Date of Publication
April 15, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

08 to 14 MARCH 2024

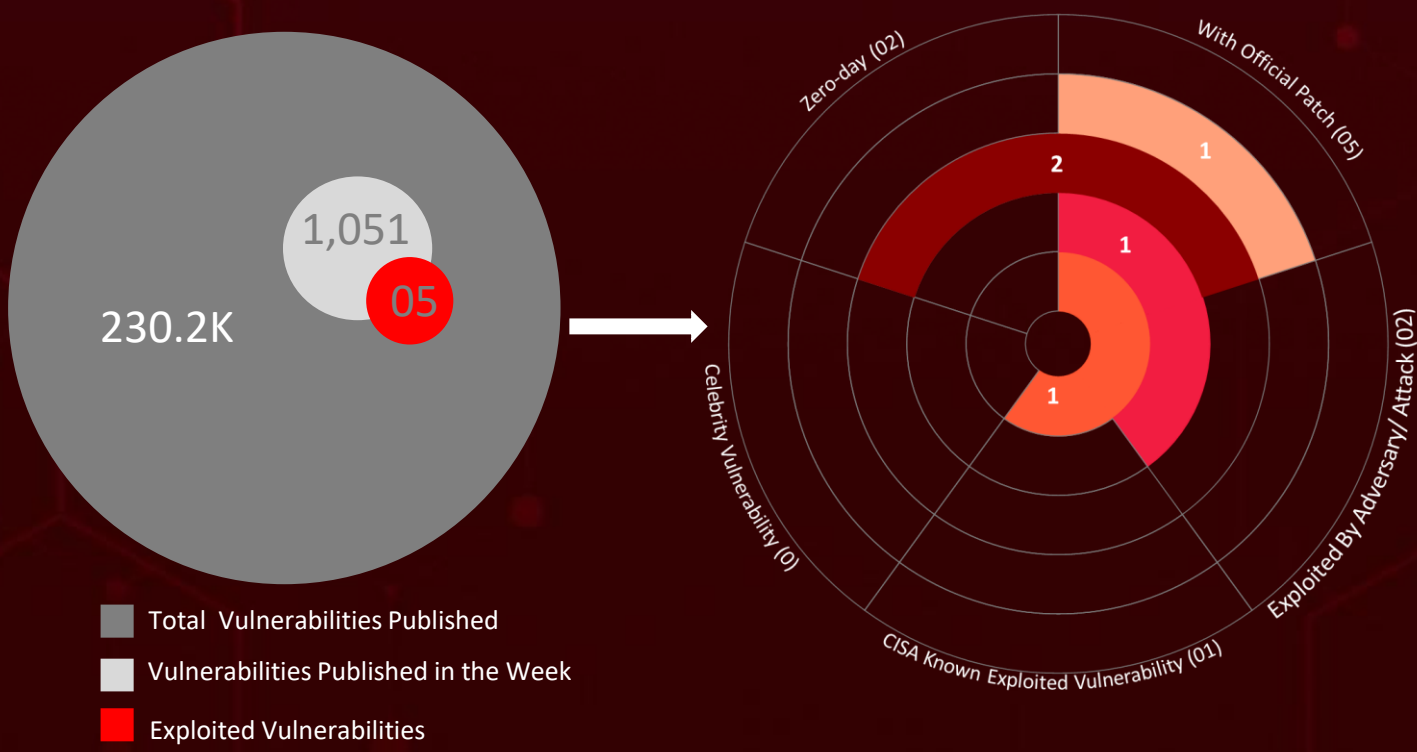
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries in the realm of cybersecurity threats. In the past week alone, HiveForce Labs discovered **six** executed attacks, uncovered **five** vulnerabilities, and identified **four** active adversaries. These findings underscore the persistent and escalating danger posed by cyberattacks.

Furthermore, HiveForce Labs discovered that cyber attackers have exploited a previously addressed critical vulnerability in **Magento**. They are specifically targeting e-commerce platforms to distribute a Stripe payment skimmer. **Latrodectus**, a newly emerged malware believed to be an evolution of the IcedID loader, was initially observed in the hands of **TA577**, followed by **TA578**.

Moreover, Microsoft's April 2024 Patch Tuesday addresses **two zero-day** vulnerabilities. **Lazy Koala** orchestrated a string of successful attacks, primarily targeting government entities across multiple countries in Eastern Europe and Central Asia. These attacks are on the rise, posing a significant and immediate threat to users worldwide.



High Level Statistics

6
Attacks Executed

5
Vulnerabilities Exploited

4
Adversaries in Action

- Latrodectus
- Nitrogen
- Raspberry Robin
- LazyStealer
- Rhadamanthys
- PrintSpoofer

- CVE-2024-20720
- CVE-2024-3273
- CVE-2024-26234
- CVE-2024-29988
- CVE-2023-45590

- TA577
- TA578
- Lazy Koala
- TA547

Insights

E-commerce Under Siege: Cybercriminals Strike with Magento Vulnerability Exploit

IcedID's Offspring: Latrodectus Malware Spotted in Malicious Campaigns Orchestrated by TA577 & TA578

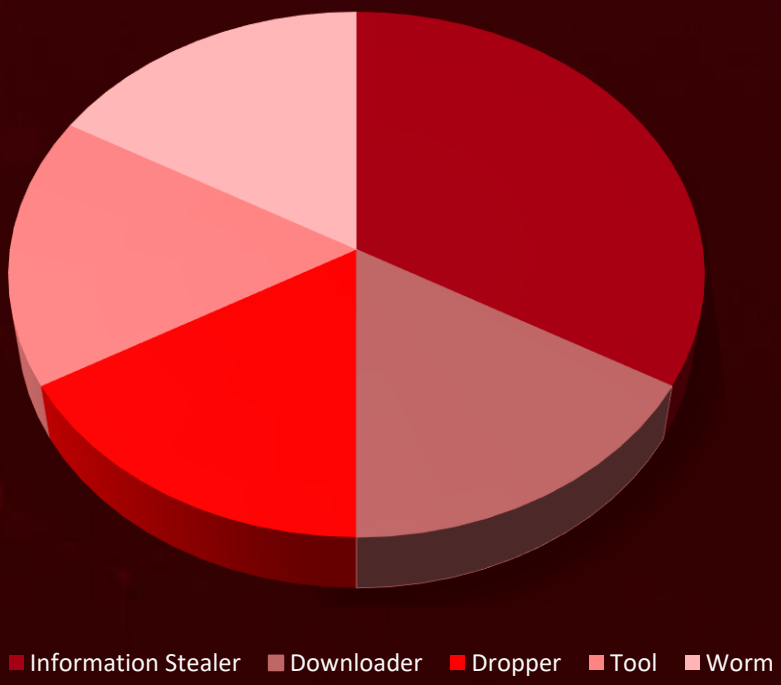
Urgent Alert: Unsupported D-Link NAS Devices Vulnerable to Exploitation (CVE-2024-3273)

Rogue Tactics: Lazy Koala's Successful Cyber Attacks Unveiled LazyStealer.

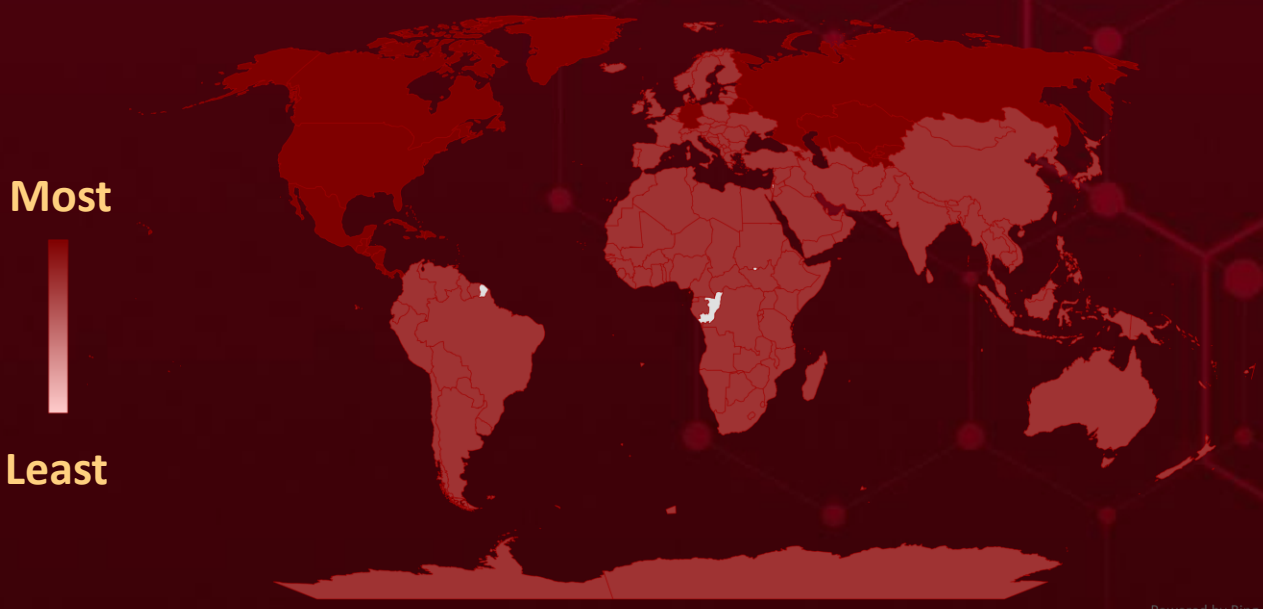
Invoice Phishing: TA547 Cybercriminals Spread Rhadamanthys Malware, Putting German Organizations Under Siege.

Notepad++ Nightmare: Hackers Inject Malware via MIME Tools Plugin

Threat Distribution

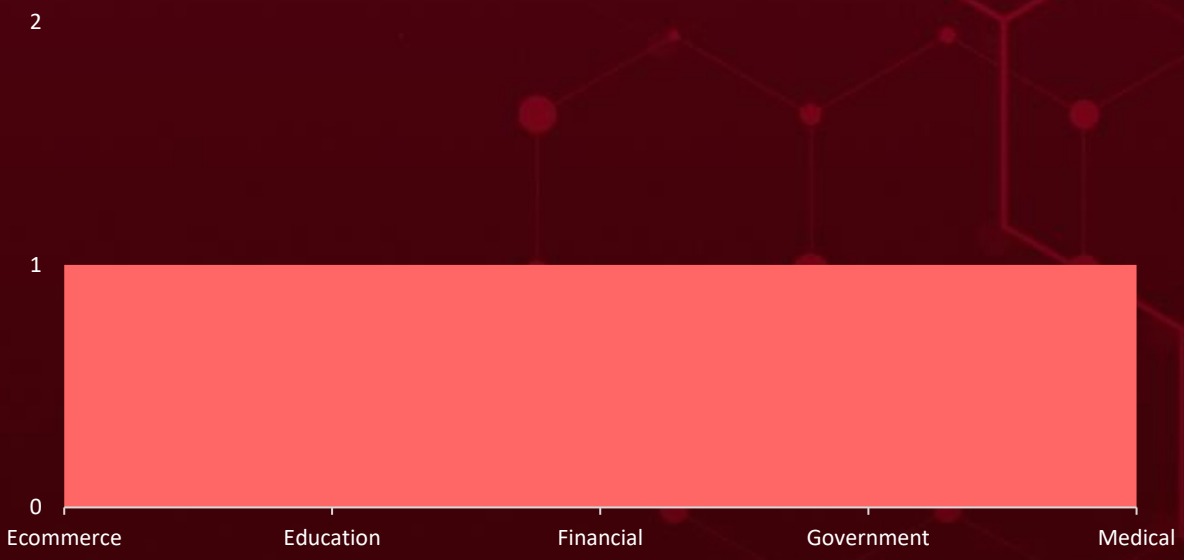


Targeted Countries



Countries	Countries	Countries	Countries
Germany	Saint Kitts and Nevis	Somalia	San Marino
Kyrgyzstan	Guatemala	Easter Island	Equatorial Guinea
Canada	Saint Barthélemy	Solomon Islands	Samoa
Uzbekistan	Greenland	Bulgaria	Djibouti
Haiti	Russia	Slovenia	Vatican City
United States	El Salvador	Iraq	Suriname
Curaçao	Puerto Rico	Slovakia	Vanuatu
U.S. Virgin Islands	Dominica	Thailand	Christmas Island
Belarus	Panama	Venezuela	Zimbabwe
Turks and Caicos Islands	Cuba	Ethiopia	Cameroon
Jamaica	Nicaragua	Sint Eustatius	Uruguay
Trinidad and Tobago	Cayman Islands	Cyprus	Brazil
Grenada	Montserrat	Singapore	Zambia
Tajikistan	British Virgin Islands	Central African Republic	Spain
Dominican Republic	Mexico	Sierra Leone	United Kingdom
Sint Maarten	Belize	Bonaire	Isle of Man
Costa Rica	Armenia	Seychelles	Saba
Saint Vincent and the Grenadines	Barbados	South Africa	Indonesia
Bermuda	Antigua and Barbuda	Serbia	Rwanda
Saint Pierre and Miquelon	Anguilla	Iceland	Hong Kong
Bahamas	Aruba	Senegal	United Arab Emirates
Saint Martin	Gabon	Guinea	Guyana
Kazakhstan	South Ossetia	Saudi Arabia	Romania
Saint Lucia	Comoros	Ghana	Togo
Honduras	Somaliland	São Tomé and Príncipe	Qatar
	Heard Island and McDonald Islands	Finland	Greece
			Ukraine

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1036** Masquerading
T1055 Process Injection	**T1204** User Execution	**T1082** System Information Discovery	**T1543** Create or Modify System Process	**T1497** Virtualization/ Sandbox Evasion
T1574 Hijack Execution Flow	**T1068** Exploitation for Privilege Escalation	**T1574.002** DLL Side-Loading	**T1083** File and Directory Discovery	**T1588.005** Exploits
T1140 Deobfuscate/ Decode Files or Information	**T1203** Exploitation for Client Execution	**T1204.002** Malicious File	**T1567** Exfiltration Over Web Service	**T1105** Ingress Tool Transfer

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Latrodectus	Latrodectus, a newly emerged malware believed to be an evolution of the IcedID loader, has been detected in malicious email campaigns since November 2023. It is suspected that the creators of IcedID are behind Latrodectus. Latrodectus functions as an emerging downloader, equipped with advanced sandbox evasion capabilities.	Phishing email	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		System Compromise, Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
TA577 and TA578			-
IOC TYPE	**VALUE**		
SHA256	fc21a125287c3539e11408587bcaa6f3b54784d9d458facbc54994f05d7ef1b0, 465f931e8a44b7f8dff8435255240b88f88f11e23bc73741b21c20be8673b6b7, 9e7fdc17150409d594eeed12705788fbc74b5c7f482a64d121395df781820f46		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Nitrogen	Nitrogen malware strains through fake advertisements posing as installations for well-known system tools like FileZilla or PuTTY. Using a DLL sideloading technique, the malware executes a malicious DLL file by launching a legitimate program.	Malvertising	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		System Compromise, Information Theft	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281, 2037ec95c91731f387d3c0c908db95184c93c3b8412b6b3ca3219f9f8ff60945, 033a286218baca97da19810446f9ebbaf33be6549a5c260889d359e2062778cf		

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
Raspberry Robin	The Raspberry Robin malware campaign, active since March 2024, employs malicious Windows Script Files (WSFs) to disseminate its malware. The Raspberry Robin employs a spectrum of anti-analysis and virtual machine (VM) detection mechanisms. The final payload remains dormant until the malware discerns that it is operating on a genuine end-user device rather than within a sandbox environment.	Social engineering and malvertising.	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Espionage	Windows
Worm			**PATCH LINK**
ASSOCIATED ACTOR			-
-			
IOC TYPE	**VALUE**		
SHA256	553b9eaa741adfb9073638e001d369441a802b406d3bca50436aea1df5b16da5, 4c87daaa84c41706156d3706036021479882622 9f5dedd6c46c821d879409509, 4e93fb810189d3e1df1d0ef0f30642b8891e4140301a4aaaf5cb93955588734d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LazyStealer	A cybercriminal group known as Lazy Koala orchestrated a string of successful attacks. Despite the simplicity of their methods, the malware they deployed, named LazyStealer, demonstrated remarkable effectiveness. The stolen data is either sold or repurposed for subsequent attacks, often aimed at corporate internal systems.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Information Theft, Espionage	-
Information Stealer			**PATCH LINK**
ASSOCIATED ACTOR			-
Lazy Koala			
IOC TYPE	**VALUE**		
MD5	4f060c5c6813e269f01e6cba1d3ac4cd, 641932b66490630005dde2aef405e5e9, 882d63c5ff749f232a3ce70a36c95b83		

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
Rhadamanthys	TA547, a financially motivated cybercriminal group in the recent attack campaign employed Rhadamanthys information stealer. The Rhadamanthys malware is directly downloaded into the system's memory. This technique, known as a fileless attack, bypasses traditional disk-based detection methods, making it more challenging to identify and prevent.	Phishing email	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, System Compromise, Espionage and Financial Loss	Windows
Information Stealer			
ASSOCIATED ACTOR			PATCH LINK
TA547			-
IOC TYPE	VALUE		
Domain	indscpm[.]xyz		
IPv4:Port	94[.]131[.]104[.]223:443		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PrintSpoofer	PrintSpoofer, a tool for privilege escalation, leveraging PowerShell's "invoke-webrequest" command. This tool exploits the SeImpersonatePrivilege to escalate user privileges and is employed in attacks targeting vulnerable services like web servers or database service providers.	Exploiting Redis services	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Information Theft, Espionage, Financial Loss	Redis
Tool			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
MD5	dbdcbacbc74b139d914747690ebe0e1c, b26b57b28e61f9320cc42d97428f3806		

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-2024-20720	✗	Adobe Commerce: 2.3.7 - 2.4.6-p3, Magento Open Source: 2.4.4 - 2.4.6-p3	Unknown
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:adobe:commerce:-:*:*:*:*:*:*:*	Stripe payment skimmer
Adobe OS Command Injection Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://helpx.adobe.com/security/products/magento/apsb24-03.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-3273	✗	DNS-320L Version 1.11, Version 1.03.0904.2013, Version 1.01.0702.2013 DNS-325 Version 1.01 DNS-327L Version 1.09, Version 1.00.0409.2013 DNS-340L Version 1.08	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:d-link:dns-320l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-325:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-327l:*:*:*:*:*:*:*:* cpe:2.3:a:d-link:dns-340l:*:*:*:*:*:*:*:*	skid.x86 (Mirai variant)
D-Link NAS Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-77	T1059: Command and Scripting Interpreter	https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10383

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-26234	✗ ZERO-DAY	Windows: 10 - 11 23H2 Windows Server: 2008 – 2022 23H2	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows Proxy Driver Spoofing Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-284	T1090: Proxy	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26234

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-29988	✗ ZERO-DAY	Windows: 10 - 11 23H2 Windows Server: 2019 – 2022 23H2	-
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows SmartScreen Prompt Security Feature Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-693	T1190: Exploit Public-Facing Application, T1040: Network Sniffing	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29988

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2023-45590</td><td>  </td><td rowspan="2">FortiClientLinux version 7.2.0, 7.0.6 through 7.0.10 and 7.0.3 through 7.0.4</td><td rowspan="2">-</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:fortinet:forticlient:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Fortinet FortiClient 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-94</td><td>T1059: Command and Scripting Interpreter</td><td>https://www.fortiguard.com/psirt/FG-IR-23-087</td></tr>
</table>

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
TA577 (aka Hive0118)</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gain</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Latrodectus downloader</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0040: Impact; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1055: Process Injection; T1497: Virtualization/Sandbox Evasion; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TA578	-	All	Worldwide
	MOTIVE		
	Financial Gain		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	Latrodectus downloader	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0040: Impact; TA0011: Command and Control; TA0010: Exfiltration; T1566: Phishing; T1059: Command and Scripting Interpreter; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1055: Process Injection; T1497: Virtualization/Sandbox Evasion; T1083: File and Directory Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Lazy Koala	-	Government, Financial, Medical, and Educational Institutions	Russia, Belarus, Kazakhstan, Uzbekistan, Kyrgyzstan, Tajikistan, and Armenia
	MOTIVE		
	Information Theft and Espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	LazyStealer	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; TA0010: Exfiltration; T1204.002: Malicious File; T1204: User Execution; T1140: Deobfuscate/Decode Files or Information; T1555.003: Credentials from Web Browsers; T1555: Credentials from Password Stores; T1567: Exfiltration Over Web Service; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.006: Python; T1055: Process Injection; T1211: Exploitation for Defense Evasion; T1027: Obfuscated Files or Information; T1212: Exploitation for Credential Access			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
TA547 (aka SCULLY SPIDER)</td><td>-</td><td rowspan="3">All</td><td rowspan="3">Germany</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gain, Financial Crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Rhadamanthys</td><td>Windows</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; T1566.001: Spearphishing Attachment; T1566: Phishing; T1204: User Execution; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1059.001: PowerShell; T1059: Command and Scripting Interpreter; T1036: Masquerading; T1204.002: Malicious File</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerabilities** and block the indicators related to the threat actors **TA577, TA578, Lazy Koala, TA547,** and malware **Latrodectus, Nitrogen, Raspberry Robin, LazyStealer, Rhadamanthys, PrintSpoofer.**

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 **TA577, TA578, Lazy Koala, TA547,** and malware **WikiLoader, Latrodectus, Nitrogen, Raspberry Robin, LazyStealer, Metasploit Stager, and PrintSpoofer** in Breach and Attack Simulation(BAS).

Threat Advisories

Hackers Pocket Payment Data via Magento Exploitation

Critical RCE Flaw Found in EoL D-Link NAS Devices

Notepad++ Plugin Compromised to Inject Malicious Code

Latrodectus The Silent Assassin Sneaking Past Defenses

Critical Rust Flaw Renders Windows Systems Vulnerable

Microsoft's April 2024 Patch Tuesday Addresses Two Zero-day Vulnerabilities

Malvertising Campaign Unleashes Nitrogen Malware Via Fake Installers

Critical RCE Flaw Found in Fortinet FortiClientLinux

Raspberry Robin Expands Reach via WSF

LazyStealer the Unconventional Approach to Cyber Espionage

TA547 Malware Campaign Hits German Businesses

Attackers Exploit 8-Year-Old Redis Servers to Deploy Metasploit Meterpreter

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
Latrodectus	URLs	hxxps://mazdakrichest[.]com/live/, hxxps://riverhasus[.]com/live/, hxxps://peermangoz[.]me/live/, hxxps://aprettopizza[.]world/live/, hxxps://nimeklroboti[.]info/live/, hxxps://frotneels[.]shop/live/, hxxps://arsimonopa[.]com/live, hxxps://lemonimonakio[.]com/live, hxxps://flurаresto[.]me/live/, hxxps://mastralakkot[.]live/live/, hxxps://postolwepok[.]tech/live/, hxxps://trasenanoyr[.]best/live/, hxxps://miistoria[.]com/live, hxxps://plwskoret[.]top/live, hxxps://sluitionsbad[.]tech/live/, hxxps://grebiunti[.]top/live/, hxxps://zumkoshapsret[.]com/live/, hxxps://jertacco[.]com/live/
	SHA256	fc21a125287c3539e11408587bcaa6f3b54784d9d458facbc54994f05d7ef1b0, 465f931e8a44b7f8dff8435255240b88f88f11e23bc73741b21c20be8673b6b7, 9e7fdc17150409d594eeed12705788fbc74b5c7f482a64d121395df781820f46, 53b0d542af077646bae5740f0b9423be9fb3c32e04623823e19f464c7290242f, 9fad77b6c9968ccf160a20fee17c3ea0d944e91eda9a3ea937027618e2f9e54e,

Attack Name	TYPE	VALUE
Latrodectus	SHA256	d8b902568386f588fb2d42a77cd39062ada13c9a3fed0adf20ab6510f3b4a681, 805b59e48af90504024f70124d850870a69b822b8e34d1ee551353c42a338bf7, d855daede0b97277d68e04c73ef0f2a36690faa77539914aa7948ee045427042
Nitrogen	URL	amplex-amplification[.]com/wp-includes/FileZilla_3.66.1_win64.zip, newarticles23[.]com/wp-includes/putty-64bit-0.80-installer.zip, support[.]hosting-hero[.]com/wp-includes/putty-64bit-0.80-installer.zip, mkt.geostrategy-ec[.]com/installer.zip
	SHA256	ecde4ca1588223d08b4fc314d6cf4bce82989f6f6a079e3eefe8533222da6281, 2037ec95c91731f387d3c0c908db95184c93c3b8412b6b3ca3219f9f8ff60945, 033a286218baca97da19810446f9ebbaf33be6549a5c260889d359e2062778cf
	IPv4	94.156.65[.]98, 94.156.65[.]115
Raspberry Robin	Domains	chroococcoid.sbs, polyideism.sbs, ophthalmomyositis.sbs, quarrelers.sbs, counterboring.sbs, brittlebush.sbs, noematachograph.sbs, hemimetabolism.sbs, spendthriftiness.sbs, misalienate.sbs, smartville.sbs, refractorily.sbs, syllabication.sbs, uninsolvent.sbs, mammaterijekasumy.sbs, dechlorinatingdermatropic.sbs, axiologies.sbs, okruzihealdsburg.sbs, halsalkalindivvies.sbs, squeezably.sbs, contretemps.sbs, indulgement.sbs, viandelarkishness.sbs,

Attack Name	TYPE	VALUE
Raspberry Robin	Domains	cunyguddlefrodina.sbs, audiovisuals.sbs, perrputtnomi.sbs, azoospermia.sbs, metriconetimeagley.sbs, dundeelieflydeflect.sbs, juniorstwosometogt.sbs, nametagsweatseyelike.sbs, glubeulaufuggy.sbs, bootedpindusvalenba.sbs, rockerstalbertcerate.sbs, biltongpumpsiecrumrod.sbs, jossesdialykreamer.sbs, ingressfloor-walker.sbs, freamingrafttwoway.sbs, craighleserapic.sbs, acid-fastlindbom.sbs, annuelertimes.sbs, kepfoipnjw.sbs, semantical.sbs, dominieunflaming.sbs, urvkwwqhjb.sbs, undefinitely.sbs, 294unmendaciously.sbs, oilproofing.sbs, sphere-born.sbs, 294anacamptometer.sbs, proconsulships.sbs, unthematically.sbs, hockersmixtecsquier.sbs, arctiidkwatumaindwelt.sbs, curricular.sbs, buxbaumiaceae.sbs, subextensibleness.sbs, unconstrainedness.sbs, anguilliform.sbs
	SHA256	553b9eaa741adfb9073638e001d369441a802b406d3bca50436aea1df5b16da5, 4c87daaa84c41706156d3706036021479882622 9f5dedd6c46c821d879409509, 4e93fb810189d3e1df1d0ef0f30642b8891e4140301a4aaaf5cb93955588734d, 0b369277901fff2ac52bf04e366318aa9018e7ea570779f476b2a0e676c9db83, ca6f46bdfd14021c102d4e4d95597a20bb9685628b4067b9ba85f18644ad6cdb,

Attack Name	TYPE	VALUE
Raspberry Robin	SHA256	98ad6aad996e4005389ea7e4782a4a082c1e83a8a20ad07bb3a3eed4047b3603, 9303b89abe2c0393e78991f74a90d9202a2f14dc267367277da7af705733eb32, 229c6b0dc9298a6868a24aad6cf3c8b08feb97f809f2d67fb6dc2e71ebee876b, 78ae67f650400ef6db9a85aa3d10ab7684f789e587ef33420a352a9b53916364, dd576545834e9c439491d62a8a6d9578a58693cef9f5cd2783fc80f49275dac8, fbdbe211e66792f3cefc50da6b3b88d82d497be1cd25f4654d4d122c0ed10a42, a3de553cae9671bd94aae75f76f8de2dd9abb41780d25f012debf7761a579ea9, 479d1cb582c03c679cb23ccb6b5dd1611822f59f311a6cdc82bd6eef5f53da14, d5dd3f1dd787746403843100c8dec9c70c20d8098071aafc5bfeef20b95fd93f, b4566c3cbfa193ad6dc7173d8b5d93734f06d940085110f6a2c7812524c2c236, 752ccebfcf2d63d44bf3073b2f30e83758aa0ae26d3bdca59de6e53e6d33b19e, a81176e32b8d73fbbd11d1a1da32789c8b18cf6aa79e1b4cae8ed031b7e9dbbf, 99d1e9839922063d3655583d541ac6908000222cd847c95c919a27c9d2b01301, 07b19580d9c5febb2b7d1da395022ca790372104bc99b35a8b18d506dfa2f9c0, 8921a869a93b4e9cec50b66b81793af67c2664aec5028c48738bae03f7026560, 981e56f56ab9c3dc81deed819ad3cd7367b8d44449a1ebbf1aad5033f2bd4547, 068f7a941ca655d71dd894c1564a24bbe9d67a6aa9e60b0692f558512e28c3a4, f2e1130b4baf1dc611fdde8029234348b4df69d5ebe32edc540e6fe1caaadd0a
LazyStealer	MD5	4f060c5c6813e269f01e6cba1d3ac4cd, 641932b66490630005dde2aef405e5e9, 882d63c5ff749f232a3ce70a36c95b83, fe245cf57be8b3daf8cdb3882de99f35, 8e233b0250d85ae63076af45ee829c55, 032a586d08e7f31e2aedbec61d5d0f62, 8cb819b48958540fac07244188508156, 2d51a6620c976e1d736448082338e0b1, 763eb39787756744b4062336eb945750,

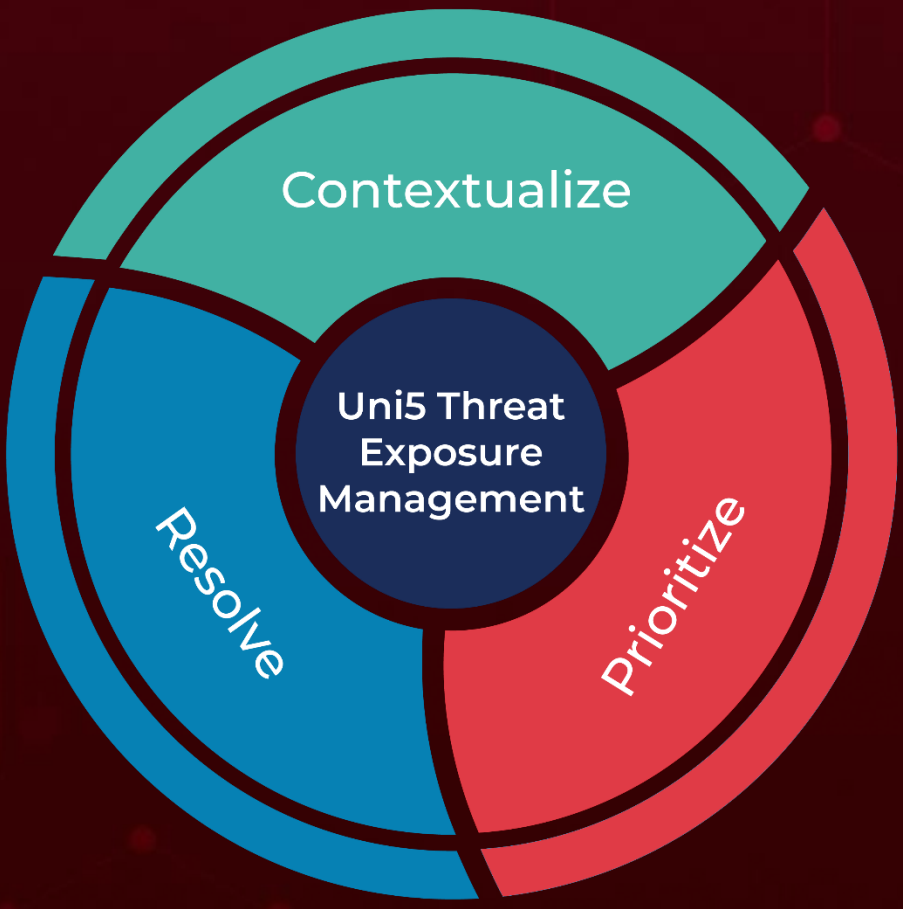
Attack Name	TYPE	VALUE
LazyStealer	MD5	5b84b516760773c538647bc6e4d26d37, 1dedf5772ea1126b79b5e22ca10cefd3, 0f5727bada96b3b62573bba51538e9e3, c3242bce783d5fa0ab0ce645f1283c64, 1cff5f65c85d8cf614beedf8fd5112d7, 98914403f428abeea89c94e0b7edaaa9
	SHA1	4f0a1831d4d8c09f46e8f5fbe8b17b024daa6eee, 9bad63eab92144b8a365428aa68531c80fc2da0f, cd1f89f3d56df6a775d8694c1cbf588961dc7f06, 40789ef406772e52a0dfc86509cc7617fa8b54a3, ec14cf28fe8764d4f285b95ee7001af49ff0af68, 51ad91409698d8f4017defbd0a382cce9e69ed6f, 1f204cfb02df849f935c296a5e4b2f120bfa563b, 755ade0ddaceaabe9577d22a240e0430375f502f, 7685dd23d64fa94bb8d2d54dd2e104fbe5379ec5, 3e497222f9bc13d43d6a3e5fbdcae3474b3d2d22, 140968b7004aca9785a0a1f0a6712322db22fd6c, 6f54d068423cee9b2cf5ef50b4348025f983e220, 845be44fb0d663636e500187d7d394714e562e08, c10637e35dfe326bd2c9a92f432d483f2f7591bd, 9866dfedbd311ed2f838ec56947cdf4ccabe8634
	SHA256	9fd197b7402285ed2a75dac9a5ce3ef499a58342fd0dcefe1c40443a12bc6832, e419a8158c6fe326dc7ab16dbd5f3b2723dffe8c9561fe835bb16f62a8fa61f5, a6e68f3066424daae4a54b2e0b01a4474a9a381469ae69daae6fef9a1626fa6d, 1db3d0ac68515b5c9876634605ba8492ba558f7df435bff2b20a74239107f3ec, 5ecdf5efe2a74db93450f2b35e942b91ee6dd1b0f545c04810d2794b748b1dea, 9fc75a6a17238ec3833dce0605b334c03fd84363f56313a5bf58d57ff286a9f9, 7d3733513e0645e66009e3d677af76653baa75c8ddf0d126aa0f270b56183272, 216f4e858f84269bee999fdc29dafbd79ec2270575e19a8626e25d5fe72a8f25, 8246e66ff043374477c06a612602f6e8a2cb487a33d8b046357a6c4870648ed1, ef6fb63259eac9f7642e468726a042f5a29576bf9f846b96fa6ded8bf145b64c, f2a8088f1a634e62a2d0e5b2d6427d67fae640bf03dd04c8571006e1f31d7992, bfa3718f6492dd337c127ccdbd8033b503ca089699ddbff3ac5c45f5f95f01e8,

Attack Name	TYPE	VALUE
LazyStealer	SHA256	1549114ea6d86198d29f79a009218ca991aa17d215a84b90e3c91ef3268180e4, 864a38b028d5b9e41fa0d4eee7cfa3a284d0ab9874b42cc4d50f1e2b2e26e1e5, 18e00bb5dee23815a89067258b11ef13d6327bcb3555d70596c906d4875ed8c2
Rhadamanthys	Domain	indscpm[.]xyz
	IPv4:Port	94[.]131[.]104[.]223:443
PrintSpoofer	MD5	dbdcbacbc74b139d914747690ebe0e1c, b26b57b28e61f9320cc42d97428f3806
	URL	hxxp://35.185.187[.]24/PrintSpoofer.exe

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

April 15, 2024 • 3:30 AM

More at www.hivepro.com