Date of Publication
May 1, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

24 to 30 APRIL 2023

Table Of Contents

Summary

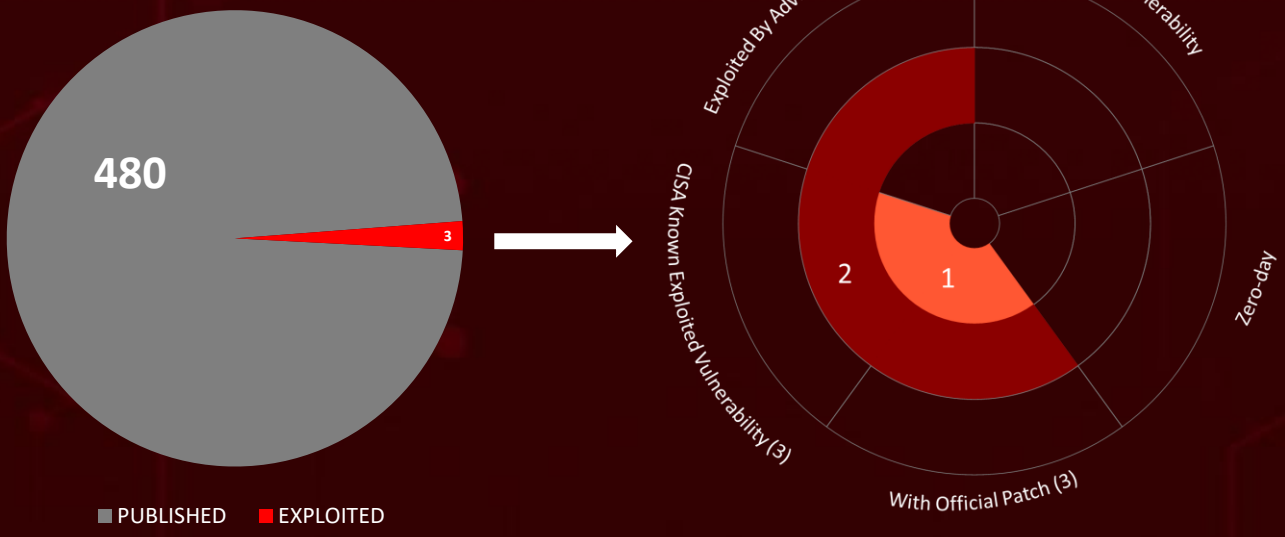
HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, they identified a total of **eight** attacks that were executed. These attacks were taking advantage of **three** different vulnerabilities in various systems. Additionally, HiveForce Labs identified **six** different adversaries that were actively carrying out these attacks.

Interestingly, all the **three** vulnerabilities are part of the known exploited vulnerability catalog by CISA.

Moreover, HiveForce Labs also found that **APT28** was exploiting a five-year-old vulnerability by deploying **Jaguar Tooth**.

Furthermore, they identified new Linux malware variants of the famous **PingPull** as well as a new macOS malware **RustBucket** surfaced online.

Apart from these threats, there was also a new ransomware strain named **CrossLock**. **Charming Kitten** was observed using a malware **BellaCiao** which is based on an Italian song. 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

3
Vulnerabilities Exploited

6
Adversaries in Action

- CrossLock
- Jaguar Tooth
- EvilExtractor
- MgBot
- BellaCiao
- PingPull
- VEILEDSIGNAL
- RustBucket

- CVE-2017-6742
- CVE-2023-27350
- CVE-2022-47966

- APT28
- Tomiris
- Daggerfly
- Charming Kitten
- Alloy Taurus
- BlueNoroff

Insights

EvilExtractor

A New Comprehensive Malware in Cybercrime

PaperCut Under the Radar:

Critical Security Vulnerabilities Exploited in the Wild

Daggerfly APT

Deploys New MgBot Plugins in African Telco Hack

APT28

Exploits Cisco Routers with Weak SNMP Strings to deploy **Jaguar Tooth** malware

After 2 Years

Russian-Speaking APT Group Tomiris Resurfaces

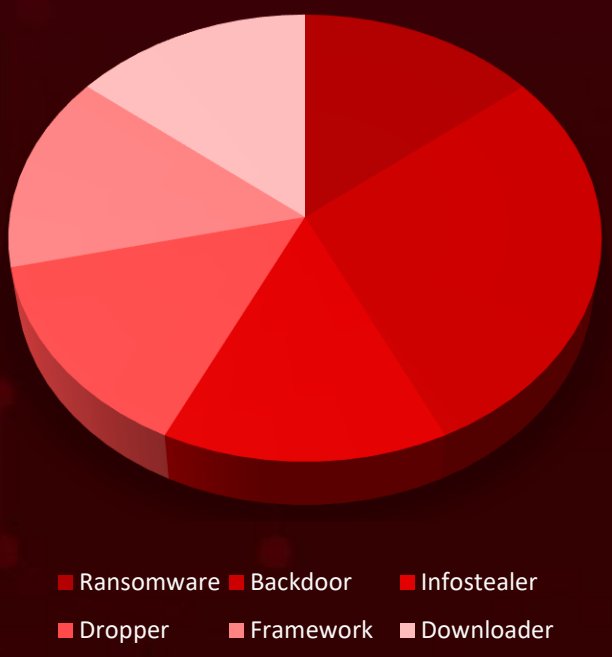
Charming Kitten APT

Unleashes Sophisticated **BellaCiao** Malware

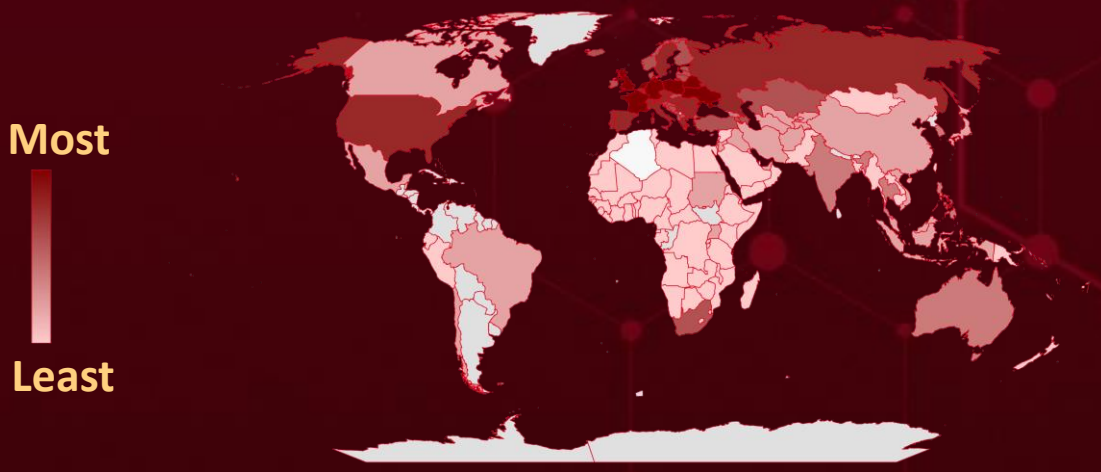
Alloy Taurus

Group Linked to Linux-Targeting **PingPull** Backdoor

Threat Distribution



Targeted Countries



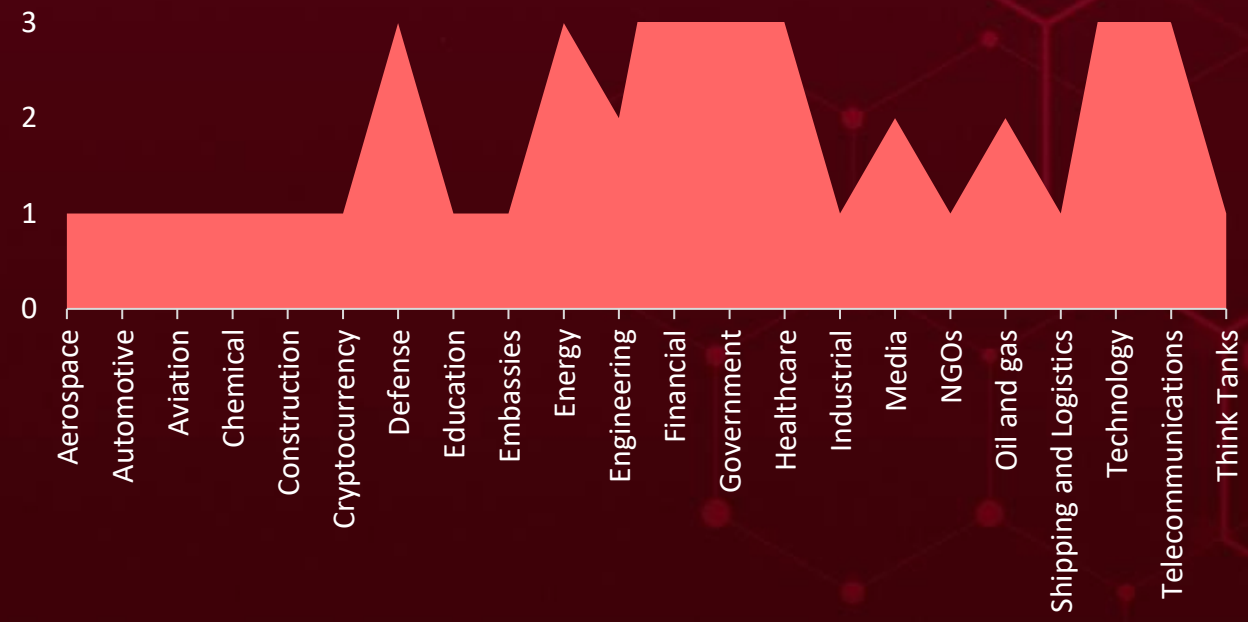
Countries
Germany
Netherlands
Ukraine
Belarus
Poland
France
UK
Austria
Serbia
Romania
Greece
Sweden
Hungary
Portugal
Switzerland
Russia
Bulgaria
Spain
Moldova
Belgium
Czech Republic
Italy
USA
Azerbaijan
Andorra
Liechtenstein
Latvia
Albania
Kazakhstan
Iceland
Lithuania
Bosnia and Herzegovina
Luxembourg
Slovenia
Malta
Croatia
Denmark
Armenia
Monaco
San Marino
Montenegro

Countries
Slovakia
Estonia
South Africa
North Macedonia
Ireland
Norway
Turkey
Finland
Thailand
Cyprus
Philippines
Georgia
Australia
India
South Korea
Holy See
Malaysia
Afghanistan
Iran
Chile
Iraq
Brazil
Israel
Canada
Japan
Mexico
Singapore
China
Sudan
Hong Kong
Brunei
Indonesia
UAE
Jordan
Tajikistan
Kyrgyzstan
Turkmenistan
Vatican City
Uganda
Vietnam
Uzbekistan

Countries
Burundi
Eritrea
Seychelles
Malawi
Tanzania
Guinea-Bissau
Sao Tome & Principe
Mali
Egypt
Central African Republic
Syria
Mauritania
Tunisia
Mauritius
Rwanda
Ghana
Senegal
Chad
Bahrain
Cabo Verde
Equatorial Guinea
Mongolia
Benin
Kenya
Taiwan
Morocco
Timor-Leste
Mozambique
Cambodia
Namibia
Botswana
Comoros
Djibouti
Gabon
Saudi Arabia
Gambia
DR Congo

Countries
Nigeria
Ecuador
Congo
Somalia
Côte d'Ivoire
Burma
Oman
Zambia
Pakistan
Eswatini
Palestine
Taipei
Papua
Burkina Faso
Peru
Libya
Kuwait
Togo
Bangladesh
Ethiopia
Guinea
Cameroon
Qatar
Algeria
Laos
Madagascar
Angola
New Guinea
New Zealand
Yemen
Lebanon
Zimbabwe
Lesotho
Liberia
Niger
Sierra Leone

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

T1190
Exploit Public-Facing Application

T1083
File and Directory Discovery

T1497
Virtualization/ Sandbox Evasion

T1518
Software Discovery

T1564
Hide Artifacts

T1056
Input Capture

T1588
Obtain Capabilities

T1036
Masquerading

T1095
Non-Application Layer Protocol

T1016
System Network Configuration Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
CrossLock	CrossLock ransomware, implemented in Go programming language, uses double extortion technique to encrypt and exfiltrate data, posing a significant threat to businesses and organizations.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data loss, unauthorized access, and infrastructure damage	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
MD5	9756b1c7d0001100fdde3efefb7e086f
SHA1	55de88118fe8abefb29dec765df7f78785908621
SHA256	495fbfecbcadb103389cc33828db139fa6d66bece479c7f70279834051412d72

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Jaguar Tooth	Jaguar Tooth is a non-persistent malware that exploits the patched SNMP vulnerability to collect device information, exfiltrate it over TFTP, and enable unauthenticated backdoor access to target Cisco IOS routers.	Via SNMP vulnerability in Cisco IOS routers	CVE-2017-6742
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Unknown		Obtain device information	Cisco IOS and IOS XE Software
ASSOCIATED ACTOR			**PATCH LINK**
			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

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
EvilExtractor	EvilExtractor is a novel type of malware that functions as an all-in-one stealer, allowing cybercriminals to extract sensitive information and files from Windows operating systems.	Via Phishing email campaign	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Infostealer		Data loss	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
IPV4	45[.]87[.]81[.]184 193[.]42[.]33[.]232		
Domain	evilextractor[.]com		
SHA256	352efd1645982b8d23a841107007c8b4b024eb6bb5d6b312e5783ce4aa62b685 023548a5ce0de9f8b748a2fd8c4d1ae6c924c40acbde32e9599c868115d11f4e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MgBot	MgBot is a modular malware framework that is actively maintained and equipped with various plugins, allowing attackers to gather extensive information from compromised machines, indicating that the attackers' primary objective was information-gathering.	Legitimate AnyDesk remote desktop software	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Framework		Data theft and espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
Daggerfly			-
IOC TYPE	**VALUE**		
SHA256	c89316e87c5761e0fc50db1214beb32a08c73d2cad9df8c678c8e44ed66c1dab 90e15eaf6385b41fcbf021ecbd8d86b8c31ba48c2c5c3d1edb8851896f4f72fe 706c9030c2fa5eb758fa2113df3a7e79257808b3e79e46869d1bf279ed488c36 017187a1b6d58c69d90d81055db031f1a7569a3b95743679b21e44ea82cfb6c7 cb8aede4ad660adc1c78a513e7d5724cac8073bea9d6a77cf3b04b019395979a		

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
BellaCiao	BellaCiao is a personalized dropper malware used to deliver other malware payloads, with samples tailored to specific victims and countries, and named after an Italian folk song.	Unknown	CVE-2022-47966
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Data loss, unauthorized access, and infrastructure damage	Zoho ManageEngine
ASSOCIATED ACTOR			**PATCH LINK**
Charming Kitten			https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html
IOC TYPE	**VALUE**		
MD5	284cdf5d2b29369f0b35f3ceb363a3d1 2daa29f965f661405e13b2a10d859b87 3fbea74b92f41809f46145f480782ef9 5a487c41efa2f3055d641591d601977c 7df50cb7d4620621c2246535dd3ef10c		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PingPull	The PingPull malware variant that targets Linux systems is linked to Alloy Taurus, and it communicates with a domain over HTTPS to receive encrypted commands for executing specific functions.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft and espionage	-
ASSOCIATED ACTOR			**PATCH LINK**
Alloy Taurus			-
IOC TYPE	**VALUE**		
SHA256	cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae 5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507 e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253		
IPV4	5.181.25[.]99 196.216.136[.]139		

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
VEILEDSIGNAL	VEILEDSIGNAL backdoor uses Windows named pipes for C2 communication and can execute shellcode.	Via trojanized X_Trader	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Compromise critical infrastructure and sensitive data	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	f8c370c67ffb3a88107c9022b17382b5465c4af3dd453e50e4a0bd3ae9b012ce 19442d9e476e3ef990ce57b683190301e946ccb28fc88b69ab53a93bf84464ae e185c99b3d1085aed9fda65a9774abd73ecf1229f14591606c6c59e9660c4345 cc4eedb7b1f77f02b962f4b05278fa7f8082708b5a12cacf928118520762b5e2		
URLs	hxxps[://]www.tradingtechnologies[.]com/trading/order-management		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RustBucket	RustBucket macOS malware family split into two stages, with the second stage application appearing as a legitimate PDF viewer but becoming malicious when a specific PDF is loaded.	Via PDF Viewer App	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Compromise critical infrastructure and sensitive data	-
ASSOCIATED ACTOR			**PATCH LINK**
BlueNoroff			-
IOC TYPE	**VALUE**		
MD5	dabb4372050264f389b8adcf239366860662ac52 0be69bb9836b2a266bfd9a8b93bb412b6e4ce1be e0e42ac374443500c236721341612865cd3d1eec ac08406818bbf4fe24ea04bfd72f747c89174bdb 72167ec09d62cdfb04698c3f96a6131dceb24a9c		

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-2017-6742	ZERO-DAY	Cisco IOS: 15.6.3 M1 - 16.5.1; Cisco IOS XE: 3.16.1aS	APT28
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco_systems:cisco_ios:*:*:*:*:*:*:*:*	Jaguar Tooth
Cisco SNMP Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-120	T1574: Hijack Execution Flow; T1499.004: Endpoint Denial of Service: Application or System Exploitation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170629-snmp

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-27350	ZERO-DAY	PaperCut MF: before 22.0.9; PaperCut NG: before 22.0.9	-
	AFFECTED CPE		ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:papercut:papercut_mf:*:*:*:*:*:*:*:*; cpe:2.3:a:papercut:papercut_ng:*:*:*:*:*:*:*:*;	-
PaperCut MF/NG Improper Access Control Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1505: Server Software Component	https://www.papercut.com/kb/Main/PO-1216-and-PO-1219

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2022-47966</td><td>  </td><td rowspan="2">Zoho ManageEngine Multiple Products</td><td rowspan="2">Charming Kitten</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>  </td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:zohocorp:manageengine:*:*:*:*:*:*:*:*</td><td rowspan="2">BellaCiao</td></tr>
<tr><td rowspan="3">Zoho ManageEngine Multiple Products Remote Code Execution Vulnerability</td><td>  </td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-20</td><td>T1574: Hijack Execution Flow; T1059: Command and Scripting Interpreter; T1027: Obfuscated Files or Information; T1499: Endpoint Denial of Service; T1090: Proxy</td><td>https://www.manageengine.com/security/advisory/CVE/cve-2022-47966.html</td></tr>
</table>

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
APT28(Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium , Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12 , ITG05, TAG-0700, UAC-0028, Grey-Cloud)</td><td>Russia</td><td rowspan="3">Automotive, Aviation, Chemical, Construction, Defense, Education, Embassies, Engineering, Financial, Government, Healthcare, Industrial, IT, Media, NGOs, Oil and gas, Think Tanks and Intelligence organizations.</td><td rowspan="3">Asia, Europe, North America, South America, Oceania, Africa</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>CVE-2017-6742</td><td>Jaguar Tooth</td><td>Cisco IOS and IOS XE Software</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1190: Exploit Public-Facing Application; T1078: Valid Accounts; T1078.001: Default Accounts; T1590: Gather Victim Network Information; T1556: Modify Authentication Process; T1601: Modify System Image; T1601.001: Patch System Image; T1048: Exfiltration Over Alternative Protocol; T1048.003: Exfiltration Over Unencrypted Non-C2 Protocol; T1020: Automated Exfiltration; T1119: Automated Collection; T1602: Data from Configuration Repository; T1602.002: Network Device Configuration Dump; T1018: Remote System Discovery; T1083: File and Directory Discovery; T1016: System Network Configuration Discovery: T1082: System Information Discovery</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Russia	Government and Diplomatic Entities	Commonwealth of Independent States (CIS)
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Tomiris	-	-	-
TTPs			
T1059: Command and Scripting Interpreter; T1068: Exploitation for Privilege Escalation; T1566: Phishing; T1027: Obfuscated Files or Information; T1189: Drive-by Compromise; T1041: Exfiltration Over C2 Channel; T1127: Trusted Developer Utilities Proxy Execution: T1110: Brute Force; T1105: Ingress Tool Transfer; T1049: System Network Connections Discovery			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	China	Telecommunication	South Africa
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
Daggerfly(Bronze Highland, Evasive Panda)	-	MgBot	-
TTPs			
T1012: Query Registry; T1016: System Network Configuration Discovery; T1018: Remote System Discovery; T1027: Obfuscated Files or Information; T1027.005: Indicator Removal from Tools; T1036: Masquerading; T1055: Process Injection; T1056: Input Capture; T1056.001: Keylogging; T1057: Process Discovery; T1070: Indicator Removal; T1070.004: File Deletion; T1070.006: Timestomp; T1082: System Information Discovery; T1083: File and Directory Discovery; T1106: Native API; T1112: Modify Registry; T1125: Video Capture; T1129: Shared Modules; T1497: Virtualization/Sandbox Evasion			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Charming Kitten (aka Magic Hound, APT 35, Cobalt Illusion, Cobalt Mirage, TEMP.Beanie, Timberworm, Tarh Andishan, TA453, Phosphorus, TunnelVision, UNC788, Yellow Garuda, Educated Manticore, Mint Sandstorm)	Iran	Defense, Energy, Financial, Government, Healthcare, IT, Oil and gas, Technology, Telecommunications	US, Europe, the Middle East, and India
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2022-47966	BellaCiao	Zoho ManageEngine Multiple Products
TTPs			
T1071.001: Web Protocols; T1071: Application Layer Protocol; T1190: Exploit Public-Facing Application; T1027: Obfuscated Files or Information; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1584: Compromise Infrastructure; T1203: Exploitation for Client Execution; T1083: File and Directory Discovery; T1059: Command and Scripting Interpreter; T1059.001: Power Shell; T1071.004: DNS; T1104: Multi-Stage Channels; T1505: Server Software Component; T1505.003: Web Shell; T1048: Exfiltration Over Alternative Protocol; T1505: Server Software Component; T1036: Masquerading; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Alloy Taurus (GALLIUM, Softcell, Phantom Panda)	China	Financial, Government & Telecommunications	Southeast Asia, Europe and Africa
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PingPull	-
TTPs			
T1059: Command and Scripting Interpreter; T1059.004: Unix Shell; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1027: Obfuscated Files or Information; T1027.005: Indicator Removal from Tools; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1082: System Information Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1071: Application Layer Protocol; T1095: Non-Application Layer Protocol; T1571: Non-Standard Port			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 

BlueNoroff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet)</td><td>North Korea</td><td rowspan="3">Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology and BitCoin exchange</td><td rowspan="3">Australia, Bangladesh, Belgium, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Netherlands, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime</td></tr>
<tr><td></td><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td></td><td>-</td><td>RustBucket</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1082: System Information Discovery; T1071: Application Layer Protocol; T1564: Hide Artifacts; T1564.001: Hidden Files and Directories; T1518: Software Discovery; T1518.001: Security Software Discovery; T1095: Non-Application Layer Protocol; T1573: Encrypted Channel; T1547: Boot or Logon Autostart Execution; T1070: Indicator Removal; T1070.006: Timestomp; T1222: File and Directory Permissions Modification: T1553: Subvert Trust Controls; T1553.002: Code Signing; T1083: File and Directory Discovery; T1566: Phishing; T1036: Masquerading</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerability** and block the indicators related to the threat actor **APT28, Tomiris, Daggerfly, Charming Kitten, Alloy Taurus and BlueNoroff** and malware **CrossLock, Jaguar Tooth, EvilExtractor, MgBot, BellaCiao, PingPull, VEILEDSIGNAL and RustBucket.**

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 **three exploited vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT28, Tomiris, Daggerfly, Charming Kitten, Alloy Taurus and BlueNoroff** and malware **CrossLock, Jaguar Tooth, EvilExtractor, MgBot, BellaCiao, PingPull, VEILEDSIGNAL and RustBucket** in Breach and Attack Simulation(BAS).

Threat Advisories

A New CrossLock Ransomware Threat with Cross-Platform Capabilities and Double Extortion Techniques

APT28's SNMP Attack on Cisco Routers

Critical PaperCut Security Vulnerabilities Actively Exploited in the Wild

New Tomiris APT Group Targets Governments

Malevolent EvilExtractor Stealer Attacks Strike Europe and US

Daggerfly APT Deploys MgBot to Target African Telecoms Organization

Charming Kitten Hackers Utilize New Tactics with BellaCiao Malware

New PingPull Malware Variant Targets Linux Systems

North Korean-Backed Group's Sparks X_Trader Supply Chain Attack

New macOS malware RustBucket attributed to North Korean group BlueNoroff

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
CrossLock	MD5	9756b1c7d0001100fdde3efefb7e086f
	SHA1	55de88118fe8abefb29dec765df7f78785908621
	SHA256	495fbfecbcadb103389cc33828db139fa6d66bece479c7f70279834051412d72
EvilExtractor	SHA256	352efd1645982b8d23a841107007c8b4b024eb6bb5d6b312e5783c e4aa62b685 023548a5ce0de9f8b748a2fd8c4d1ae6c924c40acbde32e9599c8681 15d11f4e 75688c32a3c1f04df0fc02491180c8079d7fdc0babed981f5860f22f5 e118a5e 826c7c112dd1ae80469ef81f5066003d7691a349e6234c8f8ca9637b 0984fc45 b1ef1654839b73f03b73c4ef4e20ce4ecdef2236ec6e1ca36881438b c1758dcd 17672795fb0c8df81ab33f5403e0e8ed15f4b2ac1e8ac9fef1fec4928 387a36d
	IPV4	45[.]87[.]81[.]184 193[.]42[.]33[.]232
	Domain	evilextractor[.]com

Attack Name	TYPE	VALUE
MgBot	SHA256	c89316e87c5761e0fc50db1214beb32a08c73d2cad9df8c678c8e44ed66c1dab 90e15eaf6385b41fcbf021ecbd8d86b8c31ba48c2c5c3d1edb8851896f4f72fe 706c9030c2fa5eb758fa2113df3a7e79257808b3e79e46869d1bf279ed488c36 017187a1b6d58c69d90d81055db031f1a7569a3b95743679b21e44ea82cfb6c7 cb8aede4ad660adc1c78a513e7d5724cac8073bea9d6a77cf3b04b019395979a 2dcf9e556332da2a17a44dfceda5e2421c88168aafea73e2811d65e9521c715c a6ed16244a5b965f0e0b84b21dcc6f51ad1e413dc2ad243a6f5853cd9ac8da0b ee6a3331c6b8f3f955def71a6c7c97bf86ddf4ce3e75a63ea4e9cd6e20701024 585db6ab2f7b452091ddb29de519485027665335afcdb34957ff1425ecc3ec4b 29df6c3f7d13b259b3bc5d56f2cdd14782021fc5f9597a3ccece51ffac2010a0 ea2be3d0217a2efeb06c93e32f489a457bdea154fb4a900f26bef83e2053f4fd 54198678b98c2094e74159d7456dd74d12ab4244e1d9376d8f4d864f6237cd79 d9eec27bf827669cf13bfdb7be3fdb0fdf05a26d5b74adecaf2f0a48105ae934 cb7d9feda7d8ebfba93ec428d5a8a4382bf58e5a70e4b51eb1938d2691d5d4a5 2c0cfe2f4f1e7539b4700e1205411ec084cbc574f9e4710ecd4733fbf0f8a7dc a16a70b0a1ac0718149a31c780edb126379a0d375d9f6007a6def3141bec6810 0bcdcc0515d30c28017fd7931b8a787feebe9ee3819aa2b758ce915b8ba40f99 C31b409b1fe9b6387b03f7aedeafd3721b4ec6d6011da671df49e241394da154 db489e9760da2ed362476c4e0e9ddd6e275a84391542a6966dbcda0261b3f30a 632cd9067fb32ac8fbbe93eb134e58bd99601c8690f97ca53e8e17dda5d44e0e C1e91a5f9cc23f3626326dab2dcdf4904e6f8a332e2bce8b9a0854b371c2b35 5a0976fef89e32ddcf62c790f9bb4c174a79004e627c3521604f46bf5cc7bea2 7bcff667ab676c8f4f434d14cfc7949e596ca42613c757752330e07c5ea2a453

Attack Name	TYPE	VALUE
MgBot	SHA256	3f75818e2e43a744980254bfdc1225e7743689b378081c560e824a36e0e0a195 1b8500e27edc87464b8e5786dc8c2beed9a8c6e58b82e50280cebb7f233bcde4 03bc62bd9a681bdcb85db33a08b6f2b41f853de84aa237ae7216432a6f8f817e ae39ced76c78e7c2043b813718e3cd610e1a8adac1f9ad5e69cf06bd6e38a5bd f6f6152db941a03e1f45d52ab55a2e3d774015ccb8828533654e3f3161cfcd21 2f4a97dc70f06e0235796fec6393579999c224e144adcff908e0c681c123a8a2 22069984cba22be84fe33a886d989b683de6eb09f001670dbd8c1b605460d454 7b945fb1bdeb27a35fab7c2e0f5f45e0e64df7821dd1417a77922c9b08acfdc3 e8be3e40f79981a1c29c15992da116ea969ab5a15dc514479871a50b20b10158 b5c46c2604e29e24c6eb373a7287d919da5c18c04572021f20b8e1966b86d585 53d2506723f4d69afca33e90142833b132ed11dd0766192a087cb206840f3692 26d129aaa4f0f830a7a20fe6317ee4a254b9caac52730b6fed6c482be4a5c79d b45355c8b84b57ae015ad0aebfa8707be3f33e12731f7f8c282c8ee51f962292 17dce65529069529bcb5ced04721d641bf6d7a7ac61d43aaf1bca2f6e08ead56 98b6992749819d0a34a196768c6c0d43b100ef754194308eae6aaa90352e2c13 6d5be3e6939a7c86280044eebe71c566b48981a3341193aa3aff634a3a5d1bbd 1cf04c3e8349171d907b911bc2a23bdb544d88e2f9b8fcc516d8bcf68168aede
BellaCiao	MD5	284cdf5d2b29369f0b35f3ceb363a3d1 2daa29f965f661405e13b2a10d859b87 3fbea74b92f41809f46145f480782ef9 5a487c41efa2f3055d641591d601977c 7df50cb7d4620621c2246535dd3ef10c 95c6fdc4f537bccca3079d94e65bc0b0 c450477ed9c347c4c3d7474e1f069f14 c6f394847eb3dc2587dc0c0130249337 e7149c402a37719168fb739c62f25585 f56a6da833289f821dd63f902a360c31

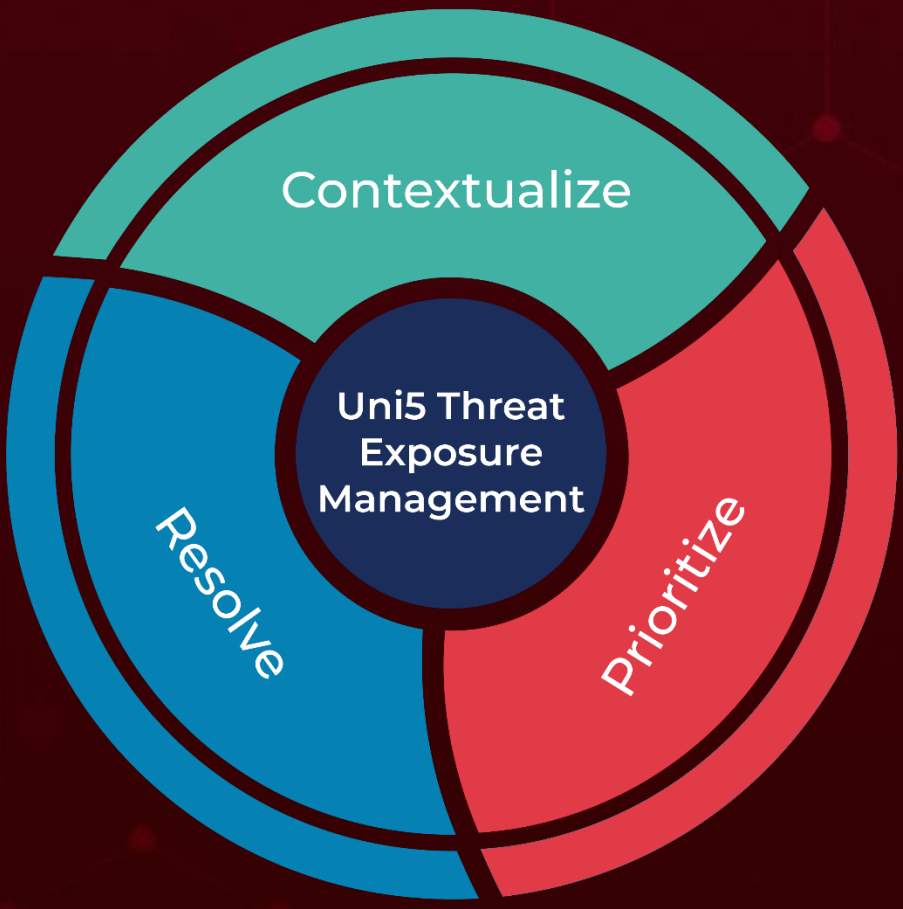
Attack Name	TYPE	VALUE
BellaCiao	SHA256	2aa1bbbe47f04627a8ea4e8718ad21f0d50adf6a32ba4e6133ee46ce2cd13780 ca57391cdbac224f159e858425d231d068aa76316e0345cb8d58c716b9eff587
	SHA1	736ba9daf63a2add3217c79fa9d83088358f7012
	Domains	mail-updateservice[.]info maill-support[.]com mailupdate[.]com mailupdate[.]info msn-center[.]uk msn-service[.]co twittsupport[.]com
	IPV4	188[.]165[.]174[.]199 88[.]80[.]148[.]162
PingPull	SHA256	cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae 5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507 e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253
	Domains	yrhsywu2009.zapto[.]org *.saspecialforces.co[.]za vpn729380678.softether[.]net
	IPV4	5.181.25[.]99 196.216.136[.]139
VEILEDSIGNAL	SHA256	cb0922d8b130504bf9a3078743294791201789c5a3d7bc0369afd096ea15f0ae 5ba043c074818fdd06ae1d3939ddfe7d3d35bab5d53445bc1f2f689859a87507 e39b5c32ab255ad284ae6d4dae8b4888300d4b5df23157404d9c8be3f95b3253
	URLs	hxxps[://]www.tradingtechnologies[.]com/trading/order-management
RustBucket	Domains	cloud[.]dnx[.]capital deck[.]31ventures[.]info
	File Path	/Users/Shared/Internal PDF Viewer.app

Attack Name	TYPE	VALUE
RustBucket	SHA1	dabb4372050264f389b8adcf239366860662ac52 0be69bb9836b2a266bfd9a8b93bb412b6e4ce1be e0e42ac374443500c236721341612865cd3d1eec ac08406818bbf4fe24ea04bfd72f747c89174bdb 72167ec09d62cdfb04698c3f96a6131dceb24a9c fd1cef5abe3e0c275671916a1f3a566f13489416 ca59874172660e6180af2815c3a42c85169aa0b2 d9f1392fb7ed010a0ecc4f819782c179efde9687 9121509d674091ce1f5f30e9a372b5dcf9bcd257 a1a85cba1bc4ac9f6eafc548b1454f57b4dff7e0 7a5d57c7e2b0c8ab7d60f7a7c7f4649f33fea8aa 182760cbe11fa0316abfb8b7b00b63f83159f5aa 7e69cb4f9c37fad13de85e91b5a05a816d14f490

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 1, 2023 . 8:00 AM

More at www.hivepro.com