The Record.
Recorded Future® News

BAKU, THE CAPITAL OF AZERBAIJAN. IMAGE: ULADZISLAU PETRUSHKEVICH VIA UNSPLASH

Daryna Antoniuk

November 15th, 2023

Nation-state | News | Government

Cyber-espionage operation on embassies linked to Russia's Cozy Bear hackers

Russian state-sponsored hackers have targeted embassies and international organizations in a recent cyber-espionage campaign, Ukrainian government cybersecurity researchers have found.

The attacks were attributed to the infamous hacker group labeled APT29, also known as Cozy Bear or Blue Bravo. Analysts previously have linked it to Russia's Foreign Intelligence Service (SVR), which gathers political and economic information from other countries.

The campaign, analyzed by Ukraine's National Cyber Security Coordination Center (NCSCC), occurred in September of this year. The group used similar tools and tactics in its previous campaigns, particularly during an operation against embassies in Kyiv in April.

The most recent operation had "the primary goal of infiltrating embassy entities," the NCSCC said, including targets in Azerbaijan, Greece, Romania and Italy. Another victim was the major Greek internet provider Otenet, the NCSCC said.

Diplomatic accounts, especially those associated with the foreign affairs ministries in Azerbaijan and Italy, suffered the most, according to researchers. One possible reason is that Russian intelligence was attempting to gather information regarding Azerbaijan's strategic activities, especially leading up to the Azerbaijani invasion of the Nagorno-Karabakh region.

In total, APT29's campaign targeted over 200 email addresses, but it's not clear how many attacks were successful.

Tactics and techniques

APT29 exploited a recently discovered vulnerability in the Windows file archiver tool WinRAR. Identified as CVE-2023-38831, the bug was utilized by state-controlled hackers connected to Russia and China in early 2023 before being patched. Unpatched versions of the tool remain vulnerable.

According to NCSCC, this vulnerability still "poses a significant threat" as it allows attackers to execute arbitrary code through the exploitation of a specially crafted ZIP archive.

In the recent campaign, Cozy Bear sent victims phishing emails containing a link to a PDF document and a malicious ZIP file that exploits the vulnerability, potentially granting attackers access to the compromised systems.

To convince their targets to open malicious files, the hackers created emails claiming to have information about the sale of diplomatic BMW cars. The same lure was used during the group's attack on the embassies in Kyiv this spring.

In this campaign, the attackers introduced a novel technique for communicating with the malicious server, researchers said. In particular, they used a legitimate tool called Ngrok that allows users to expose their local servers to the internet.

Ngrok is commonly used during web development and testing to provide temporary public URLs for local web servers but cybercriminals deployed it to obfuscate their activities and communicate with compromised systems while evading detection.

By exploiting Ngrok's capabilities in this way, threat actors can further complicate cybersecurity analysis and remain under the radar, making defense and attribution more challenging, NCSCC said.

Cozy Bear's previous attacks

During the war in Ukraine, APT29 has carried out cyberattacks against the Ukrainian military and its political parties, as well as diplomatic agencies, think tanks and nonprofit organizations.

In April, for example, the group launched a spying campaign targeting foreign ministries and diplomatic entities in NATO countries, the European Union and, "to a lesser extent," Africa.

The hackers' tactics were similar to those used in the September campaign. In particular, they sent phishing emails impersonating the embassies of European countries to specific personnel, usually including a malicious link either in the body of the message or an attached PDF inviting the target diplomat to access the ambassador's calendar.

APT29 has been blamed for several high-profile incidents prior to the war, including the SolarWinds supply chain attack in 2020 that affected thousands of organizations globally and led to a series of data breaches.

Previous article

Next article

DARYNA ANTONIUK

Daryna Antoniuk is a freelance reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.

BRIEFS

UK privacy watchdog to examine practice of web scraping to get training data for AI

| January 15th, 2024

Microsoft to keep all European cloud customers' personal data within EU

| January 13th, 2024

British cosmetics firm Lush confirms cyberattack| January 13th, 2024

FCC presses carmakers, wireless providers to protect domestic abuse survivors from stalking tools

| January 12th, 2024

Further analysis of Denmark attacks leads to warning about unpatched network gear

| January 12th, 2024

Republican lawmakers want answers on SEC social media hack — and soon

| January 11th, 2024

French hacker from 'ShinyHunters' group sentenced to three years in US prison

| January 11th, 2024

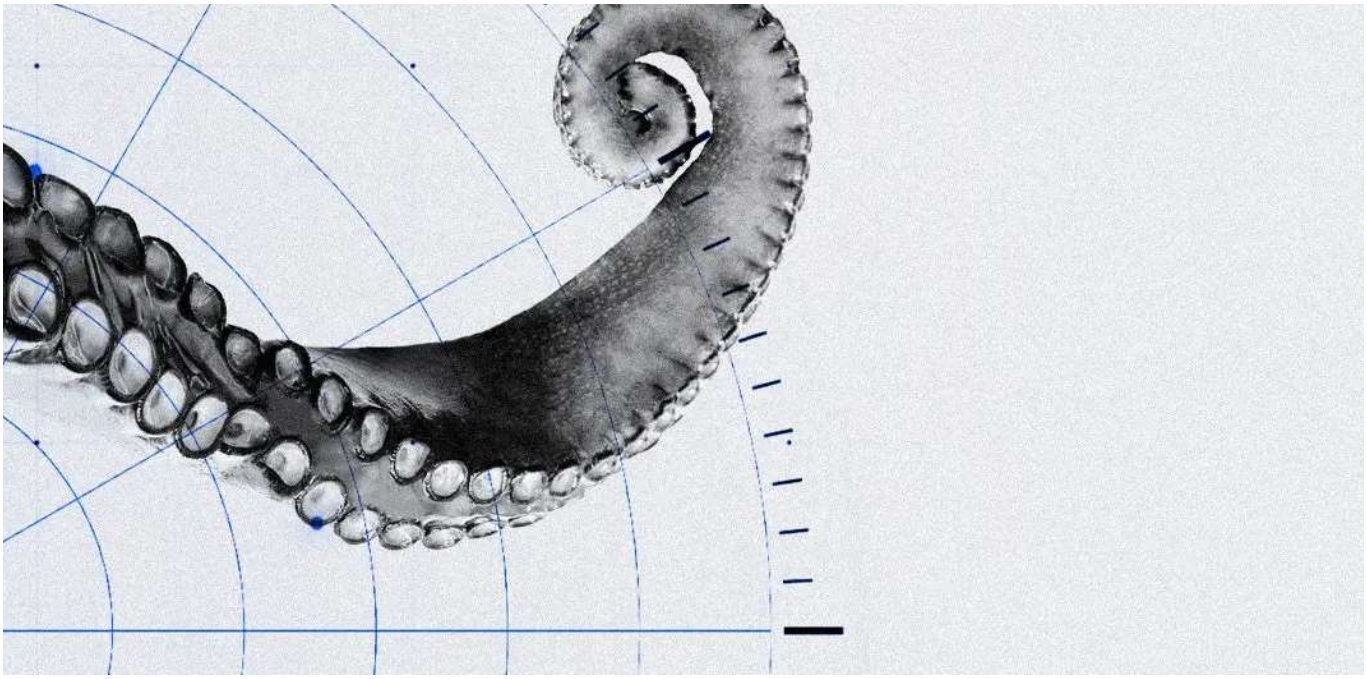
SEC's X account compromised, used to spread false bitcoin announcement

| January 10th, 2024

Nigerian national who laundered funds from romance and BEC scams gets 10-year sentence

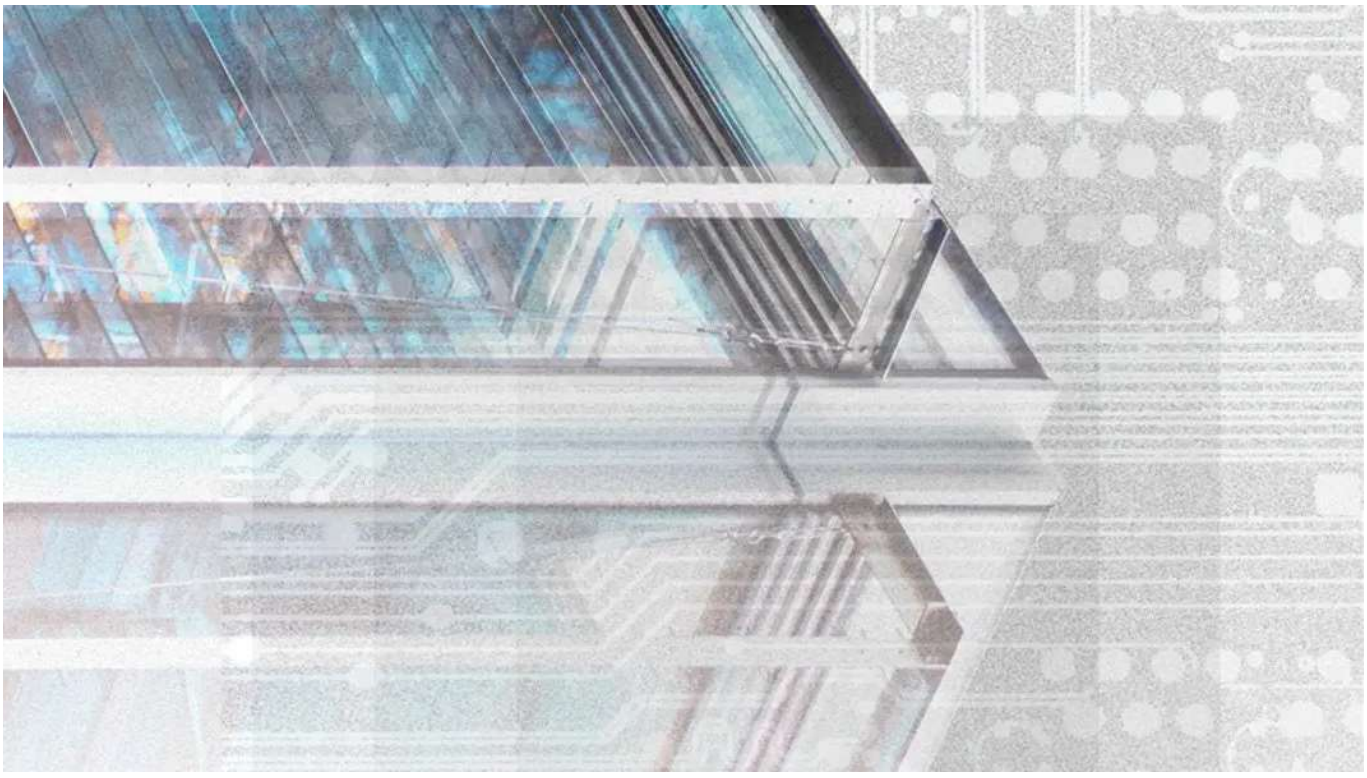
| January 10th, 2024

FLYING UNDER THE RADAR: ABUSING GITHUB FOR MALICIOUS INFRASTRUCTURE



FLYING UNDER THE RADAR: ABUSING GITHUB FOR MALICIOUS INFRASTRUCTURE

2023 ADVERSARY INFRASTRUCTURE REPORT



2023 ADVERSARY INFRASTRUCTURE REPORT

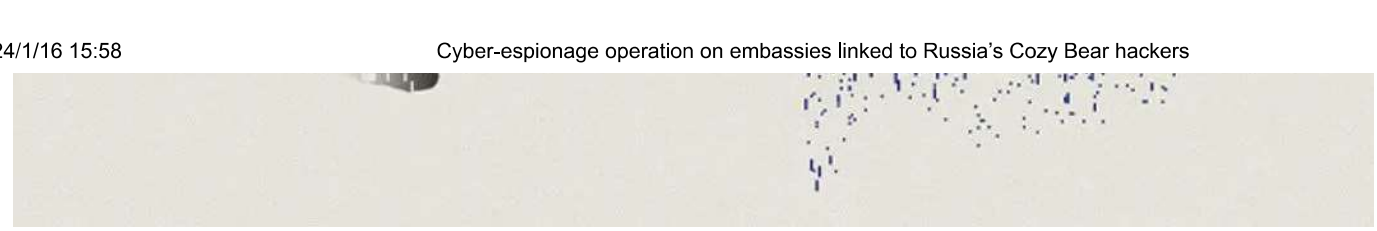
ANNUAL PAYMENT FRAUD INTELLIGENCE REPORT: 2023

ANNUAL PAYMENT FRAUD INTELLIGENCE REPORT: 2023

AGGRESSIVE MALIGN INFLUENCE THREATENS TO SHAPE US 2024 ELECTIONS

AGGRESSIVE MALIGN INFLUENCE THREATENS TO SHAPE US 2024 ELECTIONS

OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK "DOPPELGÄNGER" SIGNALS EVOLVING TACTICS



OBFUSCATION AND AI CONTENT IN THE RUSSIAN INFLUENCE NETWORK "DOPPELGÄNGER" SIGNALS EVOLVING TACTICS