Hive Pro

Threat Level

Amber

THREAT ADVISORY

ACTOR REPORT

APT28 exploits Follina to deploy CredoMap

Date of Publication	Admiralty Code	TA Number
June 23, 2022	A1	TA2022133

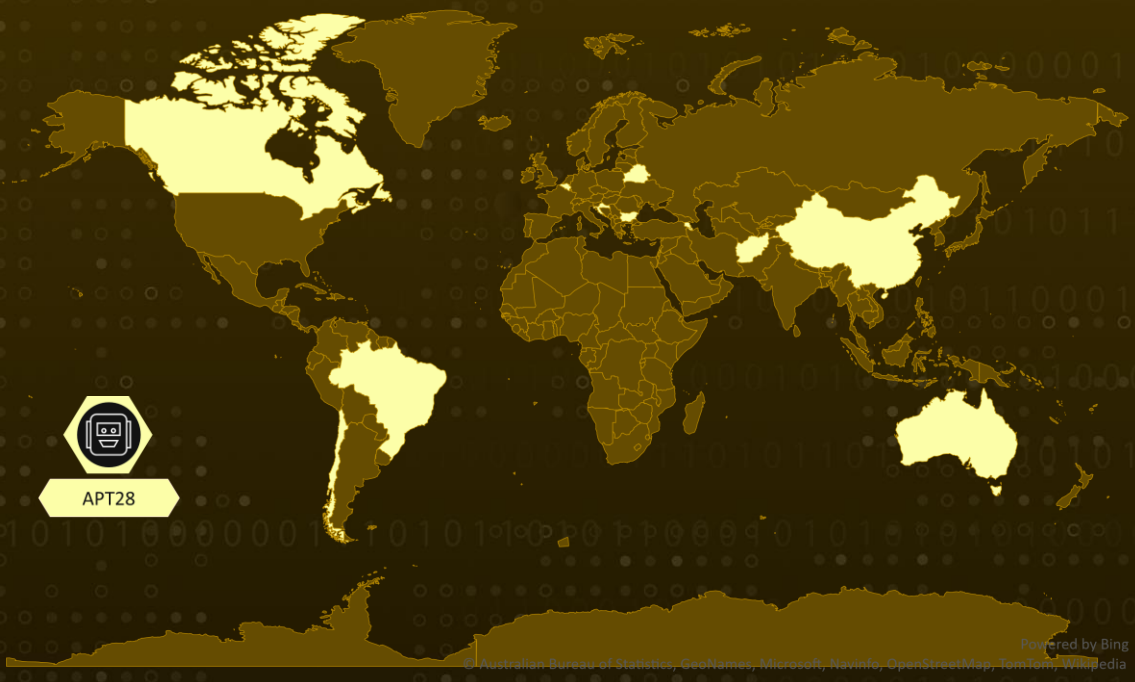
Summary

APT28 is targeting Ukraine with a phishing campaign that uses Follina to deploy CredoMap malware.

CVE Table

CVE	NAME	PATCH
CVE-2022-30190	Remote Code Execution(Follina)	✓

Actor Map



Potential MITRE ATT&CK TTPs

T1566.001 Phishing: Spearphishing Attachment	**T1566** Phishing	**TA0001** Initial Access	**T1204.002** User Execution: Malicious File
T1204 User Execution	**TA0002** Execution	**T1041** Exfiltration Over C2 Channel	**TA0010** Exfiltration

Technical Details

APT28, a Russian threat actor is conducting spear phishing attack by weaponizing documents with Follina,a zero-day remote code excecution vulnerability in Microsoft Windows Support Diagnostic Tool (MSDT). The threat actor is then deploying a malware named CredoMap which is used to exfiltrate data, cookies and account credentials from Google Chrome, Firefox and Microsoft Edge. This exfiltrated data is send to the attacker's command and control server by using IMAP protocol.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
APT28 (FANCY BEAR, STRONTIUM, Sofacy, Zebrocy, Sednit, Pawn Storm, TG-4127, Tsar-Team, Iron Twilight, Swallowtail, SNAKEMACKEREL, Frozen Lake)	Russia	Information Theft and Espionage	Afghanistan, Armenia, Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chile, China, Croatia, Cyprus, France, Georgia, Germany, Hungary, India, Iran, Iraq, Japan, Jordan, Kazakhstan, Latvia, Malaysia, Mexico, Mongolia, Montenegro, Netherlands, Norway, Pakistan, Poland, Romania, Slovakia, South Africa, South Korea, Spain, Sweden, Switzerland, Tajikistan, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan	Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-30190	Windows Server: 2008 – 2022 & Windows: 7 - 11 21H2	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	CWE-78

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	daaa271cee97853bf4e235b55cb34c1f03ea6f8d3c958f86728d41f418b0bf01, 14ae02c521b85e60b11393ffc0da5e25946c4775a84995800b73398df4bceffb, 9309fb2a3f326d0f2cc3f2ab837cfd02e4f8cb6b923b3b2be265591fd38f4961, 2318ae5d7c23bf186b88abecf892e23ce199381b22c8eb216ad1616ee8877933
MD5	eafa11070f213f16efc030f625a423d1, ab6c70af19f7d41a443feb8ccb57d264, 56a504a34d2cfbfc7eaa2b68e34af8ad, d3bddb5de864afd7e4f5e56027f4e5ea
Network	hXXp://kitten-268.frge[.]io/article.html, hXXp://kompartpomiar[.]pl/grafika/SQLite.Interop.dll, hXXp://kompartpomiar[.]pl/grafika/docx.exe, 162[.]241.216.236, kitten-268.frge[.]io, frge[.]io, kompartpomiar[.]pl , seo@specialityllc[.]com,

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

References

https://blog.malwarebytes.com/threat-intelligence/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine/

https://thehackernews.com/2022/06/russian-hackers-exploiting-microsoft.html

https://cert.gov.ua/article/341128

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

June 23, 2022 • 7:45 AM

More at www.hivepro.com