Date of Publication
November 14, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

06 NOVEMBER to 12 NOVEMBER 2023

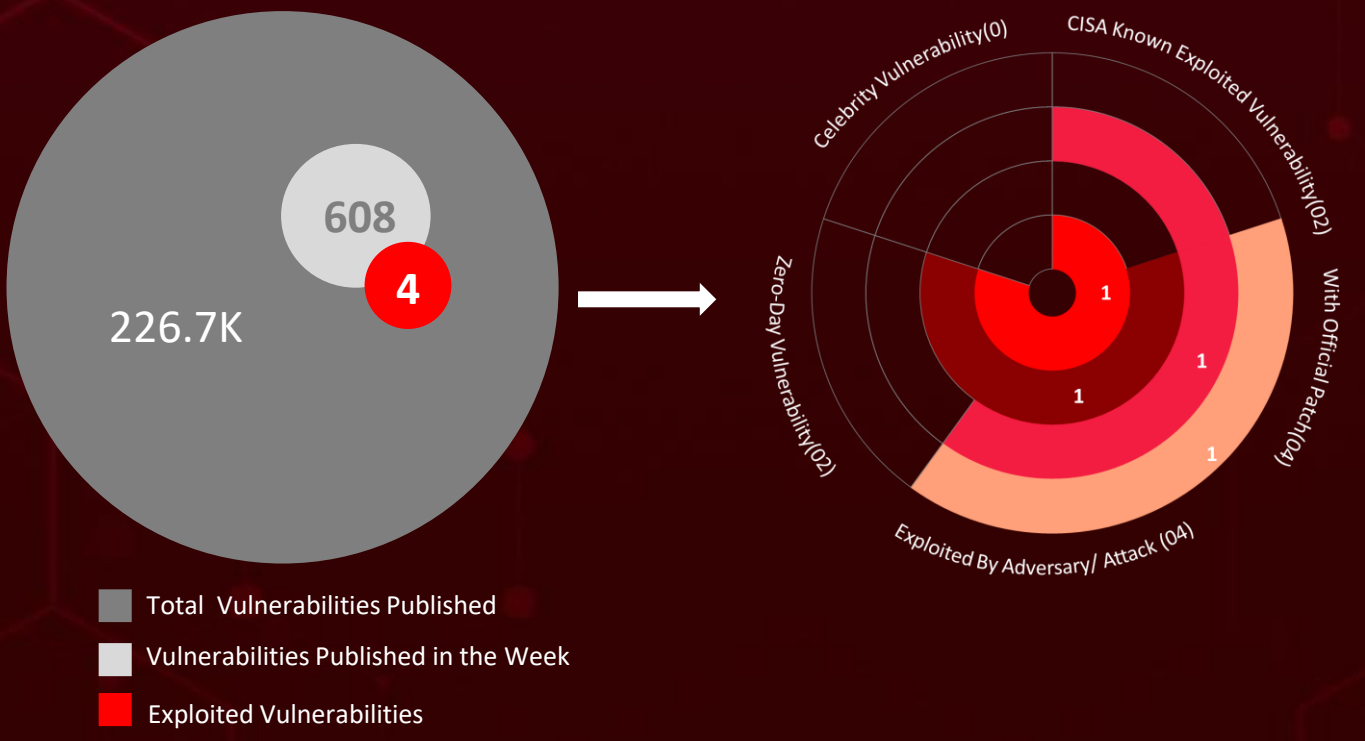
Table Of Contents

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **twenty-five** executed attacks, **six** instances of adversary activity, and **four** exploited vulnerabilities, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered an actor named **Kinsing** exploiting Looney Tunables flaws, **Farnetwork** threat group in their latest campaign, being the mastermind of Five Ransomware Strains.

Meanwhile, a critical vulnerability (**CVE-2023-47246**) in SysAid servers is being exploited by the **Lace Tempest** in various attacks. These observed attacks have been on the rise, posing a significant threat worldwide.



High Level Statistics

25
Attacks Executed

4
Vulnerabilities Exploited

6
Adversaries in Action

- Socks5Systemz
- PrivateLoader
- Amadey
- Jupyter Infostealer
- MultiLayer
- PartialWasher
- BFG Agonizer
- sqlextractor
- ObjCShellz
- RustBucket
- AllaKore RAT
- Ares RAT
- DRat
- Key RAT
- Millenium RAT
- BlazeStealer
- Nokoyawa
- JSWORM
- Nefilim
- Karma
- Nemty
- FakeBat
- Redline stealer
- Clop ransomware
- Gracewire

- CVE-2023-4911
- CVE-2017-9841
- CVE-2023-38831
- CVE-2023-47246

- Kinsing
- Agrius
- BlueNorOff
- SideCopy
- farnetwork
- Lace Tempest

Insights

Socks5Systemz
Infects 10,000 Systems

Kinsing
Exploiting Looney Tunables Vulnerability to Breach Cloud Environments in their latest campaign.

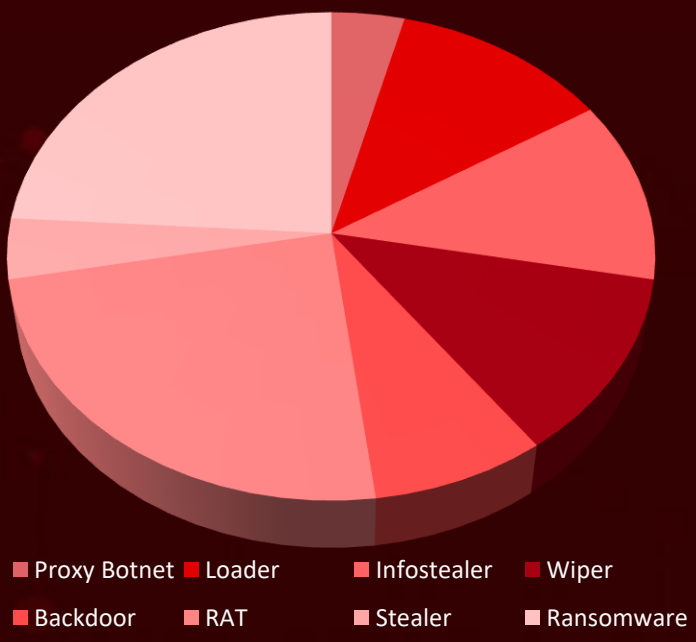
Jupyter Infostealer
aimed at evading detection and ensuring persistence

SideCopy
capitalizing on WinRAR's CVE- 2023-38831 vulnerability to target Indian government agencies.

SysAid Zero-Day
Exploited by Lace Tempest to deploy Clop ransomware

BlazeStealer
Malware discovered in Python packages on PyPI

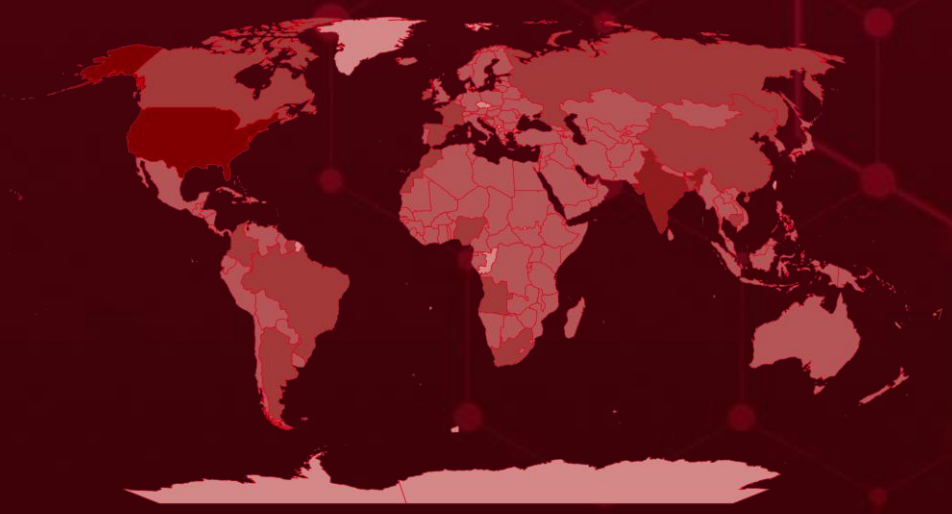
Threat Distribution



Targeted Countries

Most

Least



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

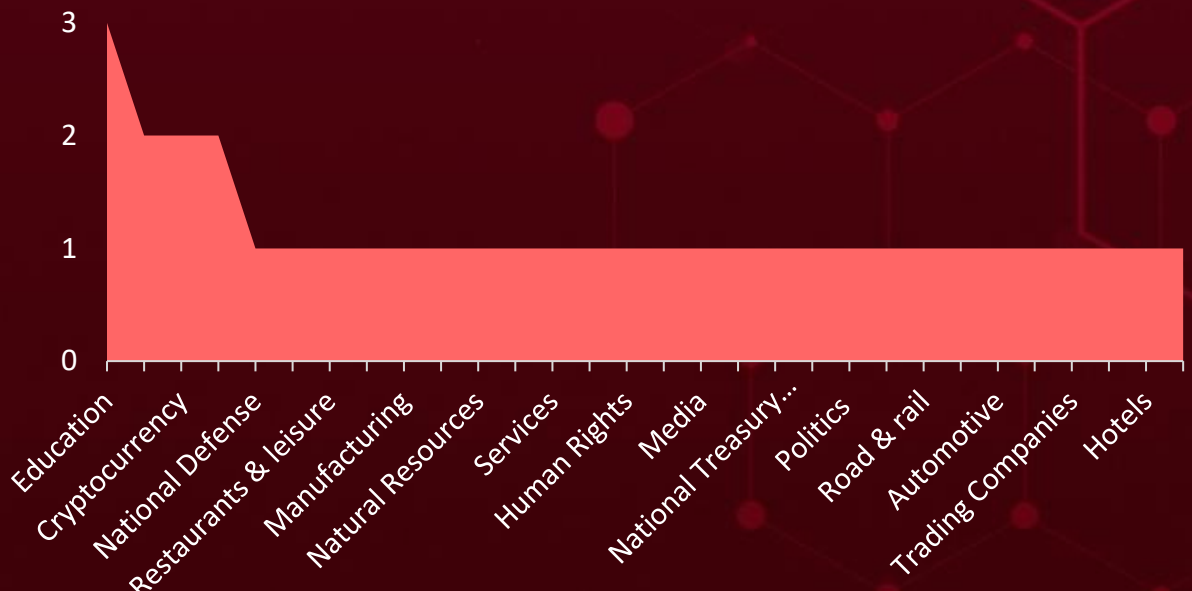
Countries
India
United States
Spain
Suriname
France
Angola
Nigeria
Argentina
Croatia
Bangladesh
Ireland
Brazil
Morocco
Cambodia
South Africa
Canada
Colombia
Israel
Saint Lucia
Monaco
Afghanistan
Bhutan

Countries
Norway
Bolivia
South Sudan
Bosnia and Herzegovina
Mali
Botswana
Nepal
Andorra
Philippines
Brunei
Sierra Leone
Bulgaria
Algeria
Burkina Faso
Madagascar
Burundi
Mauritius
Cabo Verde
Mozambique
Armenia
Niger

Countries
Cameroon
Panama
Australia
Romania
Central African Republic
Saudi Arabia
Chad
Solomon Islands
Chile
Tuvalu
China
Vietnam
Austria
Lithuania
Comoros
Malaysia
Congo
Marshall Islands
Costa Rica
Micronesia
Côte d'Ivoire
Montenegro
Azerbaijan

Countries
Namibia
Cuba
New Zealand
Cyprus
North Korea
Czech Republic (Czechia)
Pakistan
Denmark
Paraguay
Djibouti
Portugal
Dominica
Rwanda
Dominican Republic
San Marino
DR Congo
Serbia
Ecuador
Slovakia
Egypt
Belgium
El Salvador
Sri Lanka

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter

T1105 Ingress Tool Transfer

T1083 File and Directory Discovery

T1041 Exfiltration Over C2 Channel

T1005 Data from Local System

T1027 Obfuscated Files or Information

T1204 User Execution

T1113 Screen Capture

T1036 Masquerading

T1059.001 PowerShell

T1566 Phishing

T1140 Deobfuscate/ Decode Files or Information

T1547.001 Registry Run Keys / Startup Folder

T1056.001 Keylogging

T1190 Exploit Public-Facing Application

T1057 Process Discovery

T1204.002 Malicious File

T1056 Input Capture

T1588 Obtain Capabilities

T1608.001 Upload Malware

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Socks5Systemz	It is written in C++ and primarily sets up SOCKS5 proxies on victim computers that can then be used by threat actors to tunnel/hide the malicious traffic associated with other malware.	Phishing, exploit kits, malvertising, trojanized executables	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Retrieve data from the C2 servers	-
Proxy botnet			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	fee88318e738b160cae22f6c0f16c634fd16dbf11b9fb93df5d380b6427ac18f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PrivateLoader	PrivateLoader is a modular malware whose main capability is to download and execute one or several payloads. The loader implements anti-analysis techniques, fingerprints the compromised host and reports statistics to its C2 server.	Phishing, exploit kits, malvertising, trojanized executables	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Download and execute payloads	-
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	6cc7d9664c1a89c58549e57b5959bb38		
SHA1	85b665c501b9ab38710050e9a5c1b6d2e96acccc		
SHA256	27c1ed01c767f504642801a7e7a7de8d87dbc87dee88fbc5f6adb99f069afde4		

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
Amadey	Amadey is being sold for about $500 on Russian-speaking hacking forums. It periodically sends information about the system and installed AV software to its C2 server and polls to receive orders from it. Its main functionality is that it can load other payloads for targeted computers compromised by the malware.	Phishing, exploit kits, malvertising, trojanized executables	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Deliver multiple malwares, update copies of itself	-
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	68cf6c33c3a11405e8f66b1cd769ac4b9ed53fa702d06323d737f86bb238f0aa, 31fcc145a7951bdb76f7635a0b7bb4ca6649fd8b2e6d5a166dfac138a71200bc, 2260d1b05abe62e94794dfc3d91d34d4751c6ccbdd450c2d3bbf01cb1aa31eec, e865cb5fbed88a0ef8d09376530d4fd855358dba91fa3f3d1296fb03085e8e06, 3141087bc31d396d4151e1bf8b61254374b503faefe444f17316ac40ba5c845b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Jupyter Infostealer	Jupyter Infostealer is a malware variant that changing its delivery method to evade detection, use SEO poisoning to encourage malicious file downloads. The malware has demonstrated credential harvesting and encrypted C2 communication capabilities used to exfiltrate sensitive data.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft	-
Infostealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	c03ff646f732bf3a13b52e4786828af05a211ad69674cc2c11089681bc67ece9, e7ded7fb9f1aa432a3eb598d00157afb67b201647da234f785397a117f046e34, 1d322817bea6534d8b55282eb227a1fcca076b9d60b8b2fa0d3f756f4e38085c, d7f8a922f22d105d5190e91efb592335d5ccdee0fe3615dc3863cdef90a97738, 6738651649eedf22d352fcb5bb3942125487d63c26d7243fee8a25d295187996		

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
MultiLayer	Multilayer is .NET based wiper, it can destroy local as well as network files; utilizes timestomping technique and delete system logs to cover its track.	Exploiting vulnerable internet facing web servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Wiper		Wipes system data	-
ASSOCIATED ACTOR			**PATCH LINK**
Agrius			-
IOC TYPE	**VALUE**		
SHA256	38e406b17715b1b52ed8d8e4defdb5b79a4ddea9a3381a9f2276b00449ec8835, F65880ef9fec17da4142850e5e7d40ebfc58671f5d66395809977dd5027a6a3e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PartialWasher	PartialWasher is a data-wiping tool which is coded in C++. It supports command-line arguments	-	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Wipes data	-
Wiper			**PATCH LINK**
ASSOCIATED ACTOR			
Agrius			-
IOC TYPE	**VALUE**		
SHA256	ec7dc5bfadce28b8a8944fb267642c6f713e5b19a9983d7c6f011ebe0f663097		

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
BFG Agonizer	BFG Agonizeris an wiper. It has code similarities with CRYLINE-v5.0. It circumvent security measures by employing anti-hooking techniques.	Exploiting vulnerable internet facing web servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Wiper		Destroys system	-
ASSOCIATED ACTOR			**PATCH LINK**
Agrius			-
IOC TYPE	**VALUE**		
SHA256	c52525cd7d05bddb3ee17eb1ad6b5d6670254252b28b18a1451f604dfff932a4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
sqlextractor	It is a custom tool to extract information from database servers. Its purpose is to query SQL databases and extract sensitive PII data, such as ID numbers, Passport scans, Emails, Full addresses.	Exploiting vulnerable internet facing web servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Obtains sensitive data	-
ASSOCIATED ACTOR			**PATCH LINK**
Agrius			-
IOC TYPE	**VALUE**		
SHA256	a8e63550b56178ae5198c9cc5b704a8be4c8505fea887792b6d911e488592a7c		

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
ObjCShellz	The malware, written in Objective-C, operates as a remote shell, enabling attackers to execute commands on compromised systems. It communicates with its C2 server using a POST request, providing information about the victim's macOS version.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Executes custom commands	-
ASSOCIATED ACTOR			**PATCH LINK**
BlueNorOff			-
IOC TYPE	**VALUE**		
SHA256	ca6d8b8a84e40adb8949f37eef65315d1d25283583c0a65921414611e615b27d, cde067b700e5f39e276a104497bc3ae0a5677977376a1b4c87de3d03730000bf, 462f4ccc290b3cc87cdce2a82aa3f0cb48140a88b590ee175ef9c24180b545c7, fe31f8cba8fc3832da136778aa28c406bf8ef04b448cba076ff7f5f3b8be7683, 1219c2c14afd2db469b0ae479236ab45abd20f6092592b539e04ba7aceec25e2		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RustBucket	RustBucket is a new malware family that targets macOS systems. RustBucket is a multi-stage malware that uses a variety of techniques to infect its victims, including phishing emails, malicious websites, and drive-by downloads.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Steal sensitive information and install other malware	-
ASSOCIATED ACTOR			**PATCH LINK**
BlueNorOff			-
IOC TYPE	**VALUE**		
SHA256	812c795908f38bdb5cc20487569e53e04dfda8ad87ebe7156f3fb2fed1ab0b9b, 9fb57fca174506e96e2eda8db31a193b7476ce076557ff10617cdcae4d5716aa, a43c3097adb0d82eceb867957b54cc29e863d983daa547102361c59c0ac2a804, 070b2723a925d0788ddc3e5e4a214b7c64c61d44e5d01ca5bbe589f45256aa56, aa109f4fe27ed1f69e78a5aeba5356618ba24d8188077f0361c25a2e0d88874c		

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
AllaKore RAT	AllaKore RAT is an open-source remote access tool which has been modified for the purposes of SideCopy operations and is commonly observed in their intrusions.	Exploiting Vulnerability	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Keylogging, screenshotting, and gain remote access	-
ASSOCIATED ACTOR			**PATCH LINK**
SideCopy			Update WinRAR to latest version 6.23 and later.
IOC TYPE	**VALUE**		
SHA256	877dd8f41c3ba0172907fa90734fce8bcd39919bd24162788b47770da9b99a1b, afe63fb7f4841748dc56f20a2eb6a313eac613c22cdf23694af172c77af88a2d, 1c12c0c62642ebbab1fabc7bd56ffc9c1450e622f6d7ddba08b36ac3ad8b04e6, aad714bbff3546d3352baa53324c2f3e6be6ca61d5d397cc33b09ed470b4dda5, 58d88fd112acdf7161a83a29f4b74f6e697bb520c49e4ec740e9d46cacd33e8b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Ares RAT	Its is type of malicious software that allows an attacker to remotely control and monitor a victim's computer.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Steal data	-
ASSOCIATED ACTOR			**PATCH LINK**
SideCopy			Update WinRAR to latest version 6.23 and later.
IOC TYPE	**VALUE**		
SHA256	b88db92adab9bd72ef9a959de450aa1d4cad32415d0364832393820b355a238e, 6d911bfb01daa6f3acafd3ccb33b432d806c82b2b35c0c3408d822bf8c6b4c00, e93a7924bde0c145485edfa6307bdcbbba80972390f4fba35e57c215c20e8c43, 7cc6d203daa31ee9296848c85cfbd6f6e1b90126d9b02ab8b916922842b316a2, 8581920c2ddbce49fde6c18eab3853fc6ea30983215ab785fbd399d89c7bba7a		

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
DRat	DRat is capable of parsing as many as 13 commands from the C2 server to gather system data, download and execute additional payloads, and perform other file operations.	Exploiting Vulnerability	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Download and execute payload	-
ASSOCIATED ACTOR			**PATCH LINK**
SideCopy			Update WinRAR to latest version 6.23 and later.
IOC TYPE	**VALUE**		
SHA256	a216a8fd3f38baaca464642c733148d158256ef5e8156fb70b61e1993fb2abb7, 3dbb8941df5873feafec4b679522a8c237ba16fa045b8332a77b965c5a9ba167, 81259df59d29c22b1c29f178041396605ad2cacd696afe10cd3ba5ffc08278a3, 2f908408f0584fc2f529620c1ac492e766f603ca90618f1d4943ec214018d86b, ff7ca2e01237a0eaaed1f4523069f4c167cf84029dc766157ab10304e9d8c315		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Key RAT	Key RAT is a Windows based Remote Access Trojan, used by Threat Actor SideCopy in a campaign along side Ares RAT.	Exploiting Vulnerability	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Steal data	-
ASSOCIATED ACTOR			**PATCH LINK**
SideCopy			Update WinRAR to latest version 6.23 and later.
IOC TYPE	**VALUE**		
SHA256	df2426f378c8440ee906e3353513f57bd5e531b813e3d944ed85f995da1771e6, 28d45335ac6d45d1d7fbe9297f993dafce3dbc894c1719ca3f7f2ca458ec2c4d, 4a6e7e12ae447b26cc9f490a324ba1795444987e7a5a602a167ba0716ad8d911, 22b366c6bd4e5d8669f01a806eaf2a3aedcc77fb018ada01c31c5c7867b6be35, 6104be5bb34e14ebbeaa330085cd08dfca0782a2cca7099594cc85cf87dd6abc		

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
Millenium RAT	The Millenium RAT, a Win32 executable built on .NET, specifically version 2.4, can be found on GitHub and is available for purchase for $30, granting lifetime access.	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
RAT		Collect user data	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	eba4be8ed0e9282976f8ee0b04fb2474		
SHA1	f4d698ece0ff6af36c1a2e9108ea475518df0aa7		
SHA256	6d207c1e954f9d60f693e17e63df73fb8e954d02544b5d52b8b18c4ab86a267e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlazeStealer	The BlazeStealer payload can extract a malicious script from an external source, giving attackers complete control over the victim's computer. BlazeStealer runs a bot carried via the Discord messaging service using a unique identifier.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Download files, deactivate Windows Defender and Task Manager, and lock a computer by overloading the CPU	-
Stealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	77e183e63c70a44e87277be35b63817e185efcf1b8ab46937626904923251bbe, fb58f3f04e149b97a01c16a3bfedcb0ff33dc476dbab469fe011e3a379f2b00a, 87fda7a9d8156a9b3ca3ea92173c9c5c5abbd4a7e9f17c1b81e8921914cd5306, ccec28cfab447c153bc82993857b2ae865eab73c996d4db705ab1df6f1f29c40, b6c51f8700c067604354dc3f41cafb76ac7e3235fa7983c7407e18729dd94187		

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
Nokoyawa	Nokoyawa Ransomware, first discovered in February 2022, is written in Rust making it cross-platform and found to be sharing code with Karma ransomware family. It employs double-extortion technique.	-	-
		IMPACT	AFFECTED PRODUCTS
		Encrypts data	-
TYPE			PATCH LINK
Ransomware			
ASSOCIATED ACTOR			-
farnetwork			
IOC TYPE	VALUE		
SHA256	8800e6f1501f69a0a04ce709e9fa251c, 1e4dd35b16ddc59c1ecf240c22b8a4c4, f23be19024fcc7c8f885dfa16634e6e7, a2313d7fdb2f8f5e5c1962e22b504a17, 46168ed7dbe33ffc4179974f8bf401aa		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JSWORM	JSWORM is a malicious program classified as ransomware: a program designed to encrypt data and deliver a ransom-demand message. When a computer is infected with a virus of this type, the victim loses access to stored data.	-	-
		IMPACT	AFFECTED PRODUCTS
		Encrypts data	-
TYPE			PATCH LINK
Ransomware			
ASSOCIATED ACTOR			-
farnetwork			
IOC TYPE	VALUE		
SHA256	46761b8b727f3002d1c73fa6c8568ebcf2ec0066666251f66dcda9d4268e03e8		

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
Nefilim	Nefilim is a Ransomware as a Service(RaaS) operation first discovered in March 2020. Nefilim ransomware replaces the original files with encrypted versions.	-	-
		IMPACT	AFFECTED PRODUCTS
		Encrypt Data	-
TYPE			PATCH LINK
Ransomware			
ASSOCIATED ACTOR			-
farnetwork			
IOC TYPE	VALUE		
SHA256	08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, 205ddcd3469193139e4b93c8f76ed6bdbbf5108e7bcd51b48753c22ee620276, 5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, eacbf729bb96cf2eddac62806a555309d08a705f6084dd98c7cf93503927c34f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Karma	Karma is a type of malware that encrypts your files and demands a ransom payment to decrypt them. This ransomware is particularly dangerous because it uses strong encryption algorithms that make it very difficult to recover your files without paying the ransom.	-	-
		IMPACT	AFFECTED PRODUCTS
		Encrypt Data	-
TYPE			PATCH LINK
Ransomware			
ASSOCIATED ACTOR			-
farnetwork			
IOC TYPE	VALUE		
SHA256	a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0, 3ff1b90dbad5d78397fdc731c3a3c080d91fc488ac9152793b538b74a1e2d8f3, 4dec9a9044631caef283c7f39a576e4e5c1cc1e6a97ce5c60936a3a3d0097818, 124f3a5caf6eb464027f2865225a6a1238c3639e5b4a399f0f7f2dda7bd75aec, 0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27		

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
Nemty	Nemty is ransomware with an unusually complex encryption algorithm. This malware encrypts user files and demands money so that they can be unlocked again.	-	-
		IMPACT	AFFECTED PRODUCTS
		Encrypt data	-
TYPE			PATCH LINK
Ransomware			
ASSOCIATED ACTOR			-
farnetwork			
IOC TYPE	VALUE		
SHA256	267a9dcf77c33a1af362e2080aaacc01a7ca075658beb002ab41e0712ffe066e, 064debda941fb6b1ac7de62e4990f658ded67870f55f48757ab72a772c640995, 17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae, c41f14cf5a0c8d407b70cf07f552a5ba26db3b23bfdbfae7b24e7ff8de7ec1a7, dd228f63f0ef02749759ef6d75f9f84d5ba8b0787dadef0d41b390176ea5d6a1		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
FakeBat	It is a malicious software loader and dropper that associated with malvertising campaigns.	Google Ads	-
		IMPACT	AFFECTED PRODUCTS
		Distribute infostealers	-
TYPE			PATCH LINK
Loader			
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	a80846156595af47a977182395583d0b981e091d1281258e81860a0edfdd0159, a1f64f609b0d28707f2132e54d3a19d80f36806557a6031cd8f3154fb8a559be, a80846156595af47a977182395583d0b981e091d1281258e81860a0edfdd0159, 37620313dd1e5277a53e3dcef980e29b2315f4fafe7376fc1a2b941432c0de39, d9c62b110e0049f7ca3f0ccaa7d0058adad9cfdca27b8ab240ec0db70a8a2193		

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
Redline stealer	Redline is a potent information-stealing malware designed to harvest sensitive data, including passwords, cookies, and cryptocurrency-related information.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Harvest information	-
Infostealer			PATCH LINK
ASSOCIATED ACTOR			-
-			
IOC TYPE	VALUE		
SHA256	9f9b6cf7810c6aaadde785a65dd4c7f941c14ec4de7f68ecc6964353fa02e01e, 80af7bf074366eb628c1b08f30f3a8ec1ce44546cf119b7111b546acedec7059, 5d50717f5a866456842ee76543682f0f500619c4f7b12c548be9ea1c0e9c981b, 78dd1b88bea0150d68adb20296c9d819cabb3c587448e046558f97851655b262, 7b867d7b59955eaf09166f3c519b468661dcce3fc54ad63e24db14a26265a080		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Clop ransomware	Clop Ransomware is a dangerous file encrypting virus which actively avoids the security unprotected system and encrypts the saved files by planting the .Clop extension. It exploits AES cipher to encrypt pictures, videos, music, databases papers.	-	CVE-2023-47246
		IMPACT	AFFECTED PRODUCTS
TYPE		Encrypt data	-
Ransomware			PATCH LINK
ASSOCIATED ACTOR			https://documentation.sysaid.com/docs/latest-version-installation-files
Lace Tempest			
IOC TYPE	VALUE		
MD5	31e0439e6ef1dd29c0db6d96bac59446, 4431b6302b7d5b1098a61469bdfca982, 5e52f75d17c80dd104ce0da05fdfc362, 8bd774fbc6f846992abda69ddabc3fb7, afe7f87478ba6dfca15839f958e9b2ef		

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 rowspan="2">Gracewire (aka FlawedGrace)</td><td rowspan="5">It is written in C++. It seems to have been developed in the second half of 2017. GraceWire infections can result in financial loss, serious privacy issues and identity theft.</td><td>-</td><td>CVE-2023-47246</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td rowspan="3">Data theft</td><td>-</td></tr>
<tr><td>TYPE</td><td rowspan="2">PATCH LINK</td></tr>
<tr><td>RAT</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td colspan="2" rowspan="2">https://documentation.sysaid.com/docs/latest-version-installation-files</td></tr>
<tr><td>Lace Tempest</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>MD5</td><td colspan="3">88695dbddd4fc57025b523f4fca268d7,
80a20106ced1a5d9f350b1401dbe7d14</td></tr>
<tr><td>SHA1</td><td colspan="3">57ab5d9b5302644e91e3953062b40c5346b236e3,
753561bf6da3cbb75711d109ed0e38b7abb28db8</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-2023-4911	✗	All systems running glibc 2.34 to 2.37	Kinsing
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:gnu:c_library:*:*:*:*:*:*:*:*	-
Glibc Buffer Overflow Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1574: Hijack Execution Flow	Upgrade glibc to 2.38 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-9841	✗	Oracle Communications Diameter Signaling Router	Kinsing
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:phpunit_project:phpunit:*:*:*:*:*:*:*:*	-
PHPUnit Command Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1055: Process Injection	https://www.oracle.com/security-alerts/cpuoct2021.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗ ZERO-DAY	WinRAR version 6.22 and older versions	SideCopy
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*:*	AllaKore RAT, Ares RAT, DRat, Key RAT
RARLAB WinRAR Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-47246	✗ ZERO-DAY	SysAid: 21.4.45 - 23.3.35	Lace Tempest
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:sysaid:sysaid:-:*:*:*:*:*:*:*	Clop ransomware, Gracewire
SysAid path traversal vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1588.006: Vulnerabilities	https://documentation.sysaid.com/docs/latest-version-installation-files

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Kinsing (aka Money Libra)	-	Cryptocurrency	Worldwide
	MOTIVE		
	Information Theft		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-4911 CVE-2017-9841	-	GNU C Library (glibc), Oracle Communications Diameter Signaling Router

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0040: Impact; T1059: Command and Scripting Interpreter; T1059.006: Python; T1059.007: JavaScript; T1505: Server Software Component; T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1027: Obfuscated Files or Information; T1003: OS Credential Dumping; T1082: System Information; Discovery; T1083: File and Directory Discovery; T1140: Deobfuscate/Decode Files or Information; T1496: Resource Hijacking

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Agrius (aka Agonizing Serpens, DEV-0227, BlackShadow, SharpBoys, AMERICIUM, Pink Sandstorm)</td><td>Iran</td><td rowspan="2">Education, Technology</td><td rowspan="2">Hong Kong, Israel, South Africa</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Sabotage and destruction</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>MultiLayer, PartialWasher, BFG Agonizer, sqlextractor</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0040:Impact; T1595: Active Scanning; T1190:Exploit Public-Facing Application; T1003: OS Credential Dumping; T1560: Archive CollectedData; T1490: Inhibit System Recovery; T1574: Hijack Execution Flow; T1059: Command and Scripting Interpreter; T1110: Brute Force; T1005: Data from Local System; T1041: Exfiltration Over C2 Channel; T1485: Data Destruction; T1561: Disk Wipe;</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 BlueNorOff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet, TAG-71)	North Korea	Cryptocurrency, Financial	-
	MOTIVE		
	Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ObjCShellz, RustBucket	-
TTPs			
TA0005: Defense Evasion; TA0010: Exfiltration; TA0011: Command and Control; TA0002: Execution; TA0040: Impact; TA0042: Resource Development; T1583: Acquire Infrastructure; T1583.001: Domains; T1059: Command and Scripting Interpreter; T1204: User Execution; T1204.001: Malicious Link; T1588.001: Malware; T1588: Obtain Capabilities; T1020: Automated Exfiltration; T1071: Application Layer Protocol; T1105: Ingress Tool Transfer			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 SideCopy	Pakistan	Government	India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-38831	AllaKore RAT, Ares RAT, DRat, Key RAT	WinRAR

TTPs

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1583: Acquire Infrastructure; T1583.001: Domains; T1584: Compromise Infrastructure; T1584.001: Domains;T1588: Obtain Capabilities; T1588.001: Malware; T1588.002: Tool; T1608: Stage Capabilities; T1608.001: Upload Malware; T1608.005: Link Target; T1566: Phishing; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1106: Native API; T1129: Shared Modules; T1059: Command and Scripting Interpreter; T1047: Windows Management Instrumentation;T1203: Exploitation for Client Execution; T1204: User Execution;T1204.001: Malicious Link;T1204.002: Malicious File; T1053: Scheduled Task/Job;T1053.003: Cron;T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder;T1547.013: XDG Autostart Entries; T1036: Masquerading;T1036.005: Match Legitimate Name or Location; T1140: Deobfuscate/Decode Files or Information;T1218: System Binary Proxy Execution;T1218.005: Mshta; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading;T1222: File and Directory Permissions Modification; T1222.002: Linux and Mac File and Directory Permissions Modification;T1027: Obfuscated Files or Information; T1027.009: Embedded Payloads;T1027.010: Command Obfuscation; T1012: Query Registry;T1033: System Owner/User Discovery; T1057: Process Discovery;T1082: System Information Discovery; T1083: File and Directory Discovery;T1016: System Network Configuration Discovery; T1016.001: Internet Connection Discovery;T1518: Software Discovery; T1518.001: Security Software Discovery;T1005: Data from Local System; T1056: Input Capture;T1056.001: Keylogging; T1074: Data Staged;T1074.001: Local Data Staging; T1119: Automated Collection; T1113: Screen Capture;T1125: Video Capture; T1105: Ingress Tool Transfer;T1571: Non-Standard Port; T1573: Encrypted Channel;T1071: Application Layer Protocol; T1071.001: Web Protocols;T1041: Exfiltration Over C2 Channel

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
farnetwork (aka farnetworkl, jingo, jsworm, razvrat, piparkuka, and farnetworkit)</td><td>-</td><td rowspan="3">Utilities, Construction, Engineering, Trading Companies, Healthcare, Hotels, Restaurants & leisure, Distributors, Road & rail, Media, Education Services, and Automotive</td><td rowspan="3">United States, Korea, Canada, Morocco, Saint Kitts and Nevis</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Develop ransomware</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Nokoyawa, JSWORM, Nefilim, Karma, and Nemty</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0040: Impact; T1190: Exploit Public-Facing Application; T1059.001: PowerShell; T1027: Obfuscated Files or Information; T1083: File and Directory Discovery; T1113: Screen Capture; T1114: Email Collection; T1005: Data from Local System; T1490: Inhibit System Recovery; T1048: Exfiltration Over Alternative Protocol: T1486: Data Encrypted for Impact; T1491: Defacement; T1555: Credentials from Password Stores; T1059: Command and Scripting Interpreter</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
Lace Tempest (aka DEV-0950, FIN11)</td><td>-</td><td rowspan="3">Defense, Education, Energy, Financial, Hospitality, Retail, Telecommunications, Technology, Transportation</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime, Financial gain</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2023-47246</td><td>Clop ransomware, Gracewire</td><td>SysAid servers</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1588.006: Vulnerabilities; T1588: Obtain Capabilities; T1059.001: PowerShell; T1543: Create or Modify System Process; T1505: Server Software Component; T1564: Hide Artifacts; T1059: Command and Scripting Interpreter; T1083: File and Directory Discovery; T1046: Network Service Discovery; T1057: Process Discovery; T1070: Indicator Removal; T1570: Lateral Tool Transfer; T1213: Data from Information Repositories; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actor **Kinsing, Agrius, BlueNorOff, SideCopy, farnetwork, Lace Tempest** and malware **Socks5Systemz, PrivateLoader, Amadey, Jupyter Infostealer, MultiLayer, PartialWasher, BFG Agonizer, sqlextractor, ObjCShellz, RustBucket, AllaKore RAT, Ares RAT, DRat, Key RAT, Millenium RAT, BlazeStealer, Nokoyawa,JSWORM, Nefilim, Karma, Nemty, FakeBat, Redline stealer, Clop ransomware, Gracewire.**

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 **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Kinsing, Agrius, BlueNorOff, SideCopy, farnetwork, Lace Tempest** and malware **Socks5Systemz, PrivateLoader, Amadey, Jupyter Infostealer, MultiLayer, PartialWasher, BFG Agonizer, sqlextractor, ObjCShellz, RustBucket, AllaKore RAT, Ares RAT, DRat, Key RAT, Millenium RAT, FakeBat, Redline stealer, Clop ransomware, Gracewire** in Breach and Attack Simulation(BAS).

Threat Advisories

Socks5Systemz Proxy Botnet Infects 10,000 Systems

Kinsing Exploits Looney Tunables Vulnerability to Breach Cloud Environments

Jupyter Infostealer Returns with New Addition to Its Arsenal

Iran-Backed Agrius APT's Attacks on Israeli Institutions

BlueNoroff Unleashes New macOS Malware ObjCShellz

SideCopy Leverages Multi-platform RAT, Assaults Indian Government Entities

Millenium RAT the $30 Access Ticket to Data Theft

Chinese APT Masquerading as Cloud Services in Cambodia

BlazeStealer Malware Uncovered in Python Packages on PyPI

Farnetwork the Mastermind of Five Ransomware Strains

Malicious CPU-Z App Distributed Through Ads on Fake Windows News Site

Lace Tempest Exploits Zero-Day in a Strategic Strike on SysAid

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 been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Socks5Systemz	SHA256	fee88318e738b160cae22f6c0f16c634fd16dbf11b9fb93df5d380b6427ac18f
PrivateLoader	MD5	6cc7d9664c1a89c58549e57b5959bb38
	SHA1	85b665c501b9ab38710050e9a5c1b6d2e96acccc
	SHA256	27c1ed01c767f504642801a7e7a7de8d87dbc87dee88fbc5f6adb99f069afde4
Amadey	SHA256	68cf6c33c3a11405e8f66b1cd769ac4b9ed53fa702d06323d737f86bb238f0aa, 31fcc145a7951bdb76f7635a0b7bb4ca6649fd8b2e6d5a166dfac138a71200bc, 2260d1b05abe62e94794dfc3d91d34d4751c6ccbdd450c2d3bbf01cb1aa31eec, e865cb5fbed88a0ef8d09376530d4fd855358dba91fa3f3d1296fb03085e8e06, 3141087bc31d396d4151e1bf8b61254374b503faefe444f17316ac40ba5c845b, 39a5de74cb6a87c849ac4d30e9902368f6638f27b98149b13ee8c6e6c4dd646f, d6780e515a8143aa9d8097deae4cba874790690f6743c51f8e03a1af4cf7c0b8, 8a9dda4423be29f85da1210beb83aab506609b9c03fcefd7bf022bd97823a808,

Attack Name	TYPE	VALUE
Amadey	SHA256	a6bd53b43ef7820cb928829288276a9dc67c2746b8e07f0e83413cfacd2edfea, 4b4e85691ca2565dff2b966ff4ad72d617bf65cf02b541add5c66fb8a6747385, b8df7f85014ca1cd332cb971f07e4f78356e9d8c55cfcda3d88ea3c82806c555, 8543412d724c9c2353dc04e956e594341ae71a8aa4cb65778cd77d117014a94d, 25fdb52a6c215c2d3f797ffd349a0d30526f2d5a2d3a6309ff257591f1cf8f00, d721fb8b3424db73480e0f470438275fdea19ec670d7b0107f40571d44612f9f, d3f2db4b59bc69967a1f9206c6f79420247c72bac298c840bbfedd75937bc6b2, 371c1e62cbc18626b2cc6ba6893b71e9a9d945fc5391b5b85ee4ff2b7500f11e, 61afafb954376565e69f6a48e335320c00d529bf0677fe150f1217bf1a7efce3, 1fb2e848188b19f262e131fe524d450413b8e739c50c252a40291e6434bf396b, 06fcfe784a220b6515b8db1471567625bd8150878b404c8c96954e37c556488e, 931008fbe82fffa6412e9539e6a32e309032e76bba0b112ef730a9551df80110
Jupyter Infostealer	SHA256	c03ff646f732bf3a13b52e4786828af05a211ad69674cc2c11089681bc67ece9, e7ded7fb9f1aa432a3eb598d00157afb67b201647da234f785397a117f046e34, 1d322817bea6534d8b55282eb227a1fcca076b9d60b8b2fa0d3f756f4e38085c, d7f8a922f22d105d5190e91efb592335d5ccdee0fe3615dc3863cdef90a97738, 6738651649eedf22d352fcb5bb3942125487d63c26d7243fee8a25d295187996, df3bba9d570e70caa2f7eb716d9c2c371b535171fee4320af359a85662c45af7, 31cff99a12e1f7b8ae8966021b305d9bf2e2b7276b5c6857bfc45e8d833868f7, 67ddf04e5f8d7668ce666d00af3b3d7212bff8ded5999d36d131a77a4d5bd890, 8dae48b2f3cb1a57d4aff42417bbeace09e7329e0e06c525140a8f65755075df, 23e725d71caa459c745bdad9267d6164096223a4f5f2df03a92d9b49b195386f, 631685a0368e3b2dccea434258beb18dddb47532c17144b455f4218215ba8ceb,

Attack Name	TYPE	VALUE
Jupyter Infostealer	SHA256	cc3d26f0938038eaa113e22640f330275c791e997ff7e822101c174cb693cba0, 1d944510c663c8c452c1784920172d16af4fa1db8a47aba9a5af973665a02a5a, 4f97380eaf66818246136a840df90424e06d6a931a630a42581c0ef5d9825736, 3f55947c29d8b3c50038dd7756e4bb1edb3908318df6f0df082d311582cc7df9
MultiLayer	SHA256	38e406b17715b1b52ed8d8e4defdb5b79a4ddea9a3381a9f2276b00449ec8835, f65880ef9fec17da4142850e5e7d40ebfc58671f5d66395809977dd5027a6a3e
PartialWasher	SHA256	ec7dc5bfadce28b8a8944fb267642c6f713e5b19a9983d7c6f011ebe0f663097
BFG Agonizer	SHA256	c52525cd7d05bddb3ee17eb1ad6b5d6670254252b28b18a1451f604dfff932a4
sqlextractor	SHA256	a8e63550b56178ae5198c9cc5b704a8be4c8505fea887792b6d911e488592a7c
ObjCShellz	SHA256	ca6d8b8a84e40adb8949f37eef65315d1d25283583c0a65921414611e615b27d, cde067b700e5f39e276a104497bc3ae0a5677977376a1b4c87de3d03730000bf, 462f4ccc290b3cc87cdce2a82aa3f0cb48140a88b590ee175ef9c24180b545c7, fe31f8cba8fc3832da136778aa28c406bf8ef04b448cba076ff7f5f3b8be7683, 1219c2c14afd2db469b0ae479236ab45abd20f6092592b539e04ba7aceec25e2
RustBucket	SHA256	812c795908f38bdb5cc20487569e53e04dfda8ad87ebe7156f3fb2fed1ab0b9b, 9fb57fca174506e96e2eda8db31a193b7476ce076557ff10617cdcae4d5716aa, a43c3097adb0d82eceb867957b54cc29e863d983daa547102361c59c0ac2a804, 070b2723a925d0788ddc3e5e4a214b7c64c61d44e5d01ca5bbe589f45256aa56, aa109f4fe27ed1f69e78a5aeba5356618ba24d8188077f0361c25a2e0d88874c

Attack Name	TYPE	VALUE
AllaKore RAT	IP	38.242.149[.]89:61101
	SHA256	877dd8f41c3ba0172907fa90734fce8bcd39919bd24162788b47770da9b99a1b, afe63fb7f4841748dc56f20a2eb6a313eac613c22cdf23694af172c77af88a2d, 1c12c0c62642ebbab1fabc7bd56ffc9c1450e622f6d7ddba08b36ac3ad8b04e6, aad714bbff3546d3352baa53324c2f3e6be6ca61d5d397cc33b09ed470b4dda5, 58d88fd112acdf7161a83a29f4b74f6e697bb520c49e4ec740e9d46cacd33e8b, faa422583f5a7e7d7c02be9a26babe2554412caa46135069f5ebb8673e9ef87b, 4896f8e0166fd0a313727ee94a65fe3a641e2feed3055523e2330fb0028b2c16, c6e59cefdff4dfc83aebf8e4a7a054f6a0820f7f52ceb03566a837823d29a7c7, c1ef58bc181bd3175d8b2f023299d261d40642bced2692251eb254cf5fdc3182
Ares RAT	IP	38.242.220[.]166:9012, 161.97.151[.]220:7015
	SHA256	b88db92adab9bd72ef9a959de450aa1d4cad32415d0364832393820b355a238e, 6d911bfb01daa6f3acafd3ccb33b432d806c82b2b35c0c3408d822bf8c6b4c00, e93a7924bde0c145485edfa6307bdcbbba80972390f4fba35e57c215c20e8c43, 7cc6d203daa31ee9296848c85cfbd6f6e1b90126d9b02ab8b916922842b316a2, 8581920c2ddbce49fde6c18eab3853fc6ea30983215ab785fbd399d89c7bba7a, 1a763a883378ba1b4a22706267612ca7a19ff30217266622d2f094d7846c654f, 23ef884798a128d49ac864e9cfe49047d3d10e845ec330ab22f059f0d4e35436, f5dddb1cd616f63a21d85d5970b5826c803069ca83b21e9751d28579ee6ebfec, e750e151e11eba9d0ab2f814dd24b2d1551eaf9cb95ab99e951d66619159219e, bf399563930b4af267c2d415b5d5cb208c2eeb9a37536437c993a311e0211e95

Attack Name	TYPE	VALUE
DRat	IP	38.242.149[.]89:9828
	SHA256	a216a8fd3f38baaca464642c733148d158256ef5e8156fb70b61e1993fb2abb7, 3dbb8941df5873feafec4b679522a8c237ba16fa045b8332a77b965c5a9ba167, 81259df59d29c22b1c29f178041396605ad2cacd696afe10cd3ba5ffc08278a3, 2f908408f0584fc2f529620c1ac492e766f603ca90618f1d4943ec214018d86b, ff7ca2e01237a0eaaed1f4523069f4c167cf84029dc766157ab10304e9d8c315, 20b4d856ee4b11e2a859bd83d2cd0e0a8c92c739a9753b5c98ee36af27b017e3, 612a094dc4324cb185b17ec8ce76404768b5c620059b2d7fc99a2fdc43e3a182, ee26deb66c5dbcf66c0bcc6334826d203373fcd59a8db4ce0173ece660506267, 64937789f8faba1ef5eba05ba2c2ffaaf8bbc80c016efac1b377ffadf8677da9, 5d42a118f2f693c04e46ca7c89d4d10e8d2cf46ab2841d283d66c17859c0ee57, ec5f5674c3172d59252dac023e52f99f530c89c35bd2a03197a868fbf58d40f3
Key RAT	IP	207.180.192[.]77:6023
	SHA256	df2426f378c8440ee906e3353513f57bd5e531b813e3d944ed85f995da1771e6, 28d45335ac6d45d1d7fbe9297f993dafce3dbc894c1719ca3f7f2ca458ec2c4d, 4a6e7e12ae447b26cc9f490a324ba1795444987e7a5a602a167ba0716ad8d911, 22b366c6bd4e5d8669f01a806eaf2a3aedcc77fb018ada01c31c5c7867b6be35, 6104be5bb34e14ebbeaa330085cd08dfca0782a2cca7099594cc85cf87dd6abc, c7b70220ffa115b777b782698bd435dedf7e4d5aaebabc2230b85b26b55d189c, 68597413352459cb460a08d9fcacfd7650c36223bd0bc3eaa42a1c2f9c2dd939, 9d34900d4d58aa60f09f6d428be018ac9d2850b05a432d371d1c236ae3e204b2, 7dcdc9d0722b6e103bd80394e8eee19d8201a67f387a1e24a9d0b6c260ecf5ec, 7636f7f8f573b806bd473e89a82d404fa692085b8ebd3d03238f69e61e20aa14

Attack Name	TYPE	VALUE
Millenium RAT	MD5	eba4be8ed0e9282976f8ee0b04fb2474
	SHA1	f4d698ece0ff6af36c1a2e9108ea475518df0aa7
	SHA256	6d207c1e954f9d60f693e17e63df73fb8e954d02544b5d52b8b18c4ab86a267e
BlazeStealer	SHA256	77e183e63c70a44e87277be35b63817e185efcf1b8ab46937626904923251bbe, fb58f3f04e149b97a01c16a3bfedcb0ff33dc476dbab469fe011e3a379f2b00a, 87fda7a9d8156a9b3ca3ea92173c9c5c5abbd4a7e9f17c1b81e8921914cd5306, ccec28cfab447c153bc82993857b2ae865eab73c996d4db705ab1df6f1f29c40, b6c51f8700c067604354dc3f41cafb76ac7e3235fa7983c7407e18729dd94187, 9c3637d925b3bb46ad68e7667e5958cc6e0926d9b12f022c6e0e990d63f45a9d, a0422225d67779574006c04bd95bb19c02c5dd94f0af009606d58cf0b3854d6d, 14288b82c089fd1edd66feef6b0ff656d723f2e893b8c2574495b64c48b762a5, 51d5f41603a4a311c63e3db5d1cf8d5ddba28aa5cdabff62cad9f646fce8b5da, 716df8c14081570de5489c54a6e1d87d28f5d9d6848ab2b11654a5a3fbb29880
Nokoyawa	MD5	8800e6f1501f69a0a04ce709e9fa251c, 1e4dd35b16ddc59c1ecf240c22b8a4c4, f23be19024fcc7c8f885dfa16634e6e7, a2313d7fdb2f8f5e5c1962e22b504a17, 46168ed7dbe33ffc4179974f8bf401aa, 2e936942613b9ef1a90b5216ef830fbf, feb7b1e0161df136c3d385bfd2d4b247, c159afb7d2111690326cad610776db34
JSWORM	SHA256	46761b8b727f3002d1c73fa6c8568ebcf2ec0066666251f66dcda9d4268e03e8
Nefilim	SHA256	08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, 205ddcd3469193139e4b93c8f76ed6bdbbf5108e7bcd51b48753c22ee620276, 5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599,

Attack Name	TYPE	VALUE
Nefilim	SHA256	eacbf729bb96cf2eddac62806a555309d08a705f6084dd98c7cf93503927c34f, ee9ea85d37aa3a6bdc49a6edf39403d041f2155d724bd0659e6884746ea3a250, f51f128bca4dc6b0aa2355907998758a2e3ac808f14c30eb0b0902f71b04e3d5, fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7, 24ada19b269279612370bdf16f2becc1d5b7e0f69821050e2d9b48cfc874dca0, b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e, 7de8ca88e240fb905fc2e8fd5db6c5af82d8e21556f0ae36d055f623128c3377, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, 5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1, 24f1b3b9562ffa9b87b1497397c3da9dffa9f872f96b77d2643b18f9846aafaa, b227fa0485e34511627a8a4a7d3f1abb6231517be62d022916273b7a51b80a17, 0125e74c95d3e2762f7e29dc833592f33d5ded892ba4708e2b519eb5f400c2ee, 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7, 35a0bced28fd345f3ebfb37b6f9a20cc3ab36ab168e079498f3adb25b41e156f, 5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6, 3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953, ea6ced3730495e2231c1a755fcc1aefac7622ac4bd5e269b2a5996572acb42f9, 2e25bdd600695cfed0d4ee3aca4f121bfebf0de889593e6ba06282845cf39ea, d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3, 5104b8abb22cca1b078dd5b86e61f515a73404b0269fe7e6765ec818fbdf830b, 2b4b2a707662973236ae9b2fc732533b5d7236b279a2fccb2874da07e09af4b3, 7d7c44f9c577c0af913d905b51797f17399d650de0331885abc8828c2696d37f,

Attack Name	TYPE	VALUE
Nefilim	SHA256	8b35aa930dd7260060f12ff92f1447850fc1a6bd79a28ba05a2d4e54a3aad504, fd3c8be2d1ead92101e8909a85695a0a40c2576c87eefeef6d32376a7fe22f1c, fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020, 3bac058dbea51f52ce154fed0325fd835f35c1cd521462ce048b41c9b099e1e5, 8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b, 353ee5805bc5c7a98fb5d522b15743055484dc47144535628d102a4098532cd5
Karma	SHA256	a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0, 3ff1b90dbad5d78397fdc731c3a3c080d91fc488ac9152793b538b74a1e2d8f3, 4dec9a9044631caef283c7f39a576e4e5c1cc1e6a97ce5c60936a3a3d0097818, 124f3a5caf6eb464027f2865225a6a1238c3639e5b4a399f0f7f2dda7bd75aec, 0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27, 1c41acdc2e9d8b89522ebb51d65b4c41d7fd130a14ce9d449edb05f53bbb8d59, ad841882052c3f9d856ad9a393232e0a59d28e17c240d23258f1dac62f903ab8, 19417c0a38a1206007a0cc82c0fc2e19db897214d27d0998bc4dbac53cc2788d, a63937d94b4d0576c083398497f35abc2ed116138bd22fad4aec5714f83371b0, 34629751d8202be456dcf149b516afefc980a9128dd6096fd6286fee530a0d20, 0d037ee0252e4f26800bcf7c750f61d0c549b7ba0a522c75e8d96dcf4f689e27, 6c98d424ab1b9bfba683eda340fef6540ffe4ec4634f4b95cf9c70fe4ab2de90
Nemty	SHA256	267a9dcf77c33a1af362e2080aaacc01a7ca075658beb002ab41e0712ffe066e, 064debda941fb6b1ac7de62e4990f658ded67870f55f48757ab72a772c640995, 17f746d82695fa9b35493b41859d39d786d32b23a9d2e00f4011dec7a02402ae, c41f14cf5a0c8d407b70cf07f552a5ba26db3b23bfdbfae7b24e7ff8de7ec1a7, dd228f63f0ef02749759ef6d75f9f84d5ba8b0787dadef0d41b390176ea5d6a1,

Attack Name	TYPE	VALUE
Nemty	SHA256	4cf87dd16d57582719a8fe6a144360f3dfa5d21196711dc140ce1a738ab9816e, abf148370f7cc9c16e20c30590a08f85208f4e594062c8a9e59c0c89cd8ff43f, ddadfcc43e4576de65f5844396a08fec47410663a6b6921991206b7a0df32ada, 57e25a37d8279fe563415d636b1983d447b5521ec6c024e18fd4d578840d2e20, 9913afe01dc4094bd3c5ff90ca27cc9e9ef7d77b6a7bdbf5f3042a8251b96325, 1d828a6c85bd5896ea27eeb17483dfe3bef81e0bf31521c91bcdf2559a03da1f, 31ee05823a66851cf6965f32d02e767206785d0bf0c9fa65e7dcf1ffed32c18e, 12da8dee83df90880d7d9cb4b0a7b608950bb57e9bc59c8b96f68c364350447c, d809ab5906fe6dba964cb30a21753213f5b077e28abb67680b2f28d65cbfc83b, a7558decb9516122781243e791c982977660152813817fb7ed00359365fcb0d3, e410854d9c8afe6e691c0ae638dfd04d792c3745dbb9e335f6f949e7a6b298d8, 5439452012a052851fdd0625abc4559302b9d4f4580e2ec98680e9947841d75d, a9f6d5ad40d5b073be92fc46666ce1f96e30c50494a018d472cfee56ff2b8c65, a5590a987d125a8ca6629e33e3ff1f3eb7d5f41f62133025d3476e1a6e4c6130, 3a061909a2631041b16d1d57212c1f44baca897efce50d095a141f8b7563db0b, 17864c4e21c0ebaf30cca1f35d67f46d3c3c33a5b8ea87d4c331e9d86d805965, a127323192abed93aed53648d03ca84de3b5b006b641033eb46a520b7a3c16fc, 2c41b93add9ac5080a12bf93966470f8ab3bde003001492a10f63758867f2a88, b227fa0485e34511627a8a4a7d3f1abb6231517be62d022916273b7a51b80a17, b8066b7ec376bc5928d78693d236dbf47414571df05f818a43fb5f52136e8f2e, 7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599, fcc2921020690a58c60eba35df885e575669e9803212f7791d7e1956f9bf8020, 8be1c54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b,

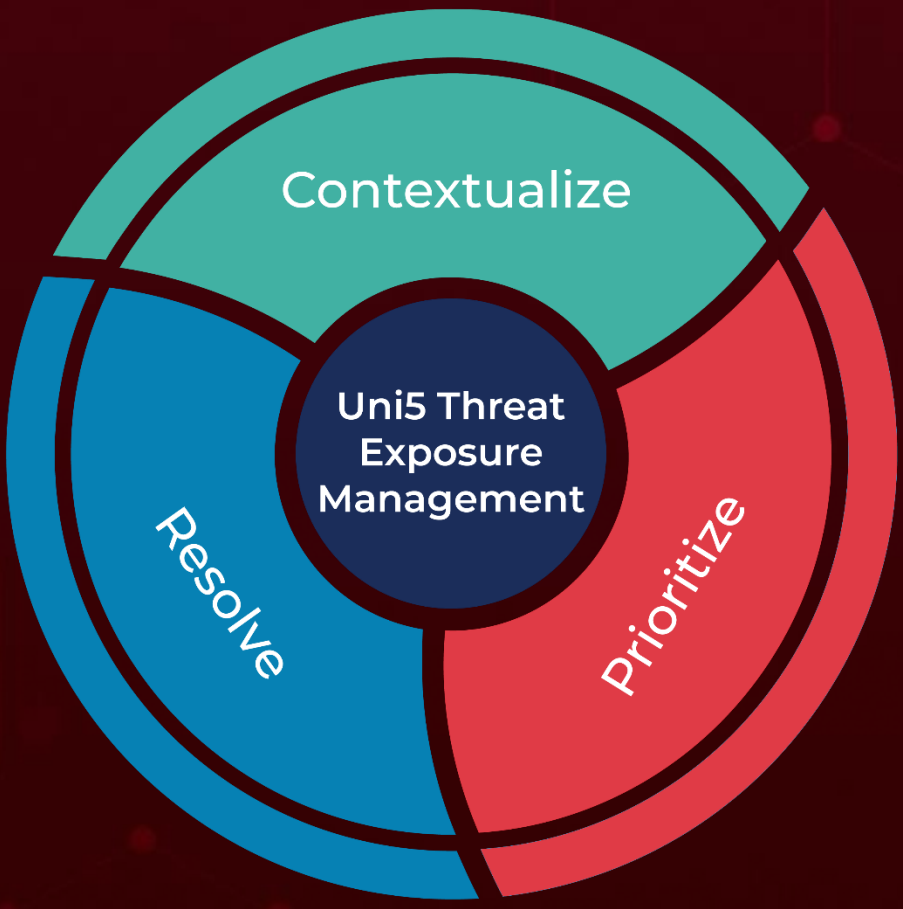
Attack Name	TYPE	VALUE
Nemty	SHA256	3080b45bab3f804a297ec6d8f407ae762782fa092164f8ed4e106b1ee7e24953, 5ab834f599c6ad35fcd0a168d93c52c399c6de7d1c20f33e25cb1fdb25aec9c6, d4492a9eb36f87a9b3156b59052ebaf10e264d5d1ce4c015a6b0d205614e58e3, 35a0bced28fd345f3ebfb37b6f9a20cc3ab36ab168e079498f3adb25b41e156f, 08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641, 3bac058dbea51f52ce154fed0325fd835f35c1cd521462ce048b41c9b099e1e5, 353ee5805bc5c7a98fb5d522b15743055484dc47144535628d102a4098532cd5, 52e25bdd600695cfed0d4ee3aca4f121bfebf0de889593e6ba06282845cf39ea, 7de8ca88e240fb905fc2e8fd5db6c5af82d8e21556f0ae36d055f623128c3377
FakeBat	SHA256	a80846156595af47a977182395583d0b981e091d1281258e81860a0edfdd0159, a1f64f609b0d28707f2132e54d3a19d80f36806557a6031cd8f3154fb8a559be, a80846156595af47a977182395583d0b981e091d1281258e81860a0edfdd0159, 37620313dd1e5277a53e3dcef980e29b2315f4fafe7376fc1a2b941432c0de39, d9c62b110e0049f7ca3f0ccaa7d0058adad9cfdca27b8ab240ec0db70a8a2193
Redline stealer	SHA256	9f9b6cf7810c6aaadde785a65dd4c7f941c14ec4de7f68ecc6964353fa02e01e, 80af7bf074366eb628c1b08f30f3a8ec1ce44546cf119b7111b546acedec7059, 5d50717f5a866456842ee76543682f0f500619c4f7b12c548be9ea1c0e9c981b, 78dd1b88bea0150d68adb20296c9d819cabb3c587448e046558f97851655b262, 7b867d7b59955eaf09166f3c519b468661dcce3fc54ad63e24db14a26265a080
Clop ransomware	MD5	31e0439e6ef1dd29c0db6d96bac59446, 4431b6302b7d5b1098a61469bdfca982, 5e52f75d17c80dd104ce0da05fdfc362, 8bd774fbc6f846992abda69ddabc3fb7, afe7f87478ba6dfca15839f958e9b2ef, dd5cee48cdd586045c5fb059a1120e15, f59d2a3c925f331aae7437dd7ac1a7c8

Attack Name	TYPE	VALUE
Clop ransomware	SHA1	40b7b386c2c6944a6571c6dcfb23aaae026e8e82, 46b02cc186b85e11c3d59790c3a0bfd2ae1f82a5, 4fa2b95b7cde72ff81554cfbddc31bbf77530d4d, 77ea0fd635a37194efc1f3e0f5012a4704992b0e, a1a628cca993f9455d22ca2c248ddca7e743683e, a6e940b1bd92864b742fbd5ed9b2ef763d788ea7, ac71b646b0237b487c08478736b58f208a98eebf, ba5c5b5cbd6abdf64131722240703fb585ee8b56
Gracewire	MD5	88695dbddd4fc57025b523f4fca268d7, 80a20106ced1a5d9f350b1401dbe7d14
	SHA1	57ab5d9b5302644e91e3953062b40c5346b236e3, 753561bf6da3cbb75711d109ed0e38b7abb28db8
	SHA256	f92dbf7943590c2c4011f911ba9ba445010c9d5895b5c8b57a5da9c8708c221d, 6d15a0807858dce0be652e480fa7f298482c7bbf2c1e116e6cf0a3d3df95180f

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

November 14, 2023 . 8:16 PM

More at www.hivepro.com