Date of Publication
August 21, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

14 to 20 AUGUST 2023

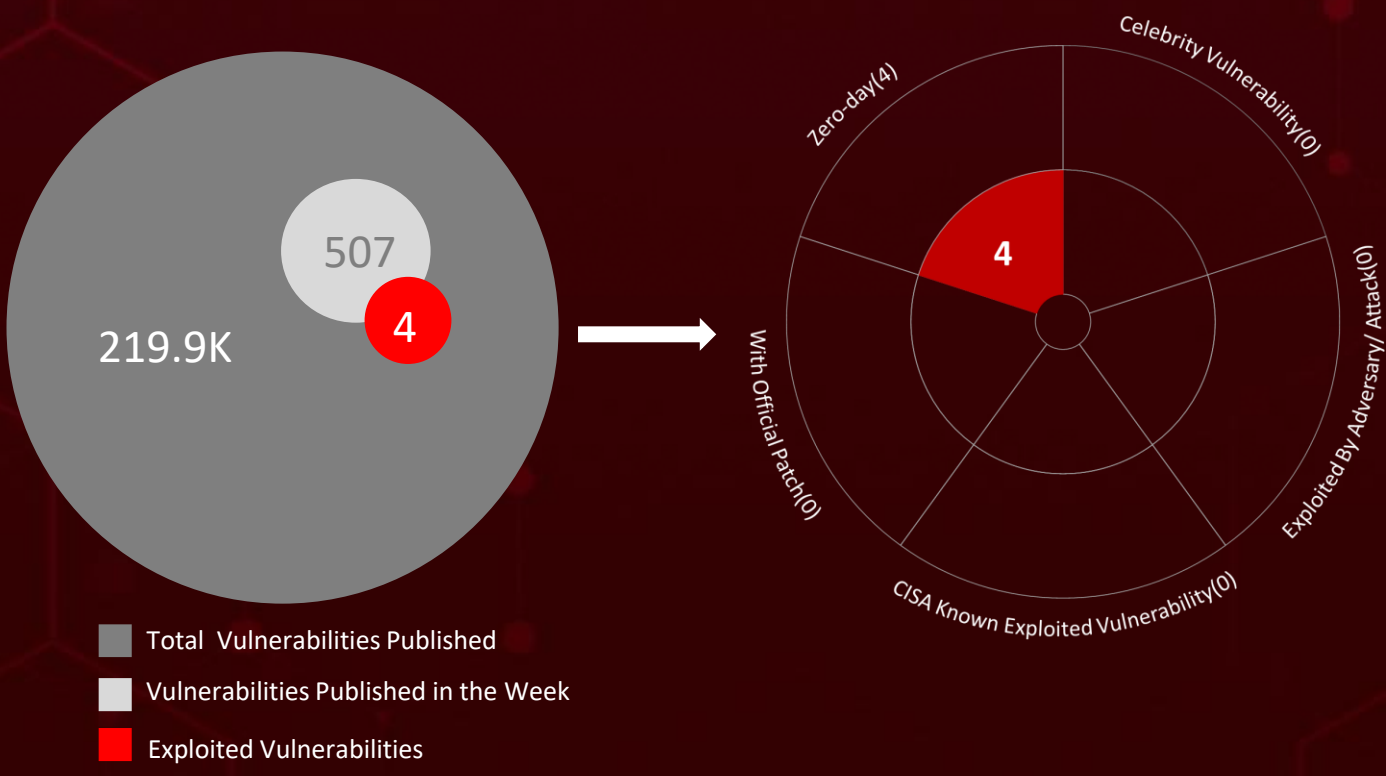
Table Of Contents

Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **eight** executed attacks, **one** instance of adversary activity, and **four** zero-day vulnerabilities. All of these are Tunnelcrack vulnerabilities that affect most VPN products, highlighting the ever-present danger of cyber attacks.

Furthermore, HiveForce Labs uncovered a new Linux version of the **Monti Ransomware** that employs distinct tactics for encryption and virtual machine termination. This version is targeting government and legal sectors.

Meanwhile, **Bronze Starlight**, a China-based threat actor, is currently focusing its efforts on the Southeast Asian gambling industry with the objective of deploying Cobalt Strike beacons on compromised systems. These observed attacks have been on the rise, posing a significant threat to users worldwide.



High Level Statistics

8
Attacks Executed

4
Vulnerabilities Exploited

1
Adversaries in Action

- LummaC Stealer
- Amadey Bot
- SectopRAT
- Monti Ransomware
- JanelaRAT
- BX RAT
- AdLoad
- HUI Loader

- CVE-2023-35838
- CVE-2023-36673
- CVE-2023-36672
- CVE-2023-36671

- Bronze Starlight

Insights

JanelaRAT, a financial malware, is directed towards users in Latin America (LATAM) with the ability to seize sensitive data.

Monti Ransomware

A new Linux variant using distinct tactics for encryption and virtual machine termination

Tunnelcrack

vulnerabilities are a set of four vulnerabilities that affect most VPN products

AdLoad

malware persists on Mac systems with a new proxy application payload, converting infected devices into a proxy botnet

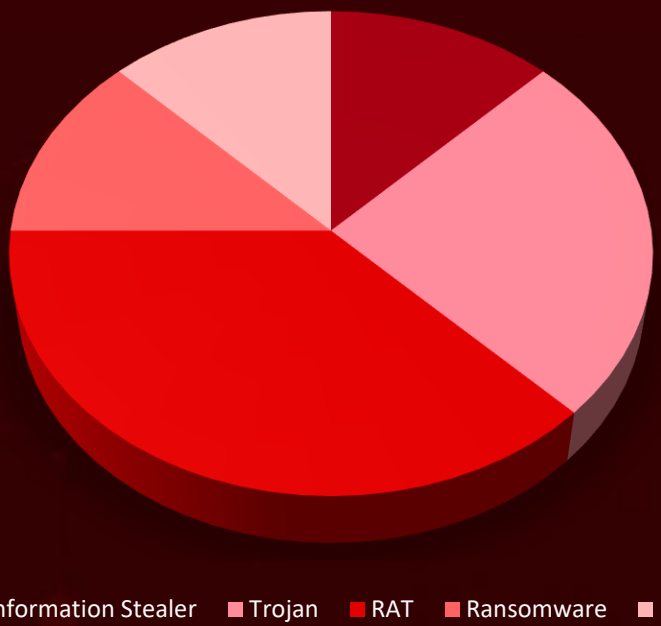
Bronze Starlight

China-based actor targeting Southeast Asian gambling industry with the objective of deploying Cobalt Strike beacons on compromised systems

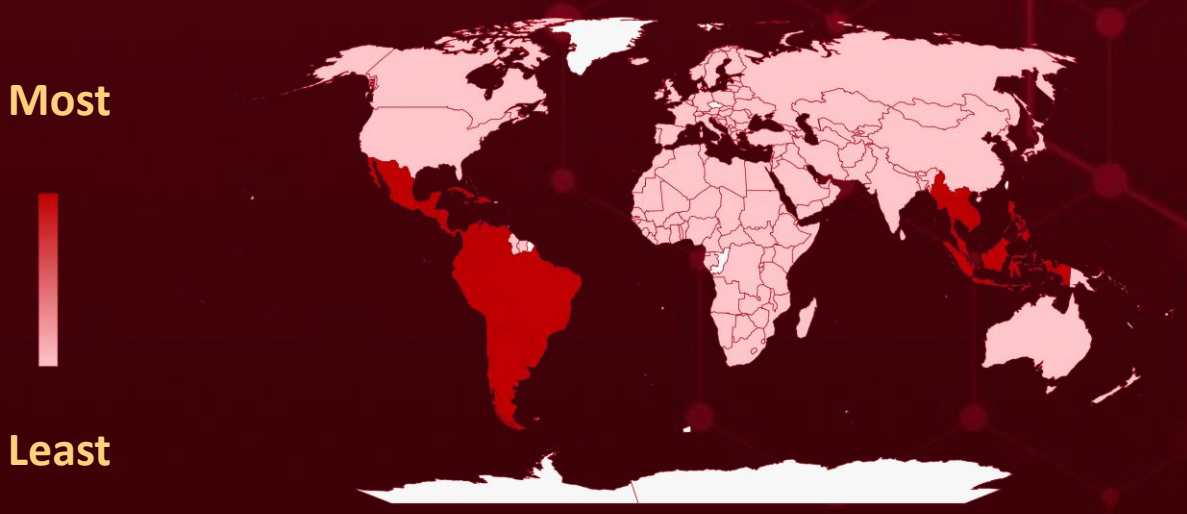
SectopRAT

A new method for spreading SectopRAT has emerged. This approach involves using the Amadey bot, obtained from the LummaC stealer, to distribute the SectopRAT payload.

Threat Distribution



Targeted Countries



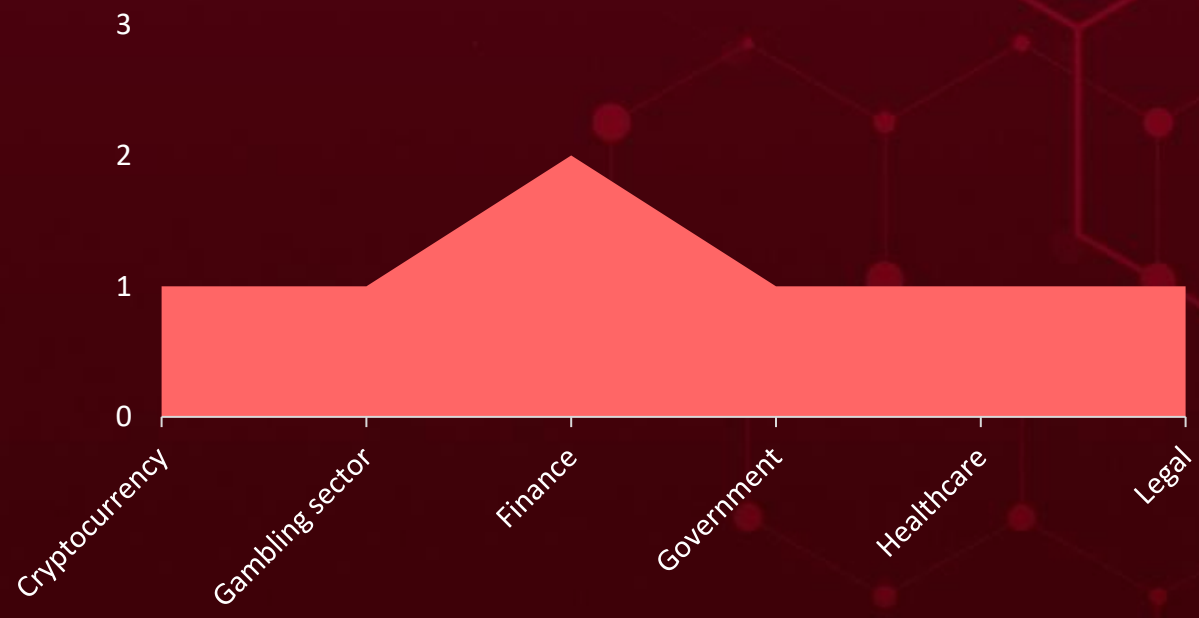
Countries
Timor-Leste
Myanmar
Laos
Argentina
Peru
Belize
Indonesia
Bolivia
Malaysia
Brazil
Panama
Brunei
Singapore
Cambodia
Honduras
Chile
Jamaica
Colombia
Vietnam
Costa Rica
Mexico
Cuba

Countries
Nicaragua
Dominican Republic
Paraguay
Ecuador
Philippines
El Salvador
Thailand
Guatemala
Uruguay
Haiti
Venezuela
South Korea
North Macedonia
Moldova
Armenia
Saint Kitts & Nevis
China
Tonga
Australia
Nauru
Comoros
Burundi
Congo
Seychelles

Countries
Austria
Sweden
Côte d'Ivoire
United Arab Emirates
Croatia
Morocco
Azerbaijan
Antigua and Barbuda
Cyprus
Palau
Czech Republic (Czechia)
Qatar
Denmark
Sao Tome & Principe
Djibouti
Slovenia
Dominica
St. Vincent & Grenadines
Bahamas
Tanzania
DR Congo

Countries
Turkmenistan
Bahrain
Uzbekistan
Egypt
Mongolia
Bangladesh
Angola
Equatorial Guinea
Netherlands
Spain
Germany
Sudan
Ghana
Syria
Greece
Canada
Grenada
Tunisia
Barbados
Uganda
Guinea
United States
Guinea-Bissau
Micronesia

Targeted Industries



TOP MITRE ATT&CK TTPS

T1140 Deobfuscate/ Decode Files or Information	**T1573** Encrypted Channel	**T1497** Virtualization/ Sandbox Evasion	**T1083** File and Directory Discovery	**T1027** Obfuscated Files or Information
T1059 Command and Scripting Interpreter	**T1547** Boot or Logon Autostart Execution	**T1588.005** Exploits	**T1071** Application Layer Protocol	**T1059.001** PowerShell
T1486 Data Encrypted for Impact	**T1203** Exploitation for Client Execution	**T1005** Data from Local System	**T1070.004** File Deletion	**T1547.001** Registry Run Keys / Startup Folder
T1566 Phishing	**T1588** Obtain Capabilities	**T1012** Query Registry	**T1105** Ingress Tool Transfer	**T1057** Process Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LummaC Stealer	LummaC Stealer is a malware that steals sensitive information from infected devices. It is distributed through a Malware-as-a-Service (MaaS) model on Russian-speaking forums. The malware is written in C language and is constantly being updated with new features.	Malware-as-a-Service	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1deecd4e2aeae42cba		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Amadey Bot	Amadey Bot is a modular Trojan malware that steals sensitive information and can download other malware. It can be customized to perform a variety of tasks.	Phishing emails, exploit kits, and drive-by downloads	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Theft, Malicious Downloads	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d		
URLs	hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp://enfantfoundation[.]com/amday[.]exe		

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
SectopRAT	SectopRAT is a remote access trojan (RAT) that is used to steal sensitive information from infected devices. It is a .NET-based malware that is first compiled in November 2019. It can steal a variety of data, including browser history, cookies, and cryptocurrency wallet information.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	a3ceda3ef0a7b72145124def334dd3fa337614a1170960826016996151188fc5, 033cafb9fcd3d50d858164c117ee2a1c9e7fe95b4d027315bc9d1186e655d583, 81f4e0d6a70f14c3e07241196bd7f5318e302c28c64ca4bb876f4e25fbc3e5d2, ffd45c2b562d30113cb9a4823025a9a162503017e9d81fd96ddb5b98e5bb89bd, 501444c9d25c15ca62bafe062b6bb8a3b3f69f0ca13aff057e3b8b1a0595f3a4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Monti	Monti ransomware, resembling Conti, resurfaces after a break, targeting legal and government sectors. A new Linux variant diverges significantly, using distinct tactics for encryption and virtual machine termination.	Phishing emails	CVE-2021-44228 (Log4Shell)
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data and Financial loss	VMware Horizon
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.vmware.com/security/advisories/VMSA-2021-0028.html
IOC TYPE	**VALUE**		
SHA1	F1c0054bc76e8753d4331a881cdf9156dd8b812a, a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef		
URLs	hxxp://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid[.]onion, hxxp://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid[.]onion		

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
BX RAT	BX RAT is a remote access trojan (RAT) that was first discovered in 2014. It is a modular malware, meaning that it can be customized to perform a variety of tasks. BX RAT is primarily used to steal sensitive information from infected devices	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Steal	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA1	be7e5282efe58018b462a5ba0a78a7f01108460d		
MD5	7e4592e02951be844a2ee603d75070a6		
SHA256	c6b3f1648f7137df91606f6aaaa6d25d672e18c8adcb178c6d8cdcf3148a3c81		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
JanelaRAT	JanelaRAT is a remote access trojan (RAT) that is targeting users in Latin America (LATAM). It is a heavily modified variant of BX RAT, which was first discovered in 2014. JanelaRAT can steal a variety of sensitive information from infected devices.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data steal	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	99bf0fba15aa3a9a59cbf442a80364e5, 999a9af2cd20a8c4bcf652e3523aafa3, 8b83e6b2d891cdf9250e9afd17081eab, E56d8632db98b07d2b49423f7dd64b42, C2f4cb0da89b4ea86ab5369a942428be		

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
AdLoad	AdLoad malware persists on Mac systems with a new proxy application payload, converting infected devices into a proxy botnet. This scheme, involving thousands of IP addresses, points to a monetization strategy by a company offering proxy services, emphasizing the evolving nature of cyber threats.	Phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Data Steal, system damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b, 956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472, 6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc, 3d063efde737b7b2e393926358cbb32469b76395e1a05e8c127a12e47550f264, 2d595880cfb1691dd43de02d1a90273919f62311a7668ef078709eff2fd6bd87		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HUI Loader	HUI Loader is a malware loader that is used to download and install other malware on infected devices. It is distributed through a variety of methods. Once HUI Loader is installed on a victim's computer, it will download and install other malware.	Phishing emails, Malvertising	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data steal, compromise system	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	8502852561fcb867d9cbf45ac24c5985fa195432b542dbf8753d5f3d7175b120, 62fea3942e884855283faf3fb68f41be747c5baa922d140509237c2d7bacdd17		
SHA1	a75e9b702a892cc3e531e158ab2e4206b939f379, 64f5044709efc77230484cec8a0d784947056022		
MD5	b16bb2f910f21e2d4f6e2aa1a1ea0d8b		

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-2023-35838		WireGuard Client 0.5.3 on Windows	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:wireguard:client:0.5.3:*	-
WireGuard Client Denial of Service Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1498: Network Denial of Service	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36673		Avira Phantom VPN through 2.23.1 for macOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:avira:phantom_vpn:*	-
Avira Phantom VPN DNS Spoofing Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1498: Network Denial of Service, T1566: Phishing	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36672	✗	Clario VPN client through 5.9.1.1662 for macOS	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:clario:vpn_client:*	-
Clario VPN Plaintext Traffic Leakage Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1562: Impair Defenses	-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-36671	✗	Clario VPN client through 5.9.1.1662 for macOS	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:clario:vpn_client:*	-
Clario VPN Traffic to The Real IP Address of The VPN Server Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-200	T1562: Impair Defenses	-

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Bronze Starlight (aka DEV-0401, Cinnamon Tempest, SLIME34, Emperor Dragonfly)	China	Gambling sector	Southeast Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Windows, Linux, macOS
TTPs			
T1053:Scheduled Task/Job, T1129:Shared Modules, T1574:Hijack Execution Flow, T1574.002:DLL Side-Loading, T1027:Obfuscated Files or Information, T1027.002:Software Packing, T1036:Masquerading, T1070.006:Timestomp, T1140:Deobfuscate/Decode Files or Information, T1497:Virtualization/Sandbox Evasion, T1562.001:Disable or Modify Tools, T1010:Application Window Discovery, T1012:Query Registry, T1057:Process Discovery, T1083:File and Directory Discovery, T1560:Archive Collected Data, T1071:Application Layer Protocol, T1095:Non-Application Layer Protocol, T1573:Encrypted Channel, T1018:Remote System Discovery, T1082:System Information Discovery			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **four exploited vulnerabilities** and block the indicators related to the threat actor **Bronze Starlight** and **LummaC Stealer, Amadey Bot, SectopRAT, Monti Ransomware, JanelaRAT, BX RAT, AdLoad, and HUI Loader** 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 **four exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Bronze Starlight** and **LummaC Stealer, Amadey Bot, SectopRAT, Monti Ransomware, JanelaRAT, BX RAT, AdLoad, and HUI Loader** in Breach and Attack Simulation(BAS).

Threat Advisories

LummaC Stealer Enlists Amadey Bot to Unleash SectopRAT

Unveiling The TunnelCrack VPN Vulnerabilities

Monti Ransomware's New Linux Variant Enhanced Encryption

JanelaRAT Strikes at Latin American Financial Sector

AdLoad Malware Persists on Mac Systems with New Proxy Payload

Decoding Bronze Starlight's Strategy in the Gambling Sector

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
LummaC Stealer	MD5	507bddfabd74a3d024b2ad5f67d666ea
	SHA1	78eac92e0040e033406e6786b58b8a367fe171fa
	SHA256	f85d8adf012c96a63fcb989b8b0e71894b12b769ce78f6a62064a4002954b144, ca21c5b129c001c2b51359d5f74c0a99667028810623b779190b13f0de86369e, 929f7b467d96d8d9c73bfa9b8adf758c1b3993c9438f23368c69e1201beea622, 515ab212127cc722326043d77dda60943145798bfe8b17178937a254989367f1, 0d8dee5e24500219f037e673324479f22cc5649c2aafdfe47b35375b6b76e60b, e0ac5909e219d4527691ea695185313376a0ccb075907b1decd4e2aeae42cba, 9252e999b76b9628ad0942df2649e1203ca078d1b45dab6a8f1ede3e22b99625, 51cb8641ed75c5037fa657ed2aa33c71350e01f5f949054f17582ca41c260280, f819a1d2234c2755a8dc844f89e765de56c1c927f3964a1453961cec4fd38bae
	URL	hxxp[:]//exitlife[.]xyz/c2sock
Amadey Bot	MD5	952d825a264745bb52b6977ba5983568
	SHA1	627a0a841c2fe194dd54f9ec6b0c1231d7da135f
	SHA256	d35d55bb74a7cf4349e2fa4a92839e2a88f17a1fee9725801d0d97b2bf0d311c,

Attack Name	TYPE	VALUE
Amadey Bot	SHA256	0539d46a6e61dd3ce32a4b41c0554f925f4b26054c49451accec7ccad0409846, 2c256a4a1ac022bcd3784d19e66934056015e20b49d58238ce4f3dfb37bfd98d
	URLS	hxxp[:]//africatechs[.]com/Amdaygo[.]exe, hxxp[:]//45[.]9[.]74[.]182/b7djSDcPcZ/index[.]php, hxxp://enfantfoundation[.]com/amday[.]exe
SectopRAT	MD5	F290ed868caae994bbfae1b63aca1d28
	SHA1	5ac7b60e56281dc0c72f7c1125b165867df56ed9
	SHA256	501444c9d25c15ca62bafe062b6bb8a3b3f69f0ca13aff057e3b8b1a0595f3a4, a3ceda3ef0a7b72145124def334dd3fa337614a1170960826016996151188fc5, 033cafb9fcd3d50d858164c117ee2a1c9e7fe95b4d027315bc9d1186e655d583, 81f4e0d6a70f14c3e07241196bd7f5318e302c28c64ca4bb876f4e25fbc3e5d2, ffd45c2b562d30113cb9a4823025a9a162503017e9d81fd96ddb5b98e5bb89bd, 501444c9d25c15ca62bafe062b6bb8a3b3f69f0ca13aff057e3b8b1a0595f3a4, fb553e12381d42a612c713968078424201794a35fd13c681ae7faa77bf18e553, 641710df66c792439f85b79879a268caa17b78ea0bf6924369fa6131fda01cd5
	URLs	hxxp[:]//patriciabono[.]com/BRR[.]exe, hxxp://fuji-iasi[.]ro/BRR[.]exe, hxxps://earthqik[.]co[.]za/BR[.]exe, hxxp://silversoft[.]in/BR[.]exe, hxxp://tbmcoats[.]com/BRRR[.]exe, hxxp://aviangas[.]co[.]ke/BRRRRAS[.]exe
	IP:PORT	95[.]143[.]190[.]57:15648
Monti Ransomware	SHA1	f1c0054bc76e8753d4331a881cdf9156dd8b812a, a0c9dd3f3e3d0e2cd5d1da06b3aac019cdbc74ef
	URLs	hxxp://monti5o7lvyrpyk26lqofnfvajtyqruwatlfaazgm3zskt3xiktudwid[.]onion, hxxp://mblogci3rudehaagbryjznltdp33ojwzkq6hn2pckvjq33rycmzczpid[.]onion
JanelaRAT	Domains	cnt-blackrock[.]geekgalaxy[.]com, aigodmoney009[.]access[.]ly, freelascdmx979[.]couchpotatofries[.]org, 439mdxmex[.]damnserver[.]com,

Attack Name	TYPE	VALUE
JanelaRAT	Domains	897midasgold[.]ddns[.]me, disrupmoney979[.]ditchyourip[.]com, kakarotomx[.]dnsfor[.]me, skigoldmex[.]dvrcam[.]info, i89bydzi[.]dynns[.]com, infintymexbrock[.]geekgalaxy[.]com, brockmex57[.]golffan[.]us, j1d3c3mex[.]homesecuritypc[.]com, myfunbmdablo99[.]hosthampster[.]com, irocketxmtm[.]hopto[.]me, hotdiamond777[.]loginto[.]me, imrpc7987bm[.]mmafan[.]biz, dmrpc77bm[.]myactivedirectory[.]com, jxjmrpc797bm[.]mydissent[.]net, askmrpc747bm[.]mymediapc[.]net, myinfintyme09[.]geekgalaxy[.]com, infintymex747[.]geekgalaxy[.]com, infintymexb[.]geekgalaxy[.]com, jinfintymexbr[.]geekgalaxy[.]com, minfintymexbr[.]geekgalaxy[.]com, cinfintymex[.]geekgalaxy[.]com, 9mdxmex[.]damnserver[.]com, ikmidasgold[.]ddns[.]me, rexsrupmoney979[.]ditchyourip[.]com, kktkarotomx[.]dnsfor[.]me, megaskigoldmex[.]dvrcam[.]info, izt89bydzi[.]dynns[.]com, zeedinfintymexbrock[.]geekgalaxy[.]com
	IPv4	191.96.224[.]215, 192.99.169[.]240, 191.96.79[.]24, 167.88.168[.]132, 102.165.46[.]28, 189.89.15[.]37
	MD5	99bf0fba15aa3a9a59cbf442a80364e5, 999a9af2cd20a8c4bcf652e3523aafa3, 8b83e6b2d891cdf9250e9afd17081eab, e56d8632db98b07d2b49423f7dd64b42, c2f4cb0da89b4ea86ab5369a942428eb, 897e8483b673db70fdc5d3d111600cac, 72c02b3181c763d0e67f060e91635a97, c39f75423862c1525f089a5e966b9d04, e841f4691e5107fe360b1528384a96f0, 526a0b2d142567d8078e24ab0758fad7
BX RAT	MD5	7e4592e02951be844a2ee603d75070a6

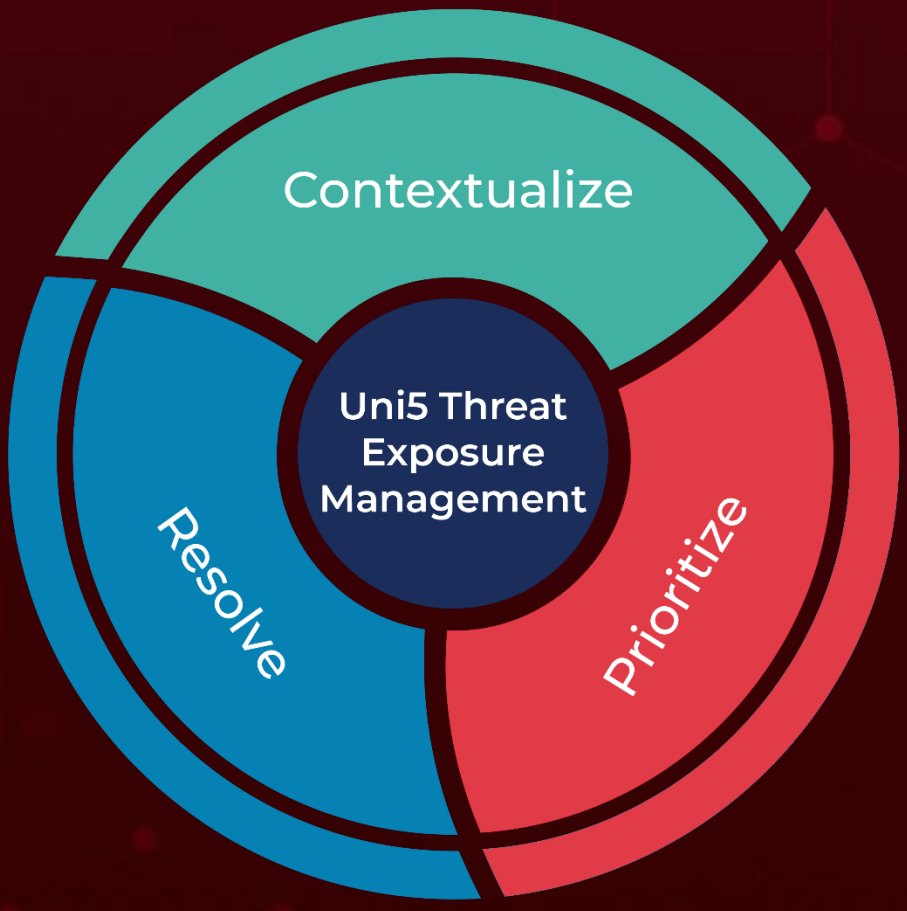
Attack Name	TYPE	VALUE
BX RAT	SHA1	be7e5282efe58018b462a5ba0a78a7f01108460d
	SHA256	c6b3f1648f7137df91606f6aaaa6d25d672e18c8adcb178c6d8cdcf3148a3c81
AdLoad	SHA256	d94f62ec4b6ffcec35d5e639d02a52ce226629a5eb3e2a7190174ea8d3b40b5b, 956aae546af632ea20123bfe659d57e0d5134e39cdb5489bd6f1ba5d8bbd0472, 6587e61a8a7edb312da5798ffccf4a5ef227d3834389993b4df3ef0b173443dc, 3d063efde737b7b2e393926358cbb32469b76395e1a05e8c127a12e47550f264, 2d595880cfb1691dd43de02d1a90273919f62311a7668ef078709eff2fd6bd87, 7cb10a70fd25645a708c81f44bb1de2b6de39d583ae3a71df0913917ad1dffc3, 4a7c9829590e1230a448dd7a4272b9fbfbafccf7043441967c2f68f6082dde32, 68b6beb70bd547b75f2d36d70ca49f8b18542874480d39e33b09ee69eb1048b3, 1904b705105db4550371d678f8161826b98b1a9fca139fa41628214ed816d2f5, 2fb1d8e6454f43522f42675dcf415569e5df5d731e1d1390f793c282cce4a7aa, ee9ebdb1d9a7424cd64905d39820b343c5f76e29c9cd60c0cdd3bfe069fb7d51, c7721ab85bad163576c166a0a71c0dbe4cc491dda68c5a5907fd1d8cac50780d
	URLs	hxxp://m.skilledobject[.]com/a/rep, hxxp://m.browseractivity[.]com/a/rep, hxxp://m.enchantedreign[.]com/a/rep, hxxp://m.activitycache[.]com/a/rep, hxxp://m.activityinput[.]com/a/rep, hxxp://m.opticalupdater[.]com/a/rep, hxxp://m.connectioncache[.]com/a/rep, hxxp://m.analyzerstate[.]com/a/rep, hxxp://m.essencecuration[.]com/a/rep, hxxp://m.microrotator[.]com/a/rep, hxxp://m.articlesagile[.]com/a/rep, hxxp://m.progresshandler[.]com/a/rep, hxxp://m.originalrotator[.]com/a/rep, hxxp://m.productiveunit[.]com/a/rep, hxxp://api.toolenviroment[.]com/l, hxxp://api.inetfield[.]com/l, hxxp://api.operativeeng[.]com/l, hxxp://api.launchertasks[.]com/l,

Attack Name	TYPE	VALUE
AdLoad	URLs	hxxp://api.launchelemnt[.]com/l, hxxp://api.validexplorer[.]com/l, hxxp://api.majorsprint[.]com/l, hxxp://api.essentialenumerator[.]com/l, hxxp://api.transactioneng[.]com/l, hxxp://api.macreationsapp[.]com/l, hxxp://api.commondevice[.]com/l, hxxp://api.compellingagent[.]com/l, hxxp://api.lookupindex[.]com/l, hxxp://api.practicalsync[.]com/l, hxxp://api.accessiblelist[.]com/l, hxxp://api.functionconfig[.]com/l
HUI Loader	MD5	b16bb2f910f21e2d4f6e2aa1a1ea0d8b, 809fcab1225981e87060033d72edaeaf
	SH1	a75e9b702a892cc3e531e158ab2e4206b939f379, 64f5044709efc77230484cec8a0d784947056022
	SHA256	8502852561fcb867d9cbf45ac24c5985fa195432 b542dbf8753d5f3d7175b120, 62fea3942e884855283faf3fb68f41be747c5baa 922d140509237c2d7bacdd17

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 21, 2023 • 9:30 AM

More at www.hivepro.com