Date of Publication
February 26, 2024

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

19 to 25 FEBRUARY 2024

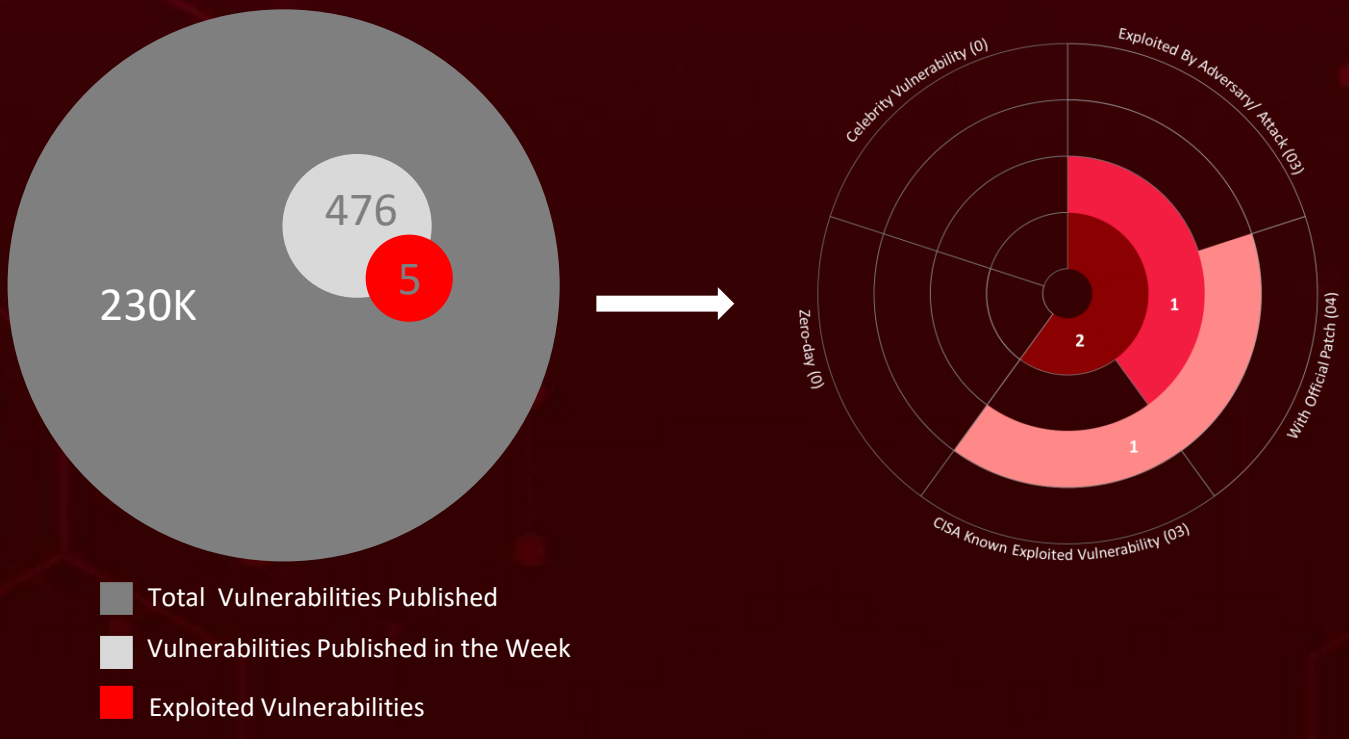
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **fifteen** attacks were executed, **five** vulnerabilities were uncovered, and **five** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs uncovered Chinese threat entity as **Earth Preta**, targeting numerous Asian countries by employing a customized version of the PlugX backdoor known as **DOPLUGS**.

Meanwhile, critical vulnerabilities in ScreenConnect **CVE-2024-1709** and **CVE-2024-1708**, allow attackers unauthorized access without credentials, and enables remote code execution respectively. Over 8200 vulnerable instances are identified and observed 643 IPs exploiting CVE-2024-1709.



High Level Statistics

15
Attacks Executed

5
Vulnerabilities Exploited

5
Adversaries in Action

- SNS Sender
- Akira Ransomware
- POWERSTAR
- POWERLESS
- NOKNOK
- BASICSTAR
- EYEGLASS
- TrollAgent
- MrAgent
- Mario Ransomware
- VietCredCare
- DOPLUGS
- LockBit Ransomware
- AsyncRAT
- Migo

- CVE-2020-3259
- CVE-2024-22245
- CVE-2024-1708
- CVE-2024-1709
- CVE-2023-43770

- Charming Kitten
- Lazarus
- Kimsuky group
- RansomHouse group
- Earth Preta

Insights

VietCredCare

completely takeover Facebook accounts of prominent businesses and organizations

Enhanced Authentication Plug-in

VMware has issued a warning to administrators regarding two unaddressed security vulnerabilities necessitating the removal of an outdated authentication plugin

SNS Sender

a malicious Python script that leverages AWS SNS for cloud based attacks

Akira Ransomware

utilizing the Cisco AnyConnect SSL VPN as its initial access vector, specifically exploiting the CVE-2020-3259 vulnerability

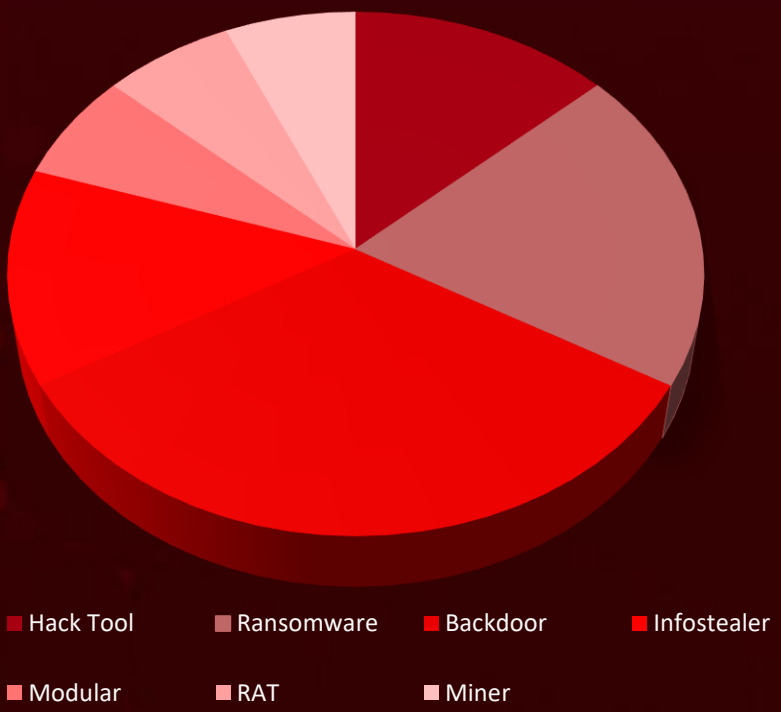
Charming Kitten

Iranian threat actor, targeting the Middle East, deploying a new backdoor called BASICSTAR through a deceptive webinar portal

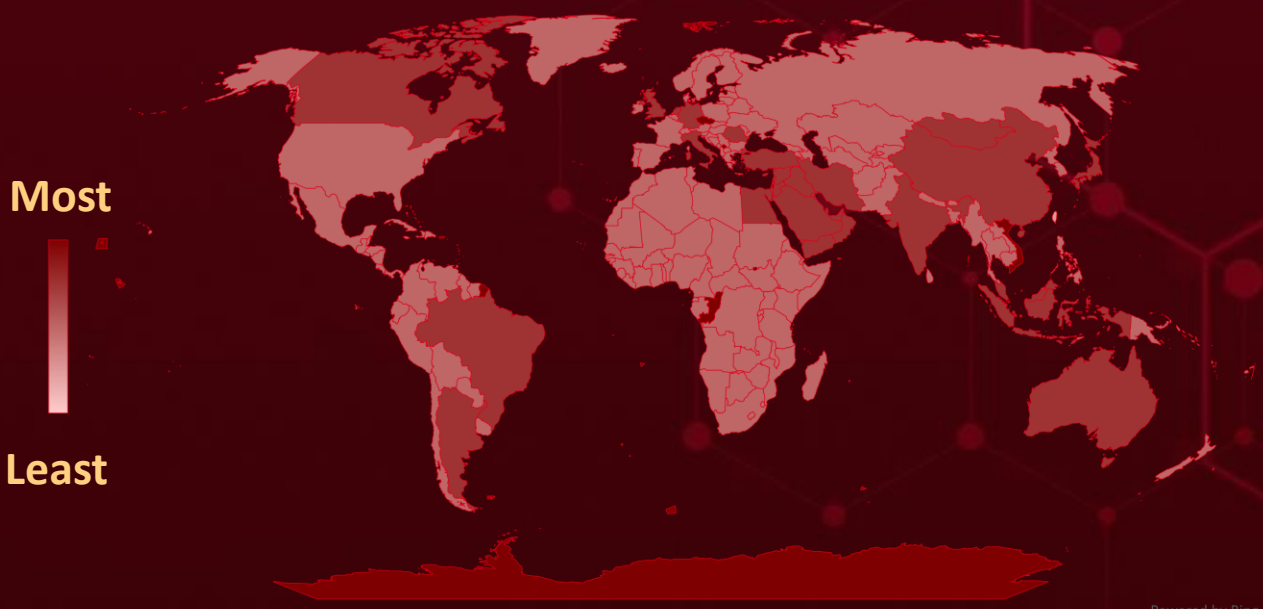
Lazarus

targeting the global defense industry, to acquire data pertaining to advanced military technology

Threat Distribution

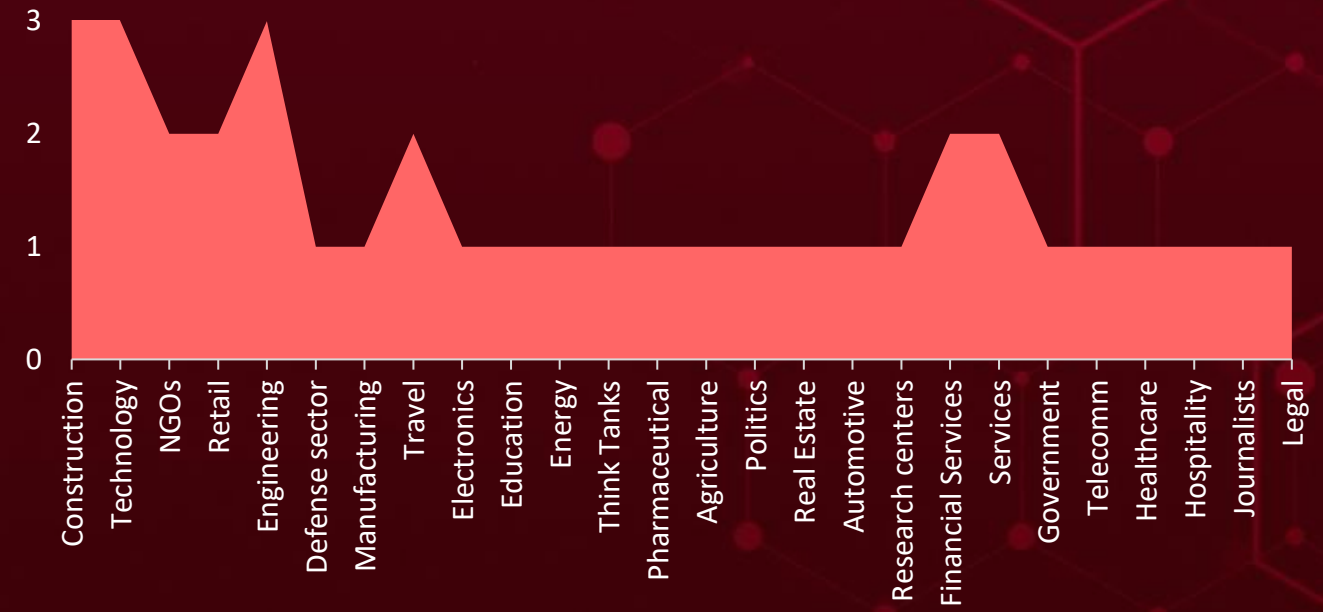


Targeted Countries



Countries	Countries	Countries	Countries
Vietnam	Iran	Morocco	Equatorial Guinea
Japan	Singapore	Cuba	Angola
Qatar	Iraq	Nicaragua	Eritrea
Malaysia	Turkey	Armenia	Nigeria
Australia	Israel	Palau	Estonia
Syria	United Kingdom	Czech Republic (Czechia)	Brunei
Bahrain	Italy	Bulgaria	Eswatini
Kuwait	Yemen	Denmark	Papua New Guinea
Brazil	South Korea	Sao Tome & Principe	Ethiopia
Netherlands	North Macedonia	Djibouti	Poland
Canada	Moldova	Slovenia	Fiji
Saudi Arabia	Chile	Dominica	Russia
China	Saint Kitts & Nevis	St. Vincent & Grenadines	Finland
United Arab Emirates	Albania	Dominican Republic	Samoa
Cyprus	Tonga	Tanzania	France
Jordan	Colombia	DR Congo	Senegal
Egypt	Nauru	Turkmenistan	Gabon
Argentina	Comoros	Ecuador	Cabo Verde
Lebanon	Peru	Uzbekistan	Gambia
Germany	Congo	Algeria	Somalia
Mongolia	Seychelles	Botswana	Georgia
India	Costa Rica	El Salvador	Spain
Oman	Sweden	Myanmar	Austria
Indonesia	Côte d'Ivoire		Sudan
Romania	Antigua and Barbuda		Ghana
	Croatia		

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1027** Obfuscated Files or Information	**T1204.002** Malicious File	**T1566** Phishing	**T1566.002** Spearphishing Link
T1036 Masquerading	**T1082** System Information Discovery	**T1140** Deobfuscate/Decode Files or Information	**T1588.006** Vulnerabilities	**T1204** User Execution
T1059.001 PowerShell	**T1190** Exploit Public-Facing Application	**T1562** Impair Defenses	**T1547.001** Registry Run Keys / Startup Folder	**T1583.004** Server
T1027.002 Software Packing	**T1555.003** Credentials from Web Browsers	**T1041** Exfiltration Over C2 Channel	**T1566.001** Spearphishing Attachment	**T1049** System Network Connections Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SNS Sender	SNS Sender, a Python script that uses AWS Simple Notification Service (SNS) to send bulk SMS messages for the purpose of phishing, aka Smishing.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Hack Tool		Smishing	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	8fd501d7af71afee3e692a6880284616522d709e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Akira Ransomware	Akira ransomware operations were initiated in March 2023. It operates through a Ransomware-as-a-Service (RaaS) model, featuring distinctive payment choices and double extortion methods. Actors behind Akira practice multi-extortion tactics and host a TOR-based (.onion) website where victims are listed along with any stolen data should a victim fail to comply with the ransom demands.	Exploiting Vulnerabilities	CVE-2020-3259
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypts files, System Compromise	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)
ASSOCIATED ACTOR			**PATCH LINK**
-			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB
IOC TYPE	**VALUE**		
SHA256	d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184, 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643, 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d		

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
POWERSTAR	POWERSTATS is a backdoor written in powershell. Its capabilities, include the ability to remotely execute PowerShell and CSharp commands, establish persistence through diverse methods, dynamically update configurations, utilize multiple C2 channels, and conduct system reconnaissance and monitoring of existing persistence mechanisms.	Through deceptive webinar portal	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Steal Data	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
SHA256	b79d28fe5e3c988bb5aadb12ce442d53291dbb9ede0c7d9d64eec078beba5585, 9777f106ac62829cd3cfdbc156100fe892cfc4038f4c29a076e623dc40a60872, 977cf5cc1d0c61b7364edcf397e5c67d910fac628c6c9a41cf9c73b3720ce67f, 823ffbcc62bd3296957a47fbf8c238949584996911e71d5140a25d0a8f6abd80, 991620817274d4031889134d40294cc6e086cf56e738a8ea78c49860c6dccdce		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
POWERLESS	POWERLESS is a PowerShell backdoor that contains a broad feature set including AES-encrypted communication, downloading executables, downloading files, executing shell commands, screenshot capture.	Through deceptive webinar portal	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Execute file and commands, capture Screenshots	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
SHA256	37bb42720bfc1cf5d0e9d7b66be134b6431055ed8bdfd384f61ab7ac061d26eb, f1ee5dd179f66f597edfeb4b2c73c6adb4b7b6d4dcfb0bef33ee5c285148d085, a8622dccb40a9fe9c2123f661e32e0a6bc40e95c88c9c2b764e603ce5eccb311, 9ef84d6a709adbd6f29813ee145dbf542a69150e5ab4261e0d58de7ee371a8ef		

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
NOKNOK	NokNok is a backdoor that infiltrates Mac computers, often disguised as a legitimate app, stealing files and collecting user information. It can capture screenshots, record videos and audio, and install other viruses on the infected Mac, often without the user's knowledge.	Through deceptive webinar portal	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
SHA256	7ce3140d5db6d716deefeaba6c5472684eddafa792a0697dbdba5f51a1efa682, dcb99f07abbe6b6a442e276856f1945f891628882964940d2f72b6ff9734707d, f9437370b013c76da8cba7c07af72d816c9bc245a3d91f540fae63481ab0fa0d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BASICSTAR	BASICSTAR, a Visual Basic Script (VBS) malware, is capable of gathering basic system information, remotely executing commands relayed from a command-and-control (C2) server, and downloading and displaying a decoy PDF file.	Through deceptive webinar portal	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Exfiltrate data and System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
SHA256	c6f91e5585c2cbbb8d06b7f239e30b271f04393df4fb81815f6556fa4c793bb0, f6f0f682668f78dbecfc30a0e0c76b6a3d86298869fb44b39adf19fdcdca5762, 1ffc0bb577e4605059143a5cca213fbe0762c320c74174fe3c2a8f4878c85fc0, 13b659e009577ab7890157ce00cc5c3641049f46135d5be2b1c17ca88a1490f9		

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
EYEGLASS	EYEGLASS malware is capable of extracting sensitive information from compromised hosts. EYEGLASS had been set up as the default handler for the TIF file extension	Through deceptive webinar portal	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TrollAgent	TrollAgent Infostealer provides the ability to steal a variety of information related to web browsers, including credential information, cookies, bookmarks, history, and extensions stored in Chrome and Firefox web browsers.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky group			-
IOC TYPE	**VALUE**		
SHA256	2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6d6569a55e, 61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92, 6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9, 955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b, a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9		

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
MrAgent	A new tool named 'MrAgent' is created by Ransomhouse group that automates the deployment of its data encrypter across multiple VMware ESXi hypervisors. MrAgent's core function is to identify the host system, turn off its firewall, and then automate the ransomware deployment process across multiple hypervisors simultaneously, compromising all managed VMs.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Hack Tool		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
RansomHouse group			-
IOC TYPE	**VALUE**		
SHA256	8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973, bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mario Ransomware	Mario ransomware is operated by Ransom House. It was found in a Joint Campaign with BianLian and White Rabbit targeting publicly-traded financial services firms. It uses .emario extension for its files.	Infected email attachments (macros), torrent websites, malicious ads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypts files, System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
RansomHouse group			-
IOC TYPE	**VALUE**		
SHA256	3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e, afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501, 2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d, 2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e		

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
VietCredCare	VietCredCare's core functionality to filter out Facebook credentials. VietCredCare is marketed as a Stealer-as-a-Service, making it "alarmingly" accessible to cybercriminals who wish to exploit stolen data.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	bd9eb106e265c5d0ae7a9e9d2d5925d558128599b1ba4a4cbc29b6fc7b3f48f0, 71c4d0fc03bc4e083f64b2f80b2242618fb725efd64f362446f98c6d2051834f, b5621b540d1ca1dd802397822145ae4f80e96e59b81fdc8d0a7b18919ceadd12, 17598536cf0bac6cb0d589410682e2cd9f813ea52bc931fe85292b149dbeb659, 20ac10ea3a964c25f09b0008406388cf4195828eed6daaeda139c55ce84986f4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DOPLUGS	It is a customized version of the PlugX backdoor known as DOPLUGS. DOPLUGS is a downloader with four backdoor commands, one of the commands is designed to download the general type of the PlugX malware.	Spearphishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Modular		Data Theft, execute commands	-
ASSOCIATED ACTOR			**PATCH LINK**
Earth Preta			-
IOC TYPE	**VALUE**		
SHA256	651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859, f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5, 67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6, b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb, 88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b		

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
LockBit Ransomware	LockBit ransomware is malicious software designed to block user access to computer systems in exchange for a ransom payment. LockBit will automatically vet for valuable targets, spread the infection, and encrypt all accessible computer systems on a network.	Exploiting Vulnerabilities	CVE-2024-1708 CVE-2024-1709
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypts files, System Compromise	ConnectWise ScreenConnect
ASSOCIATED ACTOR			**PATCH LINK**
-			https://screenconnect.connectwise.com/download
IOC TYPE	**VALUE**		
SHA256	d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668, 54489dfab5d689cd969e26e32285029095088c2673f96a9bc3df6ec14ca0a6b2, a35c3274a726b27cbcef5abe3f28d8f9675a30883490d37f23b4d730d72eca42, 56ff8149e3694e8cc919bec6739d599881d3bd9cb503eca7f6cc31e71f4f1df9, af4cddd01266e97f5b3ea0ccb6e3f8c21c313b2dca7cee581023ef23dbfee9ee		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AsyncRAT	AsyncRAT is a remote access trojan (RAT) released in 2019, primarily as a credential stealer and loader for other malware, including ransomware. It is designed to remotely monitor and control other computers through a secure encrypted connection.	Exploiting Vulnerabilities, spear-phishing, malvertising, exploit kit	CVE-2024-1708 CVE-2024-1709
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Encrypt data, System Compromise	ConnectWise ScreenConnect
ASSOCIATED ACTOR			**PATCH LINK**
Earth Preta			https://screenconnect.connectwise.com/download
IOC TYPE	**VALUE**		
SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9		

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>Migo</td><td rowspan="6">Migo is a novel Golang ELF binary that comes fitted with compile-time obfuscation and the ability to persist on Linux machines. It aims to compromise Redis servers for the purpose of mining cryptocurrency on the underlying Linux host.</td><td>Phishing</td><td>-</td></tr>
<tr><td>TYPE</td><td rowspan="2">IMPACT</td><td rowspan="2">AFFECTED PRODUCTS</td></tr>
<tr><td>Miner</td></tr>
<tr><td rowspan="3">System Compromise</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">8cce669c8f9c5304b43d6e91e6332b1cf1113c81f355877dabd25198c3c3f208,
c5dc12dbb9bb51ea8acf93d6349d5bc7fe5ee11b68d6371c1bbb098e21d0f685,
2b03943244871ca75e44513e4d20470b8f3e0f209d185395de82b447022437ec,
364a7f8e3701a340400d77795512c18f680ee67e178880e1bb1fcda36ddbc12c</td></tr>
</table>

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-2020-3259	✗	Cisco Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:* cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*	Akira Ransomware
Cisco ASA and FTD Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-22245	✗	Enhanced Authentication Plug-in (EAP): All versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:Enhanced AuthenticationPlug-in:*:*:*:*:*:*:*	-
VMware Arbitrary Authentication Relay Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1588.006: Vulnerabilities, T1068: Exploitation for Privilege Escalation	Uninstall the EAP Plugin

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1708	✗	ScreenConnect 23.9.7 and prior	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:*	-
ConnectWise ScreenConnect Path-Traversal Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities	https://screenconnect.connectwise.com/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1709		ScreenConnect 23.9.7 and prior	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:*	-
ConnectWise ScreenConnect Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application, T1588.006: Vulnerabilities, T1068: Exploitation for Privilege Escalation	https://screenconnect.connectwise.com/download

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-43770		Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
Roundcube Webmail Persistent Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1588.006: Vulnerabilities, T1204: User Execution	https://roundcube.net/news/2023/09/15/security-update-1.6.3-released

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm, Ballistic Bobcat, CharmingCypress)	Iran **MOTIVE** Information theft and espionage	Defense, Energy, Financial, Government, Healthcare, IT, Manufacturing, Oil and gas, Technology, Telecommunications, Politics, Think Tanks, NGOs, Journalists	Akrotiri and Dhekelia, Bahrain, Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syria, Turkey, United Arab Emirates, Yemen, Afghanistan, Brazil, Canada,Morocco, Pakistan, Spain, UK, USA, Venezuela
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCTS**
	-	POWERSTAR, POWERLESS, NOKNOK, BASICSTAR, EYEGLASS	-

TTPs
TA0043: Reconnaissance; 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; T1595: Active Scanning; T1587.001: Malware; T1588.002: Tool; T1190: Exploit Public-Facing Application; T1059.003: Windows Command Shell; T1569.002: Service Execution; T1555.003: Credentials from Web Browsers; T1018: Remote System Discovery; T1140: Deobfuscate/Decode Files or Information; T1027: Obfuscated Files or Information; T1001: Data Obfuscation; T1566.002: Spearphishing Link; T1059.001: PowerShell; T1036: Masquerading; T1055: Process Injection; T1123: Audio Capture; T1105: Ingress Tool Transfer; T1070.004: File Deletion; T1204.002: Malicious File

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 

Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Who is Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</td><td>North Korea</td><td rowspan="3">Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology and BitCoin exchanges</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Sabotage and destruction, Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1133: External Remote Services; T1059: Command and Scripting Interpreter; T1078: Valid Accounts; T1070: Indicator Removal; T1140: Deobfuscate/Decode Files or Information; T1040: Network Sniffing; T1046: Network Service Discovery; T1021: Remote Services; T1213: Data from Information Repositories; T1001: Data Obfuscation; T1071: Application Layer Protocol; T1572: Protocol Tunneling; T1041: Exfiltration Over C2 Channel; T1566: Phishing; T1566.001: Spearphishing Attachment</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Kimsuky group (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)</td><td>North Korea</td><td rowspan="3">Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Construction</td><td rowspan="3">Japan, South Korea, Thailand, USA and Europe</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>TrollAgent</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0007: Discovery; TA0005:Defense Evasion; TA0011: Command and Control; TA0009: Collection; TA0006: Credential Access; T1217: Browser Bookmark Discovery; T1218.011: Rundll32; T1218: System Binary Proxy Execution; T1204: User Execution; T1204.002: Malicious File; T1036: Masquerading; T1584: Compromise Infrastructure; T1608.001: Upload Malware; T1608: Stage Capabilities; T1027.002: Software Packing; T1555.003: Credentials from Web Browsers; T1555: Credentials from Password Stores; T1005: Data from Local System; T1480: Execution Guardrails; T1027: Obfuscated Files or Information</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 

RansomHouse group</td><td>-</td><td rowspan="2">Construction, Engineering, Healthcare, Electric Utilities, Financial Services</td><td rowspan="2">USA, Indonesia</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>MrAgent, Mario Ransomware</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0042: Resource Development; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1016: System Network Configuration Discovery; T1021.001: Remote Desktop Protocol; T1021.002: SMB/Windows Admin Shares; T1059.004: Unix Shell; T1071: Application Layer Protocol; T1078.002: Domain Accounts; T1190: Exploit Public-Facing Application; T1486: Data Encrypted for Impact; T1560: Archive Collected Data; T1567.002: Exfiltration to Cloud Storage; T1583.004: Server; T1588.001: Malware</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Earth Preta (aka Mustang Panda, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Camaro Dragon, Stately Taurus)</td><td>China</td><td rowspan="3">Aviation, Education, Government, NGOs, Think Tanks, Telecommunications</td><td rowspan="3">Australia, Bangladesh, Belgium, Bulgaria, China, Cyprus, Czech, Ethiopia, France, Germany, Greece, Hong Kong, Hungary, India, Indonesia, Japan, Mongolia, Myanmar, Malaysia, Nepal, Pakistan, Philippines, Russia, Singapore, Slovakia, South Africa, South Korea, South Sudan, Sweden, Taiwan, Thailand, UK, USA, Vietnam and UN</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>DOPLUGS</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; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; T1583.004: Server; T1587.001: Malware; T1585.002: Email Accounts; T1588.002: Tool; T1608.001: Upload Malware; T1608.005: Link Target; T1566.002: Spearphishing Link; T1090: Proxy; T1204.002: Malicious File; T1547.001: Registry Run Keys / Startup Folder; T1574.002: DLL Side-Loading; T1053.005: Scheduled Task; T1140: Deobfuscate/Decode Files or Information; T1036.005: Match Legitimate Name or Location; T1070.009: Clear Persistence; T1564.001: Hidden Files and Directories; T1056.001: Keylogging; T1083: File and Directory Discovery; T1016.001: Internet Connection Discovery; T1049: System Network Connections Discovery; T1082: System Information Discovery; T1012: Query Registry; T1091: Replication Through Removable Media; T1005: Data from Local System; T1025: Data from Removable Media; T1071.001: Web Protocols; T1573: Encrypted Channel</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **Charming Kitten, Lazarus, Kimsuky group, RansomHouse group, Earth Preta** and malware **SNS Sender, Akira Ransomware, POWERSTAR, POWERLESS, NOKNOK, BASICSTAR, EYEGLASS, TrollAgent, MrAgent, Mario Ransomware, VietCredCare, DOPLUGS, LockBit Ransomware, AsyncRAT, Migo.**

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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Lazarus, Earth Preta** and malware **Akira Ransomware, MrAgent, Mario Ransomware, VietCredCare, DOPLUGS, Migo** in Breach and Attack Simulation(BAS).

Threat Advisories

Novel Smishing Kit Leverages Cloud Platform

Akira Ransomware Exploits Cisco Flaw for Maximum Impact

Iranian Threat Actor Adapts Tactics to Stay One Step Ahead

North-Korean Cyber-Espionage Operations Grapples Defense Sector

Admins Urged to Uninstall VMware EAP Amid Critical Flaws

Kimsuky Disseminate TrollAgent Leveraging Stolen Certificates

RansomHouse's MrAgent Reshaping Automation in Cyber Attacks

VietCredCare Operates As Stealer-as-a-Service, Targeting Meta Sessions

Earth Preta's DOPLUGS Leaves its Mark in Asia

Critical Vulnerabilities in ScreenConnect Under Active Exploitation

Roundcube Webmail Faces Unrelenting Exploitation

Migo Targets Redis Servers for Cryptojacking Attacks

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
SNS Sender	MD5	8fd501d7af71afee3e692a6880284616522d709e
Akira Ransomware	SHA256	d5558ec7979a96fe1ddcb1f33053a1ac3416a9b65d4f27b5cc9fd0a816296184, 2db4a15475f382e34875b37d7b27c3935c7567622141bc203fde7fe602bc8643, 99c1cd740fa749a163ce8cdf93722191c4ba5d97de81576623a8bbcb622473d6, ca651d0eb676923c3b29190f7941d8d2ac8f14e4ad6c26c466069bbc59df4d1d, c9a1d8240147075cb7ffd8d568e6d3c517ac4cfdddccd5bb37857e7bde6d2eb7, 2727c73f3069457e9ad2197b3cda25aec864a2ab8da3c2790264d06e13d45c3d, 678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33, 77fe1619aa07d2ab169a2fa23feb22d7433bf07e856cda1402cf60205beddd7f, f1f82d3b62f92f4fe8af320afea6c346210bb51774bb1567149e308469d40c92, ffcddd8544bca0acde69f49abd1ea9dbee5f4eb73df51dd456b401c045a0b6af, aca0f5e76dacc4b9145c17a25a639aeb2e4cf76b7859bcb27224c42e404013a2, 08207409e1d789aea68419b04354184490ce46339be071c6c185c75ab9d08cba, ee0a27f3de6f21463f8125dbfc95268ff995ef8ea464660d67cf9f77e240e1ab,

Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	030db5fb2a639b0c1a63bbd209bd1f043dbc4dbb306102f1726cdd4a6500fb83, b7bbfb66338a3413f981561115bd8ef8a4014479bcc320de563499cfc73a3de2, 58e9cd249d947f829a6021cf6ab16c2ca8e83317dbe07a294e2035bb904d0cf3, 56f1014eb2d145c957f9bc0843f4e506735d7821e16355bcfbb6150b1b5f39db, 6270cef0c8cc45905556c40c9273391d71ef8d73c865d44d2254a8a4943ae5b4, 5009343ce7e6e22a777b22440480fe2eb26098d4a2ecc62e6df4498819e26b5c
POWERSTAR	SHA256	b79d28fe5e3c988bb5aadb12ce442d53291dbb9ede0c7d9d64eec078beba5585, 9777f106ac62829cd3cfdbc156100fe892cfc4038f4c29a076e623dc40a60872, 977cf5cc1d0c61b7364edcf397e5c67d910fac628c6c9a41cf9c73b3720ce67f, 823ffbcc62bd3296957a47fbf8c238949584996911e71d5140a25d0a8f6abd80, 991620817274d4031889134d40294cc6e086cf56e738a8ea78c49860c6dccdce
	SHA1	2581e9bf9fa219cb1bce393f7492212612228221, e588837d652d2cd96c5cb44f8f98fd7d82cc5d30, 214bf21a567b678ec4250c1aca4cf71275e2860e, 0161ba63e65a2b39b754b9d16cf2bc62de98e99a, 5671ff66d0ea0cd93b04ca0ab35ff4e33e33833a
	MD5	f5eddfaeb353ceca4b8713f88f030604, 99dc6ab3f88629069b5109f5ed530e25, 5398e9063ee0d6189cf59c8d4403a40d, e4e8864f88724b736ec3568fd8916796, a2b407eac00422b2bc7ac59a74fc47e0
POWERLESS	SHA256	37bb42720bfc1cf5d0e9d7b66be134b6431055ed8bdfd384f61ab7ac061d26eb, f1ee5dd179f66f597edfeb4b2c73c6adb4b7b6d4dcfb0bef33ee5c285148d085, a8622dccb40a9fe9c2123f661e32e0a6bc40e95c88c9c2b764e603ce5eccb311, 9ef84d6a709adbd6f29813ee145dbf542a69150e5ab4261e0d58de7ee371a8ef
	SHA1	195e939e0ae70453c0817ebca8049e51bbd4a825, 27b38cf6667936c74ed758434196d2ac9d14deae, 5bdec05bdca8176ae67054a3a7dc8c5ef0ac8deb, c3fd8ed68c0ad2a97d76fc4430447581414e7a7e
	MD5	c79d85d0b9175cb86ce032543fe6b0d5, 9b6c308f106e72394a89fac083de9934, 859a9e523c3308c120e82068829fab84, 5fc8668f9c516c2b08f34675380e2a57

Attack Name	TYPE	VALUE
NOKNOK	SHA256	7ce3140d5db6d716deefeaba6c5472684eddafa792a0697dbdba5f51a1efa682, dcb99f07abbe6b6a442e276856f1945f891628882964940d2f72b6ff9734707d, f9437370b013c76da8cba7c07af72d816c9bc245a3d91f540fae63481ab0fa0d
BASICSTAR	SHA256	c6f91e5585c2cbbb8d06b7f239e30b271f04393df4fb81815f6556fa4c793bb0, f6f0f682668f78dbecfc30a0e0c76b6a3d86298869fb44b39adf19fdcdca5762, 1ffc0bb577e4605059143a5cca213fbe0762c320c74174fe3c2a8f4878c85fc0, 13b659e009577ab7890157ce00cc5c3641049f46135d5be2b1c17ca88a1490f9, fdc5d6caaaa4fb14e62bd42544e8bb8e9b02220e687d5936a6838a7115334c51, 07384ab4488ea795affc923851e00ebc2ead3f01b57be6bf8358d7659e9ee407
	SHA1	cdce8a3e723c376fc87be4d769d37092e6591972, 1f974d7634103536e524a41a79046785ca7ae3d6, 729346dfdd2203a9943119bac03419d63554c4b8, 09b527ddb848d7697f34ab34c2bce30da6f24238, 2a2610344bf8db66b1e13302e54e4ef77712aada, 25005352eff725afc93214cac14f0aa8e58ca409
	MD5	2edea0927601ef443fc31f9e9f8e7a77, 78e4975dc56e62226f4c56850efb452b, 3fbf3ce1a9b452421970810bd6b6b37a, a517bcb4d8c24dfe750110a91252c26c, e851147f1d5dc5236ed2085cd5e513e7, 853687659483d215309941dae391a68f
EYEGLASS	SHA256	f2dec56acef275a0e987844e98afcc44bf8b83b4661e83f89c6a2a72c5811d5f
TrollAgent	MD5	013c4ee2b32511b11ee9540bb0fdb9d1, 035cf750c67de0ab2e6228409ac85ea3, 19c2decfa7271fa30e48d4750c1d18c1, 27ef6917fe32685fdf9b755eb8e97565, 2aaa3f1859102aab35519f0d4c1585dd, 2b678c0f59924ca90a753daa881e9fd3, 4168ff8b0a3e2f7e9c96afb653d42a01, 4222492e069ac78a55d3451f4b9b9fca, 42ea65fda0f92bbeca5f4535155125c7, 6097d030fe6f05ec0249e4d87b6be4a6, 62fba369711087ea37ef0b0ab62f3372, 7457dc037c4a5f3713d9243a0dfb1a2c, 7b6d02a459fdaa4caa1a5bf741c4bd42, 87429e9223d45e0359cd1c41c0301836, 88f183304b99c897aacfa321d58e1840, c8e7b0d3b6afa22e801cacaf16b37355, d67abe980a397a94e1715df6e64eedc8, dc636da03e807258d2a10825780b4639,

Attack Name	TYPE	VALUE
TrollAgent	MD5	E4a6d47e9e60e4c858c1314d263aa317, 9e75705b4930f50502bcbd740fc3ece1, a67cf9add2905c11f5c466bc01d554b0, b532f3dcc788896c4844f36eb6cee3d1, B97abf7b17aeb4fa661594a4a1e5c77f, 8d4af59eebdcda10f3c88049bb097a3a, 9360a895837177d8a23b2e3f79508059
	SHA1	120891212a78114fe114217012c2a000727e034b, 3d1731fa03f2bb8b3ca74ab49c83923428e58362, 4a705f58918c00431de453d5b5f621fa42ff7169, 4c8b7d968806f8108ccde6ac07a37b8174ac44bf, 4eea45c22881a092ac7a8b0a5379076d5803e83e, 6d531b021b20febf1dafa730582944eb82d9c6f3, e6be97ca9e79b45c671c6531908f70b353d47994
	URLs	hxxp://ai[.]aerosp[.]p-e[.]kr/index[.]php, hxxp://ai[.]bananat[.]p-e[.]kr/index[.]php, hxxp://ai[.]daysol[.]p-e[.]kr/index[.]php, hxxp://ai[.]kimyy[.]p-e[.]kr/index[.]php, hxxp://ai[.]kostin[.]p-e[.]kr/index[.]php, hxxp://ai[.]limsjo[.]p-e[.]kr/index[.]php, hxxp://ai[.]negapa[.]p-e[.]kr/index[.]php, hxxp://ai[.]selecto[.]p-e[.]kr/index[.]php, hxxp://ai[.]ssungmin[.]p-e[.]kr/index[.]php, hxxp://ar[.]kostin[.]p-e[.]kr/index[.]php, hxxp://ca[.]bananat[.]p-e[.]kr/index[.]php, hxxp://pi[.]selecto[.]p-e[.]kr/index[.]php, hxxp://qa[.]jaychoi[.]p-e[.]kr/index[.]php, hxxp://qi[.]limsjo[.]p-e[.]kr/index[.]php, hxxp://sa[.]netup[.]p-e[.]kr/index[.]php, hxxp://ve[.]kimyy[.]p-e[.]kr/index[.]php, hxxp://viewer[.]appofficer[.]kro[.]kr/index[.]php, hxxp://ce[.]aerosp[.]p-e[.]kr/index[.]php, hxxp://coolsystem[.]co[.]kr/admin/mail/index[.]php, hxxp://dl[.]netup[.]p-e[.]kr/index[.]php, hxxp://li[.]ssungmin[.]p-e[.]kr/index[.]php, hxxp://ol[.]negapa[.]p-e[.]kr/index[.]php, hxxp://pe[.]daysol[.]p-e[.]kr/index[.]php
	SHA256	2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6d6569a55e, 61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92, 6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9, 955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b, a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9, f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3, ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca

Attack Name	TYPE	VALUE
MrAgent	SHA256	8189c708706eb7302d7598aeee8cd6bdb048bf1a6dbe29c59e50f0a39fd53973, bfc9b956818efe008c2dbf621244b6dc3de8319e89b9fa83c9e412ce70f82f2c
Mario Ransomware	SHA256	3934b3da6bad0b4a28483e25e7bab919d7ed31f2f51cca22c56535b9f8183a0e, afe398e95a75beb4b0508c1bbf7268e8607d03776af0b68386d1e2058b374501, 2c1a4fe4a2ac4f0a49052f9521458136eb477fe23665dc4b7076fbd32de3005d, 2c1475f1b49a8b93a6c6217be078392925535e084048bf04241e57a711f0f58e, 0a77e537c64336f97a04020e59d17d09d459d1626a075878e2b796d1e1033038, d36afcfe1ae2c3e6669878e6f9310a04fb6c8af525d17c4ffa8b510459d7dd4d
VietCredCare	SHA256	bd9eb106e265c5d0ae7a9e9d2d5925d558128599b1ba4a4cbc29b6fc7b3f48f0, 71c4d0fc03bc4e083f64b2f80b2242618fb725efd64f362446f98c6d2051834f, b5621b540d1ca1dd802397822145ae4f80e96e59b81fdc8d0a7b18919ceadd12, 17598536cf0bac6cb0d589410682e2cd9f813ea52bc931fe85292b149dbeb659, 20ac10ea3a964c25f09b0008406388cf4195828eed6daaeda139c55ce84986f4, 8c6e6faa28f67ac56587a4dcea49c820b466113604900c3f829185a096c6df47, aababe351df7fc27a8d9a227f75850adc1fc3fe86248e59953def5b3fa9b8822, 67b095896e09acff1b2140c933d5efff0dd2a10c920b5db6518531f2304a8838, 1d92dd2e8b04e715954d2bf99e053f9b05eb89986e2b13651d17498f51d2de5d, e2b4e099b70a213f27a84b8534964a7dfd870004ebee3c5eb6601f239c5fd3a1, b3eaa35baecf562a018df53066e8ec438cac854b0bb30eba7aa34a9d8230aacb, 74ab0c6b96cffa75b474ba1fbf69b9cd8502981f85a89642c0b3aa35399a4bda, e0b00681a57457af72fc53866316fc2ba1b0c99d79685ca3a4e8973d023b6426, 071001dcdf87312fece26c4f9bec92f0e0c651eb88786d6ac4ea7ee128fe0aba, 83d3c0e4b813020aa8c2e917be86bbf8b48336960a7ac65f973e88fc05575263, 596f86cf3d2911f2817289be25621d9a1f93bd0d861b66f0fec2a9092b9eff3c, f1b430bed2b7c1c10f66d8551713c3bcc06c689f0c55a57129703feeab58927f,

Attack Name	TYPE	VALUE
VietCredCare	SHA256	c4616a07ab285f8a124079e6d2afd30ea1c552804c4ac689510e5a0e85e6dd3b, 3a56c8b9269a6dd225bc150dfd6bcf058aeadd2d5196ed02cec5bf00521238d9, f791d75904f434461c0bcccc0ff3d39ab4eb04eb208e9b7eed3e71376b6820b8, 5c1ef4b5e5a8cd2a80fd5e5aee0d29eb44fedcb9dd5e73e6b5c74f17e83a19cb, 1f28712c2fabfd21aa286fa70e6191f4265d808b3880b897f4c8df5778c1b785, d305ec61046d4470559480cf724b16584e65752a37c7817b8a06b208247b2ac5, aa2ce3666ff4ede662c071d07b16d4e2fadc6c2dd9fe76eb9fb4dc82817a5ec8, a2ac7a96a14f855caa520ce2862dbdb83d1cb278d0f9171e116926c5a40196aa, 27f377560d2ada287cb134b1d350eaa2fc15799a3845fe35c06e6d208e63bb71, d26634062b44a009eaf0cc024fd24e7d32d4117664904b86b925b2d5639e527b, 2eeb5b0e3d6e3e1f1422b6d8115a48c0fb6953e42e974a2754e079ea0de0819f, dafdfdf54ec92cf126f676947fb708f6354326ebf5f6e3fbd84022df179a1c85, ffc70cddcfdbdda5a941d53a2307567da14853442e00282c7e0bd57bc9f963a1, c1fb24f868d17673b41da5aaa8738730963f4a8e3d208420a0cd21a8f2a5470f, 257146b44136f54e976273759e3f3f671d1622797259091a37312d58933a4ea8, 987863291c7025bef2e2a7d8b5081f4bde9d1ca38172a99567004c1c44599010, 22b462e4e852a4f5b668c941780e4d01af7f9e645b6cf50a6f9154ce9d96ebe4, 14b8e34338e445d15d901f3b39fea324ef66eab686877d520a4b3a5cc86632ef
DOPLUGS	SHA256	651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859, f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5, 67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6, b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb, 88c8eb7d2a64e0f675cb2ac3da69cdf314a08a702a65c992bcb7f6d9ec15704b, 12c584a685d9dffbee767d7ad867d5f3793518fb7d96ab11e3636edcc490e1bd, 71bba2753da5006015bc890d30b1ed207a446e9f34c7e0157d6591bf573f3787,

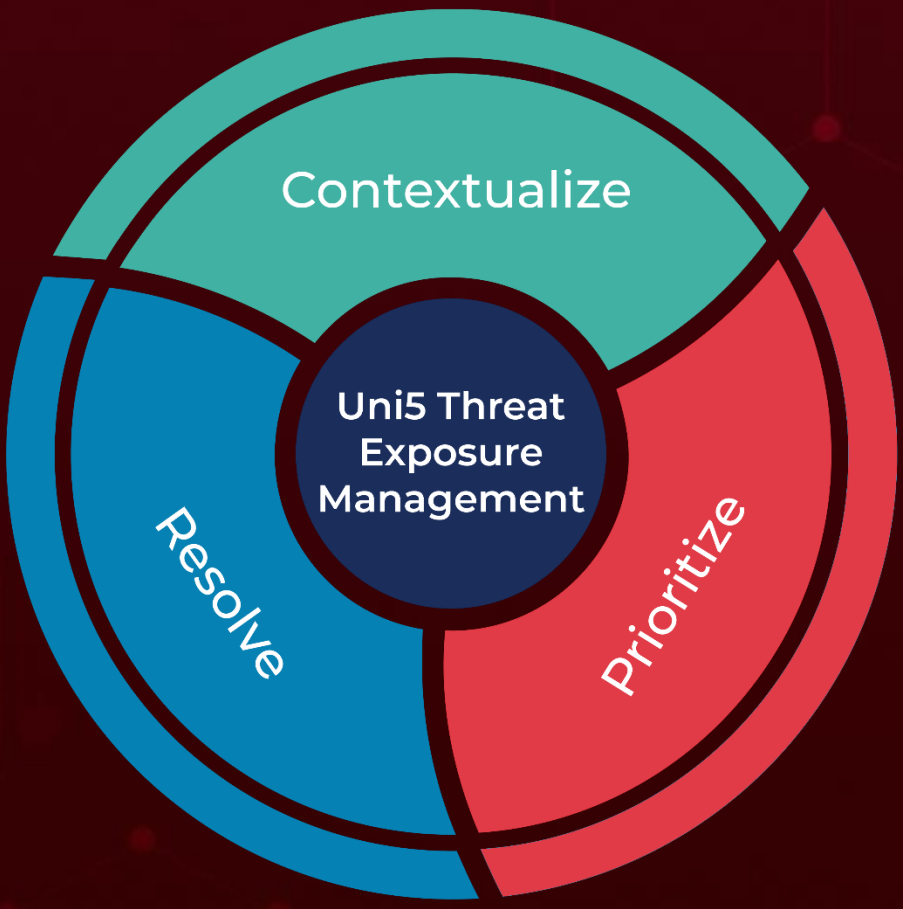
Attack Name	TYPE	VALUE
DOPLUGS	SHA256	3fa7eaa4697cfcf71d0bd5aa9d2dbec495d7eac43bdfcfbef07a306635e4973b, a0c94205ca2ed1bcdf065c7aeb96a0c99f33495e7bbfd2ccba36daebd829a916, 17225c9e46f809556616d9e09d29fd7c13ca90d25ae21e00cc9ad7857ee66b82, d0ca6917c042e417da5996efa49afca6cb15f09e3b0b41cbc94aab65a409e9dc, d64afd9799d8de3f39a4ce99584fa67a615a667945532cfa3f702adbe27724c4, c4627a5525a7f39205412a915fd52b93d83ef0115ee1b2642705fe1a08320692, 39f8288ef21f5d6135f8418a36b9045c9758c4e7a4e4cab4aff4c1c6119f901a, 42c18766b5492c5f0eaa935cf88e57d12ffd30d6f3cc2e9e0a3c0bdcdfa44ad5, 9610cbcd4561368b6612cad1693982c43c8d81b0d52bb264c5f606f2478c1c58
LockBit Ransomware	SHA256	d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668, 54489dfab5d689cd969e26e32285029095088c2673f96a9bc3df6ec14ca0a6b2, a35c3274a726b27cbcef5abe3f28d8f9675a30883490d37f23b4d730d72eca42, 56ff8149e3694e8cc919bec6739d599881d3bd9cb503eca7f6cc31e71f4f1df9, af4cddd01266e97f5b3ea0ccb6e3f8c21c313b2dca7cee581023ef23dbfee9ee, d4f150a8b26e9edccae4987433fb5b8a105970db143ba196f13652730c635668, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 92813f3c2973a00dc738f72acdf3014e914128a4b427dde5c19e73a87b5f38d1, f01909eee3dec5474a5a845deea3f8fb5502ac006f65060a7e945f91c966e266, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, c1b449af312de6828850d4b6810dca9982a6ee0ba91b8d1f5cb6573349d2744a, 2e83048c7ed1193f09ae8d293b42c105662828f2ab56a2fa1f81379ee250fc46, 12b6fead37cca9d8ca4c00c2a9d56c0a402e760ab309356f078587acb7f33396

Attack Name	TYPE	VALUE
AsyncRAT	SHA256	0054a0b839de6c8261a2f7ec0bd0efdcf2eb28161db6e6354ef94709c99b40c3, 398bf921701c72139dfa6d11b2eb41810170eaf847cc73f16ff00c8f86d6d30a, 7afcf780cb130e2d294e7eca704cb2914d50c738748da431ee275dacc3e5344e, da816e315d1130151e152d0e390be7ffec1272503ed5368c3957eeeb9c9fdea9, 5145dcd625c43d5ccbb49e6020b62991dd8140b85685a555ef4c30f28963bef8, 6f92b2cdb8b5f68d20dbc7ca23c3a3ec78c4ef1859001940dfa22e38ce459d30, 6d240a48b5e2d1cf761a8b48b146d20729d0a7a3a557e31e75ed4c120ce71aea, c7d4e119149a7150b7101a4bd9fffbf659fba76d058f7bf6cc73c99fb36e8221, 2657fe9b88321d255fc56a81b2df4b0109ab7c525442f31765c94d75c37347aa, 124c02ed924e11b06b74e1b8c1290adbb1e50dfa2a7bcf95104c6425a1f82ef5, 3c4df2d02e4b6f4acf7b19238211892db501ee6faa04065dd11b25b56483f9c4, 9a7bc24bd814ab755a8ad67e1aeebc05ff139771928f0eae883daff6f4ae161d, 65d6130ed7d3d822e1b08e7bed8e3adca4188d787d6805935213369c05eb2a99
Migo	SHA256	8cce669c8f9c5304b43d6e91e6332b1cf1113c81f355877dabd25198c3c3f208, c5dc12dbb9bb51ea8acf93d6349d5bc7fe5ee11b68d6371c1bbb098e21d0f685, 2b03943244871ca75e44513e4d20470b8f3e0f209d185395de82b447022437ec, 364a7f8e3701a340400d77795512c18f680ee67e178880e1bb1fcda36ddbc12c

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

February 26, 2024 . 7:50 AM

More at www.hivepro.com