Date of Publication
May 22, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

15 to 21 MAY 2023

Table Of Contents

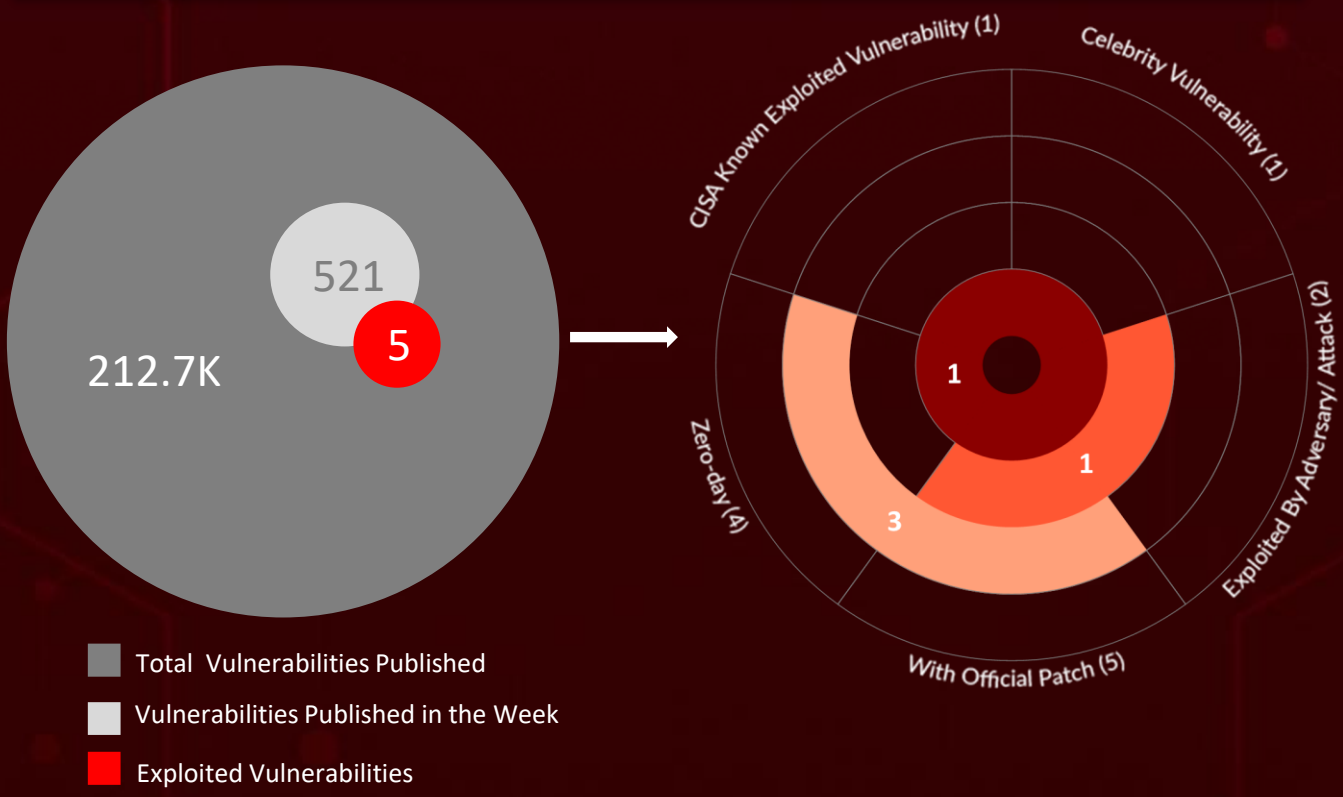
Summary

HiveForce Labs recently made significant discoveries in the field of cybersecurity threats. In the past week, they uncovered a total of **eight** attacks that were executed, taking advantage of **five** different vulnerabilities across various systems. What's interesting is that **four** of these vulnerabilities are **zero-day** vulnerabilities.

Furthermore, HiveForce Labs identified **five** different adversaries who were actively carrying out these attacks. In one case, the **8220 gang** was found to be exploiting a vulnerability that was six years old in order to deploy cryptominers.

Additionally, a new threat actor called **Water Orthrus** was observed deploying **CopperStealth** and **CopperPhish**. Another newcomer, **Lancefly APT**, was seen utilizing **Merdoor** and **ZXShell** for their attacks.

To add to the list of incidents, a new worm called **Xworm** was observed exploiting **Follina**.



High Level Statistics

8
Attacks Executed

5
Vulnerabilities Exploited

5
Adversaries in Action

- Merdoor
- ZXShell
- CopperStealth
- CopperPhish
- Rancoz
- Xworm
- Minas
- CryptNet

- CVE-2017-3506
- CVE-2022-30190
- CVE-2023-32409
- CVE-2023-28204
- CVE-2023-32373

- Lancefly APT
- RA Group
- Water Orthrus
- 8220 Gang
- Camaro Dragon

Insights

Rancoz

A New ransomware on rise

Xworm

targets Germany companies with **Follina**

Camaro Dragon

targets Europe by exploiting TP-Link routers

8220 Gang

Exploits Oracle WebLogic Server vulnerability to deploy cryptominers

Water Orthrus

Targets China to deploy CopperStealth and CopperPhish

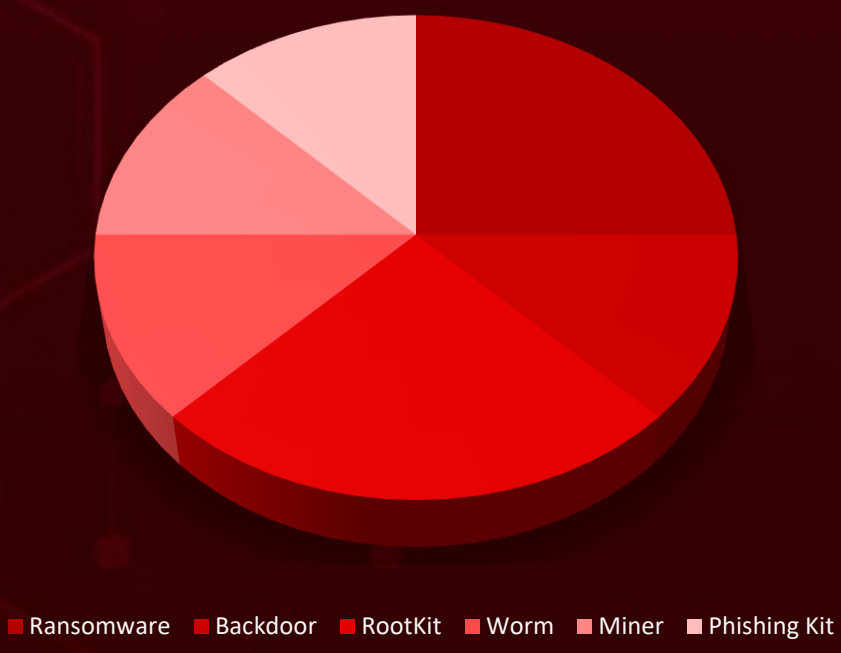
3

Vulnerabilities in macOS exploited-in-the-wild

2

New threat actors came into limelight

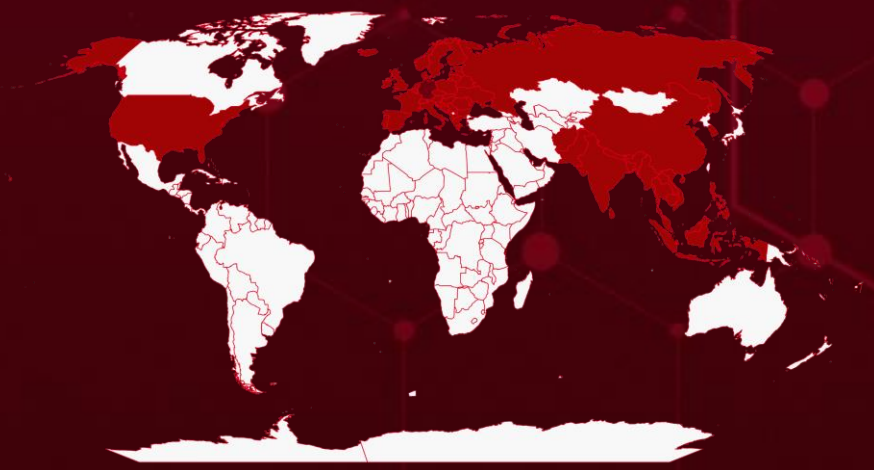
Threat Distribution



Targeted Countries

Most

Least

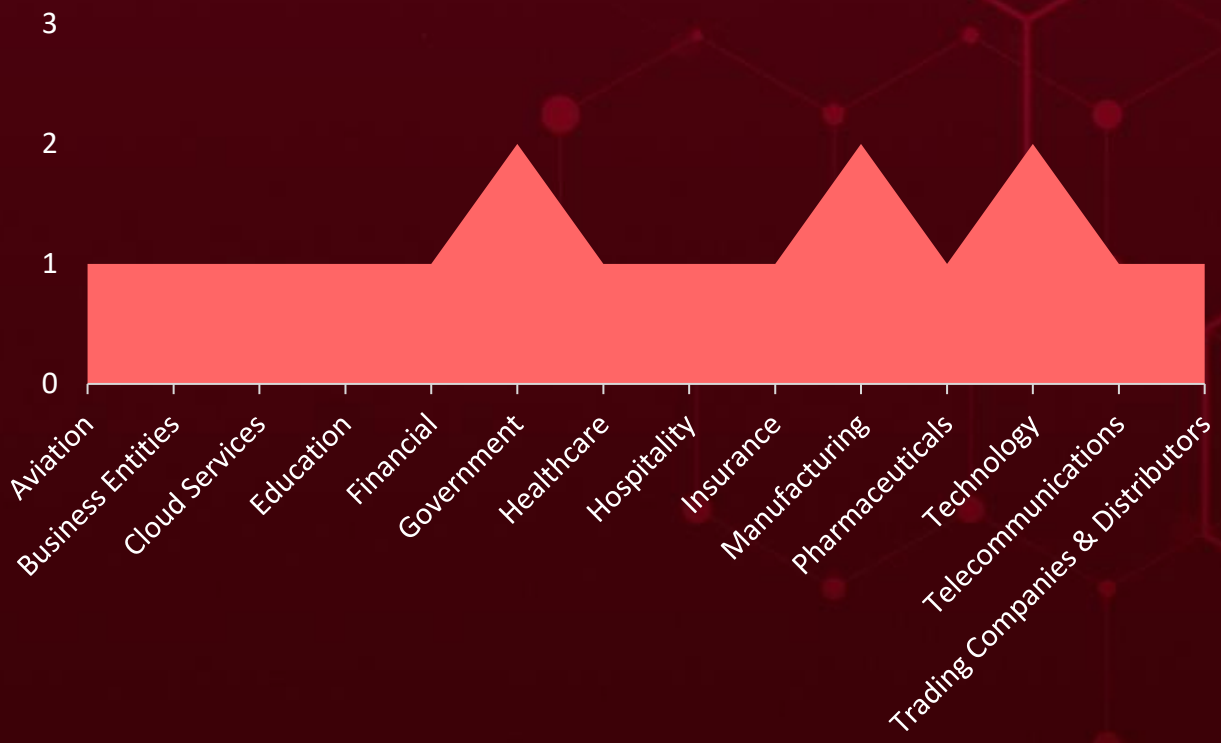


Countries
Germany
Vietnam
Romania
Myanmar
Andorra
Spain
Austria
Malta
Bangladesh
Pakistan
Belarus
Singapore
Belgium
Thailand
Bhutan
Malaysia
Bosnia and Herzegovina
Monaco
Brunei
Albania
Bulgaria
Poland
Cambodia
San Marino
China

Countries
France
Nepal
Netherlands
North Macedonia
Norway
Greece
Philippines
Holy See
Portugal
Hungary
Russia
Iceland
Serbia
India
Slovakia
Indonesia
South Korea
Ireland
Sri Lanka
Italy
Switzerland
Laos
Ukraine
Latvia
United States

Countries
Slovenia
Croatia
Sweden
Czech Republic
United Kingdom
Denmark
Afghanistan
East Timor
Maldives
Estonia
Moldova
Finland
Montenegro
Liechtenstein
Lithuania
Luxembourg
France
Nepal
Netherlands

Targeted Industries



TOP MITRE ATT&CK TTPS

T1071 Application Layer Protocol

T1059 Command and Scripting Interpreter

T1105 Ingress Tool Transfer

T1027 Obfuscated Files or Information

T1082 System Information Discovery

T1574 Hijack Execution Flow

T1566 Phishing

T1057 Process Discovery

T1070 Indicator Removal

T1055 Process Injection

T1204 User Execution

T1083 File and Directory Discovery

T1497 Virtualization/ Sandbox Evasion

T1490 Inhibit System Recovery

T1140 Deobfuscate/ Decode Files or Information

T1056 Input Capture

T1486 Data Encrypted for Impact

T1036 Masquerading

T1068 Exploitation for Privilege Escalation

T1560 Archive Collected Data

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Merdoor	Merdoor is Stealthy backdoor with diverse communication methods and capabilities for unauthorized access and control	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Covert system infiltration and control	-
ASSOCIATED ACTOR			**PATCH LINK**
Lancefly APT			-
IOC TYPE	**VALUE**		
SHA256	13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581 8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead 8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38 89e503c2db245a3db713661d491807aab3d7621c6aff00766bc6add892411ddc c840e3cae2d280ff0b36eec2bf86ad35051906e484904136f0e478aa423d7744		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ZXShell	The ZXShell rootkit was first reported by Cisco in 2014, but it has since undergone updates and continued development, as evidenced by its usage by a group called Lancefly.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Unauthorized system access and control	-
ASSOCIATED ACTOR			**PATCH LINK**
Lancefly APT			-
IOC TYPE	**VALUE**		
SHA256	1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7 180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221 592e237925243cf65d30a0c95c91733db593da64c96281b70917a038da9156ae 929b771eabef5aa9e3fba8b6249a8796146a3a4febfd4e992d99327e533f9798		

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
CopperStealth	CopperStealth deploys a rootkit to inject payloads into system processes, enabling the execution of additional tasks while blocking access to blacklisted registry keys and certain executables and drivers.	via pay-per-install (PPI) networks	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Rootkit		Stealthy system infiltration, payload injection, and access restrictions	-
ASSOCIATED ACTOR			**PATCH LINK**
Water Orthrus			-
IOC TYPE	**VALUE**		
SHA256	293a2adf60a94437cc0f92545b7caabdaed0a63007b51e2b3d449cdb1e00f5a8 6c3995155e0e5cbb17e6f71b8d8b89d4dfc77849e869da7901a79053e8e8232b 5558eaebeeeb4c5c731b531305e7c97c9cf1b1449b0466f46430aa0549c256e9 ad5f59c497f423a07cfb4affc82aac408eafeeefef22f8ba25cabff2ff991754 636772857bd9b88d5b530586c7008f48e61ec429fb50a82019d0505dcf994930		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CopperPhish	CopperPhish is a phishing kit that employs multiple persistence methods and utilizes downloaders such as PrivateLoader to distribute various types of malware.	Via a PrivateLoader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Phishing kit		Phishing risk, credential theft, malware distribution	-
ASSOCIATED ACTOR			**PATCH LINK**
Water Orthrus			-
IOC TYPE	**VALUE**		
SHA256	8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e 39c9f743528eb317340cdd53a65630785b1168f6f0a6b253ae2518fb450f0b81 28d1d1c6fb23ef5f92b16e2701c49bb34b4a81af11f95ff5674d291c5ffb3b28 07cccf04854a58e43a5043e240b662f84ac512b2d2432b1b7e4cd5465d1dde33 bff741d972e1dac7fa1197ac9365106b49bd07cea868d69c660aa569fe75f005		

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
Rancoz	Rancoz ransomware is a newly discovered variant that exhibits similarities to Vice Society ransomware. It employs advanced techniques to encrypt victims' files and extract ransom payments.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	8d9f3e223f8d5e350b87dc0908fee0a5		
SHA1	9fe3060e5cbe3a9ab6c3fb3dee40bd6cd385a6f6		
SHA256	b95a4443bb8bff80d927ac551a9a5a5cfac3e3e03a5b5737c0e05c75f33ad61e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Xworm	XWORM is a notorious worm malware known for its advanced evasion capabilities and the availability of cracked versions in the underground criminal marketplace.	Via Follina	CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Worm		Widespread infection, evasion, and facilitation of cybercrime	Microsoft Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190
IOC TYPE	**VALUE**		
SHA256	3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16		

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
Minas	Minas is a multi-stage cryptocurrency miner with a concealed presence. It evades detection through encryption, randomization, and persistence techniques, showcasing determined network compromise.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Miner		Financial loss, compromised security, performance impact	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	08da41489b4b68565dc77bb9acb1ecb4 06fe9ab0b17f659486e3c3ace43f0e3a f38a1b6b132afa55ab48b4b7a8986181 63e0cd6475214c697c5fc115d40327b4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CryptNet	CryptNet is a new ransomware-as-a-service group that employs data exfiltration and .NET code. Currently, it has two victims listed on its data leak site.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data extraction, file encryption, ransom demands, compromised backups, and financial consequences	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	2e37320ed43e99835caa1b851e963ebbf153f16cbe395f259bd2200d14c7b775 1cc7283ee218081f2f056bd2ec70514e86b8dcb921342dc9aed69e7480dec18e		

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-2017-3506	✗ ZERO-DAY	Oracle WebLogic Server: 12.1.3.0.0 - 12.2.1.2	8220 Gang
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:a:oracle:oracle_weblogic_server:*:*:*:*:*:*:*:*	-
Denial of service Vulnerability in Oracle WebLogic Server	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1498: Network Denial of Service	https://www.oracle.com/security-alerts/cpuapr2017.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	✓ ZERO-DAY	Windows Server: 2008 – 2022; Windows: 11 - 11 21H2, 10 - 10 S, 8.1 - 8.1 RT, 8 - 8 RT, 7 - 7 SP1	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Xworm
Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability **(Follina)**	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	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-2023-32409	 ZERO-DAY	macOS Ventura before 13.4	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macOS:*:*:*:*:*:*	-
Apple Sandbox Escape Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1497: Virtualization/Sandbox Evasion	https://support.apple.com/en-us/HT213758

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-28204	 ZERO-DAY	macOS Ventura before 13.4	-
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macOS:*:*:*:*:*:*	-
Apple Out-of-bounds Read Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125	T1005: Data from Local System	https://support.apple.com/en-us/HT213758

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-32373		macOS Ventura before 13.4	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:apple:macOS:*:*:*:*:*:*	-
Apple use-after-free Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1574: Hijack Execution Flow	https://support.apple.com/en-us/HT213758

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Lancefly APT	China	Government, aviation, education, and telecoms	South and Southeast Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Merdoor backdoor, ZXShell rootkit	-
TTPs			
T1057: Process Discovery; T1014: Rootkit; T1219: Remote Access Software; T1059: Command and Scripting Interpreter; T1112: Modify Registry; T1021: Remote Services; T1003: OS Credential Dumping; T1056: Input Capture; T1574: Hijack Execution Flow; T1055: Process Injection; T1090: Proxy; T1056.001: Keylogging; T1574.001: DLL Search Order Hijacking; T1218: System Binary Proxy Execution; T1027: Obfuscated Files or Information; T1566: Phishing; T1110: Brute Force; T1059.001: PowerShell; T1218.011: Rundll32; T1003.001: LSASS Memory; T1036: Masquerading; T1560.001: Archive via Utility; T1021.002: SMB/Windows Admin Shares			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 RA Group	Unknown	Manufacturing, Wealth Management, Insurance Providers, and Pharmaceuticals	United States and South Korea
	MOTIVE		
	Information theft and espionage; Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
T1083: File and Directory Discovery; T1490: Inhibit System Recovery; T1496: Resource Hijacking; T1552: Unsecured Credentials; T1560: Archive Collected: Data; T1573: Encrypted Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Water Orthrus	Unknown	-	China
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-

TTPs
T1566: Phishing; T1195: Supply Chain Compromise; T1218: System Binary Proxy Execution; T1218.002: Control Panel; T1204: User Execution; T1202: Indirect Command Execution; T1070: Indicator Removal; T1033: System Owner/User Discovery; T1041: Exfiltration Over C2 Channel; T1071: Application Layer Protocol; T1078: Valid Accounts; T1068: Exploitation for Privilege Escalation; T1542: Pre-OS Boot; T1542.003: Bootkit; T1027: Obfuscated Files or Information; T1020: Automated Exfiltration; T1087: Account Discovery; T1110: Brute Force; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1082: System Information Discovery; T1552: Unsecured Credentials; T1552.001: Credentials In Files; T1021: Remote Services; T1056: Input Capture; T1046: Network Service Discovery; T1047: Windows Management Instrumentation

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 8220 Gang (8220 Mining Group)	China	Technology, Cloud Services	Worldwide
	MOTIVE		
	Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-3506	MgBot	Oracle WebLogic Server

TTPs
T1140: Deobfuscate/Decode Files or Information; T1105: Ingress Tool Transfer; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1071: Application Layer Protocol; T1204.002: Malicious File; T1071.001: Web Protocols; T1566: Phishing; T1204: User Execution; T1190: Exploit Public-Facing Application; T1525: Implant Internal Image; T1132: Data Encoding; T1055: Process Injection; T1132.001: Standard Encoding; T1027: Obfuscated Files or Information; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1027.010: Command Obfuscation; T1055.002: Portable Executable Injection; T1620: Reflective Code Loading

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
	China	Foreign Affairs Entities	Europe
	MOTIVE		
	Information theft and Espionage; Sabotage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Camaro Dragon	-	-	-
TTPs			
T1566: Phishing; T1189: Drive-by Compromise; T1542: Pre-OS Boot; T1542.001: System Firmware; T1542.003: Bootkit; T1095: Non-Application Layer Protocol; T1210: Exploitation of Remote Services			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerability** and block the indicators related to the threat actor **Lancefly APT, RA Group, Water Orthrus, 8220 Gang, and Camaro Dragon** and malware **Merdoor, ZXShell, CopperStealth, CopperPhish, Rancoz, Xworm, Minas, and CryptNet.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Running a Scan to discover the assets impacted by the **five exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Lancefly APT, RA Group, Water Orthrus, 8220 Gang, and Camaro Dragon** and malware **Merdoor, ZXShell, CopperStealth, CopperPhish, Rancoz, Xworm, Minas, and CryptNet** in Breach and Attack Simulation(BAS).

Threat Advisories

XSS Vulnerability in Popular WordPress Plugin Affects 2 Million Sites

Lancefly APT Group Deploys Custom Backdoor ‘Merdoor’ in Targeted Attacks

RA Group's Custom Ransomware Hits US & South Korea

Water Orthrus Targets Chinese Users with CopperStealth and CopperPhish

Rancoz Ransomware Employs Advanced Techniques to Encrypt Victims' Files

8220 Gang Exploiting Vulnerabilities in Cloud Environments for Cryptocurrency Mining

MEME#4CHAN The Unconventional Phishing Campaign Spreading Xworm

Unveiling the Minas Miner's Deceptive Tactics

Apple Patches Three Exploited Zero-Day Vulnerabilities in macOS

Camaro Dragon Targets European Foreign Affairs with Malicious Firmware Implant

CryptNet A Novel Ransomware-as-a-Service

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
Merdoor	SHA256	13df2d19f6d2719beeff3b882df1d3c9131a292cf097b27a0ffca5f45e139581 8f64c25ba85f8b77cfba3701bebde119f610afef6d9a5965a3ed51a4a4b9dead 8e98eed2ec14621feda75e07379650c05ce509113ea8d949b7367ce00fc7cd38 89e503c2db245a3db713661d491807aab3d7621c6aff00766bc6add892411ddc c840e3cae2d280ff0b36eec2bf86ad35051906e484904136f0e478aa423d7744 5f16633dbf4e6ccf0b1d844b8ddfd56258dd6a2d1e4fb4641e2aa508d12a5075 ff4c2a91a97859de316b434c8d0cd5a31acb82be8c62b2df6e78c47f85e57740 14edb3de511a6dc896181d3a1bc87d1b5c443e6aea9eeae70dbca042a426fcf3 db5deded638829654fc1595327400ed2379c4a43e171870cfc0b5f015fad3a03 e244d1ef975fcebb529f0590acf4e7a0a91e7958722a9f2f5c5c05a23dda1d2c f76e001a7ccf30af0706c9639ad3522fd8344ffbdf324307d8e82c5d52d350f2 dc182a0f39c5bb1c3a7ae259f06f338bb3d51a03e5b42903854cdc51d06fced6 fa5f32457d0ac4ec0a7e69464b57144c257a55e6367ff9410cf7d77ac5b20949 fe7a6954e18feddeeb6fcdaaa8ac9248c8185703c2505d7f249b03d8d8897104

Attack Name	TYPE	VALUE
Merdoor	SHA256	f3478ccd0e417f0dc3ba1d7d448be8725193a1e69f884a36a8c97006bf0aa0f4 750b541a5f43b0332ac32ec04329156157bf920f6a992113a140baab15fa4bd3 9f00cee1360a2035133e5b4568e890642eb556edd7c2e2f5600cf6e0bdcd5774 a9051dc5e6c06a8904bd8c82cdd6e6bd300994544af2eed72fe82df5f3336fc0 d62596889938442c34f9132c9587d1f35329925e011465c48c94aa4657c056c7 f0003e08c34f4f419c3304a2f87f10c514c2ade2c90a830b12fdf31d81b0af57 139c39e0dc8f8f4eb9b25b20669b4f30ffcbe2197e3a9f69d0043107d06a2cb4 11bb47cb7e51f5b7c42ce26cbff25c2728fa1163420f308a8b2045103978caf5 0abc1d12ef612490e37eedb1dd1833450b383349f13ddd3380b45f7aaabc8a75 341d8274cc1c53191458c8bbc746f428856295f86a61ab96c56cd97ee8736200
ZXShell	SHA256	1f09d177c99d429ae440393ac9835183d6fd1f1af596089cc01b68021e2e29a7 180970fce4a226de05df6d22339dd4ae03dfd5e451dcf2d464b663e86c824b8e a6020794bd6749e0765966cd65ca6d5511581f47cc2b38e41cb1e7fddaa0b221 592e237925243cf65d30a0c95c91733db593da64c96281b70917a038da9156ae 929b771eabef5aa9e3fba8b6249a8796146a3a4febfd4e992d99327e533f9798 009d8d1594e9c8bc40a95590287f373776a62dad213963662da8c859a10ef3b4 ef08f376128b7afcd7912f67e2a90513626e2081fe9f93146983eb913c50c3a8 ee486e93f091a7ef98ee7e19562838565f3358caeff8f7d99c29a7e8c0286b28 32d837a4a32618cc9fc1386f0f74ecf526b16b6d9ab6c5f90fb5158012fe2f8c d5df686bb202279ab56295252650b2c7c24f350d1a87a8a699f6034a8c0dd849
CopperStealth	SHA256	8a21eae144a23fffd35f8714964ff316caaa37fe464e8bbc143f4485119b5575 293a2adf60a94437cc0f92545b7caabdaed0a63007b51e2b3d449cdb1e00f5a8

Attack Name	TYPE	VALUE
CopperStealth	SHA256	ad5f59c497f423a07cfb4affc82aac408eafeeefef22f8ba25cabff2ff991754 636772857bd9b88d5b530586c7008f48e61ec429fb50a82019d0505dcf994930 7246dbf235f66034bd7042408f01b8670c3f45d39082fcbf5b893d7952614833 73fd83a9eb267fed5a3178b75a9bff0bac9e0864daed830fddf6a8686c286cbb 7fd6cb3e1648dd9d1994c65762826772ae32dc58fbc7ac51179a0b3526f1395f e3f31eabaa0b3bebe0c5152fc6097a8fbf1c6fd9e57d06fe8e9bd8860e8f07a6 033ba1740ba105bf4a5081f438f46f1d7ad17a175aab132bd844edcf8e30949f ed88b019b3a8346c89aaf6ba7ce6c6be0b9a88c121312f3db9b6ebd776a9af5a ecdd5adb40297ec29c0e8a8f50223069db3d32c2a1d223adfb52c3a695d41fa2 f916f4d1d8c1df0d31b8d18b7c94109b4303412880538f64ec3eb2e257732ead 53f4306d30b4f7b731c0cd7be6df39f02613fb4c0e9b5aa85f754e145dca080c 139f8412a7c6fdc43dcfbbcdba256ee55654eb36a40f338249d5162a1f69b988 5b932eab6c67f62f097a3249477ac46d80ddccdc52654f8674060b4ddf638e5d 6994b32e3f3357f4a1d0abe81e8b62dd54e36b17816f2f1a80018584200a1b77 32882949ea084434a376451ff8364243a50485a3b4af2f2240bb5f20c164543d 50819a1add4c81c0d53203592d6803f022443440935ff8260ff3b6d5253c0c76 770f33259d6fb10f4a32d8a57d0d12953e8455c72bb7b60cb39ce505c507013a 86047bb1969d1db455493955fd450d18c62a3f36294d0a6c3732c88dfbcc4f62 bb2422e96ea993007f25c71d55b2eddfa1e940c89e895abb50dd07d7c17ca1df 06c5ebd0371342d18bc81a96f5e5ce28de64101e3c2fd0161d0b54d8368d2f1f 6661320f779337b95bbbe1943ee64afb2101c92f92f3d1571c1bf4201c38c724 f9f2091fccb289bcf6a945f6b38676ec71dedb32f3674262928ccaf840ca131a E6f764c3b5580cd1675cbf184938ad5a201a8c096607857869bd7c3399df0d12

Attack Name	TYPE	VALUE
CopperStealth	SHA256	e1cb86386757b947b39086cc8639da988f6e8018ca9995dd669bdc03c8d39d7d 4734a0a5d88f44a4939b8d812364cab6ca5f611b9b8ceebe27df6c1ed3a6d8a4 ea50f22daade04d3ca06dedb497b905215cba31aae7b4cab4b533fda0c5be620 fa9abb3e7e06f857be191a1e049dd37642ec41fb2520c105df2227fcac3de5d5 f936ec4c8164cbd31add659b61c16cb3a717eac90e74d89c47afb96b60120280 a292fd3792ef81f3a3afd73c5b19878677e0293528e646e244ef50a36c4a0fb2 8b141803aeaa4f696fb19711d45a2628c73476c893ac1ba7967eb8d84862ea9a ac4bcb31d35428d8147d413d3354b9fdf70d9e9f3463ead04783805fdd306d86 04d2cb7d5f0e28797c1fde9036f06535040c223ecd66828e21c55971241adbbf bf5ae3846ada31fdf91f7d9c03c54dd10598571a5a24ed96c582a6a6fe20006f e257b8efdb3719bf21ed15d5abb30b0cbdbf9027a3db17ad0baca319eec13889 49337a65b01dd6e634456bca17ca28118a8126e4706d92b4673afe1c9cfea638 4934e4990928dbec77463f383b693f4f4a9fc40256e72a36e98c292722b84cf1 5558eaebeeeb4c5c731b531305e7c97c9cf1b1449b0466f46430aa0549c256e9 6c3995155e0e5cbb17e6f71b8d8b89d4dfc77849e869da7901a79053e8e8232b
	URLs	hxxp[:]//cnzz.fnxitong.com[:]99/gg.html hxxp[:]//chromei.org/tj/ hxxp[:]//so.fnxitong.com[:]99/tongji.php?u=e002 hxxp[:]//so.fnxitong.com[:]99/tongji.php?u=001 hxxp[:]//cnzz.fnxitong.com[:]99/gg.txt hxxp[:]//chromei.org/encode.txt hxxp[:]//up.chromei.org/e002.txt hxxp[:]//www.chromel.cn/encode.txt
CopperPhish	URLs	hxxps[:]//0zpt4.za.com/ hxxps[:]//3hdr0.za.com/
	SHA256	48211c6f957c2ad024441be3fc32aecd7c317dfc92523b0a675c0cfec86ffdd9 8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e

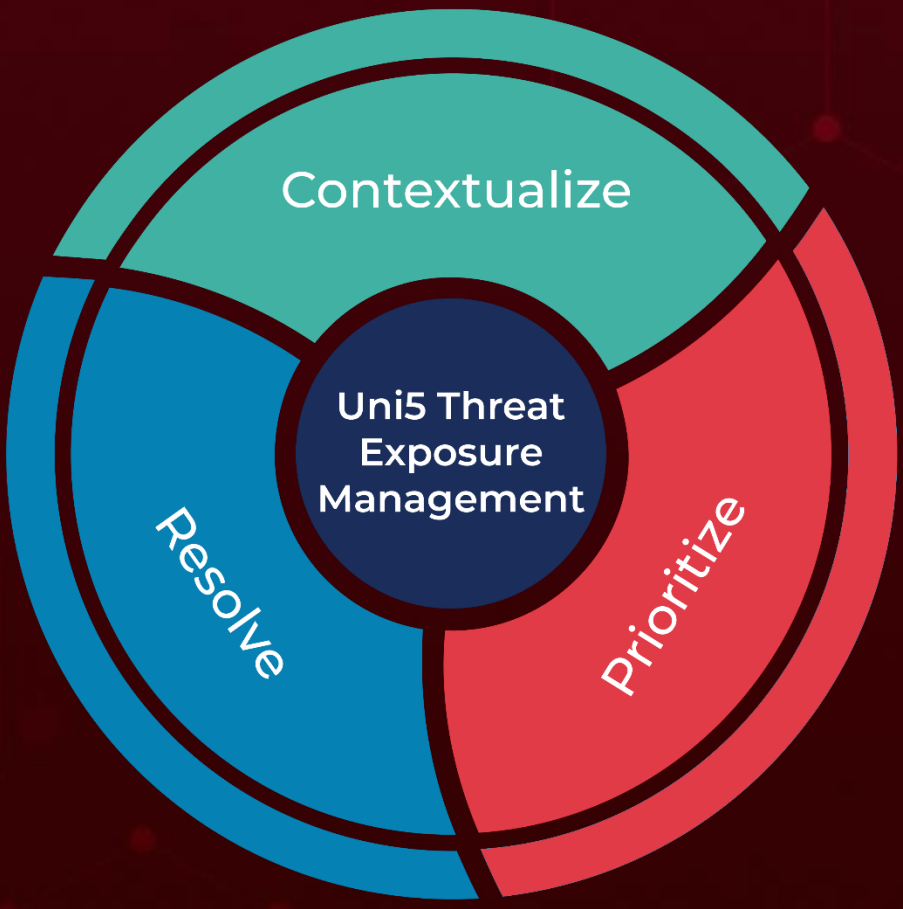
Attack Name	TYPE	VALUE
CopperPhish	SHA256	28d1d1c6fb23ef5f92b16e2701c49bb34b4a81af11f95ff5674d291c5ffb3b28 07cccf04854a58e43a5043e240b662f84ac512b2d2432b1b7e4cd5465d1dde33 bff741d972e1dac7fa1197ac9365106b49bd07cea868d69c660aa569fe75f005 036a689038dfaa195c899d57a4d3fdcf5f99b91bdbf9739a4d05f9bd1dcfe15e 65a632de69bcb62c8f344a9cc0951d3c599301ca6d8aed66bbdab9f1b977799a 971259ae3eb7dc843c6872b22154e5cf74e48ca35fb895145df63fa50e8e8792 58eb8b6fd34406316438e2e17ed3c44b6c26695b28c71db7b062a63a116ee33b 0a596289cb9c6dcb065d96fb33c1e9509f62ff42b00a0d679bb8b9e64dce8ea5 fcf49a50a3b86adeea6b1cfbb0d86dfed774673a5900570878197f822f6f2126 8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e 6f52f36d84ea04d00f307d5aafedcda98118d140c1ac1af0525ecb374c0f5cf2 688de5bbd2cb1e5556304002c1b7f5fdfe147251217f93b8733017161a834fa5 1a1a70fd2c5a012c4e8547713a3abf1dc2dbd05a81ab1fcca4ab1ad71ad36979 15430150c081728440618aac046cc1d50a4391b55fa7f8fa66325d9b462e57c3 acac571f03810d6e8408d4df25fda741cf492c7d842113155034da1f871c10ea f340e0ef5f90024b9626a83c2c1eed2011417372073088169d7c2c7ec842f228 699873a949ca1e3a15f8428d1e28e3bdf7b95ec1606e10785f3f51b118e2669e dda6bc4618cd6f723d6ad5f45f171a075c208b5b2693a35f24dd6607a3f167f0 7e3f5a8f6fc490736ba7e04389cf83d9ea47a5079e63901300e2dec79c1f77ab 1fd3c8d5ec7043fb01ea9d9985075d0b014f7153e88cd56d267fb10f1f979a1c 50fae4fe4a258854c629a3dd24262e1a35a09d317f2d1b7bb31d5a81a237c258 a5f00b52c99b951009334c6c52524c4e494c8ee77da1340a623a35a35e96b935 00ff5f2af303cee7ede802b8a013f415bc69caa023330143df746b9b23aa60fd dd3ffec50a0ef7434b85f85330cebb9a2afa2123bed19ac39179806bacf48775

Attack Name	TYPE	VALUE
Rancoz	MD5	8d9f3e223f8d5e350b87dc0908fee0a5
	SHA1	9fe3060e5cbe3a9ab6c3fb3dee40bd6cd385a6f6
	SHA256	b95a4443bb8bff80d927ac551a9a5a5cfac3e3e03a5b5737c0e05c75f33ad61e
Xworm	SHA256	3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16
Minas	MD5	08da41489b4b68565dc77bb9acb1ecb4 06fe9ab0b17f659486e3c3ace43f0e3a f38a1b6b132afa55ab48b4b7a8986181 63e0cd6475214c697c5fc115d40327b4
CryptNet	SHA256	2e37320ed43e99835caa1b851e963ebbf153f16cbe395f259bd2200d14c7b775 1cc7283ee218081f2f056bd2ec70514e86b8dcb921342dc9aed69e7480dec18e

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

May 22, 2023 . 6:30 AM

More at www.hivepro.com