Date of Publication
October 23, 2023

Hive Pro®

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities and Actors

16 to 22 OCTOBER 2023

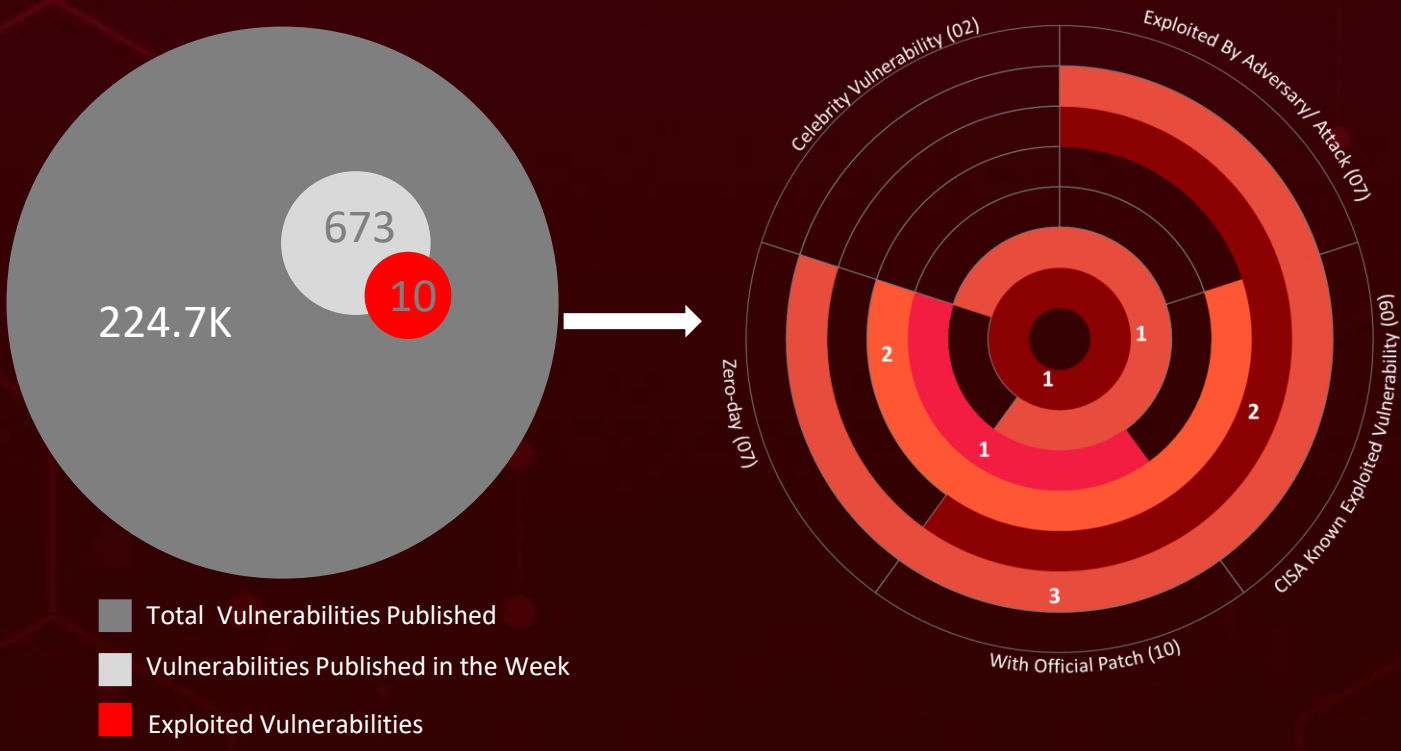
Table Of Contents

Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, a total of **twenty-three** attacks were executed, **ten** vulnerabilities were discovered, and **five** active adversaries were identified, all of which underscore the ever-present danger of cyberattacks.

Furthermore, HiveForce Labs found that among the **seven** zero-day vulnerabilities, **two** were present in **Cisco IOS XE Software**. **One** of them was exploited by **multiple state-sponsored adversaries**. Another vulnerability was discovered in **Citrix NetScaler ADC and NetScaler Gateway**, and it has been actively exploited since August 2023 and two were utilized by the **MATA Backdoor**.

Meanwhile, **OilRig** orchestrated a sophisticated eight-month campaign aimed at the **Middle East government**. The **North Korean threat** actors Lazarus and its subgroup Andariel were actively exploiting the **JetBrains TeamCity** vulnerability, and the **Kimsuky** APT upgraded its arsenal. These attacks are on the rise, posing a significant threat to users worldwide.



High Level Statistics

23
Attacks Executed

10
Vulnerabilities Exploited

5
Adversaries in Action

- PEAPOD
- XorDDoS
- Volgmer
- Scout
- BbyStealer
- SmokeLoader
- Nanocore
- Crimson
- AgentTesla
- Rhadamanthys
- xRAT
- BabyShark
- RevClient
- TinyNuke
- ForestTiger
- FeedLoad
- HazyLoad
- Phobos
- MATA
- PowerExchange
- Clipog
- Munchkin
- BlackCat

- CVE-2023-20198
- CVE-2023-38831
- CVE-2023-4966
- CVE-2023-42793
- CVE-2021-34527
- CVE-2021-1675
- CVE-2017-0213
- CVE-2021-40449
- CVE-2021-26411
- CVE-2023-20273

- Storm-0978
- Lazarus Group
- Kimsuky
- Andariel
- OilRig

Insights

Cyber Deceit at WPL Summit: Storm-0978's ROMCOM 4.0 Infiltration

The Silent Invasion: Lazarus and Andariel's Attack Puts TeamCity Vulnerability in the Spotlight

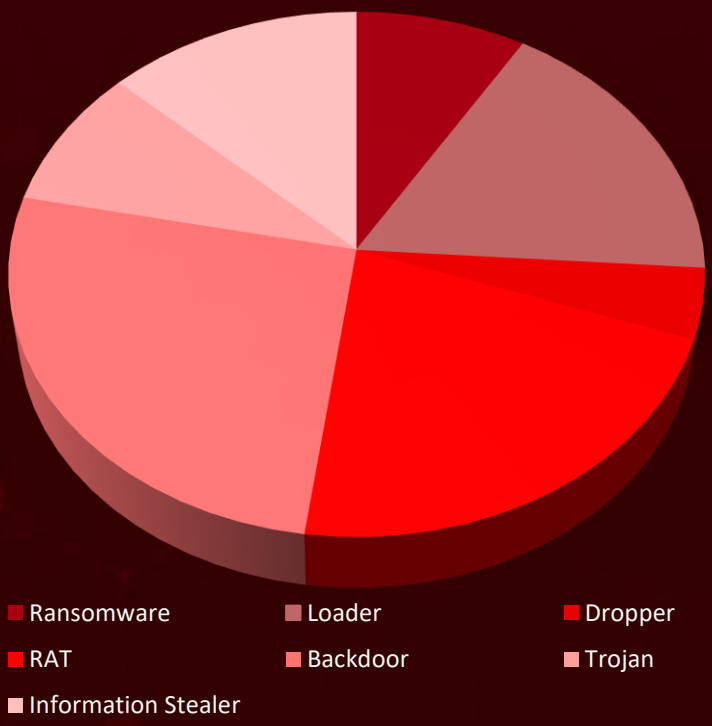
Linux's Silent Assassin : XorDDoS Trojan's 2023 DDoS Surge

MATA Malware: A Highly Evolved Backdoor Framework Targeting Eastern European Industries

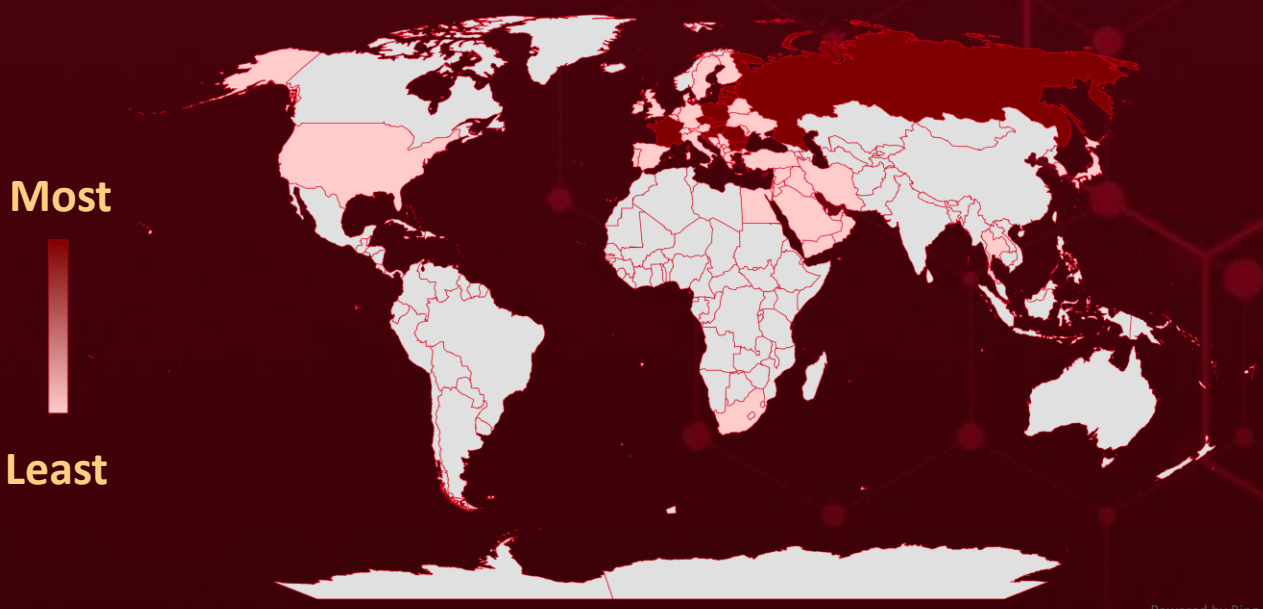
Citrix in Peril: Zero-Day **CVE-2023-4966** Exploit Menaces Citrix NetScaler ADC/Gateway devices

Cisco's Nightmare: 50K+ devices infected with implants, TA capitalizing on 2 zero-day

Threat Distribution

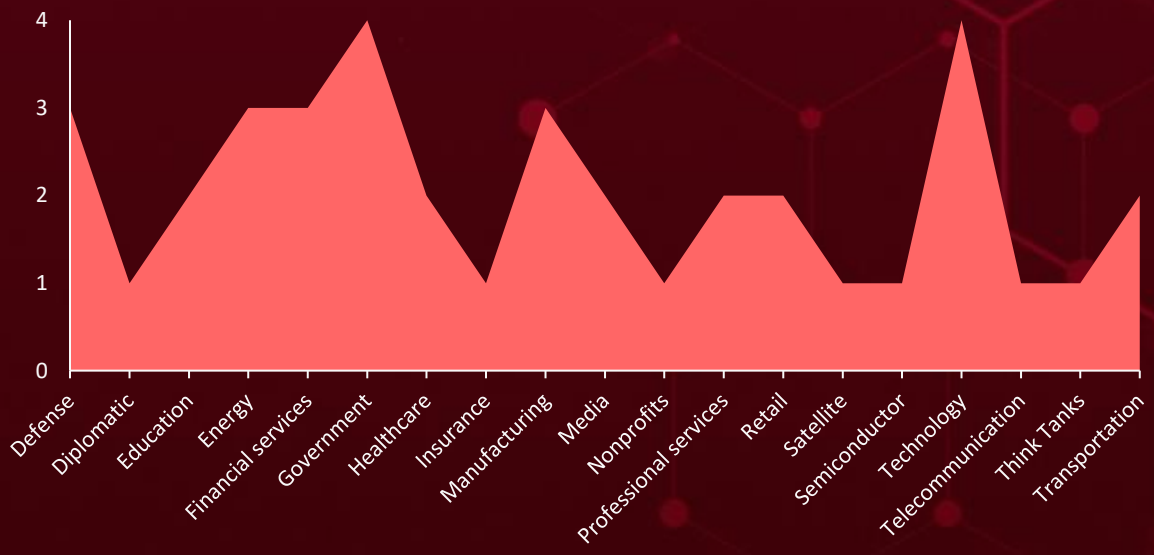


Targeted Countries



Countries	Countries	Countries
Hungary	Germany	Saudi Arabia
Russia	United Kingdom	Austria
Poland	Greece	Egypt
Bulgaria	Bahrain	Lebanon
Slovenia	Albania	South Africa
Croatia	Denmark	Akrotiri and Dhekelia
Latvia	Iran	
Cyprus	Belgium	Spain
Romania	Iraq	Luxembourg
Czech Republic	Sweden	Syria
Slovakia	Ireland	Malta
Estonia	Ukraine	Turkey
France	Israel	Moldova
Lithuania	Yemen	United Arab Emirates
Serbia	Italy	
Thailand	Palestine	Montenegro
Finland	Japan	United States
Qatar	Portugal	Netherlands
Bosnia and Herzegovina	Jordan	North Macedonia
	Belarus	Oman
South Korea	Kuwait	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1105** Ingress Tool Transfer	**T1566** Phishing	**T1021** Remote Services	**T1059.001** PowerShell
T1071 Application Layer Protocol	**T1027** Obfuscated Files or Information	**T1588.006** Vulnerabilities	**T1588** Obtain Capabilities	**T1005** Data from Local System
T1003 OS Credential Dumping	**T1574** Hijack Execution Flow	**T1070** Indicator Removal	**T1140** Deobfuscate/ Decode Files or Information	**T1204** User Execution
T1204.002 Malicious File	**T1098** Account Manipulation	**T1047** Windows Management Instrumentation	**T1136** Create Account	**T1574.002** DLL Side-Loading

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
PEAPOD (aka ROMCOM 4.0)	The latest version of RomCom, known as PEAPOD, has been simplified to include core features, allowing it to execute commands, manage files, collect system data, and even remove itself from compromised systems.	Spear-phishing emails and malvertising	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Extortion of data	-
ASSOCIATED ACTOR			**PATH LINK**
Storm-0978			-
IOC TYPE	**VALUE**		
Domains	budgetnews[.]org, wirelessvezion[.]com, redditanalytics[.]pm, netstaticsinformation[.]com		
SHA256	83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c		
File Name	pcmf-installer-23.0.5.exe		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XorDDoS	The XorDDoS Trojan, a Linux-based malware, encrypts its data using an XOR encryption key. It collects essential information about the compromised device and uses CRC codes for error detection during network communication.	Exploiting vulnerabilities	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Trojan		Denial of Service, Data Theft, and compromised systems	Linux
ASSOCIATED ACTOR			**PATCH LINK**
-			-
IOC TYPE	**VALUE**		
SHA256	b8c4d68755d09e9ad47e0fa14737b3d2d5ad1246de5ef1b3c794b1339d8fe9f8, 265a38c6dee58f912ff82a4e7ce3a32b2a3216bffd8c971a7414432c5f66ef11, 1e823ae1e8d2689f1090b09dc15dc1953fa0d3f703aec682214750b9ef8795f1,		

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
Volgmer (aka FALLCHILL, Manuscrypt)	Volgmer, a DLL-type backdoor, has been discreetly installed to masquerade as a legitimate file. Volgmer exhibits a unique characteristic of employing specific logic to randomly generate strings for the name of the Volgmer DLL file.	Spear phishing and supply chain attacks	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group			-
IOC TYPE	**VALUE**		
Registry Key	HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-5903-ed41-902f-e93a29dafef5"		
MD5	35f9cfe5110471a82e330d904c97466a, 5dd1ccc8fb2a5615bf5656721339efed, 9a5fa5c5f3915b2297a1c379be9979f0, a545f548b09fdf61405f5cc07e4a7fa1, eb9db98914207815d763e2e5cfbe96b9, fe32303e69b201f9934248cc06b32ef8,		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Scout	Scout Downloader, once activated, displays a graphical user interface (GUI), setting it apart from typical malware behaviors. Scout employs a file name-based lookup of the registry value housing encrypted configuration data.	Spear phishing and supply chain attacks	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Downloader		Data Theft and Espionage	-
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group			-
IOC TYPE	**VALUE**		
Registry Key	HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-2790-10f2-dd2a-d92f482d094f”		
MD5	05bb1d8b7e62f4305d97042f07c64679, 0b78347acf76d4bb66212bf9a41b9fb9, 0ed86587124f08325cd8f3d3d2556292, 35943aa640e122fcb127b2bfd6e29816, 394b05394ebb9b239a063a6b5839edb9, 5496adcd712d4378950ba62ad4c2423b		

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
BbyStealer	The BbyStealer malware duplicates itself, placing the copy in the startup folder to ensure persistence. Subsequently, it terminates web browser processes and proceeds to extract valuable information from the compromised system. This is achieved by creating duplicates of the user data folder and appending the ".bby" extension.	Phishing domains	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft and Espionage	Windows
ASSOCIATED ACTOR			**PATCH LINKS**
-			-

IOC TYPE	VALUE
MD5	2cf6efb8104b5d4606fb1698ae97e4f5, 3cf9c1d65d59b63d479ec26e9fd98b57,
SHA1	effb88250fcb89bbab77f46c1022f3c9c0aad37e, eab9cf1e969b5d9a3fda7714c6ae2796aaf44fd0,
SHA256	55a6a784d4acb7e9761a99fb38eb441519cdcd2943bfdf1a1558fe8513690c97, e97b03c98056d7c88bad83b7422767d51ac75fe959e7d1582cc645d6a2bae84b

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
SmokeLoader (aka Dofoil, Sharik, Smoke)	SmokeLoader can be used to drop other malware on infected systems, but operators can choose additional modules that allow for information-stealing capabilities.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINK**
-			https://www.winrar.com/singlenewsview.html

IOC TYPE	VALUE
SHA256	184f4f60f0d0438a975309e33078ec976111425f890d43799f09c0b492962d9c, 2f1e77b4703bbe3131c73b9904653f1175b6f6ec485bcdd1e517173df807d46f, 5f2256cb5470ffc8c81545b7ad9ba361adbe8b7883249412ca2ee38a1acf34aa, 0602c6de331d5133a1213be5ac970898f74d8630a7ff273eda97b1cee73a08bc, c75011e37825e51e7d884caa4c01e43e0b3fc76d31b92624d83f64aebfbab134

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
Nanocore (aka Nancrat, NanoCore)	NanoCore is a modular remote access tool developed in .NET that can be used to spy on victims and steal information.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.html
IOC TYPE	**VALUE**		
SHA256	3326240e9bddfc66fc85528944900d2afa9be59837f8e80537f3dd4cb105ec40, 85ba99319f22cde0abd25e839a7a230a730f1d52e546754873e479be88e65da1, 4eaf86877e9160a7bcb9105039f90acefec1ad130979335ff093344fed31ca22, 8b44d972bbe20975a47391ee41e7a6179a00510c6a023eadfe06fe2bd965e860, fd3b84b15d3079c8dfa2e386de838bf9406841f2eec7454ba642497f3bd524f5		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Crimson (aka SEEDOOR, Scarimson)	Crimson RAT has the ability to exfiltrate files and system info and send it to its C2 server using non-web channels. The RAT is designed to capture the screen and terminate any ongoing processes.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.html
IOC TYPE	**VALUE**		
SHA256	3198fb63145c3a354d7915a4bd1e41cb8d45396f85d179393cf744817f82196a, e38c39e302de158d22e8d0ba9cd6cc9368817bc611418a5777d00b90a9341404, ce556d55e07bf6b57e3e086e57e9c52552ac7f00adf4a7c9f99bbc21a5ac26c2, a833dbdc5c2113da51bf778351834682bc6220461394050e04592cd9096e0aba, 2110af4e9c7a4f7a39948cdd696fcd8b4cdbb7a6a5bf5c5a277b779cc1bf8577		

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
AgentTesla (aka Negasteal)	Agent Tesla is a.NET framework-based spyware Trojan. The malware can collect keystrokes, access the host's clipboard, and search the disk for credentials or other useful data. It can send data back to its command and control over HTTP(S), SMTP, FTP, or Telegram channels.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.html
IOC TYPE	**VALUE**		
SHA256	b2733739ec7e122deeed490926f1e9b50a3ac83ce3d87dd407fc3983cc1b35e4, c6e890fe05afe481cb4d8d4460424276a29566a9d15e145f13413b0d1a158d8d, 4ab7caf841130dd3052e383e4bcf300a79d284bd0f35c777ca25c823c97f5ea5, c34e81fe62af4f81b2bf0d42095b27a0e70db3dc28d0399e1c3477ad9bdf6764, c4ab03eb1096d5643db922730824168efa45ba7f308c3336c47558360fa8b44b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
HazyLoad	The HazyLoad proxy tool facilitates a persistent connection between the compromised server and Andariel's servers. Regardless of the specific techniques used, the attackers ultimately extract credentials from the LSASS memory.	Exploiting Vulnerability	CVE-2023-42793
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information theft, Espionage, and compromised system	TeamCity servers
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group & Andariel			https://www.jetbrains.com/teamcity/download/other.html
IOC TYPE	**VALUE**		
SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee		
File Path	C:\Windows\Temp\temp.exe, C:\Windows\ADFS\bg\inetmgr.exe		
URLs	hxxp://147.78.149[.]201:9090/imgr.ico, hxxp://162.19.71[.]175:7443/bottom.gif		

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

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Rhadamanthys	Rhadamanthys is a stealer that is meant to steal information from affected computers. Rhadamanthys is downloaded alongside the actual software, reducing user suspicion. These sites were promoted using Google advertisements, which took precedence over legitimate Google search results.	Phishing	CVE-2023-38831
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft, compromised systems and Espionage	RARLAB WinRAR
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://www.winrar.com/singlenewsview.html
IOC TYPE	**VALUE**		
SHA256	ebad5799999c845b30f52f65cdf7ca9da64b5406d875770b854eeffcbcc42253, 0a2c9d63381141a3d3ba914626f5e08f027e644dff07009582e7ef85aaf4928a, 2cf0c41523a67a1112db28e85d7694ebf02b0e94b4b3e684e82b299d2d448a75, c77a99aebc91775a48fcbc85c0b062bb0338818860facc160cd005a3ed5801e9, 62600a3d570dd2096f9eb8bb18b7d4b4844e9c603182529dadad8831f8a067a7,		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
xRAT (aka QuasarRAT)	xRAT, now known as QuasarRAT in newer versions, is a remote access tool whose source code is openly available on GitHub. Because of this, anyone may easily clone and compile the project and is actively maintained.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-
IOC TYPE	**VALUE**		
SHA256	b1e9a85c03068ca865cd3b4951c83e43548acf7daf137e59b0ba92b6050170bb, 14d25750cb84c1c8d0fba9797ede0e3589e661ea8aeb5e357aa6c9c69cbb3b73, 69205ea8da1443cee48059eebe27c4046bcb7efac024b2d26b618544cb6d4996, b60a6257b257b668dbe48686e6ec953a4ecc13158702a8cfb37043101da105e8, d2b3682c2a7a847400cb42f338d41b054d5f0ccd63e9338903a6a11c67cfe62d		

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
BabyShark	BabyShark is a malware family that uses Microsoft Visual Basic (VB) scripts. Since the malware is launched from a remote site, it can be supplied via a variety of file types, including PE files and malicious documents. It sends system information to the C2 server and maintains persistent access to the system.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-
IOC TYPE	**VALUE**		
MD5	ad9a3e893abdac7549a7d66ca32142e8, 116a71365b83cc38211ccfc8059b363e, c8d589ac5c872b12e502ec1fc2fee0c7, 0d6717c3fa713c5f5f5cb0539b94b84f		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
RevClient	RevClient is an RDP-related malware that operates by accepting commands from the command-and-control server. It can conduct user account-related tasks or port forwarding, depending on the instructions provided.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
RAT		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-
IOC TYPE	**VALUE**		
MD5	be2f73a637258aa872bdf548daf55336, 02804d632675b2a3711e19ef217a2877		
IPv4:PORT	5.61.59[.]53:2086		

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
TinyNuke (aka NukeBot, Nuclear Bot, MicroBankingTrojan)	TinyNuke can steal credentials with form-grabbing and web-inject capabilities for Firefox, Internet Explorer, and Chrome, and it can also install extra payloads.	Spear-phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Banking Trojan		Espionage and compromised system	-
ASSOCIATED ACTOR			**PATCH LINKS**
Kimsuky			-
IOC TYPE	**VALUE**		
SHA256	db2027cd8687abdce3e6df39420b34494788301b9c5d892c470e975e67c65d09, 08b0b9fff5f719e1ff863c0ff2505122b4ee7e075956199ecc7b59769f719abe, 29e7bed50c7a5738ce2e69b48e94d532133491d9a99b613dc962e270cae61049, a74e7edcc211be78093e8516f8013db6f2f0c7e950cc680c2c50ab8f3f71ec8d, 5ea23633beb89010185047a47f84fa500278ba442f408f3901946ac6c5fb4cee		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
ForestTiger	ForestTiger malware serves as a backdoor, allowing threat actors to execute commands on the infected system. The ForestTiger conducts scheduled tasks on compromised systems as well as credentials and utilizes them to dump credentials via the LSASS memory.	Exploiting Vulnerability	CVE-2023-42793
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Information theft, Espionage, and compromised system	TeamCity servers
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group & Andariel			https://www.jetbrains.com/teamcity/download/other.html
IOC TYPE	**VALUE**		
File Path	C:\ProgramData\Forest64.exe, C:\ProgramData\4800-84DC-063A6A41C5C		
SHA256	e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795, 0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa		
URLs	hxxp://www.bandarpowder[.]com/public/assets/img/user64.png, hxxps://www.bandarpowder[.]com/public/assets/img/user64.png		

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
FeedLoad	FeedLoad's primary function is to install a RAT, providing the threat actors with remote control and access to the affected server. Following a successful compromise.	DLL search order hijacking	CVE-2023-42793
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Loader		Information theft, Espionage, and compromised system	TeamCity servers
ASSOCIATED ACTOR			**PATCH LINKS**
Lazarus Group & Andariel			https://www.jetbrains.com/teamcity/download/other.html

IOC TYPE	VALUE
File Path	C:\ProgramData\Version.dll, C:\ProgramData\readme.md
SHA256	f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486, fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6
URLs	hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feed.zip, hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feedmd.zip

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
Phobos	Phobos actors tend to prioritize targeting servers rather than end-user computers, and it exclusively affects Windows operating systems. Phobos ransomware is known for being a double extortion ransomware, where it first exfiltrates data and then encrypts files using the AES encryption method.	Phishing emails	CVE-2021-34527 CVE-2021-1675 CVE-2017-0213
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Espionage, Data Extortion and compromised system	Microsoft Windows Print Spooler
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213

IOC TYPE	VALUE
SHA256	d0604a3864899ac9bf0a07e47330b62a3e76b61335d6dac2e9b5a796b9fcc164, 9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c fd59543a425d2159dfadba8efd4d40178b609ef123a8bc5cf00fe3afef95623d, 482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52
MD5	aaa058858261d7c0e73fa1b8264a9a3d, 1a75878dea8f5580c25e0b9f1c734949, 25674f5426c59051960f0d00f06f0b77, 9de437c0a1f9e633186f5f631d32af8a
Emails	cadillac[.]407@aol[.]com, OttoZimmerman@protonmail[.]ch, ofizducwe111988@aol[.]com, FobosAmerika@protonmail[.]ch
IPv4	104[.]26[.]5[.]223, 185[.]112[.]82[.]235, 185[.]112[.]82[.]236, 185[.]112[.]82[.]237

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
MATA (aka Dacls)	The MATA malware is a backdoor framework that is written in C++ and the updated version is harder to detect and remove. MATA backdoor allowed the attackers to remotely control the victim's computer, steal data, and deploy additional malware. This multi-faceted attack campaign highlights the MATA cluster's advanced tactics and their ability to adapt and evolve their malware.	Spear-phishing	CVE-2021-40449 CVE-2021-26411
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Compromising financial software servers, Exfiltration of data and Financial Loss	Microsoft Internet Explorer & Windows
ASSOCIATED ACTOR			**PATCH LINKS**
-			https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449 https://potal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26411
IOC TYPE	**VALUE**		
MD5	2bf250d64e72a14f05ee190148291564, 9672437e1dc219ca8a4ee847bed25d0d, 01b3c7b2ff7e5158f80f593c09232e04, 996013c565b1f0ae68418d09d712d72b, 5f619927b586a6f776eb582f661ed55c, 91014e9b43ad489535e62e1b048feb59, 289b0d0b626b0be26ee81ed84fb94ec1		

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
PowerExchange	PowerExchange, a PowerShell-based malware, has the capability to access an Exchange Server using hardcoded credentials and monitor emails sent by the attackers. It utilizes the Exchange Server as a command and control (C&C) center.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Backdoor		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
OilRig			-
IOC TYPE	**VALUE**		
SHA256	d884b3178fc97d1077a13d47aadf63081559817f499163c2dc29f6828ee08cae		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
Clipog	Clipog is an information-stealing malware with the ability to copy clipboard data, capture keystrokes, and record the processes of the entered keystrokes.	Phishing	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Information Stealer		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
OilRig			-
IOC TYPE	**VALUE**		
SHA256	75878356f2e131cefb8aeb07e777fcc110475f8c92417fcade97e207a94ac372		
SHA1	56df507f945d6149a1f0090a19c71254cc08c84e		
MD5	576a1d9e79bf32120d74eabae45f17ab		

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
Munchkin	Munchkin allows threat operators to run BlackCat on remote machines, as well as to deploy it for the purpose of encrypting remote SMB and CIFS network shares. Munchkin runs on a customized version of Alpine Linux and is delivered in the form of an ISO file.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Dropper		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-
IOC TYPE	**VALUE**		
SHA256	1a4082c161eafde7e367e0ea2c98543c06dce667b547881455d1984037a90e7d		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
BlackCat (aka AlphaV, AlphaVM, ALPHV-ng, or Noberus)	BlackCat ransomware drew attention due to its use of the Rust programming language and its Ransomware-as-a-Service (RaaS) business model. BlackCat is extremely customizable and can be tailored to create targeted Executables.	Unknown	-
TYPE		**IMPACT**	**AFFECTED PRODUCTS**
Ransomware		Data Theft, Espionage and Financial Loss	-
ASSOCIATED ACTOR			**PATCH LINKS**
-			-
IOC TYPE	**VALUE**		
SHA256	b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2, e69a13add1245bc1b7b6337e64eee9b53395b9574f2b85d32f891680c7165ff5, aa236a7ae9949fa1bc6111e6613f2a2e05f33b95c28d19c1f0fd5417736ecbe0, 3a7866a23339baf6997fe08d7e7dac97d3f8754af552acee3457c3604abaf4c5, f5f645ae6dfa3f957412eb44a5d251e93b37678862baf16b08dc8e142da6f998		

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-2023-20198		Cisco IOS XE- All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco_systems:cisco_ios_xe:*	-
Cisco IOS XE Web UI Privilege Escalation Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1068: Exploitation for Privilege Escalation; T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z#REC

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-38831		WinRAR: 3.20 - 6.23 beta 1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rarlab:winrar:*:*:*:*:*:*:*:*	SmokeLoader, Nanocore RAT, Crimson RAT, AgentTesla, BOXRAT and Rhadamanthys info stealer
WinRAR Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1059: Command and Scripting Interpreter	https://www.winrar.com/singlenewsview.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-4966	✗	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-8.50, 13.1 before 13.1-49.15 & 13.0 before 13.0-92.19, NetScaler ADC 13.1-FIPS before 13.1-37.164 & 12.1-FIPS before 12.1-55.300, NetScaler ADC 12.1-NDcPP before 12.1-55.300	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:-:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Buffer Overflow Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1574: Hijack Execution Flow; T1499.004: Application or System Exploitation; T1563: Remote Service Session Hijacking; T1548.002: Bypass User Account Control; T1210: Exploitation of Remote Services	https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-42793	✗	TeamCity: 2023.05 - 2023.05.3	Lazarus Group & Andariel
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jetbrains:teamcity:*:*:*:*:*:*:*:*	ForestTiger, FeedLoad, RollSling, HazyLoad
JetBrains TeamCity Authentication Bypass Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-288	T1190: Exploit Public-Facing Application; T1040: Network Sniffing	https://www.jetbrains.com/teamcity/download/other.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-34527	PrintNightmare	Windows: 7 - 10 S, Windows Server: 2008 - 2019 2004	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows_10:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	Phobos Ransomware
Microsoft Windows Print Spooler Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-269	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-1675	PrintNightmare	Windows: 7 - 10 S, Windows Server: 2008 - 2019 2004	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	Phobos Ransomware
Microsoft Windows Print Spooler Remote Code Execution Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-94	T1059: Command and Scripting Interpreter	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2017-0213	✗	Windows: 7 – 10, Windows Server: 2008 - 2016	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Phobos Ransomware
Microsoft Windows Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-264	T1068: Exploitation for Privilege Escalation; T1204: User Execution;	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-40449	✗	Windows: 7 - 11 21H2 Windows Server: 2008 - 2019 2004	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:* cpe:2.3:o:microsoft:windows_server:-:*:*:*:*:*:*:*	MATA Backdoor
Microsoft Windows Win32k Privilege Escalation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1068: Exploitation for Privilege Escalation; T1204: User Execution	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-26411	✗	Microsoft Internet Explorer: 9 - 11	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:edge:-:*:*:*:*:*:*:* cpe:2.3:a:microsoft:internet_explorer:-:*:*:*:*:*:*:*	MATA Backdoor
Microsoft Internet Explorer Memory Corruption Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-416	T1005: Data from Local System; T1499: Endpoint Denial of Service; T1211: Exploitation for Defense Evasion; T1212: Exploitation for Credential Access	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26411

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-20273		Cisco IOS XE- All versions	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:cisco_systems:cisco_ios_xe:*	-
Cisco IOS XE Web UI Arbitrary Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter	https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-dublin-

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Storm-0978 (aka Tropical Scorpius, RomCom, Void Rabisu, DEV-0978)	Russia	Construction, Education, Energy, Financial, Government, Healthcare, High-Tech, Manufacturing, Shipping and Logistics, Transportation.	European Union
	MOTIVE		
	Information theft and espionage, Financial gain		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PEAPOD (aka ROMCOM 4.0)	-
TTPs			
T1566: Phishing;T1566.002: Spearphishing Link;T1608: Stage Capabilities;T1608.001: Upload Malware;T1574: Hijack Execution Flow;T1574.002: DLL Side-Loading;T1587: Develop Capabilities;T1587.002: Code Signing Certificates;T1071: Application Layer Protocol;T1071.001: Web Protocols;T1204: User Execution;T1204.002: Malicious File			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 OilRig (aka Crambus, Helix Kitten, APT 34, Twisted Kitten, Chrysene, Cobalt Gypsy, TA452, IRN2, ATK 40, ITG13, EUROPIUM, Hazel Sandstorm)	Iran	Government	Middle East
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	PowerExchange, Clipog	-
TTPs			
T1566: Phishing;T1059: Command and Scripting Interpreter;T1059.001: PowerShell;T1003: OS Credential Dumping;T1016: System Network Configuration Discovery;T1021.001: Remote Desktop Protocol;T1005: Data from Local System;T1041: Exfiltration Over C2 Channel;T1105: Ingress Tool Transfer;T1056.001: Keylogging;T1113: Screen Capture			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 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)	North Korea	Satellite, Software, Media, Defense, Manufacturing, ICT, And Financial Sectors.	Korea
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-42793	Volgmer, Scout, ForestTiger, FeedLoad, RollSling, and HazyLoad	TeamCity
TTPs			
T1071.001: Web Protocols;T1059: Command and Scripting Interpreter;T1573.001: Symmetric Cryptography;T1098: Account Manipulation;T1566: Phishing;T1195: Supply Chain Compromise;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			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Kimsuky (aka Velvet Chollima, Thallium, Black Banshee, SharpTongue, ITG16, TA406, APT 43, ARCHIPELAGO, Emerald Sleet)	North Korea	Defense, Diplomatic, Education, Media industries, Energy, Government, Healthcare, Manufacturing, Think Tanks	France, Japan, Russia, South Africa, South Korea, United Kingdom, United States, Thailand, Europe
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	-	xRAT, BabyShark, RevClient, TinyNuke	-
TTPs			
T1047: Windows Management Instrumentation;T1055: Process Injection;T1087: Account Discovery;T1140: Deobfuscate/Decode Files or Information;T1016: System Network Configuration Discovery;T1497: Virtualization/Sandbox Evasion;T1566: Phishing;T1566.001: Spearphishing Attachment;T1021: Remote Services;T1056: Input Capture;T1059: Command and Scripting Interpreter;T1059.001: PowerShell;T1059.003: Windows Command Shell;T1059.005: Visual Basic;T1204: User Execution;T1204.002: Malicious File;T1204.001: Malicious Link;T1105: Ingress Tool Transfer;T1104: Multi-Stage Channels;T1041: Exfiltration Over C2 Channel			

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED COUNTRIES
 Andariel (aka Silent Chollima, Stonefly, Plutonium, Onyx Sleet)	North Korea	-	Worldwide
	MOTIVE		
	Information theft and espionage		
	TARGETED CVEs	**ASSOCIATED ATTACKS/RANSOMWARE**	**AFFECTED PRODUCTS**
	CVE-2023-42793	ForestTiger, FeedLoad, RollSling, HazyLoad	TeamCity
TTPs			
T1588: Obtain Capabilities;T1588.006: Vulnerabilities;T1059: Command and Scripting Interpreter;T1059.001: PowerShell;T1574: Hijack Execution Flow;T1574.001: DLL Search Order Hijacking;T1105: Ingress Tool Transfer;T1136: Create Account;T1021: Remote Services;T1021.001: Remote Desktop Protocol;T1003: OS Credential Dumping;T1003.001: LSASS Memory;T1007: System Service Discovery			

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **ten exploited vulnerabilities** and block the indicators related to the threat actors **Storm-0978, Lazarus Group, Kimsuky, Andariel, OilRig,** and malware **PEAPOD, XorDDoS, Volgmer, Scout, BbyStealer, SmokeLoader, Nanocore, Crimson, AgentTesla, Rhadamanthys, xRAT, BabyShark, RevClient, TinyNuke, ForestTiger, FeedLoad, HazyLoad, Phobos, MATA, PowerExchange, Clipog, Munchkin, BlackCat**.

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 **ten exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Storm-0978, Lazarus Group, Kimsuky, Andariel, OilRig,** and malware **PEAPOD, XorDDoS, Volgmer, Scout, BbyStealer, SmokeLoader, Nanocore, Crimson, AgentTesla, Rhadamanthys, xRAT, BabyShark, RevClient, TinyNuke, ForestTiger, FeedLoad, HazyLoad, Phobos, MATA, PowerExchange, Clipog, Munchkin, BlackCat** in Breach and Attack Simulation(BAS).

Threat Advisories

Storm-0978 unleashes PEAPOD to target Women Political Leaders

A New XorDDoS Linux Trojan That Launches Powerful DDoS Attacks

Lazarus Group's Targeted Attacks on Korean Sectors

Unpatched Zero-Day Vulnerability Actively Exploited in Cisco IOS XE

BbyStealer's Tactic for Targeting VPN Users

Multiple State-Sponsored Groups Exploit WinRAR Vulnerability in Phishing Attacks

Kimsuky Unveils New Addition to Its Malware Arsenal

A Longstanding Zero-Day in Citrix Devices Exploited Since August

North Korean Actors Behind Active Exploitation of TeamCity Vulnerability

In-Depth Analysis of Phobos Ransomware

MATA Backdoor Targets Eastern European Industrial Companies

Prolonged Pursuit of OilRig APT Targeting Middle East Government

BlackCat Incorporates 'Munchkin' into Its Arsenal

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
PEAPOD	Domains	budgetnews[.]org, wirelessvezion[.]com, redditanalytics[.]pm, netstaticsinformation[.]com
	URL	hXXps://onedrive[.]live[.]com/?authkey=%21AAdO%2Di5%2DikrnuaA&id=79E2A760F4732317%21106&cid=79E2A760F4732317
	SHA256	83448756a4cafbfd784d36add719cffa65b912e550d3a5fd63d407201c6ff94c
	File Name	pcmf-installer-23.0.5.exe
XorDDoS	SHA256	b8c4d68755d09e9ad47e0fa14737b3d2d5ad1246de5ef1b3c794b1339d8fe9f8, 265a38c6dee58f912ff82a4e7ce3a32b2a3216bffd8c971a7414432c5f66ef11, 1e823ae1e8d2689f1090b09dc15dc1953fa0d3f703aec682214750b9ef8795f1, 989a371948b2c50b1d45dac9b3375cbbf832623b30e41d2e04d13d2bcf76e56b, 20f202d4a42096588c6a498ddb1e92f5b7531cb108fca45498ac7cd9d46b6448, 9c5fc75a453276dcd479601d13593420fc53c80ad6bd911aaeb57d8da693da43, ce0268e14b9095e186d5d4fe0b3d7ced0c1cc5bd9c4823b3dfa89853ba83c94f, aeb29dc28699b899a89c990eab32c7697679f764f9f33de7d2e2dc28ea8300f5

Attack Name	TYPE	VALUE
Volgmer	Registry Key	HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-5903-ed41-902f-e93a29dafef5"
	MD5	35f9cfe5110471a82e330d904c97466a, 5dd1ccc8fb2a5615bf5656721339efed, 9a5fa5c5f3915b2297a1c379be9979f0, a545f548b09fdf61405f5cc07e4a7fa1, eb9db98914207815d763e2e5cfbe96b9, fe32303e69b201f9934248cc06b32ef8, 64965a88e819fb93dbabafc4e3ad7b6c, 6da7d8aec65436e1350f1c0dfc4016b7, e3d03829cbec1a8cca56c6ae730ba9a8, 0171c4a0a53188fe6f9c3dfcc5722be6, 17eacf4b4ae2ca4b07672dcc12e4d66d, 1e2acecce7b5e9045b07d65e9e8afe1f, 226cc1f17c4625837b37b5976acbd68e, 3e6119ebfacd1d88acbd2ca460c70b49, 4753679cef5162000233d69330208420, 5473fa2c5823fbab2b94e8d5c44bc7b4, 570a4253ae80ee8c2b6b23386e273f3a, 5c87373eef090bed525b80aef398ee8a, 693afaedf740492df2a09dfcc08a3dff, 6e21cc6669ada41e48b369b64ec5f37b, 72756e6ebb8274d9352d8d1e7e505906, 8b3ec4b9c7ad20af418e89ca6066a3ad, 947124467bd04b7624d9b31e02b5ee7f, 9a87f19609f28d7f7d76f9759864bd08, b1225fa644eebafba07f0f5e404bd4fd, cf2ff5b59c638a06d8b81159b9a435ea, d52b5d8c20964333f79ff1bce3385d0b, e273803ae6724a714b970dd86ca1acd0, ea5d322648ff108b1c9cbdd1ef4a5959
Scout	Registry Key	HKLM\SYSTEM\CurrentControlSet\Control\WMI\Security / “626e7376-2790-10f2-dd2a-d92f482d094f”
	MD5	05bb1d8b7e62f4305d97042f07c64679, 0b78347acf76d4bb66212bf9a41b9fb9, 0ed86587124f08325cd8f3d3d2556292, 35943aa640e122fcb127b2bfd6e29816, 394b05394ebb9b239a063a6b5839edb9, 5496adcd712d4378950ba62ad4c2423b, 64cac69ab1e9108e0035f9ce38b47db7, 695e5b8dc9615ec603fe2cbb7326a50f, c07e04d388fb394ac190aace51c03c33, c41eb1ea59fab31147c5b107cc1c5a51, cc5a8a15d5808002e62d5daf2d4f31b3, 0b746394c9d23654577f4c0f2a39a543, 225cdc9b452b6d5a3f7616dcc9333d7d, 43f218d3a4b2199468b00a0b43f51c79, 4b1f1db4f169ca6b57015b313d665045,

Attack Name	TYPE	VALUE
Scout	MD5	80d34f9ca10b0e8b49c02139e4615b7a, 855e26d530e69ddc77bb19561fb19d90, 9ec3a4257564658f651896abc608680e, a76624578ed42cceba81c76660977562, b517e7ad07d1182feb4b8f61549ff233, fa868a38ceeb46ee9cf8bd441a67ae27, 1f1a3fe0a31bd0b17bc63967de0ccc29, fa3e49c877a95f37fd25dbd62f9e274c, 202a7eec39951e1c0b1c9d0a2e24a4c4, b457e8e9d92a1b31a4e2197037711783, 8543667917a318001d0e331aeae3fb9b, c16a6178a4910c6f3263a01929f306b9, 1c89fb4aee20020bfd75713264df97cd, 76f02ab112b8e077544d0c0a6e0c428a, 7ba37d662f19bef27c3da2fd2cee0e3a, 7f0e773397808b4328ad11d6948a683f, bf5d815597018fe7f3dfb52d4f7e1f65
BbyStealer	MD5	2cf6efb8104b5d4606fb1698ae97e4f5, 3cf9c1d65d59b63d479ec26e9fd98b57, f1da9126a48197897644a62135c0df46, 352ba438532e9a7a9941875f3824c1cd, 71e0b2a2372398776297cee13c8efa55, bbc3364d8040296b910cf61280cd6ad7, 0d2071be3f76d4b25f19b54d56ff6cb7, 1f8eda53714be873e2280d494c9eacbf, bcd419817ebb4d2ec7e21fbdaf61dd3b, 4ee5a9ffd40f8c0970e53e832bfb9acd
	SHA1	effb88250fcb89bbab77f46c1022f3c9c0aad37e, eab9cf1e969b5d9a3fda7714c6ae2796aaf44fd0, 8fcbf76cccb573d3007032a2148da458f81ffbb1, d72c3e3b1fdaa271629676d7d0215cc396a106c4, c9fd398ed07a2daeeaf526ab094634adbd851934, bdd5dec13109f9cfe992ce325f746c0d3bad6c72, 8a7fab41932aa2dbe8da17697926d69b15dc6c63, aae16faf79be993b27791fb7a6a3663320067876, 61fd361edcfaecb87dbf3711ecb1dd448d6a2ab2, 0ee35e1992b93dbeb7adcd2ccdfcafcb3a1dfdae
	SHA256	55a6a784d4acb7e9761a99fb38eb441519cdcd2943bfdf1a1558fe8513690c97, e97b03c98056d7c88bad83b7422767d51ac75fe959e7d1582cc645d6a2bae84b, 7a27aca062c7b4b180190452afbc6ba4026a13ca8c9503372459a5b214b68ff9, 50ab07bd922546f90d2d62565a3618ba7251459c8aaf007945feb3e7c9f29458, f46017c2c5c98d89a1d35510ed8eeae263a3f8f60092df2bb13db6918d691a32, 833ba04dfe7c93f397117690bf656bdf1cf2768b216f40f525bb0c7527897b9a,

Attack Name	TYPE	VALUE
BbyStealer	SHA256	8b93ed446668642a0d3b8dc45b794d76ce71ebd7552de8437975da2b228df9c7, a26a2a95b6ad1449bf4fe5814533b408cdcc67ad5c234c900b6e0b31300018b0, ae4ea904741b95f044edf0e16ce244dc5a4015050dd9ecf23f2f831435e1ccbc, 058caf0c1750391e8a625ee3310c804e1a0034ce890aef4773ef6cfff3ccCed5
SmokeLoader	SHA256	184f4f60f0d0438a975309e33078ec976111425f890d43799f09c0b492962d9c, 2f1e77b4703bbe3131c73b9904653f1175b6f6ec485bcdd1e517173df807d46f, 5f2256cb5470ffc8c81545b7ad9ba361adbe8b7883249412ca2ee38a1acf34aa, 0602c6de331d5133a1213be5ac970898f74d8630a7ff273eda97b1cee73a08bc, c75011e37825e51e7d884caa4c01e43e0b3fc76d31b92624d83f64aebfbab134, cdbdd07a270d1d907798fabe6c680b677f98f119cd93987de5b6a2db7597d5b4, 2769d9ba9625f530819789fd7750ede220f53e3e5c8612a7994abd124e93966b, 0145682b82083b4c90ab5adc2e31ace000d27c89ebf867f1bab5538ecb0e847c, 30a492bdeae90d129df25f025dcd1e014a371461d35be9239673e36a2d7e1718, aa8fd2c68d244547148a554400661572879c9a9916a6651f27bd703fae2a2cc8
Nanocore	SHA256	3326240e9bddfc66fc85528944900d2afa9be59837f8e80537f3dd4cb105ec40, 85ba99319f22cde0abd25e839a7a230a730f1d52e546754873e479be88e65da1, 4eaf86877e9160a7bcb9105039f90acefec1ad130979335ff093344fed31ca22, 8b44d972bbe20975a47391ee41e7a6179a00510c6a023eadfe06fe2bd965e860, fd3b84b15d3079c8dfa2e386de838bf9406841f2eec7454ba642497f3bd524f5, f72da1620877b354290e9152bd9389fa8e8ea18d292a06e93d82641987a3e678, 9b56deee6d3d191f4cb38a3771bf1d818baed58ab18dd968341f2016a8a5cf50, 73142b5f2ad334785424e3c6f8ca97b3796b9a0d6c8c13c52866f988b6f9650d, 93e080fc54f12414da2606f38855227f8e90bb50345a3bbd082395ee359bfc4d, d77804f10b391fb2dc77a749ab27cbf71e2effc0a149888f4962112f1ad61575

Attack Name	TYPE	VALUE
Crimson	SHA256	3198fb63145c3a354d7915a4bd1e41cb8d45396f85d179393cf744817f82196a, e38c39e302de158d22e8d0ba9cd6cc9368817bc611418a5777d00b90a9341404, ce556d55e07bf6b57e3e086e57e9c52552ac7f00adf4a7c9f99bbc21a5ac26c2, a833dbdc5c2113da51bf778351834682bc6220461394050e04592cd9096e0aba, 2110af4e9c7a4f7a39948cdd696fcd8b4cdbb7a6a5bf5c5a277b779cc1bf8577, e38c39e302de158d22e8d0ba9cd6cc9368817bc611418a5777d00b90a9341404, 2110af4e9c7a4f7a39948cdd696fcd8b4cdbb7a6a5bf5c5a277b779cc1bf8577, a833dbdc5c2113da51bf778351834682bc6220461394050e04592cd9096e0aba, ce556d55e07bf6b57e3e086e57e9c52552ac7f00adf4a7c9f99bbc21a5ac26c2, 7df319a67e11d9b5196f9da64e8413f8448c6f2f1319be4f48dfbb3a045ed645
AgentTesla	SHA256	b2733739ec7e122deeed490926f1e9b50a3ac83ce3d87dd407fc3983cc1b35e4, c6e890fe05afe481cb4d8d4460424276a29566a9d15e145f13413b0d1a158d8d, 4ab7caf841130dd3052e383e4bcf300a79d284bd0f35c777ca25c823c97f5ea5, c34e81fe62af4f81b2bf0d42095b27a0e70db3dc28d0399e1c3477ad9bdf6764, c4ab03eb1096d5643db922730824168efa45ba7f308c3336c47558360fa8b44b, c7728266367cb088e58dd7c5207e86c2c00a36a45e7267732bb5322af0fc82b2, ca399dc8b5bd33a6536454774e350400d0693b4ceef2738d06b8cb73a9e262e6, cabf5777651e17c1d64384cefbf5f7ce2fc7abedff68901c96174dd16612caf1, cbd2e33daf09934c60b689bb54205a2072ae6ae9f748eec21f3508a5cbfb532b, ce2bdcc4087d372411c30e4d003a90c7794accf14004a5200fab1948b0c94659
Rhadamanthys	SHA256	ebad5799999c845b30f52f65cdf7ca9da64b5406d875770b854eeffcbcc42253, 0a2c9d63381141a3d3ba914626f5e08f027e644dff07009582e7ef85aaf4928a, 2cf0c41523a67a1112db28e85d7694ebf02b0e94b4b3e684e82b299d2d448a75,

Attack Name	TYPE	VALUE
Rhadamanthys	SHA256	c77a99aebc91775a48fcbc85c0b062bb0338818860facc160cd005a3ed5801e9, 62600a3d570dd2096f9eb8bb18b7d4b4844e9c603182529dadad8831f8a067a7, 74a434ab27dee2234cc149fa8d34c6d5af5beaa0060ffad7523fde8ec923f983, 8ba72f675acf5bc12805d4fff0bda437ea419d15e4237c916554a7f7df1b0b36, b45536b641815e8e230c3519ee7b9dcb4bf186ed2f4dc73b4be00066550731aa, b76d7c7450892b61891be2cbcfdb364e7b6f3c39a30ea1a3727d57b5683cd237, c46f2fcce113e720cfd68123663b96ea24203591c40caafa70cb518fa9e31fac
xRAT	SHA256	b1e9a85c03068ca865cd3b4951c83e43548acf7daf137e59b0ba92b6050170bb, 14d25750cb84c1c8d0fba9797ede0e3589e661ea8aeb5e357aa6c9c69cbb3b73, 69205ea8da1443cee48059eebe27c4046bcb7efac024b2d26b618544cb6d4996, b60a6257b257b668dbe48686e6ec953a4ecc13158702a8cfb37043101da105e8, d2b3682c2a7a847400cb42f338d41b054d5f0ccd63e9338903a6a11c67cfe62d, 37b810b19d1cd5c18e78d0b2e24a58e79a023ad95350d4fcfef53364ab61cda2, 5aca307743008434d993c21b5291ae0fbbcba0b31f91276010dc7f184fe234d7, 06d532b874eb678faa3b9d14cd9b2a10c401a241e05e2c1aea6947ae31857b79, bfdf4add1fdb2daf0c4a3f5102130461f437347a2221a7370e17e157ba895ede, 3c5d54bafaa699f1aa27dfa437569ab284051ab8947dde26bd9743da9139f011
BabyShark	MD5	ad9a3e893abdac7549a7d66ca32142e8, 116a71365b83cc38211ccfc8059b363e, c8d589ac5c872b12e502ec1fc2fee0c7, 0d6717c3fa713c5f5f5cb0539b94b84f
	URLs	hxxps://onessearth[.]online/up/upload_dotm.php, hxxps://powsecme[.]co/up/upload_dotm.php
RevClient	MD5	be2f73a637258aa872bdf548daf55336, 02804d632675b2a3711e19ef217a2877
	IPv4:PORT	5.61.59[.]53:2086

Attack Name	TYPE	VALUE
TinyNuke	SHA256	db2027cd8687abdce3e6df39420b34494788301b9c5d892c470e975e67c65d09, 08b0b9fff5f719e1ff863c0ff2505122b4ee7e075956199ecc7b59769f719abe, 29e7bed50c7a5738ce2e69b48e94d532133491d9a99b613dc962e270cae61049, a74e7edcc211be78093e8516f8013db6f2f0c7e950cc680c2c50ab8f3f71ec8d, 5ea23633beb89010185047a47f84fa500278ba442f408f3901946ac6c5fb4cee, c59a7541b0c51a0bc912971f1fc729240c5d27398eef580484b956818cde06e2, 47b5e55165a20b834e42bbd13c304ae73107e65bb902798cfa2de61ce75fc1cb, 795d99db27ef00d4e8c53bb1e97aeb6f7bcb0693b1e0fd5eb4d700847011b3b9, fdea22e1aebe4daa925455dd4015518fe681562c350a994720be7abe606cd444, 81b308fe77fc1b3539e6b859f2aadbe6f7944964cea8ed0e63f54505fa5eeabd
ForestTiger	File Path	C:\ProgramData\Forest64.exe, C:\ProgramData\4800-84DC-063A6A41C5C
	SHA256	e06f29dccfe90ae80812c2357171b5c48fba189ae103d28e972067b107e58795, 0be1908566efb9d23a98797884f2827de040e4cedb642b60ed66e208715ed4aa
	URLs	hxxp://www.bandarpowder[.]com/public/assets/img/user64.png, hxxps://www.bandarpowder[.]com/public/assets/img/user64.png, hxxp://www.aeon-petro[.]com/wcms/plugins/addition_contents/user64.png
FeedLoad	File Path	C:\ProgramData\Version.dll, C:\ProgramData\readme.md
	SHA256	f251144f7ad0be0045034a1fc33fb896e8c32874e0b05869ff5783e14c062486, fa7f6ac04ec118dd807c1377599f9d369096c6d8fb1ed24ac7a6ec0e817eaab6
	URLs	hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feed.zip, hxxp://www.mge[.]sn/themes/classic/modules/ps_rssfeed/feedmd.zip

Attack Name	TYPE	VALUE
HazyLoad	File Path	C:\Windows\Temp\temp.exe, C:\Windows\ADFS\bg\inetmgr.exe
	URLs	hxxp://147.78.149[.]201:9090/imgr.ico, hxxp://162.19.71[.]175:7443/bottom.gif
	SHA256	000752074544950ae9020a35ccd77de277f1cd5026b4b9559279dc3b86965eee
Phobos	SHA256	d0604a3864899ac9bf0a07e47330b62a3e76b61335d6dac2e9b5a796b9fcc164, 9215550ce3b164972413a329ab697012e909d543e8ac05d9901095016dd3fc6c, fd59543a425d2159dfadba8efd4d40178b609ef123a8bc5cf00fe3afef95623d, 482754d66d01aa3579f007c2b3c3d0591865eb60ba60b9c28c66fe6f4ac53c52, 2a50a42d3c44e6e3890a53228cb84f6fdb17e38b31422c68b8634a06d36cc324, 78732997a6c9d975b97da85fc511533d44083a9f9da60dae8393274a59b7bfce, 8f60d17bbaefd66fe94d34ea3262a1e94b0f8f0702c437d19d3e292c72f1cedc, 698b2a9cf9ce16f1cb5cff4576e902888cb14db7414b8e6ac4eb728f8c87d209, aedbddbf7494baaaf759a720d9cd17540d3c171b9cc52a02e0ef9a592bd9cd63, f595f91a9966808cc85d11981e66e98043af9aeaaaa3893ef058b9a79c474f17, d4cb20dba15d88c38c35be69fe04538b4f9bb0a12edb51ff23c0171b584edf08, 7e18ff461e3fc159c9b6634c9250600ea4c62da604885697c95d9bac794109b8, b0b7a65f4821d5c9e8c782ee5ccca1c1a6a05236c27a4a136eb370302db2b35e, f709d1f84e4f0a845ebb4a9fb1500aa2a9fd600e97cbea32ffc3e49c1084f467, ab3985e07195465b9a9d8c5a9959e783e2a30f6d6e7fdda3ab153de4d7fc6fe6, f5d99d4548470b4699b215453e9be29e48aa20616d45f704c335bd3bbe3e0a4f, 8e5f99b92349381fd772b1bdb18cce2c6595181fcad0f68de25593276d61620f, d7cb8a2d60e1818d0638a4c38cd6fae475dc83ab7b2bde9827ecc4e4a7ce6ed7, 32c9c069c7fe9ffdd9086b957e45c03993863730cd1eed4815e226dc1b7b436e, 691eaa4c48666b69ca180b9aae1a4035fefb29cef1f0a3cfbc91c020b0b09f40, fe025cd046edabab5a07d058bfcbb884c144511581d5206681064355fb2834bc,

Attack Name	TYPE	VALUE
Phobos	SHA256	9f40b69060a52731107baec84a0c0f8a1bfc1a62e8471b9cd69509aade9cb7f1, 97a4d094f86b757b3fb0e189f2843a7af8d0ec43f9805214e89992528e83b5d7, 795b951e16aa4aa0557c24eedad4897e457864838393fcf66220da85ad8be9d8, 1c1eed8f9b2c44bb7290690521cc5f4e02929d5eeb3cc8fc2bf042cf3b789b8e, 681f180735ec833997bea4eb26c58f9c2e39980cd0a351e0b5cd99c502b33ae8, ebbbc1d293ce864c83cf874c3f8051dd636bd1303f013d3fa0cc97eada3266ac, 667F88E8DCD4A15529ED02BB20DA6AE2E5B195717EB630B20B9732C8573C4E83, 6E9C9B72D1BDB993184C7AA05D961E706A57B3BECF151CA4F883A80A07FDD955, 31dba1a23db70ffb952f0e597acf95d16ab60423018a83d0ccb4f57ce0471793, 56bd92cb5c9800338f01a5c8d6fdda4d602717d7a279ec499d15b8a2df36ec92, 62d67fe5548da330b0074f8fd162833e2675f8973899ae5778c10ef33a3f06af, 58626a9bfb48cd30acd0d95debcaefd188ae794e1e0072c5bde8adae9bccafa6, 94e5a07113b228991a294f9b972d2727695ecd68520f56741ae4ad649d5d529b, 52507e8ce8151bd4fa072949245a50f002ed7973b322968b9690927d061d506f, 703cb9286dd4c0219dcb85fc960d0d662a784b5d9bf3ab78b379ac195fc72595, a91491f45b851a07f91ba5a200967921bf796d38677786de51a4a8fe5ddeafd2, 596f40f23a1284b4e844e4159f07b92d0bdcfdc7ce00180a2b70af4f6843bed4, 25dce15057f3e9f904ea28e039fe0d2945308d7f41ea5386e99af4840c2e6762, c918ba4319356db7b86b34849baba40eb2fdc96b05c5ead8bf7375373ced3bcd, e443920a2306dd8b0182dedadc7c1254bd9c43e576c4876a1970886d06b1cccf, ffbafce6dc32dd8e1dc28d5de250f08f2f32d12b061c3ad5d7ee8125298bfc07, 61f5fcb639e3ad7b671a16e243bf0731e1759dcffde00eb14df56415856edbdb, 02db45a4a6821114adc7aad6eb875ff0db66f0ce1e63387dd02fd499e9a0b745, e30169690074a26afb368ec33e8195a89bd33a48f879913a100a67a960d033bb, 43f846c12c24a078ebe33f71e8ea3b4f75107aeb275e2c3cd9dc61617c9757fc,

Attack Name	TYPE	VALUE
Phobos	SHA256	9ab71ecc8338329b63410ba744c564c014eb5628eeed774302ef99bcc4e44d00, 9d298673b975048819034f7e746f9a2f4e011ae47ba87b48b9375e151326e7b1, 69e479f062e247568bb995ee0eed042d5cf1e37f4f41843981b52c55c10f6c7a, 409ef3b1cf30687fde062ac12af5ceebe5f91dd261f515231d172a4c0687ce72, 97e4ffdb8be8d108e5c81af0d8edda6e3bed9f37e170a05221199742f4de309c, a394878332e9c10950a04d9d735d23dc65e8d102fbfd04b790af7db40b60c5d5, 88d3bdfba7c8f0a49e6a296662e4d5ac13440ab38235602d75dbff3342cd2642, 55135de67a5816c6622ae671c934d5a2bfac1b8f3f09083f64a3ae5997bfbfdf, b4965b7fb169577c87cc40e303a002e497fb4812a1376b73e9ba85813917c733, 3b272c1e76e72bf4acc236b2305dd1c6b12dae729620e6c82f25b74a38b73044, 6575de46c36289308b49fa67bce7cf2c964d5367893391427487900069948bef7, 35920652147ca2dc1150f8605ed50036a8c50d869f328dc9912628a33db40b3a, f6b60839de0ac933f0788bc1e12dee859950010f938a05544ad51c424954b9a6, 7f8f8c82fec8acbb0947a192dd5cbe8b95ffdba4e252b582eae127f1c062399b, 2cadd0ff146e1cdf1270894be4fb1523bfdcc7a31760e0ca5cfd9d8e6b525c21, 4ff1f8a052addbc5a0388dfa7f32cc493d7947c43dc7096baa070bfc4ae0a14e, cfc5fb8385f662b109c6cf866ff70e598964dd37dc3498d5bd45ad2c8f4c7d59, b93fcbafc42d24b88abeb354defad342110bb3928e7e24de4315b905dc74dd86, f0aec57001a184ea82122a59c6e5be48042f75d6f11a40125995ba9531aab718, ccc167391bb396f08e365eec5421786ccf1578ba8d3250debb9321767d33dff2, 4ce04ba4acc3645c66c9da89eb05e7708408e4463b5a901fc15be2479b9bdaf5, 2eff58738b5a7717a3fcdf7a4171c6fa18492bc200eddc26bf608fa35d28466e, F17D535192C421BF7C587C11190AE3BA6CC7EEE392DCCD86AD981D3547868D49, 883162246c3d0a2c10e5c35a2a43ff444a24dbcf9e64dc5cc09009b9cd0ab48e, 0b4c743246478a6a8c9fa3ff8e04f297507c2f0ea5d61a1284fe65387d172f81,

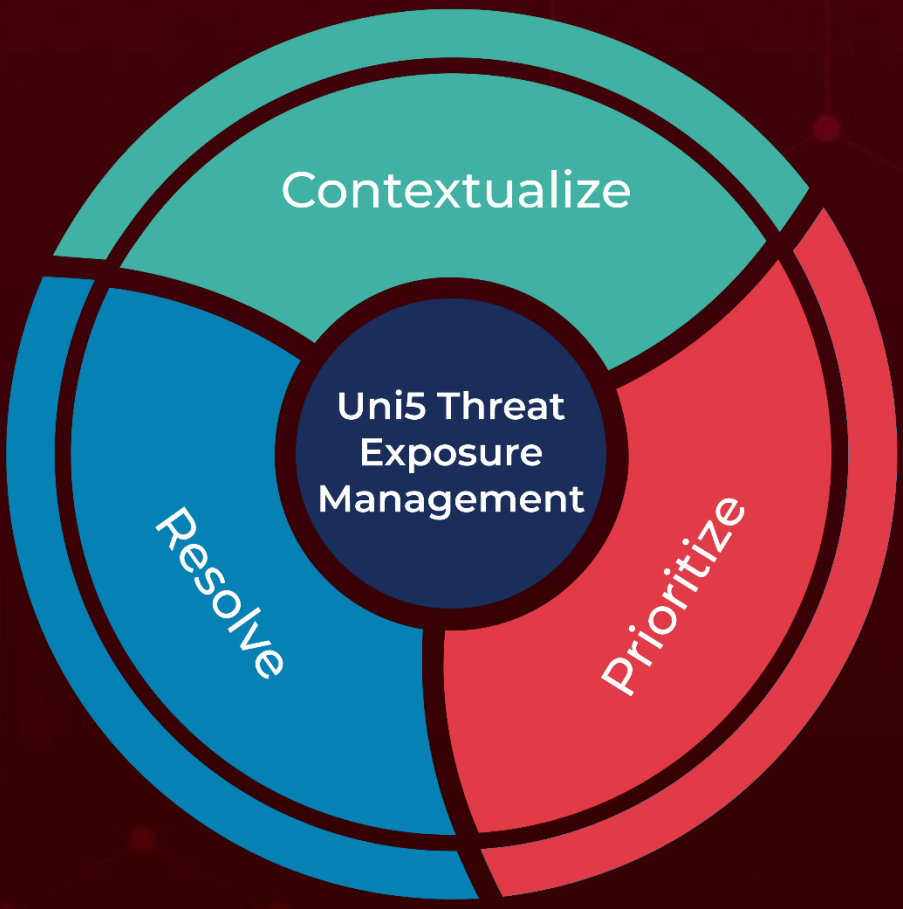
Attack Name	TYPE	VALUE
Phobos	SHA256	527918fbd218787f202dcfb20024375238aca2dc64c1661bdc71f8833240e7f8, f0d6846da6d45180a695201888edc4f9c512fb0d11ed56394aae9daa874ba88c, fab5850b79de211ba1d789f80a4684657b3a79c849d46761decb2de95931162b, 51220927e71a1b8c5cc0ca85c454dc93f3aaae25bb3ec0dc3a9837236687d45f, f97cc59b803e60dcca4461975ecd5e6fc4c64dc31db89e187e5874503af1eb4d, 9f67b6057e5b5dc4b2ec3b370ca3062e0bed91a934b227911af2a3de17164ee5
	MD5	aaa058858261d7c0e73fa1b8264a9a3d, 1a75878dea8f5580c25e0b9f1c734949, 25674f5426c59051960f0d00f06f0b77, 9de437c0a1f9e633186f5f631d32af8a, 792b27b961ee8ae67855b952859053c7, 86e50a7bd09c2a5fc2eac716c29ea6c7, 6ad6c98f75c3133b94026c2fdd06a6f1, d62a9ae1380402cc467cced405ba4aa0, 840d99c89f366505d06259a89273f8b1, 4f25e57d4f754f0cea4f30d9da4156fd, 373a7a21c65d50861b0f7fa81d998165, 90bfa1d3b743c1546a053a206e49cac6, 4942b6f7a7b009cf5bb1ef7d31270b98, 733035ba7c294dd365d2a9601b900b4a, 471cb7869b9c4078717156e809e24001, 719000d0db27119867daf91dd1e8a20b, 2ec9ad510241a00a53f3090af9899250
	Emails	cadillac[.]407@aol[.]com, OttoZimmerman@protonmail[.]ch, ofizducwe111988@aol[.]com, FobosAmerika@protonmail[.]ch, posiccimen1982@aol[.]com, kipp[.]swindlehurst@aol[.]com, lachneyorlachb@aol[.]com, abbott_wearing@aol[.]com, decryptyourfiles@firemail[.]cc, 1decryption1@protonmail[.]com[.]
	IPv4	104[.]26[.]5[.]223, 185[.]112[.]82[.]235, 185[.]112[.]82[.]236, 185[.]112[.]82[.]237
	URLs	https://paste[.]ee/r/1q1gD, https://paste[.]ee/r/OwAyf, https://www[.]patreon[.]com/ccatss, hxxp://178[.]62[.]19[.]66/campo/v/v,

Attack Name	TYPE	VALUE
Phobos	File Paths	%LocalAppData%\horsemoney[.]exe, %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\horsemoney[.]exe, %AllUsersProfile%\Microsoft\Windows\Start Menu\Programs\StartUp\horsemoney[.]exe
	Registry Keys	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney, HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Windows\CurrentVersion\Run\horsemoney
MATA	MD5	2bf250d64e72a14f05ee190148291564, 9672437e1dc219ca8a4ee847bed25d0d, 01b3c7b2ff7e5158f80f593c09232e04, 996013c565b1f0ae68418d09d712d72b, 5f619927b586a6f776eb582f661ed55c, 91014e9b43ad489535e62e1b048feb59, 289b0d0b626b0be26ee81ed84fb94ec1
PowerExchange	SHA256	d884b3178fc97d1077a13d47aadf63081559817f499163c2dc29f6828ee08cae
Clipog	SHA256	75878356f2e131cefb8aeb07e777fcc110475f8c92417fcade97e207a94ac372
	SHA1	56df507f945d6149a1f0090a19c71254cc08c84e
	MD5	576a1d9e79bf32120d74eabae45f17ab
Munchkin	SHA256	1a4082c161eafde7e367e0ea2c98543c06dce667b547881455d1984037a90e7d
BlackCat	SHA256	b4dd6e689b80cfcdd74b0995250d63d76ab789f1315af7fe326122540cddfad2, e69a13add1245bc1b7b6337e64eee9b53395b9574f2b85d32f891680c7165ff5, aa236a7ae9949fa1bc6111e6613f2a2e05f33b95c28d19c1f0fd5417736ecbe0, 3a7866a23339baf6997fe08d7e7dac97d3f8754af552acee3457c3604abaf4c5, f5f645ae6dfa3f957412eb44a5d251e93b37678862baf16b08dc8e142da6f998, 53c62e81c89160f56647bc526e11923842187f557ae42669cc0cfa9f7f1e7203, 841424257c677da6b679f6ce45ee141d05b99deb4a694d0480549b747c1ec6b4, 841424257c677da6b679f6ce45ee141d05b99deb4a694d0480549b747c1ec6b4, d7657ff830673017fb420bc90249c4f1ecbaa778e032a3b203b10d8866741bd4, 3a7866a23339baf6997fe08d7e7dac97d3f8754af552acee3457c3604abaf4c5

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

October 23, 2023 . 7:30 AM

More at www.hivepro.com