Date of Publication
August 14, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

7 to 13 AUGUST 2023

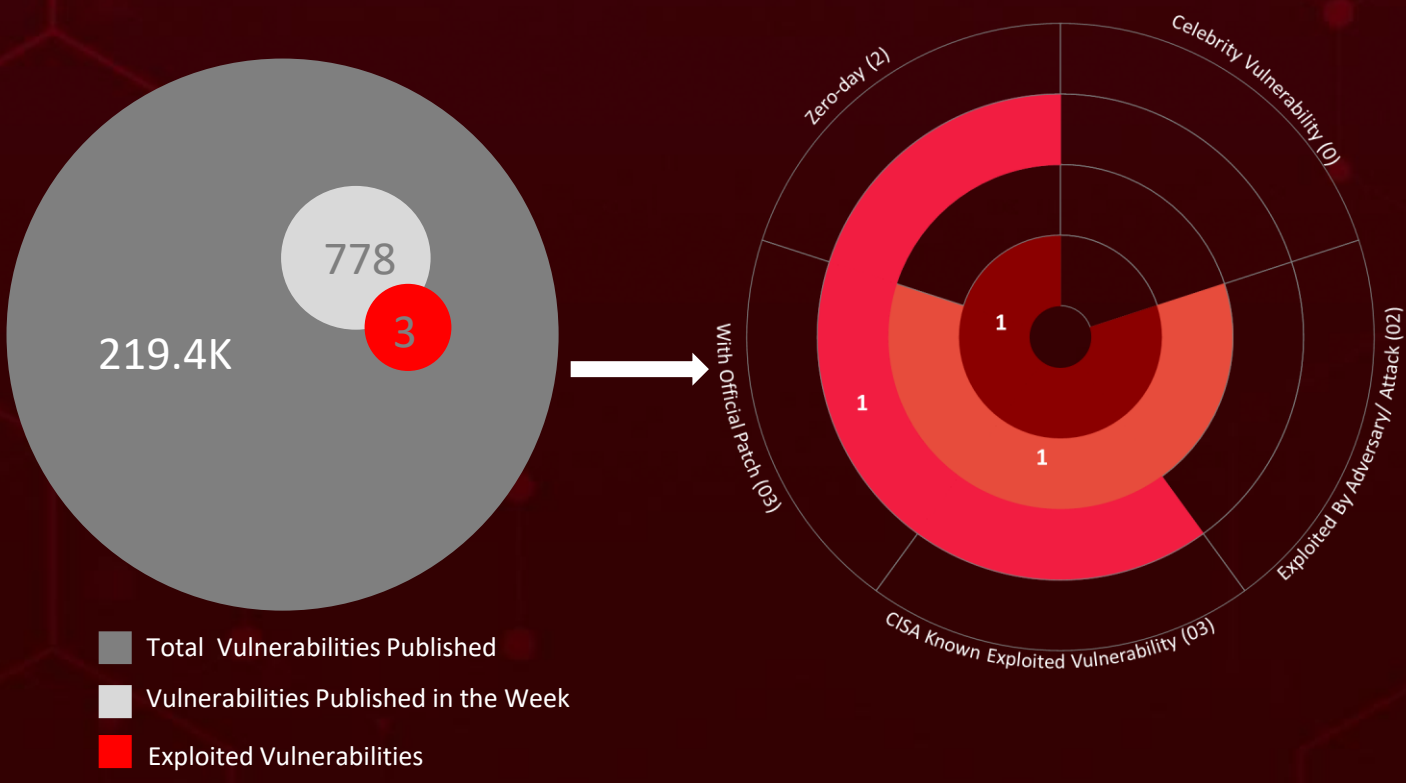
Table Of Contents

Summary

HiveForceLabs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **eleven** attacks executed, **three** vulnerabilities, and **three** different adversaries highlights the ever-present danger of cyber attacks.

Moreover, HiveForceLabs also discovered that both the **Winnti Group** and the **UNC3886** Chinese APT groups employed two malware to carry out espionage attacks on South Korea. Furthermore, they identified the **Gafgyt Botnet** exploiting a critical five-year-old vulnerability that has been present in Zyxel Routers.

Meanwhile, cybercriminals were found to be using **five** types of ransomware and **two** remote-access trojans in various orchestrated campaigns. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

11
Attacks Executed

3
Vulnerabilities Exploited

3
Adversaries in Action

- STRRAT
- TargetCompany Ransomware
- Remcos RAT
- Yashma Ransomware
- WannaCry Ransomware
- Reptile
- Mélofée
- LOLKEK Ransomware
- Rhysida Ransomware
- Gafgyt Botnet
- DroxiDat

- CVE-2023-38180
- CVE-2023-36884
- CVE-2017-18368

- Winnti Group
- UNC3886
- RomCom

Insights

STRRAT A Java-Based RAT Masterfully Harnessing Diverse Capabilities

Five-Year-Old Critical Vulnerability in Zyxel Routers Exploited by **Gafgyt Botnet**

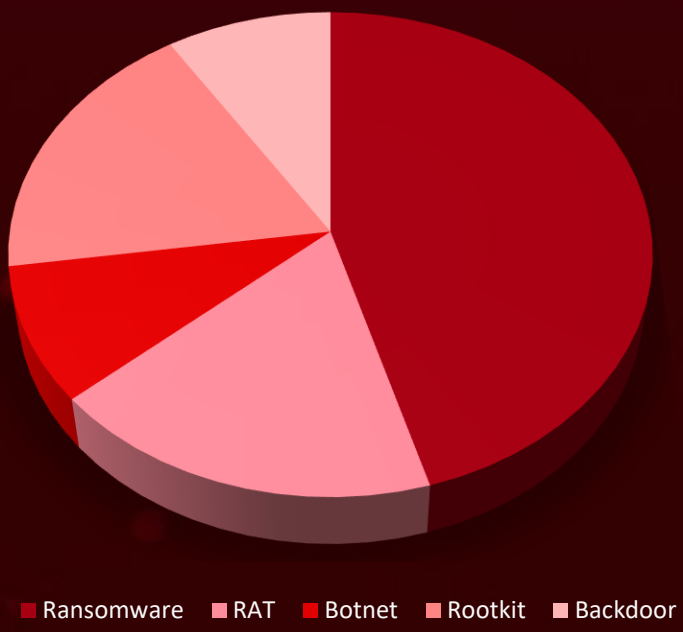
Yashma Ransomware Variant Wielded by Vietnamese-Origin Threat Actor

2 Zero-Day Vulnerabilities Snagged in Microsoft's Patch Tuesday Sweep

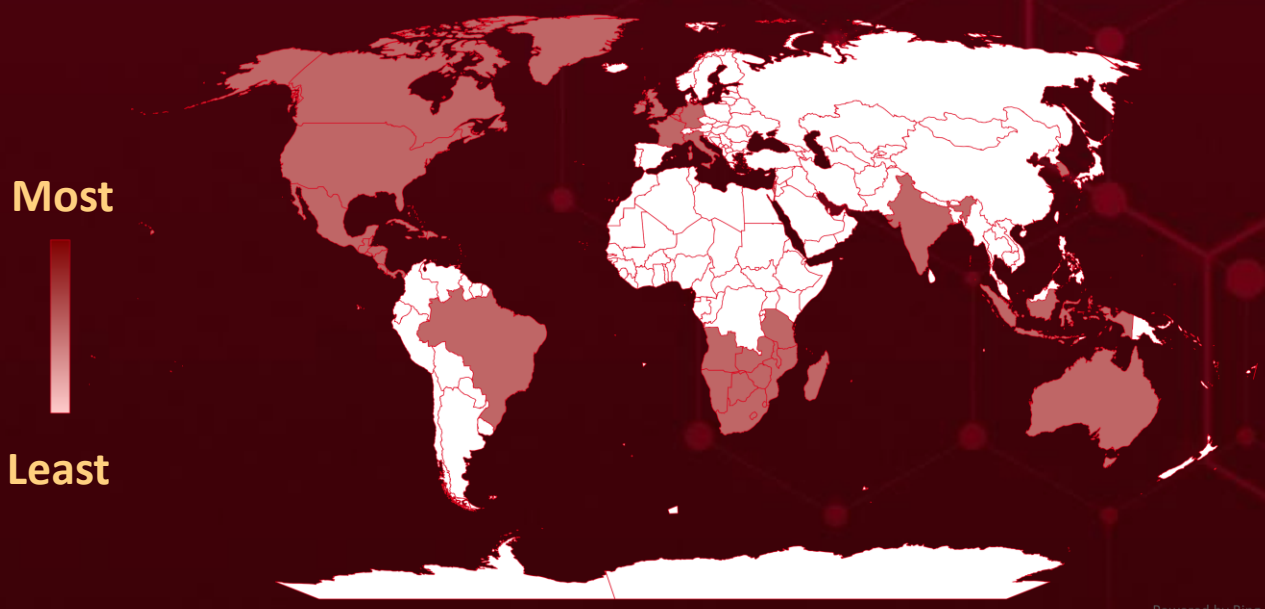
2-Fold Threat **Winnti Group** & **UNC3886** Deploy Open-Source Linux Rootkits for Targeted Attacks in **South Korea**

DroxiDat Sets Sights on Southern African Power Utility

Threat Distribution



Targeted Countries

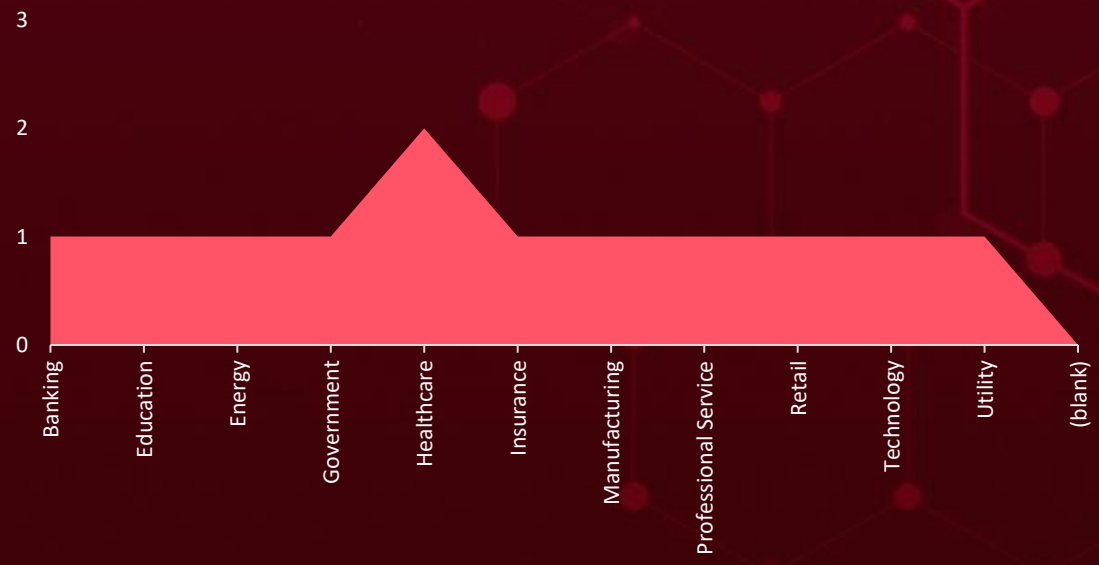


Countries
South Korea
Montserrat
Lesotho
Anguilla
Saint Kitts and Nevis
Antigua and Barbuda
Zimbabwe
Aruba
Martinique
Australia
Nicaragua
Bahamas
Saint Vincent and the Grenadines
Barbados
United Kingdom
Belgium
Italy
Belize
Madagascar
Bermuda
Mexico
Botswana
Namibia
Brazil
Puerto Rico

Countries
British Virgin Islands
Saint Martin
Canada
Sint Maarten
Caribbean Netherlands
Trinidad and Tobago
Cayman Islands
US Virgin Islands
Clipperton Island
Angola
Comoros
Jamaica
Costa Rica
Luxembourg
Cuba
Malawi
Curaçao
Mauritius
Dominica
Monaco
Dominican Republic
Mozambique
El Salvador
Netherlands
Eswatini

Countries
Panama
France
Saint Barthélemy
Germany
Saint Lucia
Greenland
Saint Pierre and Miquelon
Grenada
Singapore
Guadeloupe
South Africa
Guatemala
Tanzania
Haiti
Turks and Caicos Islands
Honduras
United States
India
Zambia
Indonesia
Ireland
Israel

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059
Command and Scripting Interpreter

T1027
Obfuscated Files or Information

T1486
Data Encrypted for Impact

T1547.001
Registry Run Keys / Startup Folder

T1071
Application Layer Protocol

T1070.004
File Deletion

T1082
System Information Discovery

T1036
Masquerading

T1027.009
Embedded Payloads

T1490
Inhibit System Recovery

T1547
Boot or Logon Autostart Execution

T1059.001
PowerShell

T1566
Phishing

T1070
Indicator Removal

T1083
File and Directory Discovery

T1005
Data from Local System

T1566.001
Spearphishing Attachment

T1059.003
Windows Command Shell

T1140
Deobfuscate/ Decode Files or Information

T1588
Obtain Capabilities

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
STRRAT	STRRAT, a Java-based RAT, its latest version, STRRAT 1.6, is notable for employing diverse infection paths and conducting startup host queries to understand system architecture and anti-virus defenses.	Spam Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Extraction	Chrome, Firefox, Internet Explorer, Outlook, Thunderbird, and Foxmail
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	9714dce49616e48fc4851d05453056939ab08bf140fe9a786616fa914debb4f4
SHA1	433b6ac1169a9bd7e0cfe7029954070cc2b4ebdf
MD5	9bc8ac6d3a38357488de33952e929143

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TargetCompany Ransomware (aka Mallox, Fargo, and Tohnichi)	The new TargetCompany ransomware version begins by exploiting insecure SQL servers to consistently install its first stage. The routine attempts persistence by altering the URLs or suitable routes until it successfully locates a location to run the Remcos RAT.	Exploiting vulnerabilities in SQL servers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA256	26a674f981da653d72d139331e0a46e7dc09142ce2bc602655d6fbb37626c668, bcff44c6673ded04c8fb76b733837ce109ac6cbb0e4d1ba5b290f76632a4e718, 1ef8aebbb3816d7d534a581c1d1d8730a73355068e8b39587b2363ccbe692c08
IPv4	80.66.75[.]*

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
Remcos RAT	The Remcos RAT, which acts as a loader, is delivered with TargetCompany Ransomware campagin. Remcos is a lightweight, easy-to-use, and highly flexible Remote Administration Tool with many features.	TargetCompany Ransomware	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	734803d815af2b27fbbb7b4516df3f6fb29ed76d1b16c661a38dbe860831b906, d59f6e95075026e755a415a5dd5fd4b617516c99d064b833e01c7e5d583cf2fd, 2aa688bebce1788d58ca8d42628b5642a4891adaf275b3ac246f7859f6280115		
URL	hxxp://185.209.230[.]21:8080		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Yashma Ransomware	The Yashma ransomware was identified in May 2022 as a modified variant of the Chaos malware. The ransom message used in this effort looks like the well-known WannaCry ransomware note, potentially misleading attribution. The message includes a Bitcoin wallet address but no payment information for ransom payments.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data and Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Vietnamese-origin threat actor			-
IOC TYPE	**VALUE**		
SHA256	3ea6df18492d21811421659c4cf9b88e64c316f2bef8a19766b0c79012476cac		
Email	nguyenvietphat[.]n[at]gmail[.]com		
URL	hxxps[://]github[.]com/nguyenvietphat/Ransomware[.]git		

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
WannaCry Ransomware	WannaCry Ransomware encrypts files or locks the device down. It then demands payment in the form of a cryptocurrency, such as Bitcoin, using GitHub's unique ransom note distribution method.	Exploiting vulnerabilities in the Windows OS	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data and Financial Loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
Vietnamese-origin threat actor			-
IOC TYPE	**VALUE**		
SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa, 74d72f5f488bd3c2e28322c8997d44ac61ee3ccc49b7c42220472633af95c0c0, 994b41a5d3b6d031d9256ed757da213829c7345580819ae574c21eda19ae29db, 4a45fba2077320cbe23c36a025dc37006f73aa97b57abf8404e6c72e7223f0c8, 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Reptile	Reptile, a malware with extensive capabilities that is an open-source kernel module rootkit targeting Linux computers, has surfaced. Its availability on GitHub makes it freely available, and it goes beyond standard malware by providing more than simply concealing techniques. Reptile, unlike other rootkits, includes a reverse shell functionality that gives attackers direct access to infiltrated computers.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Exfiltration of Data	Linux
ASSOCIATED ACTOR			**PATCH LINK**
Winnti Group (aka APT 41, Blackfly, Wicked Panda), UNC3886			-
IOC TYPE	**VALUE**		
MD5	d1abb8c012cc8864dcc109b5a15003ac, f8247453077dd6c5c1471edd01733d7f		

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
Mélofée	The Mélofée malware incorporates a kernel-mode rootkit based on the Reptile open-source project. Discovered linkages to the Winnti Group, which operates out of China, based on the malware and infrastructure utilized in the attacks.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Exfiltration of Data	Linux
ASSOCIATED ACTOR			**PATCH LINK**
Winnti Group (aka APT 41, Blackfly, Wicked Panda), UNC3886			-

IOC TYPE	VALUE
Domains	update[.]ankining[.]com, www.data-yuzefuji.com, ssm[.]awszonwork[.]com
IPv4	156.67.208[.]192, 5.61.57[.]80

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LOLKEK Ransomware (aka GlobeImposter)	LOLKEK is a ransomware family that has been around since 2016. New samples have been observed in the wild in May 2023. These samples use a number of new tactics to evade detection, including obfuscation of the code, use of legitimate tools and services, and encryption of network shares in addition to local drives.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Financial and Information loss	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
SHA1	ed247b58c0680b7c92632209181733e92f1b0721, 768b8d81a6b0f779394e4af48755ca3ad77ed951
SHA256	08029396eb9aef9b413582d103b070c3f422e2b56e1326fe318bef60bdc382ed, 58ac26d62653a648d69d1bcaed1b43d209e037e6d79f62a65eb5d059e8d0fc3f

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
Rhysida Ransomware	The Rhysida ransomware-as-a-service (RaaS) emerged in May 2023, in parallel with the launch of their victim assistance chat platform, accessible via the TOR network.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA1	69b3d913a3967153d1e91ba1a31ebed839b297ed, 338d4f4ec714359d589918cee1adad12ef231907, b07f6a5f61834a57304ad4d885bd37d8e1badba8		
SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Gafgyt Botnet (aka Bashlite, Lizkebab, PinkSlip, Qbot, Torlus, and LizardStresser)		Exploiting Zyxel routers	CVE-2017-18368
TYPE		**IMPACT**	**AFFECTED PRODUCT**
Botnet		Compromise of sensitive data and complete takeover of affected devices.	Zyxel P660HN-T1A Routers
ASSOCIATED ACTOR			**PATCH DETAILS**
-			The Zyxel P660HN-T1A is a legacy product that has reached end-of-life. For the best defense, legacy products should be rep laced with newer-generation equipment.
IOC TYPE	**VALUE**		
SHA256	21ecc53c3fe5336dd717b50fa70e281c5612b0c770f68d9f38c93e13e8357e21, 08d221d2d98a81d85e8bf0e8f3c8c4ddb35cc32c268a2cfe2cb2837e7f8fc731, e1cb8cf85745f7a771b33eab060e04556b1b33d186a65ae069377668fcea47b7, 9fea55b5dd337dcd5c00f4b9c1a09ad2ed5cb7f2c69dc21a7f50f55af0809f89, 06ad76f4b19be8706f98441d926142af824bd2983217f6c2c02201dbb07d0224		

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
DroxiDat	In a targeted operation, an unidentified actor strategically deployed the advanced DroxiDat proxy-capable backdoor alongside Cobalt Strike beacons. The operation was aimed at a critical power utility.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Sensitive Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
MD5	8d582a14279920af10d37eae3ff2b705, 19567b140ae6f266bac6d1ba70459fbd
SHA1	fd9016c64aea037465ce045d998c1eead3971d35, f98b32755cbfa063a868c64bd761486f7d5240cc
SHA256	a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e, a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4

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-2023-38180		.NET: 6.0.0 - 7.0.9, Visual Studio: 17.2.0 17.2.32505.173 - 17.6.5 17.6.33829.357, ASP.NET Core: before 2.1.40	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:.net:-:*:*:*:*:*:*:*	-
.NET and Visual Studio Denial of Service Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-20	T1499.004:Application or System Exploitation, T1499:Endpoint Denial of Service	https://msrc.microsoft.com/vulnerability/CVE-2023-38180

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36884	✗	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2, Microsoft Office: 2013 – 2019, Microsoft Word: 2013 Service Pack 1 – 2019	RomCom
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:office:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	-
Microsoft Office and Windows HTML Remote Code Execution Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-20	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-18368	✗	Zyxel P660HN-T1A Routers	-
	ZERO-DAY		
	✗	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:billion:5200w-t_firmware:-:*:*:*:*:*:*:*	Gafgyt Botnet
Zyxel P660HN-T1A Routers Command Injection Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-78	T1059: Command and Scripting Interpreter	The Zyxel P660HN-T1A is a legacy product that has reached end-of-life. For the best defense, legacy products should be replaced with newer-generation equipment.

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Winnti Group (Blackfly, APT41, Wicked Panda)	China	Materials, composites semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food.	South Korea
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Reptile and Mélofée	Linux
TTPs			
T1105: Ingress Tool Transfer, T1070.004: File Deletion, T1070: Indicator Removal, T1014: Rootkit, T1205.001: Port Knocking, T1205: Traffic Signaling, T1059: Command and Scripting Interpreter, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information, T1095: Non-Application Layer Protocol, T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 UNC3886	China	Defense, Technology, and Telecommunication.	South Korea
	MOTIVE		
	Financial Crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Reptile and Mélofée	Linux
TTPs			
T1105: Ingress Tool Transfer, T1070.004: File Deletion, T1070: Indicator Removal, T1014: Rootkit, T1205.001: Port Knocking, T1205: Traffic Signaling, T1059: Command and Scripting Interpreter, T1140: Deobfuscate/Decode Files or Information, T1027: Obfuscated Files or Information, T1095: Non-Application Layer Protocol, T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Russia	Finance, Telecommunications, Political, Defense, and Government	Worldwide
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
RomCom (Storm-0978, DEV-0978)	CVE-2023-36884	-	Windows: 10 - 11 22H2, Windows Server: 2008 - 2022 20H2, Microsoft Office: 2013 – 2019, Microsoft Word: 2013 Service Pack 1 – 2019
TTPs			
T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation, T1588: Obtain Capabilities, T1588.006: Vulnerabilities, T1588.005: Exploits, T1040: Network Sniffing, T1005: Data from Local System, T1036: Masquerading, T1574: Hijack Execution Flow, T1211: Exploitation for Defense Evasion			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actor **Winnti Group**, **UNC3886**, **RomCom,** and **STRRAT, TargetCompany Ransomware, Remcos RAT, Yashma Ransomware, WannaCry Ransomware, Reptile, Mélofée, LOLKEK Ransomware, Rhysida Ransomware, Gafgyt Botnet,** and **DroxiDat** 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 **three exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Winnti Group**, **UNC3886**, **RomCom** and **STRRAT, TargetCompany Ransomware, Remcos RAT, Yashma Ransomware, WannaCry Ransomware, Reptile, Mélofée, LOLKEK Ransomware, Rhysida Ransomware, Gafgyt Botnet,** and **DroxiDat** in Breach and Attack Simulation(BAS).

Threat Advisories

STRRAT a Java-Powered Versatile Remote Access Trojan

TargetCompany Ransomware's FUD Obfuscation Maneuvers

New Yashma Ransomware Variant Mimics WannaCry in New Attack

Reptile Rootkit Targets Linux Systems in South Korea

Microsoft's August Patch Tuesday Addresses Active Zero-Day Exploits

LOLKEK Ransomware Evolving New Tactics to Evade Detection

Knocking the Surface of Rhysida Ransomware

Gafgyt Botnet Exploiting Five Years Old Critical Vulnerability in Zyxel Routers

DroxiDat Targets Southern African Power Utility

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
STRRAT	SHA256	3d3cb10a1a9059900ddeb58209edcfa52461806558ebbee422c417c6535aa3a5, 8250d324bbc14e3b3a7abc032b6b55aa0699ff9bc784d6c67fdd381edc3b9e56, c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20, 9714dce49616e48fc4851d05453056939ab08bf140fe9a786616fa914debb4f4, c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20, 6ec3e682fbbd0c23fb4e3a2c2b28f03431b90a88651d227ae3f33b6fadf507cf, 058c764614c8b0b457852a71ab93b559f81abb9e13b7fc2d6c6a4962881bf062, 5536bd8910de7571b6e14b2dd8af6da658f0f702321966d5bef85e9d41f6de21, 5536bd8910de7571b6e14b2dd8af6da658f0f702321966d5bef85e9d41f6de21, cbe7d5663fd5359a72f88e44d083703d9625235929c31e0f5b16a0b42cb44d35, 8cae71910574fa96fdf20ddab8897e90d155e50036ddb2f3d033a7b13a45b90f, c9380f51f0dd7167f833669eda3063a1a8f34cc3e2d536f29153952772dc8b20, b74a0e8adc5f0681405c94a684d6b887fdc20cd6d198d069f0981d6ba7d658c6, 31c2e51efcbff0aa489aa6af1a48cf78f6a9febfb449a19d029f8cc8ebb4495f,

Attack Name	TYPE	VALUE
STRRAT	SHA256	ab6f8c51d1f15a18cd23e1ad5a34c82c83746befb7d11cce2860c971be35adaa, d634982709d3ebf1641b1160ed6452fa9e3bf2cc8d28f397e56ca9687b28ec84, a0670c21968e2b1256d72799c22a512e503597ab375d20c49d9ec43428c4c3b2, 3a74d083e1c4e30f1eedcb90c842bf1a7e65a979edab40e37885607bd566bee8, 569f5f6de156bec90f9b0b0e4e707a702c0fea26ab6a0711e32f4a413995ae7c, 176e45016749ec233b8fe1ce32ce2cd47dd5bc8da3663f1c6cf054f6ad58a187, 3094952f4e4c826cdfbc7b146212eec6094f5104b4ba0d70d3b2920a263add27, 4bf781354d02ca0d67a3a180fd6f0d183c6fba763caa660f986752be8b4bb586, 6f7180a451691ee975f516cfc6fb3f0c983bc80aebd1d662a899ff4344e4077e
	SHA1	4651326299d02ac07c0b51c0abb7067f24293a65, 8fa3c76f427f73cbfa864c380769825018cf72f5, f726bf1b6bc380c02d76d273765c888f6b41f197, 433b6ac1169a9bd7e0cfe7029954070cc2b4ebdf
	MD5	9af7e66c85e07a1e182fcb024e7048a2, c7130bf8bca520792f6eff1592a112b2, 61522d1e3290906215d580b8b59e6341, 9bc8ac6d3a38357488de33952e929143
	Domain	talibangeneral[.]dynamic-dns[.]net
	URLs	hxxp://jbfrost[.]live/strigoi/server/?hwid=1&lid=m&ht=5, hxxps://tatchumbemerchants[.]co.ke/Invo-0728403[.]zip.
	File Name	Invo-0728403.zip
TargetCompany Ransomware	SHA256	734803d815af2b27fbbb7b4516df3f6fb29ed76d1b16c661a38dbe860831b906, d59f6e95075026e755a415a5dd5fd4b617516c99d064b833e01c7e5d583cf2fd, 2aa688bebce1788d58ca8d42628b5642a4891adaf275b3ac246f7859f6280115, 26a674f981da653d72d139331e0a46e7dc09142ce2bc602655d6fbb37626c668, bcff44c6673ded04c8fb76b733837ce109ac6cbb0e4d1ba5b290f76632a4e718, 22816dc4dda6beec453e9a48520842b8409c54933cc81f1a338bc77199ab917e,

Attack Name	TYPE	VALUE
TargetCompany Ransomware	SHA256	52fe40246265e29ab791c26e57e568b18cbc4f57c3db5b12beb1415c416d64bb, 1ef8aebbb3816d7d534a581c1d1d8730a73355068e8b39587b2363ccbe692c08, 2efdffd1cf3adab21ff760f009d8893d8c4cbcf63b2c3bfcc1139457c9cd430b, 094d1476331d6f693f1d546b53f1c1a42863e6cde014e2ed655f3cbe63e5ecde, f0e68af393967d8a236461815dd601baf7ebced7b807c224bceb51d0e8bb4b87, 18c909a2b8c5e16821d6ef908f56881aa0ecceeaccb5fa1e54995935fcfd12f7, 08cfd5a321a47a55c5e8732e3d12bf937ca32426dcd668c7d620cfae48159348, e8a3e804a96c716a3e9b69195db6ffb0d33e2433af871e4d4e1eab3097237173, e0d4dc05991211e86c920092966d7025f8e40b77a799428f8491c4f7fa6078a6, 12842d49038c066464ac723b9665ff93f634042646bdd6947b54042fd0e06342, bf28b8a8576beb4755ec6a9d93fc4539e40dee7197b6399dfad5224f5ee74b19, eb75b7d31a9bd3686fcb0088c6849724396871711013 68ebf9134a53abac3c20, 3c665d38c5ccb0b41983ad492b31c499b176219ca7a93494fd902f592cee2ff6, 777a5782426e5b42e0e5e8445dd9602d123e8acc27aca4daa8e9c053f3d5b899, 4b1949536f3f6140da0a9fc87eb0430b61206852145ada5cecbc279b242bce10
	URLs	hxxp://80.66.75[.]37, hxxp://185.209.230[.]21:8080, hxxps[:]//whyers[.]io/QWEwqdsvsf/ap[.]php
	IPv4	195.3.146[.]183, 80.66.75[.]116, 80.66.75[.]*
Remcos RAT	SHA256	734803d815af2b27fbbb7b4516df3f6fb29ed76d1b16c661a38dbe860831b906, d59f6e95075026e755a415a5dd5fd4b617516c99d064b833e01c7e5d583cf2fd, 2aa688bebce1788d58ca8d42628b5642a4891adaf275b3ac246f7859f6280115
	URL	hxxp://185.209.230[.]21:8080

Attack Name	TYPE	VALUE
Yashma Ransomware	SHA1	367411a1e2efde7eb9d39de66be90a96012d5d7b
	SHA256	3ea6df18492d21811421659c4cf9b88e64c316f2bef8a19766b0c79012476cac, de68f4bce05a856ad949e6fb1738559fc506d491d4f6227553695aa9558b64be
	Hostname	www.fxxz[.]com
WannaCry Ransomware	SHA256	ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa, 74d72f5f488bd3c2e28322c8997d44ac61ee3ccc49b7c42220472633af95c0c0, 994b41a5d3b6d031d9256ed757da213829c7345580819ae574c21eda19ae29db, 4a45fba2077320cbe23c36a025dc37006f73aa97b57abf8404e6c72e7223f0c8, 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Reptile	MD5	1957e405e7326bd2c91d20da1599d18e, 246c5bec21c0a87657786d5d9b53fe38, 5b788feef374bbac8a572adaf1da3d38, 977bb7fa58e6dfe80f4bea1a04900276, bb2a0bac5451f8acb229d17c97891eaf, c3c332627e68ce7673ca6f0d273b282e, cb61b3624885deed6b2181b15db86f4d, d1abb8c012cc8864dcc109b5a15003ac, f8247453077dd6c5c1471edd01733d7f
	SHA1	0c6d838c408e88113a4580e733cdb1ca93807989, 2ca4787d2cfffac722264a8bdae77abd7f4a2551, 3cc2d6bf5215de3c24fb194c232a0411cede78e0, 467ea946ac857471e2f01bbdc4258a0ff31c01ce, 76d6cb6b6e9b40b07944153b1f140e786e3ae381, 783736e9274bd2bb90390bb9c23a62c387cde3ef, 7d9eaefeb0c95473ad86abbdcffdbdf6950b8dd2, a5f6162c6b6b6f0c177771a56a6b1eb5d7b593a0, ee295ec546158e425a3660a4a9402916087ccd97
	SHA256	133d3e070e30c94a591450b0930daf9f751debc0f4384fac6ace63f60a383818, 1425a4a89b938d5641ed438333708d1728cfed8c124451180d011f6bbb409976, 15e4e936b2f47eb3fa2455b7c22b2714bebe9f8c01b24bbf7cb5f9559999d292, 17bbebd7d8982d580cc3dea35d988ae2bfd62d708b69662419c41682274e0a14, 4305c04df40d3ac7966289cc0a81cedbdd4eee2f92324b26fe26f57f57265bca,

Attack Name	TYPE	VALUE
Reptile	SHA256	7ce7b914bd434f8a45db1cb3ec783237a5485b7abcee4df06275ea274e095295, 99ffc0099277bef59a37a4cfcf4cdd71df13ad33d1c7bf943dc87f803e75dd2c, cbe9107185c8e42140dbd1294d8c20849134dd122cc64348f1bfcc90401379ec, d182239d408da23306ea6b0f5f129ef401565a4d7ab4fe33506f8ac0a08d37ba
Mélofée	Domain	update[.]ankining[.]com, www.data-yuzefuji.com, ssm[.]awszonwork[.]com
	IPv4	156.67.208[.]192, 5.61.57[.]80
LOLKEK Ransomware	SHA1	ed247b58c0680b7c92632209181733e92f1b0721, 768b8d81a6b0f779394e4af48755ca3ad77ed951, 88baff4e1751bd364cdb1a4bb5fda4a37ee127c4, 456b0bda3f6d9ec9a874daac050b75fc28174510
	SHA256	08029396eb9aef9b413582d103b070c3f422e2b56e1326fe318bef60bdc382ed, 58ac26d62653a648d69d1bcaed1b43d209e037e6d79f62a65eb5d059e8d0fc3f, 2c66e5f96470526219f40c6adfd6990cc28d520975da1fdb6bb5497d55a54117, 0b179973dc267d9c300e9b7d3c27c67a18d7c79b2cc34927cbe5a465f83c6190
	Domains	mmcbkgua72og66w4jz3qcxkkhefax754pg6iknmtfujvkt2j65ffraad[.]onion, filessupport[@]onionmail[.]org
	URL	https[:]//yip[.]su/2QstD5
	MD5	518a38b47292b1e809c5e6f0bb1858be
Rhysida Ransomware	SHA1	69b3d913a3967153d1e91ba1a31ebed839b297ed, 338d4f4ec714359d589918cee1adad12ef231907, b07f6a5f61834a57304ad4d885bd37d8e1badba8, 7abc07e7f56fc27130f84d1c7935a0961bd58cb9, 2543857b275ea5c6d332ab279498a5b772bd2bd4, eda3a5b8ec86dd5741786ed791d43698bb92a262, 69b3d913a3967153d1e91ba1a31ebed839b297ed, 338d4f4ec714359d589918cee1adad12ef231907, b07f6a5f61834a57304ad4d885bd37d8e1badba8
	MD5	59a9ca795b59161f767b94fc2dece71a

Attack Name	TYPE	VALUE
Rhysida Ransomware	SHA256	a864282fea5a536510ae86c77ce46f7827687783628e4f2ceb5bf2c41b8cd3c6, 6903b00a15eff9b494947896f222bd5b093a63aa1f340815823645fd57bd61de, 3bc0340007f3a9831cb35766f2eb42de81d13aeb99b3a8c07dee0bb8b000cb96, 2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951bd6d1b2, 250e81eeb4df4649ccb13e271ae3f80d44995b2f8ffca7a2c5e1c738546c2ab1, 2a3942d213548573af8cb07c13547c0d52d1c3d72365276d6623b3951Bd6d1b2
	URL	hxxps://ipapi[.]com/json/
Gafgyt Botnet	SHA256	21ecc53c3fe5336dd717b50fa70e281c5612b0c770f68d9f38c93e13e8357e21, 08d221d2d98a81d85e8bf0e8f3c8c4ddb35cc32c268a2cfe2cb2837e7f8fc731, e1cb8cf85745f7a771b33eab060e04556b1b33d186a65ae069377668fcea47b7, 9fea55b5dd337dcd5c00f4b9c1a09ad2ed5cb7f2c69dc21a7f50f55af0809f89, 06ad76f4b19be8706f98441d926142af824bd2983217f6c2c02201dbb07d0224, 2481e420138bb0bcc52d43a127e76887cc7419ac46e7495f55493d7fccbbec1b, fc76a4046efbaaab93261806f52afcd6cdf88c2784ec2ed7e862089f3d6bbbb8, 8131b5119e869e1ebf7ebce50837f12fa86fa24008d5534b757c23e91e8f401f, 20770419f79550e46c9bdc2dab792cc96792b7ec4dbd8fcc0cedd7c726ae7987, b8baa7b5d0d60070ef78ad846e17198e891093a84a00e3029dad0ffd77c78b7a, 4f6d665fa107ba9d7313ff6bf1527dddf18bcf178ae34c0e573b3afcb52d685f, b14eb9596f91c1625c3df29413fa08ba313a6b9e6d7fb1297fba74761c135568, a908289bef30086660453ab8809af758af3d445ecda4010211282eb067fef3ab, 9db1a5e089a0b16b3b9a584cb3e5e55eb68620d0ab6b229cf24d49f32b9391be, 94797cd702cf50fea6d780ab0d94cb2a0aa8ee9aa5332e71479adaa7a5245f27, 8ef658a73b292410dd6a570bc65a0f398e838b5adb141eb9dc81ad124fb46f80,

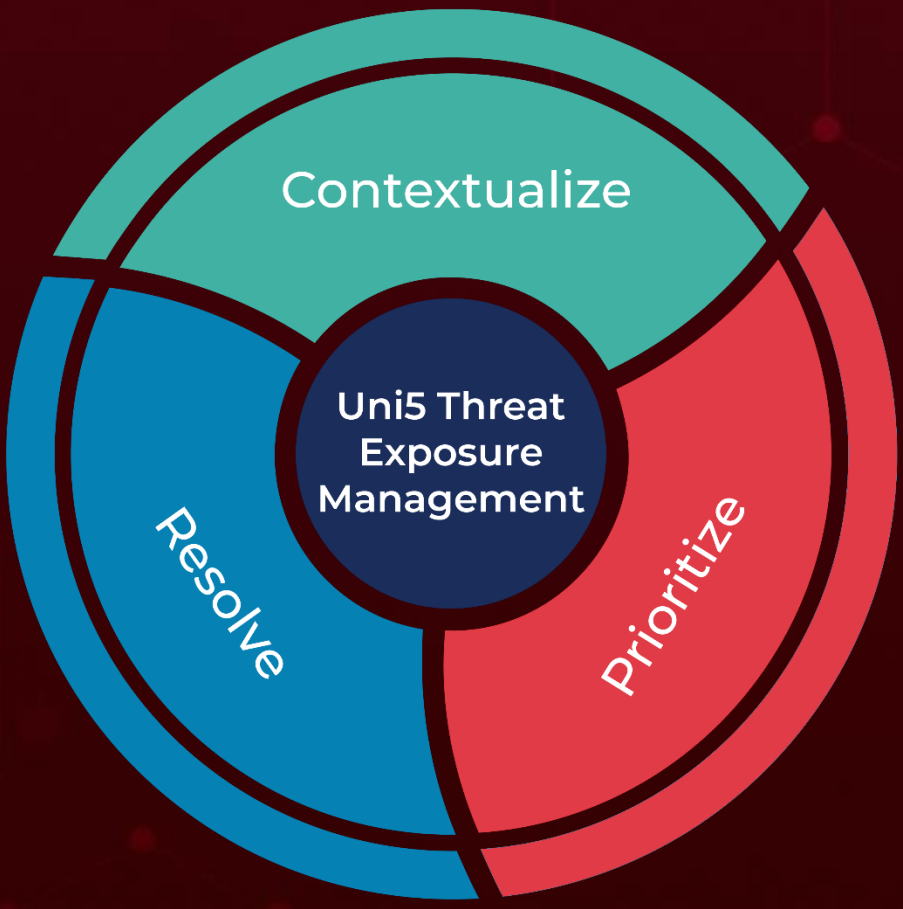
Attack Name	TYPE	VALUE
Gafgyt Botnet	SHA256	8d65b1c26285a08ee8cb11aa868984bd37553e2d2a8e5171d2460c32ca89a2e6, bf4178df292e66a5b2eca7a70df0feb76dfb4463cf70d92ee27d71c77af24f2d, 503a6e977c8fb68ffd015b1f882acdd9f90b98612dd41b676ee08ff10c7d0a90, 84d19f243cae6d14a15eced6cadd77f95dc494058f18a463fdcb18c0b382fe0e, ac0151ff4434a5bb31a4ecbfecc0ba66a6deaf344b6a10a9abf7cce7f6eb094a, be98fcecb03b2638632ebb05c1274d276918408b5f6543c6c7f57c80a7802e98, b95c0e0ba3004f72e0da0f618fe230d5053b8ddd402fdb17088e1ad6e605ef4e, 7917138fac54741ec12ed4d79594f399854996b1abd81ae5fb040b14b8ff483c, 208e4ae853feeede9be36b9385aa38e8547d83c979825ba7b9cb53a53c51c513, ea92d80d8b7d8be657eb667347be9e92004a54bf6f124e143744b6efada650cc, 881e7126f65751a41d59e846908246030f834ec03b15c1ef2cae8c4a1098cf15, 8347e8933783cd4129240b96ae5e665cedc5848ce1cbb7d9f58eb97aaa29b108, 18c58f83cf1e51d23eff699bec82fdef08f8a6585f51610bce162c9de25bc549, 60372d900506da46bf83e318f5f8f8c3219dcda3fca977f0172367d6825dfcdb, 1ef241ca77d2de374113db8b9e9bad4133142326683f2c7954bbab6415780dff, ec83fcc94d1fd981d13c7e5f3318671f3c96e677eaa956c7c1df4de2444c326f, 46ff9f7c0e437df7dd6e1c69790c8fc94e65091e9f3cf1f3243c808f1a1e8621, f0eb89b91e787324bb6f4a082fccea951b00f32ae62f31c80d9d83f4c53a0a65, a580c913a1e16d3fe4e7ebf8d155ac9cb08c1fabf831905776aa5ad6a6361f6f,
DroxiDat	SHA1	be9e23e56c4a25a8ea453c093714eed5e36c66d0, f98b32755cbfa063a868c64bd761486f7d5240cc, fd9016c64aea037465ce045d998c1eead3971d35
	MD5	1957deed26c7f157cedcbdae3c565cff, 8d582a14279920af10d37eae3ff2b705, 19567b140ae6f266bac6d1ba70459fbd

Attack Name	TYPE	VALUE
DroxiDat	Domain	powersupportplan[.]com, epowersoftware[.]com
	SHA256	926fcb9483faa39dd93c8442e43af9285844a1fbbe493f3e4731bbbaecffb732, a00ca18431363b32ca20bf2da33a2e2704ca40b0c56064656432afd18a62824e, a002668f47ff6eb7dd1b327a23bafc3a04bf5208f71610960366dfc28e280fe4
	IPv4	93.115.25[.]41, 179.60.146[.]6, 194.165.16[.]63
	File Paths	C:\perflogs\syscheck.exe, C:\perflogs\a.dll, C:\perflogs\hos.exe, C:\perflogs\host.exe, C:\perflogs\hostt.exe, C:\perflogs\svch.dll, C:\perflogs\svchoct.dll, C:\perflogs\admin\svcpost.dll, C:\perflogs\admin\syscheck.exe, C:\perflogs\sk64.dll, C:\perflogs\clinic.exe

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

August 14, 2023 . 9:00 AM

More at www.hivepro.com