Infosecurity Magazine Home » News » Russia’s APT29 Targets Embassies With Ngrok and WinRAR Exploit

NEWS 20 NOV 2023

Russia’s APT29 Targets Embassies With Ngrok and

Infosecurity Magazine

Phil Muncaster
UK / EMEA News Reporter, Infosecurity Magazine
Email Phil Follow @philmuncaster

Ukrainian security researchers have revealed a major new Russian cyber-espionage campaign which they claim may have been designed to harvest information on Azerbaijan’s military strategy.

APT29 (aka Cozy Bear, Nobelium and many other monikers) was behind the attacks, according to a new report from the Ukrainian National Security and Defense Council (NDSC).

It targeted embassies in Azerbaijan, Greece, Romania and Italy, as well as international institutions such as the World Bank, European Commission, Council of Europe, WHO, UN and others.

“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," said the NDSC.

"It's noteworthy that the countries targeted – Azerbaijan, Greece, Romania, and Italy – maintain significant political and economic ties with Azerbaijan."

Read more on APT29: Diplomats in Ukraine Targeted by "Staggering" BMW Phishing Campaign

The campaign itself began as a spear-phishing email, using the lure of a diplomatic car for sale. The RAR attachment featured CVE-2023-3883, a bug which enables threat actors to insert malicious folders with the same name as benign files in a .zip archive.

"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," the NDSC explained.

In this attack, when a user clicks on the RAR archive contained in the phishing email it will execute a script to display a PDF of the car 'for sale,' whilst

hosted on a Ngrok instance.

"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," noted the report.

This isn't the first time hackers have exploited CVE-2023-3883. It was observed being exploited by the Russian Sednit APT group (APT28) in August, shortly after Group-IB first notified about what was then a zero-day vulnerability.

You may also like

NEWS 13 JAN 2023

Pro-Russian Hacktivist Group Targets Czech Presidential Election

NEWS 15 JUN 2023

Microsoft Names Russian Threat Actor "Cadet Blizzard"

NEWS 16 NOV 2022

Botnets, Trojans, DDoS From Ukraine and Russia Have Increased Since Invasion

NEWS 10 JAN 2024

Ukrainian “Blackjack” Hackers Take Out Russian ISP

NEWS 13 NOV 2023

EU Formalizes Cybersecurity Support For Ukraine

What’s hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

1

NEWS 12 JAN 2024

Human Error and Insiders Expose Millions in UK Law Firm Data Breaches

2

NEWS 15 JAN 2024

HelloFresh Fined £140K After Sending 80 Million Spam Messages

3

NEWS 12 JAN 2024

Vulnerability Puts Bosch Smart Thermostats at Risk of Compromise

4

NEWS 11 JAN 2024

NCSC Publishes Practical Security Guidance For SMBs

5

NEWS FEATURE 12 DEC 2023

Top 10 Cyber-Attacks of 2023

6

NEWS 10 JAN 2024

Cyber Insecurity and Misinformation Top WEF Global Risk List

Infosecurity® Magazine

The magazine

About Infosecurity

Meet the team

Contact us

Contributors

Forward features

Op-ed

Next-gen submission

Advertisers

Media pack

Terms and Conditions

Privacy Policy

Intellectual property statement

Cookies Settings

Cookie Policy

Sitemap