Date of Publication
May 6, 2024

Hive Pro

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

29 APRIL to 5 MAY 2024

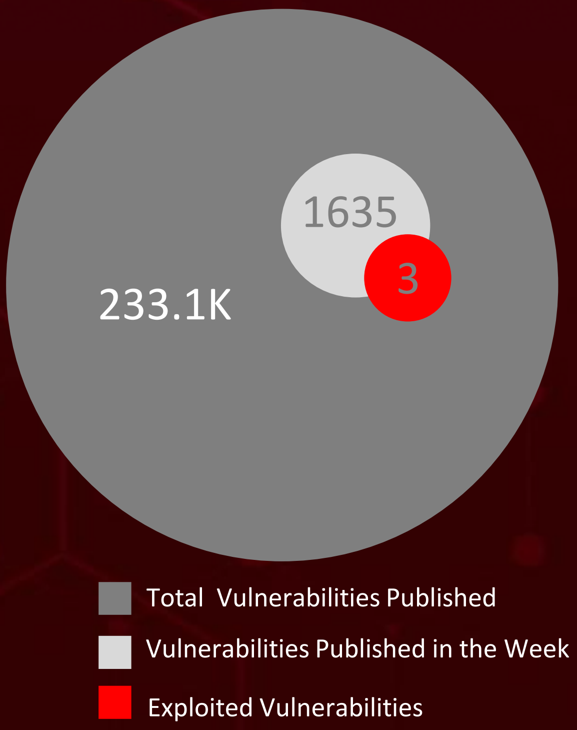
Table Of Contents

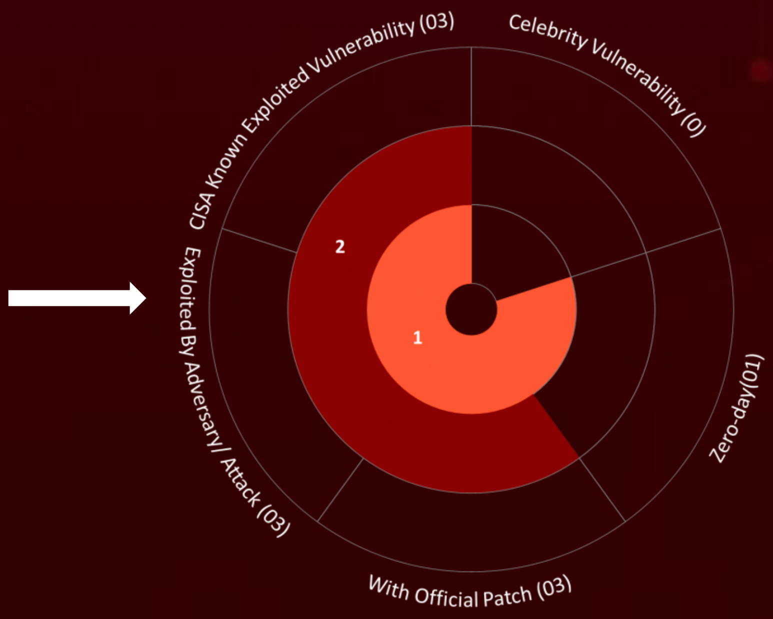
Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, a total of **three** attacks were executed, **three** vulnerabilities were uncovered, and **two** active adversaries were identified. These findings underscore the persistent danger of cyberattacks.

Furthermore, HiveForce Labs discovered that the newly emerged **Goldoon botnet** exploits a decade-old vulnerability (**CVE-2015-2051**) in D-Link systems, enabling remote attackers to execute arbitrary commands and gain control over compromised devices. This allows extraction of system information and communication with a central server, enabling further attacks like DDoS assaults.

APT28 threat actors exploited compromised EdgeRouters to conduct covert cyber operations, repurposing Ubiquiti routers for various malicious activities. These attacks are on the rise, posing a significant threat to users worldwide.





High Level Statistics

3
Attacks Executed

- Akira
- Goldoon
- Cuckoo

3
Vulnerabilities Exploited

- CVE-2023-20269
- CVE-2020-3259
- CVE-2015-2051

2
Adversaries in Action

- Muddling Meerkat
- APT28

Insights

Goldoon Botnet

Exploits a decade-old vulnerability (CVE-2015-2051) in D-Link systems to gain control over compromised devices

Akira Ransomware

As of January 1, 2024, the ransomware group has affected more than 250 organizations and declared around $42 million USD in ransomware earnings

APT28

Threat actors utilized compromised EdgeRouters to execute covert cyber operations

Muddling Meerkat

Conducts cyber operations via DNS, generating widespread queries using open DNS resolvers

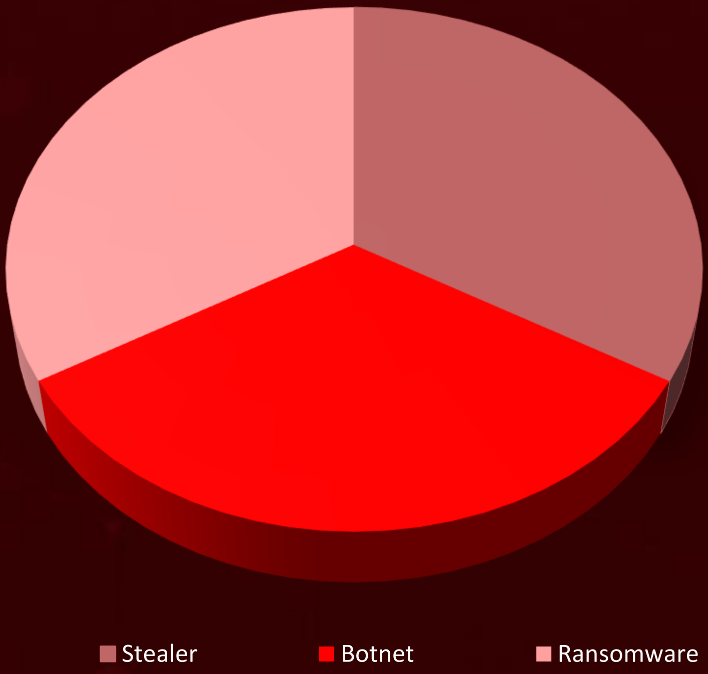
Docker Hub

Millions of fake repositories on Docker Hub aim to deceive developers with phishing scams or malware downloads

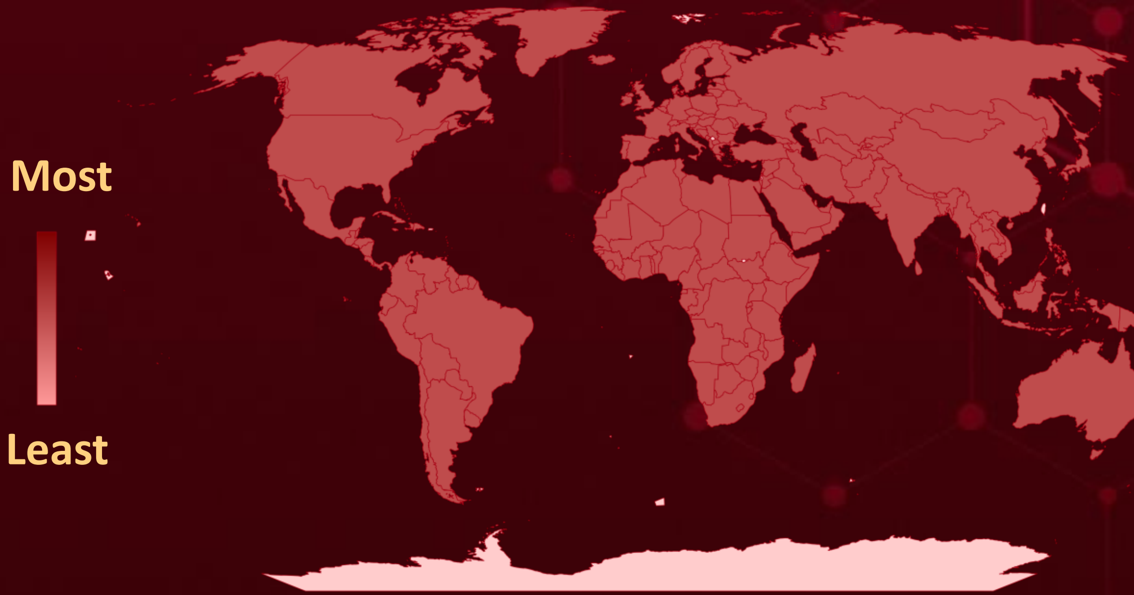
Cuckoo macOS

Malware displaying traits of both an infostealer and spyware

Threat Distribution



Targeted Countries



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

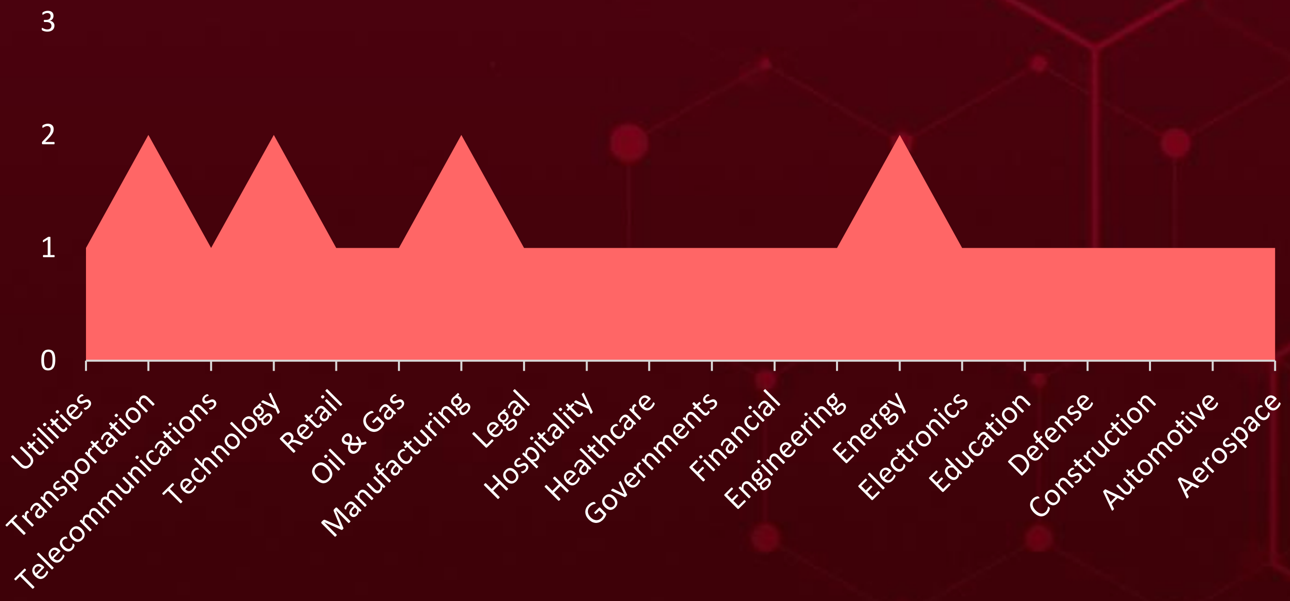
	Countries
🟥	Australia
🟥	United States
🟥	Norway
🟥	Afghanistan
🟥	South Sudan
🟥	Andorra
🟥	Monaco
🟥	Angola
🟥	Saint Lucia
🟥	Antigua and Barbuda
🟥	Trinidad and Tobago
🟥	Argentina
🟥	Mali
🟥	Armenia
🟥	Nepal
🟥	Albania
🟥	Philippines
🟥	Austria
🟥	Sierra Leone
🟥	Azerbaijan
🟥	Switzerland
🟥	Bahamas
🟥	Algeria

	Countries
🟥	Bahrain
🟥	Madagascar
🟥	Bangladesh
🟥	Mauritius
🟥	Barbados
🟥	Mozambique
🟥	Belarus
🟥	Niger
🟥	Belgium
🟥	Panama
🟥	Belize
🟥	Romania
🟥	Benin
🟥	Saudi Arabia
🟥	Bhutan
🟥	Solomon Islands
🟥	Bolivia
🟥	State of Palestine
🟥	Bosnia and Herzegovina
🟥	Thailand
🟥	Botswana
🟥	Tuvalu
🟥	Brazil
🟥	Vietnam

	Countries
🟥	Brunei
🟥	Lithuania
🟥	Bulgaria
🟥	Malaysia
🟥	Burkina Faso
🟥	Marshall Islands
🟥	Burundi
🟥	Micronesia
🟥	Cabo Verde
🟥	Montenegro
🟥	Cambodia
🟥	Namibia
🟥	Cameroon
🟥	New Zealand
🟥	Canada
🟥	North Korea
🟥	Central African Republic
🟥	Pakistan
🟥	Chad
🟥	Paraguay
🟥	Chile
🟥	Portugal
🟥	China

	Countries
🟥	Rwanda
🟥	Colombia
🟥	San Marino
🟥	Comoros
🟥	Serbia
🟥	Congo
🟥	Slovakia
🟥	Costa Rica
🟥	South Africa
🟥	Côte d'Ivoire
🟥	Sri Lanka
🟥	Croatia
🟥	Suriname
🟥	Cuba
🟥	Tajikistan
🟥	Cyprus
🟥	Togo
🟥	Czech Republic (Czechia)
🟥	Turkey
🟥	Denmark
🟥	Ukraine
🟥	Djibouti
🟥	Vanuatu
🟥	Dominica

Targeted Industries



TOP MITRE ATT&CK TTPs

T1057
Process Discovery

T1059
Command and Scripting Interpreter

T1219
Remote Access Software

T1018
Remote System Discovery

T1562.001
Disable or Modify Tools

T1041
Exfiltration Over C2 Channel

T1562
Impair Defenses

T1083
File and Directory Discovery

T1016
System Network Configuration Discovery

T1566
Phishing

T1204.002
Malicious File

T1041
System Binary Proxy Execution

T1588
Obtain Capabilities

T1588.005
Exploits

T1055
Process Injection

T1027
Obfuscated Files or Information

T1036
Masquerading

T1133
External Remote Services

T1082
System Information Discovery

T1190
Exploit Public-Facing Application

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Akira	The Akira ransomware group has become notorious for its malicious activities, having accrued a staggering $42 million through unauthorized means by infiltrating the networks of over 250 victims as of January 2024.	Exploiting Vulnerabilities	CVE-2023-20269 CVE-2020-3259
TYPE		IMPACT	AFFECTED PRODUCTS
Ransomware		Encrypt Data	-
ASSOCIATED ACTOR			PATCH LINK
-			https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

IOC TYPE	VALUE
SHA256	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca, dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e, bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138, 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf, 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386

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
Goldoon	The Goldoon botnet is a recent malware threat targeting a critical vulnerability in D-Link DIR-645 routers. This decade-old flaw (CVE-2015-2051) allows attackers to remotely take control of the router. Once infected, the Goldoon malware can steal information about the network, establish a persistent presence, and even launch denial-of-service	Exploiting vulnerability	CVE-2015-2051
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet		Data theft and launch denial-of-service	Dir-645: All versions
ASSOCIATED ACTOR			PATCH LINK
-			https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

IOC TYPE	VALUE
SHA256	66f21251d7f8c58316f149fec104723beb979a1215ad4e788d83f0ee6fd34696, 712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c, d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee, fdf6dae772f7003d0b7cdc55e047434dbd089e0dc7664a3fae8ccfd9d10ece8c, aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Cuckoo	Cuckoo malware, named after the parasitic bird, targets macOS systems as a dual infostealer and spyware, clandestinely gathering sensitive data and monitoring user activities for malicious purposes	-	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer and Spyware		Data theft	macOS
ASSOCIATED ACTOR			PATCH LINK
-			-

IOC TYPE	VALUE
SHA256	254663d6f4968b220795e0742284f9a846f995ba66590d97562e8f19049ffd4b, 1827db474aa94870aafdd63bdc25d61799c2f405ef94e88432e8e212dfa51ac7, d8c3c7eedd41b35a9a30a99727b9e0b47e652b8f601b58e2c20e2a7d30ce14a8, 39f1224d7d71100f86651012c87c181a545b0a1606edc49131730f8c5b56bdb7, a709dacc4d741926a7f04cad40a22adfc12dd7406f016dd668dd98725686a2dc

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-2023-20269	✗	WordPress Automatic plugin	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:wordpress:automatic_plugin:*:*:*:*:*:*:*:*	Akira rasnomware
Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-863, CWE-288	T1068: Exploitation for Privilege Escalation, T1110 : Brute Force	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-3259	✗	Cisco Adaptive Security Appliance (ASA): 9.5 - 9.13 Cisco Firepower Threat Defense (FTD): 6.2.3 - 6.5.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*	Akira ransomware
Cisco ASA and FTD Information Disclosure Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-200	T1082 : System Information Discovery, T1190: Exploit Public-Facing Application	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2015-2051	✗	Dir-645: All versions	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:dlink:dir-645_firmware:*:*:*:*:*:*:*:* cpe:2.3:h:dlink:dir-645:a1:*:*:*:*:*:*:*	Goldoon Botnet
D-Link DIR-645 Router Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1190 : Exploit Public-Facing Application, 1505 : Server Software Component	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10051

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Muddling Meerkat	China	All	All
	MOTIVE		
	-		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	-	-
TTPs			
TA0042: Resource Development; TA0043: Reconnaissance; TA0040: Impact; T1594: Search Victim-Owned Websites; T1584: Compromise Infrastructure; T1584.002: DNS Server; T1584.003: Virtual Private Server; T1584.001: Domains; T1584.005: Botnet; T1595: Active Scanning; T1595.002: Vulnerability Scanning; T1596: Search Open Technical Databases; T1593: Search Open Websites/Domains; T1498: Network Denial of Service			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">APT28 (aka 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, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard,BlueDelta,TA422, Fighting Ursa,Blue Athena)</td><td>Russia</td><td rowspan="3">Aerospace, Defense, Education, Energy, Utilities, Governments, Hospitality, Manufacturing, Oil & Gas, Retail, Technology, Transportation</td><td rowspan="3">Worldwide</td></tr>
<tr><td><b>MOTIVE</b></td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td><b>TARGETED CVEs</b></td><td><b>ASSOCIATED ATTACKS/RANSOMWARE</b></td><td><b>AFFECTED PRODUCTS</b></td></tr>
<tr><td>-</td><td>-</td><td>-</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0006: Credential Access; TA0011: Command and Control; TA0042: Resource Development; T1562: Impair Defenses; T1556: Modify Authentication Process; T1055: Process Injection; T1587: Develop Capabilities; T1584: Compromise Infrastructure; T1203: Exploitation for Client Execution; T1082: System Information: Discovery; T1546: Event Triggered Execution; T1557; Adversary-in-the-Middle; T1059: Command and Scripting Interpreter; T1219: Remote Access Software; T1018: Remote System Discovery; T1041: Exfiltration Over C2 Channel; T1562.001: Disable or Modify Tools; T1588: Obtain Capabilities</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **three exploited vulnerabilities** and block the indicators related to the threat actors **Muddling Meerkat, APT28** and malware **Akira, Goldoon, Cuckoo.**

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 vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Muddling Meerkat, APT28** and malware **Akira, Goldoon, Cuckoo** in Breach and Attack Simulation(BAS).

Threat Advisories

Akira Ransomware Nets $42 Million from 250+ Victims

The Enigmatic 'Muddling Meerkat’ Poses a Nation-State DNS Puzzle

Over 2 Million Malicious Repositories Planted on Docker Hub

Goldoon Botnet Exploits Longstanding D-Link Vulnerability

Cuckoo Malware Operates as Both an Infostealer and Spyware

Cybercriminals Forge Alliances via Compromised Routers

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 have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	d2fd0654710c27dcf37b6c1437880020824e161dd0bf28e3a133ed777242a0ca, dcfa2800754e5722acf94987bb03e814edcb9acebda37df6da1987bf48e5b05e, bc747e3bf7b6e02c09f3d18bdd0e64eef62b940b2f16c9c72e647eec85cf0138, 73170761d6776c0debacfbbc61b6988cb8270a20174bf5c049768a264bb8ffaf, 1b60097bf1ccb15a952e5bcc3522cf5c162da68c381a76abc2d5985659e4d386, aaa647327ba5b855bedea8e889b3fafdc05a6ca75d1cfd98869432006d6fecc9, 7d6959bb7a9482e1caa83b16ee01103d982d47c70c72fdd03708e2b7f4c552c4, 36cc31f0ab65b745f25c7e785df9e72d1c8919d35a1d7bd4ce8050c8c068b13c, 3298d203c2acb68c474e5fdad8379181890b4403d6491c523c13730129be3f75, 0ee1d284ed663073872012c7bde7fac5ca1121403f1a5d2d5411317df282796c, ffd9f58e5fe8502249c67cad0123ceeeaa6e9f69b4ec9f9e21511809849eb8fc, dfe6fddc67bdc93b9947430b966da2877fda094edf3e21e6f0ba98a84bc53198, 131da83b521f610819141d5c740313ce46578374abb22ef504a7593955a65f07, 9f393516edf6b8e011df6ee991758480c5b99a0efbfd68347786061f0e04426c,

Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	9585af44c3ff8fd921c713680b0c2b3bbc9d56add848ed62164f7c9b9f23d065, 2f629395fdfa11e713ea8bf11d40f6f240acf2f5fcf9a2ac50b6f7fbc7521c83, 7f731cc11f8e4d249142e99a44b9da7a48505ce32c4ee4881041beeddb3760be, 95477703e789e6182096a09bc98853e0a70b680a4f19fa2bf86cbb9280e8ec5a, 0c0e0f9b09b80d87ebc88e2870907b6cacb4cd7703584baf8f2be1fd9438696d, C9c94ac5e1991a7db42c7973e328fceeb6f163d9f644031bdfd4123c7b3898b0, aaa6041912a6ba3cf167ecdb90a434a62feaf08639c59705847706b9f492015d, 18051333e658c4816ff3576a2e9d97fe2a1196ac0ea5ed9ba386c46defafdb88, 5e1e3bf6999126ae4aa52146280fdb913912632e8bac4f54e98c58821a307d32, 8317ff6416af8ab6eb35df3529689671a700fdb61a5e6436f4d6ea8ee002d694, 892405573aa34dfc49b37e4c35b655543e88ec1c5e8ffb27ab8d1bbf90fc6ae0, 0b5b31af5956158bfbd14f6cbf4f1bca23c5d16a40dbf3758f3289146c565f43, 0d700ca5f6cc093de4abba9410480ee7a8870d5e8fe86c9ce103eec3872f225f, a2df5477cf924bd41241a3326060cc2f913aff2379858b148ddec455e4da67bc, 03aa12ac2884251aa24bf0ccd854047de403591a8537e6aba19e822807e06a45, 2e88e55cc8ee364bf90e7a51671366efb3dac3e9468005b044164ba0f1624422, 40221e1c2e0c09bc6104548ee847b6ec790413d6ece06ad675fff87e5b8dc1d5, 5ea65e2bb9d245913ad69ce90e3bd9647eb16d99230114537256548 6c77568a2, 643061ac0b51f8c77f2ed202dc91afb9879f796ddd974489209d45f84f644562, 6f9d50bab16b2532f4683eeb76bd25449d83bdd6c85bf0b05f716a4b49584f84, fef09b0aa37cbdb6a8f60a6bd8b473a7e5bffdc7fd2e952444f781574abccf64,

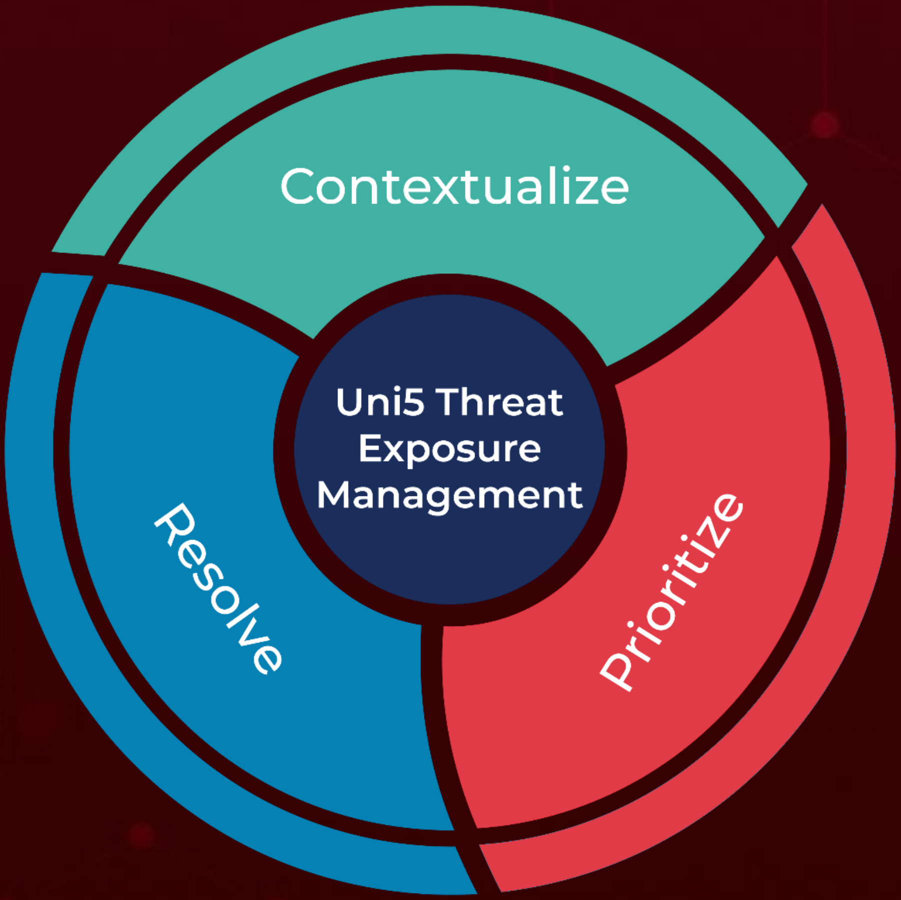
Attack Name	TYPE	VALUE
Akira Ransomware	SHA256	e1321a4b2b104f31aceaf4b19c5559e40ba35b73a754d3ae13d8e90c53146c0f, 74f497088b49b745e6377b32ed5d9dfaef3c84c7c0bb50fabf30363ad2e0bfb1, 3d2b58ef6df743ce58669d7387ff94740ceb0122c4fc1c4ffd81af00e72e60a4,
	MD5	7a647af3c112ad805296a22b2a276e7c
Goldoon	SHA256	66f21251d7f8c58316f149fec104723beb979a1215ad4e788d83f0ee6fd34696, 712d9abe8fbdff71642a4d377ef920d66338d73388bfee542f657f2e916e219c, d7367d41d19baa4f1022f8eb47f7ff1e13f583265c7c26ab96d5f716fa0d61ee, fdf6dae772f7003d0b7cdc55e047434dbd089e0dc7664a3fae8ccfd9d10ece8c, aa9e6006bce7d0b4554165dba76e67c4a44d98090c9e6ac9f3dca726f6e9adbf, fc44018b7432d9e6a1e98f723b0402101fa6e7483d098b10133aac142c0a4a0b, e7b78f16d0dfc91b4c7e8fd50fc31eba1eb22ec7030af9bf7c551b6019c79333, 0e6eb17664943756cab434af5d94fcd341f154cb36fc6f1ef5eb5cfdce68975f, 9af8720766c5f3978718c026c2263801b08634443c93bd67022c56c6ef531ef3, df71219ba6f5835309479b6e3eaca73b187f509b915420656bfe9a9cc32596c2, 48130a7c09a5c92e15b3fc0d2e1eb655e0bd8f759e01ba849f7734e32dbc2652, 8eb9c1eaecd0dcdd242e1bc8c62a1052915b627abe2de8ce147635fb7da3bfcc, b050a1ff0d205f392195179233493ff5b6f44adc93fe0dba1f78c4fe90ebcc46, ffd2d3888b6b1289e380fa040247db6a4fbd2555db3e01fadd2fe41a0fa2debc, 88cea61218bdeea94537b74c67873e75b8ada6d050a30d311569c3118d161c46, 115e15fbee077a9e126cc0eb349445df34cc9404245520c702fadc5f75b6f859, b10e47db989e29ace6c23ed15e29f313993f95e5e615711060881dfa84618071,

Attack Name	TYPE	VALUE
Goldoon	SHA256	037331ab84a841b9d3cfb6f8797c1695e2dc0a2cdcc3f8f3c794dfaa50bcf0df, 5631980fab33525f4de1b47be606cd518403f54fa71b81186f02dbf7e9ed0004, 246142a5e3f3d3f84d8b38f98ff6897b03628e06e31016b8fafc9eb8c2b6201d, 3123a458a6346fd14c5bd7d41cda6c9c9bdabc786366a9ab3d5e7c00132ff835, 45bf2c9c6628d87a3cb85ee78ae3e92a09949185e6da11c41e2df04a53bb1274, c81cfe4d3b98d0b28d3c3e7812beda005279bc6c67821b27571240eba440fa49
Cuckoo	SHA256	254663d6f4968b220795e0742284f9a846f995ba66590d97562e8f19049ffd4b, 1827db474aa94870aafdd63bdc25d61799c2f405ef94e88432e8e212dfa51ac7, d8c3c7eedd41b35a9a30a99727b9e0b47e652b8f601b58e2c20e2a7d30ce14a8, 39f1224d7d71100f86651012c87c181a545b0a1606edc49131730f8c5b56bdb7, a709dacc4d741926a7f04cad40a22adfc12dd7406f016dd668dd98725686a2dc
	Domains	http://tunesolo[.]com, http://fonedog[.]com, http://tunesfun[.]com, http://dumpmedia[.]com, http://tunefab[.]com
	URLs	http://146[.]70[.]80[.]123/static[.]php, http://146[.]70[.]80[.]123/index[.]php

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 6, 2024 • 5:30 AM

More at www.hivepro.com