Date of Publication
January 03, 2024

Hive Pro®

HiveForce Labs

WEEKLY
THREAT DIGEST

Attacks, Vulnerabilities and Actors

25 to 31 DECEMBER 2023

Table Of Contents

Summary 03

High Level Statistics 04

Insights 05

Targeted Countries 06

Targeted Industries 07

Top MITRE ATT&CK TTPs 07

Attacks Executed 08

Vulnerabilities Exploited 12

Adversaries in Action 15

Recommendations 18

Threat Advisories 19

Appendix 20

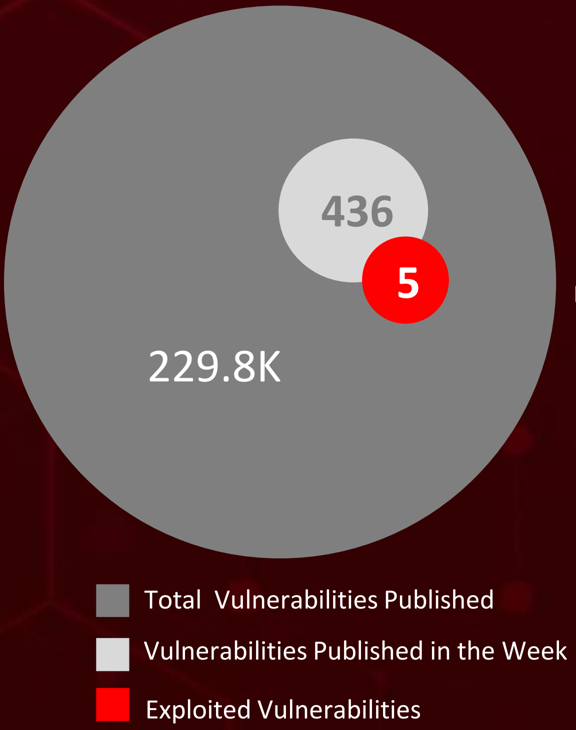
What Next? 23

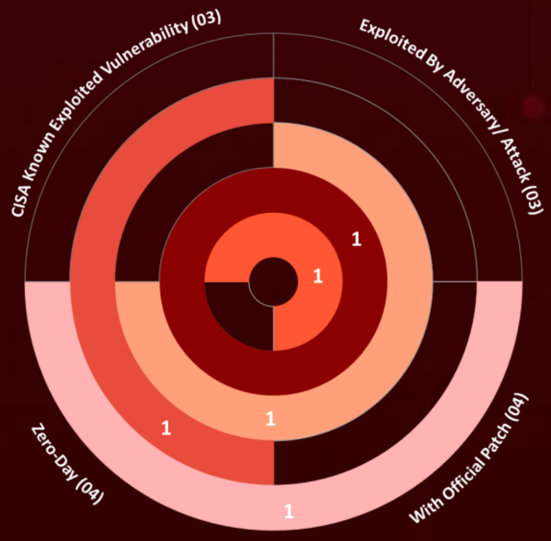
Summary

HiveForce Labs has recently made several significant discoveries related to cybersecurity threats. Over the past week, we identified a total of **eight** executed attacks, **four** instances of adversary activity, and **five** exploited vulnerability, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered **Operation RusticWeb**, targeting India to deploying Rust-based malware.

Meanwhile, a high severity zero-day vulnerability (**CVE-2023-51467**), in Apache OFBiz that could result in bypass authentication to achieve a simple Server-Side Request Forgery (SSRF) or enable arbitrary code execution. These observed attacks have been on the rise, posing a significant threat worldwide.





High Level Statistics

8

Attacks Executed

- MetaStealer
- LONEPAGE
- SEASPY
- SALTWATER
- AppleSeed
- AlphaSeed
- Meterpreter
- TinyNuke

5

Vulnerabilities Exploited

- CVE-2017-11882
- CVE-2023-38831
- CVE-2023-7102
- CVE-2023-7101
- CVE-2023-51467

4

Adversaries in Action

- Cloud Atlas
- UAC-0099
- UNC4841
- Kimsuky

Insights

CVE-2023-51467

a critical authentication bypass vulnerability in Apache OFBiz, leads to arbitrary code execution if exploited

MetaStealer surfaced in discreet online marketplaces with a pricing structure of USD 125 per month or
USD 1000 for an unlimited subscription

Kimsuky

group has been actively utilizing weaponized LNK files to deploy the AppleSeed malware

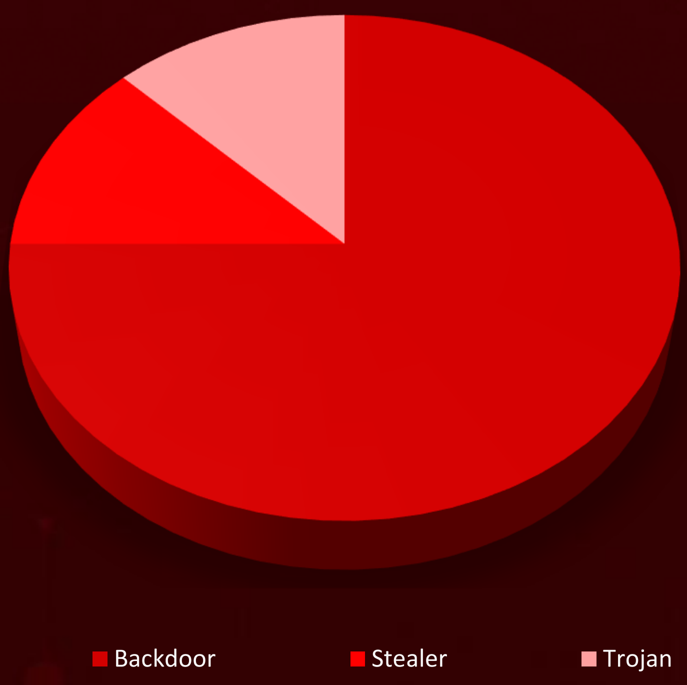
Cloud Atlas exploiting CVE-2017-11882, a six-year-old memory corruption vulnerability in Microsoft Office to initiate the execution of malicious payloads

UAC-0099 threat actor targeting Ukraine by leverage a critical vulnerability CVE-2023-38831 in WinRAR, to deploy LONEPAGE malware

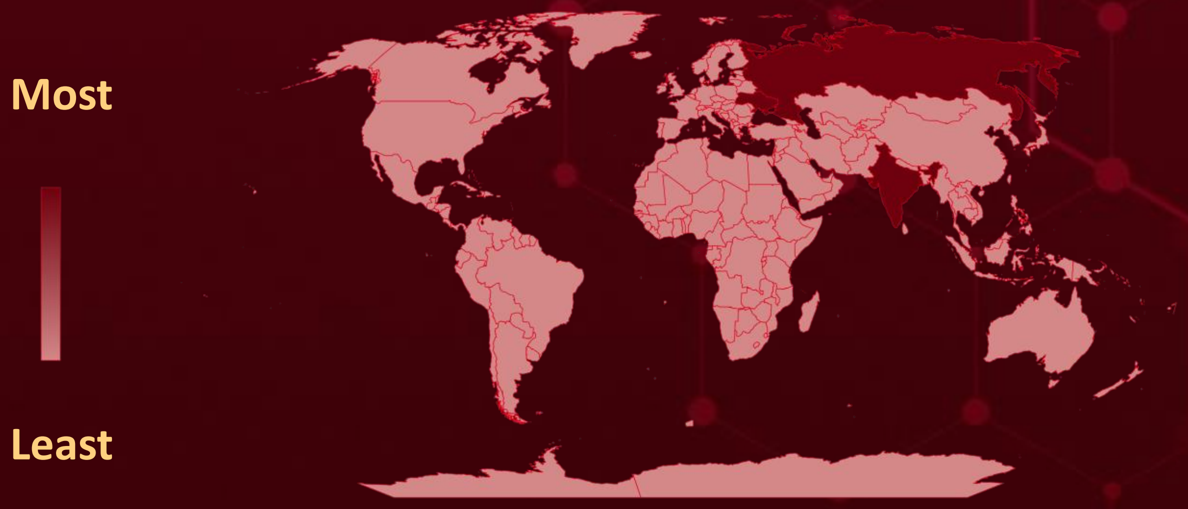
Operation RusticWeb

A phishing campaign targeting the Indian government and defense sector, deploying Rust-based malware

Threat Distribution



Targeted Countries



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

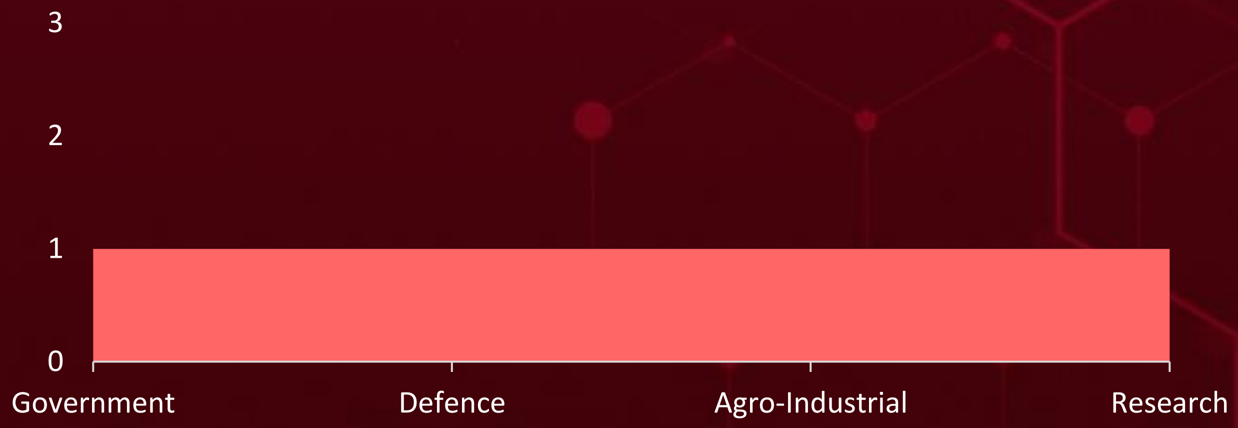
	Countries
■	Ukraine
■	Russia
■	India
□	Oman
□	Liechtenstein
□	State of Palestine
□	Angola
□	Mongolia
□	Antigua and Barbuda
□	Mexico
□	Argentina
□	Tuvalu
□	Armenia
□	Malta
□	Australia
□	Netherlands
□	Austria
□	Poland
□	Azerbaijan
□	Singapore
□	Bahamas
□	Thailand
□	Bahrain

	Countries
□	Vanuatu
□	Bangladesh
□	Malawi
□	Italy
□	Mexico
□	Belarus
□	Myanmar
□	Belgium
□	Nigeria
□	Belize
□	Mexico
□	Benin
□	Algeria
□	Bhutan
□	Japan
□	Bolivia
□	South Sudan
□	Bosnia and Herzegovina
□	Switzerland
□	Botswana
□	Trinidad and Tobago
□	Brazil

	Countries
□	Algeria
□	United Kingdom
□	Brunei
□	Zambia
□	Bulgaria
□	Luxembourg
□	Germany
□	Maldives
□	Burundi
□	Mauritania
□	Cabo Verde
□	Moldova
□	Cambodia
□	Morocco
□	United Arab Emirates
□	Nauru
□	Canada
□	South Africa
□	Central African Republic
□	North Macedonia
□	South Korea
□	Turkey
□	Chile
□	Peru

	Countries
□	China
□	Qatar
□	Colombia
□	Saint Kitts & Nevis
□	Comoros
□	Sao Tome & Principe
□	Congo
□	Seychelles
□	Costa Rica
□	Andorra
□	Côte d'Ivoire
□	Sri Lanka
□	Croatia
□	United States
□	France
□	Tajikistan
□	Cyprus
□	Iran
□	Czech Republic (Czechia)
□	Turkey
□	Denmark
□	Albania
□	Djibouti

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1071** Application Layer Protocol	**T1547** Boot or Logon Autostart Execution	**T1588** Obtain Capabilities
T1547.001 Registry Run Keys / Startup Folder	**T1036** Masquerading	**T1659** Content Injection	**T1566.001** Spearphishing Attachment	**T1071.001** Web Protocols
T1588.006 Vulnerabilities	**T1203** Exploitation for Client Execution	**T1204.002** Malicious File	**T1588.005** Exploits	**T1583.001** Domains
T1608.001 Upload Malware	**T1059.001** PowerShell	**T1587.001** Malware	**T1059.005** Visual Basic	**T1027** Obfuscated Files or Information

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
MetaStealer	A new information-stealing malware, available for sale for USD125 per month or USD1000 for unlimited use. Crafted to stealthily infiltrate target systems, facilitating the potential theft of passwords, cryptocurrency wallets, banking information, identity compromise, and financial losses.	Emails	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Theft of passwords, cryptocurrency wallets, banking information, identity compromise, and financial losses	-
Stealer			
ASSOCIATED ACTOR			**PATCH LINK**
-			-

IOC TYPE	VALUE
Domains	wgcuwcgociewewoo[.]xyz, ockimqekmwecocug[.]xyz, kiqewcsyeyaeusag[.]xyz
SHA256	949c5ae4827a3b642132faf73275fb01c26e9dce151d6c5467d3014f208f77ca, 99123063690e244f95b89d96759ec7dbc28d4079a56817f3152834047ab047eb

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LONEPAGE	The VBS malware LONEPAGE, when executed, it creates a hidden PowerShell process that communicates with a hardcoded C2 URL to fetch a text file	-	CVE-2023-38831
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Deploying additional payloads like keyloggers, data stealers, and screenshot tools	WinRAR
Backdoor			
ASSOCIATED ACTOR			**PATCH LINK**
UAC-0099			Update WinRAR version to 6.23 or later versions

IOC TYPE	VALUE
SHA256	8aca535047a3a38a57f80a64d9282ace7a33c54336cd08662409352c23507602, 4e8de351db362c519504509df309c7b58b891baf9cb99a3500b92fe0ef772924, a10209c10bf373ed682a13dad4ff3aea95f0fdcd48b62168c6441a1c9f06be37

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
SEASPY	This malware is a persistent backdoor that masquerades as a legitimate network service. The malware is designed to listen to commands received from the Threat Actor's Command-and-Control through TCP packets.	Exploiting Vulnerabilities	CVE-2023-7102 CVE-2023-7101
		IMPACT	AFFECTED PRODUCTS
TYPE		Monitor Traffic, Execute commands	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::Parse Excel
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC4841			https://www.barracuda.com/company/legal/esg-vulnerability
IOC TYPE	VALUE		
MD5	7b83e4bd880bb9d7904e8f553c2736e3		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SALTWATER	SALTWATER is a module for the Barracuda SMTP daemon (bsmtpd) that has backdoor functionality. SALTWATER can upload or download arbitrary files, execute commands, and has proxy and tunneling capabilities	Exploiting Vulnerabilities	CVE-2023-7102 CVE-2023-7101
		IMPACT	AFFECTED PRODUCTS
TYPE		Upload and download files, execute commands	Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::Parse Excel
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
UNC4841			https://www.barracuda.com/company/legal/esg-vulnerability
IOC TYPE	VALUE		
MD5	d493aab1319f10c633f6d223da232a27		

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
AppleSeed	AppleSeed is a backdoor that can receive the threat actor’s commands from the C&C server and execute the received commands. The threat actor can use AppleSeed to control the infected system.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft, install additional malwares, take screenshots	-
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-

IOC TYPE	VALUE
MD5	db5fc5cf50f8c1e19141eb238e57658c, 6a968fd1608bca7255c329a0701dbf58, cafc26b215550521a12b38de38fa802b
URL	hxxp://bitburny.kro[.]kr/aha/, hxxp://bitthum.kro[.]kr/hu/

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
AlphaSeed	AlphaSeed is a malware developed in Golang and supports similar features to AppleSeed such as command execution and infostealing.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data theft	-
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-

IOC TYPE	VALUE
MD5	d94c6323c3f77965451c0b7ebeb32e13, 52ff761212eeaadcd3a95a1f8cce4030, 4cb843f2a5b6ed7e806c69e6c25a1025, b6ab96dc4778c6704b6def5db448a020

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
Meterpreter	Meterpreter is a backdoor provided by Metasploit and is used to control infected systems.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Backdoor			-
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
MD5	232046aff635f1a5d81e415ef64649b7, 58fafabd6ae8360c9d604cd314a27159, e582bd909800e87952eb1f206a279e47, ac99b5c1d66b5f0ddb4423c627ca8333		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
TinyNuke	TinyNuke, also known as Nuclear Bot, is a banking malware. It includes features such as HVNC (HiddenDesktop/VNC), reverse SOCKS4 proxy, and form grabbing.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal passwords and inject arbitrary content	-
Trojan			
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
MD5	e34669d56a13d607da1f76618eb4b27e		
IP	45.114.129[.]138:33890		

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

Vulnerabilities Exploited

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2017-11882</td><td>✗</td><td rowspan="2">Microsoft Office 2007 - 2016</td><td rowspan="2">Cloud Atlas</td></tr>
<tr><th>ZERO-DAY</th></tr>
<tr><td>✗</td><th>AFFECTED CPE</th><th>ASSOCIATED ATTACKS/RANSOMWARE</th></tr>
<tr><th>NAME</th><th>CISA KEV</th><td rowspan="2">cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*
cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:*
cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*
cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Microsoft Office Memory Corruption Vulnerability</td><td>✓</td></tr>
<tr><th>CWE ID</th><th>ASSOCIATED TTPs</th><th>PATCH LINK</th></tr>
<tr><td>CWE-119</td><td>T1059: Command and Scripting Interpreter</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831	✗	WinRAR version 6.22 and older versions	UAC-0099
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:6.23:beta 1:*:*:*:*:*:*	LONEPAGE
RARLAB WinRAR Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	Update WinRAR version to 6.23 or later versions

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7102	✗	Barracuda’s Email Security Gateway (ESG): 5.1.3 - 9.2.1.001	UNC4841
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:barracuda:esg_appliance:9.2.1.001:*:*:*:*:*:*:*	SEASPY and SALTWATER
Barracuda ESG Arbitrary Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-1104	T1059: Command and Scripting Interpreter	https://www.barracuda.com/company/legal/esg-vulnerability

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-7101	☒	Spreadsheet::ParseExcel version 0.65	UNC4841
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:douglas_wilson:spreadsheet_parseexcel:0.65:*:*:*:*:*:*:*	SEASPY and SALTWATER
Spreadsheet::ParseExcel Arbitrary Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-95	T1059: Command and Scripting Interpreter	Not yet Patched

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-51467	☒	Apache OFBiz before 18.12.11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:ofbiz:*:*:*:*:*:*:*:*	-
Apache OFBiz Pre-authentication Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-918 CWE-287	T1059: Command and Scripting Interpreter	https://ofbiz.apache.org/download.html

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Cloud Atlas (aka Inception Framework, Oxygen, ATK 116, Blue Odin, The Rocra)	Russia	Russian agro-industrial enterprise and a state-owned research company	Afghanistan, Armenia, Austria, Azerbaijan, Belarus, Belgium, Brazil, Congo, Cyprus, France, Georgia, Germany, Greece, India, Indonesia, Iran, Italy, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Lithuania, Malaysia, Moldova, Morocco, Mozambique, Oman, Pakistan, Paraguay, Portugal, Qatar, Romania, Russia, Saudi Arabia, South Africa, Suriname, Switzerland, Tajikistan, Tanzania, Turkey, Turkmenistan, Uganda, Ukraine, UAE, USA, Uzbekistan, Venezuela, Vietnam
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2017-11882	-	Microsoft Office

TTPs

TA0043: Reconnaissance; TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0011: Command and Control; T1589: Gather Victim Identity Information; T1589.002: Email Addresses; T1583: Acquire Infrastructure; T1583.001: Domains; T1585: Establish Accounts; T1585.002: Email Accounts; T1587: Develop Capabilities; T1587.001: Malware; T1587.004: Exploits; T1608: Stage Capabilities; T1608.001: Upload Malware; T1566: Phishing; T1566.001: Spearphishing Attachment; T1559: Inter-Process Communication; T1559.001: Component Object Model; T1203: Exploitation for Client Execution; T1204: User Execution; T1204.002: Malicious File; T1059: Command and Scripting Interpreter; T1059.005: Visual Basic; T1547: Boot or Logon Autostart Execution; T1547.001: Registry Run Keys / Startup Folder; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1070: Indicator Removal; T1070.004: File Deletion; T1564: Hide Artifacts; T1564.004: NTFS File Attributes; T1221: Template Injection; T1218: System Binary Proxy Execution; T1218.005: Mshta; T1082: System Information Discovery; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1105: Ingress Tool Transfer

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">UAC-0099</td><td>-</td><td rowspan="3">-</td><td rowspan="3">Ukraine</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>CVE-2023-38831</td><td>LONEPAGE</td><td>WinRAR</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1547: Boot or Logon Autostart Execution; T1053: Scheduled Task/Job; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.005: Visual Basic; T1560: Archive Collected Data; T1106: Native API; T1176: Browser Extensions; T1566: Phishing; T1566.001: Spearphishing Attachment; T1036: Masquerading; T1041: Exfiltration Over C2 Channel; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1071: Application Layer Protocol; T1071.001: Web Protocols;</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="5">UNC4841</td><td>China</td><td rowspan="3">-</td><td rowspan="3">-</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>CVE-2023-7102
CVE-2023-7101</td><td>SEASPY and SALTWATER</td><td>Barracuda Email Security Gateway (ESG) Appliance, Spreadsheet::Parse Excel</td></tr>
<tr><td colspan="4"><b>TTPs</b></td></tr>
<tr><td colspan="4">TA0002: Execution; TA0042: Resource Development; T1588: Obtain Capabilities; T1588.006: Vulnerabilities; T1204.002: Malicious File; T1203: Exploitation for Client Execution; T1588.005: Exploits; T1659: Content Injection</td></tr>
</table>

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	AppleSeed, AlphaSeed, Meterpreter, TinyNuke	-
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; T1547: Boot or Logon Autostart Execution; T1056: Input Capture; T1036: Masquerading; T1543: Create or Modify System Process; T1071: Application Layer Protocol; T1102: Web Service; T1113: Screen Capture; T1059: Command and Scripting Interpreter; T1059.007: JavaScript; T1021: Remote Services; T1566: Phishing; T1566.002: Spearphishing Link			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **five exploited vulnerability** and block the indicators related to the threat actor **Cloud Atlas, UAC-0099, UNC4841, Kimsuky** and malware **MetaStealer, LONEPAGE, AppleSeed, AlphaSeed, Meterpreter, TinyNuke.**

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 **Cloud Atlas, UAC-0099, UNC4841, Kimsuky** and malware **MetaStealer, LONEPAGE, AppleSeed, AlphaSeed, Meterpreter, TinyNuke** in Breach and Attack Simulation(BAS).

Threat Advisories

MetaStealer a $125 Ticket to Digital Chaos

Operation RusticWeb: Coordinated Strikes on Indian Government

Cloud Atlas Exploits Six-Year-Old Flaw to Target Russian Companies

UAC-0099 Utilizes WinRAR Exploit to Deploy LONEPAGE Malware

Barracuda Fixes ACE Zero-day Vulnerability Exploited by Attackers

Terrapin Attack Downgrading the Fortresses of SSH

Kimsuky Group's Intriguing Exploits with AppleSeed Malware

Zero-Day Authentication Bypass Exploit in Apache OFBiz

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.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
MetaStealer	Domains	wgcuwcgociewewoo[.]xyz, ockimqekmwecocug[.]xyz, kiqewcsyeyaeusag[.]xyz, cewgwsyookogmmki[.]xyz, startworkremotely[.]com, csyeywqwyikqaiim[.]xyz, iqaeaoeueeqouweo[.]xyz, mmswgeewswyyywqk[.]xyz, accounts[.]google[.]com, iqwgwsigmigiqgoa[.]xyz
	SHA256	949c5ae4827a3b642132faf73275fb01c26e9dce151d6c5467d3014f208f77ca, 99123063690e244f95b89d96759ec7dbc28d4079a56817f3152834047ab047eb, c5597da40dee419696ef2b32cb937a11fcad40f4f79f9a80f6e326a94e81a90f
LONEPAGE	SHA256	8aca535047a3a38a57f80a64d9282ace7a33c54336cd08662409352c23507602, 4e8de351db362c519504509df309c7b58b891baf9cb99a3500b92fe0ef772924, a10209c10bf373ed682a13dad4ff3aea95f0fdcd48b62168c6441a1c9f06be37, 39d56eab8adfe9eb244914dde42ec7f12f48836d3ba56c479ab21bdbc41025fe, 96ab977f8763762af26bad2b6c501185b25916775b4ed2d18ad66b4c38bd5f0d,

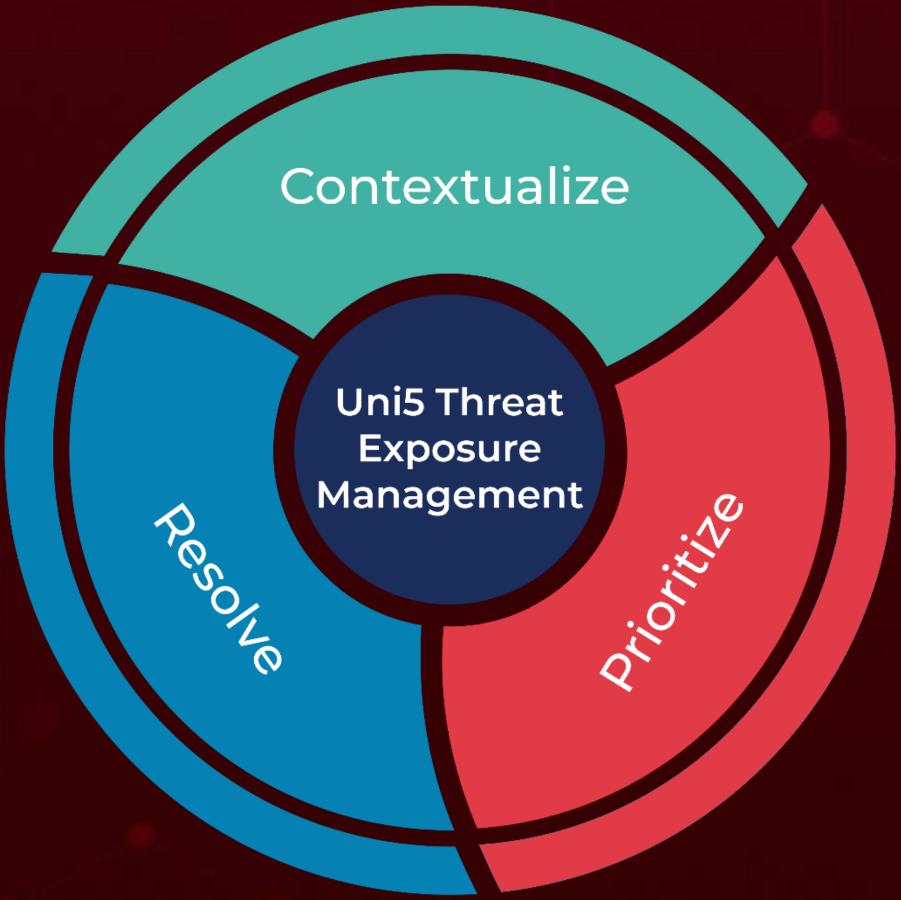
Attack Name	TYPE	VALUE
LONEPAGE	SHA256	e34fc4910458e9378ea357baf045e9c0c21515a0b8818a5b36daceb2af464ea0, 6f5f265110490158df91ca8ad429a96f8af69ca30b9e3b0d9c11d4fef74091e8
SEASPY	MD5	7b83e4bd880bb9d7904e8f553c2736e3
SALTWATER	MD5	d493aab1319f10c633f6d223da232a27
AppleSeed	MD5	db5fc5cf50f8c1e19141eb238e57658c, 6a968fd1608bca7255c329a0701dbf58, cafc26b215550521a12b38de38fa802b, 76831271eb117b77a57869c80bfd6ba6, b5d3e0c3c470d2d41967229e17259c87, 4511e57ae1eacdf1c2922bf1a94bfb8d, 02843206001cd952472abf5ae2b981b2, 8aeacd58d371f57774e63d217b6b6f98, cacf04cd560b70eaaf0e75f3da9a5e8f, 7a7937f8d4dcb335e96db05b2fb64a1b, f3a55d49562e41c7d339fb52457513ba, 5d3ab2baacf2ad986ed7542eeabf3dab, d4ad31f316dc4ca0e7170109174827cf, 1f7d2cbfc75d6eb2c4f2b8b7a3eec1bf, ae9593c0c80e55ff49c28e28bf8bc887, b6f17d59f38aba69d6da55ce36406729, 153383634ee35b7db6ab59cde68bf526, c560d3371a16ef17dd79412f6ea99d3a, 0cce02d2d835a996ad5dfc0406b44b01
	URL	hxxp://bitburny.kro[.]kr/aha/, hxxp://bitthum.kro[.]kr/hu/, hxxp://doma2.o-r[.]kr//, hxxp://my.topton.r-e[.]kr/address/, hxxp://nobtwoseb1.n-e[.]kr//, hxxp://octseven1.p-e[.]kr//, hxxp://tehyeran1.r-e[.]kr//, hxxp://update.ahnlaib.kro[.]kr/aha/, hxxp://update.doumi.kro[.]kr/aha/, hxxp://update.onedrive.p-e[.]kr/aha/, hxxp://yes24.r-e[.]kr/aha/
AlphaSeed	MD5	d94c6323c3f77965451c0b7ebeb32e13, 52ff761212eeaadcd3a95a1f8cce4030, 4cb843f2a5b6ed7e806c69e6c25a1025, b6ab96dc4778c6704b6def5db448a020
Meterpreter	MD5	232046aff635f1a5d81e415ef64649b7, 58fafabd6ae8360c9d604cd314a27159, e582bd909800e87952eb1f206a279e47, ac99b5c1d66b5f0ddb4423c627ca8333

Attack Name	TYPE	VALUE
Meterpreter	IP	104.168.145[.]83:993, 159.100.6[.]137:993, 38.110.1[.]69:993, 107.148.71[.]88:993
TinyNuke	MD5	e34669d56a13d607da1f76618eb4b27e
	IP	45.114.129[.]138:33890

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

January 03, 2023 • 7:00 AM

More at www.hivepro.com