MAHACYBER ADVISORY

FANCY BEAR (APT28)

CERTMH_CTI_2025_25

29TH MAY 2025

Prepared by
MAHACYBER

Table of Contents

APT 28

Origin:Russia
Active Seen:2004

Introduction

Sofacy, also known as APT28, Fancy Bear or Sednit Gang is a threat group linked to Russia's Main Intelligence Directorate of the Russian General Staff. They are motivated to engage in cyber espionage and interference activities, particularly targeting Eastern European governments, security organizations, and global multilateral institutions. Sofacy employs various tactics like spear-phishing campaigns, zero-day exploits, and malware deployment to compromise systems and exfiltrate sensitive information.

In a typical scenario, threat actors associated with Sofacy might send phishing emails to employees of government entities or political organizations, pretending to be from trusted sources to lure victims into clicking on malicious links or providing login credentials.

Once the system is compromised, Sofacy would utilize keyloggers, backdoors, or malware to gather intelligence or disrupt operations. Their methods involve careful planning and strategic targeting to achieve their goals of collecting valuable information or influencing public opinion.

Motivations and Targets

→ Motivations

- Cyber Espionage
- Political Influence Operations
- Data Leaks & Destabilizations

→ Target Sectors

- Aerospace & Defense
- Automotive
- BFSI
- Chemicals
- Construction
- Education
- Energy & Utilities
- Government & LEA
- Healthcare
- IT & ITES
- Manufacturing
- Media & Entertainment
- Organisation

Major Cyber Attacks + Timeline

- **2007 - Pawn Storm:** First identified spear-phishing and malware campaigns against Georgian and NATO-aligned targets
- **2014 -** X-Agent on Ukrainian artillery forums
- **2016 -** DNC & WADA Breaches
- **July- Aug 2016:** Leak of World Anti-Doping Agency Testing data
- **2017 -** French & German election interference
- **2020 -** Norwegion Parliament hack
- **Aug 2020 -** APT28 Forced Multiple email accounts of Norway's Stortinget
- **2023 -** "RoundPress" Webmail XSS Campaign
- **2024 -** "Olympics Planning Espionage In France" - ANSII Attributes a 2021-2024 series of hacks on French ministeries, local Governements and
- **2024 -** Paris-Games Organizers

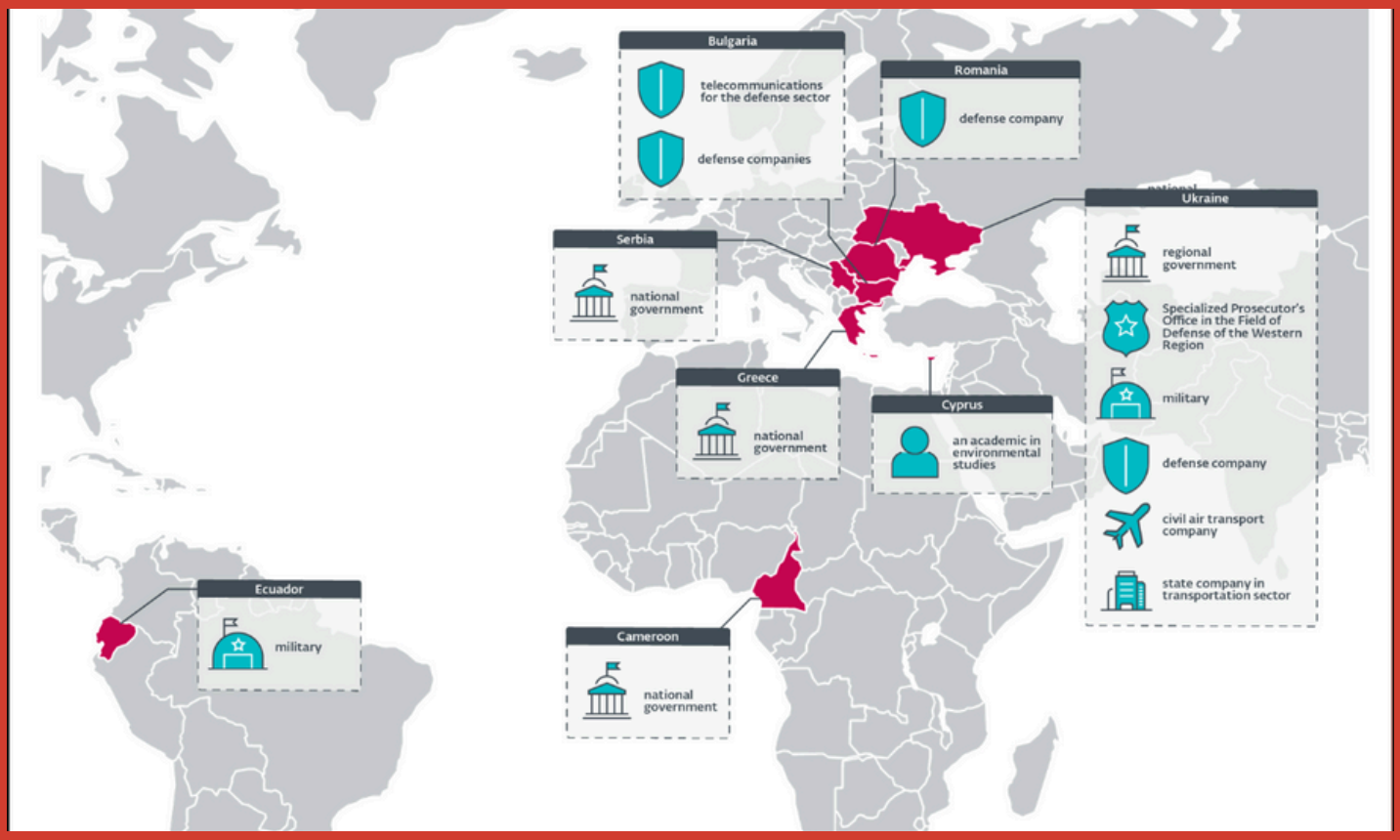
Recent Attack

Key points of the Attacks:

- In Operation RoundPress, the compromise vector is a spearphishing email leveraging an XSS vulnerability to inject malicious JavaScript code into the victim's webmail page.
- In 2023, Operation RoundPress only targeted Roundcube, but in 2024 it expanded to other webmail software including Horde, MDaemon, and Zimbra.
- For MDaemon, APT28 used a zero-day XSS vulnerability. The vulnerability to the developers on November 1st, 2024 and it was patched in version 24.5.1.
- Most victims are governmental entities and defense companies in Eastern Europe, although we have observed governments in Africa, Europe, and South America being targeted as well.
- These payloads are able to steal webmail credentials, and exfiltrate contacts and email messages from the victim's mailbox.
- Additionally, SpyPress.MDAEMON is able to set up a bypass for two-factor authentication.

On September 29, 2023, a spearphishing email exploiting CVE-2023-43770 in Roundcube was observed, originating from a sender address closely resembling those used in past Sednit/APT28 operations. Infrastructure links were identified between **cerioss[.]info and global-world-news[.]net,** the latter being directly tied to Operation RoundPress. These similarities in infrastructure and tactics support a medium-confidence attribution to APT28.

Map of operation RoundPress victims in 2024

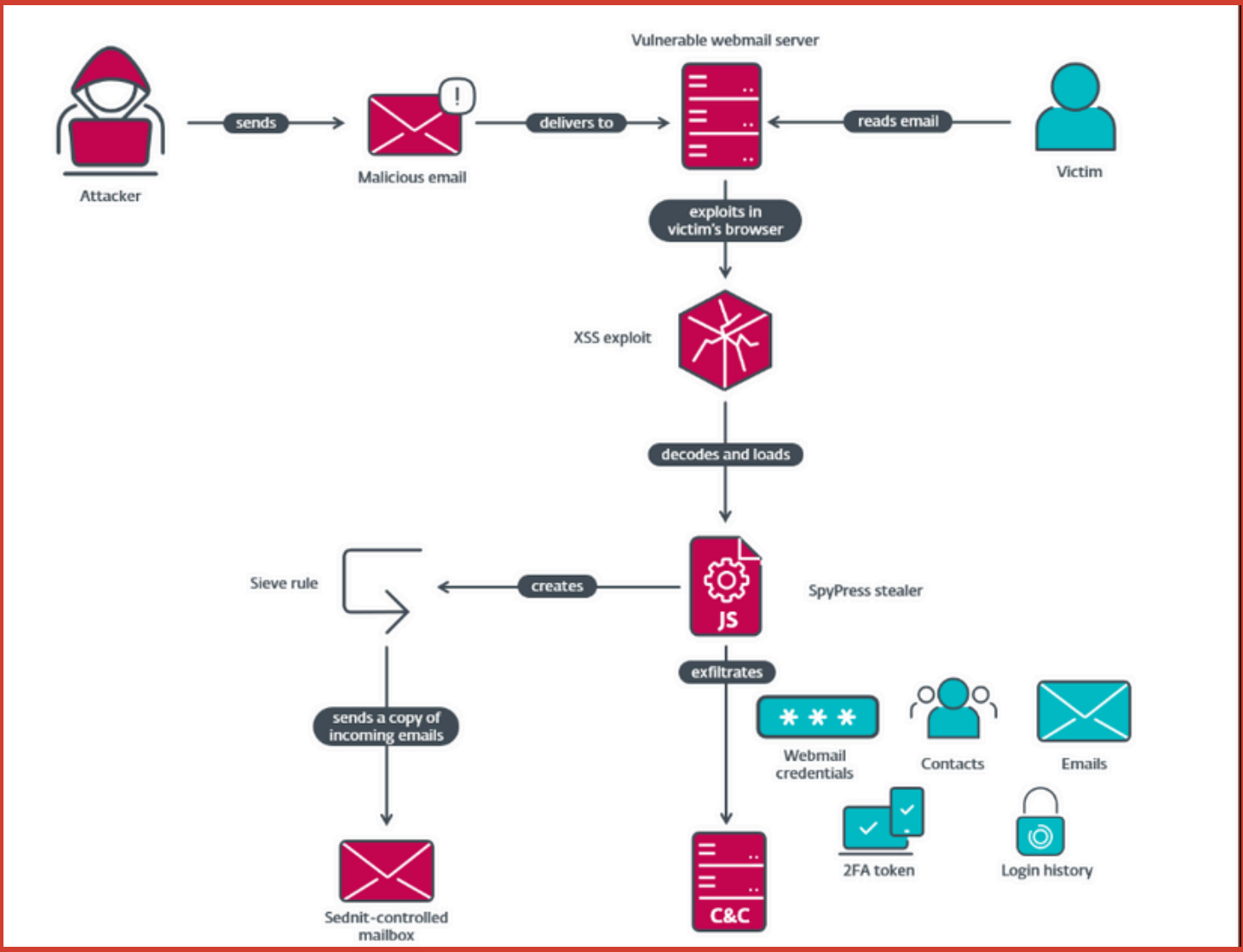


Victimology

The 2024 targets primarily include:

1. Ukrainian government entities
2. Defense companies in Bulgaria and Romania, notably those supplying Soviet-era weapons to Ukraine
3. Other targets include African, EU, and South American governments.

Infection Chain



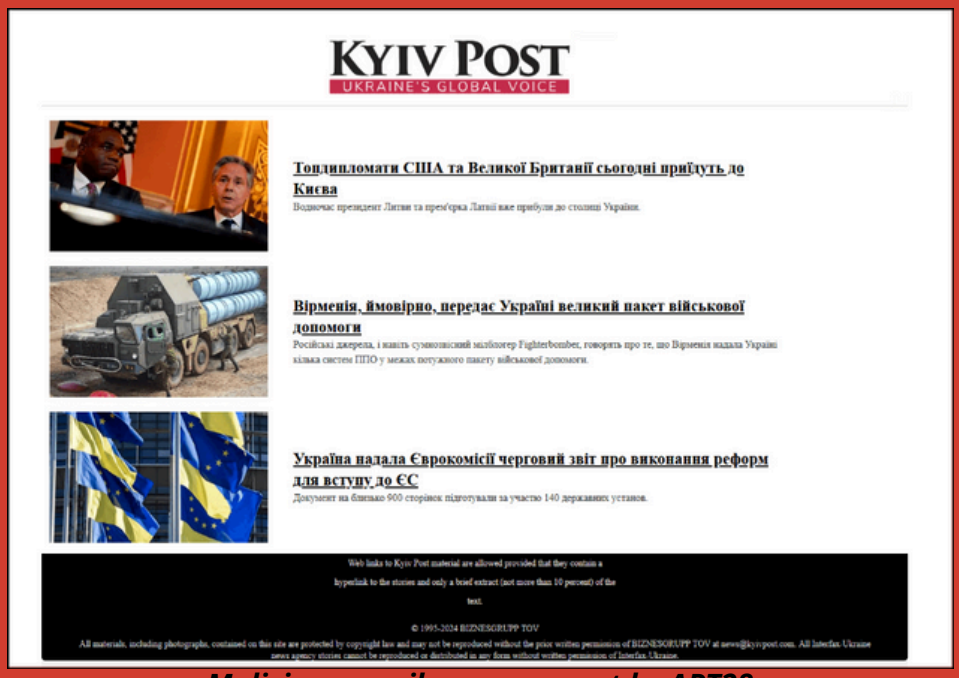
Above picture: Operation RoundPress compromise chain

In 2024, we observed different XSS vulnerabilities being used to target additional webmail software: Horde, MDaemon, and Zimbra. APT28 also started to use a more recent vulnerability in Roundcube, CVE-2023-43770. The MDaemon vulnerability (CVE-2024-11182, now patched) was a zero day, most likely discovered by same threat actor, while the ones for Horde, Roundcube, and Zimbra were already known and patched.

They sends these XSS exploits by email. The exploits lead to the execution of malicious JavaScript code in the context of the webmail client web page running in a browser window. Therefore, only data accessible from the victim's account can be read and exfiltrated.Note that, in order for the exploit to work, the target must be convinced to open the email message in the vulnerable webmail portal. This means that the email needs to bypass any spam filtering and the subject line needs to be convincing enough to entice the target into reading the email message.

The email message looks benign and contains text about news events. For example, on September 11th, 2024, a Ukrainian target received a phishing email from kyivinfo24@ukr[.]net with the subject СБУ схопила банкіра, який працював на ворожу воєнну розвідку в Харкові (machine translation: SBU arrested a banker who worked for enemy military intelligence in Kharkiv).

The message body contains excerpts (in Ukrainian) and links to articles from Kyiv Post, a well-known newspaper in Ukraine. The malicious code that triggers the XSS vulnerability is inside the HTML code of the email message's body and is not directly visible to the user.



Malicious email message sent by APT28

Another example is an email from **office@terembg[.]com** to a Bulgarian target on November 8th, 2024, with the subject Путин се стреми Тръмп да приеме руските условия вдвустранните отношения (machine translation: Putin seeks Trump's acceptance of Russian conditions in bilateral relations). The message body again contains excerpts (in Bulgarian) and links to articles from News.bg, a legitimate Bulgarian newspaper.

Another malicious email sent by APT28

Roundcube: CVE-2023-43770

For targets using Roundcube webmail: in 2023, Sednit used the XSS vulnerability CVE-2020-35730, while in 2024, it switched to CVE-2023-43770.
The more recent vulnerability was patched on September 14th, 2023 in this GitHub commit. The fix is in a regex in the rcube_string_replacer.php script. The exploit used by APT is quite simple and is depicted in below pitcure

```
[<script> /* The following is the entire license notice for the JavaScript code in this page */
document.currentScript.parentElement.style.display='none';window.parent.eval(window.parent.atob('KGFzeW5jIGZ1bmN0aW9uKCl7Y29
uc3QgYTBfMHg[...]'))</script>] https://roundcube.net/
```

Exploit for CVE-2023-43770 in Roundcube

IN RCUBE_STRING_REPLACER.PHP, URLS ARE CONVERTED TO HYPERLINKS, AND THE HYPERLINK TEXT IS WHAT IS EXPECTED TO BE PROVIDED BETWEEN THE OUTER SET OF SQUARE BRACKETS. THE BUG LIES IN THE FACT THAT THE HYPERLINK TEXT IS NOT PROPERLY SANITIZED, ALLOWING THE CHARACTERS < AND >. THIS ENABLES AN ATTACKER TO PROVIDE JAVASCRIPT CODE CONTAINED BETWEEN <SCRIPT> AND </SCRIPT>, WHICH IS DIRECTLY ADDED TO THE PAGE WHEN THE EMAIL IS RENDERED IN ROUNDCUBE.

Persistence : The JavaScript payloads (SpyPress) loaded by the XSS vulnerabilities don't have true persistence, but they are reloaded every time the victim opens the malicious email. In addition, we detected a few SpyPress.ROUNDCUBE payloads that have the ability to create Sieve rules. SpyPress.ROUNDCUBE creates a rule that will send a copy of every incoming email to an attacker-controlled email address. Sieve rules are a feature of Roundcube and therefore the rule will be executed even if the malicious script is no longer running.

Credential Access : All SpyPress payloads have the ability to steal webmail credentials by trying to trick the browser or password manager to fill webmail credentials into a hidden form. In addition, some samples also try to trick the victim by logging them out of their webmail account and displaying a fake login page.

Collection and Exfiltration: Most SpyPress payloads collect email messages and contact information from the victim's mailbox. The data is then exfiltrated via an HTTP POST request to a hardcoded C&C server.

What is SpyPress Camaign ?

SpyPress sophisticated cyberespionage campaign attributed with medium confidence to the Russia-aligned Fancy Bear group. Active since 2023, the campaign leverages SpyPress malware, a malicious JavaScript payload, to exfiltrate sensitive email data from high-value webmail servers. It primarily targets Ukrainian governmental entities and defense contractors in Bulgaria and Romania, focusing on firms producing Soviet-era weapons for Ukraine. The campaign also affects government organizations in African countries, the EU, and South America, underscoring its geopolitical scope.

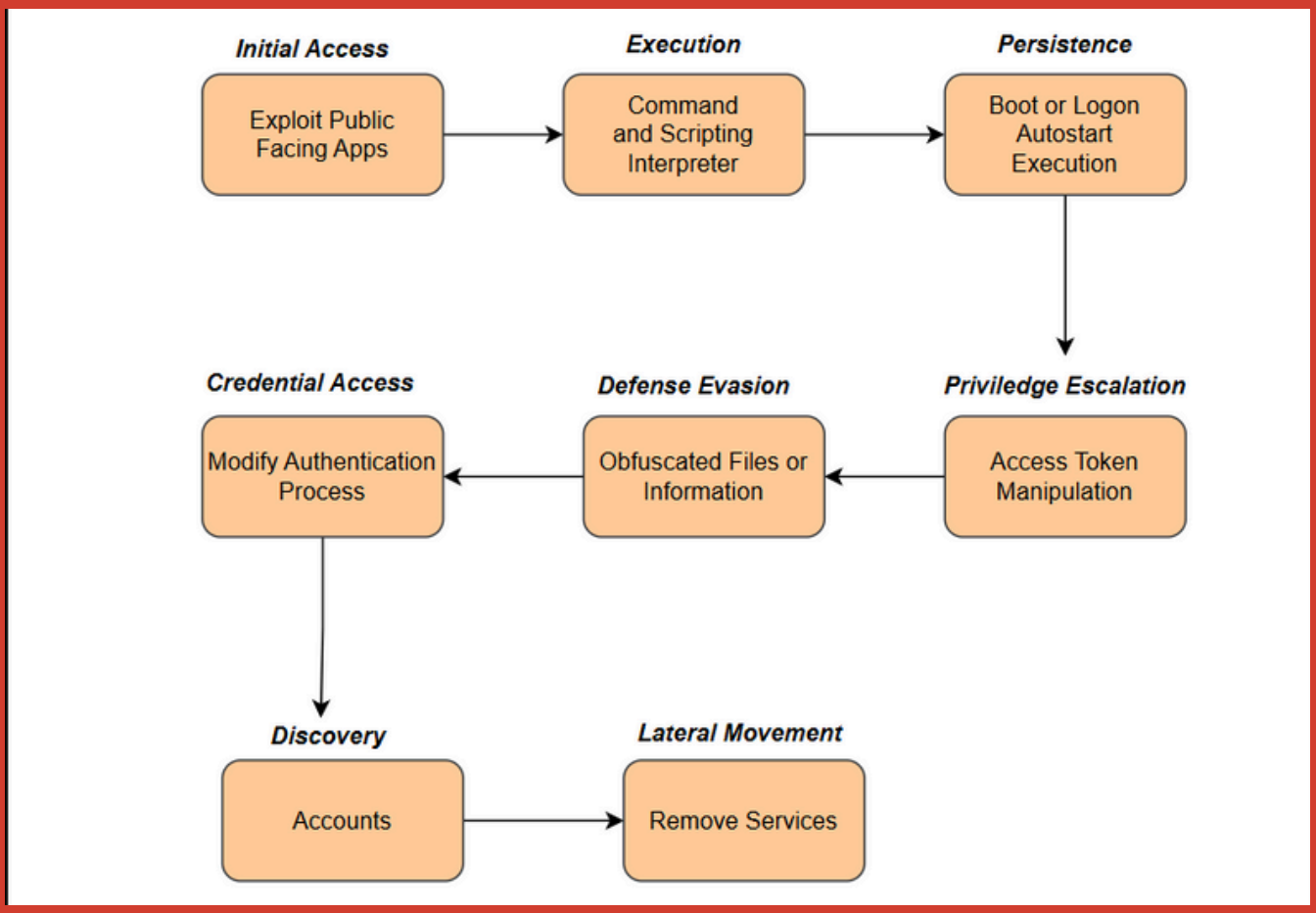
The attack begins with spearphishing emails that exploit cross-site scripting (XSS) vulnerabilities, enabling Fancy Bear to inject SpyPress into victims' webmail interfaces. In 2023, SpyPress was deployed against Roundcube webmail, exploiting CVE-2020-35730 to execute arbitrary JavaScript, granting access to email content, contacts, and credentials.

By 2024, Fancy Bear expanded SpyPress's deployment to Horde, MDaemon, and Zimbra platforms, exploiting platform-specific XSS flaws. A notable 2024 attack involved a zero-day XSS vulnerability in MDaemon (CVE-2024-11182), where SpyPress manipulated the HTML parser using a crafted <̀img> ̀element and a <̀noembed> ̀tag within a <̀p> ̀ element's title attribute.

Researcher disclosed this flaw to MDaemon developers on November 1, 2024, prompting a patch in version 24.5.1. For Roundcube in 2024, SpyPress exploited CVE-2023-43770, patched in September 2023, which abused a regex flaw in the r̀cube_string_replacer.php ̀ script to create malicious hyperlinks.

SpyPress is designed for stealth, enabling persistent access to webmail environments and efficient data exfiltration. Its adaptability across multiple webmail platforms highlights Fancy Bear's technical prowess.

MITRE ATT&CK


Initial Access
Exploit Public Facing Apps
Execution
Command and Scripting Interpreter
Persistence
Boot or Logon Autostart Execution
Priviledge Escalation
Access Token Manipulation
Defense Evasion
Obfuscated Files or Information
Credential Access
Modify Authentication Process
Discovery
Accounts
Lateral Movement
Remove Services

Indicator of Compromise

IOC - Hash SHA-1	Detection
6ef845938f064de39f4bf6450119a0cdbb61378c	c9bb17ae1dc2f92131473c8b61fe0a79.eml
65a8d221b9eced76b9c17a3e1992df9b085cecd7	sample1.js
41FE2EFB38E0C7DD10E6009A68BD26687D6DBF4C	JS/Agent.RSO
60D592765B0F4E08078D42B2F3DE4F5767F88773	JS/Exploit.Agent.NSH
1078C587FE2B246D618AF74D157F941078477579	JS/Exploit.Agent.NSH
8EBBBC9EB54E216EFFB437A28B9F2C7C9DA3A0FA	HTML/Phishing.Agent.GNZ
F95F26F1C097D4CA38304ECC692DBAC7424A5E8D	HTML/Phishing.Agent.GNZ
2664593E2F5DCFDA9AAA1A2DF7C4CE7EEB1EDBB6	JS/Agent.SJU
B6C340549700470C651031865C2772D3A4C81310	JS/Agent.SJU
65A8D221B9ECED76B9C17A3E1992DF9B085CECD7	HTML/Phishing.Gen
6EF845938F064DE39F4BF6450119A0CDBB61378C	N/A
8E6C07F38EF920B5154FD081BA252B9295E8184D	JS/Agent.RSP
AD3C590D1C0963D62702445E8108DB025EEBEC70	JS/Agent.RSN
EBF794E421BE60C9532091EB432C1977517D1BE5	JS/Agent.RTD
F81DE9584F0BF3E55C6CF1B465F00B2671DAA230	JS/Agent.RWO
A5948E1E45D50A8DB063D7DFA5B6F6E249F61652	JS/Exploit.Agent.NSG

IP Address	Details
185.225.69[.]223	SpyPress C&C Server
193.29.104[.]152	SpyPress C&C Server
193.29.104[.]152	SpyPress C&C Server
45.137.222[.]24	SpyPress C&C Server
91.237.124[.]164	SpyPress C&C server
185.195.237[.]106	SpyPress C&C server
91.237.124[.]153	SpyPress C&C server
146.70.125[.]79	SpyPress C&C server
89.44.9[.]74	SpyPress C&C server
111.90.151[.]167	SpyPress C&C server

References

Fancy Bear spearphishing exploiting CVE-2024-11182 to deliver SpyPress

Fancy Bear is a Russian Threat Actor group that uses spearphishing to deliver SpyPress

Broadcom

Insights, news, education and announcements from PolySwarm | SpyPress

SpyPress | Analyze suspicious files and URLs, at scale, millions of times per day. Get real-time threat intel from a crowdsourced network of security experts and antivirus companies competing to protect you.

PolySwarm