Date of Publication
June 5, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

29 MAY to 4 JUNE 2023

Table Of Contents

Summary

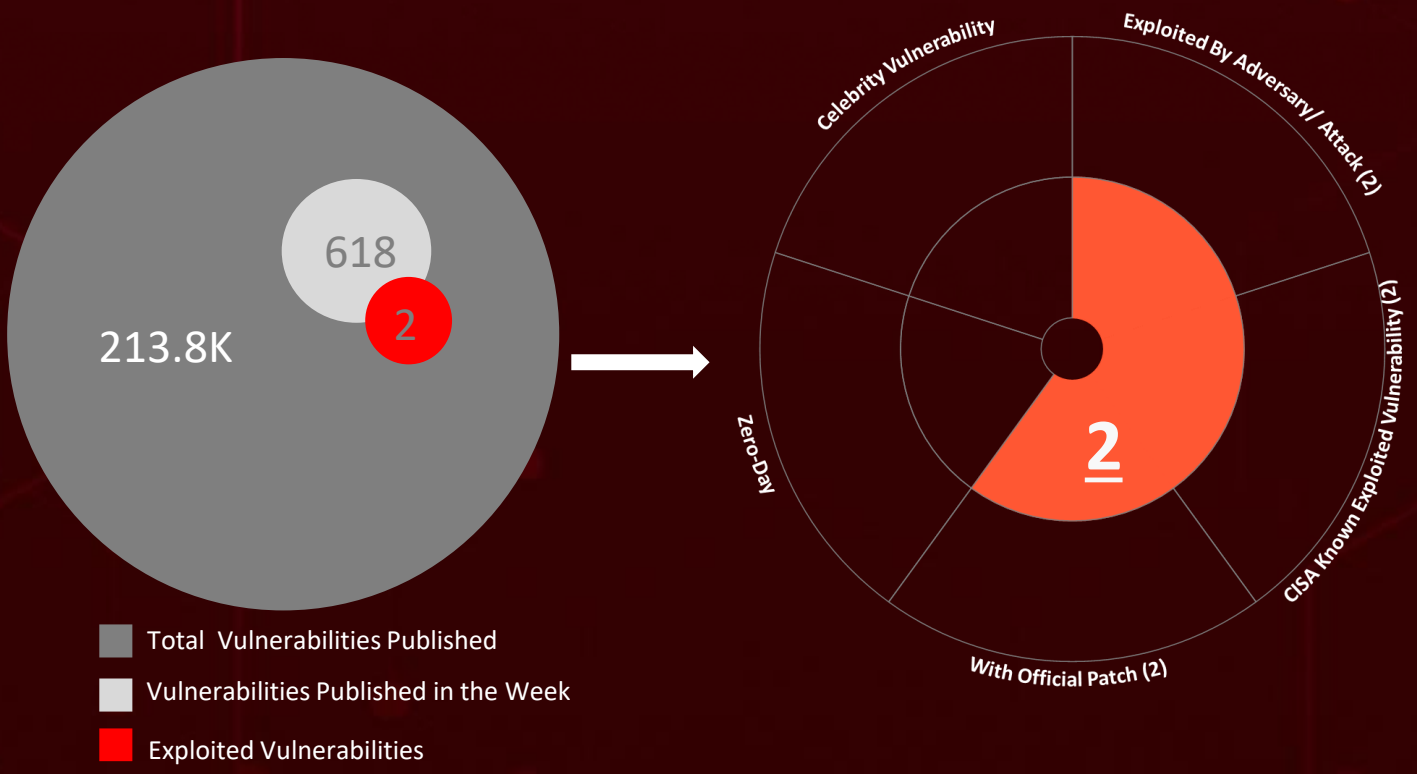
HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, **three** attacks were executed, taking advantage of **two** different vulnerabilities in various systems, and involving **one** adversary highlighting the ever-present danger of cyber-attacks.

Interestingly, these **two** vulnerabilities are part of the known exploited vulnerability catalog by CISA.

Moreover, HiveForce Labs also found that **Blacktail** was exploiting vulnerabilities like PaperCut NG, exfiltrating data, and distributing ransomware.

Furthermore, we identified a new remote access trojan (RAT) named **GobRAT** has emerged and is currently spreading among Linux routers in Japan. It primarily targets routers with vulnerable web interfaces, allowing unauthorized access and potential control by malicious actors.

Meanwhile, an unidentified threat actor recently deployed a botnet program, **Horabot**, to target Spanish-speaking users in the Americas. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

3
Attacks Executed

2
Vulnerabilities Exploited

1
Adversaries in Action

- Buhti Ransomware
- GobRAT
- Horabot
- CVE-2023-27350
- CVE-2022-47986
- Blacktail

Insights

GobRAT

the Menacing New RAT, Ravages Linux Routers in Japan

Two vulnerabilities

Harnessed by Blacktail Threat Actor to Steal Data and Unleash Devastating Ransomware!

Horabot

Sinister Botnet, Wielding Banking Trojan, and Spam Arsenal, Preying on Spanish-Speaking Users in the Americas

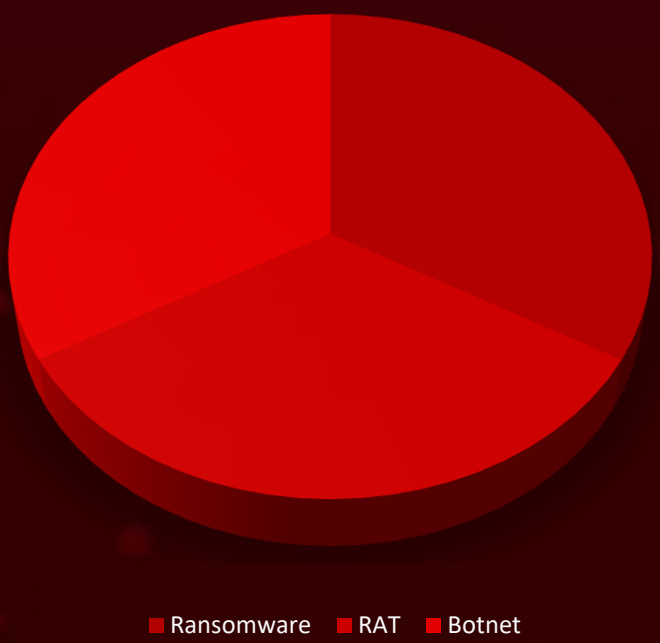
Buhti Ransomware

Employs LockBit and Babuk Variants, Tracing Its Roots to the Notorious Blacktail Hackers!

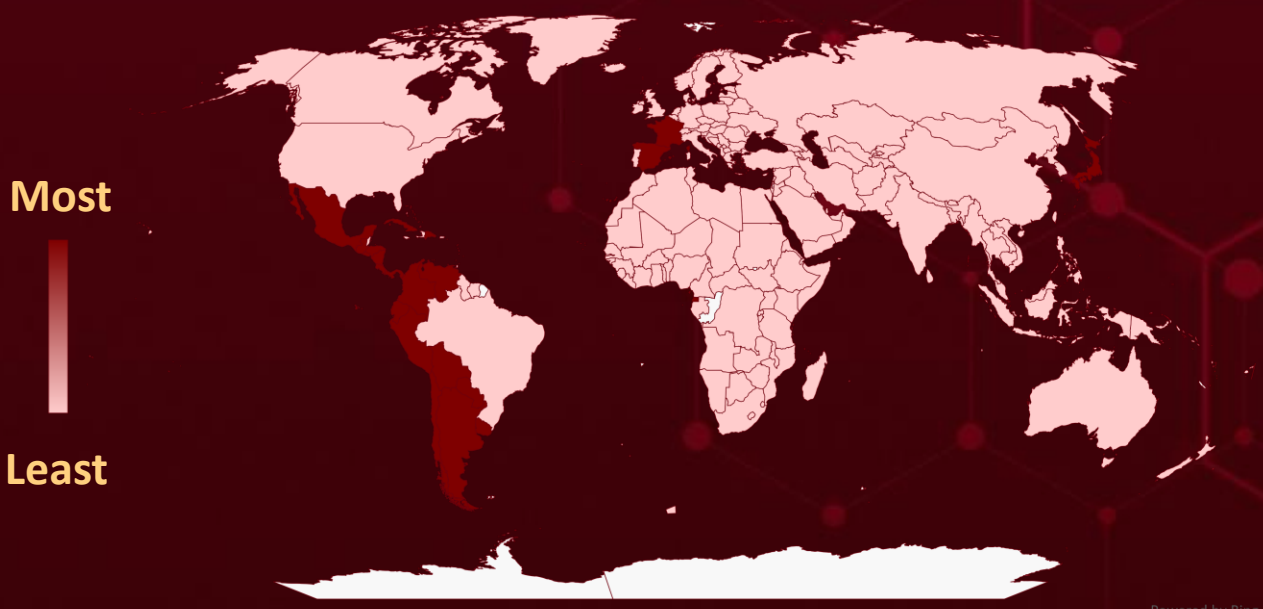
Bullseye Nations

Japan, **Mexico**, **France**, and **Peru** Among the Prime Targets in the Week's Attack Frenzy

Threat Distribution



Targeted Countries



Countries
Mexico
France
Peru
Argentina
Honduras
Bolivia
Panama
Chile
Uruguay
Colombia
Guatemala
Costa Rica
Japan
Cuba
Nicaragua
Dominican Republic
Paraguay
Ecuador
Spain
El Salvador
Equatorial Guinea
Venezuela
Niger
Tunisia
Saudi Arabia
Belgium

Countries
Australia
Belize
Philippines
Benin
Bangladesh
Bermuda
Malawi
Bhutan
Mozambique
Akrotiri and Dhekelia
Oman
Bonaire
Rwanda
Bosnia and Herzegovina
Slovakia
Botswana
Taiwan
Bouvet Island
United States
Brazil
Malta
British Indian Ocean Territory
Mongolia
British Virgin Islands
Nepal
Brunei

Countries
North Korea
Bulgaria
Azerbaijan
Burkina Faso
Puerto Rico
Burundi
Saint Lucia
Cambodia
Sierra Leone
Cameroon
Somaliland
Canada
Suriname
Cayman Islands
Togo
Central African Republic
Uganda
Chad
Belarus
Albania
Maldives
China
Mauritania
Clipperton Island
Moldova
Algeria

Countries
Montserrat
Comoros
Namibia
Congo
New Zealand
Cook Islands
Niue
Coral Sea Islands
Northern Cyprus
American Samoa
Palau
Croatia
Bahamas
Andorra
Poland
Cyprus
Romania
Czech Republic
Saint Barthélemy
Denmark
Samoa
Djibouti
Serbia
Dominica
Sint Eustatius
Angola

Targeted Industries

In the span of the previous week, a trilogy of attacks unfolded, unleashing a cascading attack that resounded across diverse sectors, inflicting profound repercussions upon every industry it touched.

TOP MITRE ATT&CK TTPS

T1027 Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1083** File and Directory Discovery	**T1497** Virtualization/ Sandbox Evasion	**T1190** Exploit Public-Facing Application
T1003 OS Credential Dumping	**T1036** Masquerading	**T1056.001** Keylogging	**T1082** System Information Discovery	**T1047** Windows Management Instrumentation
T1566 Phishing	**T1204** User Execution	**T1057** Process Discovery	**T1584** Compromise Infrastructure	**T1021** Remote Services
T1185 Browser Session Hijacking	**T1059.001** PowerShell	**T1486** Data Encrypted for Impact	**T1070** Indicator Removal	**T1574** Hijack Execution Flow
T1070.004 File Deletion	**T1588** Obtain Capabilities	**T1078** Valid Accounts	**T1140** Deobfuscate/ Decode Files or Information	**T1489** Service Stop

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Buhti Ransomware	Buhti ransomware, linked to Blacktail threat actors, employs leaked code of LockBit and Babuk variants. By exploiting vulnerabilities like PaperCut NG, they exfiltrate data and distribute ransomware. The addition of a custom Golang exfiltration tool heightens the evolving threat.	Exploiting known vulnerabilities	CVE-2023-27350 CVE-2022-47986
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data theft	PaperCut MF and NG & IBM Aspera Faspex
ASSOCIATED ACTOR			**PATCH LINK**
Blacktail			https://www.papercut.com/kb/Main/PO-1216-and-PO-1219 https://www.ibm.com/support/pages/node/6952319

IOC TYPE	VALUE
IPV4	91.215.85[.]183 81.161.229[.]120
SHA256	063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7 eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206 d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74E1a6b7d6

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
GobRAT	GobRAT, a new RAT, is infecting Linux routers in Japan through vulnerable web interfaces, granting attackers remote control and the ability to execute commands.	Exploiting known vulnerabilities In WEBUI accessible routers	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data theft	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
URLs	https[:]//su.vealcat[.]com http[:]//su.vealcat[.]com:58888 https[:]//ktlvz.dnsfailover[.]net http[:]//ktlvz.dnsfailover[.]net:58888		
SHA256	060acb2a5df6560acab9989d6f019fb311d88d5511f3eda0effcbd9fc6bd12bb feaef47defd8b4988e09c8b11967e20211b54e16e6df488780e2490d7c7fa02a		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Horabot	Horabot was deployed by a threat actor since November 2020. The botnet delivers a banking trojan and spam tool to victim machines. The attacker primarily targets Spanish-speaking users in the Americas, with a focus on Mexico.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		Collection of sensitive information	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
IPV4	139[.]177[.]193[.]74 185[.]45[.]195[.]226 216[.]238[.]70[.]224		
SHA256	63535100bbc1ba8ce9afb5883a59a4138e95c8e33a4585b8285ea7a39e0ead3e ffd43b32655fc6f1e1c10f88660b68e2c2ad7da271b0f2e3eda70ccdcb3bcee4 720c126f372b68ff79ef13bd1ae6fc9a6aef10669269490d7e8fb589d7d49064		

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-2023-27350	ZERO-DAY	PaperCut NG: before 22.0.9 PaperCut MF: before 22.0.9	-
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:*	Bl00dy Ransomware, Clop Ransomware, LockBitRansomware, DiceLoader, TrueBot, and Cobalt Strike Beacons
PaperCut MF/NG Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-47986	ZERO-DAY	IBM Aspera Faspex for Windows: 4.4.1 - 4.4.2 PL1 & IBM Aspera Faspex for Linux: 4.4.1 - 4.4.2 PL1	Blacktail
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ibm:aspera_faspex:*:*:*:*:*:*:*:*	Buhti Ransomware
IBM Aspera Faspex Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059:Command and Scripting Interpreter, T1068:Exploitation for Privilege Escalation	https://www.ibm.com/support/pages/node/6952319

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Blacktail	Unknown	-	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-27350 CVE-2022-47986	Buhti Ransomware	PaperCut MF and NG & IBM Aspera Faspex
TTPs			
T1047:Windows Management Instrumentation;T1059:Command and Scripting Interpreter;T1129:Shared Modules; T1027:Obfuscated Files or Information; T1036:Masquerading; T1497:Virtualization/Sandbox Evasion; T1003:OS Credential Dumping;T1056:Input Capture;T1056.001:Keylogging;T1057:Process Discovery;T1082:System Information Discovery; T1083:File and Directory Discovery;T1518:Software Discovery; T1518.001:Security Software Discovery; T1005:Data from Local System; T1185:Browser Session Hijacking;T1486:Data Encrypted for Impact; T1489:Service Stop			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actor **Blacktail** and **Buhti Ransomware**, **GobRAT**, and **Horabot** 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 **two exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Blacktail** and **Buhti Ransomware**, **GobRAT**, and **Horabot** in Breach and Attack Simulation(BAS).

Threat Advisories

Buhti Ransomware Operation Repurposes Leaked Encryptors

A New RAT Named GobRAT Targeting Linux Routers in Japan

A New Horabot Botnet Threat Targeting Spanish-Speaking Users in the Americas

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
Buhti Ransomware	IPV4	91.215.85[.]183 81.161.229[.]120
	SHA256	063fcedd3089e3cea8a7e07665ae033ba765b51a6dc1e7f54dde66a79c67e1e7 eda0328bfd45d85f4db5dbb4340f38692175a063b7321b49b2c8ebae3ab2868c e5d65e826b5379ca47a371505678bca6071f2538f98b5fef9e33b45da9c06206 d65225dc56d8ff0ea2205829c21b5803fcb03dc57a7e9da5062cbd74e1a6b7d6 d259be8dc016d8a2d9b89dbd7106e22a1df2164d84f80986baba5e9a51ed4a65 8b5c261a2fdaf9637dada7472b1b5dd1d340a47a00fe7c39a79cf836ef77e441 898d57b312603f091ff1a28cb2514a05bd9f0eb55ace5d6158cc118d1e37070a 515777b87d723ebd6ffd5b755d848bb7d7eb50fc85b038cf25d69ca7733bd855 4dc407b28474c0b90f0c5173de5c4f1082c827864f045c4571890d967eadd880

Attack Name	TYPE	VALUE
Buhti Ransomware	SHA256	22e74756935a2720eadacf03dc8fe5e7579f354a6494734e2183095804ef19fe 18a79c8a97dcfff57e4984aa7e74aa6ded22af8e485e807b34b7654d6cf69eef 01b09b554c30675cc83d4b087b31f980ba14e9143d387954df484894115f82d4 7eabd3ba288284403a9e041a82478d4b6490bc4b333d839cc73fa665b211982c 287c07d78cafc97fb4b7ef364a228b708d31e8fe8e9b144f7db7d986a1badd52 32e815ef045a0975be2372b85449b25bd7a7c5a497c3facc2b54bcffcbb0041c 5b3627910fe135475e48fd9e0e89e5ad958d3d500a0b1b5917f592dc6503ee72 d59df9c859ccd76c321d03702f0914debbadc036e168e677c57b9dcc16e980cb de052ce06fea7ae3d711654bc182d765a3f440d2630e700e642811c89491df72 65c91e22f5ce3133af93b69d8ce43de6b6ccac98fc8841fd485d74d30c2dbe7b 8041b82b8d0a4b93327bc8f0b71672b0e8f300dc7849d78bb2d72e2e0f147334 8b2cf6af49fc3fb1f33e94ad02bd9e43c3c62ba2cfd25ff3dfc7a29dde2b20f2 97378d58815a1b87f07beefb24b40c5fb57f8cce649136ff57990b957aa9d56a c33e56318e574c97521d14d68d24b882ffb0ed65d96203970b482d8b2c332351 9b8adde838c8ea2479b444ed0bb8c53b7e01e7460934a6f2e797de58c3a6a8bf 9f0c35cc7aab2984d88490afdb515418306146ca72f49edbfbd85244e63cfabd ca6abfa37f92f45e1a69161f5686f719aaa95d82ad953d6201b0531fb07f0937 Bdfac069017d9126b1ad661febfab7eb1b8e70af1186a93cb4aff93911183f24
GobRAT	URLs	https[:]//su.vealcat[.]com http[:]//su.vealcat[.]com:58888 https[:]//ktlvz.dnsfailover[.]net http[:]//ktlvz.dnsfailover[.]net:58888
	Domains	su.vealcat[.]com ktlvz.dnsfailover[.]net wpksi.mefound[.]com

Attack Name	TYPE	VALUE
GobRAT	SHA256	060acb2a5df6560acab9989d6f019fb311d88d5511f3eda0effcbd9fc6bd12bb feaef47defd8b4988e09c8b11967e20211b54e16e6df488780e2490d7c7fa02a 3e44c807a25a56f4068b5b8186eee5002eed6f26d665a8b791c472ad154585d1 60bcd645450e4c846238cf0e7226dc40c84c96eba99f6b2cffcd0ab4a391c8b3 a8b914df166fd0c94106f004e8ca0ca80a36c6f2623f87a4e9afe7d86b5b2e3a aeed77896de38802b85a19bfcb8f2a1d567538ddc1b045bcdb29cb9e05919b60 6748c22d76b8803e2deb3dad1e1fa7a8d8ff1e968eb340311fd82ea5d7277019 e133e05d6941ef1c2e3281f1abb837c3e152fdeaffefde84ffe25338fe02c56d 43dc911a2e396791dc5a0f8996ae77ac527add02118adf66ac5c56291269527e af0292e4de92032ede613dc69373de7f5a182d9cbba1ed49f589ef484ad1ee3e 2c1566a2e03c63b67fbdd80b4a67535e9ed969ea3e3013f0ba503cfa58e287e3 98c05ae70e69e3585fc026e67b356421f0b3d6ab45b45e8cc5eb35f16fef130c 300a92a67940cfafeed1cf1c0af25f4869598ae58e615ecc559434111ab717cd a363dea1efda1991d6c10cc637e3ab7d8e4af4bd2d3938036f03633a2cb20e88 0c280f0b7c16c0d299e306d2c97b0bff3015352d2b3299cf485de189782a4e25 f962b594a847f47473488a2b860094da45190738f2825d82afc308b2a250b5fb 4ceb27da700807be6aa3221022ef59ce6e9f1cda52838ae716746c1bbdee7c3d 3e1a03f1dd10c3e050b5f455f37e946c214762ed9516996418d34a246daed521 3bee59d74c24ef33351dc31ba697b99d41c8898685d143cd48bccdff707547c0 c71ff7514c8b7c448a8c1982308aaffed94f435a65c9fdc8f0249a13095f665e
Horabot	IPV4	139[.]177[.]193[.]74 185[.]45[.]195[.]226 216[.]238[.]70[.]224 51[.]38[.]235[.]152 137[.]220[.]53[.]87

Attack Name	TYPE	VALUE
Horabot	IPV4	212[.]46[.]38[.]43 191[.]101[.]2[.]101
	Domains	tributaria[.]website facturacionmarzo[.]cloud m9b4s2[.]site wiqp[.]xyz ckws[.]info amarte[.]store
	SHA256	63535100bbc1ba8ce9afb5883a59a4138e95c8e33a4585b8285ea7a39e0ead3e ffd43b32655fc6f1e1c10f88660b68e2c2ad7da271b0f2e3eda70ccdcb3bcee4 720c126f372b68ff79ef13bd1ae6fc9a6aef10669269490d7e8fb589d7d49064 aaf456575c8761f3af9b61e015282d9162325ed09b699732bf65b53ae7b7d252 fd932d83965d20683ea7f99244dc672e0b4187c9e7588578b626b99d67ac71a6 39194718b460ea174784f6a7edbccd1e3324fe1043be806927cece7a86f15611 474b25badb40f524a7b2fe089e51eb7dbafd2e3e03a9f6750f72055d05b13d76 07f7575af922da1aea5aa26436a3cfcd91b419bbf31d77bf6c9d921290bc04da 74a7d13289029d8439e38e0acb4d3b526c63ae863a41218a511182d8f0e6ebef 26e06886d9dde7c9ecdc9b223e5f325d0af27cc9b470179a8e493ac300bd783e 294363039bf93d4c34c8769e581b9c47f8ea210e427fc1feed128bd9bf979a4a
	URLs	hxxps[://]tributaria[.]website/ hxxps[://]tributaria[.]website/ESP/12/151222/UP/UP hxxps[://]tributaria[.]website/A/08/150822/AU/TST/INDEX[.]PHP?LIST hxxps[://]tributaria[.]website/a/09/01092022/au/tst/index[.]php?list hxxps[://]tributaria[.]website/a/08/150822/up/up hxxps[://]tributaria[.]website/esp/12/151222/up/up hxxps[://]tributaria[.]website/a/W_/X\\W_YY/au/au hxxps[://]tributaria[.]website/a/08/150822/au/au hxxp[://]tributaria[.]website:443/ hxxps[://]tributaria[.]website/A/08/150822/AU/AU hxxps[://]tributaria[.]website/esp/12/151222/au/au hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0703[.]html

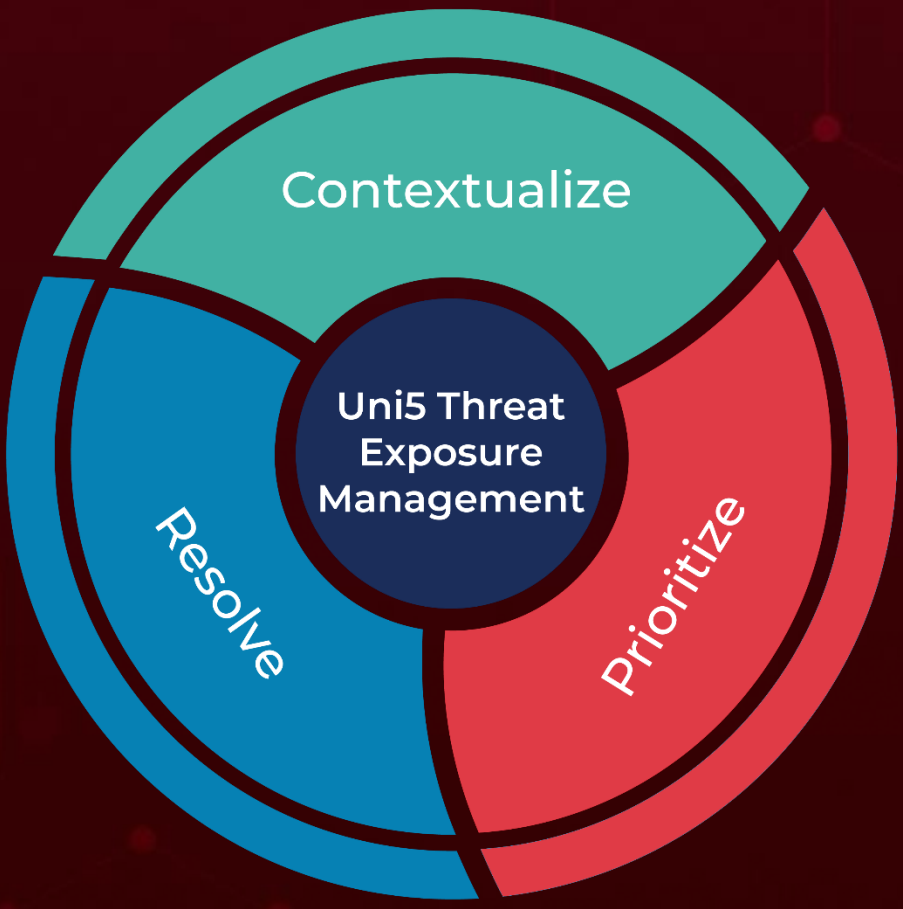
Attack Name	TYPE	VALUE
Horabot	URLs	hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/adjuntos_0703[.]html hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/logs/index[.]php?CHLG hxxp[://]139[.]177[.]193[.]74/ hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/tst/index[.]php?list hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2102[.]html hxxp[://]139[.]177[.]193[.]74/09/01092022/au/adjuntos_2102[.]html hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]htm hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_0102[.]html hxxp[://]139[.]177[.]193[.]74:443/ hxxp[://]139[.]177[.]193[.]74/a/08/150822/au/adjuntos_2012[.]html hxxp[://]139[.]177[.]193[.]74/A/08/150822/AU/ADJUNTOS_2012[.]HTML hxxp[://]139[.]177[.]193[.]74/esp/12/151222/au/gm/index[.]php?CHLG hxxp[://]ec2-54-234-37-57[.]compute-1[.]amazonaws[.]com/m/documento-pdf[.]html hxxp[://]ec2-54-234-37-57[.]compute-1[.]amazonaws[.]com/m/index[.]php?va hxxps[://]facturacionmarzo[.]cloud/m/archivos[.]pdf[.]html hxxps[://]facturacionmarzo[.]cloud/e/archivos[.]pdf[.]html hxxp[://]216[.]238[.]70[.]224/20/t/e/m.zip hxxp[://]ckws[.]info/ hxxps[://]ckws[.]info/a/310122/up/up hxxps[://]ckws[.]info/a/310122/au/au hxxp[://]ckws[.]info/a/07/080722/up/up hxxp[://]ckws[.]info/a/07/080722/au/au hxxps[://]ckws[.]info/A/07/080722/UP/UP hxxps[://]ckws[.]info/a/0511/ hxxp[://]ckws[.]info/a/0511 hxxps[://]ckws[.]info/a/0511/up/up hxxp[://]ckws[.]info/a/0511/au/au hxxp[://]m9b4s2[.]site/ hxxps[://]m9b4s2[.]site/ hxxps[://]m9b4s2[.]site/a1/u hxxps[://]m9b4s2[.]site/a1/u/ hxxps[://]m9b4s2[.]site/2001525248/12457856[.]html%20%20Servicio% 20de%20Administraci%C3%B3n%20Tributaria

Attack Name	TYPE	VALUE
Horabot	URLs	hxxp[://]m9b4s2[.]site/2001525248/12457856[.]html hxxps[://]m9b4s2[.]site/2001525248/12457856[.]html=0A= hxxps[://]m9b4s2[.]site/tst/index[.]php?list hxxps[://]m9b4s2[.]site/a1/u/a/xml[.]dat hxxps[://]m9b4s2[.]site/a1/u/a/index[.]php hxxps[://]m9b4s2[.]site/a1/u/a/index[.]p[.]h[.]p hxxps[://]m9b4s2[.]site/a1/u/a/xml[.]dat' hxxp[://]m9b4s2[.]site/N/I hxxp[://]m9b4s2[.]site/k/I hxxp[://]m9b4s2[.]site/A/I hxxp[://]m9b4s2[.]site/k hxxp[://]m9b4s2[.]site/a/i hxxp[://]m9b4s2[.]site/K/I hxxp[://]m9b4s2[.]site/A/I' hxxp[://]m9b4s2[.]site/k/I hxxps[://]m9b4s2[.]site/i7_5_7_3_3_2E9Uogmx/i7_5_7_3_3_2E9Uog/i7 _5_7_3_3_2E9Uogal/i7_5_7_3_3_2E9Uog hxxps[://]m9b4s2[.]site/M1S8823HSN34/?1538567474 hxxp[://]wiqp[.]xyz/ hxxps[://]wiqp[.]xyz/ hxxps[://]wiqp[.]xyz/09/01092022/au/au hxxp[://]wiqp[.]xyz/09/01092022/up/up hxxps[://]amarte[.]store/ hxxps[://]amarte[.]store/a/08/150822/au/au hxxps[://]amarte[.]store/a/08/150822/up/up hxxp[://]51[.]38[.]235[.]152/20/a/m/m[.]zip hxxp[://]137[.]220[.]53[.]87/20/t/p/m[.]zip hxxp[://]212[.]46[.]38[.]43/m/1 hxxp[://]212[.]46[.]38[.]43/e/1 hxxp[://]191[.]101[.]2[.]101/m/1

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.



REPORT GENERATED ON

June 5, 2023 . 4:44 AM

More at www.hivepro.com