Date of Publication
July 10 , 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

3 to 9 JULY 2023

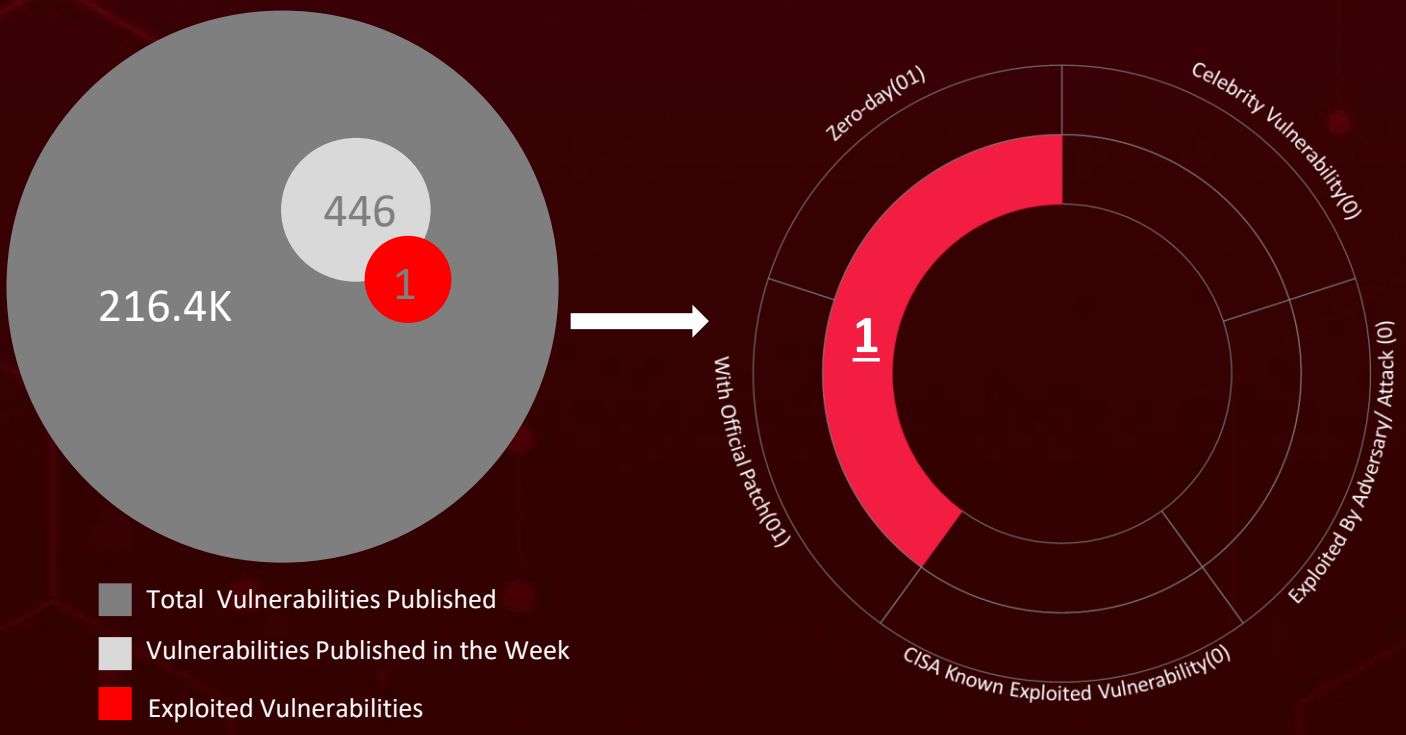
Table Of Contents

Summary

HiveForceLabs recently made several significant discoveries related to cybersecurity threats. Over the past week, the fact that there were a total of **eight** attacks executed, a **zero-day** vulnerability in the WordPress Plugin, and **three** different adversaries highlights the ever-present danger of cyber attacks.

Moreover, HiveForceLabs also discovered that **Charming Kitten** employed four malware, in its recent attack targeting US and Middle East. Furthermore, we identified **LockBit Ransomware** demands a 70-million-dollar ransom for claims of data exfiltration from TSMC systems.

Meanwhile, the **RUSTBUCKET** malware family is actively developing, adding persistence capabilities, while the REF9135 operation by the DPRK targets cryptocurrency service providers. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



High Level Statistics

8
Attacks Executed

- Lockbit Ransomware
- PlugX variant
- RUSTBUCKET
- Crysis Ransomware
- Venus Ransomware
- GorjolEcho
- CharmPower
- NokNok

1
Vulnerabilities Exploited

- CVE-2023-3460

3
Adversaries in Action

- Lazarus
- 8Base
- Charming Kitten

Insights

RUSTBUCKET
A New Variant of North Korea-Linked macOS Malware Emerges

$70 million was demanded by the **LockBit** ransomware gang, striking **TSMC IT supplier**

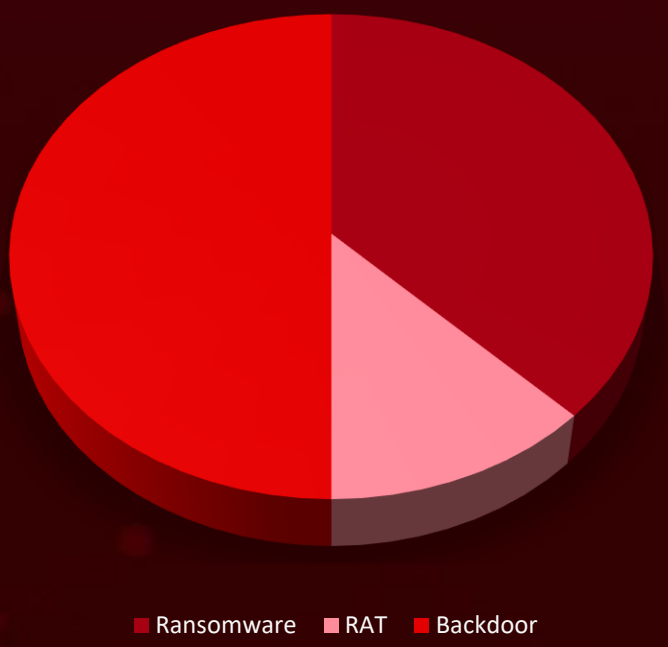
8Base
Ransomware Group Emerges as a Menacing Threat

200K Installs: Ultimate Member WordPress Plugin Vulnerable to Zero-Day Exploit

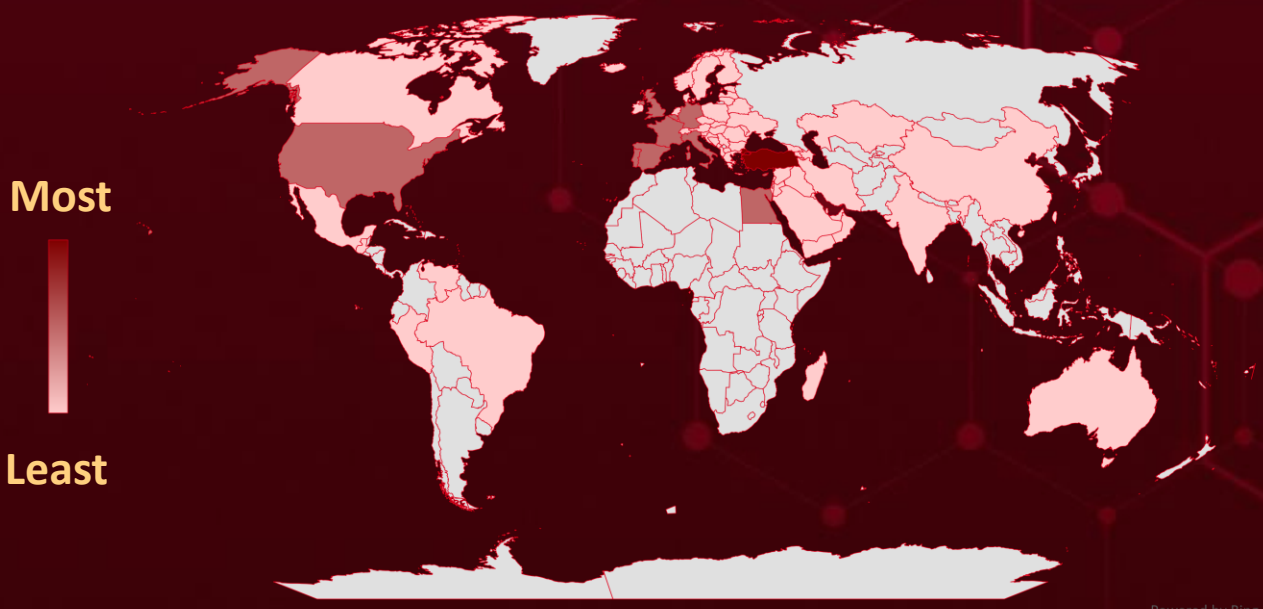
SmugX Campaign
Chinese Nation-State Group Launches Persistent Assault on Europe's Foreign Affairs Ministries and Embassies

Crysis
Threat Actors Harness RDP Connections to Disseminate Ransomware

Threat Distribution



Targeted Countries



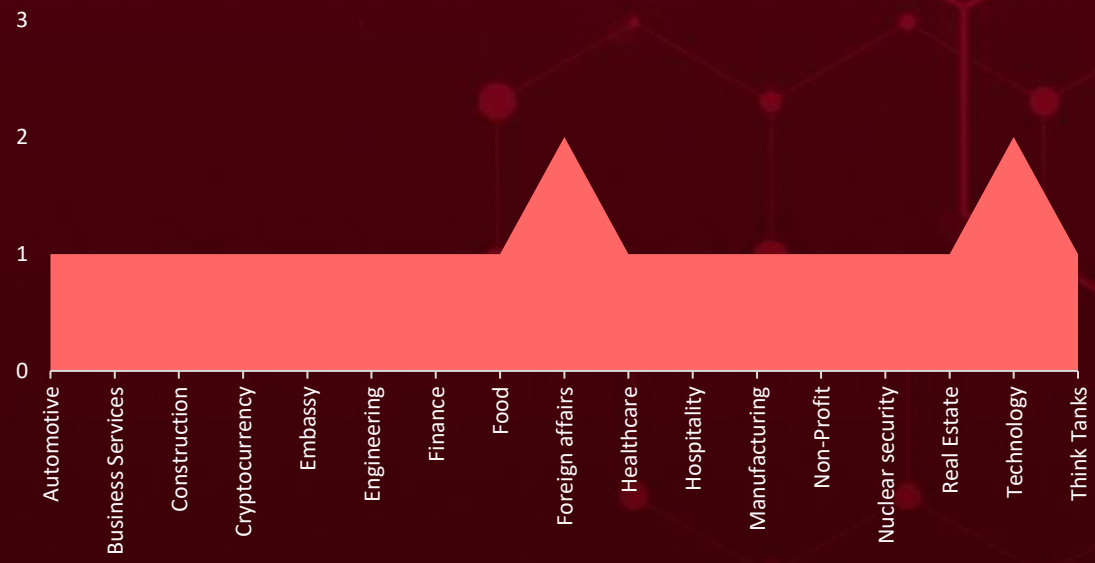
Countries
Turkey
Portugal
Italy
Germany
Cyprus
United States
Egypt
Belgium
Spain
France
United Kingdom
Luxembourg
Romania
North Macedonia
Bulgaria
Switzerland
Canada
Moldova
China
Peru
Croatia
Slovakia
Andorra
Ukraine
Czechia

Countries
Malta
Denmark
Montenegro
Armenia
Oman
Estonia
Belarus
Finland
Saudi Arabia
Australia
Albania
Georgia
Taiwan
Austria
Lithuania
Greece
Madagascar
Guatemala
Mexico
Hungary
Monaco
Iceland
Netherlands
India
Norway

Countries
Iran
Palestine
Iraq
Poland
Ireland
Qatar
Israel
San Marino
Azerbaijan
Serbia
United Arab Emirates
Slovenia
Bahrain
Sweden
Venezuela
Syria
Akrotiri and Dhekelia
Bosnia and Herzegovina
Lebanon
Brazil
Liechtenstein
Jordan

Countries
Vatican City
Kazakhstan
Yemen
Kuwait
Latvia

Targeted Industries



TOP MITRE ATT&CK TTPS

T1547 Boot or Logon Autostart Execution

T1059 Command and Scripting Interpreter

T1036 Masquerading

T1027 Obfuscated Files or Information

T1082 System Information Discovery

T1566 Phishing

T1547.001 Registry Run Keys / Startup Folder

T1486 Data Encrypted for Impact

T1071 Application Layer Protocol

T1562 Impair Defenses

T1562.001 Disable or Modify Tools

T1140 Deobfuscate/ Decode Files or Information

T1490 Inhibit System Recovery

T1070.004 File Deletion

T1057 Process Discovery

T1595 Active Scanning

T1071.001 Web Protocols

T1027.002 Software Packing

T1497 Virtualization/ Sandbox Evasion

T1190 Exploit Public-Facing Application

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Lockbit Ransomware	The Lockbit Ransomware group, National Hazard Agency, has claimed of targeting TSMC and is demanding a 70-million-dollar Ransom, Attackers are claiming to be in possession of sensitive information and threaten to release data in the public domain	Unkown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Exfiltration, Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f, af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16, 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d, 2cee882bd0dc4267bacf099ac4571c319ac547be12b955f7ccb2f0144ae4876		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PlugX variant	A Chinese nation-state group has been persistently conducting a SmugX campaign targeting Foreign Affairs ministries and embassies in Europe. They employ HTML smuggling techniques to distribute a new variant of the PlugX remote access trojan.	Spear-Phishing Emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Information Theft and Espionage.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	edb5d4b454b6c7d3abecd6de7099e05575b8f28bb09dfc364e45ce8c16a34fcd, 736451c2593bc1601c52b45c16ad8fd1aec56f868eb3bba333183723dea805af, 0e4b81e04ca77762be2afb8bd451abb2ff46d2831028cde1c5d0ec45199f01a1, 989ede1df02e4d9620f6caf75a88a11791d156f62fdea4258e12d972df76bc05, 10cad59ea2a566597d933b1e8ba929af0b4c7af85481eacaab708ef4ddf6e0ee		

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
RUSTBUCKET	The RUSTBUCKET malware family is undergoing active development, incorporating new persistence capabilities and focusing on reducing its signature detection. This variant of RUSTBUCKET specifically targets macOS systems.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Lazarus			-
IOC TYPE	**VALUE**		
SHA256	9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747, 7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387, ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41, de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500, 4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Crysis Ransomware	The CrySIS aka Dharma ransomware family is operating as ransomware-as-a-service (RaaS) model. Crysis ransomware scoured the internet using brute force or dictionary attacks, searching for vulnerable RDP endpoints.	Externally Exposed RDP	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	786ce74458720ec55b824586d2e5666d		
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
Venus Ransomware	The threat actors behind the Crysis ransomware are currently utilizing the Venus ransomware as a component of their attack strategy, with a primary focus on targeting vulnerable systems through active RDP.	Externally Exposed RDP	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	67b1a741e020284593a05bc4b1a3d218		
SHA1	026ce3bceb3a82452f0fc38c0b9abfa90f2c9d87, 06757be6174bdc9ef8fe899bcbe5e6e5547dc059		
SHA256	04d75593f6acdfe0c959345b8d6702166537d7533abfeb4b568339dee1986b5e, 0a4e5832841ffff9f8d27ce8216d655c8743b682fff0f90dee6bd3ea83dec028		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GorjolEcho	A new PowerShell backdoor called GorjolEcho establishes persistence on compromised systems. GorjolEcho enables the threat actor to conduct intrusive activities such as information exfiltration and potential module downloads for espionage purposes.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
Domain	library-store.camdvr[.]org, fuschia-rhinestone.cleverapps[.]io, filemanager.theworkpc[.]com		
IPv4	144.217.129[.]176		

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
CharmPower (aka GhostEcho or POWERSTAR)	The new modular PowerShell-based framework dubbed CharmPower, is used to establish persistence, gather information, and execute commands.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft, and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
SHA256	b79d28fe5e3c988bb5aadb12ce442d53291dbb9ede0c7d9d64eec078beba5585, 9777f106ac62829cd3cfdbc156100fe892cfc4038f4c29a076e623dc40a60872, 977cf5cc1d0c61b7364edcf397e5c67d910fac628c6c9a41cf9c73b3720ce67f, 823ffbcc62bd3296957a47fbf8c238949584996911e71d5140a25d0a8f6abd80		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
NokNok	Charming Kitten ported its malware and attempted to launch an Apple-flavored infection chain dubbed NokNok.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage, Information Theft, and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			-
IOC TYPE	**VALUE**		
SHA256	1fb7f1bf97b72379494ea140c42d6ddd53f0a78ce22e9192cfba3bae58251da4, e98afa8550f81196e456c0cd4397120469212e190027e33a1131f602892b5f79, 5dc7e84813f0dae2e72508d178aed241f8508796e59e33da63bd6b481f507026, b6916b5980e79a2d20b4c433ad8e5e34fe9683ee61a42b0730effc6f056191eb, acfa8a5306b702d610620a07040262538dd59820d5a42cf01fd9094ce5c3487c		
Domain	library-store[.]camdvr[.]org		
IPv4	144.217.129[.]176		

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-2023-3460		WordPress Ultimate Member Plugin <= 2.6.6	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:ultimatemember:ultimate-member:2.6.5:*:*:*:*:wordpress:*:*	-
WordPress unauthenticated Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH DETAILS
	CWE-269	T1595- Active Scanning, T1595.002- Vulnerability Scanning, T1068- Exploitation for Privilege- Escalation, T1190- Exploit Public-Facing- Application, T1136- Create Account, T1078- Valid Accounts	Update the plugin to version 2.6.7 or higher. You can update the plugin version to the required version through the WordPress Admin dashboard.

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5"> 

Lazarus (aka Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, Diamond Sleet)</td><td>North Korea</td><td rowspan="3">Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology, and Cryptocurrency</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage, Sabotage and destruction, Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>RUSTBUCKET</td><td>macOS</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1071.001- Web Protocols, T1071- Application Layer Protocol, T1106- Native API, T1059- Command and Scripting Interpreter, T1647- Plist File Modification, T1547- Boot or Logon Autostart Execution, T1082- System Information Discovery, T1218- System Binary Proxy Execution, T1102- Web Service, T1566- Phishing, T1036- Masquerading, T1105-Ingress Tool Transfer, T1204- User Execution</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 8Base	-	United States, Brazil, Australia, Germany, United Kingdom, Mexico, Portugal, Belgium, Egypt, China, Spain, Madagascar, France, Peru, Canada, Turkey, Guatemala, Venezuela, India, Italy	Business Services, Finance, Manufacturing, Technology, Healthcare, Real Estate, Construction, Hospitality, Non-Profit, Automotive, Engineering, Food
	MOTIVE		
	Monetary Gains		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1588- Obtain Capabilities, T1588.001- Malware, T1547- Boot or Logon Autostart Execution, T1547.001- Registry Run Keys/Startup Folder, T1134- Access Token Manipulation, T1134.001- Token Impersonation/ Theft, T1562- Impair Defenses, T1562.001- Disable or Modify Tools, T1027- Obfuscated Files or Information, T1027.002- Software Packing, T1135- Network Share Discovery, T1486- Data Encrypted for Impact, T1490- Inhibit System Recovery, T1561- Disk Wipe			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, TarhAndishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)	Iran	Foreign affairs, Think Tanks, and Nuclear security	Middle East, United States
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	GorjolEcho, NokNok, CharmPower, and BellaCiao	macOS, Windows
TTPs			
T1071- Application Layer Protocol, T1041- Exfiltration Over C2 Channel, T1059-Command and Scripting Interpreter, T1590-Gather Victim Network Information, T1547-Boot or Logon Autostart Execution, T1082- System Information Discovery, T1218- System Binary Proxy Execution, T1102- Web Service, T1566- Phishing, T1036- Masquerading, T1204- User Execution, T1059.005- Visual Basic, T1204.001- Malicious Link, T1059.001- PowerShell, T1055- Process Injection			

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 **Lazarus, 8Base, Charming Kitten** and **Lockbit Ransomware, PlugX variant, RUSTBUCKET, Crysis Ransomware, Venus Ransomware, GorjolEcho, CharmPower,** and **NokNok** 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 **Lazarus, 8Base, Charming Kitten** and **Lockbit Ransomware, PlugX variant, RUSTBUCKET, Crysis Ransomware, Venus Ransomware, GorjolEcho, CharmPower,** and **NokNok** in Breach and Attack Simulation(BAS).

Threat Advisories

Lockbit Ransomware strikes, demands $70-million Ransom

Vulnerability in WordPress Plugin threatens Website takeover

European Ministries Fall Victim to Chinese Hacker’s SmugX Campaign

New Variant of RUSTBUCKET MalwareTargeting Cryptocurrency Providers

Surge in 8Base Ransomware Group Activity

Crysis Threat Actors Unleash Venus Ransomware via RDP

Charming Kitten's Latest Malware Arsenal and Targeting Strategies

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
Lockbit Ransomware	SHA256	0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, 498e3b7a867d41b5a3af3910d2aa6231612c787ce8a4bc14ab03f800caab130f, af4c28fb1c65ebe93181b67d279733e864cafab5919a7aa7eced93fc8113df16, 984d96730ae19d4532325c6fcbd34580fb02fbe454781b589d2eea6090ea2b6d, 2cee882bd0dc4267bacf099ac4571c319ac547be12b955f7ccb2f0144ae4876, 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75, 40406fd8c1d7e3c44dff7dfe669dd0a681e22aea3a4a31ba7df7e3a9c5e4be75, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, a736269f5f3a9f2e11dd776e352e1801bc28bb699e47876784b8ef761e0062db, 8022060ef633e157518037122a6003813cc0a3066d456a1164275a211efc8f5c, 5a13ac97ce91d5b095c7154fe756615fa0730c17ddf432ae4af6c42d2c29946d,

Attack Name	TYPE	VALUE
Lockbit Ransomware	SHA256	9aa5bcee06109d52fade97ad21317ff951abc656ba4c800441bacfec00328fd8, 379c4620d6f482e153d7033bba21da5d8027387c0e60e3497b63d778dcafd888, 0845a8c3be602a72e23a155b23ad554495bd558fa79e1bb849aa75f79d069194, b964a5253c25465633ef8c2e7f77703d27227bfc0b13a7ca49d187dadc4d38ae, ba0eefdfbd1421d37d47f3feaae8e768a4679d6b544bb97f5237319e8ab0b122, f9dbdb825067616070c64565b6b27dc872c4a7219856eb5f8eb3eb1eb1463423, 2e218735fa53e036659ea721bfd7b97e2af67b7eda648e9e2579356eb20899d9, 1f0e4cbc1a4b52b6d7e4188e4a835a904cf783c75db9a066df4201452bd9647d, de7f501e4a17898e85229b962e2f43b9a20d995c8a9fe0cad4536adc8fbd9f48, 8989a9aec8d2c4d61fa399a97807f8e62814b1a55fecbd38d11d4d35fdf4a7d1, 01bf78841b63bcdd8280157c486b45ad74811c0251140a054de81a925ce7f716, ab4d20b73c7358f1e3a60145d5debc791a17416e2a88eb39f80ec1f53985fad5, 9366a5b8021d0283156986bbf020c99ae5e2a3dcbbaa03db934e94bfa7088b86, 4bdda7dd3bbe1f9cb0a7d42f6947ba0f6442e52758bd2638541f9409b573d5c9, 6b4502d8ba3cff1a3139f72cdad863d53551b65b8c38d7b838d64212822e4630, 4d0f95028bb6a04e64550872ddeef6b0c6fa4a5bd368736da47401420df2bee7, cfc45c36b4c731f2308e19a087c3dc3fb7b12eef93e171e8e86e2134ead325ee, 4134d5d8f7b038e23e7887db56bb3ad295341a1aaf0bebe6be21d901d06dd662, 153fc9e90b955e2cfaf91b86888a29fdd8685144a3802f5e90b95b64116cdd33, 00accc2c186201607d3e36c1b013872ac51d4f805f23e625dc70154fb58fd4f4, 734955fdb84b29fa1aa87aa0af2ebf155125917a6b61ffe4b4dc7030dd212309, e47b928d0fc16348b828abeb3c2106a6d752512f60ef4583d6532cc0dbebebbf, 239c9969fd07e1701a129cfd033a11a93ee9e88e4df4f79b7c5c0dd5bba86390,

Attack Name	TYPE	VALUE
Lockbit Ransomware	SHA256	a439c5093801d3b12e2f79b64c0b65bdf148eb6eca8c1e3d179af5ab4995034d, 54ac7ac6db6fcec5234454430513d1d2787ee8a48aa60fbf95c1af27534fdb4a, A9abab8ab44ccec6321da83d9960a1f30ba783e02b6e0ba3f2e9d19cee76b39b, 286726ecca68f8c2752116258aba0cd35c051a6342043ee1add84b890654276f
PlugX variant	SHA256	edb5d4b454b6c7d3abecd6de7099e05575b8f28bb09dfc364e45ce8c16a34fcd, 736451c2593bc1601c52b45c16ad8fd1aec56f868eb3bba333183723dea805af, 0e4b81e04ca77762be2afb8bd451abb2ff46d2831028cde1c5d0ec45199f01a1, 989ede1df02e4d9620f6caf75a88a11791d156f62fdea4258e12d972df76bc05, 10cad59ea2a566597d933b1e8ba929af0b4c7af85481eacaab708ef4ddf6e0ee, 324bfb2f414be221e24aaa9fb22cb49e4d4c0904bd7c203afdff158ba63fe35b, c96723a68fc939c835578ff746f7d4c5371cb82a9c0dffe360bb656acea4d6e1, 9ce5abd02d397689d99f62dfbd2a6a396876c6629cb5db453f1dcbbc3465ac9a, 5f751fb287db51f79bb6df2e330a53b6d80ef3d2af93f09bb786b62e613514db, baca1159acc715545a787d522950117eae5b7dc65efacfe86383f62e6b9b59d3, 720a70ca6ee1fbaf06c7cb60d14e27391130407e34e13a092d19f1df2c9c6d05, 460c459db77c5625ed1c029b2dd6c6eae5e631b81a169494fb0182d550769f76, 277390cc50e00f52e76a6562e6e699b0345497bd1df26c7c41bd56da5b6d1347, 3c6ace055527877778d989f469a5a70eb5ef7700375b850f0b1b8414151105ee, 27a61653ce4e503334413cf80809647ce5dca02ff4aea63fb3a39bc62c9c258c, ce308b538ff3a0be0dbcee753db7e556a54b4aeddbddd0c03db7126b08911fe2, fd0711a50c8af1dbc5c7ba42b894b2af8a2b03dd7544d20f5a887c93b9834429, 3489955d23e66d6f34b3ada70b4d228547dbb3ccb0f6c7282553cbbdeaf168cb, 04b99518502774deb4a9d9cf6b54d43ff8f333d8ec5b4b230c0e995542bb2c61,

Attack Name	TYPE	VALUE
PlugX variant	SHA256	bd3881964e351a7691bfc7e997e8a2c8ce4a8e26b79e3712d0cbdc484a5646b6, ea2869424df2ffbb113017d95ae48ae8ed9897280fd21b26e046c75b3e43b25a, b00c252a60171f33e32e64891ffe826b8a45f8816acf778838d788897213a405, 2bc30ced135acd6a506cfb557734407f21b70fecd2f645c5b938e14199b24f1e, 0d13a503d86a6450f71408eb82a196718324465744bf6b8c4e0a780fd5be40c0, 0bdfb922a39103658195d1d37ff584d24f7bd88464e7a119e86d6e3579958cc1, a0879dd439c7f1ed520aad0c309fe1dbf1a2fc41e2468f4174489a0ec56c47c7, bddbc529f23ab6b865bc750508403ef57c8cf77284d613d030949bd37078d880, 4547914e17c127d9b53bbc9d44de0e5b867f1a86d2e5ede828cd3188ed7fe838, 0032d5430f1b5fcfb6a380b4f1d226b6b919f2677340503f04df04235409b2d0, 62c2e246855d589eb1ec37a9f3bcc0b6f3ba9946532aff8a39a4dc9d3a93f42c, f7d35cb95256513c07c262d4b03603e073e58eb4cd5fa9aac1e04ecc6e870d42, bf4f8a5f75e9e5ecd752baa73abddd37b014728722ac3d74b82bffa625bf09b5, 8a6ef9aa3f0762b03f983a1e53e8c731247273aafa410ed884ecd4c4e02c7db8, ec3e491a831b4057fc0e2ebe9f43c32f1f07959b6430b323d35d6d409d2b31e4, bf8e512921522e49d16c638dc8d01bd0a2803a4ef019afbfc2f0941875019ea1, ba55542c6fa12865633d6d24f4a81bffd512791a6e0a9b77f6b17a53e2216659, 8ea34b85dd4fb64f7e6591e4f1c24763fc3421caa7c0f0d8350c67b9bafa4d32, 8cac6dfb2a894ff3f530c29e79dcd37810b4628279b9570a34f7e22bd4d416b3, ea5825fa1f39587a88882e87064caae9dd3b79f02438dc3a229c5b775b530c7d, 1acb061ce63ee8ee172fbdf518bd261ef2c46d818ffd4b1614db6ce3daa5a885, 08661f40f40371fc8a49380ad3d57521f9d0c2aa322ae4b0a684b27e637aed12
	Domains	jcswcd[.]com, newsmailnet[.]com

Attack Name	TYPE	VALUE
PlugX variant	IPv4	45[.]90[.]58[.]69, 62[.]233[.]57[.]136, 217[.]12[.]207[.]164, 152[.]152[.]12[.]12
	Paths	C:\Users\<username>\VirtualFile, C:\Users\Public\VirtualFile, C:\Users\<username>\SamsungDriver, C:\Users\Public\SamsungDriver, C:\Users\Public\SecurityScan
RUSTBUCKET	SHA256	788261d948177acfcfeb1f839053c8ee9f325bd6fb3f07637a7465acdbbef76a, 1031871a8bb920033af87078e4a418ebd30a5d06152cd3c2c257aecdf8203ce6, 9ca914b1cfa8c0ba021b9e00bda71f36cad132f27cf16bda6d937badee66c747, 7fccc871c889a4f4c13a977fdd5f062d6de23c3ffd27e72661c986fae6370387, ec8f97d5595d92ec678ffbf5ae1f60ce90e620088927f751c76935c46aa7dc41, de81e5246978775a45f3dbda43e2716aaa1b1c4399fe7d44f918fccecc4dd500, 4f49514ab1794177a61c50c63b93b903c46f9b914c32ebe9c96aa3cbc1f99b16, fe8c0e881593cc3dfa7a66e314b12b322053c67cbc9b606d5a2c0a12f097ef69, 7887638bcafd57e2896c7c16698e927ce92fd7d409aae698d33cdca3ce8d25b8
	Domains	webhostwatto.work[.]gd, crypto.hondchain[.]com, starbucls[.]xyz, jaicvc[.]com, docsend.linkpc[.]net, companydeck[.]online
	IPv4	104.168.167[.]88, 64.44.141[.]15
Crysis Ransomware	FilePath	bild.exe_
	MD5	786ce74458720ec55b824586d2e5666d
	SHA256	419bc8196013d7d8c72b060da1a02d202d7e3eb441101f7bcb6d7667871a5c16, 5c2fb1c42f007093be5e463f70ee7e7192990b3385a3cbcc71043980efa312e0, 6a0017262def9565b504d04318c59f55bea136ac3dd48862d1ae90ff6b963811,

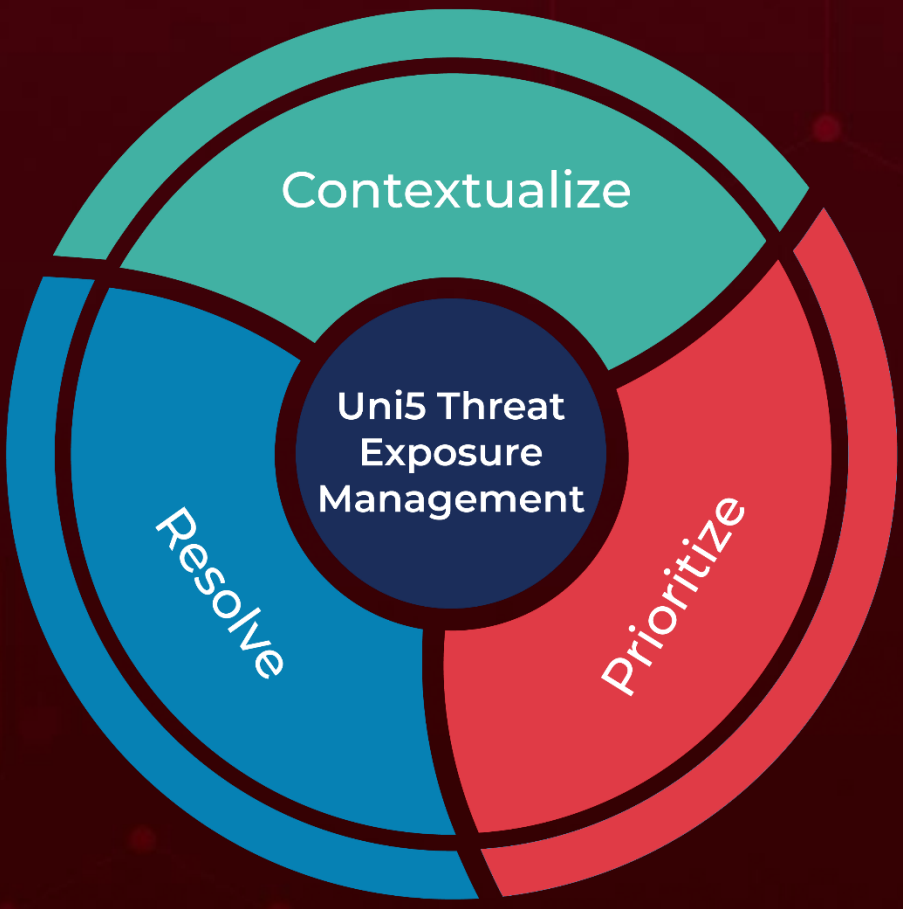
Attack Name	TYPE	VALUE
Crysis Ransomware	SHA256	b557bf11d82d3d64d028a87584657d25dba0480295ed08447f10c7a579dee048, b3984a2de76eee3ad20c4b13e0c0cbbab2dd6db65e3f6ca34418e79c21cf5c39, E9253218e30b30c8bb690b2ab02eef47b8b5c8991629d814b2af6664151e9a2f
Venus Ransomware	FilePath	1.exe_
	MD5	67b1a741e020284593a05bc4b1a3d218
	SHA1	026ce3bceb3a82452f0fc38c0b9abfa90f2c9d87, 06757be6174bdc9ef8fe899bcbe5e6e5547dc059, 0d0bbcecc80ea3b1712678b24ba925ac2903531f, 102b8625e5662c89efe4547dc2cb173be8b08851, 10f2ed474a9e0065fed2afebbfe81dc596f46542, 13315ee0ba756ac3e7edf2b9a4028b7649ece754, 1482e7fdbab29c3e8a2f3ccd1c6ddd48a54c06b0, 14d031138fb0aad2432cadf2e0d241ca75b2dfbb, 1970f6c17567d56c3e7840fe33a6959dd887fca2, 1992336a5d752187c979e24a95a871d8932ade6d, 1cb7e2ab7012990bd5051120c3ef8a438035aa88, 1fb9b8115d74cf38d6a90b9049c73ea6eb743643, 326dc3ca63d10968054153305a9564fac2a37ba3, 5166d17d8e9a91a3a36b5edaf168699b03bb13de, 5d1229ece791a55823f60298cb7dcf9c0494f3ee, 62383813a6ca85fc9c70051c361e0273e135593d, 6bf35f44a2267755c2646c89c836bd618c4e964c, 6e530c9a3eddabc29c2f8f6aca6c6f786ae052d6
GorjolEcho	Domain	library-store.camdvr[.]org, fuschia-rhinestone.cleverapps[.]io, filemanager.theworkpc[.]com
	IPv4	144.217.129[.]176
CharmPower	SHA256	b79d28fe5e3c988bb5aadb12ce442d53291dbb9ede0c7d9d64eec078beba5585, 9777f106ac62829cd3cfdbc156100fe892cfc4038f4c29a076e623dc40a60872, 977cf5cc1d0c61b7364edcf397e5c67d910fac628c6c9a41cf9c73b3720ce67f, 823ffbcc62bd3296957a47fbf8c238949584996911e71d5140a25d0a8f6abd80
NokNok	SHA256	1fb7f1bf97b72379494ea140c42d6ddd53f0a78ce22e9192cfba3bae58251da4, e98afa8550f81196e456c0cd4397120469212e190027e33a1131f602892b5f79,

Attack Name	TYPE	VALUE
NokNok	SHA256	5dc7e84813f0dae2e72508d178aed241f8508796e59e33da63bd6b481f507026, b6916b5980e79a2d20b4c433ad8e5e34fe9683ee61a42b0730effc6f056191eb, acfa8a5306b702d610620a07040262538dd59820d5a42cf01fd9094ce5c3487c
	Domain	library-store[.]camdvr[.]org
	IPv4	144.217.129[.]176

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 10, 2023 • 5:00 AM

More at www.hivepro.com