

Date of Publication
September 30, 2024



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

23 to 29 September 2024

Table Of Contents

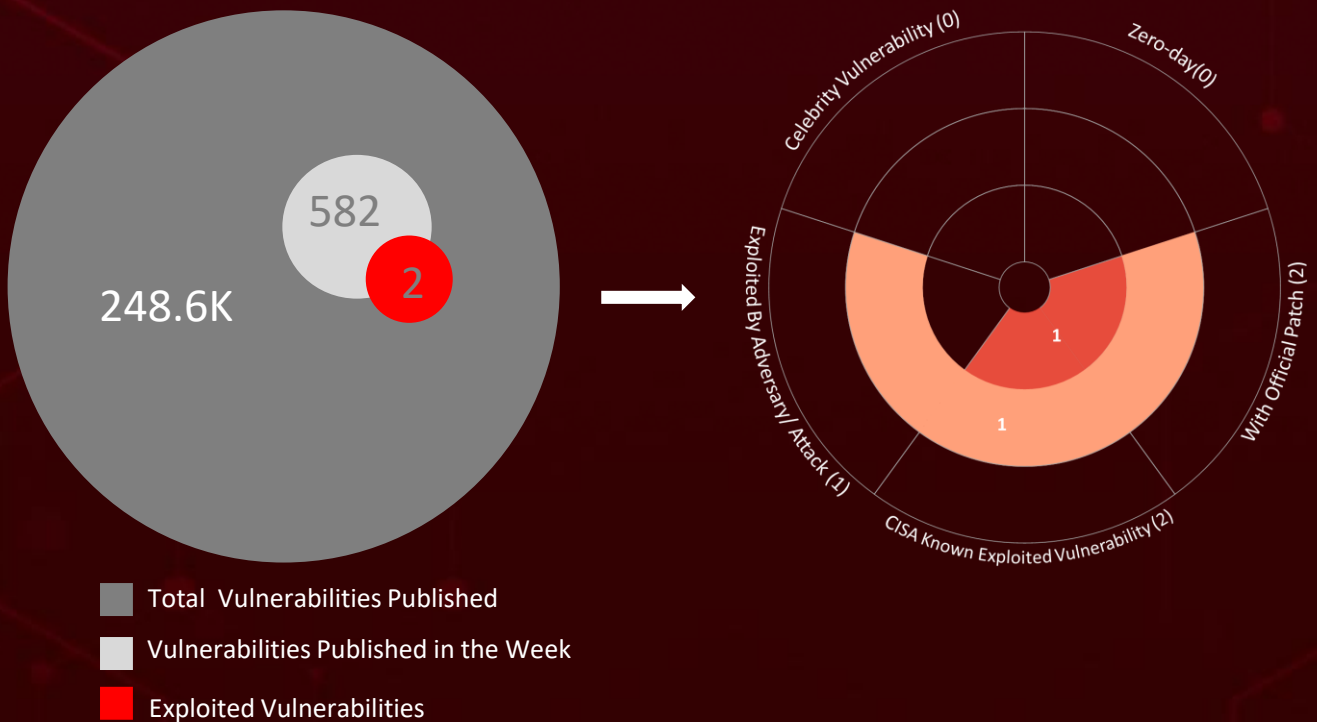
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	15
<u>Adversaries in Action</u>	16
<u>Recommendations</u>	20
<u>Threat Advisories</u>	21
<u>Appendix</u>	22
<u>What Next?</u>	27

Summary

HiveForce Labs has recently made significant advancements in identifying cybersecurity threats. Over the past week, they detected **twelve** attacks, reported **two** vulnerabilities, and identified **four** active adversaries. These findings underscore the relentless and escalating danger of cyber intrusions.

Additionally, **Earth Baxia** is a cyber espionage group targeting Asia-Pacific government organizations, particularly in Taiwan, utilizing spear-phishing tactics and the GeoServer vulnerability (**CVE-2024-36401**). This campaign aims to steal sensitive data from organizations through sophisticated attacks.

Furthermore, this week, North Korea's Lazarus Group has persisted with two active cyber campaigns, **PondRAT malware**, hidden in Python packages on PyPI, targeting software developers, and "**Operation Dream Job**," a phishing campaign aimed at the energy and aerospace sectors to deploy the **MISTPEN** backdoor via the **BURNBOOK** launcher. These rising threats pose significant and immediate dangers to users worldwide.



High Level Statistics

12

Attacks
Executed

2

Vulnerabilities
Exploited

4

Adversaries in
Action

- [Diamorphine](#)
- [EAGLEDOOR](#)
- [PondRAT](#)
- [POOLRAT](#)
- [BURNBOOK](#)
- [TEARPAGE](#)
- [MISTPEN](#)
- [SnipBot](#)
- [RomCom](#)
- [KLogExe](#)
- [FPSpy](#)
- [RIPCOY](#)

- [CVE-2024-36401](#)
- [CVE-2024-7593](#)

- [TeamTNT](#)
- [Earth Baxia](#)
- [Gleaming
Pisces](#)
- [Sparkling
Pisces](#)



Insights

Critical flaw discovered in **Microchip Advanced Software Framework (ASF)**, which could potentially lead to remote code execution.

SnipBot, a newly identified variant from the RomCom malware family, employs advanced infection and evasion techniques.

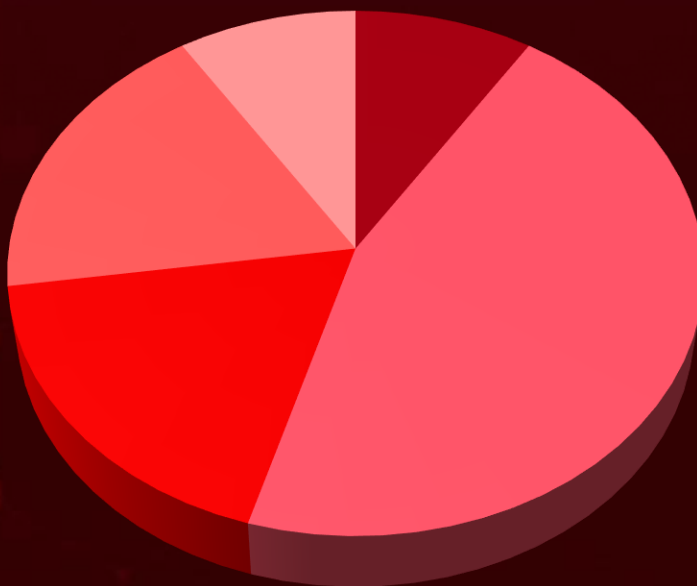
TeamTNT, a cybercriminal group, has resurfaced, now targeting VPS infrastructures running CentOS to deploy cryptocurrency miners.

Earth Baxia is a cyber espionage group targeting Taiwan's government using spear-phishing and exploiting the GeoServer vulnerability (CVE-2024-36401) with the **EAGLEDOOR** backdoor for data exfiltration.

The Lazarus Group, recently targeted software developers with PondRAT malware in Python packages and launched "**Operation Dream Job**" phishing campaigns aimed at the energy and aerospace sectors to deploy the MISTPEN backdoor via the BURNBOOK launcher.

Sparkling Pisces (aka Kimsuky), has deployed KLogEXE and FPSpy malware strains to enhance their cyber espionage operations.

Threat Distribution



■ Rootkit ■ Backdoor ■ Loader ■ RAT ■ Keylogger ■ Trojan

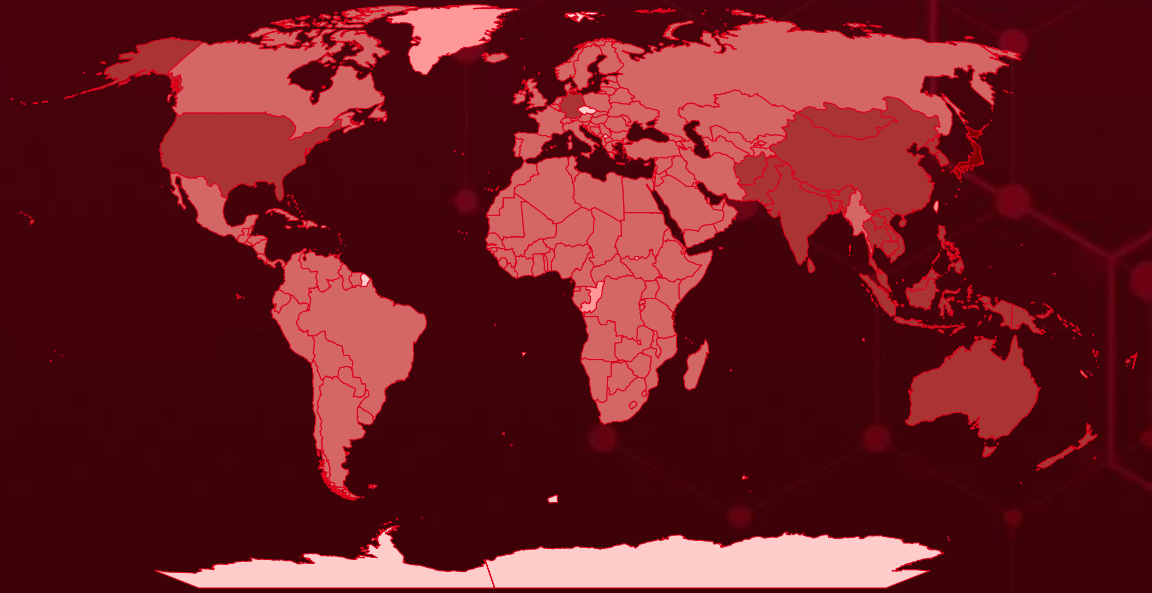


Targeted Countries

Most



Least

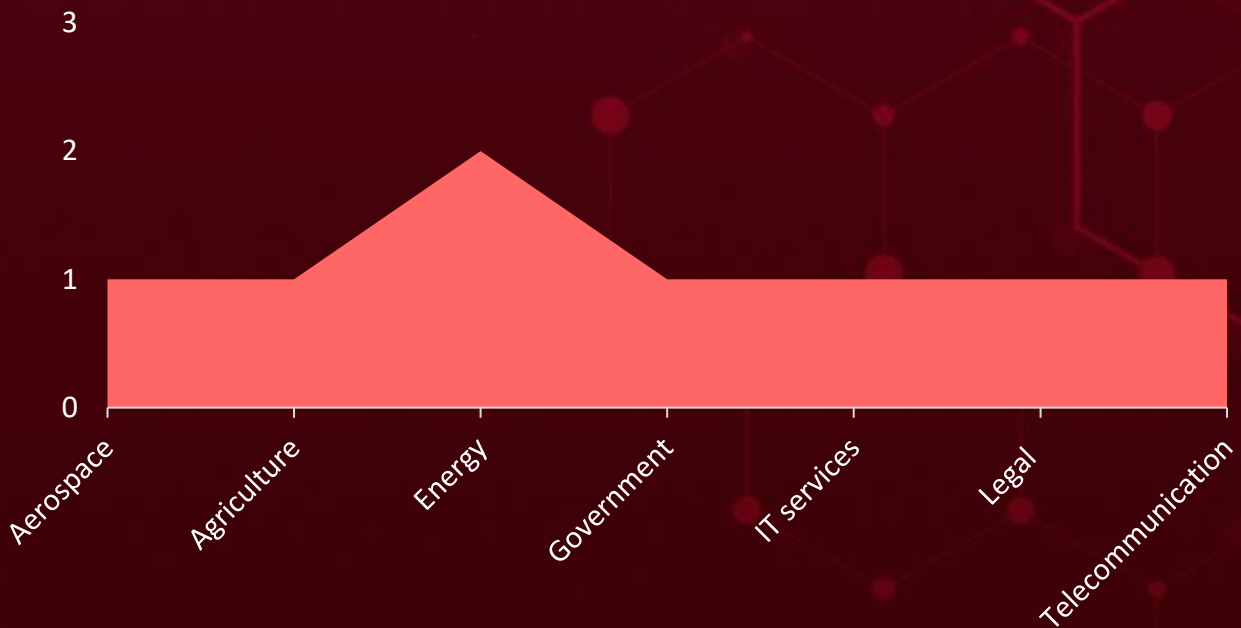


Powered by Bing

© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Countries	Countries	Countries	Countries
Japan	Solomon Islands	Cuba	Eswatini
Tonga	Kiribati	Uruguay	Norway
Palau	Sri Lanka	Cyprus	Ethiopia
Nepal	Vanuatu	Namibia	Panama
Australia	Timor-Leste	Czech Republic (Czechia)	Armenia
South Korea	Vietnam	Bosnia and Herzegovina	Bulgaria
Bangladesh	Tuvalu	Denmark	Finland
Marshall Islands	Malaysia	Paraguay	Romania
Bhutan	Maldives	Djibouti	France
North Korea	Laos	Rwanda	Saint Lucia
Brunei	Antigua and Barbuda	Dominica	Gabon
Afghanistan	Botswana	Serbia	Saudi Arabia
Cambodia	Montenegro	Dominican Republic	Gambia
Thailand	Colombia	South Africa	Sierra Leone
China	San Marino	DR Congo	Georgia
United States	Comoros	Suriname	Burundi
Fiji	Turkey	Ecuador	Albania
Mongolia	Congo	Togo	South Sudan
Germany	Bolivia	Egypt	Ghana
New Zealand	Costa Rica	Ukraine	State of Palestine
India	Portugal	El Salvador	Greece
Pakistan	Côte d'Ivoire	Monaco	Switzerland
Indonesia	Slovakia	Equatorial Guinea	Grenada
Papua New Guinea	Croatia	Mozambique	Cameroon
Philippines	Tajikistan	Eritrea	Guatemala
Singapore	Niger	Andorra	Trinidad and Tobago

Targeted Industries



TOP MITRE ATT&CK TTPs

T1588

Obtain Capabilities

T1059

Command and Scripting Interpreter

T1588.006

Vulnerabilities

T1566

Phishing

T1105

Ingress Tool Transfer

T1574

Hijack Execution Flow

T1041

Exfiltration Over C2 Channel

T1027

Obfuscated Files or Information

T1070

Indicator Removal

T1083

File and Directory Discovery

T1036

Masquerading

T1204

User Execution

T1204.002

Malicious File

T1190

Exploit Public-Facing Application

T1082

System Information Discovery

T1071.001

Web Protocols

T1055

Process Injection

T1068

Exploitation for Privilege Escalation

T1057

Process Discovery

T1566.001

Spearphishing Attachment

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Diamorphine</u>	Diamorphine is a Linux rootkit that allows attackers to hide processes, files, and network connections from system monitoring tools. It operates at the kernel level, making it difficult to detect and remove. Often used to maintain covert access, it grants attackers elevated privileges and can manipulate logs.	Exploit vulnerabilities	-
		IMPACT	AFFECTED PRODUCTS
		Stealthy access and System control	CentOS
			PATCH LINK
TYPE			
Rootkit			
ASSOCIATED ACTOR			
TeamTNT			-
IOC TYPE	VALUE		
SHA256	3be13d69a4c9b94179a6cf45a310acfaa7c5455cba908982fb36277486b5ea86, 3cd21bf96050d89d3bcf8f4d7612c8d60dcc2a9fc2b8764fc6f9c08aabf81c5a, 4a411cf9f0e30eb8c8fd23d38413d2455b0f6e81b0082e749b8ca64cb9ab1e4c, bf46bd921cb615fb7490b50b0ead98ff4ebdbd599eeb3736f568c64f19eab980, d99d7b090da1f1c14a0a554492ba99a506472eab66b057435261a246c2405be5		

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
<u>EAGLEDOOR</u>	EAGLEDOOR is a backdoor malware linked to Earth Baxia, used in their cyberespionage campaigns. It allows attackers to remotely execute commands on compromised systems, enabling them to control infected devices and steal sensitive data. EAGLEDOOR is deployed through spear-phishing attacks and exploits vulnerabilities, including in platforms like GeoServer.	Exploit vulnerabilities and Spear-phishing	CVE-2024-36401
		IMPACT	AFFECTED PRODUCTS
		Unauthorized access	GeoServer
			PATCH LINK
TYPE			
Backdoor			
ASSOCIATED ACTOR			
Earth Baxia			https://geoserver.org/download/
IOC TYPE	VALUE		
SHA256	b3b8efcaf6b9491c00049292cdff8f53772438fde968073e73d767d51218d189, cef0d2834613a3da4befa2f56ef91afc9ab82b1e6c510d2a619ed0c1364032b8, 061bcd5b34c7412c46a3acd100167336685a467d2cbcd1c67d183b90d0bf8de7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>PondRAT</u>	PondRAT is a lightweight Linux and macOS remote access trojan (RAT) discovered in a campaign using poisoned Python packages. It shares significant code similarities with POOLRAT, malware attributed to the North Korean threat actor Gleaming Pisces. PondRAT facilitates file uploads, downloads, command execution, and system control for attackers.	Python software packages	-
		IMPACT	AFFECTED PRODUCTS
		Unauthorized access	Linux and macOS
			PATCH LINK
TYPE			
Backdoor			
ASSOCIATED ACTOR			
Gleaming Pisces			--
IOC TYPE	VALUE		
SHA256	973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c, 0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7, 3c8dbfcb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e, bce1eb513aaac344b5b8f7a9ba9c9e36fc89926d327ee5cc095fb4a895a12f80, bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b		

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
<u>POOLRAT</u>	<p>POOLRAT, also known as SIMPLESEA, is a macOS backdoor attributed to the North Korean hacking group Gleaming Pisces, specifically used in sophisticated supply chain attacks. This malware enables attackers to gain remote access to infected systems, allowing for file manipulation, command execution, and data exfiltration. Recent analyses reveal that POOLRAT shares significant code similarities with newer malware variants like PondRAT.</p>	Python software packages	-
TYPE		<p>IMPACT</p> <p>Unauthorized access</p>	AFFECTED PRODUCTS
Backdoor			Linux and macOS
ASSOCIATED ACTOR			PATCH LINK
Gleaming Pisces			--
IOC TYPE	VALUE		
SHA256	b3b8efcaf6b9491c00049292cdf8f53772438fde968073e73d767d51218d189, cef0d2834613a3da4bfa2f56ef91afc9ab82b1e6c510d2a619ed0c1364032b8, 061bcd5b34c7412c46a3acd100167336685a467d2cbcd1c67d183b90d0bf8de7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>BURNBOOK</u>	<p>BURNBOOK is a malware loader designed to download and execute additional malicious payloads onto infected systems. It acts as an intermediary, facilitating the launch of more harmful malware like ransomware or spyware. BURNBOOK typically operates covertly, evading detection while delivering its secondary payloads to targets.</p>	Phishing	-
TYPE		<p>IMPACT</p> <p>Loads other malware and espionage</p>	AFFECTED PRODUCTS
Loader			-
ASSOCIATED ACTOR			PATCH LINK
Lazarus Group			-
IOC TYPE	VALUE		
MD5	57e8a7ef21e7586d008d4116d70062a6, f3baee9c48a2f744a16af30220de5066		
File name	libmupdf.dll		

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
<u>TEARPAGE</u>	TEARPAGE is a malicious loader used by North Korean Lazarus cyber espionage group. It operates through DLL search order hijacking, facilitating the execution of the MISTPEN backdoor by decrypting an encrypted payload from a file located in the user's AppData directory.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Loads other malware and espionage	-
Loader			PATCH LINK
ASSOCIATED ACTOR			-
Lazarus Group			
IOC TYPE	VALUE		
MD5	006cbff5d248ab4a1d756bce989830b9		
File Path	%APPDATA%\Roaming\Microsoft\BDE UI Launcher\wtsapi32.dll		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>MISTPEN</u>	MISTPEN is a lightweight backdoor written in C, primarily designed to download and execute Portable Executable (PE) files from command-and-control (C2) servers. MISTPEN employs sophisticated evasion techniques, including encrypted communications and stealthy operations, making it particularly dangerous for critical sectors like energy and aerospace.	Through BURNBOOK and TEARPAGE	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Unauthorized access	-
Backdoor			PATCH LINK
ASSOCIATED ACTOR			-
Lazarus Group			
IOC TYPE	VALUE		
MD5	0b77dcee18660bdccaf67550d2e00b00, b707f8e3be12694b4470255e2ee58c81, cd6dbf51da042c34c6e7ff7b1641837d, eca8eb8871c7d8f0c6b9c3ce581416ed		
File name	binhex.dll		

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	
<u>SnipBot</u>	SnipBot, a newly identified variant from the RomCom malware family, employs advanced infection and evasion techniques. Typically delivered via phishing emails posing as PDF attachments, it downloads additional malicious payloads from remote command-and-control servers. This malware showcases capabilities for remote command execution and data exfiltration while using anti-sandbox methods to evade detection.	Phishing	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
RAT				Windows
ASSOCIATED ACTOR				PATCH LINK
-				
ASSOCIATED ACTOR	Remote control			

IOC TYPE	VALUE
SHA256	0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e01677501, 1cb4ff70f69c988196052eaacf438b1d453bbfb08392e1db3df97c82ed35c154, 2c327087b063e89c376fd84d48af7b855e686936765876da2433485d496cb3a4, 5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aaeb688129, 57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781fd42312

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs	
<u>RomCom</u>	RomCom malware is a sophisticated cyber threat that emerged in 2022, used primarily for cyber espionage and ransomware campaigns. It typically involves phishing emails or malicious software disguised as legitimate programs to infiltrate systems. Once inside, it steals sensitive information and can manipulate network configurations to expand its reach.	Phishing	-	
TYPE		IMPACT	AFFECTED PRODUCTS	
RAT				Windows
ASSOCIATED ACTOR				PATCH LINK
-				
ASSOCIATED ACTOR	Remote control and data theft			

IOC TYPE	VALUE
SHA256	1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f

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
<u>KLogEXE</u> TYPE Keylogger ASSOCIATED ACTOR Sparkling Pisces	KLogEXE is a keylogger used by the Kimsuky group, designed to capture keystrokes and steal sensitive information like credentials. It operates stealthily, using anti-detection and anti-analysis techniques to evade cybersecurity defenses. This tool is a critical part of Sparkling Pisces's espionage campaigns, particularly against South Korean targets.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Data theft and Keystroke recording	-
			PATCH LINK
			-
IOC TYPE	VALUE		
SHA256	990b7eec4e0d9a22ec0b5c82df535cf1666d9021f2e417b49dc5110a67228e27, a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb22162895641dda0dc2, faf66019333f4515f241c1d3fcfc25c67532463245e358b90f9e498fe4f6801		




NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>FPSpy</u> TYPE Backdoor ASSOCIATED ACTOR Sparkling Pisces	FPSpy is a malware variant associated with the North Korean threat group Sparkling Pisces, primarily delivered through spear-phishing emails containing malicious ZIP file attachments. It functions as a backdoor, capable of gathering system information, executing arbitrary commands, and enumerating files on compromised machines.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Remote control and data theft	-
			PATCH LINK
			--
IOC TYPE	VALUE		
SHA256	c69cd6a9a09405ae5a60acba2f9770c722afde952bd5a227a72393501b4f5343, 2e768cee1c89ad5fc89be9df5061110d2a4953b336309014e0593eb65c75e715		




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	
<u>RIPCOY</u>	RIPCOY is a malware variant employed by the Earth Baxia threat group, typically distributed via spear-phishing emails with ZIP file attachments. RIPCOY employs the GrimResource technique to download malicious files from a public cloud service, typically AWS, after tricking users into executing an obfuscated VBScript within a decoy MSC or Ink file.	Phishing	CVE-2024-36401	
TYPE		IMPACT	AFFECTED PRODUCTS	
Trojan				GeoServer
ASSOCIATED ACTOR				PATCH LINK
Earth Baxia		https://geoserver.org/download/		
IOC TYPE	VALUE			
SHA256	916f3f4b895c8948b504cbf1beccb601ff7cc6e982d2ed375447bce6ecb41534, 4edc77c3586ccc255460f047bd337b2d09e2339e3b0b0c92d68cddedf2ac1e54, 6be4dd9af27712f5ef6dc7d684e5ea07fa675b8cbcd3094612a6696a40c664ce, 1e6c661d6981c0fa56c011c29536e57d21545fd11205eddf9218269ddf53d448, 4ad078a52abeced860ceb28ae99dda47424d362a90e1101d45c43e8e35dfd325			


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-2024-36401		GeoServer	Earth Baxia
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:a:geoserver:geoserver: *:~::~*:~::~*	EAGLEDOOR, RIPCOY
OSGeo GeoServer GeoTools Eval Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-95	T1059: Command and Scripting Interpreter T1190: Exploit Public-Facing Application	https://geoserver.org/download/ ; https://sourceforge.net/projects/geotools/files/


CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-7593		Ivanti Virtual Traffic Manager Versions: 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1, 22.7R1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:ivanti:vtm:*:*:*:*: *:*:*	-
Ivanti Virtual Traffic Manager Authentication Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287, CWE-303	T1068 : Exploitation for Privilege Escalation, T1190 : Exploit Public-Facing Application	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593

Adversaries in Action


NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 TeamTNT (aka Adept Libra)	Germany	Cryptocurrency, Financial	Worldwide
	MOTIVE		
	Information theft and Financial gain		
	TARGETED CVEs	ASSOCIATED ATTAC KS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	CentOS

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1110: Brute Force; T1057: Process Discovery; T1082: System Information Discovery; T1105: Ingress Tool Transfer; T1083: File and Directory Discovery; T1490: Inhibit System Recovery; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1222: File and Directory Permissions Modification; T1562: Impair Defenses; T1562.001: Disable or Modify Tools; T1562.003: Impair Command History Logging; T1562.004: Disable or Modify System Firewall; T1562.012: Disable or Modify Linux Audit System; T1070: Indicator Removal; T1070.006: Timestamp; T1014: Rootkit; T1609: Container: Administration Command; T1053: Scheduled Task/Job; T1053.003: Cron; T1583.003: Virtual Private Server; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Earth Baxia	China	Government, Telecommunication, and Energy	Asia–Pacific
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	CVE-2024-36401	EAGLEDOOR	GeoServer
TTPs			
TA0007: Discovery; TA0011: Command and Control; T1566.001: Spearphishing Attachment; T1574.002: DLL Side-Loading; TA0005: Defense Evasion; TA0010: Exfiltration; T1566: Phishing; TA0001: Initial Access; T1071.001: Web Protocols: TTPs; TA0002: Execution; T1071.004: DNS; T1574.014: AppDomainManager; T1574: Hijack Execution Flow; T1027.010: Command Obfuscation; T1105: Ingress Tool Transfer; T1027: Obfuscated Files or Information; T1082: System Information Discovery; T1620; T1190: Reflective Code Loading Exploit Public-Facing Application; T1001: Data Obfuscation; T1071: Application Layer Protocol; T1027.013: Encrypted/Encoded File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Gleaming Pisces (aka Citrine Sleet, Lazarus, Labyrinth Chollima, Group 77, Hastati Group, Who is Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</u></p>	North Korea	Energy, Aerospace	United States, United Kingdom, Netherlands, Cyprus, Sweden, Germany, Singapore, Hong Kong, Australia
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE
	-	PondRAT, POOLRAT, BURNBOOK, TEARPAGE, MISTPEN Backdoor	Linux and macOS
TTPs			
<p>TA0009: Collection; TA0011: Command and Control; : TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA; TA0010: Exfiltration; TA0001: Initial Access; T1070: Indicator Removal; TA0002: Execution; T1070.004: File Deletion; T1195: Supply Chain Compromise; T1036: Masquerading; T1222: File and Directory Permissions Modification; T1059.004: Unix Shell; T1027: Obfuscated Files or Information; T1059.006: Python; T1140: Deobfuscate/Decode Files or Information; T1059: Command and Scripting Interpreter; T1213:Data from Information Repositories; T1222.002: Linux and Mac File and Directory Permissions Modification; T1195.001: Compromise Software Dependencies and Development Tools; T1566: Phishing; T1566.001: Spearphishing Attachment; T1204: User Execution; T1204.002: Malicious File; T1547: Boot or Logon Autostart Execution; T1543: Create or Modify System Process; T1574: Hijack Execution Flow; T1574.001: DLL Search Order Hijacking; T1212: Exploitation for Credential Access; T1010: Application Window Discovery; T1083: File and Directory Discovery; T1057: Process Discovery; T1105: Ingress Tool Transfer; T1574.002: DLL Side-Loading; T1041: Exfiltration Over C2 Channel</p>			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Sparkling Pisces (aka Kimsuky, Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082, UAT-5394)</u></p>	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks	South Korea and Japan
	MOTIVE		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	KLogEXE and FPSpy	-	
TTPs			
TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; T1566: Phishing; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1070: Indicator Removal; T1070.006: Timestomp; T1041: Exfiltration Over C2 Channel; T1056: Input Capture; T1056.001: Keylogging; T1105: Ingress Tool Transfer; T1048: Exfiltration Over Alternative Protocol; T1082: System Information Discovery; T1083: File and Directory Discovery; T1074: Data Staged; T1057: Process Discovery; T1027: Obfuscated Files or Information			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **two exploited vulnerabilities** and block the indicators related to the threat actors **TeamTNT, Earth Baxia, Gleaming Pisces, Sparkling Pisces** and malware **Diamorphine, EAGLEDOOR, PondRAT, POOLRAT, BURNBOOK, TEARPAGE, MISTPEN, SnipBot, RomCom, KLogExe, FPSpy, RIPC0Y**.

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 **two exploited vulnerabilities**.

Testing the efficacy of their security controls by simulating the attacks related to the threat actor **TeamTNT, Earth Baxia, Gleaming Pisces, Sparkling Pisces** and malware **Diamorphine, PondRAT, POOLRAT, SnipBot, RomCom, KLogExe, FPSpy, RIPC0Y** in Breach and Attack Simulation(BAS).

Threat Advisories

[TeamTNT Reboots with New Weaponry: Rootkits and More](#)

[Earth Baxia: A New Threat to APAC Governments](#)

[Shield Your Site: WordPress Houzez Theme and Plugin Flaws Uncovered](#)

[PondRAT Malware Hidden in Python Packages Targets Developers](#)

[North Korean Hackers Weaponize Job Offers Featuring MISTPEN](#)

[Flaw in Apache Tomcat Poses DoS Risk, Threatening Service Availability](#)

[SnipBot: Unpacking the Latest RomCom Malware Variant](#)

[Critical Flaw in Microchip ASF Exposes Devices to Remote Code Execution](#)

[CVE-2024-45817: Deadlock Flaw in XenServer and Citrix Hypervisor](#)

[Sparkling Pisces's Latest Tools Unveiled: KLogEXE and FPSpy Enhance Espionage Efforts](#)

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
<u>Diamorphine</u>	SHA256	3be13d69a4c9b94179a6cf45a310acfaa7c5455cba908982fb36277486b5ea86, 3cd21bf96050d89d3bcf8f4d7612c8d60dcc2a9fc2b8764fc6f9c08aabf81c5a, 4a411cf9f0e30eb8c8fd23d38413d2455b0f6e81b0082e749b8ca64cb9ab1e4c, bf46bd921cb615fb7490b50b0ead98ff4ebdbd599eab3736f568c64f19eab980, d99d7b090da1f1c14a0a554492ba99a506472eab66b057435261a246c2405be5, d947b70347ce1f0088b107a3344c033cdd666782e7b382cd4bccb64724a28575, 4fdadd8b65ce5975745596f9afcd3532d89a80f01e29993ed3842318b56c58b0, 49117f048c668c3d4959796aa447d89899b0ede84dbfb486adb34c92d8cedd2f, 351d0bdab940e0195dd3c5e5da61ea4d46a0cce34a8ea9f78e27b1d233a2486f, 69e144206b607522da3b571823f93125d121065ba55c0ead651696a48e92bdcf, ddfdb25d6a30a6d63c705e25e818553fb21ee89f3b988aae7b65c10eec805a1b, b0c4456420e0d650912a99acc9fe4d4eeee9f75921facafc718c2c82ea0365b5, 9ba2a5fcc9ab9b229c7d7a139dd1768858738ed3f4ff0e07e23bc59a90418ea1, f79eb2930012ac45e4c4434f8559e0bc40fa269b51fcc297ca4b78c2b61bfc7, 0d0de2151d7fcd14b1bdb64dab802e2290a5a130ba7ed7db6a6e4d5b5b095463,

Attack Name	TYPE	VALUE
<u>Diamorphine</u>	SHA256	4114d57edae1d877d62d8b5642bd93cfb457b12cf657d53a185e37d0 9ae51891, 91d9421125adceb27e5e40f27a8da6cb5de8971b2e8d081a18020a6c 0b44e453, 1936270dc97c4e2e7bbdfd0c337ed1acdf72df6dc9598b396f6fdf4c0a d8f904, a158fc3982b8ccbec4655b9a3017eba167e0f0bb61f78f870898a51f7f 6076bb, 29913a342bca81ec1084c9abc1c6be8d431d0da40fadba465a3ca3481 193904b, a931bc92999eeefdcb79bf6dc294608cb825b2d8f2627b1b3ab0b71e7 4d8d835, 5bc5883c31f7e1432663d2f277d6cb2c849cfc1e095bca27bd5d17ff11 229fed, 8b7eaea5fc2f184ad9ef6abf069bdb78d42662c891b09c3c6a9d48995 26b17c8, 825b5ab1e44f6744e2fb686c07c145d3b9cbe30e25ba8f6a4b5bf8603 c7ecf3a, 678d3846429bff6c54e386f65331791e932dd5f2bafc5d0c4877a493cd 0ee355, c8e29d0d02610b5d9aa92a13013ea292fd3472cf62ba09f5c1b72ab73 619ddc4, afe0498385984eca996d17b37851fdf9213910426f4841da29c6d9c33 e98e013, 08ffdaafb82fefde776f7e0f9d5824f15cea7ff8043fb7a200e8f4e60a05 e82a, e029e90d6767f2b84e9e2d618db105573404d4f09eece52734b9faae 5fc25c2c, be40eee5b8b3b3dfa0c453b191ed0fccac9532a41f062c6fce56db11d 366250, 5d3373476bcded34f0e2436587254fcc8edab9a771b9a040cbf59c57a b30b4da, b061611f11c620be049ee85651e2950f51e299e91f7488045c5e3b98 5c769898, 44233d8b9de16b9fa0fc1f048300927671a60f03394ad41b0fb7e91a8 03e4a5c, 5d637915abc98b21f94b0648c552899af67321ab06fb34e33339ae384 01734cf, 370fff5098eda6b9ec9ae942c1ce32098e07d7e91d4a5c6e978d8bb22 747e6df, 12d6326bd7e7bc8e81e0e161b5537096847253076334bca8c16a3c3f 4c2c0e5b, 76c01ef5aaef29e2894beddd8f23726b75f6a8d335499333b60a0e381 5de5b2e, 1a9382e491598fea6f418427f36a0e127135ed4886adc846b3339e05 05284971, be8e8ef049dedc7c56e7d61f4f50a0ed324a42e1b1febe66aea77156b c6f02a0, 400f3a425ed047442d87ab96e7469f63c6dbc78424771eb2e4b9c305 ea44d0b6,

Attack Name	TYPE	VALUE
<u>Diamorphine</u>	SHA256	d00771a4fd8f314417441d76812466c0a84ab053a8e5960037526d0ff4cba37d, b627725d7f4ee5b969c200c65d61123027df30a8f2b5930c7df5bfbe8a613f6b, 6d388ee0ee34d5ec409c55cee65b8d65aacbf7f3bf207db47e3fef0d7860877, 954a5905607d1bd1160b6471a36679af9aa57a5fbf777751f68492ecc54d45e1, c2b0588ff7a6d5790cbd5587fc307e6b36a618ccc90c47264b4e1bcc0a549931, 6436303b20b2836d08595a90cfd82806c6dce16f33964aa4749a86b343d0abbb, 8bf0ddff6d2921257fbd3a3791c72fc1ebc7347a84ab4bf0298085d91e5ef0d5, 12360ddc28cfa104377d7c7a92a190933c424c3dd407b65f7b69b1b5c67dca1b, 1fdda23de5a1dbfb70698f2b548c80c1d2967cb0f8d9bba41d64131aa a7532a3
<u>RIPCOY</u>	SHA256	916f3f4b895c8948b504cbf1becb601ff7cc6e982d2ed375447bce6ecb41534, 4edc77c3586ccc255460f047bd337b2d09e2339e3b0b0c92d68cddedf2ac1e54, 6be4dd9af27712f5ef6dc7d684e5ea07fa675b8cbcd3094612a6696a40c664ce, 1e6c661d6981c0fa56c011c29536e57d21545fd11205eddf9218269ddf53d448, 4ad078a52abeced860ceb28ae99dda47424d362a90e1101d45c43e8e35dfd325, 04b336c3bcfe027436f36dfc73a173c37c66288c7160651b11561b39ce2cd25e
<u>EAGLEDOOR</u>	SHA256	b3b8efcaf6b9491c00049292cdff8f53772438fde968073e73d767d51218d189, cef0d2834613a3da4befa2f56ef91afc9ab82b1e6c510d2a619ed0c1364032b8, 061bcd5b34c7412c46a3acd100167336685a467d2cbcd1c67d183b90d0bf8de7
	Domain	msa.hinet[.]ink
	IPv4	167[.]172[.]89[.]142, 167[.]172[.]84[.]142
<u>PondRAT</u>	SHA256	973f7939ea03fd2c9663dafc21bb968f56ed1b9a56b0284acf73c3ee141c053c, 0b5db31e47b0dccfdec46e74c0e70c6a1684768dbacc9eacbb4fd2ef851994c7, 3c8dbfcb4fccbaf924f9a650a04cb4715f4a58d51ef49cc75bfcef0ac258a3e, bce1eb513aaac344b5b8f7a9ba9c9e36fc89926d327ee5cc095fb4a895a12f80, bfd74b4a1b413fa785a49ca4a9c0594441a3e01983fc7f86125376fdbd4acf6b, cbf4cfa2d3c3fb04fe349161e051a8cf9b6a29f8af0c3d93db953e5b5dc39c86,

Attack Name	TYPE	VALUE
<u>PondRAT</u>	Domains	jdkgradle[.]com, rebelthumb[.]net
<u>POOLRAT</u>	SHA256	f3b0da965a4050ab00fce727bb31e0f889a9c05d68d777a8068cfc15a71d3703, 5c907b722c53a5be256dc5f96b755bc9e0b032cc30973a52d984d4174bace456,
	Domains	www[.]talesseries[.]com/write[.]php, rgedist[.]com/sfxl[.]php,
<u>BURNBOOK</u>	MD5	57e8a7ef21e7586d008d4116d70062a6, f3baee9c48a2f744a16af30220de5066
	Domain	libmupdf.dll
<u>TEARPAGE</u>	MD5	006cbff5d248ab4a1d756bce989830b9
	File Path	%APPDATA%\Roaming\Microsoft\BDE UI Launcher\wtsapi32.dll
<u>MISTPEN</u>	MD5	0b77dcee18660bdccaf67550d2e00b00, b707f8e3be12694b4470255e2ee58c81, cd6dbf51da042c34c6e7ff7b1641837d, eca8eb8871c7d8f0c6b9c3ce581416ed
	Domain	binhex.dll
	File Path	%APPDATA%\Roaming\Thumbs.ini
<u>SnipBot</u>	SHA256	0be3116a3edc063283f3693591c388eec67801cdd140a90c4270679e01677501, 1cb4ff70f69c988196052eaacf438b1d453bbfb08392e1db3df97c82ed35c154, 2c327087b063e89c376fd84d48af7b855e686936765876da2433485d496cb3a4, 5390ba094cf556f9d7bbb00f90c9ca9e04044847c3293d6e468cb0aaeb688129, 57e59b156a3ff2a3333075baef684f49c63069d296b3b036ced9ed781fd42312
<u>RomCom</u>	SHA256	1a7bb878c826fe0ca9a0677ed072ee9a57a228a09ee02b3c5bd00f54f354930f, 419bc8196013d7d8c72b060da1a02d202d7e3eb441101f7bcb6d7667871a5c16, 5c2fb1c42f007093be5e463f70ee7e7192990b3385a3cbcc71043980efa312e0, 6a0017262def9565b504d04318c59f55bea136ac3dd48862d1ae90ff6b963811, b557bf11d82d3d64d028a87584657d25dba0480295ed08447f10c7a579dee048, b3984a2de76eee3ad20c4b13e0c0cbbab2dd6db65e3f6ca34418e79c21cf5c39
<u>KLogExe</u>	SHA256	990b7eec4e0d9a22ec0b5c82df535cf1666d9021f2e417b49dc5110a67228e27 a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb22162895641dda0dc2 faf666019333f4515f241c1d3fcfc25c67532463245e358b90f9e498fe4f6801

Attack Name	TYPE	VALUE
<u>FPSpy</u>	SHA256	c69cd6a9a09405ae5a60acba2f9770c722afde952bd5a227a72393501b4f5343 2e768cee1c89ad5fc89be9df5061110d2a4953b336309014e0593eb65c75e715

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

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

September 30, 2024 • 11:30 PM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com