Date of Publication
June 10, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

03 to 09 JUNE 2024

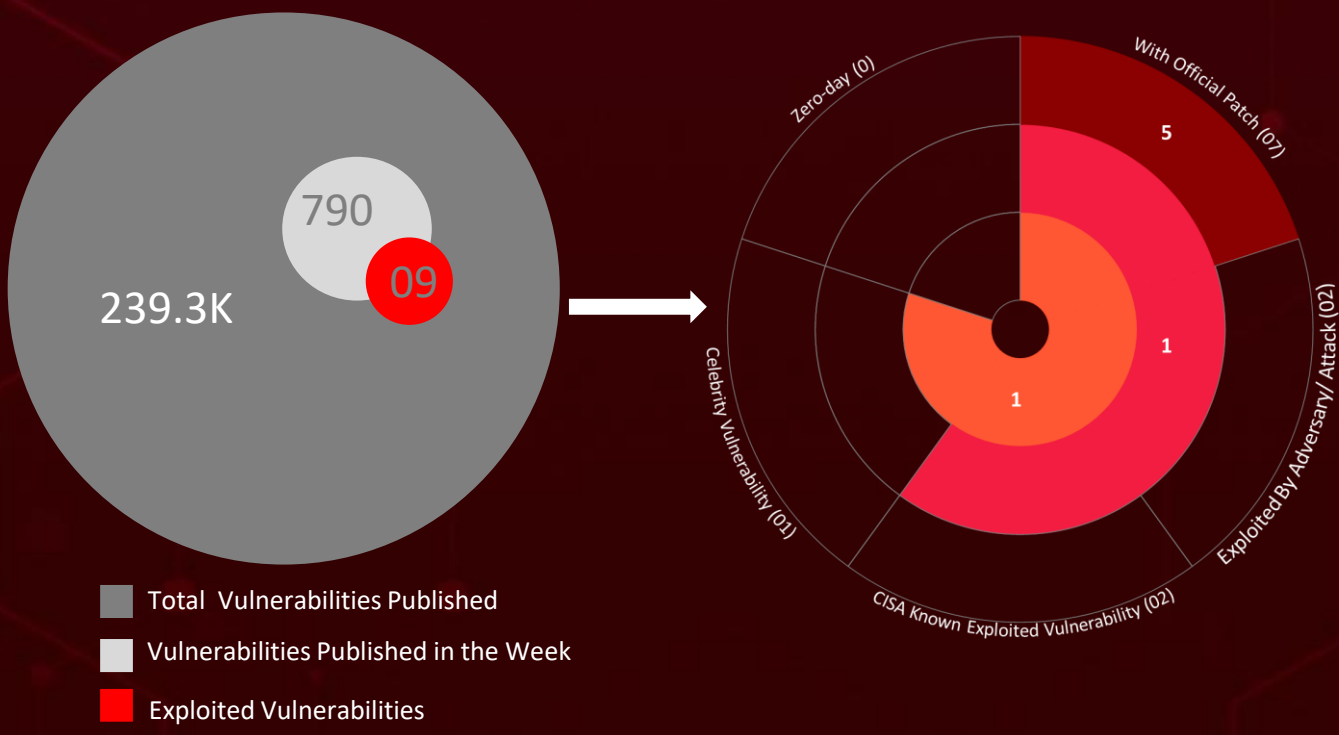
Table Of Contents

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week alone, HiveForce Labs has detected **six** executed attacks, reported **nine** vulnerabilities, and identified **two** active adversaries. These findings highlight the relentless and escalating danger of cyber intrusions.

Additionally, a new banking trojan, **CarnavalHeist**, has been targeting Brazilian users since February 2024. In another development, a sophisticated cyber attack has been identified in Ukraine, involving the threat actor known as **Operation Ghostwriter**.

Furthermore, the data theft operation by **LilacSquid**, a newly identified threat actor, closely mirrors the tactics of North Korean APT groups and has been operational since at least 2021. The ransomware group **TargetCompany** has developed a new Linux variant aimed at VMware ESXi environments, increasing the potential for disruption and ransom payments. These rising threats pose a significant and immediate danger to users worldwide.



High Level Statistics

6
Attacks Executed

9
Vulnerabilities Exploited

2
Adversaries in Action

- PurpleInk
- CarnavalHeist
- TargetCompany
- RansomHub
- Knight ransomware
- Muhstik

- CVE-2024-1800
- CVE-2024-4358
- CVE-2024-29972
- CVE-2024-29973
- CVE-2024-29974
- CVE-2024-29975
- CVE-2024-29976
- CVE-2020-1472
- CVE-2023-33246

- LilacSquid
- Operation Ghostwriter

Insights

From Excel to Exploit: Ukraine Faces New Cyber Attack with Cobalt Strike

Knight Reborn: **RansomHub**'s Strategic Entry into RaaS Market

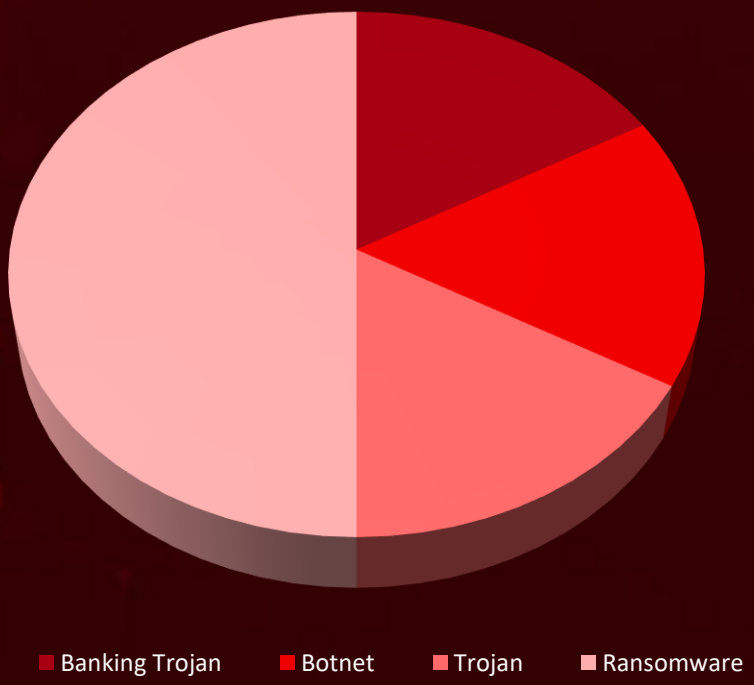
Mimicking the Masters: **LilacSquid**'s North Korean APT-Style Cyber Operations

Ransomware Rampage: **TargetCompany**'s Custom Shell Script Attacks ESXi

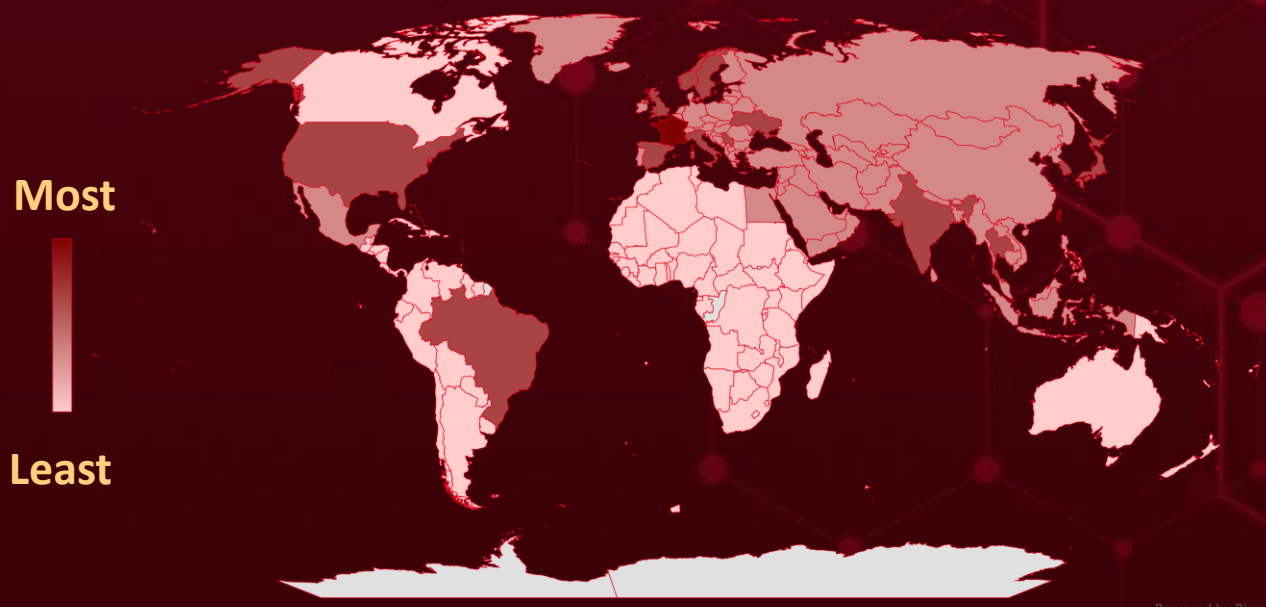
CarnavalHeist's Credential Carnage: A New Threat to Brazil's Banking Sector

RocketMQ Vulnerability Leads to **Muhstik** Malware Infestation

Threat Distribution

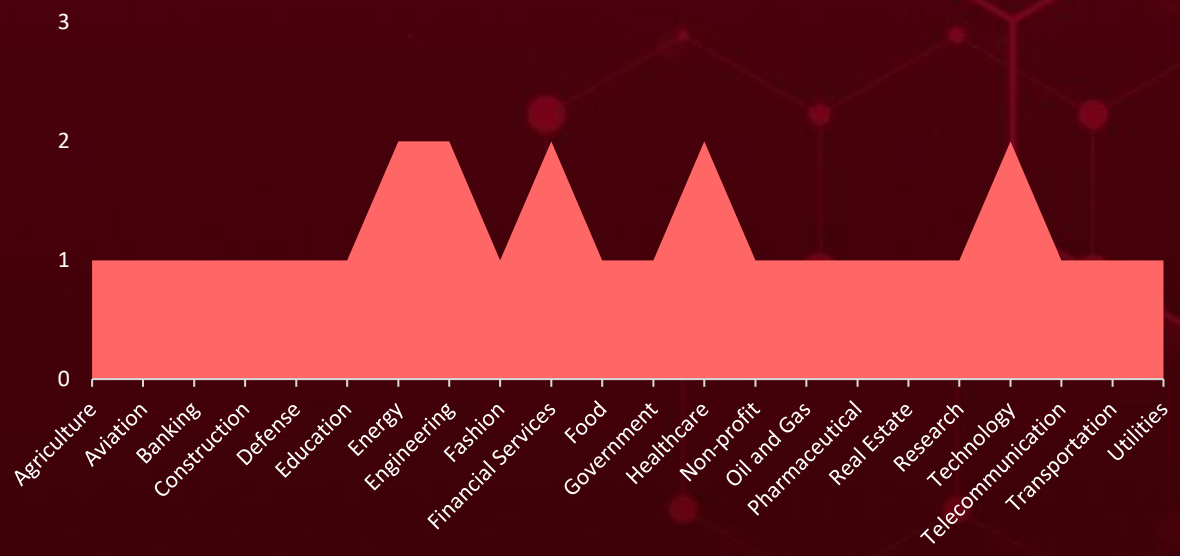


Targeted Countries



Countries	Countries	Countries	Countries
France	Qatar	Guernsey	Jordan
Taiwan	Czech Republic	Turkmenistan	Azerbaijan
South Korea	Slovenia	Hong Kong	Kazakhstan
Norway	Denmark	Malaysia	Slovakia
Brazil	Syria	Hungary	Kosovo
India	East Timor	Malta	Bahrain
Serbia	United Arab Emirates	Iceland	Kuwait
Italy		Moldova	Bangladesh
Spain	Egypt	Åland	Armenia
Sweden	Mexico	Mongolia	Svalbard
Thailand	Estonia	Indonesia	Uzbekistan
Japan	Montenegro	Myanmar	Switzerland
Ukraine	Faroe Islands	Iran	Vietnam
United Kingdom	North Korea	Netherlands	Belgium
United States	Finland	Iraq	Abkhazia
Palestine	Oman	North Macedonia	Bhutan
Maldives	Akrotiri and Dhekelia	Ireland	Liechtenstein
Sri Lanka		Austria	Turkey
Brunei	Poland	Isle of Man	Lithuania
Nepal	Georgia	Pakistan	Bosnia and Herzegovina
Bulgaria	Russia	Israel	
Saudi Arabia	Germany	Philippines	Luxembourg
Cambodia	Singapore	Albania	Afghanistan
Transnistria	Gibraltar	Portugal	Macao
China	South Ossetia	Andorra	Kyrgyzstan
Monaco	Greece	Romania	Vatican City
Croatia	Belarus	Jersey	Laos
Northern Cyprus	Greenland	San Marino	Yemen
Cyprus	Tajikistan		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1190** Exploit Public-Facing Application	**T1105** Ingress Tool Transfer	**T1082** System Information Discovery	**T1041** Exfiltration Over C2 Channel
T1055 Process Injection	**T1027** Obfuscated Files or Information	**T1588.006** Vulnerabilities	**T1071** Application Layer Protocol	**T1547** Boot or Logon Autostart Execution
T1587.001 Malware	**T1036** Masquerading	**T1566** Phishing	**T1057** Process Discovery	**T1588** Obtain Capabilities
T1059.004 Unix Shell	**T1486** Data Encrypted for Impact	**T1068** Exploitation for Privilege Escalation	**T1547.001** Registry Run Keys / Startup Folder	**T1070** Indicator Removal

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PurpleInk	A customized version of QuasarRAT, termed PurpleInk, is used as the primary implant after successfully breaching vulnerable internet-exposed application servers. PurpleInk is extensively obfuscated and highly versatile. It can execute new applications, perform file operations, gather system information, and enumerate directories and running processes.	Exploiting Vulnerable Application Servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Compromised Infrastructure, Information Theft, Resource Hijacking	-
ASSOCIATED ACTOR			**PATCH LINK**
LilacSquid			-
IOC TYPE	**VALUE**		
SHA256	2eb9c6722139e821c2fe8314b356880be70f3d19d8d2ba530adc9f466ffc67d8		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CarnavalHeist	CarnavalHeist is a new banking trojan malware that stands out for using a Python-based loader. It targets banking desktop applications, stealing credentials through overlay attacks and keylogging.	Spam emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Credential Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	c300749ea44f886be1887b3e19b946efbdbbc3e1bf3e416c78cfbff8d23bf70a, 1b4f44a00f61b3e0c8cd6c3125f03b6d4897d6ab90c8a6dc899ed96acee80dd6, 8424e76c9a4ee7a6d7498c2f6826fcde390616dc65032bebf6b2a6f8fbf4a535		

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
TargetCompany	The TargetCompany ransomware group has developed a new Linux variant using a custom shell script for payload delivery and execution. It targets VMWare ESXi environments to increase disruption and the chances of ransom payment.	Exploiting Public-Facing Application	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage, Financial Loss	Windows, Linux, VMWare ESXi
Ransomware			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA1	dffa99b9fe6e7d3e19afba38c9f7ec739581f656, 2b82b463dab61cd3d7765492d7b4a529b4618e57,		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RansomHub	RansomHub, a newly emerged Ransomware-as-a-Service (RaaS) entity, has swiftly ascended to become one of the most prominent ransomware groups in operation. It is suspected to be an updated and rebranded iteration of the Knight ransomware. Both RansomHub's payload is written in Go, with most variants obfuscated using Gobfuscate.	Exploiting the Zerologon vulnerability	CVE-2020-1472
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Financial Gain, and Compromised infrastructure	Microsoft Netlogon
Ransomware			
ASSOCIATED ACTOR			PATCH LINK
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472
IOC TYPE	VALUE		
SHA256	02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292, 34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087, 7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a		

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
Knight ransomware	Knight Snatch, developed in Go, can initiate a reboot of an endpoint in safe mode before starting encryption. The source code for Knight, initially known as Cyclops, became available for purchase on underground online platforms in February 2024 after its creators decided to cease operations.	Exploiting the Zerologon vulnerability	CVE-2020-1472
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Financial Gain, and Compromised infrastructure	Microsoft Netlogon
Ransomware			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472
IOC TYPE	**VALUE**		
SHA256	104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2, 2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad, 36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Muhstik	The Muhstik malware has been found targeting message queuing service applications, particularly the Apache RocketMQ platform. Muhstik, a notorious threat known for targeting IoT devices and Linux-based servers, for cryptocurrency mining and DDoS attacks.	Exploiting a vulnerability in Apache RocketMQ	CVE-2023-33246
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Denial Of Service, Espionage, Resource Hijacking	RocketMQ
Botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			https://rocketmq.apache.org/download/
IOC TYPE	**VALUE**		
SHA256	9e28f942262805b5fb59f46568fed53fd4b7dbf6faf666bedaf6ff22dd416572, 1f9cda58cea6c8dd07879df3e985499b18523747482e8f7acd6b4b3a82116957, 176c57e3fa7da2fb2afcd18242b79e5881c2244f5ab836897d4846885f1bd993		

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-2024-1800	✗	Progress Telerik Report Server versions prior to 2024 Q1 (10.0.24.130)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*:*	-
Progress Telerik Report Server Insecure Deserialization Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://docs.telerik.com/report-server/implementer-guide/setup/upgrade

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4358	✗	Progress Telerik Report Server, version 2024 Q1 (10.0.24.305) or earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:progress:telerik_report_server:*:*:*:*:*:*:*:*	-
Progress Telerik Report Server Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-290	T1190: Exploit Public-Facing Application; T1040: Network Sniffing	https://docs.telerik.com/report-server/implementer-guide/setup/upgrade

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29972	✗	NAS326 V5.21(AAZF.16)C0 and earlier NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29973	✗	NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29974	⊗	NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Remote Code Execution Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-434	T1059: Command and Scripting Interpreter	https://www.zyxel.com/global/en/support/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29975	⊗	NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
	⊗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Improper Privilege Management Vulnerability	⊗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29976		NAS326 V5.21(AAZF.16)C0 and earlier, NAS542 V5.21(ABAG.13)C0 and earlier	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zyxel:nas326:*:*:*:*:*:*:*:* cpe:2.3:a:zyxel:nas542:*:*:*:*:*:*:*:*	-
Zyxel NAS Improper Privilege Management Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472		Microsoft Netlogon	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	RansomHub Ransomware
Zerologon (Microsoft Netlogon Privilege Escalation Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-330	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-33246		Apache RocketMQ 4.2.0 - 5.1.0	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:rocketmq:*:*:*:*:*:*:*:*	Muhstik Botnet
Apache RocketMQ Command Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://rocketmq.apache.org/download/

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
LilacSquid (aka UAT-4820)</td><td>-</td><td rowspan="3">Information Technology, Research, Industrial, Energy, Pharmaceutical, Oil and Gas</td><td rowspan="3">United States, Europe, Asia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>PurpleInk</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1584: Compromise Infrastructure; T1584.004: Server; T1587: Develop Capabilities; T1587.001: Malware; T1190: Exploit Public-Facing Application; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1055: Process Injection; T1005: Data from Local System; T1001: Data Obfuscation; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Operation Ghostwriter (aka UAC-0057, UNC1151, TA445, UAC-0051, PUSHCHA, DEV-0257, Storm-0257)</td><td>Belarus</td><td rowspan="2">Defense</td><td rowspan="2">Ukraine</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft, Espionage, Sabotage, and destruction</td></tr>
<tr><td></td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td></td><td>-</td><td>-</td><td>Microsoft Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1497: Virtualization/Sandbox Evasion; T1055: Process Injection; T1027: Obfuscated Files or Information; T1027.013: Encrypted/Encoded File; T1211: Exploitation for Defense Evasion; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1518: Software Discovery; T1518.001: Security Software Discovery; T1566: Phishing; T1480: Execution Guardrails; T1070: Indicator Removal; T1070.004: File Deletion; T1203: Exploitation for Client Execution; T1218: System Binary Proxy Execution; T1218.010: Regsvr32; T1218.011: Rundll32; T1140: Deobfuscate/Decode Files or Information; T1057: Process Discovery; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actors **LilacSquid, Operation Ghostwriter,** and malware **CarnavalHeist, TargetCompany Ransomware, RansomHub, Muhstik.**

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 **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **LilacSquid, Operation Ghostwriter,** and **malware CarnavalHeist, TargetCompany Ransomware, RansomHub, Muhstik** in Breach and Attack Simulation(BAS).

Threat Advisories

Chained Flaws in Progress Telerik Report Server Enable Unauthenticated RCE

Patches Made Available for Vulnerable EoL Zyxel NAS Models

Deciphering LilacSquid's Strategies for Long-Term Data Theft

CarnavalHeist: New Banking Trojan Targets Brazilian Users

Attacker Employs Multi-Stage Malware Strategy to Target Ukraine

Novel TargetCompany Ransomware Linux Variant Now Attacks ESXi

RansomHub A Rebranded Menace Exploiting the ZeroLogon Vulnerability

Muhstik Botnet Exploits Apache RocketMQ Flaw in Latest Operations

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
PurpleInk	SHA256	2eb9c6722139e821c2fe8314b356880be70f3d19d8d2ba530adc9f466ffc67d8
CarnavalHeist	IPv4	104[.]41[.]51[.]80, 191[.]239[.]116[.]217, 191[.]239[.]123[.]241, 191[.]233[.]241[.]96, 191[.]234[.]212[.]140, 191[.]235[.]233[.]246, 4[.]203[.]105[.]118, 191[.]233[.]248[.]170
	SHA256	c300749ea44f886be1887b3e19b946efbdbbc3e1bf3e416c78cfbff8d23bf70a, 1b4f44a00f61b3e0c8cd6c3125f03b6d4897d6ab90c8a6dc899ed96acee80dd6, 8424e76c9a4ee7a6d7498c2f6826fcde390616dc65032bebf6b2a6f8fbf4a535, d9877dc1ba0f977d100e687da59c216454d27e3988532652ac8f6331debbd071, 0d94547a0b8f9795e97e2a4a58b0ece65b4ea4b6e6019cbc96e1c79f373b4587, f848c0f66afc7b5a10f060c1db129529a974ae0ad71a767f7c7793351bb7ca04, e50bde1e319e699f587d3b5403c487e46deed61cc3f078fe951e7cb9f6896259, f00cb0603c055c85c7cdf9963d919d527b13013c182dc115ba733d28da57b1d9, 2c53b4dc15882cf22772994d8ed0947e4a8b70aef3a12ab190017b3317c167ea, a6d995d015c16985b456bcc5cd44377c3e5e5cf72b17771eadc51e1d02a3c6ef,

Attack Name	TYPE	VALUE
CarnavalHeist	SHA256	21e22c4736e7567b198b505ed303c3ca933e0c2d931b886756f6db18a9884a75, 2c1251ae1ec9d417bbbdd1f6ac99baa3f16a7639d0c12cb2883ef8c22c73e58e, 46e754727efdc2c891319d25a67ee999a4d8a0b21b0113db08eead42cf51b780, cd9f5773bd7672a3e09f2d05ef26775e8c7241879d5f4d13c5c5bc1704c49fa1, f2db799d892f2a7ac82bfa15826e74d778abdfa153ccafb9db1fdf56a0248a40, 5782b9bc96ce5ad011c122496ff0ff0dc08d6444c6d2e98606ada82130d5f21a, 19c02c5724622be4eedff95633f3fbaa604449aa50cc0761693bb8adb1e8cf97, 3b450994add1e3a206c56a7f8fd28e4132cffb27f3df345e07e8908d7989751f, 1e8fd8531a0851bb4d8fb6d8dd4b1a9509c8a971b11b7d95871d7b39004650ad, 8c31dcbef5c00fd98e426a1ae84163b807a2c5d1476b2d306c8f7e9d01d8df23, 2bcd8cc83cf31a77a556d5462a7e75c5e2120891414684a6e21612d61d734673, 44df224b304a9d5d089be7d68d7e5cec4c76ec58fdc16c3f86b20a671b496cf4, b8b3963967232916cd721a22c80c11cd33057bd5629dcfa3f4b03d8a6dbf1403, 883c49b7c869019951eff94699480a7ecc97c9c45060a15797ecbd5fce060d26, e7aa64726783ec6f7249483e984ae20b31a091a488a3ed0f83c210702c506d20, b152346c2679392d7e15d1cc72a39a21d24e55360c4c1c845ef3524924e93fa9, 561e6a42e23d12abe6bba8c98f84c3ba7c45a5df840bfa6fd0dfea803c9b4b7e, 7e0051d9221c13a47245359a2cd2804b4d3d9302a321fc8085da1cf1a64bac91, 056b34444abe385addd08cc581a640b72d4f2cba05de2bfd0c897d5b273a7f28, ab3a284ae6e4e466a0715c162cfab85d75522bec48fa25947b16a0891ec2358a, 7232e3318fdc370e611b2bcbaaec3d58a0d687927714c24dc81fe60767d53a31, 3c89775ae7c35fe3d1ec7e75ac9d4a19959d082d31ab412af243125440ffea6c, aadbba21380dba5028a68b44c629988b0ca517f34c1adbd68f2edd604ea507fb, 278897ee9158f9843125bc2e26c14f96c4e79d5fc578b7e5973dc8dc919a3400, 049b7067ac87e44f464cb18e454d878ca6260b667a34f48ed0046c29b45bb149,

Attack Name	TYPE	VALUE
CarnavalHeist	SHA256	8573b7aa7ac688e2fb03845aa7903b5f58d880865e3b63c4884f8e29839a3754, f92af5e770018c9e1be5d934bb5699fcf4594d870988e7b18fb65501ef43f8f9, 3445066ae58aa68c09b2476e65f96f46d0a3ae0a09366d8f9e7e592ee3f2aa0c, d3a7f22886cd294549e5f93ec18ab04e085c397ef703f5543c3b967c1172bf41
	URLs	hxxps[://]is[.]gd/38qeon?0177551.5510, hxxps[://]is[.]gd/ROnj3W?0808482.5176, hxxps[://]notafiscaleletronica[.]nf-e[.]pro/danfe/?notafiscal=00510242.500611, hxxps[://]nota-fiscal[.]nfe-digital[.]top/nota-estadual/?notafiscal=00792011.977347, hxxps[://]nfe-visualizer[.]app[.]br/notas/?notafiscal=000851113082.354934240000, hxxp[://]adobe-acrobat-visualizer[.]brazilsouth[.]cloudapp[.]azure[.]com/Documentos, hxxps[://]104[.]41[.]51[.]80@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]239[.]116[.]217@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]239[.]123[.]241@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]233[.]241[.]96@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]234[.]212[.]140@80/Documentos/files/a3[.]cmd, hxxps[://]191[.]235[.]233[.]246@80/Documentos/files/a3[.]cmd, hxxp:[//]191[.]235[.]87[.]229/Documentos/dc/c[.]cmd
TargetCompany	URLs	hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x.sh, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/x, hxxp://111.10.231[.]151:8168/general/vmeet/upload/temp/post.php
	SHA1	dffa99b9fe6e7d3e19afba38c9f7ec739581f656, 2b82b463dab61cd3d7765492d7b4a529b4618e57, 9779aa8eb4c6f9eb809ebf4646867b0ed38c97e1, 3642996044cd85381b19f28a9ab6763e2bab653c, 4cdee339e038f5fc32dde8432dc3630afd4df8a2, 0f6bea3ff11bb56c2daf4c5f5c5b2f1afd3d5098
RansomHub	SHA256	02e9f0fbb7f3acea4fcf155dc7813e15c1c8d1c77c3ae31252720a9fa7454292, 34e479181419efd0c00266bef0210f267beaa92116e18f33854ca420f65e2087, 7539bd88d9bb42d280673b573fc0f5783f32db559c564b95ae33d720d9034f5a, 8f59b4f0f53031c555ef7b2738d3a94ed73568504e6c07aa1f3fa3f1fd786de7, ea9f0bd64a3ef44fe80ce1a25c387b562a6b87c4d202f24953c3d9204386cf00

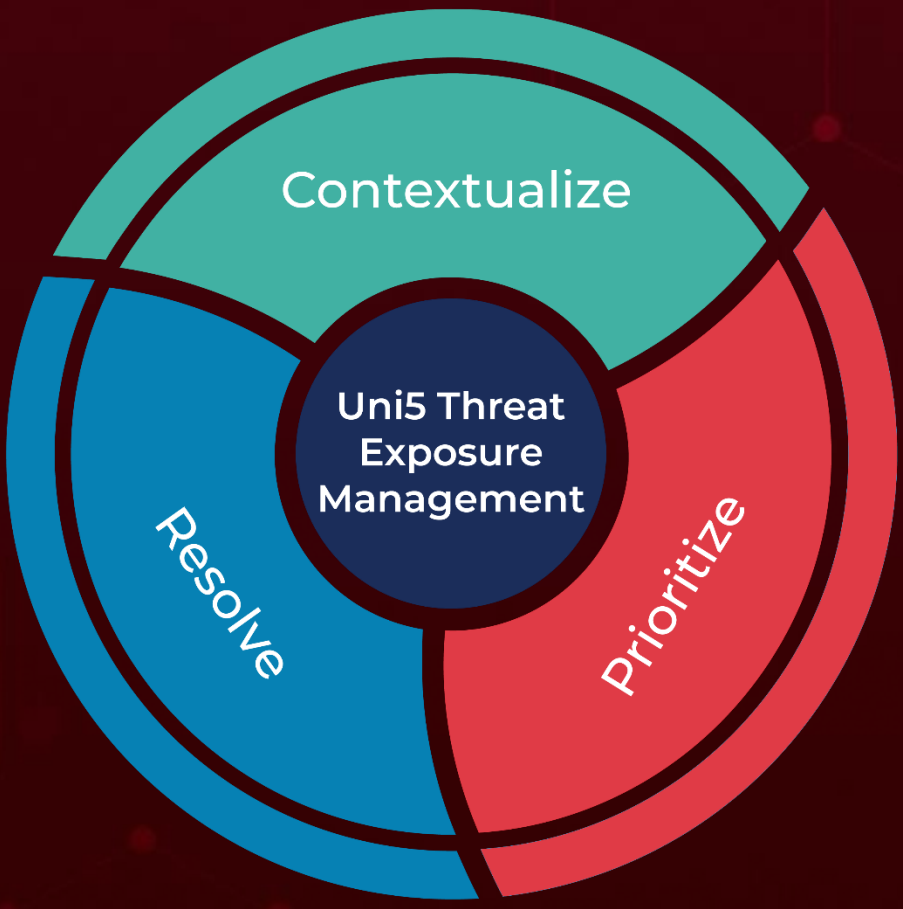
Attack Name	TYPE	VALUE
Knight Ransomware	SHA256	104b22a45e4166a5473c9db924394e1fe681ef374970ed112edd089c4c8b83f2, 2f3d82f7f8bd9ff2f145f9927be1ab16f8d7d61400083930e36b6b9ac5bbe2ad, 36e5be9ed3ec960b40b5a9b07ba8e15d4d24ca6cd51607df21ac08cda55a5a8e, 595cd80f8c84bc443eff619add01b86b8839097621cdd148f30e7e2214f2c8cb, 7114288232e469ff368418005049cf9653fe5c1cdcfcd63d668c558b0a3470f2, E654ef69635ab6a2c569b3f8059b06aee4bce937afb275ad4ec77c0e4a712f23
Muhstik	SHA256	9e28f942262805b5fb59f46568fed53fd4b7dbf6faf666bedaf6ff22dd416572, 1f9cda58cea6c8dd07879df3e985499b18523747482e8f7acd6b4b3a82116957, 176c57e3fa7da2fb2afcd18242b79e5881c2244f5ab836897d4846885f1bd993, a7bf3c031ab66265ce724fc26c8f7565442a098b06b01ea8871f13179d168713, 6730eb04edf45d590939d7ba36ca0d4f1d2f28a2692151e3c631e9f2d3612893, 86947b00a3d61b82b6f752876404953ff3c39952f2b261988baf63fbbbd6d6ae

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the 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

June 10, 2024 • 8:30 PM

More at www.hivepro.com