

Date of Publication
November 27, 2023



HiveForce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

20 to 26 NOVEMBER 2023

Table Of Contents

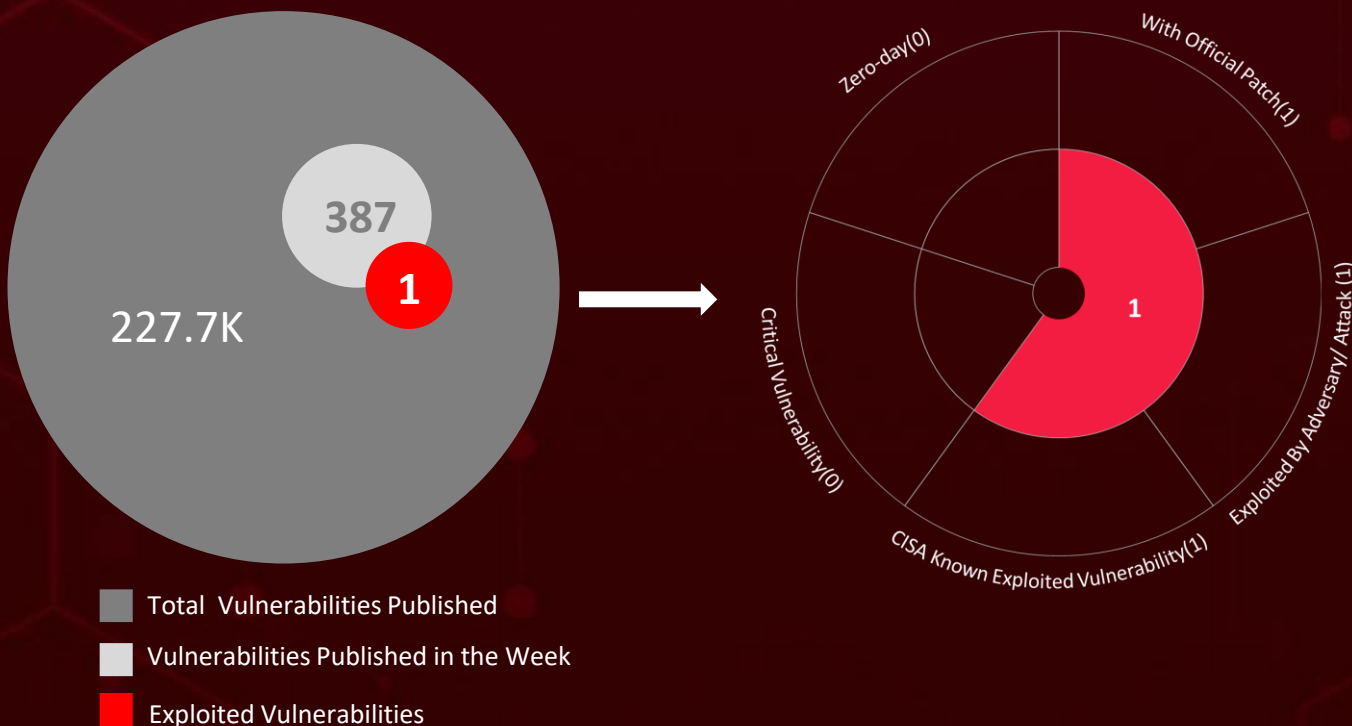
<u>Summary</u>	03
<u>High Level Statistics</u>	04
<u>Insights</u>	05
<u>Targeted Countries</u>	06
<u>Targeted Industries</u>	07
<u>Top MITRE ATT&CK TTPs</u>	07
<u>Attacks Executed</u>	08
<u>Vulnerabilities Exploited</u>	12
<u>Adversaries in Action</u>	13
<u>Recommendations</u>	17
<u>Threat Advisories</u>	18
<u>Appendix</u>	19
<u>What Next?</u>	22

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, **six** instances of adversary activity, and **one** exploited vulnerability, highlighting the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs uncovered a malware framework named **LambLoad**, utilized by the **Lazarus Group** threat group in their latest campaign, mainly targeting the Middle East region.

Meanwhile, a critical vulnerability (**CVE-2023-46604**) in Apache ActiveMQ is being exploited by the **Kinsing** in various attacks. These observed attacks have been on the rise, posing a significant threat worldwide.



High Level Statistics

8

Attacks
Executed

1

Vulnerabilities
Exploited

6

Adversaries in
Action

- [LitterDrifter](#)
 - [Kinsing](#)
 - [NetSupport](#)
 - [Nim backdoor](#)
 - [DarkGate](#)
 - [Atomic Stealer](#)
 - [LambLoad](#)
 - [InfectedSlurs](#)
- [CVE-2023-46604](#)
- [Lazarus Group](#)
 - [Gamaredon](#)
 - [SideWinder](#)
 - [Mustang Panda](#)
 - [RastaFarEye](#)
 - [TA569](#)



Insights

Mustang Panda

Targets Philippines Government Using Legitimate Software

Lazarus Group

Exploiting software vulnerabilities and introducing the Kinsing malware to gain control over their victims in latest campaign

Kinsing

Malware exploiting a critical vulnerability (CVE-2023-46604) in Apache ActiveMQ

SideWinder APT

Group recently shifted its focus to targeting Bhutan, Nepal, and Myanmar government sector

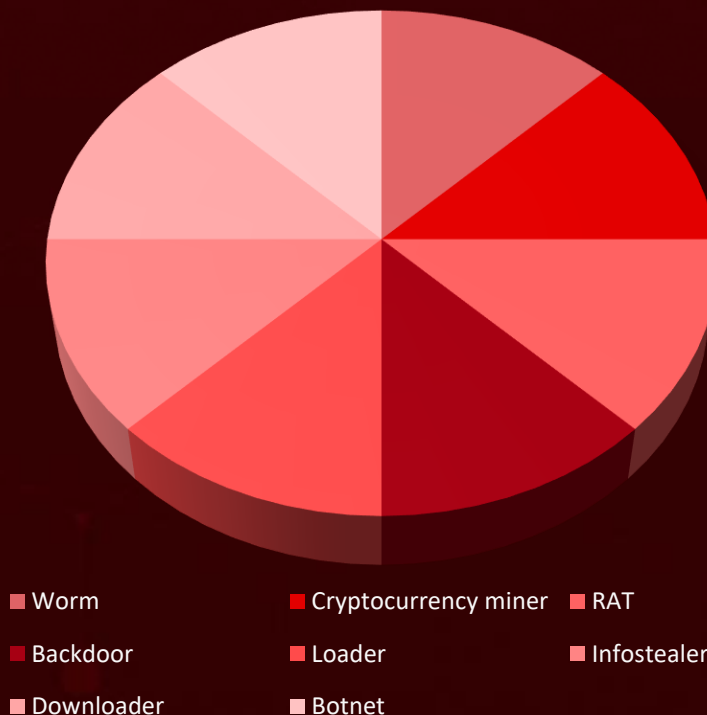
Gamaredon

Group utilizing a USB-propagating worm known as **LitterDrifter** in attacks targeting Ukrainian entities

NetSupport RAT

leading to a recent surge in infections across Education, Government, and Business Services

Threat Distribution



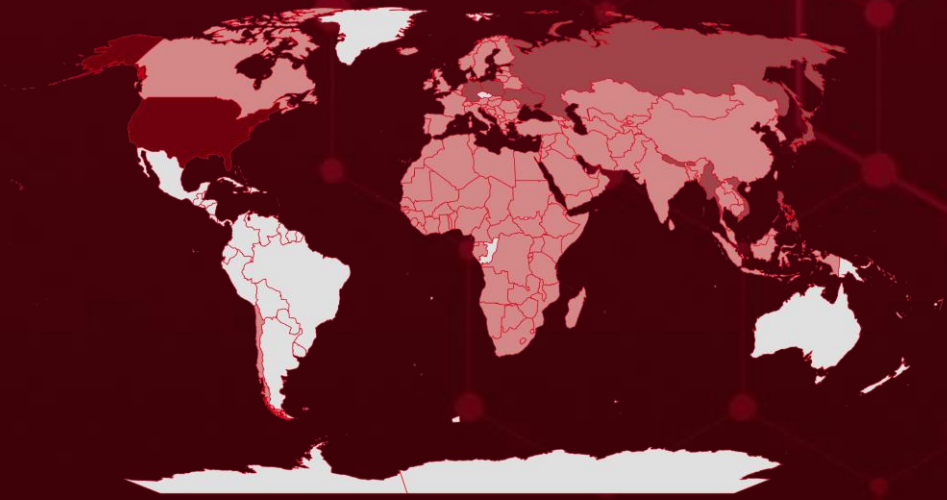


Targeted Countries

Most



Least



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

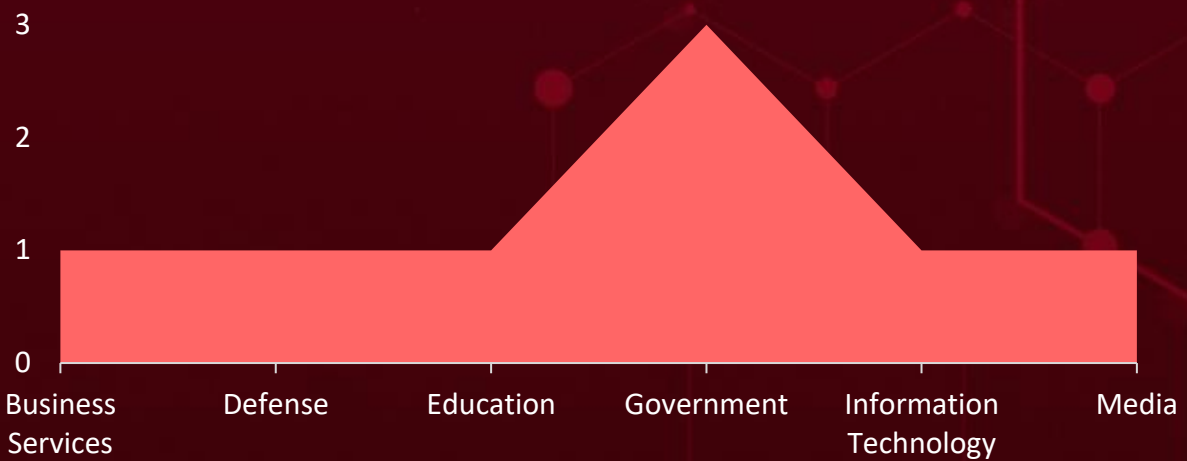
Countries
United States
Russia
Philippines
Nepal
Germany
Poland
Japan
Bhutan
Ukraine
Myanmar
Vietnam
Togo
Portugal
Montenegro
Benin
Niger
Albania
Maldives
Bosnia and Herzegovina
Nigeria
Botswana

Countries
Senegal
Brunei
Sweden
Bulgaria
Belarus
Burkina Faso
Mauritius
Burundi
Namibia
Cabo Verde
Oman
Cambodia
Rwanda
Cameroon
Singapore
Canada
Spain
Central African Republic
Tajikistan
Chad
Morocco
Greece

Countries
Uganda
Chile
Malawi
China
Malta
Comoros
Monaco
Congo
Mozambique
Côte d'Ivoire
Netherlands
Croatia
North Macedonia
Cyprus
Austria
Czech Republic (Czechia)
Romania
Denmark
Sao Tome & Principe
Djibouti
Seychelles
DR Congo

Countries
Slovenia
Egypt
South Korea
Equatorial Guinea
State of Palestine
Eritrea
Syria
Estonia
Thailand
Eswatini
Turkey
Ethiopia
United Arab Emirates
Finland
Madagascar
France
Malaysia
Gabon
Mali
Gambia
Mauritania
Georgia
Moldova

Targeted Industries



TOP MITRE ATT&CK TTPS

T1059

Command and Scripting Interpreter

T1041

Exfiltration Over C2 Channel

T1105

Ingress Tool Transfer

T1543

Create or Modify System Process

T1204.002

Malicious File

T1053

Scheduled Task/Job

T1204

User Execution

T1083

File and Directory Discovery

T1056

Input Capture

T1574

Hijack Execution Flow

T1082

System Information Discovery

T1071

Application Layer Protocol

T1059.001

PowerShell

T1027

Obfuscated Files or Information

T1190

Exploit Public-Facing Application

T1036

Masquerading

T1140

Deobfuscate/Decode Files or Information

T1071.001

Web Protocols

T1547.001

Registry Run Keys / Startup Folder

T1005

Data from Local System

🔪 Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>LitterDrifter</u>	LitterDrifter is a self-propagating worm written in VBScript that spreads through removable USB drives. It is believed to be developed by the Gamaredon APT group, which is linked to the Russian government.	USB drives	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal data, Disrupt operations	-
Worm			
ASSOCIATED ACTOR			PATCH LINK
Gamaredon			-
IOC TYPE	VALUE		
-	-		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Kinsing (aka h2miner)</u>	Kinsing malware is a type of Linux malware that has been around for several years. It is known for targeting containerized environments, such as Docker and Kubernetes, and for its ability to spread to other hosts. Kinsing is typically used to mine cryptocurrency, but it can also be used to steal data or launch other attacks.	Exploiting vulnerability	CVE-2023-46604
		IMPACT	AFFECTED PRODUCTS
TYPE		Performance degradation, Data breach, Denial-of-service attacks	ActiveMQ
Cryptocurrency miner			
ASSOCIATED ACTOR			PATCH LINK
-			https://activemq.apache.org/security-advisories.data/CVE-2023-46604
IOC TYPE	VALUE		
SHA256	7f9f8209dc619d686b32d408fed0beb3a802aa600ddceb5c8d2a9555cdb3b5e0, 8c9b621ba8911350253efc15ab3c761b06f70f503096279f2a173c006a393ee1, 511de8dd7f3cb4c5d88cd5a62150e6826cb2f825fa60607a201a8542524442e2, 4b0138c12e3209d8f9250c591fcc825ee6bff5f57f87ed9c661df6d14500e993, 999e4ebacda24b9431863e4cb1fd3e2d8e568ebb118b4a8e215a28dac8d8da32		

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>NetSupport</u>	NetSupport RAT is a that is based on a legitimate remote administration tool called NetSupport Manager. NetSupport Manager is a legitimate tool that is used by IT professionals to remotely control and manage computers. However, cybercriminals have been known to use modified versions of NetSupport Manager as RATs to gain unauthorized access to computers and steal data.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Data theft, Installing malware	-
			PATCH LINK
			-
TYPE	RAT		
ASSOCIATED ACTOR	TA569		
IOC TYPE	VALUE		
SHA256	213af995d4142854b81af3cf73dee7ffe9d8ad6e84fda6386029101dbf3df897, 28208baa507b260c2df6637427de82ad0423c20e2bceceb92ba5d76074dcd347, 2d6c6200508c0797e6542b195c999f3485c4ef76551aa3c65016587788ba1703, 2e4bd5557aedd1743da5fab1b6995fbc447d6e9491d9ec59fa93ab889d8bccd1, 38684adb2183bf320eb308a96cdbde8d1d56740166c3e2596161f42a40fa32d5		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Nim backdoor</u>	Nim backdoor is actually a variant of the C++ backdoor and is written in the Nim programming language . A backdoor is a hidden way to access a system or application that is not intended for public use.	Phishing	-
		IMPACT	AFFECTED PRODUCTS
		Data theft, Spying on victims	-
			PATCH LINK
			-
TYPE	Backdoor		
ASSOCIATED ACTOR	SideWinder		
IOC TYPE	VALUE		
SHA256	7bea8ea83d5b4fe5985172dbb4fa1468, 04e9ce276b3cd75fc2b20b9b33080f7e, 92612dc223e8f0656512cd882d66f78b, c2184d8fd3dd3df9fd6cf7ff8e32a3a4, b2ab01d392d7d20a9261870e709b18d7		

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>DarkGate</u>	DarkGate is a commodity malware that is used in a variety of cyber attacks, including targeted attacks and mass attacks. DarkGate is a versatile malware that can be used to steal data, install additional malware, launch denial-of-service attacks, and take control of infected systems.	Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Loader		Launch DDoS attacks And Data Theft	-
ASSOCIATED ACTOR			PATCH LINK
RastaFarEye			-
IOC TYPE	VALUE		
SHA256	00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df, 0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2, 10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896, 2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4, 6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>Atomic Stealer</u>	Atomic, or AMOS, macOS information-stealing malware. It is currently being delivered to targets through a deceptive web browser update chain known as ClearFake. ClearFake is a recent malware campaign that exploits compromised websites to distribute fake browser updates.	Legitimate AnyDesk remote desktop software	-
TYPE		IMPACT	AFFECTED PRODUCTS
Infostealer		Data theft	Mac OS
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	4cb531bd83a1ebf4061c98f799cdc2922059aff1a49939d427054a556e89f464, be634e786d5d01b91f46efd63e8d71f79b423bfb2d23459e5060a9532b4dcc7b, 5b5ffb0d2fb1f2de5147ec270d60a3ac3f02c36153c943fbfe2a3427ce39d13d		
Domains	wifi-ber[.]com		




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>LambLoad</u>	LambLoad is a malware family that has been active since at least 2017. It is a downloader that is used in supply chain attacks. Supply chain attacks are attacks that target third-party suppliers to gain access to their customers' systems.	Supply chain attacks, Phishing	-
TYPE		IMPACT	AFFECTED PRODUCTS
Downloader			-
ASSOCIATED ACTOR		Launch DDoS attacks And Data Theft	PATCH LINK
Lazarus Group			-
IOC TYPE	VALUE		
SHA256	166d1a6ddcde4e859a89c2c825cd3c8c953a86bfa92b343de7e5bfbfb5afb8be		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
<u>InfectedSlurs</u>	InfectedSlurs is a new Mirai-based malware botnet, and is actively conducting a sophisticated campaign by exploiting two zero-day remote code execution (RCE) vulnerabilities in routers and video recorder (NVR) devices. These vulnerabilities, currently being exploited in the wild, facilitate the creation of a distributed denial-of-service (DDoS) botnet.	Exploiting vulnerabilities	-
TYPE		IMPACT	AFFECTED PRODUCTS
Botnet			-
ASSOCIATED ACTOR		Launch DDoS attacks And Data Theft	PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8, 3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8, 75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380, f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc, 8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099		


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-2023-46604		Apache ActiveMQ 5.18.0 before 5.18.3, Apache ActiveMQ 5.17.0 before 5.17.6, Apache ActiveMQ 5.16.0 before 5.16.7, Apache ActiveMQ before 5.15.16, Apache ActiveMQ Legacy OpenWire Module 5.18.0 before 5.18.3, Apache ActiveMQ Legacy OpenWire Module 5.17.0 before 5.17.6, Apache ActiveMQ Legacy OpenWire Module 5.16.0 before 5.16.7, Apache ActiveMQ Legacy OpenWire Module 5.8.0 before 5.15.16	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:activemq:*:*:*:*:*:* :* cpe:2.3:a:apache:activemq_legacy_openwire_module:*:*:*:*:*:*	Kinsing, HelloKitty ransomware
Apache ActiveMQ Deserialization of Untrusted Data Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-502	T1059: Command and Scripting Interpreter	https://activemq.apache.org/security-advisories.data/CVE-2023-46604




Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Lazarus Group (aka Labyrinth Chollima, Guardians Of Peace, Zinc, Nickel Academy, Group 77, Hastati Group, Whois Hacking Team, Newromanic Cyber Army Team, Hidden Cobra, Appleworm, APT-C-26, Atk 3, Sectora01, ITG03, TA404, DEV-0139, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Jade Sleet, TraderTraitor)</u></p>	North Korea	Media, Defense, Information Technology	Japan, Taiwan, Canada, and the United States
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	ASSOCIATED ATTACKS/RA NSOMWARE	AFFECTED PRODUCTS
	CVE-2023-42793	LambLoad, Volgmer, Scout, ForestTiger, FeedLoad, RollSling, and HazyLoad	TeamCity
TTPs			
TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0011: Command and Control, TA0010: Exfiltration, TA0040: Impact, T1071.001: Web Protocols;T1059: Command and Scripting Interpreter;T1573.001: Symmetric Cryptography;T1098: Account Manipulation;T1566: Phishing; T1204: User Execution;T1047: Windows Management Instrumentation;T1543: Create or Modify System Process;T1574.002: DLL Side-Loading;T1070: Indicator Removal;T1573: Encrypted Channel;T1105: Ingress Tool Transfer; T1003: OS Credential Dumping; T1195.002: Compromise Software Supply Chain; T1195: Supply Chain Compromise; T1036: Masquerading			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>Gamaredon (aka Primitive Bear, Winterflounder, BlueAlpha, Blue Otso, Iron Tilden, Armageddon, SectorC08, Callisto, Shuckworm, Actinium, Trident Ursa, DEV-0157, UAC-0010, Aqua Blizzard)</u>	Russia	Defense, Government, Law enforcement, NGOs and diplomats and journalists	Ukraine, USA, Vietnam, Chile, Poland, Germany, Hong Kong
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	LitterDrifter	-	

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0011: Command and Control; T1140: Deobfuscate/Decode: Files or Information; T1027: Obfuscated Files or: Information; T1102: Web Service; T1008: Fallback Channels; T1053: Scheduled Task/Job; T1047: Windows Management: Instrumentation; T1071: Application Layer: Protocol; T1091: Replication Through: Removable Media

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>SideWinder (aka Razor Tiger, Rattlesnake, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)</u>	India	Government	Bhutan, Nepal, and Myanmar
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
-	Nim backdoor	-	


TTPs

TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; T1598: Phishing for: Information; T1566.001: Spearphishing: Attachment; T1059: Command and: Scripting Interpreter; T1083: File and Directory: Discovery; T1057: Process Discovery; T1056: Input Capture; T1053: Scheduled Task/Job; T1204: User Execution; T1547: Boot or Logon: Autostart Execution; T1543: Create or Modify: System Process; T1211: Exploitation for: Defense Evasion; T1132: Data Encoding; T1041: Exfiltration Over C2: Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>Mustang Panda (aka Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, Stately Taurus)</u></p>	China	Government	Philippines
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	-	-


TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0011: Command and: Control; T1566: Phishing; T1204: User Execution; T1204.002: Malicious File; T1574: Hijack Execution Flow; T1574.002: DLL Side-Loading; T1036: Masquerading; T1547: Boot or Logon: Autostart Execution; T1547.001: Registry Run Keys / Startup Folder

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <p><u>TA569</u></p>	Unknown	Education, Government, and Business Services	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	NetSupport RAT	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0011: Command and: Control; TA0010: Exfiltration; T1204.002: User Execution: Malicious File; T1059.001: Command and Scripting Interpreter: PowerShell; T1055: Process Injection; T1027: Obfuscated Files or Information; T1041: Exfiltration Over C2 Channel; T1074.001: Data Staged: Local Data Staging; T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder; T1057: Process Discovery

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 <u>RastaFarEye</u>	Unknown	-	United States, Europe, Regions in Asia, South America, and Africa
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	ASSOCIATED ATTACKS/RANSOMWARE	AFFECTED PRODUCTS
	-	DarkGate	-

TTPs

TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1566.001: Spearphishing Attachment; T1566.002: Spearphishing Link; T1204.002: Malicious File; T1059.001: PowerShell; T1059.003: Windows Command: Shell; T1547.001: Registry Run Keys / Startup Folder; T1055.012: Process Hollowing; T1543.003: Windows Service; T1027.002: Software Packing; T1027.007: Dynamic API: Resolution; T1027.009: Embedded Payloads; T1055.002: Portable Executable: Injection; T1574.002: DLL Side-Loading; T1622: Debugger Evasion; T1036.008: Masquerade File Type; T1555.003: Credentials from Web: Browsers; T1056.001: Keylogging; T1528: Steal Application: Access Token; T1010: Application Window: Discovery; T1217: Browser Bookmark: Discovery; T1083: File and Directory: Discovery; T1497.001: System Checks; T1614.001: System Language: Discovery; T1518.001: Security Software: Discovery; T1005: Data from Local: System; T1113: Screen Capture; T1115: Clipboard Data; T1071.001: Web Protocols; T1132.002: Non-Standard: Encoding; T1573.001: Symmetric: Cryptography; T1219: Remote Access: Software; T1041: Exfiltration Over C2: Channel; T1489: Service Stop

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **one exploited vulnerability** and block the indicators related to the threat actor **Gamaredon, SideWinder, Mustang Panda , RastaFarEye, TA569** and malware **LitterDrifter, Kinsing, NetSupport, Nim backdoor, DarkGate, Atomic Stealer, LambLoad, InfectedSlurs**.

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 **one exploited vulnerability**.
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Gamaredon, SideWinder, Mustang Panda , RastaFarEye, TA569** and malware **LitterDrifter, Kinsing, NetSupport, Nim backdoor, DarkGate, Atomic Stealer, LambLoad, InfectedSlurs** in Breach and Attack Simulation(BAS).



Threat Advisories

[Gamaredon Deploys LitterDrifter USB Worm in Cyber Espionage Operations](#)

[Kinsing Malware Utilizes Apache ActiveMQ RCE to Deploy Rootkits](#)

[The Rise of NetSupport RAT Recent Infections and Sector Impact](#)

[SideWinder's Nim Backdoor Spells Trouble for South Asian Nations](#)

[Mustang Panda Targets Philippines Government Using Legitimate Software](#)

[The Lethal Advancement of DarkGate Malware-as-a-Service](#)

[Atomic Stealer Sneaks In via Fake Browser Updates](#)

[Dissemination of the Konni Campaign Through Malicious Documents](#)

[Lazarus Group Orchestrates Supply Chain Attack on CyberLink Corp](#)

[Mirai Botnet's Offspring InfectedSlurs Exploits Dual Zero-Days](#)

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and been branded with catchy names and logos due to their impact on high-profile individuals and celebrities are also referred to as Celebrity Publicized Software Flaws.

✂ Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
<u>Kinsing</u>	SHA256	7f9f8209dc619d686b32d408fed0beb3a802aa600ddceb5c8d2a9555cdb3b5e0, 8c9b621ba8911350253efc15ab3c761b06f70f503096279f2a173c006a393ee1, 511de8dd7f3cb4c5d88cd5a62150e6826cb2f825fa60607a201a8542524442e2, 4b0138c12e3209d8f9250c591fcc825ee6bff5f57f87ed9c661df6d14500e993, 999e4ebacda24b9431863e4cb1fd3e2d8e568ebb118b4a8e215a28dac8d8da32, 1015a16078b826a0a52bf746016fedf2c758dca4a2033a48a9da20ee0b439eca
<u>Nim backdoor</u>	MD5	7bea8ea83d5b4fe5985172dbb4fa1468, 04e9ce276b3cd75fc2b20b9b33080f7e, 92612dc223e8f0656512cd882d66f78b, c2184d8fd3dd3df9fd6cf7ff8e32a3a4, b2ab01d392d7d20a9261870e709b18d7, 30ddd9ebe00f34f131efcd8124462fe3
<u>DarkGate</u>	SHA256	ad36b909721d64a3c32678f4c2ca758d81661088ba1ed57bec50ef0ac4d4a871, 00985db874d9177de4a18999f7a420260b3a4665ba2b5b32aa39433ef79819df, 0f1545a7176c45b0e7f9198cac8972167e5846e8b84cd40926f7edf338eeace2,

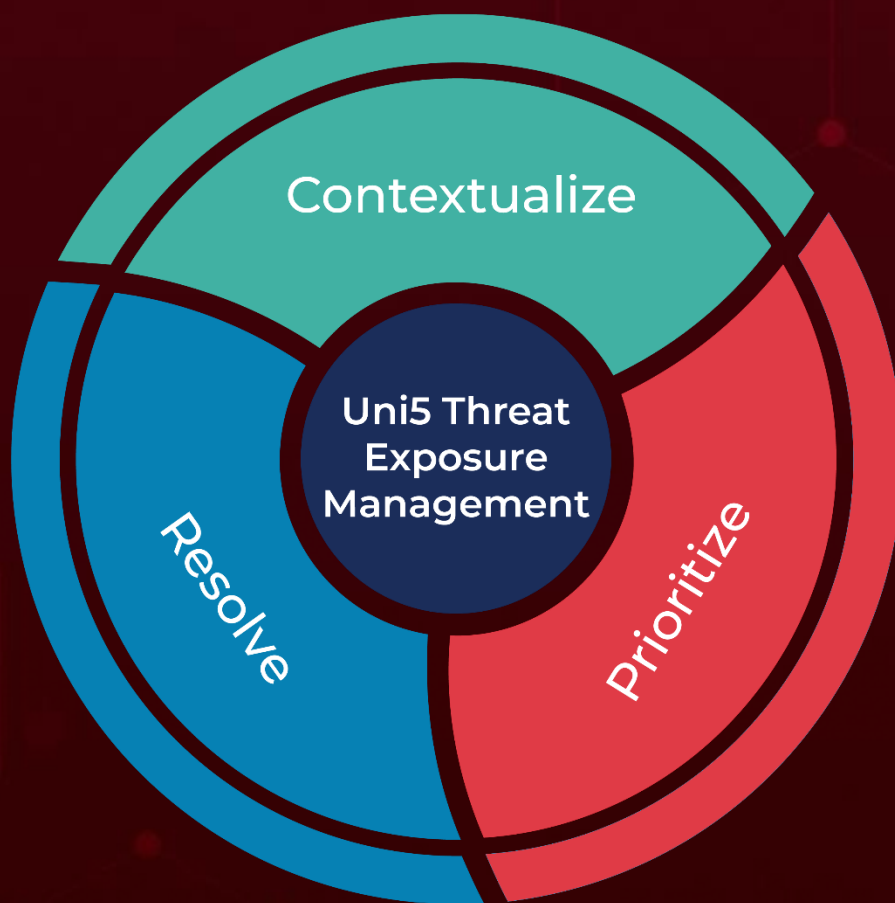
Attack Name	TYPE	VALUE
<u>DarkGate</u>	SHA256	10bfaeb0c00425c4749140d5c7d9f3d88537cf2f621ba7af5322b15cf205b896, 2b24c4c883a562d0326846ee1c92840144d1d755cdb721b24a35038ea92aa0e4, 6750f31ef5e1fe74c1121b0ab1308f93e09505a63322b6ce16fe04099ce8993e, 73c0d0f220a30b541e0855e8039b8050d1332ff03c3e0c8a35671bd5eb9d30be, 74729d4569691daf72e23849e91461471411f551639663e11e1091a48790611e, 74f21cf5ab72aad0f7f3cf3274a167c20e787f9513019510561f39d4230f3c4b, bc5ad215876055a8a6a097579e16d24e233a323a6157afbb6db49705ac12a1f1, bec37877e3bffa222efb5c5680c7defd2d917317293d7fa70e0882ad45290a40, e7b76e11101e35c46a7199851f82c69e819a3d856f6f68fa3af0636c3efde0ca
<u>Atomic Stealer</u>	SHA256	4cb531bd83a1ebf4061c98f799cdc2922059aff1a49939d427054a556e89f464, be634e786d5d01b91f46efd63e8d71f79b423bfb2d23459e5060a9532b4dcc7b, 5b5ffb0d2fb1f2de5147ec270d60a3ac3f02c36153c943fbfe2a3427ce39d13d
	IPv4	194.169.175[.]117
<u>LambLoad</u>	SHA256	166d1a6ddcde4e859a89c2c825cd3c8c953a86bfa92b343de7e5bfbfb5afb8be
<u>InfectedSlurs</u>	SHA256	dabdd4b5a3a70c64c031126fad36a4c45feb69a45e1028d79da6b443291addb8, 3f3c2e779f8e3d7f2cc81536ef72d96dd1c7b7691b6e613f5f76c3d02909edd8, 75ef686859010d6164bcd6a4d6cf8a590754ccc3ea45c47ace420b02649ec380,

Attack Name	TYPE	VALUE
<u>InfectedSIRS</u>	SHA256	f8abf9fb17f59cbd7381aa9f5f2e1952628897cee368defd6baa6885d74f3ecc, 8777f9af3564b109b43cbcf1fd1a24180f5cf424965050594ce73d754a4e1099, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1, a4975366f0c5b5b52fb371ff2cb034006955b3e3ae064e5700cc5365f27a1d26, cd93264637cd3bf19b706afc19944dfb88cd27969aaf0077559e56842d9a0f87, 8e64de3ac6818b4271d3de5d8e4a5d166d13d12804da01ce1cdb7510d8922cc6, 35fcc2058ae3a0af68c5ed7452e57ff286abe6ded68bf59078abd9e7b11ea90a, 7cc62a1bb2db82e76183eb06e4ca84e07a78cfb71241f21212afd1e01cb308b2, 29f11b5d4dbd6d06d4906b9035f5787e16f9e23134a2cc43dfc1165127c89bff, cfbcbb876064c2cf671bdae61544649fa13debbbe58b72cf8c630b5bfc0649f9, a3b78818bbef4fd55f704c96c203765b5ab37723bc87aac6aa7ebfcc76dfa06d, ac43c52b42b123e2530538273dfb12e3b70178aa1dee6d4fd5198c08bfeb4dc1

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

November 27, 2023 • 7:30 AM

© 2023 All Rights are Reserved by Hive Pro®



More at www.hivepro.com