Date of Publication
October 16, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

9 to 15 OCTOBER 2023

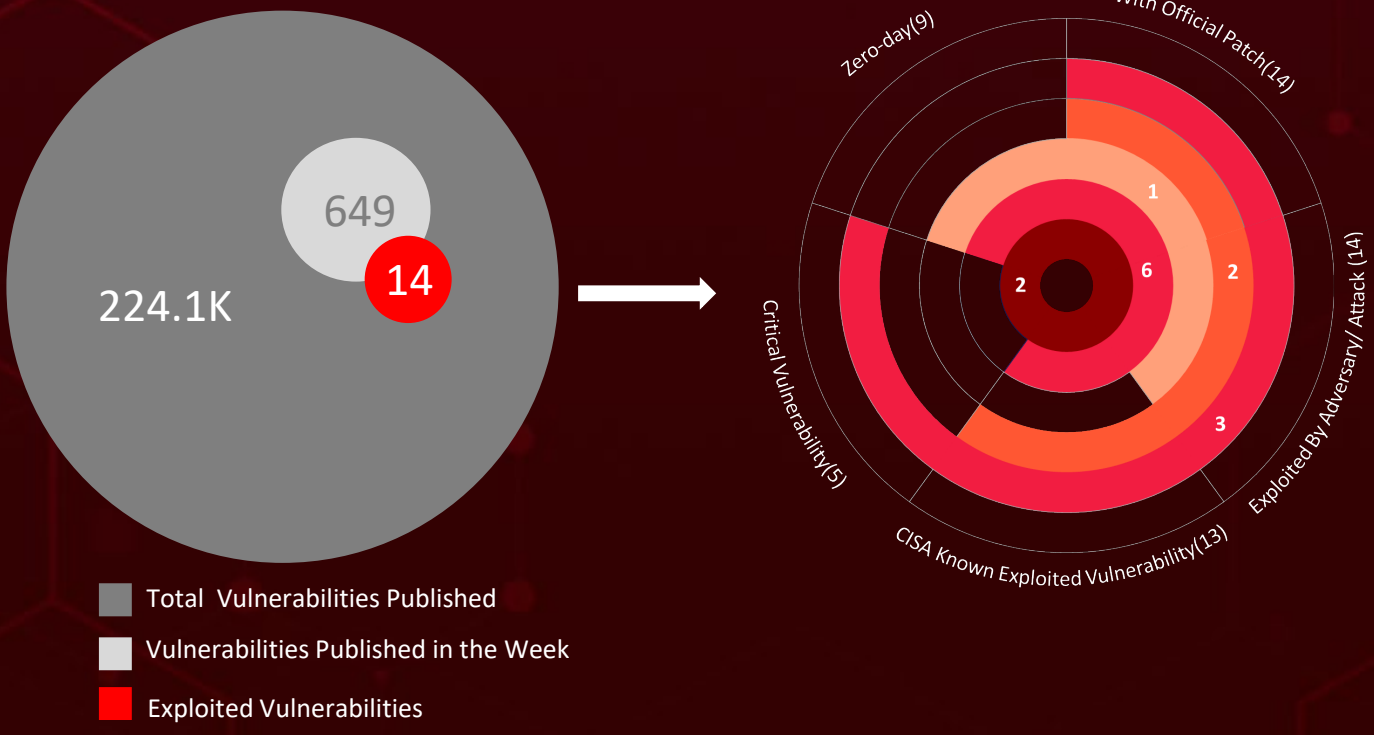
Table Of Contents

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **twenty** executed attacks, **two** instance of adversary activity, and **fourteen** vulnerabilities, including two zero-day vulnerabilities, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs discovered a CVE-2023-44487 vulnerability in HTTP/2, allowing remote attackers to launch a DoS attack using a Rapid Reset Attack.

Meanwhile, the **Stayin' Alive** campaign, affiliated with the **ToddyCat group**, employs sophisticated tactics, including spear phishing and DLL sideloading, to target specific countries in Asia, particularly entities in the Telecom industry and government. These observed attacks have been on the rise, posing a significant threat to users worldwide.



High Level Statistics

20
Attacks Executed

14
Vulnerabilities Exploited

2
Adversaries in Action

- LostTrust ransomware
- Sfile
- Mindware
- MetaEncryptor
- HyperBro
- Cobalt Strike
- ChargeWeapon Backdoor
- Mirai Botnet
- hailBot
- kiraiBot
- catDDoS
- Lu0Bot
- CurKeep
- CurLu
- CurLog
- Balada Injector
- AvosLocker ransomware
- ShellBot
- DarkGate
- SeroXen RAT

- CVE-2017-17215
- CVE-2017-11882
- CVE-2019-0803
- CVE-2023-44487
- CVE-2023-36563
- CVE-2023-41763
- CVE-2021-31207
- CVE-2021-34473
- CVE-2021-34523
- CVE-2021-26855
- CVE-2021-40539
- CVE-2021-44228
- CVE-2022-26134
- CVE-2018-19320

- Grayling APT
- ToddyCat

Insights

ShellBot

New version of shellbot using hexadecimal IP addressed to evade detection

MS Patch Tuesday

Microsoft October 2023 Patch Tuesday addressed total 103 flaws, with three zero-day vulnerabilities actively exploited and two non Microsoft vulnerabilities

LostTrust

Emerged in September 2023 and is a multi-extortion threat related to SFile and Mindware

Avoslocker ransomware

A RaaS variant that targets critical infrastructure organizations, primarily in the US, CISA released stop ransomware alert for the same

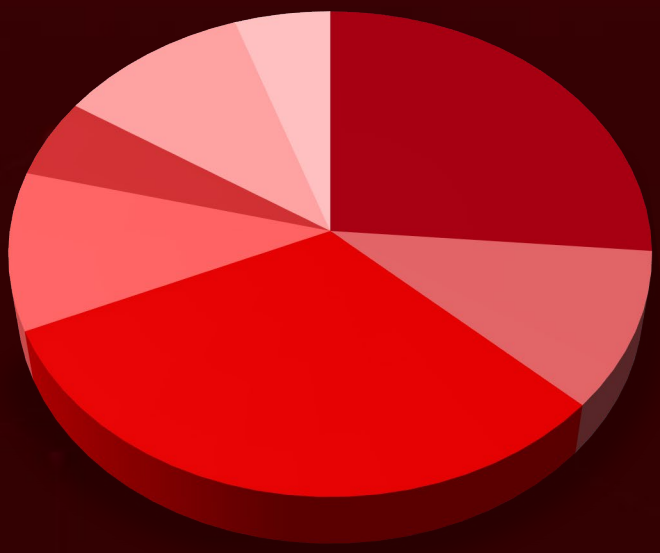
Balada Injector

Since September 2023, more than 17,000 WordPress websites compromised by Balada Injector

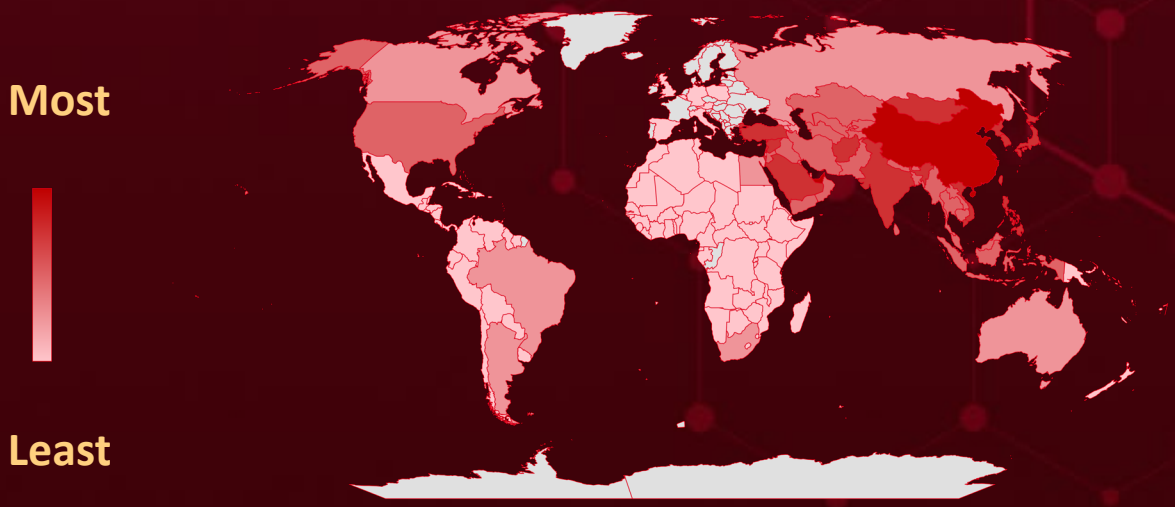
Mirai Botnet

New variant of Mirai botnet includes hailBot, kiraiBot, catDDoS are most active and are widely deployed

Threat Distribution



Targeted Countries



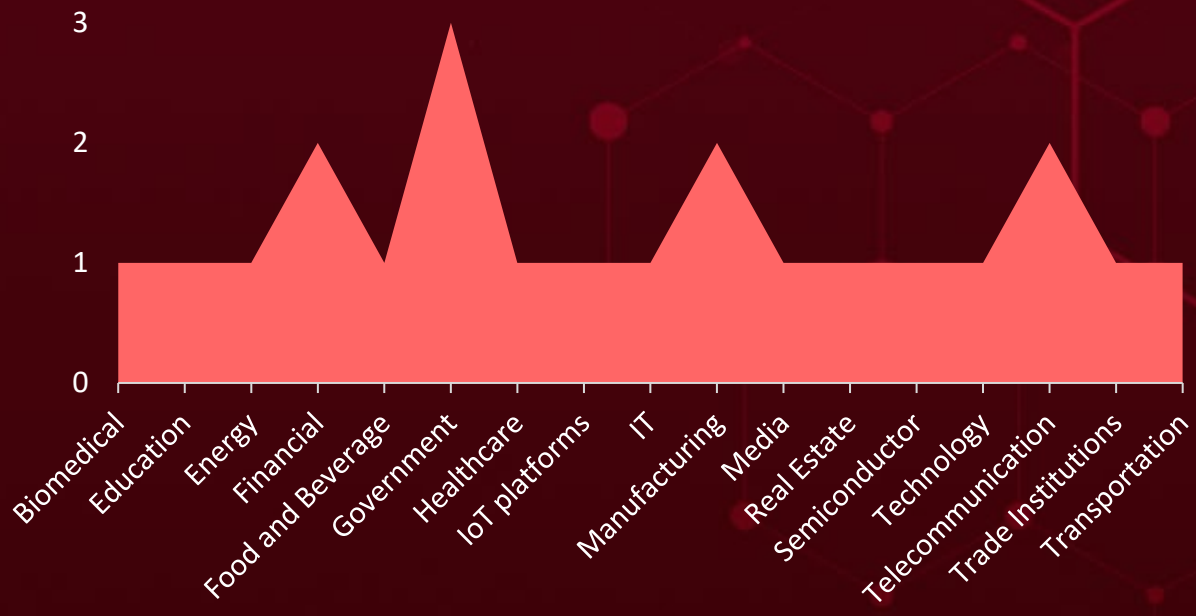
	Countries
	United Arab Emirates
	China
	Saudi Arabia
	South Korea
	Taiwan
	India
	Philippines
	Israel
	Singapore
	Japan
	Syria
	Lebanon
	Turkey
	Mongolia
	Vietnam
	North Korea
	Afghanistan
	Nepal
	Thailand
	Bahrain
	Brunei
3	Uzbekistan

	Countries
	Cambodia
	Pakistan
	Cyprus
	Bangladesh
	Indonesia
	Turkmenistan
	Iran
	Myanmar
	Iraq
	Oman
	Jordan
	Qatar
	Kazakhstan
	Sri Lanka
	Kuwait
	Tajikistan
	Kyrgyzstan
	Timor-Leste
	Laos
	United States
	Malaysia
	Yemen
	Maldives
	Bhutan
	South Africa
	Australia

	Countries
	Brazil
	Georgia
	Azerbaijan
	Canada
	State of Palestine
	Argentina
	Egypt
	Armenia
	Rwanda
	Venezuela
	South Sudan
	Ghana
	Palestine
	Grenada
	Senegal
	Guatemala
	Emirates
	Guinea
	Ethiopia
	Guinea-Bissau
	Peru
	Guyana
	Samoa

	Countries
	Haiti
	Solomon Islands
	Honduras
	Sudan
	Hong Kong
	Togo
	Angola
	Niger
	Bolivia
	Comoros
	Burkina Faso
	Papua New Guinea
	Burundi
	Poland
	Antigua and Barbuda
	Saint Lucia
	Italy
	Saudi
	Jamaica
	Sierra Leone
	Arabia
	Gabon
	Cabo Verde
	Côte d'Ivoire

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter

T1105 Ingress Tool Transfer

T1543 Create or Modify System Process

T1588.006 Vulnerabilities

T1566 Phishing

T1203 Exploitation for Client Execution

T1055 Process Injection

T1573 Encrypted Channel

T1083 File and Directory Discovery

T1588 Obtain Capabilities

T1190 Exploit Public-Facing Application

T1071 Application Layer Protocol

T1070.004 File Deletion

T1486 Data Encrypted for Impact

T1057 Process Discovery

T1027 Obfuscated Files or Information

T1059.001 PowerShell

T1204 User Execution

T1574.002 DLL Side-Loading

T1562 Impair Defenses

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LostTrust	LostTrust ransomware, emerged in September 2023, is a multi-extortion threat related to SFile and Mindware, employing techniques reminiscent of MetaEncryptor, encrypting files and demanding ransoms. It presents a serious cybersecurity concern due to its similarities to other ransomware families.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Compromised systems, and Financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	25a906877af7aed44c21b4c947a34666c3480629a929a227b67b273245ee3708
SHA1	09170b8fd03258b0deaa7b881c46180818b88381

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SFile	SFile aka SFile2, Escal malware is a ransomware that encrypts files on a victim's computer and demands a ransom payment in exchange for the decryption key. First appearing in 2021. SFile is known to be particularly difficult to detect and remove, as it uses a variety of evasion techniques.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Financial loss and Compromised systems	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	e82606b7c179cd39d0e68d9f61723c4b2c909c44e2630c69d7038cd0f1bcb595, 451c4ff0a4313c98b519179eb276914d18d01eb1d6b1a28d6af15fda1693ec34, 8396728b5267a9ff823db2ab600e3ef1d131fc36596d24747ac494e8cdfe877c, 26b7c7079cfea22cd9335b788db32453a727c81aec313a3637391a9763434f0a, 92c24d0c2075133e91f1be803c00478c733ee5be5610564efc48dd160cf2c632

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
Mindware	Mindware malware is a ransomware that targets the human mind. It is designed to exploit human psychology and manipulate people into making mistakes or taking actions that they would not otherwise take.	Social engineering	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data Theft, Financial loss and Compromised systems	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	d1a0a2dc26603b2e764ee9ab90f3f55a2f11a43e402dd72f4a32a19b0ac414b5, 32c818f61944d9f44605c17ca8ba3ff4bd3b2799ed31222975b3c812f9d1126c, c306254b44d825e008babbafbe7b07e20de638045f1089f2405bf24e7ce9c0dc, 00309d22ab53011bd74f4b20e144aa00bf8bb243799a2b48f9f515971c3c5a92, 81828762ebe7ea99b672c8ac07dc3c311487a5a246db494c7643915f6c673562		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MetaEncryptor	MetaEncryptor is a ransomware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key. It was first discovered in early 2023 and has since been used in a number of high-profile attacks.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Data theft, Financial loss and Compromised systems	Windows
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	40ec6eb75af3bf1c8406a121cbdeb4145c70f71e0523c1ffcc12265805d5441b		
SHA1	e04760f670fab000c5ff01da39d4f4994011e581		
MD5	e471f1f13de4cd91e3d4139c98c045d4		

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
HyperBro	HyperBro is a sophisticated RAT that can be used to take control of a victim's computer, steal data, and perform other malicious activities. . It was first discovered in 2017 and has since been utilized by the APT27 threat group	Social engineering	APT27
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Stealing sensitive information	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df, 7229bb62acc6feca55d05b82d2221be1ab0656431953012ebad7226adc63643b, df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348, 45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5d1e94204a8a6a00ab5, df6dd612643a778dca8879538753b693df04b9cf02169d04183136a848977ce9		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cobalt Strike	Cobalt Strike (aka Agentemis, BEACON, CobaltStrike, cobeacon) is a commercial penetration testing tool that is also used by threat actors to launch attacks against organizations. It is a powerful tool that can be used to perform a variety of malicious activities	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
-		Gaining unauthorized access, Data Theft and Financial loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	0e9f26b9a92ba13916a6e98de924397ec3adc68507a1447a0472d1b4e4d8b2df, 923bb69535e27f3493f6253abd93a1c0a9bd08bcf18dbc27d4d8d381a9220bed, 46725598f6c781f6fd178d6f1bce8c93bb21a6a27d6daebc9ff57878a1a301ad, 092188d15ff480ad9ca89f2c65984d8e3d1e7c1e7a8aa91fbd5ceb02461071b8, dc1a58694467305a98f62b7d4b6b6945398e43f0f982a0e13c2a8982ef8bb84a		

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
ChargeWeapon	ChargeWeapon is a malicious software designed to establish remote access and transmit device and network data from a compromised host to a command-and-control (C2) server under the control of an attacker	Social engineering	
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
MD5	44ee43adc8f423db4a461fc99731cdb9
SHA1	0fd8c9ed43d66022a08cc8ed7e78c4a6216cf26c
SHA256	3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135
IPv4	45[.]77[.]37[.]145:8443

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Mirai	Mirai is a malware that infects IoT devices and turns them into bots that can be used to launch distributed denial-of-service (DDoS) attacks. Since its first appearance in 2016, Mirai has evolved into multiple variants, each with its own unique features.	-	CVE-2017-17215 CVE-2017-11882
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		Launch DDoS attacks	Linux
ASSOCIATED ACTOR			PATCH LINK
-			http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

IOC TYPE	VALUE
SHA256	c6e55d1c5e4fbf79337819efa366433840bc743e8830454b06cac72723bf1687, 3dd1607d6c78a16784049978459e4a07cd1188c5419af699724b2b99c0187822, 40dcf03076a4e4114d628dcb7931d7d766b0ef0a17210e97bc6cae70089db080, 2a63ebb23958cac89eb7404fb328774031f875ac563affdf5c67abe4d2d78a4d, 516967063c380a26e75ff2b0f529913366b492efa236a8f641686bfb17443cb0

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
HailBot	HAILBOT is a new variant of the Mirai botnet that was discovered in 2023. It is known to exploit vulnerabilities in Huawei HG532 routers and to target financial and trade institutions, as well as IoT platforms.	Exploiting vulnerabilities	CVE-2017-17215 CVE-2017-11882
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks	IoT platforms
ASSOCIATED ACTOR			**PATCH LINK**
-			http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882
IOC TYPE	**VALUE**		
IPv4	34.147.16[.]24, 34.165.70[.]211, 34.176.112[.]249, 34.64.52[.]239, 34.69.75[.]60		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
KiraiBot	kiraiBot is a new variant of the Mirai botnet that was discovered in 2023. It is known to exploit vulnerabilities in a variety of devices, including routers, cameras, and NAS devices. kiraiBot is also known to target financial and trade institutions, as well as IoT platforms	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks And Data Theft	IoT platforms
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	33ea03c6fdb4bcd826f99ca7ae8b5907		
SHA1	5e0f04554264dfc3eb0ed6a22a53ff8ae26a4162		
SHA256	d619cefad993a0df9ad0ddb631159c50995f76dfd0f14b3fb334b04fce8095cd		
IPv4	179.43.155[.]231		

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
catDDoS	CatDDoS is a new variant of the Mirai botnet that was discovered in 2023 and is exploits vulnerabilities in IoT devices to turn them into bots that can be used to launch distributed denial-of-service (DDoS) attacks.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks And Data Theft	IoT platforms
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
IPv4	139.177.197[.]168, 212.118.43[.]167, 77.105.138[.]202, 84.54.47[.]93, 88.218.62[.]22		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lu0Bot	Lu0Bot Malware, a Node.js-based threat, surfaced in February 2021 as a secondary payload in GCleaner attacks. This malware acts as a bot, responding to C2 server commands and transmitting encrypted system data while employing intricate obfuscation techniques for stealth.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Launch DDoS attacks And Data Theft	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	169b23f45787a0213143bdbb4125658b4bee18e74cb9899c09c29233807bcd21, 4a6ff95b69e3af76e8b36ec5de23b7dd5f8edb72f86a98a710da1dc08f41d799, 4a6ff95b69e3af76e8b36ec5de23b7dd5f8edb72f86a98a710da1dc08f41d799, e6bf861332a771e037a76546d095dd752db63ba0e9fec254a69e0864ae248921, 31fa43d98ac742905cf04735033e154fd103bc67c255cec63a7448ad138df0cf,		

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
CurKeep	CurKeep malware that is used in the Stayin' Alive targeted attack campaign. It is a small, lightweight malware that is difficult to detect. Once CurKeep is installed on a system, it establishes persistence by creating a scheduled task and copying itself to the %APPDATA% folder. CurKeep then collects information about the infected system	Phishing Emails	CVE-2022-23748
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.audinate.com/learning/faqs/audinate-response-to-dante-discovery-mdnsresponder-exe-security-issue-cve-2022-23748
IOC TYPE	**VALUE**		
SHA256	295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719, 462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a, 437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a, 482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651, 877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CurLu	CurLu malware is a malicious downloader that is used in the Stayin' Alive targeted attack campaign. It is a small, lightweight malware that is difficult to detect.	Phishing emails	CVE-2022-23748
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.audinate.com/learning/faqs/audinate-response-to-dante-discovery-mdnsresponder-exe-security-issue-cve-2022-23748
IOC TYPE	**VALUE**		
SHA256	6eaa33812365865512044020bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746, 78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd, 4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6, da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9, 93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347		

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
CurLog	CurLog malware is a sophisticated and relatively new threat that is used in the Stayin' Alive targeted attack campaign. It is a lightweight and cross-platform downloader malware that is written in the Golang programming language.	Social engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Stealing sensitive information	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c, c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac, c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0, 2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed, 778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Balada Injector	Balada Injector is a malware that is used to inject malicious code into websites, typically WordPress websites. It is a sophisticated malware that is difficult to detect and remove. Balada Injector is used to deliver a variety of malware, including backdoors, Trojans, and ransomware.	Phishing emails and exploit vulnerabilities	CVE-2023-3169
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Injector		Information Theft	WordPress
ASSOCIATED ACTOR			**PATCH LINK**
-			https://wpscan.com/vulnerability/e6d8216d-ace4-48ba-afca-74da0dc5abb5/
IOC TYPE	**VALUE**		
IPv4	2.59.222.113, 2.59.222.119, 2.59.222.121, 2.59.222.122, 2.59.222.158,		

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>AvosLocker</td><td rowspan="6">AvosLocker, also known as Avos, was first detected on July 4, 2021, and operates as a ransomware-as-a-service (RaaS), using a double extortion technique. It has compromised organizations in various critical infrastructure sectors primarily in the United States.</td><td>Compromised RDP/VPN credentials or by exploiting vulnerabilities</td><td>CVE-2021-31206, CVE-2021-31207, CVE-2021-34473, CVE-2021-34523, CVE-2021-26855, CVE-2021-40539, CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2022-26134, CVE-2018-19320,</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Gaining unauthorized access, Data Theft and Financial loss</td><td>Windows, Linux, and VMware ESXi</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31206; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523; https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855; https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html; https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-cve-2021-44228-apache-log4j2/; https://logging.apache.org/log4j/2.x/security.html; https://issues.apache.org/jira/browse/LOG4J2-3293; https://jira.atlassian.com/browse/CONFSERVER-79016</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">6cc510a772d7718c95216eb56a84a96201241b264755f28875e685f06e95e1a2,
1198fb9117776809b11a19000161377384957bee846f7b25a610fc8ca082eb37,
794f3d25c42d383fad485f9af1d6d7c0508bcfe8ed80a1afea0e0b51bf92bc81,
bff12a83b1fc2e0ad0000ad9b68abc8eada559bb1094caaf5b9f52887df23705,
91ecad5a2010a6d8b6b738a88a1e3db30bd0e4fbc647cd49ecadebdf0a357643</td></tr>
</table>

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
ShellBot	ShellBot malware, targeting poorly managed Linux SSH servers, now employs hexadecimal IP addresses in its download URLs to evade detection.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		Launch DDoS attacks And Data Theft	Linux SSH servers
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	8e3f3cef620f28881a88e685cda157a1fae53525b4e11d83915cfdd413b53c1a, 9fc015b3841487451403a04976c4c3f975f7f686ce920ab4d9ed816bd91b2d97, c41d378249b76330232e5b4d7a59bcd55fe2d7b6e5ba2be7729907bee1fe6140		
SHA1	5daf348ae3ca2c13ff7983c5771e9436ca540695, 620a4ef784f6bbc8c9fd08c7590b691de546049f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkGate	DarkGate is a commodity malware that is used in a variety of cyber attacks, including targeted attacks and mass attacks. DarkGate is a versatile malware that can be used to steal data, install additional malware, launch denial-of-service attacks, and take control of infected systems.	Phishing emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Launch DDoS attacks And Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	4ed69ed4282f5641b5425a9fca4374a17aecb160, 549cb39cea44cf8ca7d781cd4588e9258bdff2a1, e108fe723265d885a51e9b6125d151b32e23a949, a85664a8b304904e7cd1c407d012d3575eeb2354, 924b60bd15df000296fc2b9f179df9635ae5bfed		

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
SeroXen RAT	SeroXen is a recently surfaced Remote Access Trojan (RAT) that is deceptively promoted as a legitimate tool. It is conveniently accessible and deployable through a dedicated website, making it appealing even to users with limited technical expertise.	Social engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Launch DDoS attacks, Install other malware And Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	4c6e90e178396d000b5dd5c5bb2b9ae5bbbca5986f26ffad2a6bd0845b6b2c83, 050efb70d521f74a42dcd63c703900433b03cf138fcfa1812705c8cb37deb1ea, a840fb6ea2354c5bdd1b531aa548620ed7c962a4241e4a384b03939eca8345b8, 5bcebf01c55b24ba2097f86c5074898ff8f04aca40064903d3afc2ca0593dde2, 0f0e9dfbe8a36d5a2447c1a0ae3af05779088329e7a796d17aba97fd233c3592		

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-2017-17215	✗	Huawei HG532: All versions	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:huawei:hg532_firmware:-:*:*:*:*:*:*:* cpe:2.3:h:huawei:hg532:-:*:*:*:*:*:*:*	HailBot
Huawei HG532 Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-11882	✗	Microsoft Office: 2007 - 2016	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:office:*:*:*:*:*:*:*:*	HailBot
Microsoft Office Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11882

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-44487		Microsoft IIS: 10.0, Apache Tomcat: 8.5.0 - 11.0.0-M11, Netty: 4.0.0 - 4.1.99, Jetty: 9.0.0.v20130308 - 12.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:IIS:10.0:*:*:*:*:*:*:*cpe:2.3:a:apache_foundation:apache_tomcat:11.0.0-M11:*:*:*:*:*:*:*cpe:2.3:a:netty:netty:4.1.99:*:*:*:*:*:*:*cpe:2.3:a:eclipse:jetty:9.4.53.v20230927:*:*:*:*:*:*:*	-
HTTP/2 Rapid Reset Attack Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-400	T1498: Network Denial of Service; T1584.005: Compromise Infrastructure:Botnet	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-44487; https://netty.io/downloads.html; https://mvnrepository.com/artifact/org.eclipse.jetty/jetty-servlets/9.4.53.v20231009

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-41763		Skype for Business Server: before 7.0.246.530	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:skype_for_business_server:*:*:*:*:*:*:*:*	-
Microsoft Skype for Business Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-41763

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36563		Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*:*	-
Microsoft WordPad Information Disclosure Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1082: System Information Discovery	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2023-36563

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-0803	 ZERO-DAY	Windows: 7 - 10 1809 Windows Server: 2008 - 2019 1803	Grayling APT
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:*	-
Microsoft Win32k Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1068: Exploitation for Privilege Escalation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0803

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-26134	 ZERO-DAY	Confluence Server and Confluence Data Center	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	AvosLocker ransomware
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.atlassian.com/software/confluence/download-archives

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26855	ProxyLogon	Microsoft Exchange Server: 2013 Cumulative Update 1 15.00.0712.024 - 2019 RTM 15.02.0221.012	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_21:*:*:*:*:*:*:*	AvosLocker ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26855

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473	PROXYSHELL	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	AvosLocker ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523	PROXYSHELL	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	AvosLocker ransomware
Microsoft Exchange Server Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1068: Exploitation for Privilege Escalation	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

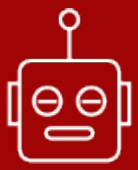
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31207	PROXYSHELL	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2019 Cumulative Update 9 15.02.0858.005	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:2013:cumulative_update_23:*:*:*:*:*:*:*	AvosLocker ransomware
Microsoft Exchange Server Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-787	T1556: Modify Authentication Process	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40539	✗	Zoho ManageEngine ADSelfService Plus: 6000 - 6113	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:*:*:*:*:*:*:*	AvosLocker ransomware
Zoho ADSelfService Plus Remote code execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-706	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228	Log4j	Apache Log4j2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:2.0:-:*:*:*:*:*:*:*	AvosLocker ransomware
Apache Log4j2 Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917 CWE-502 CWE-400 CWE-20	T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://logging.apache.org/log4j/2.x/security.html

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2018-19320</td><td>  </td><td rowspan="2">GIGABYTE APP Center: 1.05.21
AORUS GRAPHICS ENGINE: 1.0 - 1.33
XTREME GAMING ENGINE: 1.22 - 1.25
OC GURU: 2.08</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:gigabyte:aorus_graphics_engine:*:*:*:*:*:*:*:*</td><td rowspan="2">AvosLocker ransomware</td></tr>
<tr><td rowspan="3">GIGABYTE Multiple Products Unspecified Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH DETAILS</td></tr>
<tr><td>CWE-782</td><td>T1068: Exploitation for Privilege Escalation</td><td>https://www.gigabyte.com/Support/Security/1801</td></tr>
</table>

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Grayling APT	Unknown	Government, Manufacturing, IT, and Biomedical	Taiwan, Vietnam, U.S, and Asia-Pacific region
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2019-0803	-	-
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, T1070: Indicator Removal, T1083: File and Directory Discovery, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1543: Create or Modify System Process, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1562: Impair Defenses			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 ToddyCat	China	Telecommunication, Government	Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-23748	CurKeep, CurLu, CurLog	Windows
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0007: Discovery, T1083: File and Directory Discovery, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1543: Create or Modify System Process, T1574: Hijack Execution Flow, T1574.002: DLL Side-Loading, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1562: Impair Defenses, T1071: Application Layer Protocol, T1566.001: Spearphishing Attachment, T1566: Phishing, T1588.006: Vulnerabilities			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **fourteen exploited vulnerabilities** and block the indicators related to the threat actor **Grayling APT, ToddyCat** and **LostTrust ransomware, SFile, Mindware, MetaEncryptor, HyperBro loader, Cobalt Strike , ChargeWeapon Backdoor, Mirai Botnet, hailBot, kiraiBot, catDDoS, Lu0Bot, CurKeep, CurLu, CurLog, Balada Injector, AvosLocker ransomware, ShellBot, DarkGate, SeroXen RAT** malware.

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 **fourteen exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Grayling APT, ToddyCat** and **LostTrust ransomware, SFile, Mindware, MetaEncryptor, HyperBro loader, Cobalt Strike , ChargeWeapon Backdoor, Mirai Botnet, hailBot, kiraiBot, catDDoS, Lu0Bot, CurKeep, CurLu, CurLog, Balada Injector, AvosLocker ransomware, ShellBot, DarkGate, SeroXen RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

LostTrust Ransomware Unmasking the Gang Behind the Threat

China's Cyber Espionage Targets Semiconductor Giants in East Asia

Deciphering Mirai's Next Chapter: the Strategies of the Latest Players

Unveiling Lu0Bot Malware A Node.js-Based Threat

GNOME Linux Systems Exposed to 1-Click RCE Attacks

Grayling APT Emerges as a Silent Threat Targeting Taiwan

HTTP/2 Zero-Day Exploited for the Most Explosive DDoS Attacks

Microsoft’s October 2023 Patch Tuesday Addresses Three Zero-day Vulnerabilities

Unraveling the Intricate Arsenal of Stayin' Alive Campaign

Balada Injector: A Large-Scale Malware Campaign Targeting WordPress

In-Depth Analysis of AvosLocker Ransomware

ShellBot Malware Evades Detection Using Hexadecimal IP Addresses

Revealing DarkGate’s Incursion Across Continents

SeroXen RAT Leverages NuGet Packages

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
LostTrust Ransomware	MD5	4ae8efc6c80fe086aa27117619718fc2
	SHA1	09170b8fd03258b0deaa7b881c46180818b88381
	SHA256	25a906877af7aed44c21b4c947a34666c3480629a929a227b67b273245ee3708
Mindware	MD5	0d5bbc80bdc3bd5c148995dbd7f97f4a, 78d6ca966b7a7129c729e985a539ebb6, 760ea87bd570c2ea938dd55ae684ff37, 86fb4bc1f17511f7b5d14bde84272a58, 7883e7d9c4165e09afb25ab0c731fcb2
	SHA1	46ca0c5ad4911d125a245adb059dc0103f93019d, 9bc1972a75bb88501d92901efc9970824e6ee3f5, Ae974e5c37936ac8f25cfea0225850be61666874, E9b52a4934b4a7194bcbbe27ddc5b723113f11fe, F91d3c1c2b85727bd4d1b249cd93a30897c44caa
	SHA256	d1a0a2dc26603b2e764ee9ab90f3f55a2f11a43e402dd72f4a32a19b0ac414b5, 32c818f61944d9f44605c17ca8ba3ff4bd3b2799ed31222975b3c812f9d1126c, c306254b44d825e008babbafbe7b07e20de638045f1089f2405bf24e7ce9c0dc, 00309d22ab53011bd74f4b20e144aa00bf8bb243799a2b48f9f515971c3c5a92, 81828762ebe7ea99b672c8ac07dc3c311487a5a246db494c7643915f6c673562

Attack Name	TYPE	VALUE
Sfile	MD5	ae8c22cc7542b4a3dc92cca88897048f, fdc8e99745554b1138a431c15168364d, 575934448f3a30696336644d6c379db9, 0493958b9915e5799927716aa5b82191, 1875e9d8031876674d4d236ffab6b826, 4f44f3a05d014ee1a4e85f67436abcb9, 38ca7e711977058ae3ae702b2ea676b0, c83874d9e1f6531a05c61d40ebe9b82a, a1e880b1bf079e1c9ac9a9238c68e674
	SHA1	0f20e5ccdbbed4cc3668577286ca66039c410f95, 14e4557ea8d69d289c2432066d860b60a6698548, 28f73b38ace67b48e525d165e7a16f3b51cec0c0, 5ffac9dff916d69cd66e91ec6228d8d92c5e6b37, 665572b84702c4c77f59868c5fe4d0b621f2e62a, 6960beedbf4c927b75747ba08fe4e2fa418d4d9b, 8c507d26c2fec90707320ffb721ae626139bbf11, a67686b5ce1d970a7920b47097d20dee927f0a4d, bdb0c0282b303843e971fbcd6d2888d834da204c
	SHA256	e82606b7c179cd39d0e68d9f61723c4b2c909c44e2630c69d7038cd0f1bcb595, 451c4ff0a4313c98b519179eb276914d18d01eb1d6b1a28d6af15fda1693ec34, 8396728b5267a9ff823db2ab600e3ef1d131fc36596d24747ac494e8cdfe877c, 26b7c7079cfea22cd9335b788db32453a727c81aec313a3637391a9763434f0a, 92c24d0c2075133e91f1be803c00478c733ee5be5610564efc48dd160cf2c632, 97d679f364b1d0c6e3896574f1338801a0d707c137e4d220d2c974ae40fbe708, 7195995c6ea6afc08bdfa51f7227ee3398aec95f242e992c900f14eb644dd838, feddee093d72838ac1f13ea9bbfc0473e2f3df1495432d6f95d6fe8ddf7ff09b, 4576fd0e13e13c9d490bd84ff83d2f3b602272cdea5f6c54c74f75d067ac5505
MetaEncryptor	MD5	e471f1f13de4cd91e3d4139c98c045d4
	SHA1	e04760f670fab000c5ff01da39d4f4994011e581
	SHA256	40ec6eb75af3bf1c8406a121cbdeb4145c70f71e0523c1ffcc12265805d5441b

Attack Name	TYPE	VALUE
HyperBro	MD5	af43e0c21ddf7e4e087cdab2ac8d2948, 7d75561cb378e54c5711f077858a4a48, 4109ac08bdc8591c7b46348eb1bca85d, b35c698732f49f998f6e6b6b83cfa9dd, b5cb7044a189f8752ecdbc799f25ce06
	SHA1	b8d9bba99d9777c43b96f338f5bc3a08201fa05c, 692b407893846cdd5d3e75110402fe1e7bf5515e, 6423d1c324522bfd2b65108b554847ac4ab02479, 13e334a4857b8bee0283e5e193fa7983d5c0ee06, 9e08fdd7eaeffbbf6e441060e02dc29b0f66b118
	SHA256	12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df, 7229bb62acc6feca55d05b82d2221be1ab0656431953012ebad7226adc63643b, df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348, 45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5d1e94204a8a6a00ab5, df6dd612643a778dca8879538753b693df04b9cf02169d04183136a848977ce9
	URL	http://38[.]54[.]119[.]239:443/jquery-3.3.1.min.js ,
ChargeWeapon	MD5	44ee43adc8f423db4a461fc99731cdb9
	SHA1	0fd8c9ed43d66022a08cc8ed7e78c4a6216cf26c
	SHA256	3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135
	IPv4	45[.]77[.]37[.]145:8443
Cobalt Strike	SHA256	0e9f26b9a92ba13916a6e98de924397ec3adc68507a1447a0472d1b4e4d8b2df, 923bb69535e27f3493f6253abd93a1c0a9bd08bcf18dbc27d4d8d381a9220bed, 46725598f6c781f6fd178d6f1bce8c93bb21a6a27d6daebc9ff57878a1a301ad, 092188d15ff480ad9ca89f2c65984d8e3d1e7c1e7a8aa91fbd5ceb02461071b8, dc1a58694467305a98f62b7d4b6b6945398e43f0f982a0e13c2a8982ef8bb84a, 69458febe1c88d03d6b5f0a83b516481f9dcbedfb97c8720170e4d0c75c1c880, 7fa4e361cf073d65ccbc49dc937a622965977ef995a0c199a4b4aa5fddd57d17
Mirai	SHA256	c6e55d1c5e4fbf79337819efa366433840bc743e8830454b06cac72723bf1687, 3dd1607d6c78a16784049978459e4a07cd1188c5419af699724b2b99c0187822, 40dcf03076a4e4114d628dcb7931d7d766b0ef0a17210e97bc6cae70089db080,

Attack Name	TYPE	VALUE
Mirai	SHA256	2a63ebb23958cac89eb7404fb328774031f875ac563affdf5c67abe4d2d78a4d, 516967063c380a26e75ff2b0f529913366b492efa236a8f641686bfb17443cb0
hailBot	IPv4	34.147.16[.]24, 34.165.70[.]211, 34.176.112[.]249, 34.64.52[.]239, 34.69.75[.]60, 34.92.28[.]223, 35.188.240[.]127, 5.181.80[.]115, 5.181.80[.]120, 5.181.80[.]70, 5.181.80[.]71
	MD5	f30a468b56c5761e346f3e709fd098e
kiraiBot	MD5	33ea03c6fdb4bcd826f99ca7ae8b5907
	SHA1	5e0f04554264dfc3eb0ed6a22a53ff8ae26a4162
	SHA256	d619cefad993a0df9ad0ddb631159c50995f76dfd0f14b3fb334b04fce8095cd
	IPv4	179.43.155[.]231
catDDoS	MD5	12fe77575c11b698501e2068810823a4
	SHA1	3a3f37333e298c3c6f2be18da4f5473454820d2d
	SHA256	259b0c0c65f6836cc2ee8aa22da007415404231e178aabfbb4bfc11c7786f441
	IPv4	139.177.197[.]168, 212.118.43[.]167, 77.105.138[.]202, 84.54.47[.]93, 88.218.62[.]22, 88.218.62[.]221
Lu0Bot	MD5	6181206d06ce28c1bcdb887e547193fe
	SHA1	8eb65b4895a90d343f23f9228e0d53af62de3dab
	SHA256	169b23f45787a0213143bdbb4125658b4bee18e74cb9899c09c29233807bcd21, 4a6ff95b69e3af76e8b36ec5de23b7dd5f8edb72f86a98a710da1dc08f41d799,

Attack Name	TYPE	VALUE
Lu0Bot	SHA256	4a6ff95b69e3af76e8b36ec5de23b7dd5f8edb72f86a98a710da1dc08f41d799, e6bf861332a771e037a76546d095dd752db63ba0e9fec254a69e0864ae248921, 31fa43d98ac742905cf04735033e154fd103bc67c255cec63a7448ad138df0cf, ca09a22afb6d9a1853fe4fc4d36089900d24d7178642ec7ca86789cd0dbc5c67, 8ee274b430932f7e8068229a7f32c2bbaead31bf6c18dd13194a1126f5cbfb33, 3a1f00f2d35eb2fbab05c0543eaf32d29b12b856c64809393c873474a4a27083, 95fad71ca5df4eb7e390f6795d4a02d117524e9432d118a5213a484e211e1480, 7b4055eb9d72b5e5cd10c846497cb538bc366f8993198b680d195c98987d74e6, e2c630adb97cc041c5ce1835add03841493ae95223d43c9e415e26e6c4c418e2, fb808be98b583a2004b0af7b6f4bf5e3419d8b6a385c5ce4e8fab4ddc0b48428, f4b15f591e0138a46f1f5fd157f31a78b360624d72a18136a5269a05ba8b987c, 22b643071879895cd947cf37c75c71b23af5fe4228f36b49571b1a47df137d06, 28eb3941dee1a78351ee18596be6445d4fb10332d002f85aee675f672cf2fd1c, ea596ff0c0802b85cc304447799c91907ae1016283152ba5ba5dc4cb50ca8712, 9837727bf67f4a49655b5f2230fa7dad235b025c9af377e559df6fab0f4ff36a, a4a0e26bb4aa352f66952902cc9704d130593adacb46017c0b2a1be2b7a9269d, 863c612734f5ff0ff0ea3fed7fd790dfb43c47eecdc1417bcd82c0ad866419af, 9c5898b1b354b139794f10594e84e94e991971a54d179b2e9f746319ffac56aa, f17694550f57c6605f37588e37f55898bbc969c1f24b18f0be8ce416c95ab91c, 0296a426d47abf467c431db1e126b8763eac7d062e731193eccd15a51c52da7c, 149ca091b02aafdeff15610c639b442a61e0dfcd461d9bec7f8c38998a390575, 6f7ab51e9f0d382c650743cb3c06b42708cd06d64170a458864e89ad6480a237, fd746c51486e5ccb2bd801f4cffbeefaf77e7844ef1dd5d211a4c183ec26f52d, cb96ceb0b26fc150baaa7fe1cc2a65af42c7db902f54839578b3235a7d12d25c, bfc050b80ad15c6bf86ea0dce49089c56ed9ffccf5dae2b8e3b78b59dd36e0bb,

Attack Name	TYPE	VALUE
Lu0Bot	SHA256	956610a72b5e5aaf220b861aec44e08dda7b6a97ccae3d2fea0181e3a6b37228, 09a2d8ab4c255b6f78ca7534e3105014a21613cd3c6b07cbb92eb2c82b553483, 24c0997ec70f23963598b59df453f28ffcc1e8b356898d5ddc4b2cbf06f6f2ac, 0718b209bd95315b8347d3f006b7da387f9807153ebe8b2788285296e19b5973, 0739718c03bd39daad459142116b886d6138cfe887d30b02942e01b9d238dd13, b13633b31e8704b63d977921d1c9a4284bfd4780c3f35a5bee372816d7beb005, 242467ea19694c0e6cd76dcff901f5af6a309c2c999971b1dc4cd9bad253ea19, f5f8716486cab2d9b866a1e19e4f25d64d070262ce32d2ff79db283ac7fd1b05, 0bdaa27e390c5e15c3b27ae4f4168fbf97693f5d03fa0f70487c63c13030ffd8, 5920894ae997b61f27b53c9f6e598df5f928acb11a5dc09f4fa0627747f1312d, 6d265ec945dfd70f60e5a016ec26276f3d460076e9320a3c11c7a76b638da9ab, 5a2283a997ab6a9680b69f9318315df3c9e634b3c4dd4a46f8bc5df35fc81284, 742eb714457c3646f7f5dee44aaf0d57d5fa076ee294de6755818132402b06f5, 70657b04b2da77f8019be49fa3043898874bebb385317a6c91246f9e3858bf16, 858bafe27080124fc1560894b00cf8c0c672df0bd0a66dbd08cf28b4cf9e1ee5, 7374cce760bf018df8c602b12e475a66114747d96848168cb939f27afafb29e0, d5069d544f3ff1efe1851688b9625cd44fe45c6f1a9792b30f5f28c74af1d6d6, 5de7148d727fec09a0597b5f64cf1719968372a21c6ded90c51cae3f42b4c26d, 0f2c35b80a36f70ab923b56c495ea6fe9ebdd48b3d5a4ff404fec3b99ff010d9, d189c35ecd1b9665741e7e08f9d9029c307e07870cf57832426d8bfce1c48fa6, 8264e723a411381a9d837458ec39cbb36c8d582bcba14f7ed7fc45f8154c479d, 4547dab867404fa6e5cebc5794ae58c4d365355372d26e6bcd01c1aea0f91e1b, 45964a7afb9d41eb319161c26215c5bea0334b388ecfb1520b83bb2d6984ad5e, 02e4898e0a4cc85c406996e5e60274082746eb45d77a18a24eb545074a56ab3c,

Attack Name	TYPE	VALUE
Lu0Bot	SHA256	f186c2ac1ba8c2b9ab9b99c61ad3c831a6676728948ba6a7ab8345121baeaa92, 5a2264e42206d968cbcfff583853a0e0d4250f078a5e59b77b8def16a6902e3f, c88e27f257faa0a092652e42ac433892c445fc25dd445f3c25a4354283f6cdbf, 2d721df670fdb63c643b3de2dcdd46311b8d94d2753b47ad0035392644dee77a, 4c31eccb460bef397e6100e1ecd85c3a2b823b893a9a9add4bb83fde8f9b122b, 0297bbb0f00b3f591894ebcf042f2c6b0ed52e6662def1a9dbca0f8d20133cee, cb23aeac6382ff99608a71e3b416c1ca22f5f301474840239e4c319db31cef25, 9db5c02ac4e161369160fe13719a212e55377dd57ffc9f98b7141bce3b9df26c, 4c99457625e752a03693aab64e2b5129eff89872c649194e81bd87809ed1ae13, 22934e006b3f1b8225c51a93ce0acaa1874c4f1dc895fa1664bdf16b0065d2e7, 7c37b8dd32365d41856692584f4c8e943610cda04c16fe06b47ed2d1e5c6415e, 418a860f2f7f5d415ffa2c7b2662c6fde7c35e2bdafd45e378bdf7c95579fde8, fce3d69b9c65945dcfbb74155f2186626f2ab404e38117f2222762361d7af6e2
CurLu	SHA256	6eaa3381236586551204402 0bc4b95079a1cc2ddc26cdadf24a9ff76c81b1746, 78faceaf9a911d966086071ff085f2d5c2713b58446d48e0db1ad40974bb15cd, 4d52d40bc7599b784a86a000ff436527babc46c5de737e19ded265416b4977c6, da2d9ed632576eca68a0c6d8d5afd383a1d811c369012f0d7fb52cd06da8c9b9, 93e9237afaff14c6b9a24cf7275e9d66bc95af8a0cc93db2a68b47cbbca4c347, 12a7b9fa57719109b7f5d081cbe032320a59a7d57eef2dcd2cd4fe2b909162dc, 4baa4071a5eedbe0a8afa1059f7732e5cde0433dd0425e075721dd2cdec9d70d, a8a026d9bda80cc9bdd778a6ea8c88edcb2d657dc481952913bbdb5f2bfc11c9, 7418c4d96cb0fe41fc95c0a27d2364ac45eb749d7edbe0ab339ea954f86abf9e

Attack Name	TYPE	VALUE
CurKeep	SHA256	295b99219d8529d2cd17b71a7947d370809f4e1a3094a74a31da6e30aa39e719, 462c85f6972da64af08f52a4c2f3a03bcd40fdf29b29b01631bff643cd9d906a, 437cde10797b75ea92b1b68eb887972fe43b434db3ed67b756e01698cce69b4a, 482d41c4a2e14ddc072087a1b96f6e34ffda2bfc85819e21f15c97220825e651, 877579185a72fbaf1afa78d3c50dbab187780d545d5375ba4c29147083176697, a54e0352653146371efd727ca00110577f8e750e92101462e246f99d435b6172, 36b4a846d6ed3461e36ed9f4c03fb4548397659ef0a46219695666266eba1652, caa9fdda2776f681ec294ffeded04723107cf754a2889c3fbb5bc7c743d897c1, d4bd89ff56b75fc617f83eb858b6dbce7b36376889b07fa0c2417322ca361c30, 1428698cc8b31a2c0150065af7b615ef2374ea3438b0a82f2efcff306b43cee6, d33cbdbd6181deb0e8da9c9e6fb8795e98478d9608ab187e5b8809bed6b2e5c4, 2ab1121c603b925548a823fa18193896cd24d186e08957393e6a34d697aed782, 1934ac9067871a61958e3e96ea5daa227900b7683fce67a1bf1c24beff77d75a
CurLog	SHA256	409948cbbeaf051a41385d2e2bc32fc1e59789986852e608124b201d079e5c3c, c5d1ee44ec75fc31e1c11fbf7a70ed7ca8c782099abfde15ecaa1b1edaf180ac, c4f9bc7624509190e9e2a690daeff5ac9e944f094b51781734b83a364ae038d0, 2dfba1cbc0ac1793ffd591c88024fab598a3f6a91756a2ea79f84f1601a0f1ed, 778b2526965dc1c4bcc401d0ae92037122e7e7f2c41f042f95b59a7f0fe6f30e
ShellBot	IPv4	123[.]6[.]5[.]229, 124[.]222[.]211[.]66, 135[.]125[.]240[.]201, 175[.]178[.]157[.]198, 31[.]145[.]142[.]206, 39[.]107[.]61[.]230, 39[.]165[.]53[.]17, 61[.]242[.]178[.]220, 94[.]250[.]254[.]43
	MD5	7bc4c22b0f34ef28b69d83a23a6c88c5, 8853bb0aef4a3dfe69b7393ac19ddf7f, a92559ddace1f9fa159232c1d72096b2

Attack Name	TYPE	VALUE
ShellBot	SHA1	5daf348ae3ca2c13ff7983c5771e9436ca540695, 620a4ef784f6bbc8c9fd08c7590b691de546049f, a10262346ce669b28914570415a223ec09c234c8
	SHA256	8e3f3cef620f28881a88e685cda157a1fae53525b4e11d83915cfdd413b53c1a, 9fc015b3841487451403a04976c4c3f975f7f686ce920ab4d9ed816bd91b2d97, c41d378249b76330232e5b4d7a59bcd55fe2d7b6e5ba2be7729907bee1fe6140
DarkGate	SHA1	4ed69ed4282f5641b5425a9fca4374a17aecb160, 549cb39cea44cf8ca7d781cd4588e9258bdff2a1, e108fe723265d885a51e9b6125d151b32e23a949, a85664a8b304904e7cd1c407d012d3575eeb2354, 924b60bd15df000296fc2b9f179df9635ae5bfed, cec7429d24c306ba5ae8344be831770dfe680da4, d9a2ae9f5cffba0d969ef8edbbf59dc50586df00, 381bf78b64fcdf4e21e6e927edd924ba01fdf03d, 4c24d0fc57633d2befaac9ac5706cbc163df747c, 9253eed158079b5323d6f030e925d35d47756c10, 0e7b5d0797c369dd1185612f92991f41b1a7bfa2, 7d3f4c9a43827bff3303bf73ddbb694f02cc7ecc, e47086abe1346c40f58d58343367fd72165ddecd, 42fe509513cd0c026559d3daf491a99914fcc45b, 93cb5837a145d688982b95fab297ebdb9f3016bc, f7b9569a536514e70b6640d74268121162326065, d40c7afee0dd9877bbe894bc9f357b50e002b7e2, 1f550b3b5f739b74cc5fd1659d63b4a22d53a3fc, 3229a36f803346c513dbb5d6fe911d4cb2f4dab1, 6585e15d53501c7f713010a0621b99e9097064ff, 001e4eacb4dd47fa9f49ff20b5a83d3542ad6ba2, ad1667eaf03d3989e5044faa83f6bb95a023e269, a3516b2bb5c60b23b4b41f64e32d57b5b4c33574, e6347dfdaf3f1e26d55fc0ed3ebf09b8e8d60b3f, 3cbbdfc83c4ef05c0f5c37c99467958051f4a0e1, f3a740ea4e04d970c37d82617f05b0f209f72789, e6e4c7c2c2c8e370a0ec6ddb5d998c150dcb9f10, 45a89d03016695ad87304a0dfd04648e8dfeac8f
	Domains	msteamseyeappstore[.]com, Drkgatevservicceoffice[.]net, reactervnamnat[.]com, coocooncookiedpo[.]com, wmnwserviceadsmark[.]com, onlysportsfitnessam[.]com, marketisportsstumi[.]win
	IPv4:Port	5.188.87[.]58[:]2351
	URl	hxxp://corialopolova.com/vHdLtiAzZYCsHszzP118[.]bin

Attack Name	TYPE	VALUE
SeroXen RAT	SHA256	4c6e90e178396d000b5dd5c5bb2b9ae5bbbca5986f26ffad2a6bd0845b6b2c83, 050efb70d521f74a42dcd63c703900433b03cf138fcfa1812705c8cb37deb1ea, a840fb6ea2354c5bdd1b531aa548620ed7c962a4241e4a384b03939eca8345b8, 5bcebf01c55b24ba2097f86c5074898ff8f04aca40064903d3afc2ca0593dde2, 0f0e9dfbe8a36d5a2447c1a0ae3af05779088329e7a796d17aba97fd233c3592, 9936d687086d0adfd38efa1304ad52f1007fb57027ebcfa2ca243cab7ff77ee8, 969a635bd8d14fffb3ee8767eb411e4178e4a2df8289d030d54126e3a11b409b, e7dc6a2f0c65a2c6f3d7cc2a11c3fd2acb4e23af1e55a8769366766ee22278c3, 8bf56c92865fade8d06d4a57e1d049bccd3041842b2a1c71503a29729a71073d, 075acd923103e731e91140e663756699e7379a7f63ea31487434ce04cca02b02
Balada Injector	IPv4	2.59.222.113, 2.59.222.119, 2.59.222.121, 2.59.222.122, 2.59.222.158, 185.39.206.158, 185.39.206.159, 185.39.206.160, 185.39.206.161, 80.66.79.252, 80.66.79.253, 88.151.192.253, 88.151.192.254, 89.23.103.32, 89.23.103.246
	Domains	decentralappps[.]com, statisticscripts[.]com, dataofpages[.]com, listwithstats[.]com, promsmotion[.]com, stablelightway[.]com, specialtaskevents[.]com, getmygateway[.]com, stratosbody[.]com, specialnewspaper[.]com

Attack Name	TYPE	VALUE
AvosLocker ransomware	SHA256	6cc510a772d7718c95216eb56a84a96201241b264755f28875e685f06e95e1a2, 1198fb9117776809b11a19000161377384957bee846f7b25a610fc8ca082eb37, 794f3d25c42d383fad485f9af1d6d7c0508bcfe8ed80a1afea0e0b51bf92bc81, bff12a83b1fc2e0ad0000ad9b68abc8eada559bb1094caaf5b9f52887df23705, 91ecad5a2010a6d8b6b738a88a1e3db30bd0e4fbc647cd49ecadebdf0a357643, fe23d4b7a9db3c937523afecdbe14969987c27f35b9bb9c90f656bcd897bcb87, df480deb191b335dcbc3d4fc5d59594cb38caee2aaef8d877fbbc573de741301, 01792043e07a0db52664c5878b253531b293754dc6fd6a8426899c1a66ddd61f, e737c901b80ad9ed2cd800fec7c2554178c8afab196fb55a0df36acda1324721, c0a42741eef72991d9d0ee8b6c0531fc19151457a8b59bdcf7b6373d1fe56e02, 29910ea42c8e2abb22d5a88053e1725c93a104e61560a2f8d88716d619bcaa08, 27cd3e759ec4858adaea63050ad1fc22e4850c1e157d88c0943c2589fa39b5a4, 373a791f058539d72983e38ebe68e98132fcf996d04e9a181145f22a96689386, bd88d415032eb24091c352fc0732b31116f44a78d9333037bd7608289608d3cd, e62c0bdf69b88a5bd95872cbcf4da4de4eef226bc9ef0452ee652eeee519b15a, fb544e1f74ce02937c3a3657be8d125d5953996115f65697b7d39e237020706f, 43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856, 10ab76cd6d6b50d26fde5fe54e8d80fceeb744de8dbafddff470939fac6a98c4, 7c935dcd672c4854495f41008120288e8e1c144089f1f06a23bd0a0f52a544b1, 0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6, a0b4e3d7e4cd20d25ad2f92be954b95eea44f8f1944118a3194295c5677db749, e68f9c3314beee640cc32f08a8532aa8dcda613543c54a83680c21d7cd49ca0f, ad5fd10aa2dc82731f3885553763dfd4548651ef3e28c69f77ad035166d63db7, 48dd7d519dbb67b7a2bb2747729fc46e5832c30cafe15f76c1dbe3a249e5e731, 1e21c8e27a97de1796ca47a9613477cf7aec335a783469c5ca3a09d4f07db0ff,

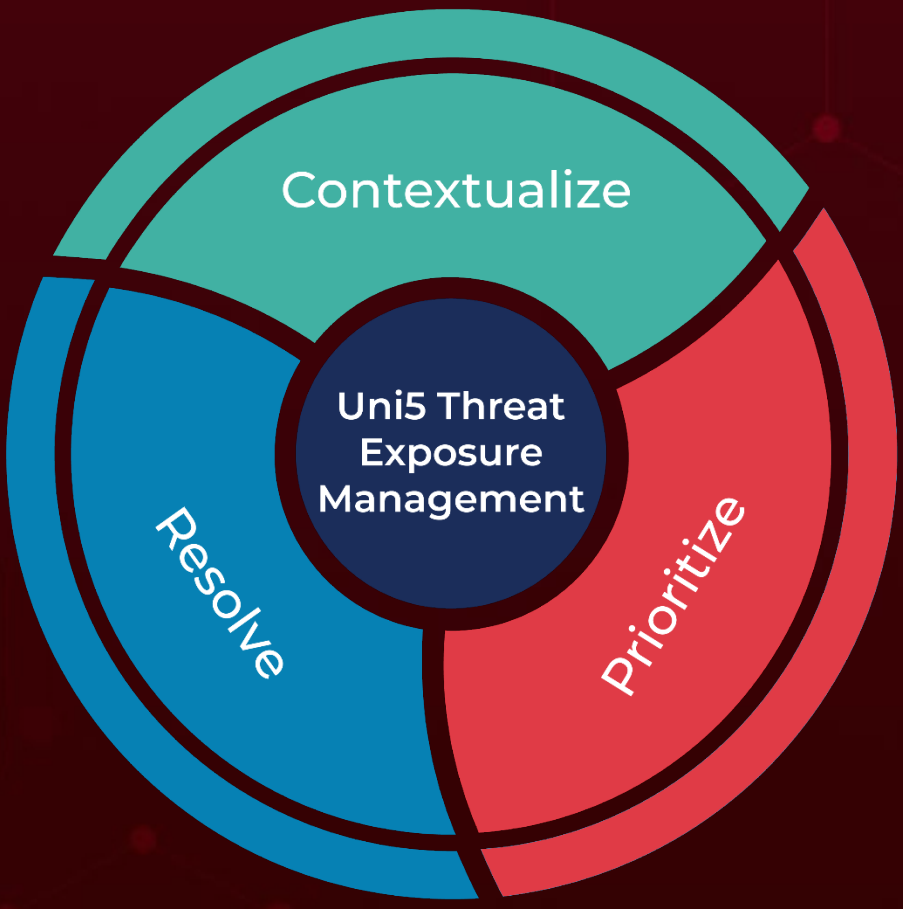
Attack Name	TYPE	VALUE
AvosLocker ransomware	SHA256	05ba2df0033e3cd5b987d66b6de545df439d338a20165c0ba96cde8a74e463e5 7731a9e1e5fff9d912b1d238dcd92c2ba671a5ea55441bb7f14b05ed40039ce1 794f3d25c42d383fad485f9af1d6d7c0508bcfe8ed80a1afea0e0b51bf92bc81 a58864dd006f0528f890c9e000e660f65ffe041ebd2bcb45903fb0228321cfb2 43b7a60c0ef8b4af001f45a0c57410b7374b1d75a6811e0dfc86e4d60f503856 a5ad3355f55e1a15baefea83ce81d038531af516f47716018b1dedf04f081f15 05ba2df0033e3cd5b987d66b6de545df439d338a20165c0ba96cde8a74e463e5 912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9 e81a8f8ad804c4d83869d7806a303ff04f31cce376c5df8aada2e9db2c1eeb98 ddcb0e99f27e79d3536a15e0d51f7f33c38b2ae48677570f36f5e92863db5a96 14f0c4ce32821a7d25ea5e016ea26067d6615e3336c3baa854ea37a290a462a8
	SHA1	9c8f5c136590a08a3103ba3e988073cfd5779519, 05c63ce49129f768d31c4bdb62ef5fb53eb41b54, dab33aaf01322e88f79ffddcbc95d1ad9ad97374, 6f110f251860a7f67657853181417e19c28841eb4, 67f0c8d81aefcfc5943b31d695972194ac15e9f2, 2d1ce0231cf8ff967c36bbfc931f3807ddba765c, 2f3273e5b6739b844fe33f7310476afb971956dd
	MD5	f659d1d15d2e0f3bd87379f8e88c6b42, e09183041930f37a38d0a776a63aa673, 31f8eedc2d82f69ccc726e012416ce33, d3cafcd46dea26c39dec17ca132e5138, 504bd1695de326bc533fde29b8a69319, eb45ff7ea2ccdcceb2e7e14f9cc01397, 829f2233a1cd77e9ec7de98596cd8165, 6ebd7d7473f0ace3f52c483389cab93f, 10ef090d2f4c8001faadb0a833d60089, 8227af68552198a2d42de51cded2ce60, 9d0b3796d1d174080cdfdbd4064bea3a, af31b5a572b3208f81dbf42f6c143f99, 1892bd45671f17e9f7f63d3ed15e348e, cc68eaf36cb90c08308ad0ca3abc17c1, 646dc0b7335cffb671ae3dfd1ebefe47, 609a925fd253e82c80262bad31637f19, c6a667619fff6cf44f447868d8edd681, 3222c60b10e5a7c3158fd1cb3f513640, 90ce10d9aca909a8d2524bc265ef2fa4, 44a3561fb9e877a2841de36a3698abc0,

Attack Name	TYPE	VALUE
AvosLocker ransomware	MD5	5cb3f10db11e1795c49ec6273c52b5f1, 122ea6581a36f14ab5ab65475370107e, c82d7be7afdc9f3a0e474f019fb7b0f7, 825d6049ba8600ee5fefd817ac5444b4
	Email Address	keishagrey994@outlook[.]com
	Virtual Currency Wallets	a6dedd35ad745641c52d6a9f8da1fb09101d152f01b4b0e85a64d21c2a0845ee, bfacebcafff00b94ad2bff96b718a416c353a4ae223aa47d4202cdbc31e09c92, 418748c1862627cf91e829c64df9440d19f67f8a7628471d4b3a6cc5696944dd, bc1qn0u8un00nl6uz6uqrw7p50rg86gjrx492jkwfn
	Tor Address	hxxp[:]//avosqxh72b5ia23dl5fgwcpndkctuzqvh2iefk5imp3pi5gfhel5klad[.]onion, hxxp[:]//avosjon4pfh3y7ew3jdwz6ofw7lljcxlbk7hcxxmnxlh5kvf2akcqjad[.]onion

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

October 16, 2023 . 8:00 AM

More at www.hivepro.com