Evolving Tactics: How Russian APT Groups Are Shaping Cyber Threats in 2024

By Flashpoint Intel Team

Published: 2024-05-23 · Archived: 2026-04-05 18:52:27 UTC

Flashpoint is observing that Russian advanced persistent threat (APT) groups are evolving their tactics, techniques, and procedures (TTPs)—while also expanding their targeting. They are using new spear-phishing campaigns to exfiltrate data and credentials by delivering malware sold on illicit marketplaces.

Flashpoint identified the following Russian APT groups have engaged in recent campaigns, listing the malware strains used in attributed attacks and their intended targets:

Threat Group	Malware	Target(s)
APT28	Credomap, Oceanmap, Masepie, Steelhook, Unidentified 114	Poland, Ukraine
APT29	ROOTSAW, WINELOADER, Quarterrig, BURNTBATTER, SPICYBEAT, MUSKYBEAT, STATICNOISE	Germany, Ukraine
APT44	Smokeloader, Rhadamanthys	Ukraine, Eastern Europe, Journalists
Gamaredon	GammaSteel	Ukraine
Gossamer Bear	Spica	NATO countries, Ukraine
Storm-097	RomCom	Europe, North America
Turla	Capibar, Kazuar	Ukraine
UAC-0050	Remcos RAT, MeduzaStealer	Poland, Ukraine
UAC-0149	COOKBOX	Ukraine
Winter Vivern	Aperitif	Poland, Ukraine

The use of spear-phishing among Russian state-sponsored actors is a noticeable shift from the start of the Ukraine-Russian War that began in 2022. At the start of the conflict, state-sponsored groups had favored the use of destructive wiper malware. However, near the end of 2023, the Ukrainian Computer Emergency Response Team (CERT) began to see a shift in their tactics, responding to over 1,700 phishing attacks, including distributing malware, harvesting credentials, and extortion incidents.

Flashpoint found that the most prevalent malware families used in these spear-phishing campaigns were Agent Tesla, Remcos, Smokeloader, Snake Keylogger, and Guloader. The attack chains used across these groups share malware and techniques for evading detection.

Here's what you should know about these APTs and their TTPs:

Russian APTs Explained

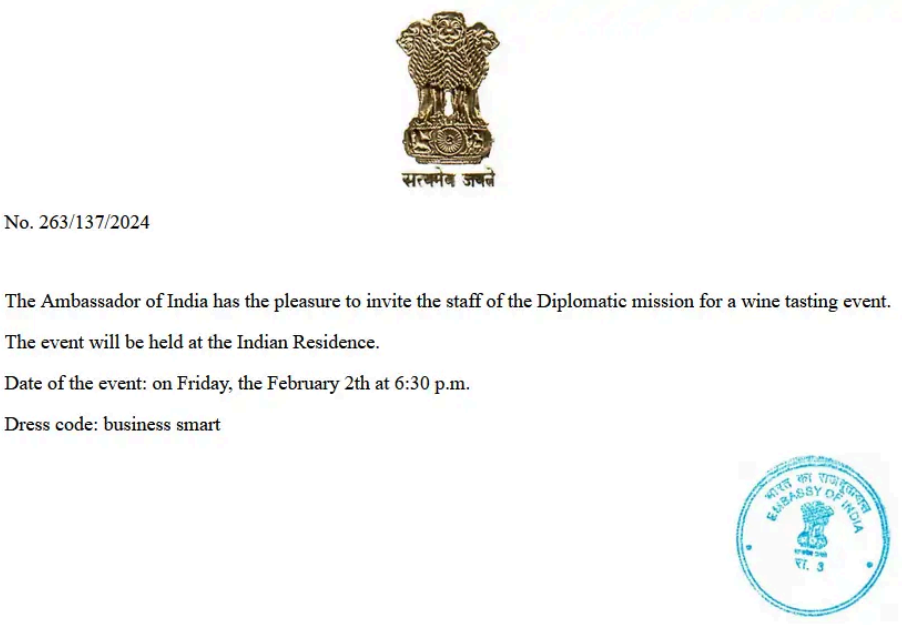
Flashpoint analysts reviewed campaigns by the following Russian groups. Each of these APT groups are currently active in 2024:

- **APT28:** APT28 phishing lures have impersonated government organizations in Argentina, Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Poland, Ukraine, and the United States. The group leveraged free hosting providers to host backdoors that target Windows operating systems.
- **APT29:** The campaigns from this group have delivered a variety of droppers and infection methods. Many samples have been observed in past campaigns, including BURNTBATTER and DONUT. Starting in February 2024, they added WINELOADER to their array of downloaders.
- **APT44:** Between December 2023 and January 2024, a group associated with APT44 targeted investigative journalists, including the Netherlands-based investigative journalist group Bellingcat. In campaigns that delivered the information-stealing malware Rhadamanthys, the group also used "Smokeloader." Both malware are purchasable on Dark Web forums.
- **GAMAREDON:** The EU CERT cites Gamaredon as the most prolific actor in the Russian war against Ukraine. Tracked since 2013, Gamaredon primarily targets Ukraine with malicious documents that deliver a variety of home-brewed malware.
- **GOSSAMER BEAR:** Also commonly known as Callisto, this group focuses on credential harvesting and targets Ukraine and North Atlantic Treaty Organization (NATO) countries. Recent campaigns delivered a custom Rust-based backdoor.
- **UAC-0050:** A group tracked by the Ukrainian CERT, targets Ukrainian and Polish government organizations. Similar to APT28 and APT29, the group's lure content has impersonated organizations from countries allied with Ukraine. UAC-0050 consistently delivers Remcos and Meduza Stealer.
- **UAC-0149:** UAC-0149 has been tracked since February 2024, when the Ukrainian CERT detected phishing attempts distributed through Signal messenger. The campaign delivered a malicious document to military personnel. When executed, the malicious documents retrieved malicious PowerShell payloads hosted on GitHub.

The Russian APT Killchain

Droppers

The most common method for infecting victims is by delivering HTML-based droppers that are often packaged in compressed archive or disk image files. State-sponsored groups such as APT29 persistently leverage HTML attachments to phishing emails that execute the JavaScript-based dropper ROOTSAW. When the HTML file is executed, the victim is presented with a lure while the malicious code executes. The purpose of this is to retrieve and execute a second-stage payload.



सत्यमेव जयते

No. 263/137/2024

The Ambassador of India has the pleasure to invite the staff of the Diplomatic mission for a wine tasting event.

The event will be held at the Indian Residence.

Date of the event: on Friday, the February 2th at 6:30 p.m.

Dress code: business smart

EMBASSY OF INDIA

While some campaigns delivered ROOTSAW with HTML file attachments, APT29 also used .HTA files that delivered WINELOADER malware, which is a backdoor delivered via phishing emails. HTA files execute outside of the security constraints of a browser, therefore allowing simple payloads to evade detection. Other APT groups such as Gamaredon also used HTA droppers in their campaigns. This infection chain is also implemented by other cybercrime campaigns that deliver infostealers and other commodity malware.

Malware

Russian APT groups develop a variety of malware including backdoors, stealers, and loaders to compromise victims. In a 2023 campaign, APT29 delivered at least six unique loaders in their spear-phishing campaigns. Recently, the group has pivoted toward WINELOADER, a variant of past payloads. When executed, WINELOADER is injected into a legitimate executable via DLL-sideloading. Once loaded, the loader communicates with the C2 over HTTP GET requests.

However, not all APT groups are developing custom payloads. Other groups simply purchase malware from illicit marketplaces. These tools are used by other cybercrime actors. Throughout 2023, the most popular malware leveraged by Russian threat actors had been freely available for purchase. Even advanced espionage actors such as APT44 have conducted campaigns leveraging Sandworm malware since the start of 2023.

Compromised Infrastructure

Russian threat groups leverage compromised websites for command and control (C2). APT29, Gamaredon, and Gossamer Bear have implemented compromised WordPress sites to impede attribution of their C2 servers.

In February 2024, the US Department of Justice disrupted a botnet of compromised routers that APT28 used for spear-phishing and credential harvesting campaigns.

NTLM Hash Stealing

In a credential-harvesting campaign in late 2023, APT28 leveraged NTLMv2 hash relay attacks. These attacks deliver a PowerShell or VBS script to the victim, which triggers an NTLMv2 authentication over HTTP and creates an HTTP listener to receive the requests.

In another campaign, APT28 leveraged an offensive PowerShell framework, to capture NTLM hashes and exfiltrated data through a free service that allows users to quickly stand up mock application programming interfaces (APIs). In Q3 2023, APT29 used a public API service to obtain a victim's IP address.

Ways to Protect Yourself Against Russian APTs

As the Ukraine-Russian War continues, Russian APT groups are continuously adapting their TTPs and malware. Many groups share delivery techniques, indicating possible collaboration between members. In addition, the use of paid tools instead of custom payloads suggests that many of these illegal campaigns have proved to be successful. What does this mean for you?

Given the use of paid tools and similar delivery techniques, organizations can help to protect themselves by:

1. Reviewing abnormal child processes of HTML and .HTA files.
2. Reviewing executions of .iso files.
3. Detecting downloads of these file types at web proxy.
4. Implementing DLL side-loading detections.
5. Reviewing network logs for communications with mock API services.
6. Proactively blocking malware sold on illicit marketplaces and forums via Flashpoint's comprehensive threat intelligence.

Stay Ahead of Cyber Threats Using Flashpoint

To defend against threats, organizations must stay vigilant by implementing robust security measures, monitoring for unusual activities, and leveraging advanced threat intelligence solutions. Sign up for a demo today and see how Flashpoint empowers organizations to stay ahead of evolving cyber threats.
