Date of Publication
July 17 , 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

10 to 16 JULY 2023

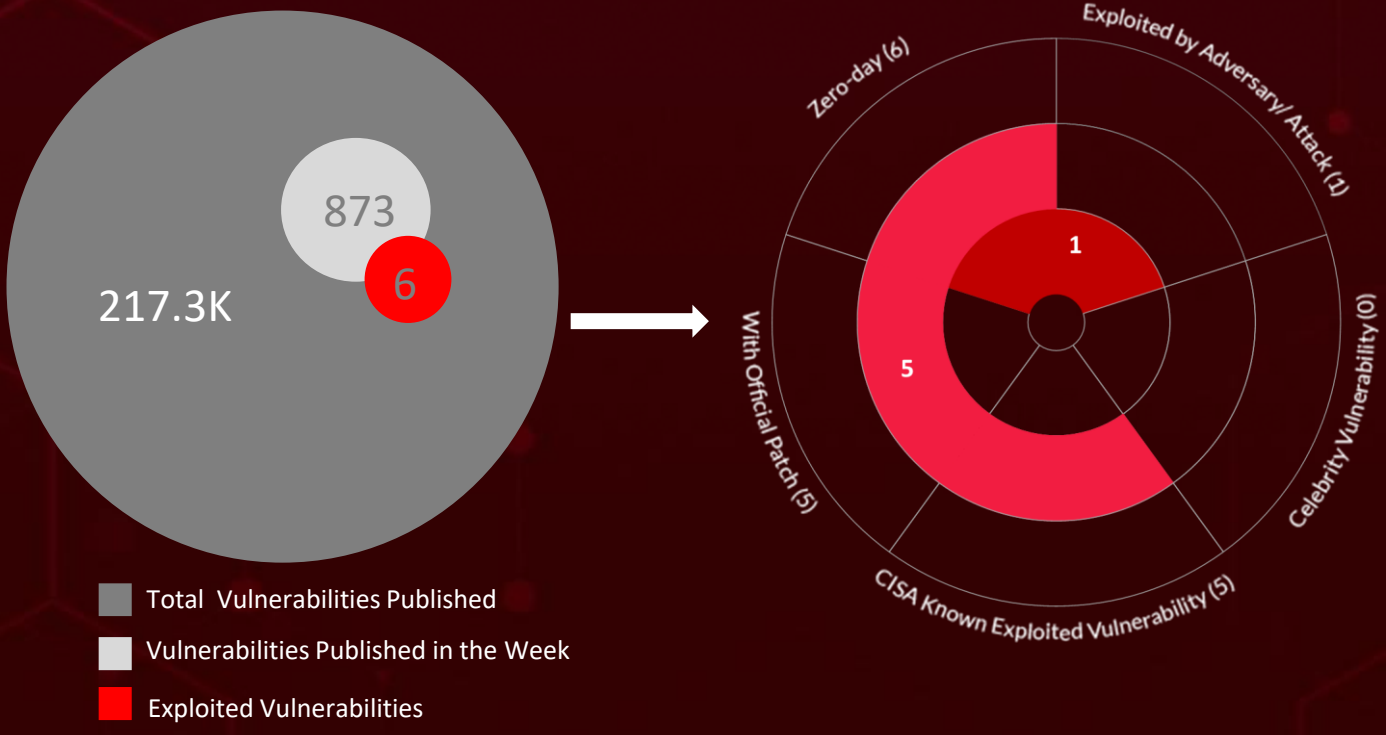
Table Of Contents

Summary

HiveForceLabs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of six attacks executed, total six **zero-day** vulnerabilities out of which **Five** vulnerabilities were found in multiple Microsoft products, and **two** different adversaries highlights the ever-present danger of cyber attacks.

Moreover, HiveForceLabs also discovered that **TA445** employed four malware, in its recent attack targeting Ukraine and Poland. Furthermore, we identified a new **Big Head Ransomware** with several variants.

Meanwhile, the **TOITOIN malware** campaign, targeting businesses in the LATAM region, employs sophisticated techniques and multi-stage infection chains. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

6
Attacks Executed

6
Vulnerabilities Exploited

2
Adversaries in Action

- Big Head Ransomware
- TOITOIN Trojan
- PyLoose
- RomCom
- PicassoLoader
- CustomerLoader

- CVE-2023-37450
- CVE-2023-36874
- CVE-2023-32049
- CVE-2023-32046
- CVE-2023-36884
- CVE-2023-35311

- Storm-0978
- TA445

Insights

PyLoose

A new Python based fileless malware targets cloud workloads

MS Patch Tuesday

Addressed 5 zero-day vulnerabilities as part of July 2023

TOITOIN Malware

Targeting businesses in the LATAM region

TA445

conducts ongoing campaigns targeting government entities, military, and civilians in Ukraine and Poland

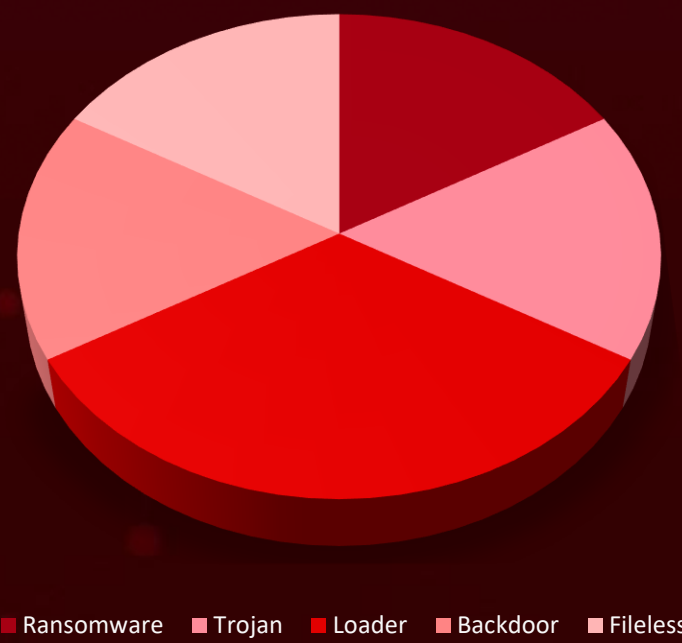
CVE-2023-37450

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

Storm-0978

Threat Actor is actively exploiting unpatched office zero-day vulnerablity

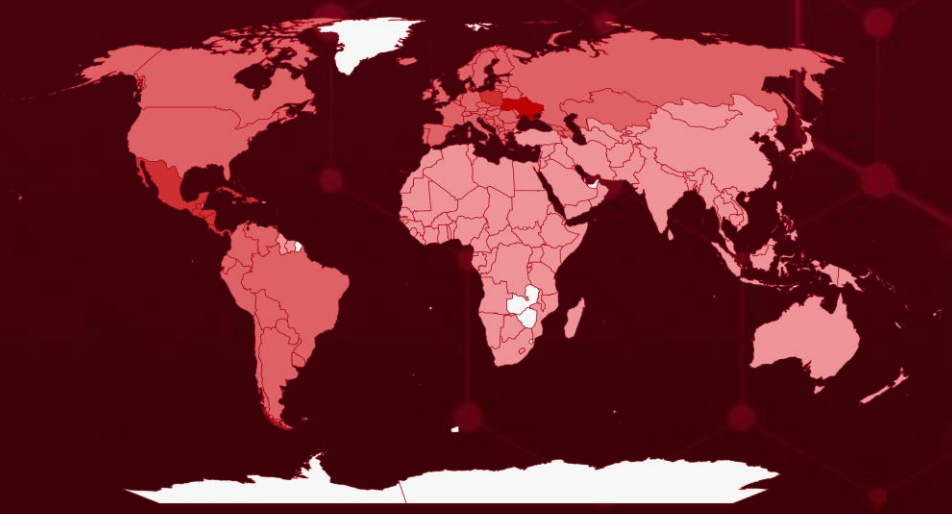
Threat Distribution



Targeted Countries

Most

Least



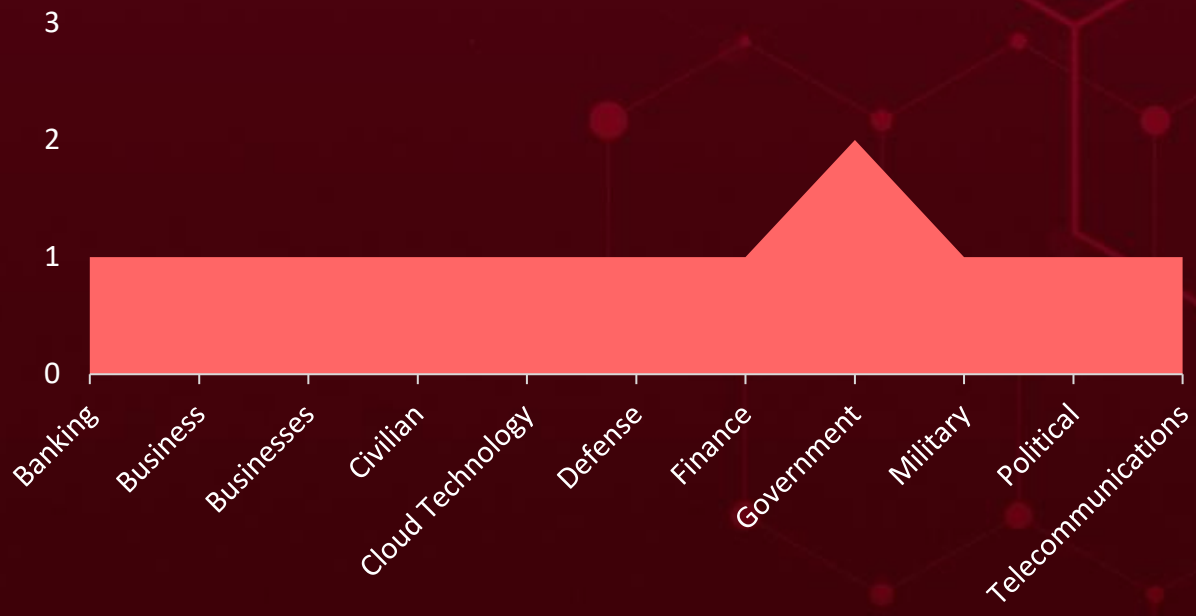
Countries
Ukraine
Mexico
Panama
Costa Rica
Haiti
Cuba
Nicaragua
Dominican Republic
Poland
El Salvador
Guatemala
Honduras
Switzerland
Barbados
Azerbaijan
Bolivia
Saint Lucia
Bosnia and Herzegovina
Liechtenstein
Brazil
Netherlands
Bulgaria

Countries
Portugal
Canada
Slovakia
Chile
Belize
Colombia
Luxembourg
Albania
Monaco
Croatia
North Macedonia
Andorra
Peru
Cyprus
Russia
Czech Republic
San Marino
Denmark
Spain
Dominica
Belgium
Antigua and Barbuda
Kosovo
Ecuador
Lithuania

Countries
Malta
Estonia
Moldova
Argentina
Finland
Montenegro
France
Bahamas
Georgia
Norway
Germany
Paraguay
Greece
Belarus
Grenada
Romania
Armenia
Saint Kitts and Nevis
Austria
Saint Vincent and the Grenadines
Venezuela
Serbia
Hungary
Slovenia

Countries
Iceland
Sweden
Ireland
Trinidad and Tobago
Uruguay
Jamaica
Kazakhstan
Latvia
Italy

Targeted Industries



TOP MITRE ATT&CK TTPS

T1071 Application Layer Protocol

T1204 User Execution

T1203 Exploitation for Client Execution

T1027 Obfuscated Files or Information

T1566 Phishing

T1059 Command and Scripting Interpreter

T1140 Deobfuscate/ Decode Files or Information

T1082 System Information Discovery

T1547 Boot or Logon Autostart Execution

T1562 Impair Defenses

T1562.001 Disable or Modify Tools

T1486 Data Encrypted for Impact

T1490 Inhibit System Recovery

T1105 Ingress Tool Transfer

T1036 Masquerading

T1057 Process Discovery

T1071.001 Web Protocols

T1190 Exploit Public-Facing Application

T1027.002 Software Packing

T1132.001 Standard Encoding

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Big Head Ransomware	Big Head ransomware is a new ransomware and its variants suggest a shared source, distributed through deceptive Windows updates and Word installer disguises.	Spear-Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438, 2a36d1be9330a77f0bc0f7fdc0e903ddd99fcee0b9c93cb69d2f0773f0afd254, 39caec2f2e9fda6e6a7ce8f22e29e1c77c8f1b4bde80c91f6f78cc819f031756, b8e456861a5fb452bcf08d7b37277972a4a06b0a928d57c5ec30afa101d77ead, ff900b9224fde97889d37b81855a976cddf64be50af280e04ce53c587d978840		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TOITOIN Trojan	TOITOIN malware campaign, targeting businesses in the LATAM region, employs sophisticated techniques and multi-stage infection chains with numerous malware samples disguised as compressed ZIP archives hosted on Amazon EC2.	Spear-Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Information Theft and System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	8fc3c83b88a3c65a749b27f8439a8416, 2fa7c647c626901321f5decde4273633, b7bc67f2ef833212f25ef58887d5035a, 690bfd65c2738e7c1c42ca8050634166, e6c7d8d5683f338ca5c40aad462263a6		

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
PyLoose	A new fileless malware called PyLoose targets cloud workloads by loading an XMRig Miner directly into memory using Python code and the memfd technique.	Exploitation	-
TYPE		IMPACT	AFFECTED PRODUCTS
Fileless		Cryptomining	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	25232290fa9fa5529240a4e893ce206dfdcfc28d0b3a1b89389f7270f1046822, 935ee206846223e6d2db3f62d05101c0bea741e7b43e1b73c1eb008f947d5ff1		
SHA1	d422493b47e4798717f2b05a482c97ef9e6b74b9, eba82ed21b329b0955ab87b2397a949628349b3f		
MD5	059f83f8969b09c29c95b17452718ea3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RomCom	The RomCom backdoor is a notorious malware, that is distributed through phishing campaigns and disguised as well-known software, allowing unauthorized access to compromised systems.	Phishing	CVE-2023-36884
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor		Espionage and Unauthorized access	Office and Windows
ASSOCIATED ACTOR			Mitigation LINK
Storm-0978			https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884
IOC TYPE	VALUE		
SHA256	419bc8196013d7d8c72b060da1a02d202d7e3eb441101f7bcb6d7667871a5c16, 5c2fb1c42f007093be5e463f70ee7e7192990b3385a3cbcc71043980efa312e0, 6a0017262def9565b504d04318c59f55bea136ac3dd48862d1ae90ff6b963811, b557bf11d82d3d64d028a87584657d25dba0480295ed08447f10c7a579dee048, b3984a2de76eee3ad20c4b13e0c0cbbab2dd6db65e3f6ca34418e79c21cf5c39,		

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
PicassoLoader	PicassoLoader is a downloader malware identified in ongoing cyberattacks targeting Ukraine and Poland. It serves as a conduit for deploying subsequent payloads like Cobalt Strike beacons and njRAT, aimed at stealing information and establishing remote access.	Malicious Microsoft Office documents	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Stealing information and establishing remote access	-
ASSOCIATED ACTOR			PATCH LINK
TA445			-
IOC TYPE	VALUE		
SHA256	f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d, 6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a, a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6, 1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac, 0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CustomerLoader	A covert .NET loader, known as CustomerLoader, was specifically designed to facilitate the retrieval, deciphering, and activation of subsequent payloads.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Malware propagation	-
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	c05c7ec4570bfc44e87f6e6efc83643b47a378bb088c53da4c5ecf7b93194dc6, b8f5519f7d66e7940e92f49c9f5f0cac0ae12cc9c9072c5308475bd5d093cdca, 3fb66e93d12abd992e94244ac7464474d0ff9156811a76a29a76dec0aa910f82		
URLs	hxxp://5.42.94[.]169/customer/735, hxxp://5.42.94[.]169/customer/770		

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-2023-37450	✗	Apple Safari up to 16.5.2 Apple iOS and iPadOS up to 16.5.1 Apple macOS up to 13.4.1.	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:safari:16.5.0:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:16.5.1:*:*:*:*:*:*:* cpe:2.3:a:apple:safari:16.5.2:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:16.5.0:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:16.5.1:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:16.5.0:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os:13.4.0:*:*:*:*:*:*:* cpe:2.3:o:apple:mac_os:13.4.1:*:*:*:*:*:*:*	-
Apple WebKit Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1595- Active Scanning, T1595.002- Vulnerability Scanning, T1068- Exploitation for Privilege- Escalation, T1190- Exploit Public-Facing- Application, T1136- Create Account, T1078- Valid Accounts	https://support.apple.com/en-gb/HT213826; https://support.apple.com/en-gb/HT213823; https://support.apple.com/en-gb/HT213825

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36874	✗	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 Windows Error Reporting Service Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1404: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32049	✗	Windows: 10 - 11 22H2 Windows Server: 2016 - 2022 20H2	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-254	T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32046	✗	Windows: 10 - 11 22H2 Windows Server: 2008 - 2022 20H2 Microsoft Internet Explorer: 11 - 11.1790.17763.0	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	-
Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-119	T1404: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046

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	Storm-0978 (aka DEV-0978, RomCom)
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:o:microsoft:windows:10:1809:*:*:*:*:*:*	RomCom Backdoor
Office and Windows HTML Remote Code Execution Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**Mitigation DETAILS**
	CWE-20	T1203: Exploitation for Client Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-35311		Microsoft Office: 2013 - 2019 Microsoft Outlook: 2013 -2016 Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:microsoft:microsoft_office:2019:*:*:*:*:*:*:*	-
Microsoft Outlook Security Feature Bypass Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH DETAILS**
	CWE-254	T1211: Exploitation for Defense Evasion	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0978 (aka DEV-0978, RomCom)	Russia	Finance, Telecommunications, Political, Defense, and Government	Europe, North America, and Ukraine
	MOTIVE		
	Espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-36884	RomCom Backdoor	Office and Windows
TTPs			
T1566: Phishing; T1204: User Execution; T1082: System Information Discovery; T1217: Browser Information Discovery; T1083: File and Directory Discovery; T1070: Indicator Removal; T1534: Internal Spearphishing; T1550: Use Alternate Authentication Material; T1486: Data Encrypted for Impact; T1490: Inhibit System Recovery; T1071: Application Layer Protocol; T1005: Data from Local System			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
TA445 (Operation Ghostwriter, UNC1151, UAC-0051, PUSHCHA, DEV-0257, Storm-0257)</td><td>Belarus</td><td rowspan="3">Government, Military, Business, Civilian</td><td rowspan="3">Ukraine and Poland</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Sabotage and destruction</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>PicassoLoader, AgentTesla, Cobalt Strike Beacon and njRAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1574: Hijack Execution Flow; T1140: Deobfuscate/Decode Files or Information; T1574.001: DLL Search Order Hijacking; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1059.005: Visual Basic; T1059: Command and Scripting Interpreter; T1564: Hide Artifacts; T1036: Masquerading; T1027: Obfuscated Files or Information; T1218.010: Regsvr32; T1218: System Binary Proxy Execution; T1218.011: Rundll32</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **one exploited vulnerability** and block the indicators related to the threat actor **Storm-0978, TA445** and **Big Head Ransomware, TOITOIN Trojan, PyLoose, RomCom, PicassoLoader,** and **CustomerLoader** 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 **one exploited vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Storm-0978, TA445** and **Big Head Ransomware, TOITOIN Trojan, PyLoose, RomCom, PicassoLoader,** and **CustomerLoader** in Breach and Attack Simulation(BAS).

Threat Advisories

Unveiling New Big Head Ransomware Variants and Their Stealthy Tactics

Apple Addresses A Zero-Day Vulnerability Which Is Actively Exploited in Wild

The Unrelenting Nature of TOITOIN Malware

Exploit found in the wild for Critical VMware Aria Operations Bug

Microsoft's July 2023 Patch Tuesday Addresses 5 Zero-day Vulnerabilities

New Python-Based Fileless Malware Named 'PyLoose' Targeting Cloud Environments

Storm-0978 actively exploited the unpatched Office zero-day

TA445 Targeting Government and Military Sectors in Ukraine and Poland

CustomerLoader Disseminating Diverse Malware Payloads

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
Big Head Ransomware	SHA256	6d27c1b457a34ce9edfb4060d9e04eb44d021a7b03223ee72ca569c8c4215438, 2a36d1be9330a77f0bc0f7fdc0e903ddd99fcee0b9c93cb69d2f0773f0afd254, 39caec2f2e9fda6e6a7ce8f22e29e1c77c8f1b4bde80c91f6f78cc819f031756, b8e456861a5fb452bcf08d7b37277972a4a06b0a928d57c5ec30afa101d77ead, ff900b9224fde97889d37b81855a976cddf64be50af280e04ce53c587d978840, 980bac6c9afe8efc9c6fe459a5f77213b0d8524eb00de82437288eb96138b9a2, f354148b5f0eab5af22e8152438468ae8976db84c65415d3f4a469b35e31710f, f59c45b71eb62326d74e83a87f821603bf277465863bfc9c1dcb38a97b0b359d, 40e5050b894cb70c93260645bf9804f50580050eb131e24f30cb91eec9ad1a6e, 64aac04ffb290a23ab9f537b1143a4556e6893d9ff7685a11c2c0931d978a931, 64246b9455d76a094376b04a2584d16771cd6164db72287492078719a0c749ab, 627b920845683bd7303d33946ff52fb2ea595208452285457aa5ccd9c01c3b0a, 037f9434e83919506544aa04fecd7f56446a7cc65ee03ac0a11570cf4f607853, 0dbfd3479cfaf0856eb8a75f0ad4fccb5fd6bd17164bcfa6a5a386ed7378958d,

Attack Name	TYPE	VALUE
Big Head Ransomware	SHA256	159fbb0d04c1a77d434ce3810d1e2c659fda0a5703c9d06f89ee8dc556783614, 1942aac761bc2e21cf303e987ef2a7740a33c388af28ba57787f10b1804ea38e, 1ada91cb860cd3318adbb4b6fd097d31ad39c2718b16c136c16407762251c5db, 1c8bc3890f3f202e459fb87acec4602955697eef3b08c93c15ebb0facb019845, 226bec8acd653ea9f4b7ea4eaa75703696863841853f488b0b7d892a6be3832a, 40d11a20bd5ca039a15a0de0b1cb83814fa9b1d102585db114bba4c5895a8a44, 603fcc53fd7848cd300dad85bef9a6b80acaa7984aa9cb9217cdd012ff1ce5f0, 6698f8ffb7ba04c2496634ff69b0a3de9537716cfc8f76d1cfea419dbd880c94, 66bb57338bec9110839dc9a83f85b05362ab53686ff7b864d302a217cafb7531, 6b3bf710cf4a0806b2c5eaa26d2d91ca57575248ff0298f6dee7180456f37d2e, 6b771983142c7fa72ce209df8423460189c14ec635d6235bf60386317357428a, 806f64fda529d92c16fac02e9ddaf468a8cc6cbc710dc0f3be55aec01ed65235, 9a7889147fa53311ba7ec8166c785f7a935c35eba4a877c1313a8d2e80e3230d, 9aa38796e0ce4866cff8763b026272eb568fa79d8a147f7d61824752ad6d8f09, 9c1c527a826d16419009a1b7797ed20990b9a04344da9c32deea00378a6eeee2, bcf8464d042171d7ecaada848b5403b6a810a91f7fd8f298b611e94fa7250463, be6416218e2b1a879e33e0517bcacaefccab6ad2f511de07eebd88821027f92d, cf9410565f8a06af92d65e118bd2dbaeb146d7e51de2c35ba84b47cfa8e4f53b, dcfa0fca8c1dd710b4f40784d286c39e5d07b87700bdc87a48659c0426ec6cb6,
TOITOIN Trojan	MD5	8fc3c83b88a3c65a749b27f8439a8416, 2fa7c647c626901321f5decde4273633, b7bc67f2ef833212f25ef58887d5035a, 690bfd65c2738e7c1c42ca8050634166, e6c7d8d5683f338ca5c40aad462263a6, c35d55b8b0ddd01aa4796d1616c09a46, 7871f9a0b4b9c413a8c7085983ec9a72

Attack Name	TYPE	VALUE
TOITOIN Trojan	URLs	ec2-3-89-143-150[.]compute-1[.]amazonaws[.]com/storage[.]php?e=Desktop-PC, ec2-3-82-104-156[.]compute-1[.]amazonaws[.]com/storage.php?e=Desktop-PC, http[:]//alemaoautopecas[.]com, http[:]//contatosclientes[.]services, http[:]//cartolabrasil[.]com, http[:]//bragancasbrasil[.]com, http[:]//afroblack[.]shop/CasaMoveis\ClienteD.php
	Domains	atendimento-arquivos[.]com, arquivosclientes[.]online, fantasiacinematica[.]online
	IPv4	91[.]252[.]203[.]222, 179[.]188[.]38[.]7
PyLoose	SHA1	d422493b47e4798717f2b05a482c97ef9e6b74b9, eba82ed21b329b0955ab87b2397a949628349b3f
	SHA256	25232290fa9fa5529240a4e893ce206dfdcfc28d0b3a1b89389f7270f1046822, 935ee206846223e6d2db3f62d05101c0bea741e7b43e1b73c1eb008f947d5ff1
	MD5	059f83f8969b09c29c95b17452718ea3, fec5b820594579f1088db47583d2c62d
	IPv4:PORT	51[.]75[.]64[.]249[:]20128
	DNS	gulf[.]moneroocean[.]stream, Pool[.]sabu-sabu[.]ml, pool[.]xiao[.]my[.]id
	Monero wallet address	85DS3ShGZwtFffeQUrDK8Db12qwCcaCHofNcZdjMkjTCfWiRv9WLe4cR2W97eGnRXwBxDhTK7BbbE2Z7t4gjXRz1VLPmhn7
RomCom	SHA256	d4a847fa9c4c7130a852a2e197b205493170a8b44426d9ec481fc4b285a92666, a61b2eafcf39715031357df6b01e85e0d1ea2e8ee1dfec241b114e18f7a1163f, e7cfeb023c3160a7366f209a16a6f6ea5a0bc9a3ddc16c6cba758114dfe6b539, d3263cc3eff826431c2016aee674c7e3e5329bebfb7a145907de39a279859f4a, 3a3138c5add59d2172ad33bc6761f2f82ba344f3d03a2269c623f22c1a35df97
	SHA1	fb4ad5d21f0d8c6755eb4addba0ac288bd2574b6
	MD5	059175be5681a633190cd9631e2975f6

Attack Name	TYPE	VALUE
PicassoLoader	SHA256	f11310f075171f8502bcd32dcb2fe5894808b17a37f6fd960fb26653871e7b7d, 6b310bd23806272f6c69b84a0381915f16d705e79ce423f19de940247543c76a, a7b7691baa21ad118348661a035b69605a6efd1cd1fa0fd52e5645c64f5f61e6, 1a0e930fbdab2266e14dc501abdbb5623b5762d687df3670d86bb05f252509ac, 0397c586fa56e672db7f14afa8c19992b6e08ab0c1d282c960df1af26371bd72, ce96fe99ebe30ae44e74c22c0b2a055005d0da131e0082a1c290ddeb79dd1114, 5039d76e697f242c36c5a0ebf7dec127757bc34ddaf33c58251c2798da3ce03e, a58da0e6a20fed03364a0cbae18008eb4f8d6bee7c9f5e8ffcdac34fb823d363, 7e35ce60d80c85e050133de142a3b261160259846c9c967c7b2bb84923328f8c, 27a061daee3ec9cff928b8152159a472797821834a3aa7639749489b90f703c3, c7ec4570524ad59d5bd7a3e8f0d23c8cf05cc0e8a98dcdbec00c9dc075084558, aea76f905b0169e4289895a8d85980896f802fd18fe246a27d601310bfa5905e, 7a9a5317a88afb53b44f6cfed59c48907f63aaa7ef63b1587f990951c423c211, 0f189246247c51a701d5a88a06e1fc4932f333d24d7ff40dc8152ad6224f6ca4, 41f050f3d003edd67ec02710c60a7b4022685465cb61ae37fc0b3193c1dab5cb, 1c118d8fb0be904b129e4552f86cd0b3e239ecd25f4d599c54cc96c1096747af, e41b3bdbfb816d5cfd4b235d2b985894153c41da6726ebfa83e45f3b5b4a1945, 6e6f5bebd6bf0fd0b626d6521cdb4faa06275f558bacd419c76702e2728f734c, dd61887d5cdf361a335fec917cd6d1bb186aad56b1f9f5d09b66355ff7f41751, 40b87c5444e03b6b4f3d38315c1525cedfafc20355fff84502cc594799dc41df, d3f012662c44293ae07d8c763914db18fc9795673da7c1cdc4d862b1a7c887b9, f00939201f7e77221e94e917a8e34c3d2143324e02fdf35058526d870a0023a0, 71c0881d35f769fe58c084883d2aaee9ec284fcdc04500e5e5272973dfc78944,

Attack Name	TYPE	VALUE
PicassoLoader	SHA256	00030b0db567afa524eb68faf6f194f25bc5361c380599668a82dbae12af088e, a7a7c4062ced46275638719c100ea2397c673148e8473e56a3ec4313ca7dc5f9, 4d9cca1d75d4691e794dfe9efb9eef6e9e64b4e978ad17831b459d4bb6722829, 4da99f963c26bcc4537ba0437c9cc1445be8bea64067d34308dda6c2e49c8c65, 4cedec3e1a2f72a917ad9a59ebe116ed50c3268567946d1e493c8163486b888b, df33b1187c20582560ffaa1c3e86b92003c4a7c8a61acbbe886ab195531c5c89, bec98a8a5e6786ef415a7a7bf7e60cbd384d43ede4e882aa560fdcb24865ac55, 00fdb03518c238dc649a39e94f0bcc95dacf3b832979d14d0ed5194b9b482b87, 991a19fb00cda372dd1ce4a42580dc40872da5c5bfbb34301615f3870ea3fb58, 2c5ba56a41f40bac2f21065fb9883545ef8d359883cb7bc351c481cb9542e104, 44fd895174a7c1c0019fc95bb04201106dc165704c70e902e3de58db98f03c7e, 30d46a740e2677c8fee383c2a4762561a10c66c5b99215262e42bfabf6bfb1aa, 924d3589d642e8fd65746dc156ff9f104d43114a04ea9509f51ee6a439d1915b, ecafe10f0f7d6a9ae94d9735b45f88492b6ea11ff58f37e62fbf7070778af20a, bc92a5b1c4205ea1fbfec9144b8aab485e095142c7105c9d616b089ec668f198, ea5a8f1052e40cb6bcebf384fe67a6920b3651fbd8f3a34a844f39789ebc4d5f, ad8e3ebd496fb4d97e5075adb4f2f1b91195cca059800d0acd182a07698c13b6, 3670115fa5fac918ad0dafe399568788690f0f205dd0bebe4f55180fd70d36e9, 5969180b072703709764d1ca40be3eeb40f2eb0090859b3743cc21b884fa2106, a5fb6b9417e50bd2260afdcdb5a9eed33e48a283a51408344a4caa2b1025b9a7, c0c455cd3e18be14d2e34cf4e3fb98e7ab0a75ef04b6049ff9f7b306d62704b8, 0f3bdbc64446555c6ff611b02f2e64250fcaf39b78237ae4cca7c74d94731b32, 35d1e819d2ac2535f0aa9e2294570135f37519386872c415e326146e931b8fb9,

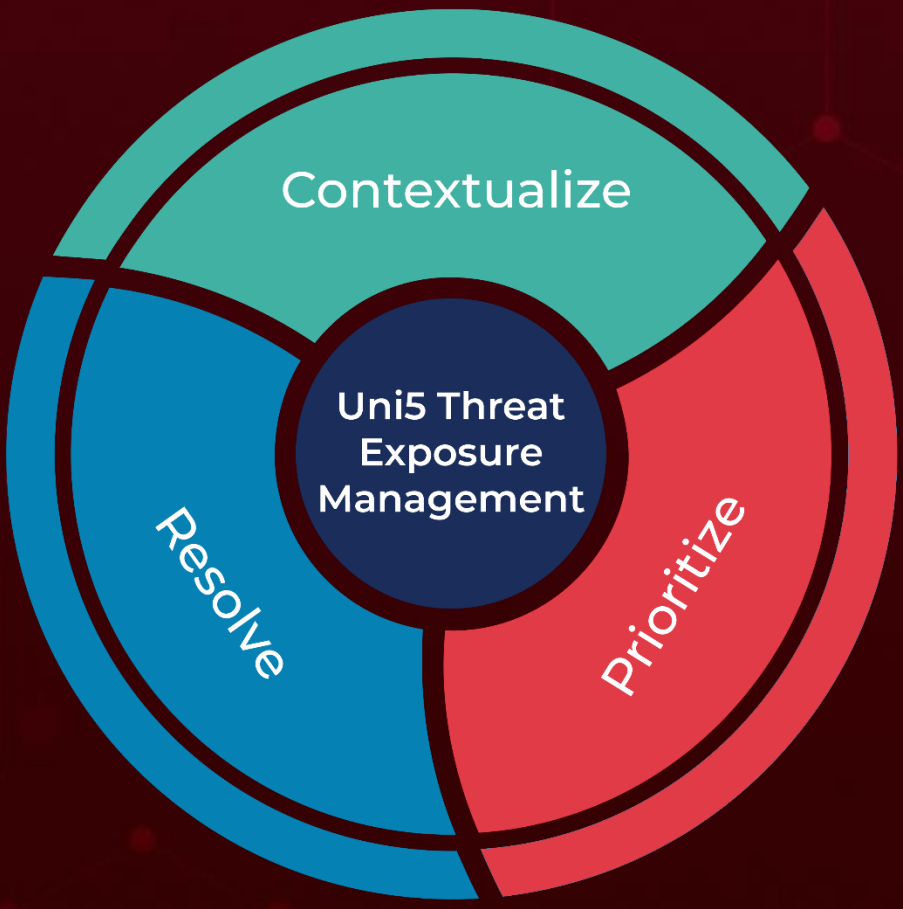
Attack Name	TYPE	VALUE
PicassoLoader	SHA256	5a4bd78a4d3d1a772e9e9b14983646a4c1c6a25cc983b804e4522774ebfa1c14, c40e6b176ad3fd7332cd217191e557352ef4b82bf91f29939121267598737990, e9bbe7c6705a6f5a78c2a9b8060a7e32374b81058f7c2f24851c4d1ea38d7411, 73a21c1492996794688d9751edd1e5c287da645fa7a960e945bb4ea69855424a, 7893965d1861c712b751bc2d5fb53a34ec0d276bcf389b7fc574728940575152
	Host Name	everything-everywhere.at.ply[.]gg
	IPv4	94.131.108[.]109
	URLs	hxxps[://]wuzhenfestival[.]site/5109c46d40f801a862c96e628f83faca[.]png, hxxps[://]onyangdol[.]site/thumb_d_F3D14F4982A256B5CDAE9BD579429AE7[.]jpg, hxxps[://]kebhana[.]site/Believe-Me-Lyrics[.]jpg, hxxps[://]wordrow[.]website/pictures-91[.]jpg, hxxps[://]ellechina[.]online/01_logo_HLW-300x168[.]jpg, hxxps[://]sellmyhousequickly[.]website/dangjiansigeyishibiaoyuxuanchuanguahua[.]jpg, hxxps[://]frivol[.]space/memnet-profiles/A10818[.]jpg, hxxps[://]wordrow[.]website/pictures-91[.]jpg, hxxps[://]simplifymedia[.]pw/images/bnd/news/23908t5[.]png, hxxps[://]hssenglish[.]pw/fonini/pundit/leaf_background[.]jpg, hxxps[://]mingxing[.]pw/content/_processed_/f/a/_742fa0bbd1[.]jpg, hxxps[://]mingxing[.]pw/datastream/thumb_b/43950sec[.]jpg, hxxps[://]carpetmarker[.]pw/images/Carpet_Shop_3b09adf[.]jpg, hxxps[://]bourns[.]space/p/covers/assets/images/lee-leopard[.]jpg
CustomerLoader	URLs	hxxp://smartmaster.com[.]my/48E003A01/48E003A01.7z, hxxp://5.42.94[.]169/customer/735, hxxps://telegra[.]ph/Full-Version-06-03-2, hxxps://tinyurl[.]com/bdz2uchr, hxxps://www.mediafire[.]com/file/nnamjnckj7h80xz/v2.4_2023.rar/file, hxxps://www.mediafire[.]com/file/lgoql94feiic0x7/v2.5_2023.rar/file, hxxp://5.42.94[.]169/customer/770,

Attack Name	TYPE	VALUE
CustomerLoader	URLs	hxxps://slackmessenger[.]site/, hxxps://slackmessenger[.]pw/slack.zip, hxxp://5.42.94[.]169/customer/798
	SHA256	d40af29bbc4ff1ea1827871711e5bfa3470d59723dd8ea29d2b19f5239e509e9, 3fb66e93d12abd992e94244ac7464474d0ff9156811a76a29a76dec0aa910f82, 65e3b326ace2ec3121f17da6f94291fdaf13fa3900dc8d997fbbf05365dd518f, 7ff5a77d6f6b5f1801277d941047757fa6fec7070d7d4a8813173476e9965ffc, c05c7ec4570bfc44e87f6e6efc83643b47a378bb088c53da4c5ecf7b93194dc6, 695f138dd517ded4dd6fcd57761902a5bcc9dd1da53482e94d70ceb720092ae6, b8f5519f7d66e7940e92f49c9f5f0cac0ae12cc9c9072c5308475bd5d093cdca
	IPv4	45.9.74[.]99, 5.42.65[.]69
	C2	missunno[.]com:80

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 17, 2023 . 8:40 AM

More at www.hivepro.com