Date of Publication
July 31 , 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

24 to 30 JULY 2023

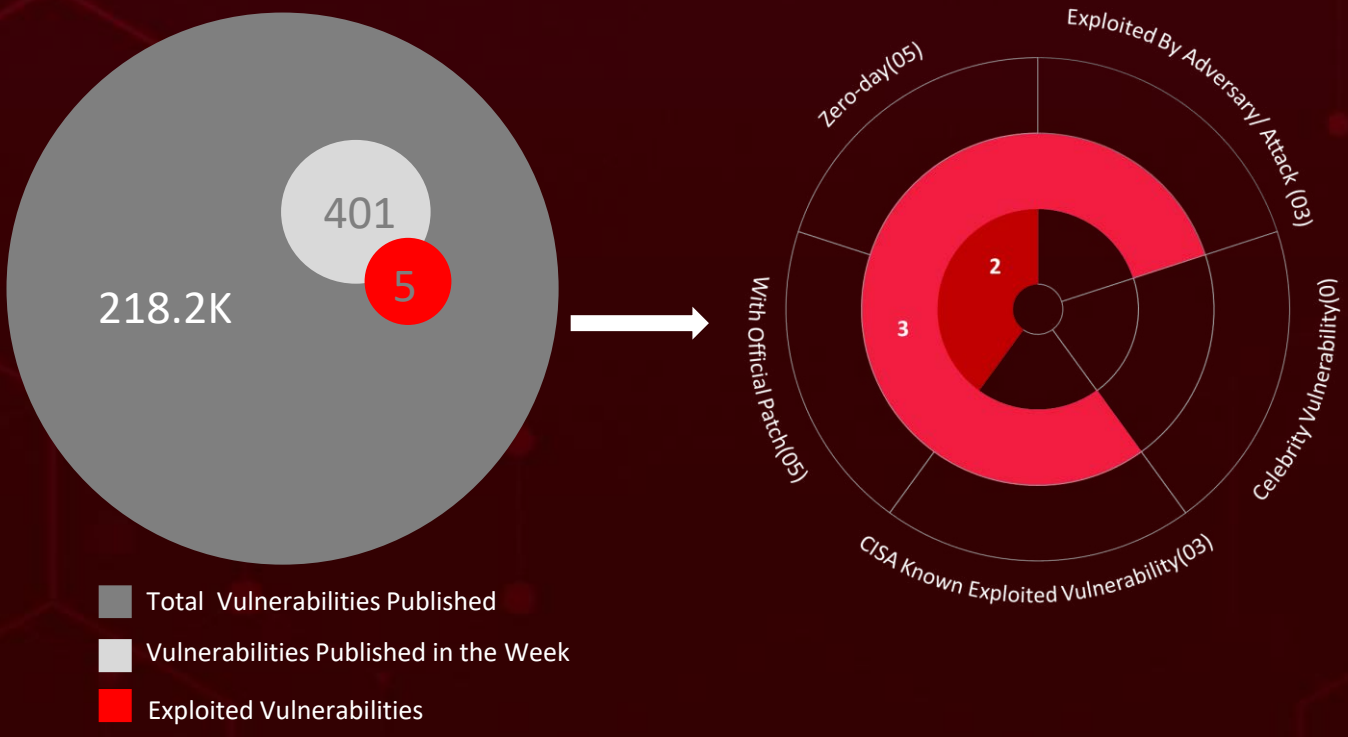
Table Of Contents

Summary

HiveForceLabs recently made several significant discoveries related to cybersecurity threats. Over the past week, We identified a total of **six** executed attacks, **one** adversary activities, and **five** zero-day vulnerabilities including widely exploited vulnerabilities in Apple products and Zimbra platform highlighting the ever-present danger of cyber attacks.

Additionally, HiveForceLabs uncovered a new **Decoy Dog** toolkit that uses DNS for C2 (Command and Control) communication, evading detection with its wildcard-type behavior and encryption methods.

Meanwhile, a China-based threat actor named **Storm-0558**, with espionage goals, was found to engage in unauthorized access to email data from various organizations. All these observed attacks have been on the rise, posing a significant threat to users worldwide.



High Level Statistics

5
Attacks Executed

5
Vulnerabilities Exploited

1
Adversaries in Action

- Cigril
- Realst Infostealer
- Fenix Botnet
- Decoy Dog
- Pupy RAT

- CVE-2023-38606
- CVE-2023-26077
- CVE-2023-26078
- CVE-2023-35078
- CVE-2023-37580

- Storm-0558

Insights

Realst Infostealer
Cleverly disguised as fake blockchain games

Ivanti Addressed **CVE-2023-35078**, Zero-day Authentication Bypass Vulnerability in **EPMM**

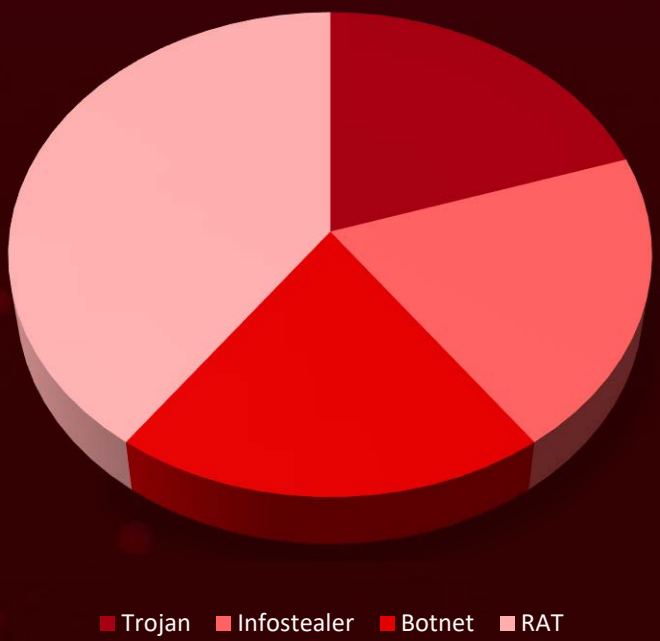
Zimbra
Fixes CVE-2023-37580, zero-day XSS flaw in the Zimbra Classic Web Client interface

Storm-0558 Threat actor is targeting email accounts in the US, Europe, Taiwan, and Uyghur

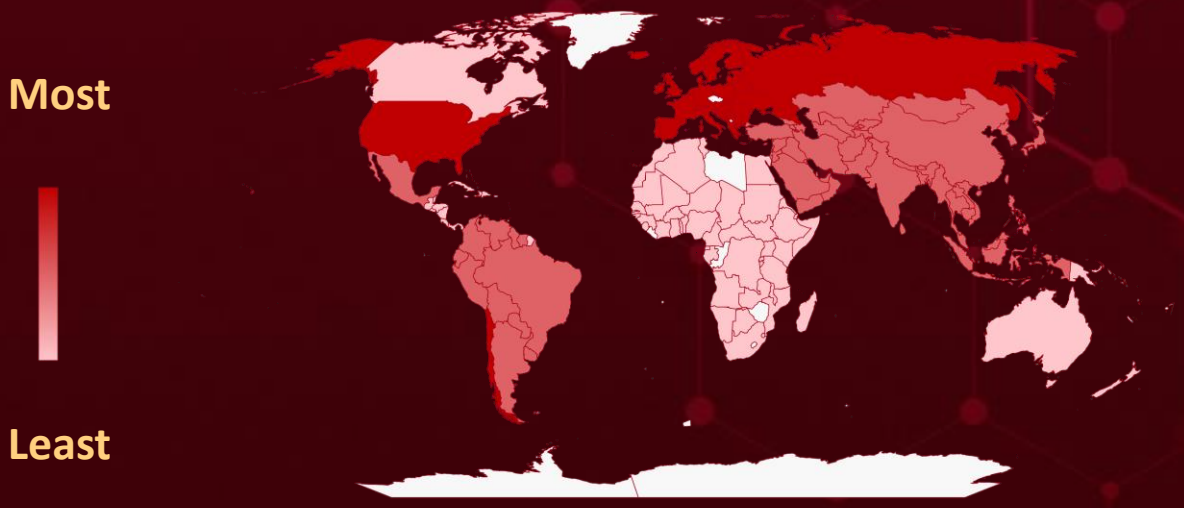
CVE-2023-38606
A zero-day vulnerability discovered in multiple Apple products is being actively exploited in the wild.

Fenix Botnet
Targets tax-paying individuals in Mexico and Chile

Threat Distribution



Targeted Countries



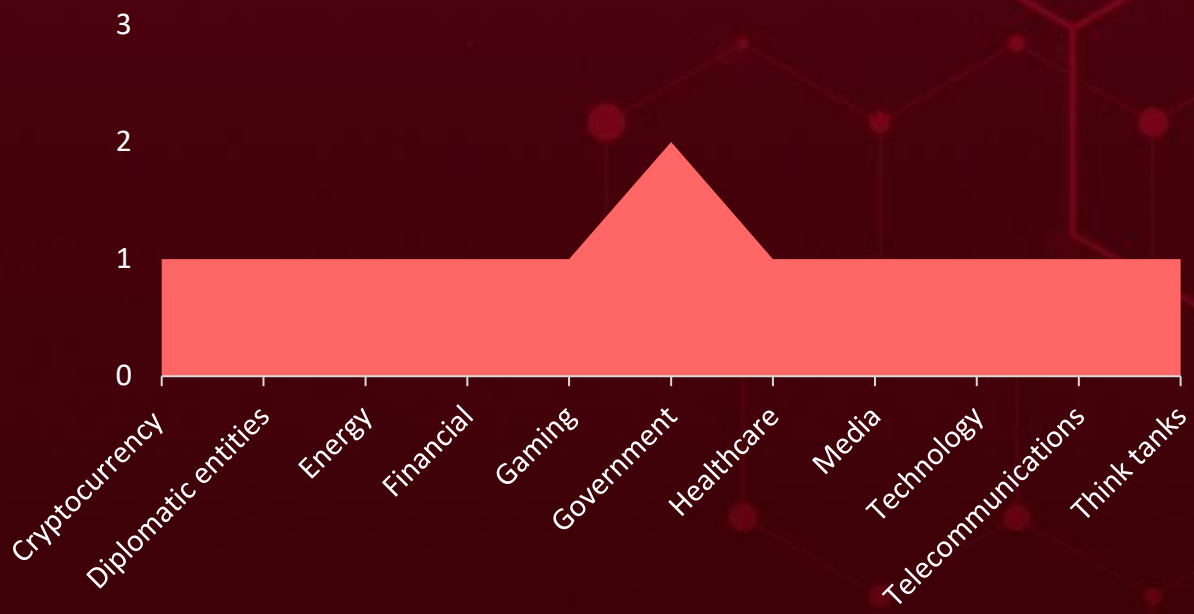
Countries
Netherlands
United States
Serbia
Albania
Malta
Andorra
Portugal
Austria
Sweden
Belarus
Lithuania
Belgium
Monaco
Bosnia and Herzegovina
Norway
Bulgaria
Russia
Chile
Slovenia
Croatia
Ukraine
United Kingdom

Countries
Czech Republic (Czechia)
Liechtenstein
Denmark
Luxembourg
Estonia
Moldova
Finland
Montenegro
France
North Macedonia
Germany
Poland
Greece
Romania
Holy See
San Marino
Hungary
Slovakia
Iceland
Spain
Ireland
Switzerland
Italy
Latvia
Turkey

Countries
Oman
Qatar
Syria
Israel
Kyrgyzstan
Kuwait
Laos
Saudi Arabia
Cyprus
State of Palestine
United Arab Emirates
Timor-Leste
Argentina
Bangladesh
Uzbekistan
Indonesia
Bhutan
Singapore
Ecuador
Armenia
Bolivia
Japan
Malaysia
Tajikistan

Countries
Maldives
Turkmenistan
Azerbaijan
Philippines
Mexico
China
Brazil
India
Georgia
Iran
Mongolia
Iraq
Brunei
Colombia
Myanmar
South Korea
Nepal
Sri Lanka
Bahrain
Suriname
North Korea
Jordan
Pakistan
Guyana
Taiwan

Targeted Industries



TOP MITRE ATT&CK TTPS

T1190 Exploit Public-Facing Application

T1588 Obtain Capabilities

T1203 Exploitation for Client Execution

T1059 Command and Scripting Interpreter

T1588.006 Vulnerabilities

T1068 Exploitation for Privilege Escalation

T1588.005 Exploits

T1082 System Information Discovery

T1001 Data Obfuscation

T1547 Boot or Logon Autostart Execution

T1041 Exfiltration Over C2 Channel

T1078 Valid Accounts

T1071 Application Layer Protocol

T1105 Ingress Tool Transfer

T1083 File and Directory Discovery

T1573 Encrypted Channel

T1071.001 Web Protocols

T1027 Obfuscated Files or Information

T1574 Hijack Execution Flow

T1059.001 PowerShell

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cigril	Cigril is a Trojan horse malware that steals sensitive information from infected devices. It can be spread through malicious attachments or links in spam emails.	Spam emails	-
TYPE		IMPACT	AFFECTED PRODUCTS
Trojan		Data Theft, Fraud	-
ASSOCIATED ACTOR			PATCH LINK
Storm-0558			-
IOC TYPE	VALUE		
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Realst	Realst Infostealer is a macOS malware that steals sensitive information, such as passwords, credit card numbers, and cryptocurrency wallets. It is distributed via malicious websites advertising fake blockchain games.	Malicious websites	-
TYPE		IMPACT	AFFECTED PRODUCTS
InfoStealer		Information Theft and System Compromise	MacOS
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	087b3bf372928279d547fb6bb0ab656717fa8c4b, 4e5a59a515981fb97bdb272e3e4acb7118e4e6b2, 0a2a853251fe28333761cc6f9c4518807354dd27, 13bdb3823b8555d846f17bdf381f9568b9a81d26, 29a7eefff22156a72577ed920eaf9b903e9f164a		

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
Fenix	Fenix Botnet is a modular botnet that targets users in Mexico and Chile. It can be used to perform a variety of malicious tasks, such as DDoS attacks, credential theft, and data exfiltration. It is spread through malicious websites and phishing emails.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Botnet		DDoS attacks, credential theft, and data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	B10B9F1F286F7AE29D9E87C5391D3653, 500B1C312163009FEFEC3F8FE7861258, 594804AA21887EE9D7B1B888F482D60C, 1C50C6D0AEAF8071F528B76B1AB242FE, D80F1780BB24E7ECDAB8A262744BCCB7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Decoy Dog	Decoy Dog, a sophisticated malware toolkit uses DNS for C2 communication, evading detection with its wildcard-type behavior and encryption methods. Its origin remains mysterious, and the malware's capabilities surpass traditional RATs like Pupy, making it highly elusive.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Financial loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	4996180b2fa1045aab5d36f46983e91dadeebfd4f765d69fa50eba4edf310acf, ab8e333ef9bc5c5a7d1ed4cab08335861e150b0639d3d0ca4c30b7def5cdccde, ad186df91282cf78394ef3bd60f04d859bcacccbcdcbfb620cc73f19ec0cec64, 6c8f413111f1abfee788dad4ee7cca37e0c2597cca66d155af958c535faf55cc, 0375f4b3fe011b35e6575133539441009d015ebecbee78b578c3ed04e0f22568		

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
Pupy	Pupy RAT is an open-source Remote Access Trojan (RAT) written in Python that is designed to steal sensitive information from infected devices. Pupy RAT is a modular malware, which means that it can be customized to perform a variety of malicious tasks.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Information Theft and Data exfiltration	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten (APT35)			-
IOC TYPE	**VALUE**		
MD5	D069812AA63B631897498621DE353519, 42A5798608F196CE7376CE196F4452FE, F365A8BDFD9B39C4F8B9D99613818207		
IPV4	103[.]79[.]76[.]40		

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-2023-38606		iOS version before: 15.7.1. macOS version: 13.0 22A380 - 13.4.1 22F82, watchOS, tvOS	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:-:*:*:*:*:*:*:*	-
Apple Multiple Products Kernel Unspecified Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-119	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter; T1068:Exploitation for Privilege Escalation	https://support.apple.com/en-us/HT213841; https://support.apple.com/en-us/HT213842; https://support.apple.com/en-us/HT213843; https://support.apple.com/en-us/HT213844; https://support.apple.com/en-us/HT213845; https://support.apple.com/en-us/HT213846; https://support.apple.com/en-us/HT213848

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26077		Atera Agent versions 1.8.3.6 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:atera:agent:1.8.3.x:*:*:*:*:*:*:*	-
Atera Agent Windows Privilege Escalation			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-379	T1404: Exploitation for Privilege Escalation	The vulnerability fixed in ATERA AGENT version 1.8.3.7

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-26078		Atera Agent versions 1.8.3.6 and before	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:atera:agent:1.8.4.x:*:*:*:*:*:*:*	-
Atera Agent Windows Privilege Escalation			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-648	T1211: Exploitation for Defense Evasion	The vulnerability fixed in ATERA AGENT version 1.8.4.9

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35078	✗	Ivanti Endpoint Manager Mobile	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1404: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	The vulnerability was fixed in Ivanti EPMM versions 11.8.1.1, 11.9.1.1, 11.10.0.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-37580	✗	Zimbra Collaboration: 8.8.15 - 8.8.15 Patch 40	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:synacor:zimbra_collaboration:8.8.15:Patch 40:*:*:*:*:*:*:*	-
Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-79	T1190: Exploit Public-Facing Application	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P41; https://wiki.zimbra.com/wiki/Security_Center

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0558	China	Government, Diplomatic entities, Media companies, Think tanks, and Telecommunications	US, Europe, Taiwan, and Uyghur
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Cigril	-
TTPs			
T1059: Command and Scripting Interpreter, T1059.001: PowerShell, T1589.001: Credentials Token , T1134.001: Token Impersonation/Theft, T1134: Access Token Manipulation , T1589: Gather Victim Identity Information, T1059.006: Python , T1505.003: Web Shell, T1505: Server Software Component, T1574.001: DLL Search Order Hijacking, T1574: Hijack Execution Flow, T1003.001: LSASS Memory, T1003: OS Credential Dumping, T1003.002: Security Account Manager, T1078: Valid Accounts , T1102: Web Service, T1567: Exfiltration Over Web Service, T1566: Phishing, T1090: Proxy, T1543.001: Launch Agent , T1543: Create or Modify System Process , T1106: Native API, T1190: Exploit Public-Facing Application			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actor **Storm-0558** and **Cigril, Realst Infostealer, Fenix Botnet, Decoy Dog,** and **Pupy 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 **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Storm-0558** and **Cigril, Realst Infostealer, Fenix Botnet, Decoy Dog,** and **Pupy RAT** in Breach and Attack Simulation(BAS).

Threat Advisories

Storm-0558 Chinese Threat Actor Targets Email Accounts

Apple Tackles Zero-Day Flaws Impacting iPhones and Macs

Atera Addressed Two Zero-Day Vulnerabilities Exploiting MSI Files

Realst Infostealer Hides Behind Phony Blockchain Games

Ivanti Addressed A Critical Zero-Day Flaw in EPMM Software

Fenix Botnet Preys on Mexico and Chile

Unmasking Decoy Dog Malware Toolkit Hiding in DNS Traffic

Zimbra Fixes A Zero-Day Vulnerability Exploited in Attacks

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and 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
Realst Infostealer	SHA1	0eeb66a08ca067f168779be8b22da25f90fe4f51, 88880772b0f8723020e0feb2bb179dc71e482072, 6ee0d99e3a56a72c60f3da790268286cd1e7a3ab, 60a747b3e8a25b885ccd16945ba1a238a66e4439, 8054b51a51c8c8f21fe4c51322ef36a9fa02b570, b8ac89eed011c0a4e5f4973acbee888323ec80f0, efccafe8cf2a7d63f82c69882195a565fbd60720, 39060bb82061c5d426d4a7bad66e07888b05b354, b1aac3888403f4597d9cf14b505f572b2fe7d485, d890822af137df48a91f4ba47a27272dcacc9920, 630b23a57d2d8e6d8e25c346173191af6273c3ab, 087b3bf372928279d547fb6bb0ab656717fa8c4b, 0a2a853251fe28333761cc6f9c4518807354dd27, 13bdb3823b8555d846f17bdf381f9568b9a81d26, 29a7eefff22156a72577ed920eaf9b903e9f164a, 2d89ffbadddd62483bc2be33e296ce4e6036c45b, 4e5a59a515981fb97bdb272e3e4acb7118e4e6b2, 9719fd9415d438722f94877c55c9495708c64fee, c205d4ba044f2d69500f10a46c31aaf068e32c44, c716a02e3bc8603fcf0bb8d63fc4f7e3afab471d, dadfbd13b7bd0e9b6d87ebae30bc48c2eeae0eb3, 09e8672af5e18ce99ad8ae608cdc0fa229f121f0, 112b5637c8cbb7d2e216d89f969515809e1dc66d, 154909cdd261130b0ed6d603d4727cb9f15ddc36, 247c50d19e7ad18f466558f9c1785ef29962ab7c, 32f06e3e9d8899f5224f3d5538724d132bda0921, 68dc1f80064f6c261e587cdbb2f01677c8f2e14a, 8b4cdd02330cf25f4e1d338b91ffd1c1dd87021a,

Attack Name	TYPE	VALUE
Realst Infostealer	SHA1	ce42d202446cc6b316f668a072c17df87dcd495c, 2f61ddd391d23a6665fa326629e004cb380c4f85, 38ae4fa8f4fec9ab98c0003c455016464b62acce, 65c175f5fad31ea1c938a96a9cdc9987413fd1f2, 80483c5c95ed92da6f086e9497cd08cf7d3b7658, c4296e1a67545e50f44c3776adb674ea1d4d4c0e, d436de35164a045e3c0f7b51cf41fcefedf7e77d, f097123a1999a656a368114abbd848b68d523ee0, 158cf7a0c89544ce1c3294453be2a8c8ced9c9b0, 294392bcf166953c552443fe95ba1e8f15487f74, 294bfc9b97092904bb5e216531b184e38fb2c11f, 3685fdd3d14b500fd73f0a3d16dafcc028035204, 4053e0ecf5f59b6f7afc06750551d77e131ebd2d, 410e4e24f6f6c4f29c8a75723f84bf60ff96c2d5, ada7a47b7fecb142ff532c6e0f01a89bcb47afc9, bfac1b17ad79719c4602a2142435f02c529ec4ab, db9fe7ba9ff8771d28a2fa504d84059faab6be5b
Fenix Botnet	IPV4	207.210.228[.]67, 139.162.73[.]58, 80.66.64[.]154
	File Names	SII_Seguro_XXXXXX.zip, Herramienta Seguridad SII.url, AT_herramienta_XXXXXX.zip, SAT_Herramienta_Seguridad.jse, 7684jasdtg.xls, ot.crypt, proxy.crypt, steal.crypt, pay.txt
	MD5	b10b9f1f286f7ae29d9e87c5391d3653, 500b1c312163009fefec3f8fe7861258, 594804aa21887ee9d7b1b888f482d60c, 1c50c6d0aeaf8071f528b76b1ab242fe, d80f1780bb24e7ecdab8a262744bccb7, 1be0606640d645ddbfb2fbdff53ca918, 7631660bdcf74b95b5806328a7668cab, eaff13d6c89ce0e2a7632bd811045c35, ea68e0cc90a88315526704bae1ca8b4a, b262b36c3b09ebeab66c95e121be4c73, 6f0b4018da4aa0887b5aa879ce315543, 7fe97d4e29e17f39e343a9ef5fde03ca

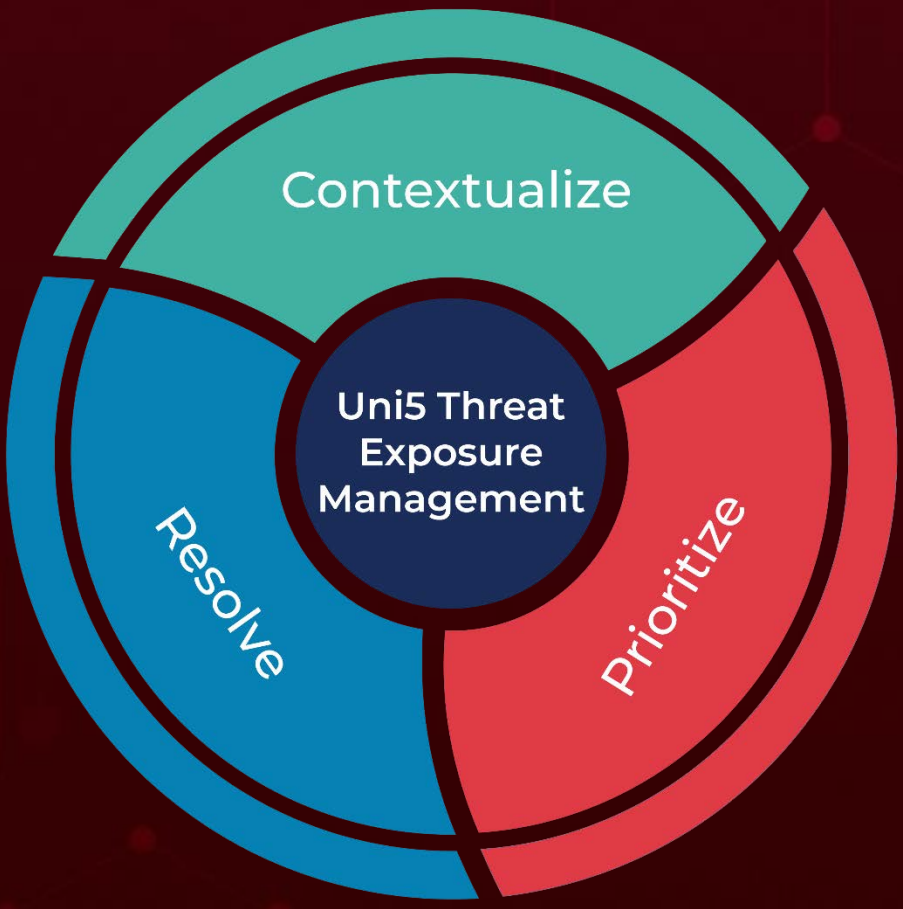
Attack Name	TYPE	VALUE
Fenix Botnet	URLs	file[:]\\139[.]162[.]73[.]58@80\SuECWRPQ\SAT_Herramienta_Seguridad[.]jse, file[:]\\139[.]162[.]73[.]58@80\YtmpEoBw\Herramienta_de_Seguridad_SII[.]jse, hxxps[:]//fja[.]com[.]mx/wp-contents/execution[.]php?tag=russian, hxxps[:]//fja[.]com[.]mx/wp-contents/init[.]php?id=1, hxxps[:]//www[.]grafoce[.]com/scripts/index[.]php?id=2, hxxps[:]//www[.]grafoce[.]com/wp-contents/execution[.]php?tag=russian, hxxps[:]//russiancl[.]top/bramx/7684jasdtg[.]xls, hxxps[:]//russiancl[.]top/bramx/post[.]php, hxxps[:]//russiancl[.]top/bramx/ot[.]crypt, hxxps[:]//russiancl[.]top/bramx/proxy[.]crypt, hxxps[:]//russiancl[.]top/bramx/steal[.]crypt
	Domains	2repuvegobmx[.]com.mx, annydesk.website, citasatmx2023[.]lat, citas-sat2023[.]com.mx, citas-satmx[.]com, citas-sregob-mexico[.]com, consultacurp-gobmx[.]com.mx, consultacurp-gobmx[.]com[.]mx, fja[.]com[.]mx, grafoce[.]com, lbci-seguro[.]com, mexico-curp[.]com, russiancl[.]top, siii-chile[.]com, sre-curpmexico[.]com, tramites-sat[.]com.mx, whatsapp.website
Pupy	MD5	D069812AA63B631897498621DE353519, 42A5798608F196CE7376CE196F4452FE, F365A8BDFD9B39C4F8B9D99613818207
	IPV4	103[.]79[.]76[.]40

Attack Name	TYPE	VALUE
Decoy Dog	Domains	ads-tm-glb[.]click, allowlisted[.]net, atlas-upd[.]com, cbox4[.]ignorelist[.]com, claudfront[.]net, hsdps[.]cc, j2update[.]cc, maxpatrol[.]net, nsdps[.]cc, rcmsf100[.]net
	IPV4	13[.]248[.]169[.]48, 156[.]154[.]132[.]200, 194[.]31[.]55[.]85, 5[.]199[.]173[.]4, 5[.]252[.]176[.]63, 5[.]252[.]176[.]22, 5[.]252[.]179[.]18, 67[.]220[.]81[.]190, 69[.]65[.]50[.]194, 69[.]65[.]50[.]223, 70[.]39[.]97[.]253, 83[.]166[.]240[.]52
	SHA256	4996180b2fa1045aab5d36f46983e91dadeebfd4f765d69fa50eba4edf310acf, ab8e333ef9bc5c5a7d1ed4cab08335861e150b0639d3d0ca4c30b7def5cdccde, ad186df91282cf78394ef3bd60f04d859bcacccbcdcbfb620cc73f19ec0cec64, 6c8f413111f1abfee788dad4ee7cca37e0c2597cca66d155af958c535faf55cc, 0375f4b3fe011b35e6575133539441009d015ebecbee78b578c3ed04e0f22568, 6c8f413111f1abfee788dad4ee7cca37e0c2597cca66d155af958c535faf55cc
	Telfhash	t1fde0f101c9395f39ecd16430b41041a59107c73c904087309fb8d0e8d87e0077129f3f

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

July 31, 2023 . 6:40 AM

More at www.hivepro.com