Date of Publication
August 7, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

31 JULY to 6 AUGUST 2023

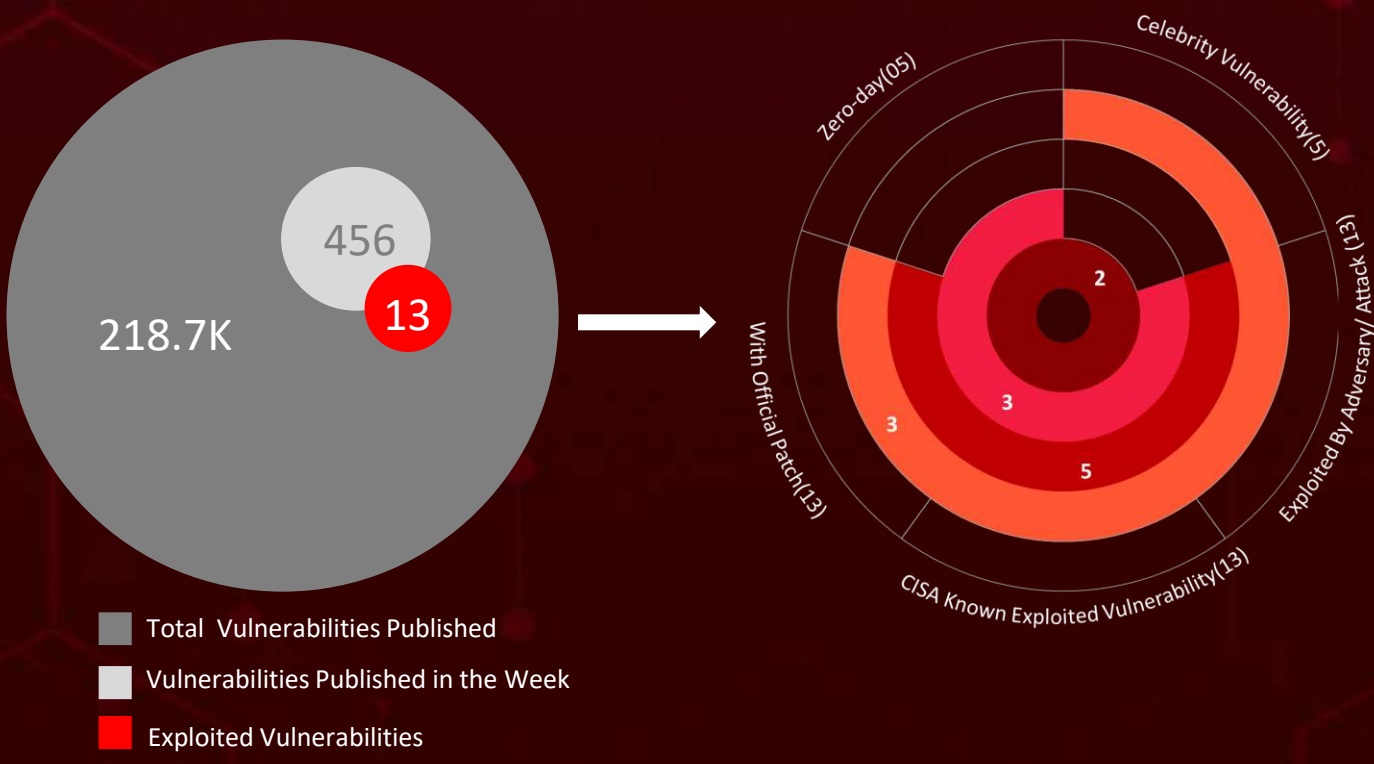
Table Of Contents

Summary

HiveForceLabs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **one** executed attack, **one** instance of adversary activity, and **thirteen** vulnerabilities, including **five zero-day** vulnerabilities. Among these, a widely exploited vulnerability was found in the **Ivanti** EPMM, highlighting the ever-present danger of cyber attacks.

Furthermore, HiveForceLabs uncovered a new version of the **Rilide Stealer** malware that adeptly evades Chrome's security measures to target Chromium-based browsers.

Meanwhile, **APT 29**, a Russia-based threat actor, employs targeted social engineering via Microsoft Teams to steal credentials. This involves leveraging compromised domains and convincing users to enter authentication codes, furthering their espionage objectives. All these observed attacks have been on the rise, posing a significant threat to users worldwide.



High Level Statistics

1
Attacks Executed

13
Vulnerabilities Exploited

1
Adversaries in Action

- Rilide Stealer

- CVE-2023-35081
- CVE-2018-13379
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-34523
- CVE-2021-40539
- CVE-2021-26084
- CVE-2021-44228
- CVE-2022-22954
- CVE-2022-22960
- CVE-2022-1388
- CVE-2022-30190
- CVE-2022-26134

- APT 29

Insights

Rilide Stealer

New version targets Chromium-based browsers in campaigns that exploit user trust through fake plugins

CVE-2023-35081

Second zero-day vulnerability discovered in **Ivanti EPMM** is being actively exploited in the wild

CISA

Released an alert on 2022 most consistently exploited vulnerabilities

STARK#MULE

Targeting Government and E-commerce sectors in **South Korea**

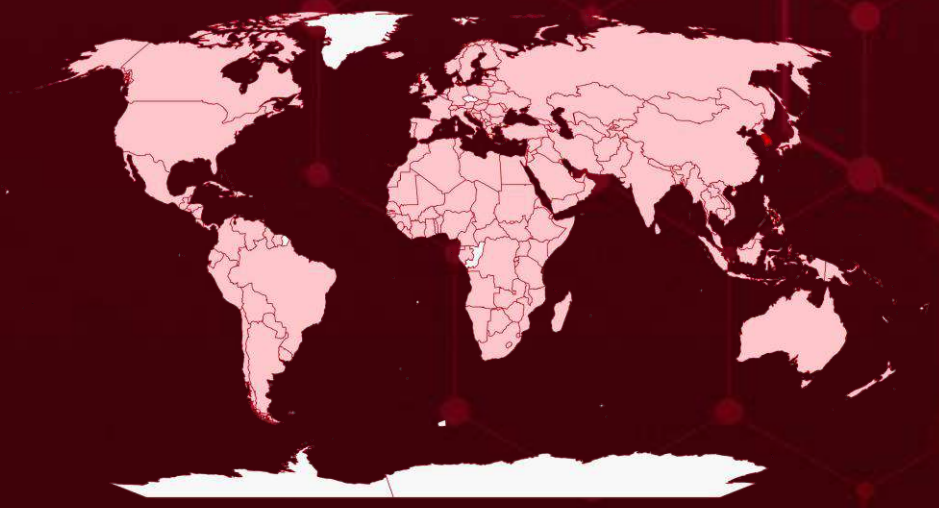
APT 29

Russia-based actor targeting **Microsoft teams** via social engineering
40 global organizations have been affected including government, NGO, IT, Tech, manufacturing, and media sectors

Targeted Countries

Most

Least



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Countries
South Korea
North Macedonia
Zambia
South Sudan
Algeria
Moldova
Andorra
Saint Kitts & Nevis
Angola
Trinidad and Tobago
Antigua and Barbuda
Maldives
Argentina
Nauru
Armenia
Peru
Australia
Seychelles
Austria
Switzerland
Azerbaijan
United Kingdom

Countries
Bahamas
Luxembourg
Bahrain
Mauritania
Bangladesh
Morocco
Barbados
Nicaragua
Belarus
Palau
Belgium
Qatar
Belize
Sao Tome & Principe
Benin
Slovenia
Bhutan
State of Palestine
Bolivia
Thailand
Bosnia and Herzegovina
Tuvalu
Botswana
Vanuatu

Countries
Liechtenstein
Brunei
Malawi
Bulgaria
Malta
Burkina Faso
Mexico
Burundi
Mongolia
Cabo Verde
Myanmar
Cambodia
Netherlands
Cameroon
Nigeria
Canada
Oman
Central African Republic
Papua New Guinea
Chad
Poland
Chile
Russia

Countries
Samoa
Colombia
Senegal
Comoros
Singapore
Congo
Somalia
Costa Rica
Sri Lanka
Côte d'Ivoire
Suriname
Croatia
Tajikistan
Cuba
Togo
Cyprus
Turkey
Czech Republic (Czechia)
Ukraine
Denmark
Uruguay
Samoa
China
Brazil

Targeted Industries

TOP MITRE ATT&CK TTPS

T1036 Masquerading

T1566 Phishing

T1059 Command and Scripting Interpreter

T1005 Data from Local System

T1588.006 Vulnerabilities

T1583 Acquire Infrastructure

T1583.001 Domains

T1588.005 Exploits

T1068 Exploitation for Privilege Escalation

T1059.001 PowerShell

T1041 Exfiltration Over C2 Channel

T1203 Exploitation for Client Execution

T1083 File and Directory Discovery

T1547 Boot or Logon Autostart Execution

T1071 Application Layer Protocol

T1190 Exploit Public-Facing Application

T1588 Obtain Capabilities

T1027 Obfuscated Files or Information

T1574 Hijack Execution Flow

T1105 Ingress Tool Transfer

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rilide Stealer	A new version of the Rilide Stealer malware, evading Chrome's security measures to target Chromium-based browsers in campaigns that exploit user trust through fake plugins and games	Phishing, Malicious Extensions	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
InfoStealer		Data Theft, Financial Loss, Espionage	Google Chrome, Microsoft Edge, Brave, and Opera
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	008b7d803d8925c578168a2bd757dd4a0b26b32b2f810ce91e3f062e1ed5cd0c, 0778c7e2ec2dde55d2e88f31168a52d8e78ce5348ccab82c8e6b2c0f3bb0b3eb, 0fd8a4468d7d5370d1f67b01badb2e7e1aacb3e6cf1689cab4f678cc7868f520, 14405eee6b03c4de6fba6b68768a943120c092280e0763ee2672b7ffdf9358bc, 1ac5e7036f862b8d2a951b1be262b498f0c9213d4d2f500e9c5f06ac8e8179b2		

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-2023-35081		Ivanti Endpoint Manager Mobile (formerly MobileIron Core): before 11.10.0.3	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ivanti:mobileiron_core:*:*:*:*:*:*:*:*	-
Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-22	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://forums.ivanti.com/s/article/CVE-2023-35081-Arbitrary-File-Write?language=en_US

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2018-13379		FortiOS: 5.6.3 - 6.0.4	MuddyWater, APT29
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*	Conti Ransomware, LockBit Ransomware
Fortinet FortiOS SSL VPN Path Traversal Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://fortiguard.com/advisory/FG-IR-18-384

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34473	PROXYSHELL	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2013 Cumulative Update 23 15.00.1497.002	UNC2596, APT35, Cadet Blizzard APT, ChamelGang
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	BlackByte Ransomware, LV Ransomware, cuba ransomware, AvosLocker Ransomware, Hive Ransomware
Microsoft Exchange Server Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-918	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34473

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-31207	PROXYSHELL	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2019 Cumulative Update 9 15.02.0858.005	ChamelGang, UNC2596, APT35, Cadet Blizzard APT
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	Blackbyte Ransomware, cuba ransomware, AvosLocker Ransomware, Hive Ransomware, LV Ransomware
Microsoft Exchange Server Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-22	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31207

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34523	PROXYSHELL	Microsoft Exchange Server: 2013 Cumulative Update 23 15.00.1497.002 - 2013 Cumulative Update 23 15.00.1497.002	UNC2596, APT35, Worok gang, Cadet Blizzard APT, ChamelGang
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:exchange_server:-:*:*:*:*:*:*:*	LockFile, Blackbyte, Cuba, AvosLocker, Hive, LV Ransomware
Microsoft Exchange Server Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-287	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34523

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40539		Zoho ManageEngine ADSelfService Plus: 6000 -6113	APT27, Volt Typhoon
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:zohocorp:manageengine_adselfservice_plus:-:*:*:*:*:*:*:*	-
Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-287	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://www.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26084	✗	Atlassian Confluence Server: 6.0.1 - 7.12.4	UNC961, Cadet Blizzard APT
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	Cerber Ransomware, Muhstik botnet
Atlassian Confluence Server and Data Center Object-Graph Navigation Language (OGNL) Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-174	T1055: Process Injection	https://jira.atlassian.com/browse/CONFSERVER-67940

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-44228	LOG4J	Apache Log4j: 2.0 - 2.14.1	Muddy Water, APT41, Lazarus, UNC961
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:-:-:*:*:*:*:*:*:*	Prophet Spider, Muhstik botnet, Deep Panda, Enemybot, LockBit, MuddyWater, Monti ransomware, Budworm
Apache Log4j2 Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-917, CWE-400, CWE-20, CWE-502	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://logging.apache.org/log4j/2.x/security.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22954		VMware Workspace ONE Access: 20.10.0.0 - 21.08.0.1	Rocket Kitten
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:identity_manager:-:*:*:*:*:*:*:*	Enemybot
VMware Workspace ONE Access and Identity Manager Server-Side Template Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-94	T1221: Template Injection	https://www.vmware.com/security/advisories/VMSA-2022-0011.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-22960		VMware Workspace ONE Access: 20.10.0.0 - 21.08.0.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:*	-
VMware Multiple Products Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-269	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://www.vmware.com/security/advisories/VMSA-2022-0011.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-1388	✗	BIG-IP: 11.6.1 - 16.1.2.1	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:f5:big-ip_access_policy_manager:*:*:*:*:*:*:*:*	Enemybot, Zerobot
F5 BIG-IP Missing Authentication Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-119	T1068: Exploitation for Privilege Escalation; T1190: Exploit Public-Facing Application	https://support.f5.com/csp/article/K23605346

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	FOLLINA	Windows Server: 2008 – 2022, Windows: 7 - 11 21H2	APT28, FIN7, GoldenJackal APT, Asylum Ambuscade
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*	JackalControl, JackalWorm, JackalSteal, JackalPerInfo and JackalScreenWatcher, Lokibot, Woody RAT, Black Basta
Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	Mitigation DETAILS
	CWE-78	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-26134		Atlassian Confluence Server: 5.0 - 7.18.0 Jira Data Center: 6.0.0 - 8.22.3	8220 Gang
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:atlassian:confluence_data_center:*:*:*:*:*:*:*:*	-
Atlassian Confluence Server and Data Center Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-74	T1203: Exploitation for Client Execution; T1059: Command and Scripting Interpreter;	https://jira.atlassian.com/browse/CONFSERVER-79016

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
APT 29 (aka Midnight Blizzard, Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo)	Russia	Government, Non-Government Organizations (NGOs), IT services, Technology, Discrete manufacturing, and Media	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Windows
TTPs			
T1036:Masquerading, T1621:Multi-Factor Authentication Request Generation, T1566:Phishing , T1110.003:Password Spraying, T1110:Brute Force , T1484.002:Domain Trust Modification, T1484:Domain Policy Modification, T1583.001:Domains, T1583:Acquire Infrastructure , T1566.003:Spearphishing via Service , T1586:Compromise Accounts , T1530:Data from Cloud Storage			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **thirteen exploited vulnerabilities** and block the indicators related to the threat actor **APT 29** and **Rilide Stealer** 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 **thirteen exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT 29** and **Rilide Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

Ivanti Addressed Second Zero-Day Flaw Exploited by Attackers

STARK#MULE Targets South Korea with US Military-themed Baits

New APT 29 Campaign Targets Organizations through Microsoft Teams

New Rilide Stealer Version Evades Chrome Manifest V3 Protections

2022 Most Consistently Exploited Vulnerabilities

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
Rilide Stealer	MD5	0f8c7037ba4cf9736a5ac22cde94b7ed, 0fb39568d9ba07e39f64d64510832a99, 172f5c41250ef3e84579645e5b1a22bc, 1c683f7e8ede935de16fe1af8d920b4e, 1de4b5ff5035d3df6ab27d12c83b18f5, 20d8abba528c323668911a7da1993336, 23fc39223b0225998a70a3cb2e05ad4b, 367300209532298c12b8678a1699b6ff, 403dd2a2a6163c07710fabc08f71bec8, 44cf3fe19f92cfac81d74ec366302104, 47c7a9d2010c0f1d1c20fec47339451b, 4a0e5fee91b361a09cd9d70e5f6ffb3d, 4aa44852969f4c603bf9e8e3799d6984, 59998a5c7c0f31adc47f3d05333ff8cc, 59e77f77b458eb0c390f90e2daa35504, 5a439a865ba82b35ef8eeacc1a778e0c, 5e8d7b2ea9c184a5a88edd0e507571ed, 614ce2b5df0dd74d1bc5b0bde55edd53, 63e9249d7950ca2e03c40a64a76a3951, 66e05bc7b8e8ccd31415e22272f03bd4, 678a0f6c5a0662b8f42fca2f6788e3c6, 79f586fe64498205b1aab8ece4b2e944, 7a60adb662556863752bd2ab1c25c727, 7ba207ff437a0df9b5a05a01c0d548b9, 7ca9216d43d51507d326a72c4d27056e, 8080ad6ea6102d445ea16169a990cb5e, 89d7bf4d70efaeb4e63eddd179df9829, 8b008a8f776b57060b5ce42b6ea2b8f6, 97a42807acd13205c1a2937850416439,

Attack Name	TYPE	VALUE
Rilide Stealer	MD5	9f806a3d233ffbbb58cf82c3e769d6a5, a404c8f69888159b85aa2b069f0d0f90, a906698ebe07eac71494052bb82cd3f2, adbc8e285c7657615b2ebee344390952, ae249d95c6ac779246b8eea93730801f, b4867df506f38736c0f6ce56decad080, bb8315ba98e0cb251453d58cf2048f3b, bc9472ab59a9625003190b2dfcd1c502, bda2f43f6a08de8e0d41aa704a796eb1, c8805c7f4224c02b173f6beab132638c, ced4052c3d3d32e21df075d68b5a4494, cfe9ec19dd3991c45c76493d9598141b, d2b07b0e4142bbcb1457d51e25da416d, D504505d18408343a5f1225a0d0f3c1b, ddddeb26f795fd7658720d5ae80a310d, df7d7dc978275f8c85ab8408abc8df95, e879d0f7540ce7b3365c7f79a461ec98, f1f97bcec87f298f3f533fbcb0de034e, f5dc1259e5300b8d4711ca7bf51c6e9f, f8653cd2a1c7cea7509abd6cd52078b3, fa3509f5adb6b3c8857194083af87edd, fc3afbea35d3844550af54a2506a5f64, fd59031e1c35e5fb1ecbaff6c64a31e8
	SHA1	018caa6adbd983fd2e2ba46670196a41669b4cef, 027268c51892ca07c36b66ae31dbe33c2afeb789, 060ac379851786e61d081b1471ee15347185e56c, 10d3d6bf88bead7180e84a2b7acf3abc60e14e81, 16f46139147f5f6dcd521840951860c299982587, 173065e688b008e208d6ffd62ea2b5a15cf66552, 18ccba913df5b8867c6ef066f121fb8cd03a7518, 2700d7a6c6f5abdea5972c9d5a67603216870af4, 29dd8609c74cc54d60bab53c6e83a3cb641f8b4a, 2c98abcaea10d3abd307c68cbf95f3e4af40ec04, 3197073f18ce0432691d61f09302f949d3283e0b, 3976d181a1bdeaca94c072d672ee90750865ee96, 397a40a2f5047db13bf84bd7e6296c12dc317933, 3c6fcd01f513df3480930924bd82d2abdb19266a, 5174127b62bd3a1e983dd8a33e3efa5ec54471c8, 52a1ee4060e13790501163c78d3475be90f05584, 552b715702d8b4b0f035a92d5ab5bb1f0712ac32, 69fb5b178f369beaac85f02791fd8f85facdd20b, 70cae8f5f2d6573510f5f4400a8baba89e5bcd2f, 76fc50665aea80dca8844282804339b7351c3267, 8316ab2ee030c859d2952a0a0ee3fb8606b88816,

Attack Name	TYPE	VALUE
Rilide Stealer	SHA1	92a030999013b6835b39d2cce951fcb258107bc8, 92d4921b1fc15ae389a59b5df90614d7926f95e9, 937e03c89c33bbd5c7727c3f8e00aecdf22afa7f, 946ac4d655bc77624b912ad42431c8a692cac6a4, a1456ea8696c755d1d2c4d1f27661f9388f805b9, a1b9fd0577f6cc0ff87010a651ff123b8285289c, a25fccb0455f8e9d3751f5127dd6867aecb58b45, a468269647f3b9909f4df27b74711d56adaf87a4, aa7929ba89295c732398c63a574a49f035b9ca52, ace802a22a69b2d6fe305d407212c0919671f81a, b0c587068505fcbdb55d263dff03f3abbeeb0842, b27a56ee3262c4d87bae60c514ea7056a4ec7c6f, b3d59d7caab786cb92639a8c8bc17f73da26c788, c84a3774eea3c7c3069964fff500eb498a3e3fa0, cba87daff1cf961fe941489cfcc80f074f8d49ed, cc7949e9587b7f64049ab5b9b3603eb831f47808, ccbf7ed9d3c2b606b753359cb4b10caa2570a571, cde2d4b70d374fca96951a13f056f778258aeb45, d033569c97f382b21ce83439dae0cab5bd28e135, d85c34f3cd20d24fde93f0e60d677d2aa8c48591, dc7fa285da2034a00ed2c66cb86c37e1a4bbd679, dd4e7e8230e14685d73d142efb337e75cb2d3581, dd6e2e93d80d9b5df93e17e714aee41534f1158a, dd7f3feb98e4d84817a84a9fdfddaed3b2719303, ddb5e3e03655fa8dd8690aeb81db00da84bd2c8b, e3476f4fb588b23bdd625bdc75a98a16d1acb4bd, e4aaef90c4284e923679e92e970396f7ef989087, ea4d7f31e889585d1a2c77e2b2823a4ccbd765d2, f2348f98a71afcc241c6e3d5777b300e5602a4e5, f5a5d008a70e1c632d7cb72b2f255f3e500b43e4, f637104610e14e2260a792fd17775a83d2551a38
	SHA256	008b7d803d8925c578168a2bd757dd4a0b26b32b2f810ce91e3f062e1ed5cd0c, 0778c7e2ec2dde55d2e88f31168a52d8e78ce5348ccab82c8e6b2c0f3bb0b3eb, 0fd8a4468d7d5370d1f67b01badb2e7e1aacb3e6cf1689cab4f678cc7868f520, 14405eee6b03c4de6fba6b68768a943120c092280e0763ee2672b7ffdf9358bc, 1ac5e7036f862b8d2a951b1be262b498f0c9213d4d2f500e9c5f06ac8e8179b2, 1c1a8d502871dbf22b404b6825b5219344a3d89ebb5da88380ba1ca158e2d92b, 1f62a8dc5e71b2826d0fe70588c4c4cbebb9518d3f1125807e6e6927b359458a,

Attack Name	TYPE	VALUE
Rilide Stealer	SHA256	2aac1089998e5e88fbdf539408be53570a4ed64a989885d1003bf73c723eea1d, 2b638291abc822a2bb5f94b196022cae4b064487a71a8e067f8d8a2fb3c7acc5, 35451261a9864614aaeb43cd8bfb8d166a483baaa4477c6e119ebcffffa0ba31, 3978acf99393c9538dedc22f97eb247bbcfe0791acead7f6c96d1079479286fd, 3aa913da9591d998a229acec529eb58b1fea14b403b92f56dde47a8425739473, 45d03f5d809664844d569d35431a147885d201ca151bda9bf66f282daec025a6, 461773a67e1a6228d0a8d02a45da72fc94ce0df97cd99aef33dcbf859d306a11, 482b3ae10d6b70c1faf55a9b3abd14bdc1b198b18d089a0aea6aa6ac6fd7ace1, 48346d8f46efca68f354f0833c3cfc9e8931d5b655ec434725fcdffb03069460, 533576b2f435591fe51d0e09d479154fac13a6440c619085dc0a11ada0f69e12, 54920cdfbc9403da38058b90bfb19a1af5caff2ca4584209d13e0f90b64c3b2c, 5f6e10bdfe78f855105843c67ff6ec69801caba328a8b1681425b06e359f888c, 687e9fc52445b8045fccc308c30713395bdfba08dac83fc85355a5c94b2bbbde, 6a83ee64b323082bf8827deb6297d4d3895f346ff83e9d9d4d125e976df5e503, 6aa388c50c8c184901db02eae71b1ec3d9e0ab9e636d22419f64a83c8b2c94b0, 6e9c56301605aeeb0efcbbfbf10008dba7a8b99963f02256d1b28fbc30df7907, 6f68fdf8c77b6deb44427322f82a6476a631ec6e4cdb0b18421bf5a0c895435e, 718b9adb3cd2f68c41234870242e312cac6beb00444ed4e21dca5f21b6fbecb9, 7465e22c5544ff885472e36dd60beec5039c68c4728d804fea240bc36e8f6794, 7dde5fe5377eaa43af2896f0aab7a6875ac88a34d0391c39d0979c3cf2861723, 7f0a71e2443cef0beaeea10a78fbbdb3a612be6c4be206acf7c13849d593fad7, 83fff7424342575d8ab6a9bd8eba71490e75a87ea825c8a84bb16945613467e1, 8caaafe787c9e3d59486ec129b4259764641999b0f1de6b5b46d3773e96442c8, a4ebe88f43d782b30fd83e1fb79b26674827cc03db4aeb77540243c303b51a6a,

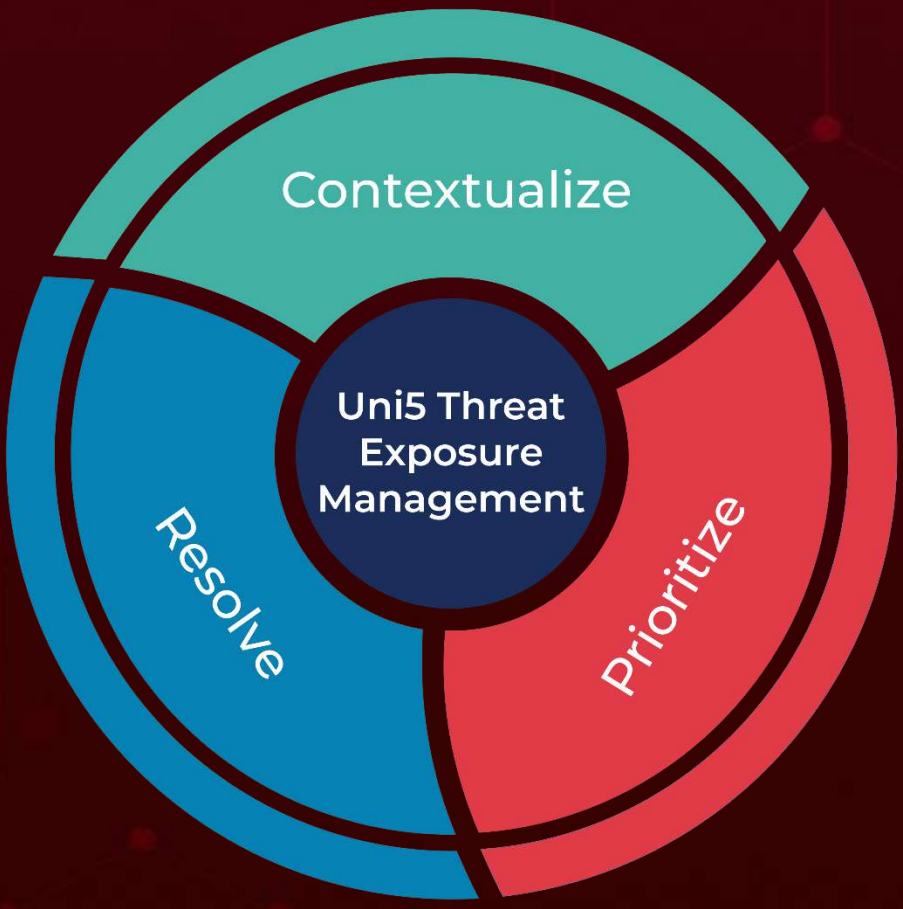
Attack Name	TYPE	VALUE
Rilide Stealer	SHA256	a7e24ead72e9bd2d74be36c201e348d5c5aa29c1c0c4e972677ce12602a74158, aa76e48528f473b171b98bfc4d4e4d839a98c255e78382dc6f020e36ed00ea5b, abae2f164e073e7aab2822b507de10e731cc1b396809728452e98be6618c149f, abe1c395c9db7df35611caf30fff0a18f23726505b2b51e4dce6547896ee6f76, ac4ae2bb49343ed24c2ae0d531cde04c3186dc4263a2352f2c2ac78812bb5c05, ad32f29f994a9d4eeceb39afeaa2a1dbda4f17931668d64026c225c738518cfd, ae5da62daf678fc0555f739c116f58fd26c5400257367dcd0f777997615a4b23, aed0c82e40f51089ef8c08df53404d61a591db8f14f07a9ef38aeeef8f4e15a8, b6043858d8b28b397ce364417a59167bb1afb32b5c8fcf0be428362af7952e27, ba1d0a41bf1bfacf41e667857cbd24b9834631613de44124b95357cd5c7637c3, c23846b1ec00890c3fda2b600b29b2fb717de6fa54b8c9bebe825aa4e0a7f2cc, cab8e0569f69efe0214dea05461cba63c3abb9c255f17e2ae48e904dfce500fd, cca6dda21c62f2665eccdec2edff5e6dfa6260a217c02709b21b3e14670ca3b7, d4ae1e54da50c3dbf7c201a42537f42fc307c5ce7700ad32aceb60f69ed7d779, d755c580cc88b6a5028e843aeda3e3a50c8f025ef1dcf66027c0c1b671024d36, dea7f22216fcd2a3355b231d57dec37164c85faf3e9279beae6cdb153051a48a, dfc0c60526e78d58f055ddace6cb91227958a0c5b413c88d00be175f084bd5da, dfff032e311776b3d62f70856a6d29ca8267beee614f756301b7f891c6325485, e39d0974b403b547b07282237f356061754375d1b70dacf731d8fa2add15d856, e669e3509aa8d6a425b61e77993b23f832071ba2f7def373af57417f661eb431, e89971bfb8375d748cc233157537856c5598fcd513ed42e862261a99843f40d0, e8a791965f8534b33736a0786ebeb0975002f3a03c31aefe2e4a64a1d4c70a34, f2931eb819db38895ccc016a6b04b90bb1456931164f2b7e15f4bc0c95fbd997, f6e81b0d239268ce0c9bb6ba7dbe09fb67ffa273a85fdfe656b14b5ea9a94568

Attack Name	TYPE	VALUE
Rilide Stealer	Domains	blackfox.lol, eaougheofhuoaez.top, edd2ed2.online, ext-panel.website, extension-login.com, extensionsupdate.com, faugzeazdezgzgfm.top, frz-panel.su, getvoyagebox.org, io-web.cc, lsadksajpenal.su, nightpredators.com, proyectopatentadomxapostol.com, pupkalazalupka.com, riotrevelry.com, silent-scale.com, tes123123t.com, web-lox.com

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 7, 2023 . 8:20 AM

More at www.hivepro.com