Date of Publication
May 21, 2024

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

13 to 19 MAY 2024

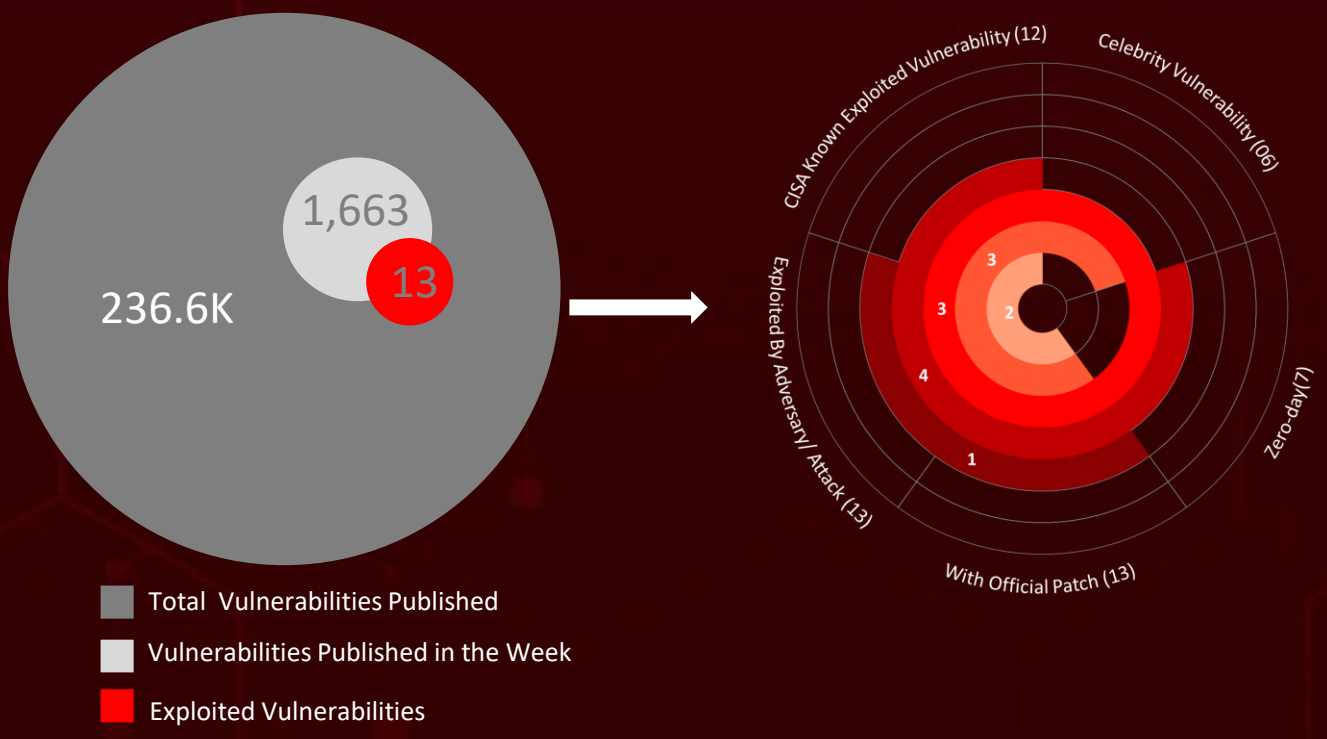
Table Of Contents

Summary

HiveForce Labs has recently unveiled several profound revelations within the domain of cybersecurity threats. Within the span of the past week alone, HiveForce Labs has unearthed **fourteen** executed attacks, disclosed **thirteen** vulnerabilities, and pinpointed **four** active adversaries. These discoveries underscore the persistent and mounting peril posed by cyber intrusions.

Furthermore, HiveForce Labs has unveiled that **Turla** is targeting entities across both the Europe and Middle East regions, infiltrated a European ministry of foreign affairs and various Middle Eastern entities, and skillfully evaded detection by discreetly deploying two previously undisclosed backdoors: LunarWeb and LunarMail.

Furthermore, Google Chrome has released three updates to its stable channel within a single week to address three actively exploited vulnerabilities. These rising attacks present a significant and immediate threat to users globally.



High Level Statistics

14
Attacks Executed

13
Vulnerabilities Exploited

4
Adversaries in Action

- DiceLoader
- Black Basta Rasnomware
- Qakbot
- Trinity Ransomware
- Cobalt Strike Beacon
- Ebury Botnet
- LunarLoader
- LunarWeb
- LunarMail
- Gomir
- Troll Stealer
- GoBear
- SugarGh0st RAT
- DarkGate

- CVE-2021-3129
- CVE-2024-1709
- CVE-2020-1472
- CVE-2021-42278
- CVE-2021-42287
- CVE-2021-34527
- CVE-2022-30190
- CVE-2024-4761
- CVE-2024-4947
- CVE-2024-30040
- CVE-2024-30051
- CVE-2021-45467
- CVE-2016-5195

- FIN7
- Turla
- Kimsuky
- UNK_SweetSpecter

Insights

LLMjacking:
Attack Method for stealing cloud credentials

Black Basta ransomware,
affecting over 500 organizations globally, using phishing, exploits, and Qakbot to gain access

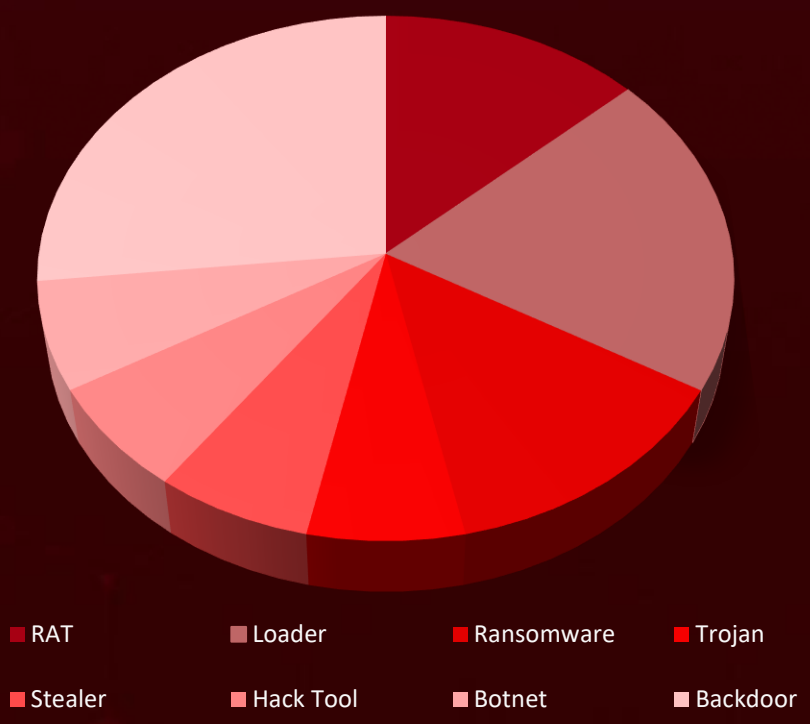
Kimsuky,
deploying a new Linux malware named Gomir, which is a variant of the GoBear backdoor

Google Chrome Zero-Day Flaws:
CVE-2024-4761 and CVE-2024-4947, vulnerabilities affect Chrome's V8 JavaScript engine, creating urgency for patching

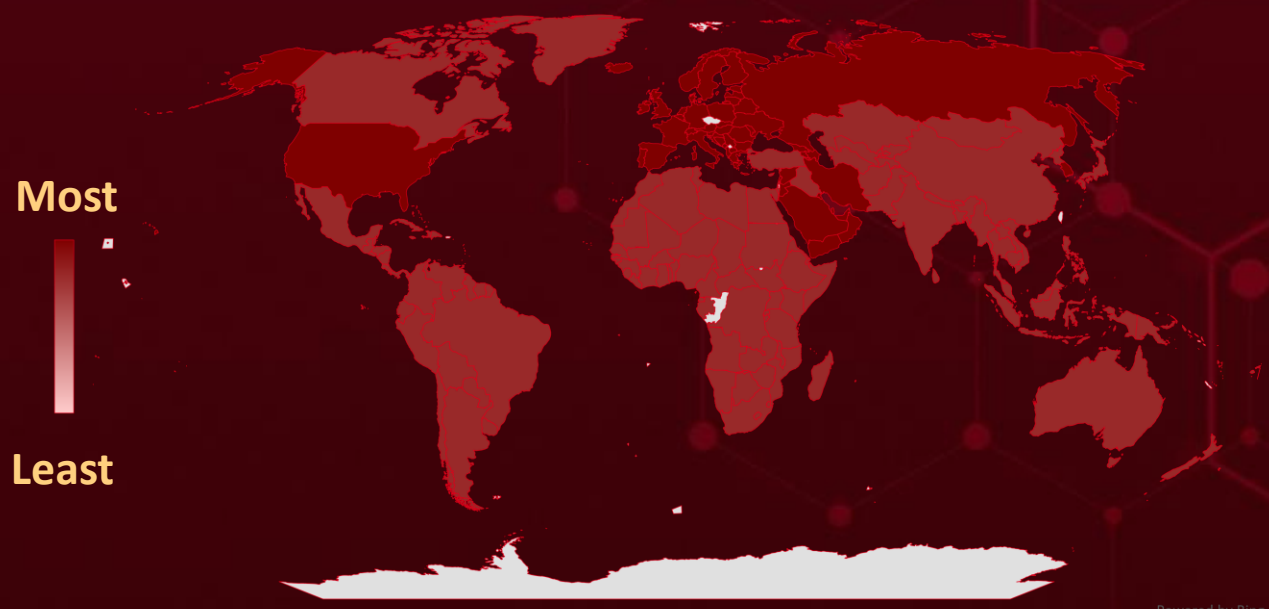
Ebury Botnet:
Linux malware botnet that has been infecting Linux servers, to steal cryptocurrency and credit card information

SugarGh0st RAT
Leveraged in a campaign targeting US organization by UNK_SweetSpecter

Threat Distribution

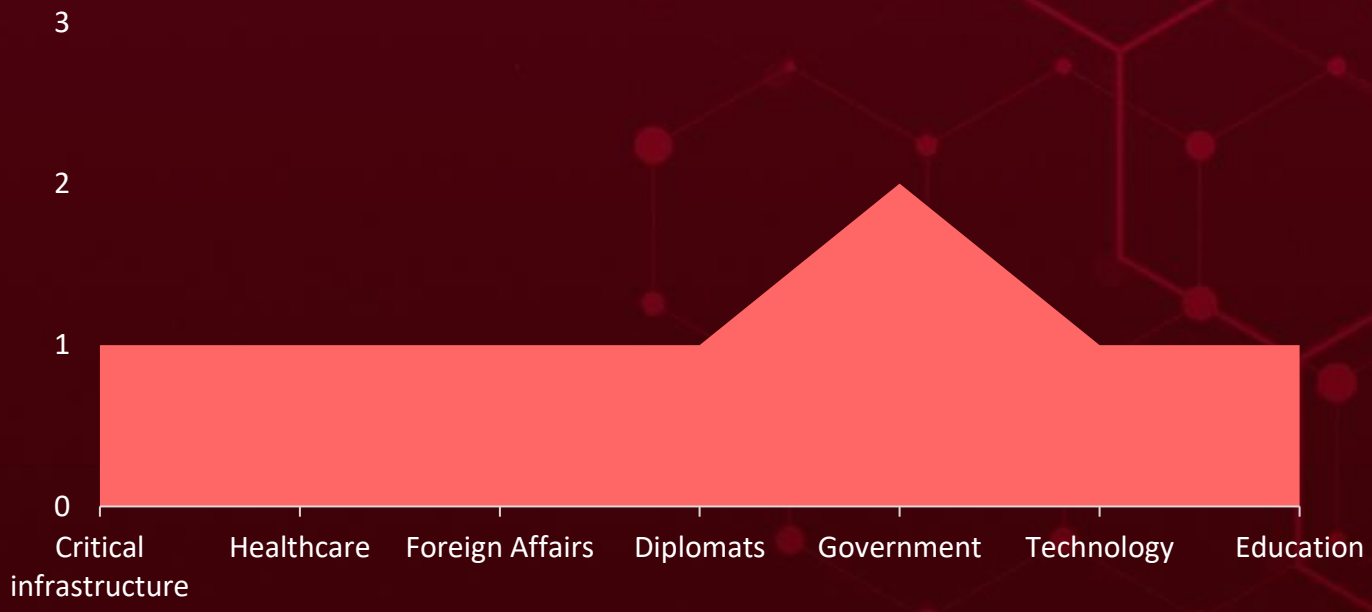


Targeted Countries



Countries	Countries	Countries	Countries
Lithuania	Croatia	Jordan	Tanzania
Saudi Arabia	Sweden	Ukraine	Colombia
Norway	Czech Republic (Czechia)	Kuwait	Timor-Leste
Albania	United Arab Emirates	United Kingdom	Morocco
Syria	Denmark	Latvia	Tonga
Andorra	Liechtenstein	Lebanon	Mozambique
Monaco	Estonia	Yemen	Tunisia
Armenia	Luxembourg	Uruguay	Myanmar
Qatar	Finland	Angola	Turkmenistan
Austria	Moldova	Costa Rica	Namibia
South Korea	France	Botswana	Uganda
Azerbaijan	Montenegro	Panama	Nauru
United States	Georgia	India	Ethiopia
Bahrain	North Macedonia	Philippines	Nepal
Malta	Germany	Indonesia	Algeria
Belarus	Oman	Argentina	Comoros
Netherlands	Greece	Brazil	Uzbekistan
Belgium	Portugal	Gambia	New Zealand
Poland	Holy See	Pakistan	Venezuela
Bosnia and Herzegovina	Romania	Belize	Nicaragua
Russia	Hungary	Djibouti	Niger
Bulgaria	San Marino	Benin	Lesotho
Slovakia	Iceland	Sri Lanka	Zimbabwe
	Serbia	Ghana	
		Turkey	
		Bhutan	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1204** User Execution	**T1140** Deobfuscate/ Decode Files or Information	**T1588** Obtain Capabilities	**T1036** Masquerading
T1204.002 Malicious File	**T1566** Phishing	**T1082** System Information Discovery	**T1027** Obfuscated Files or Information	**T1071.001** Web Protocols
T1059.001 PowerShell	**T1056** Input Capture	**T1547** Boot or Logon Autostart Execution	**T1057** Process Discovery	**T1570** Lateral Tool Transfer
T1498 Network Denial of Service	**T1005** Data from Local System	**T1562.001** Disable or Modify Tools	**T1070** Indicator Removal	**T1486** Data Encrypted for Impact

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DiceLoader	DiceLoader is a compact malware component in the FIN7 arsenal. It is deployed using a PowerShell script with specific obfuscation techniques and is often accompanied by other malware from their toolset.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
FIN7			-
IOC TYPE	**VALUE**		
MD5	bb0a503a83b1f9833c3d3d08784b78a8		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Black Basta Rasnomware	Black Basta is a ransomware-as-a-service (RaaS) variant that was first identified in April 2022. They employ a double-extortion model, where they not only encrypt the victim's systems but also exfiltrate data. This dual approach increases the pressure on victims to pay the ransom, as they face the threat of data leaks in addition to system inaccessibility.	Phishing	CVE-2021-34527 CVE-2022-30190
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Encrypt Data	Windows, Linux, macOS, and Vmware ESXi
ASSOCIATED ACTOR			**PATCH LINK**
-			https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190
IOC TYPE	**VALUE**		
SHA256	0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298, 034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79		

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

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">Qakbot</td><td rowspan="6">Classified as a banking trojan, Qakbot is designed to steal sensitive data and attempts to self-propagate to other systems within the network. Qakbot also provides remote code execution (RCE) capabilities, enabling attackers to perform manual attacks to achieve secondary objectives, such as scanning the compromised network or deploying ransomware.</td><td>Phishing</td><td>CVE-2021-34527
CVE-2022-30190</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Steal data</td><td rowspan="2">Windows, Linux, macOS, and Vmware ESXi</td></tr>
<tr><td>Trojan</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527 , https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">b3781927bcf7932c336630f636f47cbdba47e2f5aa94039f87fbb15797455535</td></tr>
</table>

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVEs</th></tr>
<tr><td rowspan="2">Trinity Ransomware</td><td rowspan="6">Trinity is a newly identified ransomware variant, believed to be an updated version of the "2023Lock" ransomware. This malware encrypts user files and appends the ".trinitylock" extension to them.</td><td>-</td><td>-</td></tr>
<tr><td>IMPACT</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>TYPE</td><td rowspan="3">Encrypt Data</td><td rowspan="2">-</td></tr>
<tr><td>Ransomware</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">36696ba25bdc8df0612b638430a70e5ff6c5f9e75517ad401727be03b26d8ec4</td></tr>
</table>

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
Cobalt Strike Beacon	Cobalt Strike is a paid penetration testing tool that allows attackers to deploy an agent called 'Beacon' on a victim's machine. Beacon offers a range of functionalities, including command execution, key logging, file transfer, SOCKS proxying, privilege escalation, mimikatz integration, port scanning, and lateral movement.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Execute Commands	-
Hack Tool			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
Domain	limitedtoday[.]com, thetrailbig[.]net		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Ebury Botnet	Ebury is a Linux malware botnet that has been infecting Linux servers for over a decade. It uses various tactics such as exploiting software vulnerabilities, using stolen credentials, and hiding behind fake identities. Once inside a server, Ebury can steal login information, act as a backdoor for further attacks, and deploy additional tools to steal credit card details and reroute traffic.	-	CVE-2021-45467 CVE-2016-5195
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal data	Linux
Botnet			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA1	0004b44d110ad9bc48864da3aea9d80edfceed3f 013647E5AD347539EEF6C5933B16AD01B1806C3C		

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
LunarLoader	LunarLoader utilizes the RC4 symmetric key cipher. It allocates memory for the PE image and decrypts the name of an exported function within the PE file, which is then executed in a new thread.	-	-
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	-
Loader			
ASSOCIATED ACTOR			PATCH LINK
Turla			-
IOC TYPE	VALUE		
SHA1	795c4127d42fe8dfaf4510b406b52ba5bede8d3a, 19d86cf2ed82eae23e019706fae8dafc60552e85		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
LunarWeb	The LunarWeb backdoor, deployed on servers, leverages HTTP(S) for its command and control (C&C) communications, emulating legitimate requests. During initialization, LunarWeb attempts to locate or generate its state file, which contains entries related to its execution.		-
		IMPACT	AFFECTED PRODUCTS
TYPE		System Compromise	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Turla			-
IOC TYPE	VALUE		
SHA1	754fb657156643fd09a68ec9fc124528578cab0c, 4c84110f1b10df5fdd612759e210e44b0f0505ef		

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
LunarMail	The LunarMail backdoor, installed on workstations, is embedded as an Outlook add-in and uses email messages for its command and control (C&C) communications. It employs steganography to hide commands within images, thereby evading detection.	-	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		System Compromise	-
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA1	fcae66f6d95c78dc829688cc0f4c39bb5a57828b, 67c6aec8d129e610378ef52f8bf934886587932f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Gomir	Gomir shares many similarities with GoBear, featuring direct C2 communication, persistence mechanisms, and support for executing a wide range of commands. Upon installation, the malware checks the group ID value to determine if it runs with root privileges on the Linux machine. If it has root privileges, it copies itself to /var/log/syslogd for persistence.	Social Engineering	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Exfiltrate data	Linux
ASSOCIATED ACTOR			**PATCH LINK**
Kimsuky			-
IOC TYPE	**VALUE**		
SHA256	30584f13c0a9d0c86562c803de350432d5a0607a06b24481ad4d92cdf7288213		

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
Troll Stealer	Troll Stealer is an information-stealing malware written in the Go language. It exfiltrates various types of data, including SSH credentials, FileZilla information, browser data, system information, and screen captures. The malware is distributed via droppers disguised as Korean security software installers and is signed with a stolen certificate.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Steal data	-
Stealer			
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	d7f3ecd8939ae8b170b641448ff12ade2163baad05ca6595547f8794b5ad013b, 36ea1b317b46c55ed01dd860131a7f6a216de71958520d7d558711e13693c9dc		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
GoBear	GoBear is a backdoor malware crafted in the Go language and authenticated with a legitimate D2innovation Co., LTD certificate. This insidious threat operates by executing malicious commands received from a C&C server. GoBear establishes persistent access to the infected system, enabling attackers to control and manipulate the device remotely.	Social Engineering	-
		IMPACT	AFFECTED PRODUCTS
TYPE		Execute Commands, Steal data	-
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
Kimsuky			-
IOC TYPE	VALUE		
SHA256	7bd723b5e4f7b3c645ac04e763dfc913060eaf6e136eecc4ee0653ad2056f3a0		

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
SugarGh0st RAT	SugarGh0st RAT is a remote access trojan, which is a customized variant of Gh0stRAT. During the infection process, it utilizes Windows Shortcut files containing malicious JavaScript to deploy DLL loaders and execute SugarGh0st binaries. This malware is capable of gathering system details, executing various file operations, enabling remote control by attackers, initiating reverse shells, and executing arbitrary commands sent by the attackers.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Execute Commands	-
RAT			
ASSOCIATED ACTOR			**PATCH LINK**
UNK_SweetSpecter			-
IOC TYPE	**VALUE**		
SHA256	351418c41f1abf7b4c8692188069fb38f1f5ce13bdea2ea7a59918cc52ee4719, 1e2413dcd36060144917e72bb862ec890ad81f2b51eaaeacee6418c2379d5704		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
DarkGate	DarkGate malware is a potent and adaptable threat that infiltrates computer systems, compromising security. It has infostealer functionality, enabling attackers to control compromised systems and extract valuable information. DarkGate has been implicated in various malicious activities, including data exfiltration, credential phishing, and ransomware deployment.	Phishing	-
		IMPACT	**AFFECTED PRODUCTS**
TYPE		Data Theft	
Loader			
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
URL	hxxp[:]//afarm[.]net/uvz2q hxxp[:]//affixio[.]com/emh0c		

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-2021-3129	✗	Laravel Ignition	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:facade:ignition:*:*:*:*:*:laravel:*:* cpe:2.3:a:laravel:laravel:*:*:*:*:*:*:*:*	-
Laravel Ignition File Upload Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter	https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/master/cves/2021/CVE-2021-3129.yaml

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-1709	✗	ConnectWise ScreenConnect	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:connectwise:screenconnect:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
ConnectWise ScreenConnect Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application	https://www.connectwise.com/company/trust/security-bulletins/connectwise-screenconnect-23.9.8

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-1472		Microsoft Netlogon	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
ZeroLogon (Microsoft Netlogon Privilege Escalation Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-330	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42278		Microsoft Active Directory Domain Services	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42278

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-42287	✓	Microsoft Active Directory Domain Services	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
NoPac (Microsoft Active Directory Domain Services Privilege Escalation Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-42287

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34527	✓	Windows Print Spooler	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
PrintNightmare (Windows Print Spooler Remote Code Execution Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2021-34527

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-30190	✓	Microsoft Windows Support Diagnostic Tool (MSDT)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*	Black Basta Rasnomware, Qakbot
Follina (Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability)	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-610	T1059: Command and Scripting Interpreter	https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2022-30190

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4761	✗	Google Chrome	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Out of bounds write in V8 Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-787	T1059.007: JavaScript T1189: Drive by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-4947		Google Chrome	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chrome Type Confusion in V8 Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1059.007: JavaScript T1189: Drive-by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30040		Microsoft Windows	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows MSHTML Platform Security Feature Bypass Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1204: User Execution	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30040

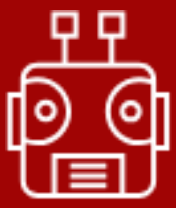
CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-30051	✗	Microsoft Windows DWM Core Library	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	-
Microsoft Windows DWM Core Library Elevation of Privilege Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-122	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30051

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-45467	✗	CentOS Web Panel	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:control-webpanel:webpanel:*:*:*:*:*:*:*:*	Ebury Botnet
CentOS Web Panel Pre-Authentication File Inclusion Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	-	T1068: Exploitation for Privilege Escalation	https://control-webpanel.com/changelog

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCTS</th><th>ASSOCIATED ACTOR</th></tr>
<tr><td rowspan="3">CVE-2016-5195</td><td>✓</td><td rowspan="2">Linux Kernel</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:o:canonical:ubuntu_linux:*:*:*:-:*:*:*</td><td rowspan="2">Ebury Botnet</td></tr>
<tr><td rowspan="3">Dirty COW (Linux Kernel Race Condition Vulnerability)</td><td>✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-362</td><td>T1068: Exploitation for Privilege Escalation</td><td>https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=19be0eaffa3ac7d8eb6784ad9bdbc7d67ed8e619</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"> 
FIN7 (aka Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, ITG14, TAG-CR1)</td><td>Russia</td><td rowspan="3">Casinos and Gambling, Construction, Education, Energy, Financial, Government, High-Tech, Hospitality, Retail, Technology, Telecommunications, Transportation</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>DiceLoader</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development; TA0043: Reconnaissance; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0011: Command and Control; T1566: Phishing; T1566.002: Spearphishing Link; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.006: Python; T1204: User Execution; T1204.001: Malicious Link; T1547: Boot or Logon Autostart Execution; T1033: System Owner/User Discovery; T1176: Browser Extensions; T1199: Trusted Relationship; T1056: Input Capture; T1036: Masquerading; T1053: Scheduled Task/Job; T1140: Deobfuscate/Decode Files or Information; T1055: Process Injection; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1518: Software Discovery; T1518.001: Security Software Discovery; T1592: Gather Victim Host Information; T1082: System Information Discovery; T1219: Remote Access Software; T1104: Multi-Stage Channels; T1132: Data Encoding; T1132.001: Standard Encoding</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 

Turla (aka Waterbug, Venomous Bear, Group 88, SIG2, SIG15, SIG23, Iron Hunter, CTG-8875, Pacifier APT, ATK 13, ITG12, Makersmark, Krypton, Belugasturgeon, Popeye, Wraith, TAG-0530, UNC4210, SUMMIT, Secret Blizzard, Pensive Ursa, Blue Python, Snake)</td><td>Russia</td><td rowspan="3">Foreign Affairs, Diplomats, Aerospace, Defense, Education, Embassies, Energy, Government, High-Tech, IT, Media, NGOs, Pharmaceutical, Research, Retail</td><td rowspan="3">Afghanistan, Algeria, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bolivia, Botswana, Brazil, China, Chile, Denmark, Ecuador, Estonia, Finland, France, Georgia, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Iraq, Italy, Jamaica, Jordan, Kazakhstan, Kyrgyzstan, Kuwait, Latvia, Mexico, Netherlands, Pakistan, Paraguay, Poland, Qatar, Romania, Russia, Serbia, Spain, Saudi Arabia, South Africa, Sweden, Switzerland, Syria, Tajikistan, Thailand, Tunisia, Turkmenistan, UK, Ukraine, Uruguay, USA, Uzbekistan, Venezuela, Vietnam, Yemen</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>LunarLoader, LunarWeb, LunarMail</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0042: Resource Development; TA0043: Reconnaissance; T1591: Gather Victim Org Information; T1583.002: DNS Server; T1583.003: Virtual Private Server; T1584.003: Virtual Private Server; T1586.002: Email Accounts; T1587.001: Malware; T1047: Windows Management Instrumentation; T1059: Command and Scripting Interpreter; T1059.001: PowerShell; T1059.003: Windows Command Shell; T1059.005: Visual Basic; T1106: Native API; T1204.002: Malicious File; T1137.006: Add-ins; T1547: Boot or Logon Autostart Execution; T1574: Hijack Execution Flow; T1027: Obfuscated Files or Information; T1027.003: Steganography; T1027.007: Dynamic API Resolution; T1027.009: Embedded Payloads; T1036.005: Match Legitimate Name or Location; T1070.004: File Deletion; T1070.008: Clear Mailbox Data; T1140: Deobfuscate/Decode Files or Information; T1480.001: Environmental Keying; T1620: Reflective Code Loading; T1007: System Service Discovery; T1016: System Network Configuration Discovery; T1057: Process Discovery; T1082: System Information Discovery; T1518.001: Security Software Discovery;</td></tr>
</table>

TTPs
T1005: Data from Local System; T1074.001: Local Data Staging; T1113: Screen Capture; T1114.001: Local Email Collection; T1560.002: Archive via Library; T1001.002: Steganography; T1001.003: Protocol Impersonation; T1071.001: Web Protocols; T1071.003: Mail Protocols; T1090.001: Internal Proxy; T1095: Non-Application Layer Protocol; T1132.001: Standard Encoding; T1573.001: Symmetric Cryptography; T1573.002: Asymmetric Cryptography; T1020: Automated Exfiltration; T1030: Data Transfer Size Limits; T1041: Exfiltration Over C2 Channel

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Kimsuky (aka Velvet Chollima, Springtail, Thallium, Black Banshee, SharpTongue, ITG16, TA406, TA427, APT 43, ARCHIPELAGO, Emerald Sleet, KTA082)	North Korea	Defense, Education, Energy, Government, Healthcare, Manufacturing, Think Tanks and Ministry of Unification, Sejong Institute and Korea Institute for Defense Analyses.	Japan, South Korea, Thailand, USA, Vietnam and Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	Gomir, Troll Stealer, GoBear	-

TTPs
TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0007: Discovery; TA0009: Collection; TA0010: Exfiltration; TA0011: Command and Control; TA0040: Impact; T1217: Browser Information Discovery; T1036: Masquerading; T1059: Command and Scripting Interpreter; T1057: Process Discovery; T1056: Input Capture; T1082: System Information Discovery; T1543: Create or Modify System Process; T1543.002: Systemd Service; T1053: Scheduled Task/Job; T1053.003: Cron; T1071: Application Layer Protocol; T1071.001: Web Protocols; T1005: Data from Local System; T1588: Obtain Capabilities; T1588.003: Code Signing Certificates; T1204: User Execution; T1204.002: Malicious File; T1189: Drive-by Compromise; T1070: Indicator Removal; T1070.004: File Deletion; T1529: System Shutdown/Reboot; T1546: Event Triggered Execution; T1546.016: Installer Packages

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="4"> 
UNK_SweetSpecter</td><td>-
MOTIVE
Espionage</td><td>Technology, Government, Education</td><td>USA</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>SugarGh0st RAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0005: Defense Evasion; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1083: File and Directory Discovery; T1570: Lateral Tool Transfer; T1071.001: Web Protocols; T1566.001: Spearphishing Attachment; T1566: Phishing; T1490: Inhibit System Recovery; T1059: Command and Scripting Interpreter; T1082: System Information Discovery; T1574: Hijack Execution Flow; T1057: Process Discovery; T1105: Ingress Tool Transfer; T1204.002: Malicious File; T1204: User Execution</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **thirteen exploited vulnerabilities** and block the indicators related to the threat actors **FIN7, Turla, Kimsuky, UNK_SweetSpecter** and malware **DiceLoader, Black Basta Rasnomware, Qakbot, Trinity Ransomware, Cobalt Strike Beacon, Ebury Botnet, LunarLoader, LunarWeb, LunarMail, Gomir, Troll Stealer, GoBear, SugarGh0st RAT, DarkGate.**

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 **thirteen exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **FIN7, Turla, Kimsuky, UNK_SweetSpecter** and malware **DiceLoader, Black Basta ransomware, Trinity Ransomware, Ebury Botnet, LunarMail, Gomir, Troll Stealer** in Breach and Attack Simulation(BAS).

Threat Advisories

LLMjacking: An Attack Method for Stealing Cloud Credentials

FIN7 Group Leverages Sponsored Ads to Disseminate Malicious Payloads

Black Basta Ransomware Impacts Over 500 Organizations Worldwide

Yet Another Google Chrome Zero-Day Exploited in the Wild

Trinity Ransomware Strikes with the Dual Extortion Strategy

Social Engineering Campaign Abuses RMM Tools, Linked to Black Basta

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

Ebury A Potent Linux Botnet Infects Over 400K Servers

LunarWeb and LunarMail: The Secret Weapons of the Turla APT

Kimsuky Expands Its Arsenal with New Backdoor

SugarGh0st RAT Infiltrates US AI Sector

DarkGate Malware: Persistent Threat in Active Distribution

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
DiceLoader	IPv4: Port	193[.]124[.]24[.]51:443, 38[.]135[.]52[.]151:273
	MD5	bb0a503a83b1f9833c3d3d08784b78a8
Black Basta Rasnomware	File path	C:\Program Files\MonitorIT\GWT.ps1,C:\Users\All Users\{redacted}\GWT.ps1,C:\Users\Public\7z.dll,C:\Users\Public\7zG.exe,C:\Users\Public\Audio\7z.dll,C:\Users\Public\Audio\7zG.exe,C:\Users\Public\Audio\db_Usr.sql,C:\Users\Public\Audio\esx.zip,C:\Users\Public\Audio\hv2.ps1,C:\Users\Public\Audio\Jun.exe,C:\Users\Public\BitData.exe,C:\Users\Public\BitLogic.dll,C:\Users\Public\DataSoft.exe,C:\Users\Public\db_Usr.sql,C:\Users\Public\DigitalText.dll,C:\Users\Public\eucr.exe,C:\Users\Public\GeniusMesh.exe,C:\Users\Public\NetApp.exe,C:\Users\Public\socksps.ps1,C:\Users\Public\Thief.exe,C:\Windows\DS_c1.dll,\Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse86.exe,\Device\Mup\{redacted}\C$\Users\Public\Music\DumpNParse.exe,\Device\Mup\{redacted}\C$\Users\Public\Music\POSTDump.exe,\Device\Mup\{redacted}\C$\Users\Public\Music\PROCEXP.sys,*\instructions_read_me.txt
	Domain	airbusco[.]net, allcompanycenter[.]com, animalsfast[.]net, artspathgroupe[.]net, artspathgroup[.]net, artstrailman[.]com,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	Domain	artstrailreviews[.]com, audsystemecll[.]net, auuditoe[.]com, bluenetworking[.]net, brendonline[.]com, businesforhome[.]com, businessprofessionalllc[.]com, buyblocknow[.]com, buygreenstudio[.]com, caspercan[.]com, childrensdolls[.]com, clearsystemwo[.]net, cloudworldst[.]net, constrtionfirst[.]com, consulheartinc[.]com, currentbee[.]net, erihudeg[.]com, garbagemoval[.]com, gartenlofti[.]com, getfnewsolutions[.]com, getfnewssolutions[.]com, investmendvisor[.]net, investmentgblog[.]net, investmentrealtyhp[.]net, investrealtydom[.]net, ionoslaba[.]com, jenshol[.]com, jessvisser[.]com, karmafisker[.]com, kekeoamigo[.]com, kolinileas[.]com, limitedtoday[.]com, magentoengineers[.]com, maluisepaul[.]com, masterunix[.]net, modernbeem[.]net, monitorsystem[.]net, monitor-websystem[.]net, myfinancialexperts[.]com, mytrailinvest[.]net, nebraska-lawyers[.]com, oneblackwood[.]com, onedogsclub[.]com, ontexcare[.]com, otxcarecosmetics[.]com, otxcosmeticscare[.]com,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	Domain	prettyanimals[.]net, protectionek[.]com, rasapool[.]net, realbumblebee[.]net, recentbeelive[.]com, recentbee[.]net, reelsysmoona[.]net, securecloudmanage[.]com, seohomee[.]com, septcntr[.]com, simorten[.]com, softradar[.]net, specialdrills[.]com, startupbizaud[.]net, startupbusiness24[.]net, startupbuss[.]com, startupmartec[.]net, startuptechnologyw[.]net, steamteamdev[.]net, stockinvestlab[.]net, taskthebox[.]net, technologgies[.]com, thesmartcloudusa[.]com, thetrailbig[.]net, tomlawcenter[.]com, topglobaltv[.]com, trackgroup[.]net, trailcocompany[.]com, trailcosolutions[.]com, trailgroupl[.]net, trailshop[.]net, treeauwin[.]net, unitedfrom[.]com, unougn[.]com, usaglobalnews[.]com, wardeli[.]com, webnubee[.]com, welausystem[.]net, wellsystemte[.]net, wipresolutions[.]com, withclier[.]com
	IPv4	104[.]21[.]26[.]145, 104[.]21[.]40[.]72, 107[.]189[.]30[.]69, 116[.]203[.]186[.]178, 151[.]101[.]130[.]159, 155[.]138[.]246[.]122,

Attack Name	TYPE	VALUE
Black Basta Rasnomware	IPv4	183[.]181[.]86[.]147, 185[.]219[.]221[.]136, 185[.]220[.]100[.]240, 185[.]220[.]101[.]149, 185[.]7[.]214[.]79, 188[.]130[.]137[.]181, 188[.]130[.]218[.]39, 207[.]126[.]152[.]242, 34[.]120[.]190[.]48, 34[.]149[.]120[.]3, 34[.]149[.]36[.]179, 34[.]160[.]17[.]71, 34[.]160[.]81[.]203, 34[.]250[.]161[.]149, 34[.]251[.]163[.]236, 35[.]190[.]31[.]54, 35[.]212[.]86[.]55, 35[.]227[.]194[.]51, 35[.]244[.]153[.]44, 46[.]161[.]27[.]151, 46[.]8[.]10[.]134, 46[.]8[.]16[.]77, 5[.]183[.]130[.]92, 5[.]78[.]115[.]67, 64[.]176[.]219[.]106, 66[.]249[.]66[.]18, 72[.]14[.]196[.]192, 72[.]14[.]196[.]2, 72[.]14[.]196[.]226, 72[.]14[.]196[.]50, 80[.]239[.]207[.]200, 83[.]243[.]40[.]10, 88[.]198[.]198[.]90, 95[.]181[.]173[.]227
	SHA256	0112e3b20872760dda5f658f6b546c85f126e803e27f0577b294f335ffa5a298, 034b5fe047920b2ae9493451623633b14a85176f5eea0c7aadc110ea1730ee79, 0554eb2ffa3582b000d558b6950ec60e876f1259c41acff2eac47ab78a53e94a, 05ebae760340fe44362ab7c8f70b2d89d6c9ba9b9ee8a9f747b2f19d326c3431, 07117c02a09410f47a326b52c7f17407e63ba5e6ff97277446efc75b862d2799,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Black Basta Rasnomware	SHA256	0a8297b274aeab986d6336b395b39b3af1bb00464cf5735d1ecdb506fef9098e, 17205c43189c22dfcb278f5cc45c2562f622b0b6280dcd43cc1d3c274095eb90, 17879ed48c2a2e324d4f5175112f51b75f4a8ab100b8833c82e6ddb7cd817f20, 1c1b2d7f790750d60a14bd661dae5c5565f00c6ca7d03d062adcecda807e1779, 3090a37e591554d7406107df87b3dc21bda059df0bc66244e8abef6a5678af35, 3337a7a9ccdd06acdd6e3cf4af40d871172d0a0e96fc48787b574ac93689622a, 350ba7fca67721c74385faff083914ecdd66ef107a765dfb7ac08b38d5c9c0bd, 360c9c8f0a62010d455f35588ef27817ad35c715a5f291e43449ce6cb1986b98, 37a5cd265f7f555f2fe320a68d70553b7aa9601981212921d1ac2c114e662004, 39939eacfbc20a2607064994497e3e886c90cd97b25926478434f46c95bd8ead, 3a8fc07cadc08eeb8be342452636a754158403c3d4ebff379a4ae66f8298d9a6, 3c50f6369f0938f42d47db29a1f398e754acb2a8d96fd4b366246ac2ccbe250a, 3c65da7f7bfdaf9acc6445abbedd9c4e927d37bb9e3629f34afc338058680407, 42f05f5d4a2617b7ae0bc601dd6c053bf974f9a337a8fcc51f9338b108811b78, 462bbb8fd7be98129aa73efa91e2d88fa9cafc7b47431b8227d1957f5d0c8ba7, 4ac69411ed124da06ad66ee8bfbcea2f593b5b199a2c38496e1ee24f9d04f34a, 51eb749d6cbd08baf9d43c2f83abd9d4d86eb5206f62ba43b768251a98ce9d3e, 58ddbea084ce18cfb3439219ebcf2fc5c1605d2f6271610b1c7af77b8d0484bd, 5942143614d8ed34567ea472c2b819777edd25c00b3e1b13b1ae98d7f9e28d43, 5b2178c7a0fd69ab00cef041f446e04098bbb397946eda3f6755f9d94d53c221, 5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa, 62e63388953bb30669b403867a3ac2c8130332cf78133f7fd4a7f23cdc939087,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Black Basta Rasnomware	SHA256	69192821f8ce4561cf9c9cb494a133584179116cb2e7409bea3e18901a1ca944, 723d1cf3d74fb3ce95a77ed9dff257a78c8af8e67a82963230dd073781074224, 7ad4324ea241782ea859af12094f89f9a182236542627e95b6416c8fb9757c59, 808c96cb90b7de7792a827c6946ff48123802959635a23bf9d98478ae6a259f9, 819cb9bcf62be7666db5666a693524070b0df589c58309b067191b30480b0c3a, 8501e14ee6ee142122746333b936c9ab0fc541328f37b5612b6804e6cdc2c2c6, 86a4dd6be867846b251460d2a0874e6413589878d27f2c4482b54cec134cc737, 882019d1024778e13841db975d5e60aaae1482fcf86ba669e819a68ce980d7d3, 88c8b472108e0d79d16a1634499c1b45048a10a38ee799054414613cc9dccccc, 8C68B2A794BA3D148CAE91BDF9C8D357289752A94118B5558418A36D95A5A45F, 90ba27750a04d1308115fa6a90f36503398a8f528c974c5adc07ae8a6cd630e7, 96339a7e87ffce6ced247feb9b4cb7c05b83ca315976a9522155bad726b8e5be, 9a55f55886285eef7ffabdd55c0232d1458175b1d868c03d3e304ce7d98980bc, a7b36482ba5bca7a143a795074c432ed627d6afa5bc64de97fa660faa852f1a6, acb60f0dd19a9a26aaaefd3326db8c28f546b6b0182ed2dcc23170bcb0af6d8f, ae7c868713e1d02b4db60128c651eb1e3f6a33c02544cc4cb57c3aa6c6581b6e, b32daf27aa392d26bdf5faafbaae6b21cd6c918d461ff59f548a73d447a96dd9, b6a4f4097367d9c124f51154d8750ea036a812d5badde0baf9c5f183bb53dd24, c26a5cb62a78c467cc6b6867c7093fbb7b1a96d92121d4d6c3f0557ef9c881e0, d15bfbc181aac8ce9faa05c2063ef4695c09b718596f43edc81ca02ef03110d1, d3683beca3a40574e5fd68d30451137e4a8bbaca8c428ebb781d565d6a70385e, D503090431fdd99c9df3451d9b73c5737c79eda6eb80c148b8dc71e84623401f,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Black Basta Rasnomware	SHA256	d73f6e240766ddd6c3c16eff8db50794ab8ab95c6a616d4ab2bc96780f13464d, df5b004be71717362e6b1ad22072f9ee4113b95b5d78c496a90857977a9fb415, e28188e516db1bda9015c30de59a2e91996b67c2e2b44989a6b0f562577fd757, f039eaaced72618eaba699d2985f9e10d252ac5fe85d609c217b45bc8c3614f4, f21240e0bf9f0a391d514e34d4fa24ecb997d939379d2260ebce7c693e55f061, fafaff3d665b26b5c057e64b4238980589deb0dff0501497ac50be1bc91b3e08, Fff35c2da67eef6f1a10c585b427ac32e7f06f4e4460542207abcd62264e435f
	MD5	2642ec377c0cee3235571832cb472870, 4c897334e6391e7a2fa3cbcbf773d5a4, B3fe23dd4701ed00d79c03043b0b952e
Trinity Ransomware	MD5	949c438e4ed541877dce02b38bf593ad
	SHA1	4c58d2d624d9bdf6b14a6f85637887850749 47a7
	SHA256	36696ba25bdc8df0612b638430a70e5ff6c5f9e75517ad401727be03b26d8ec4
Cobalt Strike Beacon	Domain	limitedtoday[.]com, thetrailbig[.]net
Ebury Botnet	IPv4	135[.]181[.]148[.]230, 141[.]164[.]52[.]243, 141[.]255[.]166[.]187, 146[.]70[.]124[.]102, 185[.]145[.]245[.]167, 185[.]59[.]103[.]8, 195[.]123[.]225[.]83, 213[.]232[.]235[.]104, 45[.]59[.]120[.]146
	Domain	a1hcy1xendd[.]net, a1k8h2xendd[.]info, a1t9y1xendd[.]info, a1z1h2xendd[.]biz, abo0u6ach9k3w[.]net, b2z6m9k1zaf3v[.]net, b8dfs5ecw9p3o[.]info, c0dbq5vcj9o3e[.]info, c1b1jfi2pdi8w1f[.]net, c1jczbhcpdi8w1f[.]biz, c1m8k5q0hfi8w1f[.]net,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Ebury Botnet	Domain	c1v9j2pahfi8w1f[.]biz, c1v9l8s6yei8w1f[.]info, c9xfb8u1cad3m[.]net, checklicence[.]net, f2y1j8v1saa3t[.]biz, f8wda5yck9i3h[.]net, fas1k9i1jap3u[.]biz, h0nct5rca9y3f[.]biz, h9g0q8a1hat3s[.]net, hdm5o8e1tas3n[.]net, idkff7m1lac3g[.]biz, k2qai2yeodm[.]net, k2rdz1yeodm[.]biz, k2t6i2yeodm[.]biz, k2zbz1yeodm[.]info, larfj7g1vaz3y[.]net, m2d4berdzej8x1o[.]info, m2kcjcj2ifj8x1o[.]biz, m2lfk2jfqdj8x1o[.]info, m2w9c4qaqdj8x1o[.]net, m7lea5yck9i3l[.]biz, mae2d2tejdt[.]info, maefu1tejdt[.]net, mag8u1tejdt[.]biz, map9u1tejdt[.]net, maved2tejdt[.]info, o5dec1berdn[.]info, o5e4l2berdn[.]net, o5lcl2berdn[.]biz, o5o8c1berdn[.]net, o5tac1berdn[.]biz, o8rad5ccx9f3r[.]net, o9f3v8r1oaj3p[.]biz, oafcffg8uee8s1v[.]net, oah5w1w4uee8s1v[.]biz, oap3p6f5lde8s1v[.]biz, oaxey7m0lde8s1v[.]info, oay4vbx7dfe8s1v[.]net, odrbz8i1jap3e[.]biz, op3f1libgh[.]biz, pbarsec[.]com, q5ncv0dekcm8a1p[.]biz, q5o2uad1cem8a1p[.]net, q5w0f4n5lfm8a1p[.]info, q5w0g7cbcem8a1p[.]biz,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Ebury Botnet	Domain	q5y6vdf7tdm8a1p[.]info, qimpj6kkofzf[.]biz, raj2p8z1aae3b[.]net, tav4h8n1baw3r[.]info, u2s0k8d1ial3r[.]info, uajdm8w1kax3j[.]info, ubjcl5ucn9g3m[.]info, v2a7q8a1hat3u[.]biz, x7sbu5hcg9b3f[.]net, xdc1h8n1baw3m[.]info, y2fad8b1gak3f[.]net, z9w8l8k1zaf3g[.]info, zbqaf5zcv9s3x[.]biz, zdm3u9x1fag3i[.]info, ibz[.]so, iptables-multi, iptables-multi-1[.]4[.]7, libcurl[.]so[.]4[.]4[.]0, libcurl[.]so[.]4[.]5[.]0, libcurl[.]so[.]4[.]6[.]0, libkeystats[.]so, libkeyutils[.]so, libkeyutils[.]so[.]1[.]5, Libllz564, libns2[.]so, libns5[.]so, libpw3[.]so, libpw5[.]so, librwctl[.]so, libsbr[.]so, libslr[.]so, libstz[.]so, mod_auth_basic[.]so, mod_authn_file[.]so, mod_authz_host[.]so, mod_authz_user[.]so, mod_dir[.]so, mod_env[.]so, nf_conntrack6[.]ko
	File path	/bin/hostname, /bin/sync, /dev/event-E4LgEFWIcy, /dev/event/loop0, /dev/stats-MxPAxNpy3x,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Ebury Botnet	File Path	/proc/udevd, /proc/ulog, /run/systemd/journal/dlog, /run/systemd/journal-YAjXO8luqOa, /run/systemd/log, /run/systemd/log-90zMvYX7uL, /run/systemd/log-wuO3nuFBHN, /sbin/auditd, /sbin/rsyslogd, /sbin/udevd, /tmp/dbus-0m9eDQpdXZ, /tmp/dbus-9XZXkmdfpN, /tmp/dbus-kZ8VEtJDOJ, /tmp/dbus-luzG4UqDt8, /tmp/dbus-n3UUkeqEZG, /tmp/dbus-vBWUDhHCHp, /tmp/dbus-VdyGBaqZws, /tmp/dbus-Xrga2cOewg, /tmp/dbus-ZP7tFO4xsL, /usr/lib/systemd/systemd-udevd, /usr/sbin/acpid, /usr/sbin/anacron, /usr/sbin/arpd, /usr/sbin/atd, /usr/sbin/crond
	SHA1	0004b44d110ad9bc48864da3aea9d80edfceed3f, 013647E5AD347539EEF6C5933B16AD01B1806C3C, 035327b42f6e910b652bbdde5d9c270cfbaa9669, 03592b8147e2c84233da47f6e957acd192b3796a, 04FF6202534A394586D826B320645AEC24CE7AA5, 051a89a7a335062829a8e938b8d4e3e2b532f6ff, 070F85BF02AD3FB0978785B3272D7B08F5C47A1A, 09c8af3be4327c83d4a7124a678bbc81e12a1de4, 0B91C3C2627F9948B8F3446822F99FAF88081267, 0daa51519797cefedd52864be0da7fa1a93ca30b, 0eb1108a9d2c9fe1af4f031c84e30dcb43610302, 10c6ce8ee3e5a7cb5eccf3dffd8f580e4fb49089, 10F94157365E6A1BBB101B3222EE3C3C675B9829, 12666F2FBEFC55F1DDB4BA86B5D85DB733889162, 12EA4595C6F38E60C23F09B2F08D78BA6EB0C1B3, 149cf77d2c6db226e172390a9b80bc949149e1dc, 15560B44286122FA0679C6C2368817CE2DC747E6, 16EE09926A2109262686D58974079ADC25E31AA1, 17c40a5858a960afd19cc02e07d3a5e47b2ab97a,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Ebury Botnet	SHA1	1918E40580291D0299A78DDFB9123923F832CEB3, 1972616a731c9e8a3dbda8ece1072bd16c44aa35, 1a9aff1c382a3b139b33eeccae954c2d65b64b90, 1d3aafce8cd33cf51b70558f33ec93c431a982ef, 1dd7a18125353d426b5314c4ba04d60674ffa837, 20467521bfd58e9ed388ce83467d73e8fd0293a7, 20599D89E4F648CF0F6EB46DEE67DB63984A8C36, 22BB2E0D1E1B0B009464E2919A381C4951D7D90D, 24e3ebc0c5a28ba433dfa69c169a8dd90e05c429, 25a819d658d02548b2e5bdb52d2002df2f65b03a, 267d010201c9ff53f8dc3fb0a48145dc49f9de1e, 27ed035556abeeb98bc305930403a977b3cc2909, 2DBF91347FA987E6199DAE5141641D04D0C963FF, 2e571993e30742ee04500fbe4a40ee1b14fa64d7, 2f382e31f9ef3d418d31653ee124c0831b6c2273, 2fc132440bafdbc72f4d4e8dcb2563cc0a6e096b, 3137DCA3F6FBD566F4ED2F49076A63D84869E13C, 32BB38D7D6B03DB4779E7A7183E7FA42DFBAFFC2, 3988D1A743E83D532130BC8090A7BC7001FE1BB0, 39ec9e03edb25f1c316822605fe4df7a7b1ad94a, 3c5ec2ab2c34ab57cba69bb2dee70c980f26b1bf, 42123cbf9d51fb3dea312290920b57bd5646cefb, 429A81BBD18A35C3C4D1DCB8BC76F5A7D9724A79, 44B04CFC095F93D17B1BD4F8820C16843FCBAC3E, 44b340e90edba5b9f8cf7c2c01cb4d45dd25189e, 471ee431030332dd636b8af24a428556ee72df37, 4A7303DD8E7BBBF063463B3852245ABDD343F5B6, 4d12f98fd49e58e0635c6adce292cc56a31da2a2, 4f40bb464526964ba49ed3a3b2b2b74491ea89a4, 4F92498FB8C1BFED97F18CFB7B36AF899F70F582, 5196a8a034611aaa112232767aafd74b8ef71279, 535C5588ED2EF9A4E960882C23E3104E81F2C079, 53829463A7DE8C4BACE97B1F6925728F3421DF53, 575bb6e681b5f1e1b774fee0fa5c4fe538308814, 580E6075C65D867667D507E2B00C8EEF79C907A1, 58f185c3fe9ce0fb7cac9e433fb881effad31421, 59F238DA1FD822AAD6FA7DF78D823854EAF8762E, 5b87807b4a1796cfb1843df03b3dca7b17995d20, 5bdf483279a4a816ed4f8a235e799d5068d14f64, 5c796dc566647dd0db74d5934e768f4dfafec0e5, 5d3ec6c11c6b5e241df1cc19aa16d50652d6fac0, 615c6b022b0fac1ff55c25b0b16eb734aed02734, 6180d8c1c6967d15a0abb0895103ccc817e43362, 62c4b65e0c4f52c744b498b555c20f0e76363147,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Ebury Botnet	SHA1	6369AD38D39562DD9D6D3E2612496A5357FFC09B, 67C1905EF4D0422DBDFAC41DC80F9C4D5C69E288, 6BEE8F88F3F145170CEF58D9F790DDD99CDFA547, 6FF132E50EFA5ABF534A005CB58C9C5B5FC39BEC, 71CA9B7C418264C2C856D47483666D123861D476, 72048DEABE7F37BBECBFDA1570E1AB6B366B72BD, 7248e6eada8c70e7a468c0b6df2b50cf8c562bc9, 7314eadbdf18da424c4d8510afcc9fe5fcb56b39, 74aa801c89d07fa5a9692f8b41cb8dd07e77e407, 74cd5ae9f6bbdf27b4eaf45c4a22c6aae07345a2, 75E8A197B6A9A7903CA43782BDD77CD9611FEFE0, 787A93F86E7F5FCF922E996B577DF532270C7184, 78c63e9111a6701a8308ad7db193c6abb17c65c4, 7adb38bf14e6bf0d5b24fa3f3c9abed78c061ad1, 858c612fe020fd5089a05a3ec24a6577cbeaf7eb, 899b860ef9d23095edb6b941866ea841d64d1b26, 8daad0a043237c5e3c760133754528b97efad459, 8f75993437c7983ac35759fe9c5245295d411d35, 9018377c0190392cc95631170efb7d688c4fd393, 907822012D6A970D676B634903F099587ED9C335, 9209D757770AAFCA0B84B9F63B8769DF8CAC3F1A, 94532111459E024BCB7E2025A6C145876A46F829, 947EEE633E9347F72625FB652F94488A4B2B37F0, 9569A8411477305FACA78E1C944D479EFA028DFB, 96FD9B3064F04EE3063B2B103F856BB729B58749, 98cdbf1e0d202f5948552cebaa9f0315b7a3731d, 98FBD545B5C1B1FE185730BA9B1CD4BEBFAE4476, 9bb6a2157c6a3df16c8d2ad107f957153cba4236, 9e2af0910676ec2d92a1cad1ab89029bc036f599, a0f18b5ee2d347961b7109a22ea06cca962693d2, a51b1835abee79959e1f8e9293a9dcd8d8e18977, a53a30f8cdf116de1b41224763c243dae16417e4, a559ee8c2662ee8f3c73428eaf07d4359958cae1, A64D6C7444FC2404A589ED7F8527E698682A3E68, a7b8d06e2c0124e6a0f9021c911b36166a8b62c5, AA0EC27C26E5484B4EB23D8424B2412221D5C7FC, ac96adbe1b4e73c95c28d87fa46dcf55d4f8eea2, AD350D7DA4BF1F7080026B683F93401CD735E974, adfcd3e591330b8d84ab2ab1f7814d36e7b7e89f, b58725399531d38ca11d8651213b4483130c98e2, b8508fc2090ddee19a19659ea794f60f0c2c23ff, bbce62fb1fc8bbed9b40cfb998822c266b95d148, bCC3B83CFADBD58256FC41AF9F0BFF50AC1F148B, bd867907a5059ab1850918d24b4b9bbe33c16b76,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Ebury Botnet	SHA1	bf1466936e3bd882b47210c12bf06cb63f7624c0, c4c28d0372aee7001c44a1659097c948df91985d, CD9A5B823906CC620B28D69DBDB11BD9FE6B3E03, CFB48909B978E91CFC6FFCAF2E4B04F27F503B34, D392022D8B72BCDDB849A94829C87731874E94AC, D39959356283DB4B3184BDB15E890E74CF1EA65C, D3D6567862B4B7811BEA76BE117E901B2B6B8399, d4eeada3d10e76a5755c6913267135a925e195c6, d552cbadee27423772a37c59cb830703b757f35e, D8647E825EFE74BF1726C0C494E3C2588FFF2262, D901D65F7A7A49296A501420F6D32BBF968F5BDE, dd7846b3ec2e88083cae353c02c559e79124a745, DDAE9417470F832DB550EFB716B5BAEAAAA35372, ddb9a74cd91217cfcf8d4ecb77ae2ae11b707cd7, DFAECF7EBFC169CDF923AF421EDD537CCE536A64, e14da493d70ea4dd43e772117a61f9dbcff2c41c, e2a204636bda486c43d7929880eba6cb8e9de068, E39667AA137E315BC26EAEF791CCAB52938FD809, E7DEBD6E453192AD8376DB5BAB03ED0D87566591, E8d392ae654f62c6d44c00da517f6f4f33fe7fed, e8d3c369a231552081b14076cf3eaa8901e6a1cd, eb352686d1050b4ab289fe8f5b78f39e9c85fb55, ebc45dd1723178f50b6d6f1abfb0b5a728c01968, EC4941BDD9FFB241968FD59A28B70BCE288ED261, ED5662F3CF80B8108D2172FBCA6119E403205EAA, EDD2DE0FAFE84EA51029FFDE38ACBB5918108DF5, ee679661829405d4a57dbea7f39efeb526681a7f, f1ada064941f77929c49c8d773cbad9c15eba322, f634f305a655b06f2647b82b58f7d3920546ac89, fa6707c7ef12ce9b0f7152ca300ebb2bc026ce0b, fc39009542c62a93d472c32891b3811a4900628a, FD6709AF6A8DC384B101A8E9ED36C1092533C404 Fdf91a8c0ff72c9d02467881b7f3c44a8a3c707a
LunarLoader	SHA1	795c4127d42fe8dfaf4510b406b52ba5bede8d3a, 19d86cf2ed82eae23e019706fae8dafc60552e85, 00006b30806f915911349d82beeb1aeb9025adb4, 94a4ce9c75bc847e7be59b96c4133d677d909414, f09e36553e48ebd42e60d9b25a390c0f57ff8de0, 2ed792e39f7d56de52bdf4aed96afc898478bfdf
LunarWeb	SHA1	754fb657156643fd09a68ec9fc124528578cab0c, 4c84110f1b10df5fdd612759e210e44b0f0505ef, 5d3975e57bdcb630a00febe5d405eefb6d119d86, 5ef771afc96c24371d367448627609cfacb34a57, 512e4fa7d6119270ff44a3b2a2359ee8825392ef

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
LunarWeb	IPv4	45[.]33[.]24[.]145, 45[.]79[.]93[.]87, 65[.]109[.]179[.]67, 74[.]50[.]80[.]35, 82[.]165[.]158[.]86, 82[.]223[.]55[.]220, 139[.]162[.]23[.]113, 158[.]220[.]102[.]80, 161[.]97[.]74[.]237, 176[.]57[.]150[.]252, 212[.]57[.]35[.]174, 212[.]57[.]35[.]176
LunarMail	File path	%LOCALAPPDATA%\Microsoft\Outlook\outlk.share
	SHA1	fcae66f6d95c78dc829688cc0f4c39bb5a57828b, 67c6aec8d129e610378ef52f8bf9348865879 32f, 9cec3972fa35c88de87bd66950e18b3e0a6df77c, 2ed792e39f7d56de52bdf4aed96afc898478bfdf, f09e36553e48ebd42e60d9b25a390c0f57ff8de0
Gomir	SHA256	30584f13c0a9d0c86562c803de350432d5a0607a06b24481ad4d92cdf7288213
Troll Stealer	SHA256	d7f3ecd8939ae8b170b641448ff12ade2163baad05ca6595547f8794b5ad013b, 36ea1b317b46c55ed01dd860131a7f6a216de71958520d7d558711e13693c9dc, 8e45daace21f135b54c515dbd5cf6e0bd28ae2515b9d724ad2d01a4bf10f93bd, 6c2a8e2bbe4ebf1fb6967a34211281959484032af1d620cbab390e89f739c339, 47d084e54d15d5d313f09f5b5fcdea0c9273dcddd9a564e154e222343f697822, 8a80b6bd452547650b3e61b2cc301d525de139a740aac9b0da2150ffac986be4, 380ec7396cc67cf1134f8e8cda906b67c70aa5c818273b1db758f0757b955d81, ff945b3565f63cef7bb214a93c623688759ee2805a8c574f00237660b1c4d3fd, cc7a123d08a3558370a32427c8a5d15a4be98fb1b754349d1e0e48f0f4cb6bfc, 8898b6b3e2b7551edcceffbef2557b99bdf4d99533411cc90390eeb278d11ac8, ecab00f86a6c3adb5f4d5b16da56e16f8e742adfb82235c505d3976c06c74e20, d05c50067bd88dae4389e96d7e88b589027f75427104fdb46f8608bbcf89edb4,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Troll Stealer	SHA256	a98c017d1b9a18195411d22b44dbe65d5f4a9e181c81ea2168794950dc4cbd3c, 831f27eb18caf672d43a5a80590df130b0d3d9e7d08e333b0f710b95f2cde0e0, bc4c1c869a03045e0b594a258ec3801369b0dcabac193e90f0a684900e9a582d, 5068ead78c226893df638a188fbe7222b99618b7889759e0725d85497f533e98
GoBear	SHA256	7bd723b5e4f7b3c645ac04e763dfc913060eaf6e136eecc4ee0653ad2056f3a0
SugarGh0st	Domain	account.gommask[.]online
	IPv4	43[.]242[.]203[.]115
	SHA256	351418c41f1abf7b4c8692188069fb38f1f5ce13bdea2ea7a59918cc52ee4719, 1e2413dcd36060144917e72bb862ec890ad81f2b51eaaeacee6418c2379d5704, 696533c07a78b8f4b3231f0a22502c1c85fefcf798c3272cdc2b05a4e8b86727, 8b9e0e9ac7c8d61252f2edd6104197ad2e2476fda86583aeef7f5994bcf85b08, ee5982a71268c84a5c062095ce135780b8c2ffb1f266c2799173fb0f7bfdd33e, fbf1038e32d41fa28286e6726f7e39c518cee67edd688615bccfe61a74dcaa86
DarkGate	URL	hxxp[:]//afarm[.]net/uvz2q, hxxp[:]//affixio[.]com/emh0c, hxxp[:]//affiliatebash[.]com/myu0f, hxxp[:]//afcmanager[.]net/jxk6m, hxxp[:]//adventsales[.]co[.]uk/iuw8a, hxxp[:]//amikamobile[.]com/ayu4d, hxxp[:]//adztrk[.]com/ixi7r, hxxp[:]//aerospaceavenue[.]com/cnz8g, hxxp[:]//amishwoods[.]com/jwa4v, hxxp[:]//smbeckwithlaw[.]com/1[.]zip, hxxp[:]//kindupdates[.]com
Qakbot	SHA256	b3781927bcf7932c336630f636f47cbdba47e2f5aa94039f87fbb15797455535, 767bfbc1a25997de2d6203b7ec79afe012f1049eda612efb5c51e4da68972b58, 8b08e73ad310f5e7e06c78b453ff8bc00851d0b9f86fa00c64a3dd42ec1632ce, 71c099ed2857f660b8431eb79cdd49300428cbf97c2cb6f98efa6e1cf30d1414,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

Attack Name	TYPE	VALUE
Qakbot	SHA256	9e2864977d0e2bf7e8def198db7d3022188cd764519c2f385797a7ca394c2283, e366c18e2f2389d4e90386f01876174074019a021b6eacfceb187aaa53560078, f3e3d35760f655af5a57029b73c2cc2f42d09de1a694b2eb22366a3e6c49a068, de29782abe28a8fcdc95dd4b031e86653c32d1497e36cdf2f6fbb9cbc48f40e4, b991ef2d58b3246bf5f313e2be71ea961fae1376ec88435173f7fb15a48b6fe2, 60b290310f67adb0ae186b4b938ca466a6b55653b2519261fa425127f5500a1f, 100805c582954d2c13b233229c9f7fe3f4b911ef16dad7aaec5b4616405f7d38, 6787a0800be339b8b6db63fe4b0cbbd68b69c736aecd45c4a85b2f02eb3e57d3, 798e44b2af6329ac38f144d816096b72889009f44c9d74aefa36c11dbdc5522a, 5cfbe018afa45304fb2d7775f635101ee4226ba594bb30cc0e5c017fd1d30da1, f1bbcc5c678d174d858ae089f4494e3ea8bcfc418098d61804a15e437f08aff7, 37d5f69a7b2718386a0c65fbfe65a16c0392428ac4915c41ccd32d7af7c373e8, c14b93f3949b9cc4ba3163a23b5cfeb1d4bea17db91703c3cdcccccbb57d2058, d2e6d3c058dd54b354e701633be148e14d96f40df7e7d3fe8778db69bbce0529, c6482951d520c93684161390507d695b8d6a90d8e1ac14e01626adf1989ab731, 8d8e136551e5ae8b82d3a25147f4291c1f0cf6b82dd3a8df89e6f866247ef83a, b7a00ad06ccceff1cf5fe5c7fed8e0d43b456662721ec668f91681196a1cb3ba, b66b7bfcdc8d6fb55fe600c20302405a22e1e7b60a0bb1e48a0ccf4e5daf8e50, fd1e4ecef5aed84a1e9cf04271111c5041d6c50c850b75959932927cf875293a, dec2d24131b54bda92b59c49acc410da4af20a730b3113c0472479ac168e3a81, e49e5a9c12fa92485943517ecba2721387a7ec8942ef92ba02b4c2e35a9dd84d, 2d7a014145e89956cd0ed6997e7efd12e5570864a12359a11e70a30c724d8b0a,

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on Uni5Xposure platform.

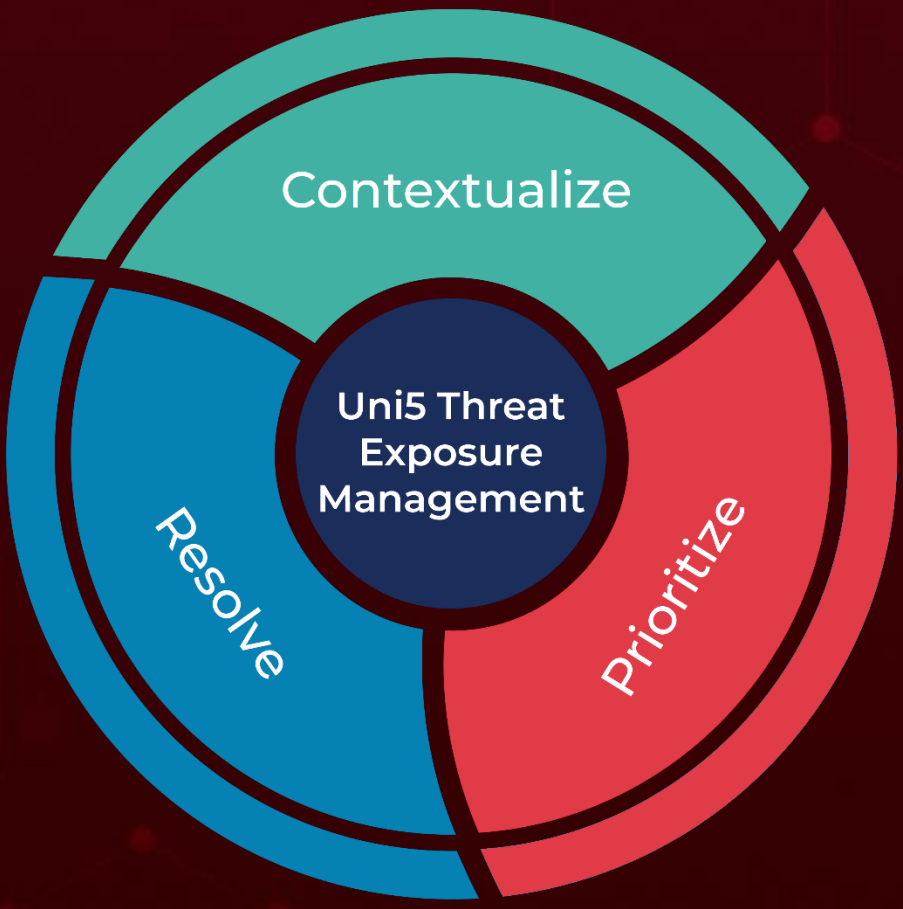
Attack Name	TYPE	VALUE
Qakbot	SHA256	146a74dfa467bb299b8e6719526f224e7643fb4c9da53d8adc1149471184f9d0, 66d36ffbcdd8919b6527110a03fe917c1e47dac123778945305b3baa395631f0, 52321edc0c5a3fcb824d591c730e7783194ec5e1c0f617b40ffe760a876924eb, e4c669aaa5e441eb95dc6baed3e93cc4bd018dd1a03013719283f12cf4322ed8, 06d60d2e4f630514526ac63ab10360a1405899f4dac32888d231f5fcf9abb2d1, a6155313935b355ed814c0df0f423e6a662ea4259dcdcc0ffbcc1e9dad715b6f, 07dc705da27544ca4d232515c665dff2bbbf6b0ab49fd07c602e20d6a512b4af, f93b8b6aedc9c13590c7eb2247c920e376ab33354e9ca4003834ab9f043006f0, d832c8f49706ff93871a111be8fb280caedbad5b368f801dd720c7786f872e86, 1aa8e55ceec841c7ca088da6fc3e018ebc265bfd3ce85cae0339106143800186, af6a9b7e7aefeb903c76417ed2b8399b73657440ad5f8b48a25cfe5e97ff868f, 59559e97962e40a15adb2237c4d01cfead03623aff1725616caeaa5a8d273a35, f407120d5118eb9f93c290461e19bfb20a456a85919c80cc47b4229716131732, f1cd2d2c9e774735e5e80040a279ca86da78bc901ecc6b92096a5a019a6d04e3, b8a97d0b236d84fd7f9406b9d341add7cb5ec4ed0f4267a2ff5c8eac21503dcc, ac256fdb6fc028a9c0cfe930535a23842d3e5c50dc720a4186750ae289245e63

Note: Comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks are available on 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

May 21, 2024 • 12:05 AM

More at www.hivepro.com