

Date of Publication
May 13, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

06 to 12 MAY 2024

Table Of Contents

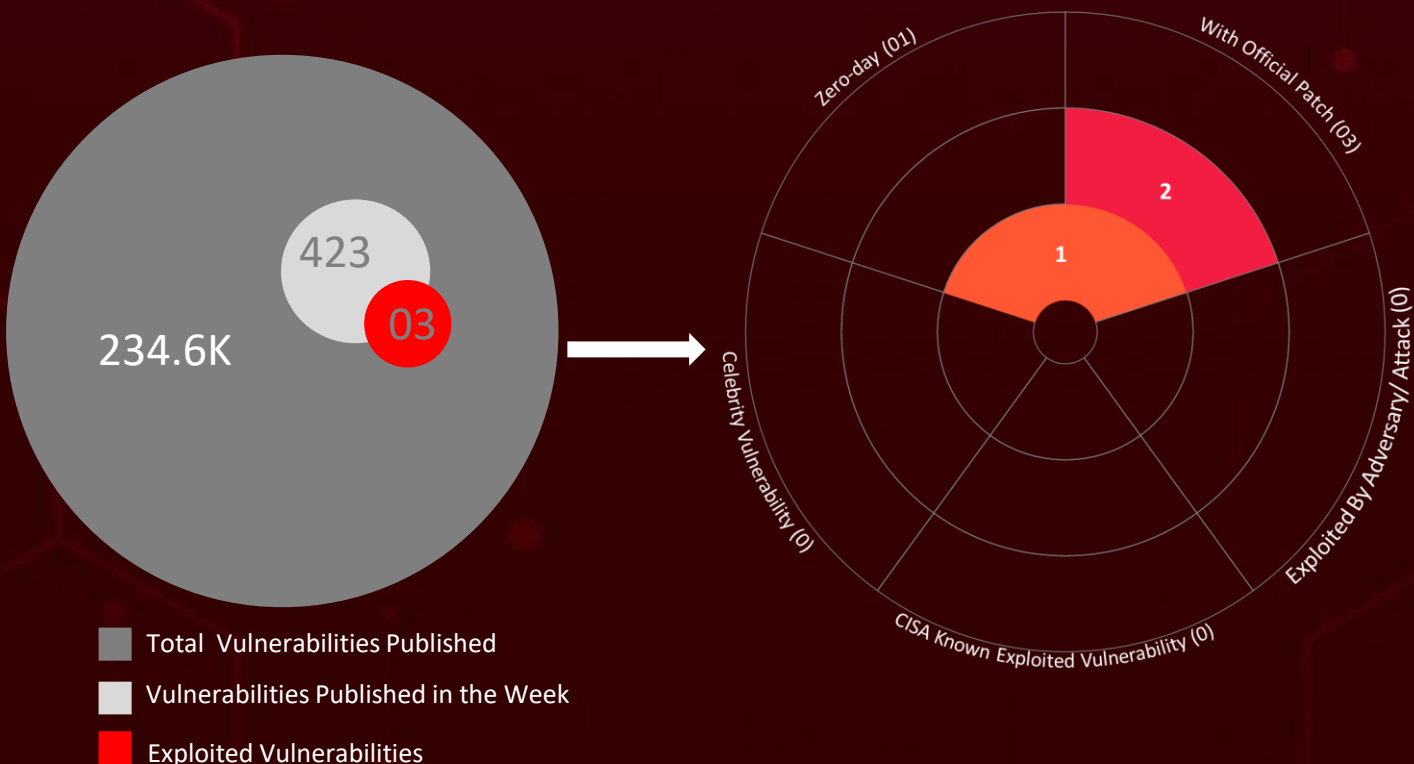
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	11
<u>Adversaries in Action</u>	13
<u>Recommendations</u>	15
<u>Threat Advisories</u>	16
<u>Appendix</u>	17
<u>What Next?</u>	21

Summary

HiveForce Labs has recently unveiled several profound revelations within the domain of cybersecurity threats. Within the span of the past week alone, HiveForce Labs has unearthed **six** executed attacks, disclosed **three** vulnerabilities, and pinpointed **two** active adversaries. These discoveries underscore the persistent and mounting peril posed by cyber intrusions.

Furthermore, HiveForce Labs has unveiled that **APT42** has been observed targeting entities across both the **Middle East and Western** regions, penetrating their cloud infrastructures and corporate networks through adept social engineering tactics. Meanwhile, **Cuttlefish** has been detected infiltrating routers at both enterprise and small office/home office (SOHO) levels, clandestinely monitoring data transmissions, and pilfering authentication credentials.

Moreover, the **zero-day** vulnerability found in Google Chrome's Visuals component, officially designated as **CVE-2024-4671**, has been rectified by Google in its recent security patch. Simultaneously, the emergence of **RokRAT** malware is specifically geared toward **South Korean** users, employing LNK files masquerading within evidently genuine documents. These attacks are on the rise, posing a significant and immediate threat to users worldwide.



High Level Statistics

6

Attacks
Executed

- [Nicecurl](#)
- [Tamecat](#)
- [Cuttlefish](#)
- [HijackLoader](#)
- [zEus](#)
- [RokRAT](#)

3

Vulnerabilities
Exploited

- [CVE-2023-49606](#)
- [CVE-2023-40000](#)
- [CVE-2024-4671](#)

2

Adversaries in
Action

- [APT42](#)
- [APT28](#)



Insights

Lockdown

Tinyproxy: CVE-2023-49606's Remote Code Execution Risk

Breaking Down APT42's

Two-Fold Attack Employing Nicecurl and Tamecat Backdoors

Chrome's Critical Patch:

Google Chrome's Urgent Call for CVE-2024-4671 Patching

Riding the Waves of Cyber

Threats: 'Cuttlefish' Malware Lurking in Routers

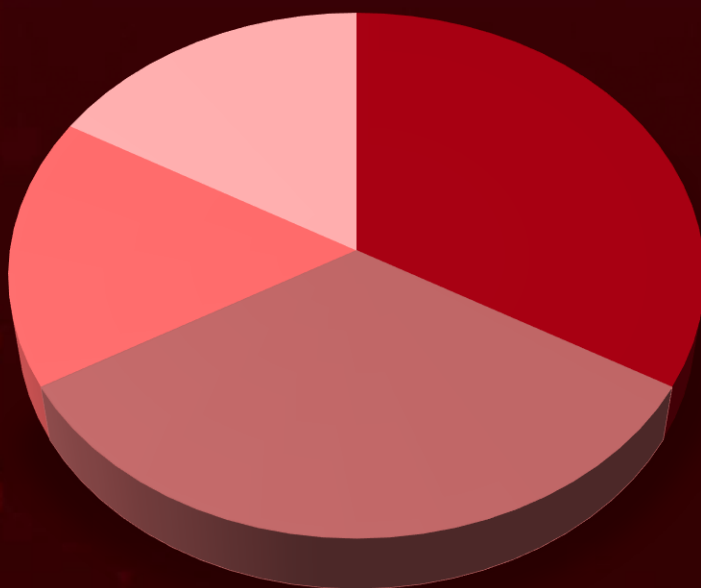
Stealth Redefined:

HijackLoader's Evolution in Evasion Tactics

Screensaver or Saboteur?

zEus Stealer's Subversive Infiltration Strategy

Threat Distribution



Information Stealer Backdoor RAT Loader

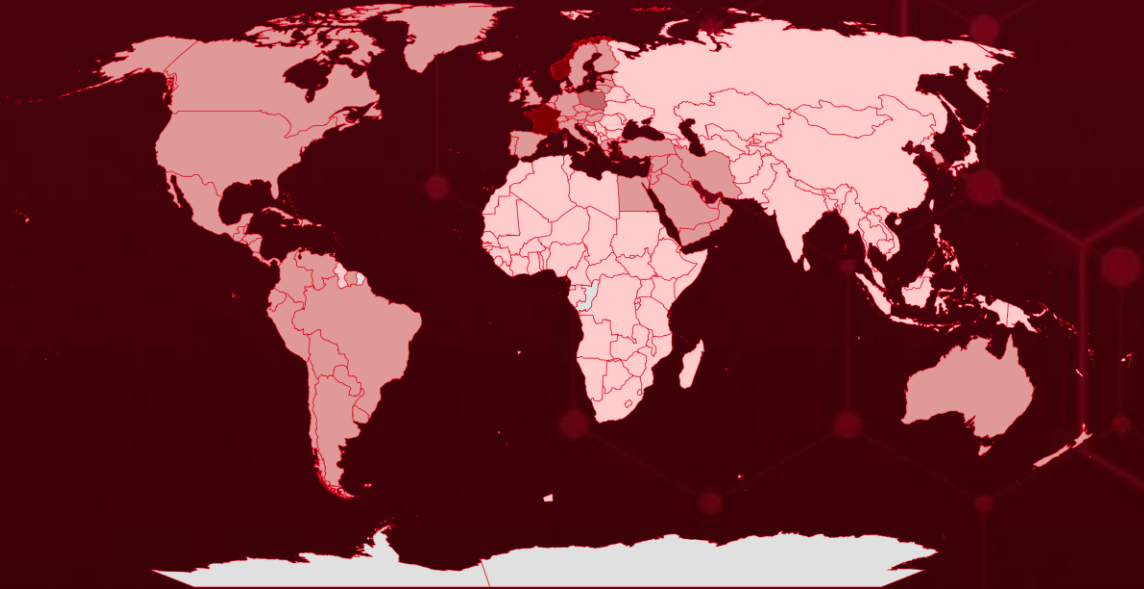


Targeted Countries

Most



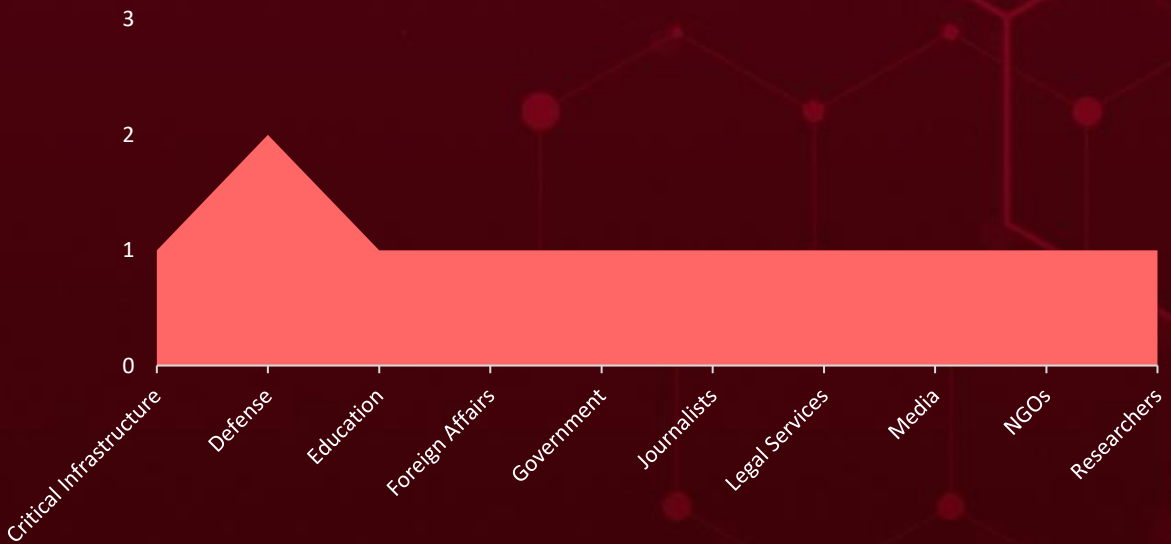
Least



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Countries	Countries	Countries	Countries
France	Colombia	Estonia	Trinidad and Tobago
Norway	Antigua and Barbuda	Netherlands	Iran
Poland	Costa Rica	Finland	United Arab Emirates
Saudi Arabia	Paraguay	Nicaragua	Iraq
Malta	Croatia	Andorra	United States
Venezuela	Saint Vincent and the Grenadines	Oman	Ireland
Australia	Cuba	Germany	Vatican City
Palestine	Slovenia	Panama	Israel
Austria	Cyprus	Peru	Yemen
Syria	Sweden	Argentina	Italy
Bahrain	Czech Republic	Portugal	Lebanon
Latvia	Turkey	Greece	Bahamas
Barbados	Denmark	Qatar	Benin
New Zealand	Uruguay	Greenland	American Samoa
Belgium	Dominica	Saint Lucia	French Polynesia
Saint Kitts and Nevis	Jamaica	Grenada	Akrotiri and Dhekelia
Belize	Dominican Republic	San Marino	East Timor
Spain	Kuwait	Guatemala	Ghana
Bolivia	Ecuador	Slovakia	Tokelau
United Kingdom	Liechtenstein	Haiti	Gibraltar
Brazil	Egypt	South Korea	Palau
Jordan	Luxembourg	Honduras	Bonaire
Canada	El Salvador	Suriname	Botswana
Lithuania	Mexico	Hungary	Bermuda
Chile		Switzerland	
Monaco		Iceland	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059

Command and Scripting Interpreter

T1027

Obfuscated Files or Information

T1055

Process Injection

T1056

Input Capture

T1588.006

Vulnerabilities

T1041

Exfiltration Over C2 Channel

T1588

Obtain Capabilities

T1140

Deobfuscate/Decode Files or Information

T1082

System Information Discovery

T1059.001

PowerShell

T1190

Exploit Public-Facing Application

T1057

Process Discovery

T1068

Exploitation for Privilege Escalation

T1566

Phishing

T1204.002

Malicious File

T1010

Application Window Discovery

T1588.005

Exploits

T1547

Boot or Logon Autostart Execution

T1033

System Owner/User Discovery

T1059.007

JavaScript



Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Nicecurl</u>	NICECURL is a backdoor coded in VBScript, skilled at obtaining extra modules for execution. These modules include data mining and executing commands as needed. NICECURL communicates securely over HTTPS.	Spear phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Information Theft, Espionage	PATCH LINK
APT42 (aka UNC2448)			
IOC TYPE	VALUE		
MD5	d5a05212f5931d50bb024567a2873642, 347b273df245f5e1fcbef32f5b836f1d, 2f6bf8586ed0a87ef3d156124de32757		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Tamecat</u>	TAMECAT serves as a PowerShell entry point capable of running custom PowerShell or C# code. It initiates its operations through a compact VBScript downloader, which utilizes Windows Management Instrumentation (WMI) to assess the antivirus solutions active on the target system.	Spear phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			
ASSOCIATED ACTOR		Information Theft, Espionage	PATCH LINK
APT42 (aka UNC2448)			
IOC TYPE	VALUE		
MD5	d7bf138d1aa2b70d6204a2f3c3bc72a7, 081419a484bbf99f278ce636d445b9d8, c3b9191f3a3c139ae886c0840709865e		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Cuttlefish</u>	<p>Cuttlefish malware has been detected penetrating enterprise-grade as well as small office/home office (SOHO) routers with the intent of covertly monitoring data transmissions and pilfering authentication credentials.</p> <p>Employing a zero-click method, Cuttlefish seamlessly siphons data from users and devices situated within the confines of the targeted network's perimeter.</p>	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Information Stealer		Credential Theft, Espionage, Information Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738ad3247f9c818478, 10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62702f18d919e89, 1168e97ccf61600536e93e9c371ee7671bae4198d4bf566550328b241ec52e89		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>HijackLoader (aka IDAT Loader)</u>	<p>The modular malware loader known as HijackLoader has undergone notable evolution, marked by the adoption of innovative evasion tactics. A fresh variant of this loader utilizes a PNG image to distribute subsequent malware stages. This advanced iteration is outfitted with numerous modules dedicated to injecting and executing code, thus amplifying both its efficacy and stealth capabilities.</p>	Unknown	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Information Theft and compromised systems	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	7a8db5d75ca30164236d2474a4719046a7814a4411cf703ffb702bf6319939d7, d95e82392d720911f7eb5d8856b8ccd2427e51645975cdf8081560c2f6967ffb,		




The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>zEus</u>	zEus stealer has adeptly infiltrated both a source pack distributed on YouTube and a Minecraft pack concealed within a WinRAR file, cleverly posing as a Windows screensaver. Its ability to gather diverse data effectively poses a significant threat, enhancing the potential for future attacks.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	Microsoft Windows
			PATCH LINK
			-
TYPE			
Information Stealer			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
SHA256	aabfbef31ab073d99c01ecae697f66bbf6f14aa5d9c295c7a6a548879381fb24, c9687714cf799e5ce9083c9afa3e622c978136d339fc9c15e272b0df9cd7e21c, d9d394cc2a743c0147f7c536cbb11d6ea070f2618a12e7cc0b15816307808b8a,		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>RokRAT</u>	The RokRAT malware spreads through LNK files hidden within seemingly genuine documents. Upon activation, this malicious software triggers PowerShell commands, which in turn initiate the execution of additional files. This process enables the extraction of user data, which is subsequently sent to the perpetrators' command and control (C2) servers.	Unknown	-
		IMPACT	AFFECTED PRODUCTS
		Information Theft, Espionage	-
			PATCH LINK
			-
TYPE			
RAT			
ASSOCIATED ACTOR			
-			
IOC TYPE	VALUE		
MD5	b85a6b1eb7418aa5da108bc0df824fc0, 358122718ba11b3e8bb56340dbe94f51, 35441efd293d9c9fb4788a3f0b4f2e6b,		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.


Vulnerabilities Exploited


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-49606		Tinyproxy 1.11.1 and Tinyproxy 1.10.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:tinyproxy:tinyproxy:1.10.0:*:*:*:*:* cpe:2.3:a:tinyproxy:tinyproxy:1.11.1:*:*:*:*:*	-
Tinyproxy HTTP Connection Headers Use-After-Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter	https://github.com/tinyproxy/tinyproxy/releases/tag/1.11.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-40000		WordPress LiteSpeed Cache Plugin versions prior 5.7.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:litespeed_technologies:litespeed_cache_plugin:*:*:*:*:*	-
WordPress LiteSpeed Cache Plugin Cross Site Scripting Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise	https://wpscan.com/vulnerability/dd9054cc-1259-427d-a4ad-1875b7b2b3b4/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-4671</u>		Google Chrome prior to 124.0.6367.201	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:google:chrome :*:*:*:*:*:*	-
Google Chrome Visuals Use After Free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1059: Command and Scripting Interpreter; T1189: Drive-by Compromise; T1203: Exploitation for Client Execution	https://www.google.com/intl/en/chrome/?standalone=1

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>APT42 (aka UNC2448)</u>	Iran	NGOs, media organizations, academia, legal services, researchers, journalists, defense, foreign affairs	Western and Middle Eastern
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOM WARE	AFFECTED PRODUCTS
	-	Nicecurl, Tamecat	-
TTPs			
TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0006: Credential Access; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1598: Phishing for Information; T1190: Exploit Public-Facing Application; T1059: Command and: Scripting Interpreter; T1059.007: JavaScript; T1059.005: Visual Basic; T1059.001: PowerShell; T1566: Phishing; T1566.002: Spearphishing Link; T1027: Obfuscated Files or Information; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1047: Windows Management Instrumentation; T1204: User Execution; T1204.001: Malicious Link; T1036: Masquerading; T1056: Input Capture; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1537: Transfer Data to Cloud Account; T1140: Deobfuscate/Decode Files or Information; T1555: Credentials from Password Stores			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES	
 <p><u>APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard, BlueDelta, TA422, Fighting Ursa, Blue Athena)</u></p>	Russia	Government, Defense, Critical Infrastructure	Poland	
	MOTIVE Information theft and espionage			TARGETED CVEs
	-	-	-	
	TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1204: User Execution; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1053.005: Scheduled Task; T1057: Process Discovery; T1082: System Information Discovery; T1204.002: Malicious File; T1029: Scheduled Transfer; T1007: System Service Discovery; T1598.003: Spearphishing Link; T1562.004: Disable or Modify System Firewall; T1564.001: Hidden Files and Directories; T1053: Scheduled Task/Job; T1055: Process Injection				

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actors **APT42, APT28**, and malware **Nicecurl, Tamecat, Cuttlefish, HijackLoader, zEus, RokRAT**.

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **three exploited vulnerabilities**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT42, APT28**, and **malware NICECURL, Cuttlefish, HijackLoader, zEus, RokRAT** in Breach and Attack Simulation(BAS).

Threat Advisories

[APT42's Operations Employ "Nicecurl" and "Tamecat" Malwares](#)

[Tinyproxy Vulnerability Exposes Hosts to Remote Code Execution](#)

[Cuttlefish Malware Silent Stalkers of Router Traffic](#)

[HijackLoader Enhances Its Arsenal with New Evasion Techniques](#)

[zEus Stealer's Undercover Operation on YouTube and Minecraft](#)

[BIG-IP Next Central Manager Flaws Lead To Administrative Control](#)

[Hackers Exploit LiteSpeed Cache for WordPress Site Takeover](#)

[APT28's Intricate Email Campaign Against Poland](#)

[Google Chrome Fixes Zero-Day CVE-2024-4671 Exploited in the Wild](#)

[The RokRAT Epidemic in South Korea](#)

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>Nicecurl</u>	MD5	d5a05212f5931d50bb024567a2873642, 347b273df245f5e1fcbef32f5b836f1d, 2f6bf8586ed0a87ef3d156124de32757, 13aa118181ac6a202f0a64c0c7a61ce7, c23663ebdfbc340457201dbec7469386, 853687659483d215309941dae391a68f
	Domain	drive-file-share[.]site, prism-west-candy[.]glitch[.]me
<u>Tamecat</u>	MD5	d7bf138d1aa2b70d6204a2f3c3bc72a7, 081419a484bbf99f278ce636d445b9d8, c3b9191f3a3c139ae886c0840709865e, dd2653a2543fa44eaefff3ca82fe3513, 9c5337e0b1aef2657948fd5e82bdb4c3
	Domain	tnt200[.]mywire[.]org, accurate-sprout-porpoise[.]glitch[.]me
<u>Cuttlefish</u>	URL	hxxp://209[.]141[.]49[.]178/dajfdfsadsfa/arm, hxxp://209[.]141[.]49[.]178/dajfdfsadsfa/i386, hxxp://209[.]141[.]49[.]178/dajfdfsadsfa/i386_i686, hxxp://209[.]141[.]49[.]178/dajfdfsadsfa/i386_x64, hxxp://209[.]141[.]49[.]178/dajfdfsadsfa/misp32, hxxp://209[.]141[.]49[.]178/dajfdfsadsfa/misp64, hxxp://209[.]141[.]49[.]178/r/arm_sniff, hxxp://209[.]141[.]49[.]178/r/i386_i686_sniff, hxxp://209[.]141[.]49[.]178/r/i386_sniff, hxxp://209[.]141[.]49[.]178/r/i386_x64_sniff, hxxp://209[.]141[.]49[.]178/r/mips32_sniff, hxxp://209[.]141[.]49[.]178/r/mips64_sniff, hxxp://209[.]141[.]49[.]178/r/s[.]sh,

Attack Name	TYPE	VALUE
Cuttlefish	URL	hxxp://209[.]141[.]49[.]178/s, hxxps://107[.]189[.]28[.]251:443/rules, hxxps://198[.]98[.]56[.]93:443/rules, hxxps://198[.]98[.]56[.]93:443/rulesinit, hxxps://198[.]98[.]56[.]93:443/upload, hxxps://205[.]185[.]122[.]121/rules, hxxps://205[.]185[.]122[.]121/rulesinit, hxxps://205[.]185[.]122[.]121/upload, hxxps://kkthreas[.]com, hxxps://kkthreas[.]com/upload, hxxps://pp[.]kkthreas[.]com
	SHA256	07df37d8168e911b189bbe0912b4842fa1fe48d5264e99738a d3247f9c818478, 10a4edbbb852a1b01fc6fbf0aa1407bc8589432bddb2001ae62 702f18d919e89, 1168e97ccf61600536e93e9c371ee7671bae4198d4bf5665503 28b241ec52e89, 23c2e7ff2602e5f76b3f2c354761ef39966facb3b12ed0555181 6f482d4d5608, 2ed174523bd80a93b7d09940d375f9c0d71e1ce8ecffb2320e0 2a78f4b601408, 2f0911fb892d448910c36a37c9fbdec8c73ccfecc274854b1fa05 3fb1cc2369b, 3d9ee05c0841ad65547c0cc8516d092cff48dad5e7bbf97c99d dd44ee94a24bc, 44b769be0c2a807082a9bfd2f33fdc744552c5c7ca88a812ef4b d0393a50f132, 4aa23fbdc27d317c6e54481b6d884b962adf6e691a4731c859d daf9af09822c6, 6295d5cb21c441066d2da81a76440bcac9bd5a7830fc9faea96 68bd0b2015046, 70693211cd0b14a7463b39b2fa801ce1fdefc85c7f3e003772d1 b4deeb78efde, 73cf20675639c18c04381b5efd7d628736d149734280988f553 58e301c1d9bb8, 94812d391160e4fce821701b944cfd8f5fd9454b3cbb8e8974d 1dc259310e500, 99d5cf32f8198e99c530be4f5e05487e280bacdb8ef26aaf38dc 20e301aad75f, eb7a7ab952080f66c82fe8350da131ce0d7766f203bd4d97b07 98b4f59283a27
HijackLoader	SHA256	7a8db5d75ca30164236d2474a4719046a7814a4411cf703ffb7 02bf6319939d7, d95e82392d720911f7eb5d8856b8ccd2427e51645975cdf808 1560c2f6967ffb,

Attack Name	TYPE	VALUE
<u>HijackLoader</u>	SHA256	fcadcee5388fa2e6d4061c7621bf268cb3d156cb879314fa2f518d15f5fa2aa2, f37b158b3b3c6ef9f6fe08d0056915fc7e5a220d1dabb6a2b62364ae54dca0f1, e0a4f1c878f20e70143b358ddaa28242bac56be709b5702f3ad656341c54fb76, cf42af2bdcec387df84ba7f8467bbcdad9719df2c524b6c9b7fff a55cfdc8844, c215c0838b1f8081a11ff3050d12fcfe67f14442ed2e18398f0c 26c47931df44, 9b15cb2782f953090caf76efe974c4ef8a5f28df3dbb3eff135d4 4306d80c29c, 56fd2541a36680249ec670d07a5682d2ef5a343d1fecbcbf2c3 da86bd546af85, 1fbf01b3cb97fda61a065891f03dca7ed9187a4c1d0e8c5f24ef 0001884a54da
<u>zEus</u>	SHA256	aabfbef31ab073d99c01ecae697f66bbf6f14aa5d9c295c7a6a5 48879381fb24, c9687714cf799e5ce9083c9afa3e622c978136d339fc9c15e27 2b0df9cd7e21c, d9d394cc2a743c0147f7c536cbb11d6ea070f2618a12e7cc0b1 5816307808b8a, c2c8a7050b28d86143f4d606a6d245b53c588bc547a639094f ce857962246da4, be9ea302bcfb52fbfdf006b2df8357388cd4c078059aabc5b59 28676c3361e50, 9d3409852348caa65d28e674008dd6bb986eed4fb507957c7a 8b73a41e00be70, b6e8b612e99c54dd98af1756f7c9b8a8c19e31ed9b2836878c 2a5144563ff1b2, 8a2f6d5f6cf7d1a7534454e3c3007337b71d7da470e86f7636e b02d68b2db8cc, df6156fdbbcc7b6f8c9cb4c5c1b0018fc3f1e1ca7d949b5538ec 27dc86d026a4, 5840f3e43a0c635be94b5fbf2e300d727545371b582361a526 82b4a9e08bcebd, 51ede75315d858209f9aa60d791c097c18d38f44b9d050b555 ff1f4de0ae672d, d1865d2aaf11e3f8bccefe9c4847510234f14aaa5378ce9e8e9 7553537cf2ca1, 9ba19d614af029c3c198b576ccdf1de87d80ac14b12103e8a1 5376229a2a7860, 6063c8285e13d10eabbe363e2ab0d8748bcd595b470698e0cf fee31ba255a566, d1a18b436f947611914ced09e4465b49807cec4f3a62b0973c 9017b6d82c9f70,

Attack Name	TYPE	VALUE
<u>zEus</u>	SHA256	1cdd580176eeb4342a0333b50454da061e473358274e6e543df1411186c12042, ed59a797521db06abdf4c88dad7b1666e5978aaa6670a5952a55b7e11f7b790e, 2ceae724f0e96e2d8c47296dd1e73ac592e22ee3288eabf11c8d039c6d6d4f8b, 03983b56d8b1a6cc43109f6cd67a13666367595a2ea07766127cb1fe4d4bb1a5, 9940da9d02d29489c3e26d27feb15b6f4bbf49547b962592125441917c952f12, fbf967295dac00f1e9cb67e9a40b6729b003dd12cf022eb15d626df09716442d, 4e0a96ab28570936d095ac3910dcd239c7ceeb2b38a070468404584f8b902dd1, 20009fd157a898ad6d50fae6b8127056c5b1f50e31f90f01d2e6c13e6b4c38f8
<u>RokRAT</u>	MD5	b85a6b1eb7418aa5da108bc0df824fc0, 358122718ba11b3e8bb56340dbe94f51, 35441efd293d9c9fb4788a3f0b4f2e6b, 68386fa9933b2dc5711dffcee0748115, bd07b927bb765ccfc94fadbc912b0226, 6e5e5ec38454ecf94e723897a42450ea, 3114a3d092e269128f72cfd34812ddc8, bd98fe95107ed54df3c809d7925f2d2c

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

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

May 13, 2024 • 6:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com