Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

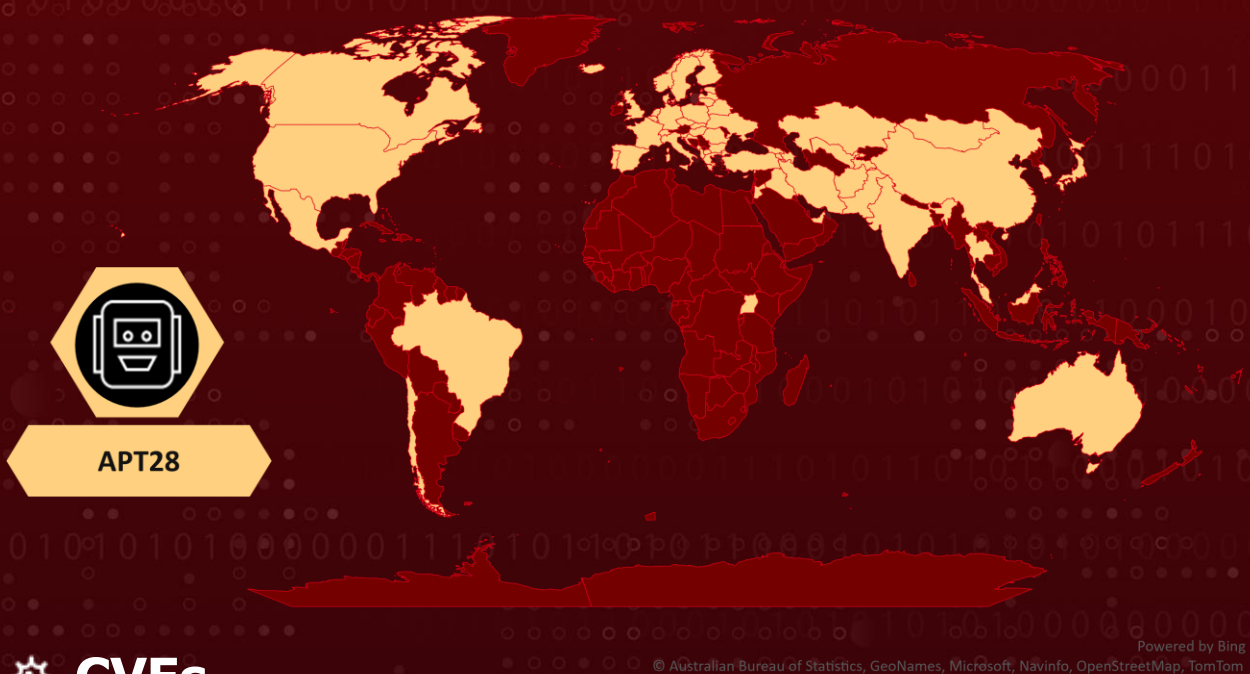
APT28's Tactical Exploitation of Critical Vulnerabilities

Date of Publication	Admiralty code	TA Number
December 8, 2023	A1	TA2023496

Summary

First Appearance: 2004
Threat Actor: APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)
Target Industries: Automotive, Aviation, Chemical, Construction, Defense, Diplomatic, Education, Electrical, Embassies, Energy, Engineering, Financial, Foreign Affairs, Government, Healthcare, Industrial, Information Technology, Intelligence organization, IT, Logistics, Media, NGOs, Oil and gas, Telecommunications, Think Tanks, Transit Pipeline, Transportation, Utilities
Target Region: Parts of Asia, Europe, North America, South America, Africa

Actor Map



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2022-30190	FOLLINA (Microsoft Windows Support Diagnostic Tool Remote Code Execution Vulnerability)	Microsoft Windows	✓	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-23397	Microsoft Office Outlook Privilege Escalation Vulnerability	Microsoft Windows	✓	✓	✓
CVE-2023-38831	WinRAR Remote Code Execution Vulnerability	RARLAB WinRAR	✓	✓	✓
CVE-2021-40444	Microsoft MSHTML Remote Code Execution Vulnerability	Windows Server & Microsoft Internet Explorer	✓	✓	✓
CVE-2021-42292	Microsoft Excel Security Feature Bypass	Microsoft Office & Excel	✓	✓	✓
CVE-2021-42321	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✓	✓	✓
CVE-2021-34473	PROXYSHELL (Microsoft Exchange Server Remote Code Execution Vulnerability)	Microsoft Exchange Server	✗	✓	✓
CVE-2020-17144	Microsoft Exchange Server Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓
CVE-2020-0688	Microsoft Exchange Server Validation Key Remote Code Execution Vulnerability	Microsoft Exchange Server	✗	✓	✓

Actor Details

#1

The APT28 adversary, also known as Fancy Bear or Forest Blizzard, originating from Russia, gained prominence following a series of sophisticated phishing activities. In these operations, the threat actor capitalized on patched vulnerabilities, sometimes employing them as an initial access point, to conduct high-volume campaigns targeting government, aerospace, education, finance, manufacturing, and technology sectors. The primary objectives were to extract user credentials or initiate subsequent malicious activities.

#2

Among the exploited vulnerabilities were CVE-2023-23397, a Microsoft Outlook elevation of privilege flaw enabling the exploitation of TNEF files and initiating NTLM negotiation, leading to the acquisition of a target's NTLM password hash. Additionally, CVE-2023-38831, a WinRAR remote code execution flaw, allowed the execution of arbitrary code when attempting to view innocuous files within a ZIP archive.

#3

APT28 also leveraged other known exploits such as CVE-2022-30190 (FOLLINA), CVE-2021-34473 (PROXYSHELL), CVE-2021-40444, CVE-2021-42292, CVE-2021-42321, CVE-2020-17144, and CVE-2020-0688. In September 2023, APT28 deployed malicious emails from various Portugalmail addresses, exploiting a WinRAR vulnerability (CVE-2023-32231) in two distinct campaigns.

#4

The email senders masqueraded as geopolitical entities, using the BRICS Summit and a European Parliament meeting as subject lures to entice targets into opening the emails. Between September 2023 and November 2023, APT28 conducted multiple campaigns utilizing Mockbin for redirection. Mockbin, a third-party service for staging code in testing environments, had been previously abused by APT28. The threat actor sent enticing lures to government and defense sector targets, initiating a sequence of malicious activities through Mockbin.

#5

In November 2023, APT28 abandoned Mockbin in favor of direct delivery through InfinityFree URLs for initial filtering and redirection. Similar to Mockbin URLs, InfinityFree URLs used in delivery stages redirected irrelevant traffic to the MSN homepage. APT28 has consistently exploited these vulnerabilities for initial access, suggesting a likelihood of continued utilization as they anticipate targets may not have patched these vulnerabilities.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
APT28 (aka Fancy Bear, Forest Blizzard, ATK 5, BlueDelta, Fighting Ursa, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Group 74, Iron Twilight, ITG05, Pawn Storm, Sednit, SIG40, Snakemackerel, Sofacy, Strontium, Swallowtail, TA422, TAG-0700, T-APT-12, TG-4127, Tsar Team, UAC-0028)	Russia **MOTIVE** Information theft and espionage	Afghanistan, Albania, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, Czech Republic, Czechia, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, India, Iran, Iraq, Italy, Japan, Jordan, Kazakhstan, Latvia, Lithuania, Luxembourg, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, North Macedonia, Norway, Pakistan, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, SouthAfrica, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, United Arab Emirates, Uganda, United Kingdom, Ukraine, United States, Uzbekistan	Automotive, Aviation, Chemical, Construction, Defense, Diplomatic, Education, Electrical, Embassies, Energy, Engineering, Financial, Foreign Affairs, Government, Healthcare, Industrial, Information Technology, Intelligence organization, IT, Logistics, Media, NGOs, Oil and gas, Telecommunications, Think Tanks, Transit Pipeline, Transportation, Utilities

Recommendations

Patch and Update Vulnerable Software: Regularly update and patch all software and systems, particularly addressing known vulnerabilities. Ensure your software remains up to date by regularly checking for and applying the latest security updates and patches from the vendor patches can help prevent exploitation by threat actors like APT28.

Email Security: Implement robust email filtering solutions to reduce the likelihood of spam and phishing emails reaching users' inboxes, thereby helping to filter out potentially harmful content. Additionally, regularly monitor user account activity for any signs of unauthorized access, as unusual login locations or patterns could be indicators of a compromised account.

Assess Third-Party Security: Evaluate the cybersecurity practices of third-party vendors and contractors who have access to your network or data. Ensure they adhere to robust security standards.

Enhance Network Monitoring: Invest in robust network monitoring and intrusion detection systems to quickly detect and respond to suspicious activities. Early detection can mitigate the damage caused by potential breaches.

Harden Server Configurations: Apply server hardening techniques to reduce the attack surface by disabling unnecessary services, closing unused ports, and following industry best practices for server security.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
T1134 Access Token Manipulation	T1098 Account Manipulation	T1583 Acquire Infrastructure	T1588.006 Vulnerabilities
T1588.005 Exploits	T1560 Archive Collected Data	T1110 Brute Force	T1059 Command and Scripting Interpreter
T1586.002 Email Accounts	T1005 Data from Local System	T1140 Deobfuscate/Decode Files or Information	T1114 Email Collection
T1203 Exploitation for Client Execution	T1068 Exploitation for Privilege Escalation	T1498 Network Denial of Service	T1566.001 Spearphishing Attachment
T1566.002 Spearphishing Link	T1057 Process Discovery	T1221 Template Injection	T1204.001 Malicious Link
T1078 Valid Accounts	T1588 Obtain Capabilities		

Indicator of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://89.96.196[.]150:8080/
SHA256	e920461b94c0eea498264b092bde3db9835072ff46e4676e53817cbf7d275bd4, 6223cc22a0b2cade34a1964dfee16bfe373b578370b4ee4d286c5708ea0cc06d, 77cf5efde721c1ff598eeae5cb3d81015d45a74d9ed885ba48330f37673bc799, 339ff720c74dc44265b917b6d3e3ba0411d61f3cd3c328e9a2bae81592c8a6e5, 5b7ac39ee65f840b2c61fcab67c8b8190dc7822a11b2aae4d6ef7d542d107be4, e699a7971a38fe723c690f37ba81187eb8ed78e51846aa86aa89524c325358b4, ed56740c66609d2bbd39dc60cf29ee47743344a9a6861bee7c08ccfb27376506, bf5d03aa427a87e6d4fff4c8980ad5d5e59ab91dc51d87a25dd91df7de33beaa, 742ba041a0870c07e094a97d1c7fd78b7d2fdf0fcdaa709db04e2637a4364185, 8dba6356fdb0e89db9b4dad10fdf3ba37e92ae42d55e7bb8f76b3d10cd7a780c, 9a798e0b14004e01c5f336aeb471816c11a62af851b1a0f36284078b8cf09847, c6a91cba00bf87cdb064c49adaac82255cbec6fdd48fd21f9b3b96abf019916b, ec64b05307ad52f44fc0bfed6e1ae9a2dc2d093a42a8347f069f3955ce5aaa89, c89735e787dd223dac559a95cac9e2c0b6ca75dc15da62199c98617b5af007d3, 8cc664ff412fc80485d0af61fb0617f818d37776e5a06b799f74fe0179b31768, 1f4792dadaf346969c5e4870a01629594b6c371de21f8635c95aa6aba24ef24c, 6dfbea81bd299e35283ea9d183df415d63788fa7dfb7292f935c804f6396c8b2
File Names	brics_summit.rar.zip, CED_Policy_Backgrounder_BRICs_Summit_FINAL.pdf .cmd, bulletin.rar.zip, 35-2023_en.pdf .cmd, SEDE-PV-2023-10-09-1_EN.docx, SEDE-PV-2023-10-09-1_EN.lnk, desktop.ini,

TYPE	VALUE
File Names	command.cmd, SEDE-PV-2023-10-09-1_EN.zip, WindowsCodecs.dll, WINWORD.EXE, war.zip, ccc.cmd, war[PADDED].EXE, war.docx
HostName	downloadfile.infinityfreeapp[.]com, opendoc.infinityfreeapp[.]com, downloadingf.infinityfreeapp[.]com, downloaddoc.infinityfreeapp[.]com, opendocument.infinityfreeapp[.]com

Patch Details

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30190

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397

Update WinRAR version to 6.23 or later versions

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-40444

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42292

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42321

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34473

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-17144

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-0688

References

https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-week-after-week

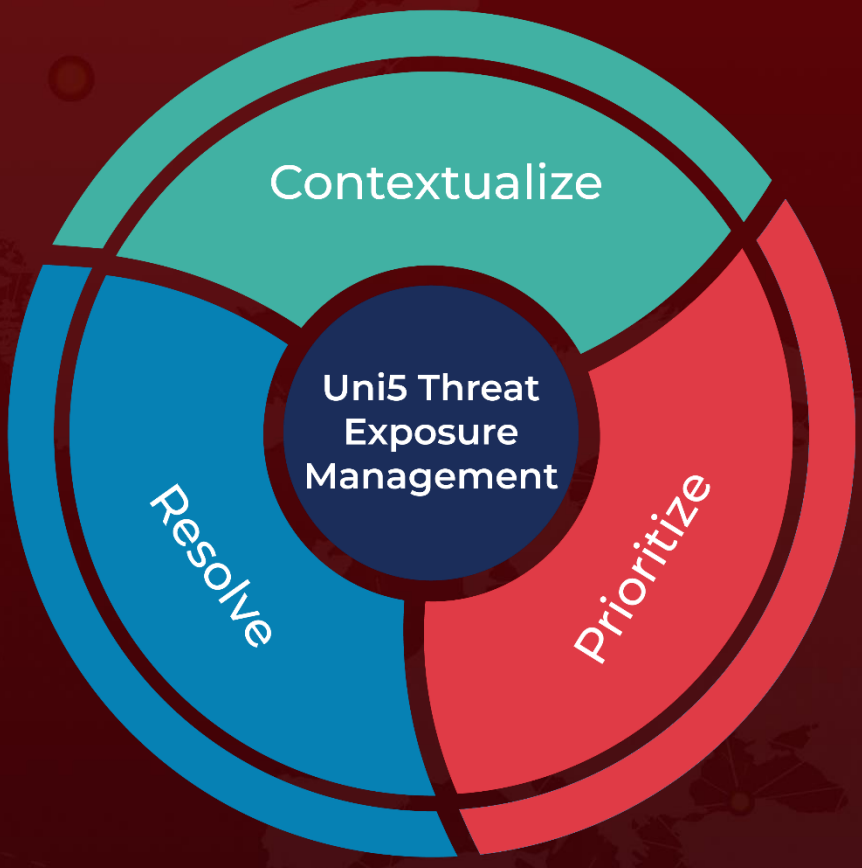
https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/

https://attack.mitre.org/groups/G0007/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 8, 2023 . 5:30 AM

More at www.hivepro.com