
filename	Car for sale.eml
md5	ff7d1fb202bac38345be8cf267fa6688
sha-1	3da35178fb0b3a8ef51b78a07c719658a628d722
sha-256	eec902a61886198a8e48ac862fabeecd628f2fa4122b78a0d7d6ee5c256ae724
url	http://d287-206-123-149-139.ngrok-free.app/b125.ps1
domain	d287-206-123-149-139.ngrok-free.app
email address	a.menmedov@outlook.com