Date of Publication
May 15, 2023

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

8 to 14 MAY 2023

Table Of Contents

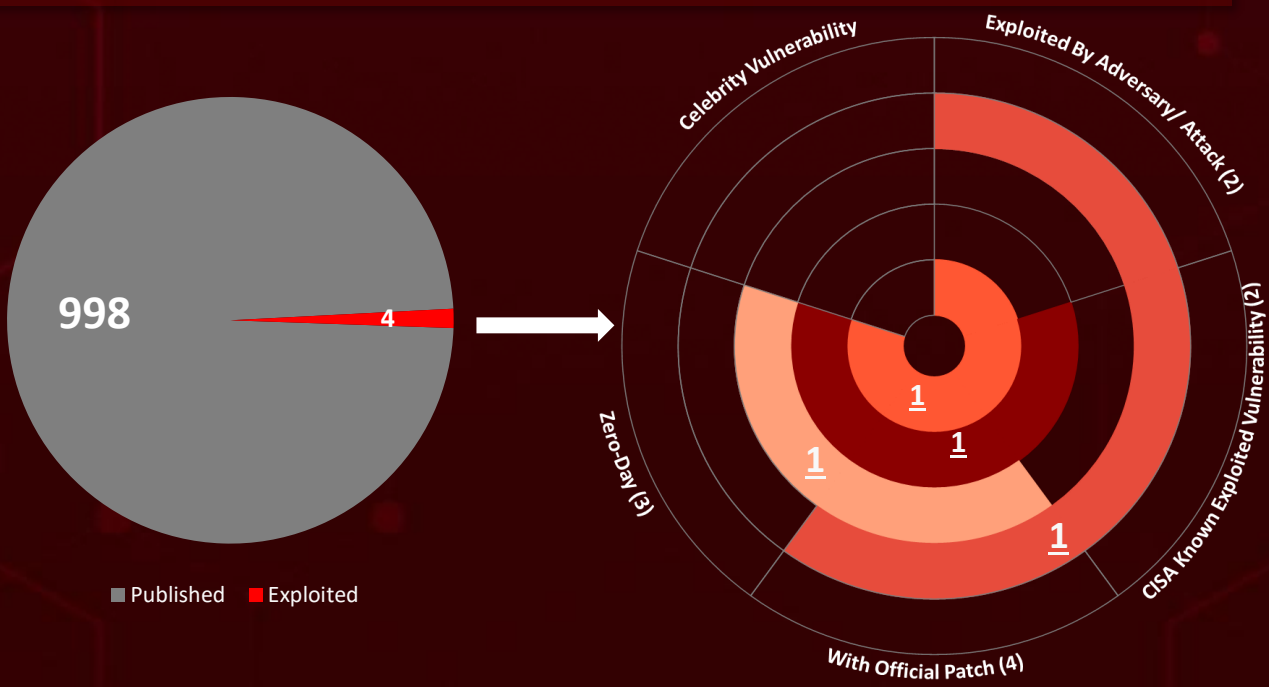
Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, they identified a total of **nine** executed attacks. These attacks took advantage of **four** different vulnerabilities in various systems. Additionally, HiveForce Labs identified **five** different adversaries actively carrying out these attacks.

The **AndoryuBot** malware exploits a critical vulnerability in Ruckus (**CVE-2023-25717**) to infect Wi-Fi access points, enabling its use in DDoS attacks. This versatile malware supports 12 different DDoS attack modes.

The **SideWinder** APT group employs sophisticated techniques such as server-side polymorphism to carry out their operations. They have been known to exploit the **CVE-2017-0199** vulnerability in order to deliver additional malicious payloads. Another notable malware, **Snake**, is a potent cyber-espionage tool attributed to the FSB and connected to the **Turla** hacker group.

Apart from these threats, the latest Microsoft Patch Tuesday release focuses on addressing **two** Zero-day vulnerabilities. All these attacks were observed to be on the rise, posing a significant threat.



High Level Statistics

9
Attacks Executed

4
Vulnerabilities Exploited

5
Adversaries in Action

- Akira ransomware
- ReconShark
- AndoryuBot
- Snake
- DarkWatchMan RAT
- DownEx
- CACTUS Ransomware
- BPFDoor
- Greatness
- CVE-2023-25717
- CVE-2023-29336
- CVE-2023-24932
- CVE-2017-0199
- Dragon Breath APT
- Kimsuky
- Turla
- SideWinder
- Red Menshen

Insights

New **Cactus** Ransomware Emerges

Turla deployed powerful cyber-espionage malware **Snake**

SideWinder exploited **CVE-2017-0199** to invade antivirus (AV) detection

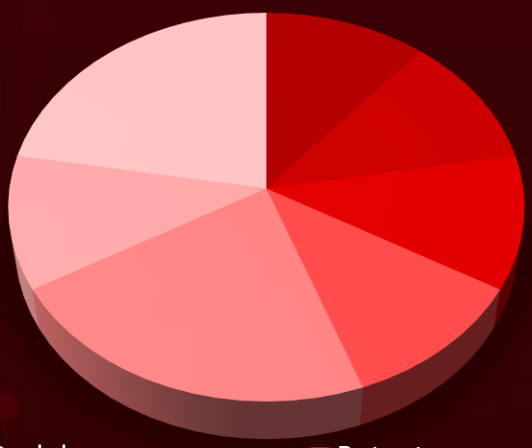
AndoryuBot targets critical Ruckus Wireless Admin panel vulnerability

Akira Ransomware Demands ransom amount from $200,000 to $1,000,000

2 Zero-day vulnerabilities addressed it Microsoft Patch Tuesday

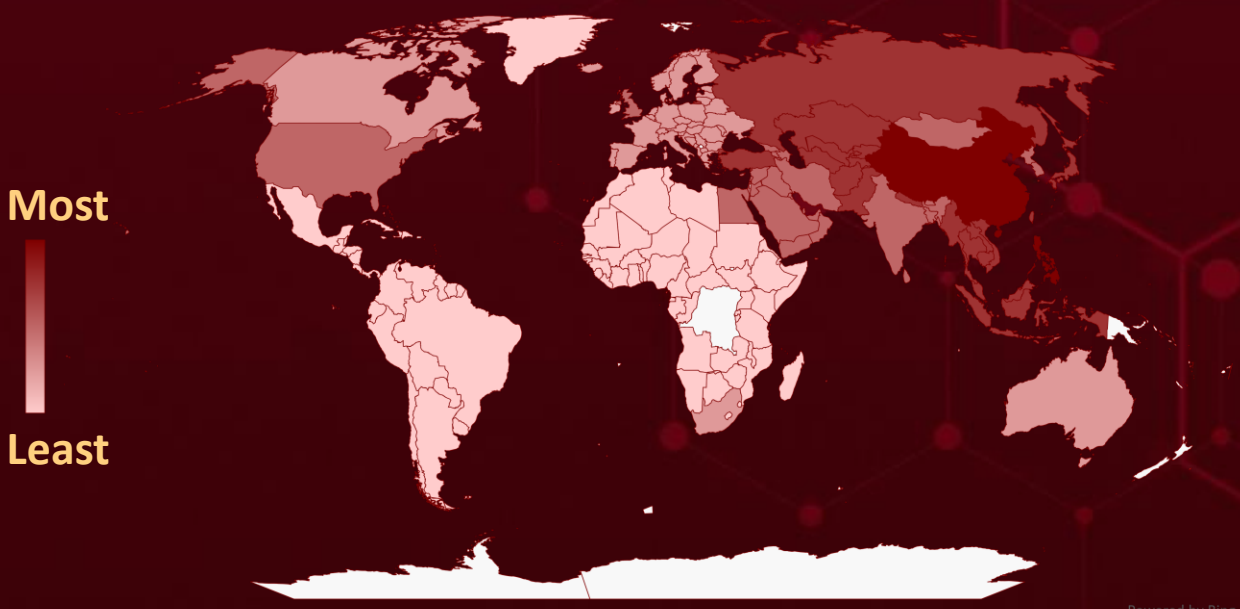
DarkWatch Man RAT Targets Russians

Threat Distribution



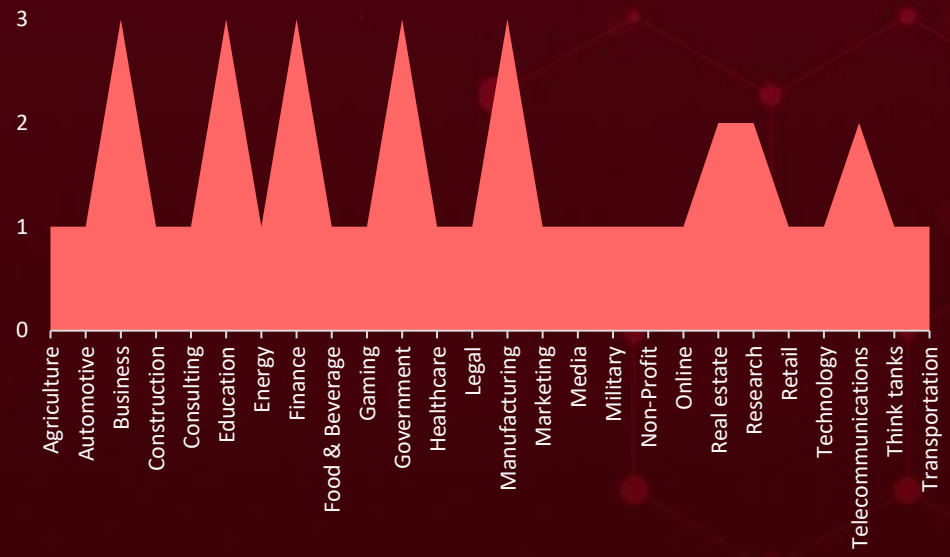
- Backdoor
- Botnets
- Fileless
- Phishing-as-a-service
- Ransomware
- RAT
- Tool

Targeted Countries



Countries	Countries	Countries	Countries	Countries
China	Vietnam	Bangladesh	Iceland	Andorra
Philippines	Bhutan	Syria	Belgium	Moldova
Singapore	Sri Lanka	Lebanon	North Macedonia	San Marino
Turkmenistan	Palestine	Cyprus	Malta	Belarus
Cambodia	Georgia	Yemen	Norway	Bosnia and Herzegovina
Nepal	Timor-Leste	UAE	Serbia	Estonia
Indonesia	India	Maldives	France	Netherlands
Thailand	North Korea	Mongolia	Slovakia	Lithuania
Japan	Iran	USA	Albania	Luxembourg
Myanmar	Saudi Arabia	Ireland	South Africa	Latvia
Kazakhstan	Iraq	Slovenia	Australia	Suriname
Pakistan	Armenia	Monaco	Spain	São Tomé and Príncipe
Russia	Israel	Italy	Bulgaria	Cuba
Brunei	UK	Liechtenstein	Sweden	Dominica
Taiwan	Jordan	Montenegro	Poland	Barbados
Kyrgyzstan	Egypt	Czechia	Vatican City	Dominican Republic
Tajikistan	Azerbaijan	Austria	Portugal	Comoros
Laos	Oman	Canada	Croatia	East Timor
Turkey	Kuwait	Ukraine	Finland	Liberia
Afghanistan	Qatar	Germany	Greece	Madagascar
Uzbekistan	Bahrain	Hungary	Romania	Seychelles
Malaysia	South Korea	Switzerland	Denmark	Malawi

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059
Command and Scripting Interpreter

T1027
Obfuscated Files or Information

T1106
Native API

T1090
Proxy

T1140
Deobfuscate/ Decode Files or Information

T1204
User Execution

T1083
File and Directory Discovery

T1566
Phishing

T1190
Exploit Public-Facing Application

T1574
Hijack Execution Flow

T1204.002
Malicious File

T1071
Application Layer Protocol

T1036
Masquerading

T1059.001
PowerShell

T1053
Scheduled Task/Job

T1027.002
Software Packing

T1082
System Information Discovery

T1087
Account Discovery

T1012
Query Registry

T1569
System Services

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Akira ransomware	Akira ransomware is a new threat targeting corporate networks and has already attacked several companies in various industries, stealing their data and demanding ransom amounts ranging from $200,000 to $1,000,000.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Compromise of Sensitive Information, and Potential Financial Losses	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488,3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c,67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ReconShark	Kimsuky, a North Korean APT group, is using a new malware tool called ReconShark to conduct global cyberattacks.	spear-phishing emails & OneDrive Links	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Reconnaissance Tool		Data Theft andCompromise of Sensitive Information	Microsoft OneDrive
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky (aka Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)			-
IOC TYPE	**VALUE**		
SHA1	86a025e282495584eabece67e4e2a43dca28e505c8f54cb73c240a1904030eb36bb2baa7db6aeb01		
Domain	yonsei[.]lol		

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td>AndoryuBot</td><td rowspan="5">AndoryuBot targets critical Ruckus Wireless Admin panel vulnerability to infect Wi-Fi access points for use in DDoS attacks, malware supports 12 DDoS attack modes and is marketed through YouTube videos.</td><td>Ruckus vulnerability</td><td>CVE-2023-25717</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>Botnets</td><td rowspan="3">Data Theft, Denial of Service and Potential Financial Losses</td><td>All Ruckus Wireless Admin panels version 10.4 and older</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://support.ruckuswireless.com/security_bulletins/315</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>IPV4</td><td colspan="3">163[.]123[.]142[.]146
45[.]153[.]243[.]39</td></tr>
<tr><td>SHA256</td><td colspan="3">ea064dd91d8d9e6036e99f5348e078c43f99fdf98500614bffb736c4b0fff408,f42c6cea4c47bf0cbef666a8052633ab85ab6ac5b99b7e31faa1e198c4dd1ee1,3441e88c80e82b933bb09e660d229d74f7b753a188700fe018e74c2db7b2aaa0</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">Snake (aka Uroburos, Urouros)</td><td rowspan="6">Snake is a powerful cyber-espionage malware developed by FSB & linked to Turla hackers. Boasts high stealth, rigorous engineering & global reach.</td><td>-</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Data Theft</td><td rowspan="2">Windows, MacOS, and Linux</td></tr>
<tr><td>Cyber Espionage Tool</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>Turla (aka IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear)</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">6a4836cd5847c3d42b846d1616cc94429ec27446555b66f9abf061e7747bdca0,3c3511a9b6d98f49943cbec9355ebb8a006706f42304f608b6d9eb6f2da79718,735808b3dfad2472c5785399b6e34bf5cccef1153ad15bd1167420ff05b1a9d8,ff51c7ab066f425f73ba2005dbf3d2be4bc5344b152f18818c0ea5da81368ef0,1c05f794c40193734a68e145ca1aaf7268b37f6fe3ea2bea5f12aa2ceB24ee60</td></tr>
</table>

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
DarkWatchMan RAT	DarkWatchMan RAT allows attackers to gain remote control over compromised systems and extract sensitive data such as keystrokes, clipboard data, and system information.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft and remote access to infected system.	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
MD5	2edf05f2130d4e12599dc44ff8bfc892 1706c64156d873ebbd0c6ecac95fec39 9afc15393e8bae03ad306ae1c50645e3 ca820517f8fd74d21944d846df6b7c20		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DownEx	The DownEx malware was discovered in a cyberattack on government institutions in Kazakhstan and Afghanistan in 2022, likely with state sponsorship.	Spear-phishing emails	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Fileless		Data Theft and espionage	Windows
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
Domain	net-certificate[.]services		
IPV4	139.99.126[.]38 84.32.188[.]123 206.166.251[.]216		
MD5	1e46ef362b39663ce8d1e14c49899f0e bb7cf346c7db1c518b1a63c83e30c602		

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
CACTUS Ransomware	CACTUS is a new strain of ransomware that targets large commercial entities, gains initial access to networks through VPN vulnerabilities, and communicates with victims through Tox, using a variety of tools and tactics.	Exploiting known vulnerabilities in VPN appliances	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Exfiltrates sensitive data and and Potential Financial Losses	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
IPV4	163[.]123[.]142[.]213		
MD5	d9f15227fefb98ba69d98542fbe7e568 3adc612b769a2b1d08b50b1fb5783bcf be7b13aee7b510b052d023dd936dc32f 26f3a62d205004fbc9c76330c1c71536		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BPFDoor	A new variant of the BPFDoor is featuring more robust encryption and reverse shell communication. It uses the BPF to bypass firewall restrictions, allowing threat actors to maintain persistence and remain undetected.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft	Linux
ASSOCIATED ACTOR			**PATCH LINK**
Red Menshen (AKA Red Dev 18)			-
IOC TYPE	**VALUE**		
SHA256	afa8a32ec29a31f152ba20a30eb483520fe50f2dce6c9aa9135d88f7c9c511d7		
Mutex	/var/run/initd[.]lock		

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
Greatness	The Phishing-as-a-Service (PaaS) platform named 'Greatness' has experienced a the surge in its operations, which target organizations utilizing Microsoft 365 in the USA	Phishing pages	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Phishing-as-a-service		Compromise critical infrastructure and sensitive data	Microsoft 365
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
URLs	hxxps[:]//bluecheckcommunication[.]com/finale/host8/admin/js/mj[.]php hxxps[:]//thesslcgroup[.]org/host10/admin/js/mj[.]php		
SHA256	c5b29072d28e35c3992015fcbedc29540dd5ffc2931257a71866affae9de31f4d07a2aa49f7b41eac954cd917aeedad3309d2856f63d51410da10dd5ff5847ce		

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-2023-25717		All Ruckus Wireless Admin panels version 10.4 and older	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:ruckuswireless:ruckus_wireless_admin:*:*:*:*:*:*:*:*	AndoryuBot
Ruckus Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059:Command and Scripting Interpreter	https://support.ruckuswireless.com/security_bulletins/315

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-29336		Windows: 10 - 10 S; Windows Server: 2008 - 2016	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*::*:*	-
Win32k Elevation of Privilege Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-119	T1068:Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-29336

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-24932	✗ ZERO-DAY	Windows: 10 - 10 S, 11 – 11 22H2; Windows Server: 2008 - 2022 20H2	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Secure Boot Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-254	T1190:Exploit Public-Facing Application, T1040:Network Sniffing	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-24932

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-0199	✗ ZERO-DAY	Microsoft Office: 2007 - 2016	SideWinder
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:microsoft_office:2016:*:*:*:*:*:*:*	-
Microsoft Office/WordPad Remote Code Execution Vulnerability with Windows API	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059:Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0199

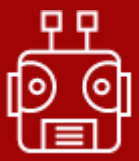
Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
	Unknown	Online Gambling, Gaming	Philippines, Japan, Taiwan, Singapore, Hong Kong, and China
	MOTIVE		
	Financial gain		
Dragon Breath APT (aka Golden Eye Dog & APT-Q-27)	**TARGETED CVEs**	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	Telegram, LetsVPN, and WhatsApp for Windows

TTPs
T1120:Peripheral Device Discovery;T1091:Replication Through Removable Media;T1059:Command and Scripting Interpreter;T1574:Hijack Execution Flow;T1574.002:DLL Side-Loading;T1055:Process Injection;T1027:Obfuscated Files or Information;T1027.002:Software Packing;T1036:Masquerading;T1070:Indicator Removal;T1070.004:File Deletion;T1070.006:Timestomp;T1057:Process Discovery;T1082:System Information Discovery;T1083:File and Directory Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Kimsuky (aka Velvet Chollima, Thallium, Cerium, Black Banshee, ITG16, TA406)	North Korea	Think tanks, Research universities, and government entities.	United States, Europe, and Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	ReconShark	Microsoft OneDrive

TTPs
T1053:Scheduled Task/Job;T1059:Command and Scripting Interpreter;T1090:Proxy;T1566:Phishing;T1566.002:Spearphishing Link;T1547:Boot or Logon Autostart Execution;T1547.001:Registry Run Keys/Startup Folder;T1132:Data Encoding;T1012:Query Registry;T1047:Windows Management Instrumentation;T1070:Indicator Removal;T1070.004:File Deletion;T1059.005:Visual Basic;T1204:User Execution;T1204.002:Malicious File;T1104:Multi-Stage Channels

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3"> 
Turla (aka IRON HUNTER, Group 88, Belugasturgeon, Waterbug, WhiteBear, Snake, Krypton, Venomous Bear)</td><td>Russia</td><td rowspan="3">Research facilities, Education, Small Businesses, Media organizations, Government facilities, Financial Services, Manufacturing, and Communications.</td><td rowspan="3">North America, South America, Europe, Africa, Asia, and Australia.</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>-</td><td>Snake (aka Uroburos, Urouros)</td><td>Windows, MacOS, and Linux</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1095:Non-Application Layer:Protocol;T1104:Multi-Stage Channels;T1106:Native API;T1001:Data Obfuscation;T1001.003:Protocol Impersonation;T1003:OS Credential Dumping;T1014:Rootkit;T1027:Obfuscated Files or Information;T1027.002:Software Packing;T1036:Masquerading;T1040:Network Sniffing;T1046:Network Service Discovery;T1055:Process Injection;T1055.001:Dynamic-link Library Injection;T1056:Input Capture;T1056.001:Keylogging;T1059:Command and Scripting Interpreter;T1059.001:PowerShell;T1071:Application Layer Protocol;T1071.001:Web Protocols;T1071.003:Mail Protocols;T1071.004:DNS;T1074:Data Staged;T1078:Valid Accounts;T1083:File and Directory Discovery;T1090:Proxy;T1090.003:Multi-hop Proxy;T1112:Modify Registry;T1119:Automated Collection;T1132:Data Encoding;T1132.002:Non-Standard Encoding;T1135:Network Share Discovery;T1140:Deobfuscate/Decode:Files or Information;T1190:Exploit Public-Facing Application;T1482:Domain Trust Discovery;T1546:Event Triggered:Execution;T1546.016:Installer Packages;T1547.006:Kernel Modules and Extensions;T1559:Inter-Process Communication;T1560.003:Archive via Custom Method;T1564:Hide Artifacts;T1569.002:Service Execution;T1570:Lateral Tool Transfer;T1572:Protocol Tunneling;T1573:Encrypted Channel;T1588:Obtain Capabilities;T1610:Deploy Container</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 SideWinder (aka Rattlesnake, T-APT-04, APT-C-17, Razor Tiger, Baby Elephant, Operation Origami)	India	Military, Government, and Business Entities	Pakistan, Turkey, Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam, Afghanistan, China, and Nepal
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-0199	-	Microsoft Windows, Windows Server, Office
TTPs			
T1518:Software Discovery;T1480:Execution Guardrails;T1574:Hijack Execution Flow;T1559:Inter-Process Communication;T1027:Obfuscated Files or Information;T1047:Windows Management Instrumentation;T1059:Command and Scripting Interpreter;T1071:Application Layer Protocol;T1105:Ingress Tool Transfer;T1140:Deobfuscate/Decode Files or Information;T1203:Exploitation for Client Execution;T1204:User Execution;T1221:Template Injection;T1204.002:Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Red Menshen (AKA Red Dev 18)	China	Telecommunications	Middle East and Asia
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	BPFDoor	-
TTPs			
T1071:Application Layer Protocol;T1205:Traffic Signaling;T1573:Encrypted Channel;T1562:Impair Defenses;T1059:Command and Scripting Interpreter;T1562.004:Disable or Modify System Firewall;T1040:Network Sniffing;T1572:Protocol Tunneling;T1205.002:Socket Filters;T1106:Native API;T1083:File and Directory Discovery			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **4 exploited vulnerabilities** and block the indicators related to the threat actor **Dragon Breath APT, Kimsuky, Turla, SideWinder,** and **Red Menshen,** and malware **Akira ransomware, ReconShark, AndoryuBot, Snake, DarkWatchMan RAT, DownEx, CACTUS Ransomware, BPFDoor,** and **Greatness.**

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 the **4 exploited vulnerabilities** impacted.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Dragon Breath APT, Kimsuky, Turla, SideWinder,** and **Red Menshen,** and malware **Akira ransomware, ReconShark, AndoryuBot, Snake, DarkWatchMan RAT, DownEx, CACTUS Ransomware, BPFDoor,** and **Greatness** in Breach and Attack Simulation(BAS).

Threat Advisories

Fortinet addresses Vulnerabilities in FortiADC, FortiOS and FortiProxy

Dragon Breath APT Evolves with Double DLL Sideloading

A New Akira Ransomware Targets Multiple Industries and Demands Millions in Extortion

Kimsuky APT Group Employs ReconShark

New AndoryuBot Malware Exploits Ruckus Wireless Flaw for DDoS Attacks

Microsoft's May 2023 update addresses two Zero-Day Vulnerabilities

Snake a Stealthy Cyber-Espionage Malware

DarkWatchMan RAT Targets Russians

Uncovering the Latest Tactics of the SideWinder APT

New DownEx Malware Campaign Targets Foreign Government Institutions in Central Asia

CACTUS Ransomware Emerges as New Threat Targeting Large Enterprises

New Variant of BPFDoor Linux Malware Features Enhanced Encryption and Stealthy Communication

Greatness a Growing Threat to Microsoft 365 Users

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
Akira ransomware	SHA256	7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488 3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c 67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
ReconShark	Domain	yonsei[.]lol
	URLs	https[:]//rfa[.]ink/bio/r.php https[:]//mitmail.tech/gorgon/r.php https[:]//rfa[.]ink/bio/t1.hta https[:]//mitmail[.]tech/gorgon/t1.hta https[:]//rfa[.]ink/bio/ca.php?na=reg.gif https[:]//mitmail.tech/gorgon/ca.php?na=reg.gif https[:]//rfa[.]ink/bio/ca.php?na=secur32.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=secur32.gif https[:]//newshare[.]online/lee/ca.php?na=secur32.gif https[:]//rfa[.]ink/bio/ca.php?na=dot_eset.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_eset.gif https[:]//rfa[.]ink/bio/ca.php?na=video.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=video.gif https[:]//rfa[.]ink/bio/ca.php?na=start2.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start2.gif https[:]//rfa[.]ink/bio/ca.php?na=start4.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start4.gif https[:]//rfa[.]ink/bio/ca.php?na=start3.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start3.gif https[:]//rfa[.]ink/bio/ca.php?na=videop.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=videop.gif

Attack Name	TYPE	VALUE
ReconShark	URLs	https[:]//rfa[.]ink/bio/ca.php?na=start1.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start1.gif https[:]//rfa[.]ink/bio/ca.php?na=vbs_esen.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=vbs_esen.gif https[:]//rfa[.]ink/bio/ca.php?na=start0.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=start0.gif https[:]//rfa[.]ink /bio/d.php?na=vbtmp https[:]//rfa[.]ink/bio/ca.php?na=vbs.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=vbs.gif https[:]//rfa[.]ink/bio/d.php?na=battmp https[:]//rfa[.]ink/bio/ca.php?na=dot_v3.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_v3.gif https[:]//rfa[.]ink/bio/ca.php?na=dot_esen.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_esen.gif http[:]//rfa[.]ink/bio/ca.php?na=dot_avg.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_avg.gif https[:]//rfa[.]ink/bio/ca.php?na=dot_kasp.gif https[:]//mitmail[.]tech/gorgon/ca.php?na=dot_kasp.gif
	SHA1	86a025e282495584eabece67e4e2a43dca28e505 c8f54cb73c240a1904030eb36bb2baa7db6aeb01
AndoryuBot	IPV4	163[.]123[.]142[.]146 45[.]153[.]243[.]39
	SHA256	ea064dd91d8d9e6036e99f5348e078c43f99fdf98500614bffb736c4b0fff408 f42c6cea4c47bf0cbef666a8052633ab85ab6ac5b99b7e31faa1e198c4dd1ee1 3441e88c80e82b933bb09e660d229d74f7b753a188700fe018e74c2db7b2aaa0 3c9998b8451022beee346f1afe18cab84e867b43c14ba9c7f04e5c559bfc4c3a b71b4f478479505f1bfb43663b4a4666ec98cd324acb16892ecb876ade5ca6f9 e740a0d2e42c09e912c43ecdc4dcbd8e92896ac3f725830d16aaa3eddf07fd5c 4fe4cff875ef7f8c29c95efe71b92ed31ed9f61eb8dfad448259295bd1080aca 2e7136f760f04b1ed7033251a14fef1be1e82ddcbff44dae30db12fe52e0a78a 1298da097b1c5bdce63f580e14e2c1b372c409476747356a8e9cfaf62b94513d 55e921a196c92c659305aa9de3edf6297803b60012f83967562a57547875fec1

Attack Name	TYPE	VALUE
Snake (aka Uroburos, Urouros)	SAH256	6a4836cd5847c3d42b846d1616cc94429ec27446555b66f9abf061e7747bdca0 3c3511a9b6d98f49943cbec9355ebb8a006706f42304f608b6d9eb6f2da79718 735808b3dfad2472c5785399b6e34bf5cccef1153ad15bd1167420ff05b1a9d8 ff51c7ab066f425f73ba2005dbf3d2be4bc5344b152f18818c0ea5da81368ef0 1c05f794c40193734a68e145ca1aaf7268b37f6fe3ea2bea5f12aa2ceb24ee60 a693fe103b7177f431889a2116a5b48cd3f59a1663667bdc6bd62920be14357e 7b9c6745870b51dbf676ddc45b91ab5b241768a614c74689e96af73a4836f136 b4a93ba9ec9dad5f5a8eb01d58ddcbb3ebc60182ed040272ae295a1ce0a53b50 088ec7b0c8c7b697a2236dbb3966bd9f03c47f63a608e2455862f30bf712635f 41eeced2b87d5e4a4b46326c14e0890a24fc17e99d82f16fd5b5976c3ab66598 10b854d66240d9ee1ce4296d2f7857d2b1c6f062ca836d13d777930d678b3ca6 55047d88678f22d87a5fcec2a27d043d028102f49362c2ca6598b2fc056d8c80
DarkWatchMan RAT	MD5	2edf05f2130d4e12599dc44ff8bfc892 1706c64156d873ebbd0c6ecac95fec39 9afc15393e8bae03ad306ae1c50645e3 ca820517f8fd74d21944d846df6b7c20
	SHA1	1f87eeb37156d64de97d042b9bcfbaf185f8737d 149ce68540a068cdd204df796f6bff7d70f16473 be450cd1fab1b708ac1de209224e0d7f7adc0fae bb91d5234f37905f4830061331beab99e51206e7
	SHA256	4e38b7519bf7b482f10e36fb3e000cc2fcbf058730f6b9598a6a7ba5543766d4 d439a3ce7353ef96cf3556abba1e5da77eac21fdba09d6a4aad42d1fc88c1e3c 706eebdf4de19d17f9a753984f7b4cff7f5487c74d7862d21684e754967d8dd4 1b5eb6d4680f7d4da7e2a1a1060b9f13565e082346e375a92244bb55672d49d7

Attack Name	TYPE	VALUE
DownEx	Domain	net-certificate[.]services
	IPV4	139.99.126[.]38 84.32.188[.]123 206.166.251[.]216
	MD5	1e46ef362b39663ce8d1e14c49899f0e bb7cf346c7db1c518b1a63c83e30c602 a45106470f946ea6798f7d42878cff51 3ac42f25df0b600d6fc9eac73f011261 14a8aad94b915831fc1d3a8e7e00a5df 457eca2f6d11dd04ccce7308c1c327b7 d310a9f28893857a0dc1f7c9b624d353 d20e4fffbac3f46340b61ab8f7d578b1 5602da1f5b034c9d2d6105cdc471852b 89f15568bc19cc38caa8fd7efca977af ae5d4b9c1038f6840b563c868692f2aa c273cdfcfd808efa49ec0ed4f1c976e0 d11fcd39a30a23176337847e54d7268c 70e4305af8b00d04d95fba1f9ade222d 1492b0079b04eb850279114b4361f10c
CACTUS Ransomware	IPV4	163[.]123[.]142[.]213
	MD5	d9f15227fefb98ba69d98542fbe7e568 3adc612b769a2b1d08b50b1fb5783bcf be7b13aee7b510b052d023dd936dc32f 26f3a62d205004fbc9c76330c1c71536 d5e5980feb1906d85fbd2a5f2165baf7 78aea93137be5f10e9281dd578a3ba73
BPFDoor	SHA256	afa8a32ec29a31f152ba20a30eb483520fe50f2dce6c9aa9135d88f7c9c511d7
	Mutex	/var/run/initd[.]lock
Greatness	URLs	hxxps[:]//bluecheckcommunication[.]com/finale/host8/admin/js/mj[.]php hxxps[:]//thesslcgroup[.]org/host10/admin/js/mj[.]php hxxps[:]//cliffordandblu[.]com/wp-includes/SimplePie/Parse/pate/procs/admin/js/mj[.]php hxxps[:]//avenzzi[.]com/ayoo/host7/admin/js/mj[.]php hxxps[:]//at[.]benconcept[.]com/wp-content/plugins/TOPXOH/offe/host6/admin/js/mj[.]php hxxps[:]//cp3955[.]com/host8/admin/js/mj[.]php hxxps[:]//schneidera[.]ga/[.]well-known/off/host8/admin/js/mj[.]php hxxp[:]//bbqpro[.]za[.]com/fb/host7/admin/js/mj[.]php hxxps[:]//www[.]c2tec[.]com[.]br/today/host16/admin/js/mj[.]php

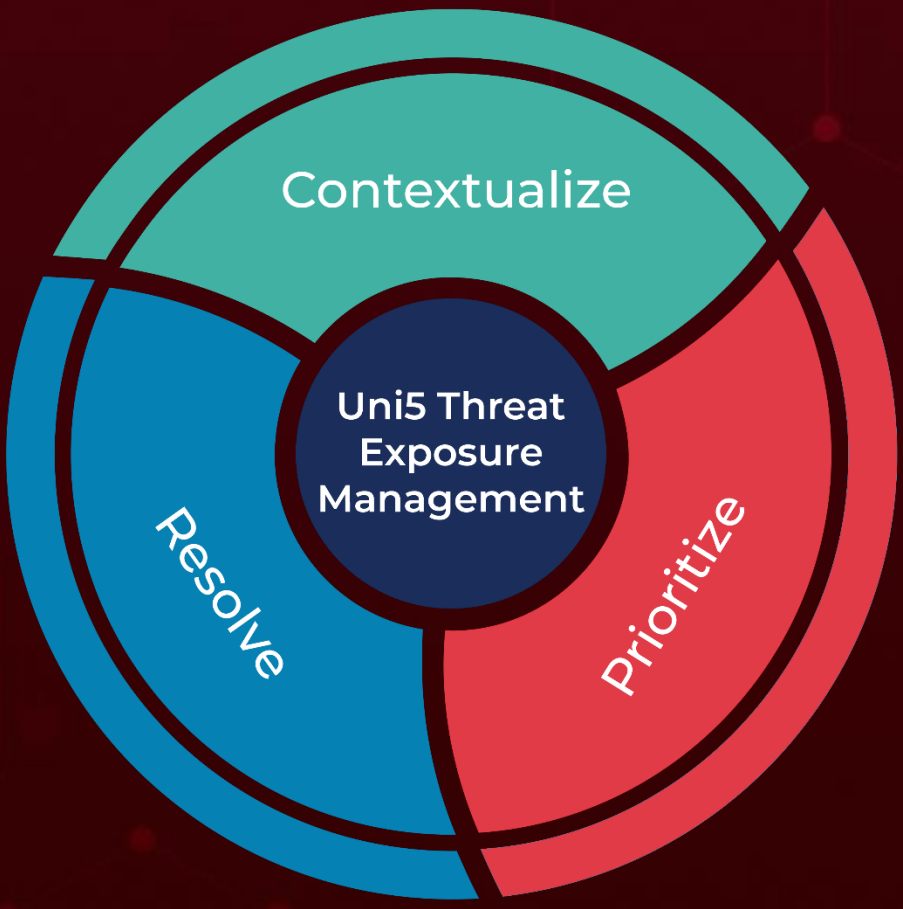
Attack Name	TYPE	VALUE
Greatness	URLs	hxxps[:]//cedarcreeklabradoodles[.]com/host6/admin/js/mj[.]php hxxps[:]//whitesomcponwmc[.]com/wnclrm/andlw/admin/js/mj[.]php hxxps[:]//hihin[.]net/wp-content/plugins/backwpup/k/host7/admin/js/mj[.]php hxxps[:]//hansarobotics[.]com/host7/admin/js/mj[.]php hxxp[:]//cloudnewsdaily[.]sa[.]com/img/host8/admin/js/mj[.]php hxxps[:]//pog[.]flylineaeru[.]com/html/admin/js/mj[.]php hxxp[:]//whitesomcponwmc[.]com/wnclrm/andlw/admin/js/mj[.]php hxxps[:]//manimot[.]ca/wp-includes/dump/host8/admin/js/mj[.]php hxxps[:]//ochrelandscapes[.]com[.]au/host9/admin/js/mj[.]php hxxps[:]//fanningcpaz[.]com/jumpjumping/host15/admin/js/mj[.]php hxxp[:]//mail[.]sorderatoluca[.]com/wp-content/host7/admin/js/mj[.]php
	SHA256	c5b29072d28e35c3992015fcbedc29540dd5ffc2931257a71866affae9de31f4 d07a2aa49f7b41eac954cd917aeedad3309d2856f63d51410da10dd5ff5847ce bbf7f77c3aca82b1531ba295cb5edb700777325dec9533d0c0341b66ddd073e3 d587c80ba12878146cfcb62262608c4a09f8b4d8647f9819ee3a5a94874b0205 492a45dd47acb19c6995acdbfce22a0cbcc135bc0263fd3efab165b1b75c9f68 61c094210d25d2e501234cc45b399b556d9bc95bc18f81c9ef4f433cc96b431a 9937f4ab00c4d41c8986a4d4e5a2a4193412e031c5a33d5f88913cc8dd0b5d4f c9375f405c6409087cfabb34bdc8e9d1333f8b1f6448395a3889856a07ba3573 8619111ae4e427ce31eea0dd4e3b1ec5fa728438b64fdbff3351256cc52d5831 ca130ace64ce6277b612c0e507a5b8e37e54b4f635b18d896992a844ca99de72 2b4ca60d215bd7eaf13891878ef4ddeac36354343cdc59f9f2882f8eb61b7234 3216d8ad022b72512c65756c4272e897d8669faa8f3fbf8c4788fd41d67477f1 Ed4cd5308bf283928dfe5e3a0985e90c82014136a87fdac13670e0748482b5ed 02212ba142819acd27377cf8fa627e230ad44f0ff9f4a31a9a1fc7d17b74c88b

Attack Name	TYPE	VALUE
Greatness	SHA256	11d980af0e1f9576b2b2fa319ee58a49ee72f4722e96141ce5990b37248cad42 8567f25398c14ca530a110909e08a383df0ff94c4562f3105b59c1b84fdbf808 cccfdf7ba2c5f740a0ddfee6d273cf286d48765334e8e66ca1d8834fb4426af7 f20aea297c4c00e78e8059572c535b4c879b5c331f552c881ff7929d6df0f6a6 fcee0c8773ecc95b846e4b45dd1364d42796387d831f7203e50e116d1ed5a750 b34b9aa0b8a36deec3157f262c5be11fa705da4c4902dc50ce6f0df2b838471c cae49fe3b224160c790fec72309f1bdb8f0e1d7c8a82a49262b12707b1789ce0

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 15, 2023 . 6:33 AM

More at www.hivepro.com