Date of Publication
April 24, 2023

Hive Pro

Hiveforce Labs

WEEKLY

# THREAT DIGEST

## Attacks, Vulnerabilities and Actors

17 to 23 APRIL 2023

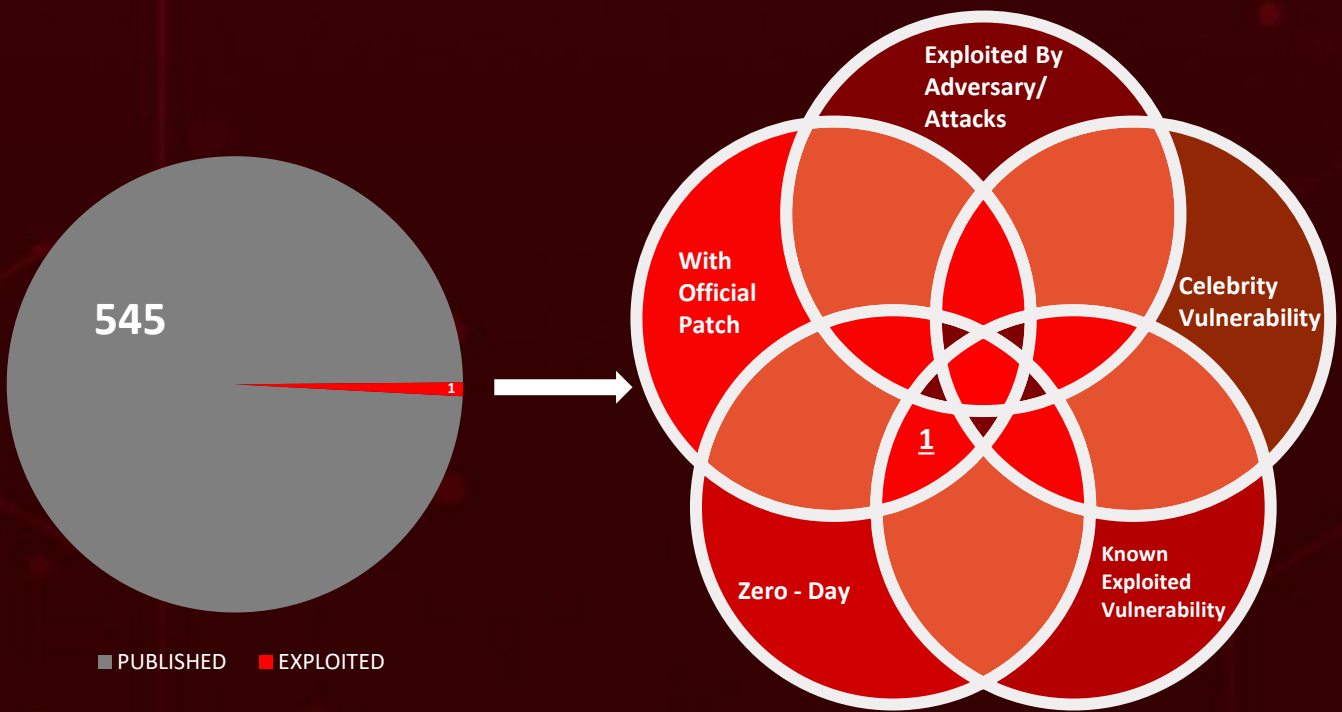
# Table Of Contents

# Summary

HiveForce Labs recently made several significant discoveries related to cybersecurity threats. Over the past week, they identified a total of **ten** attacks that were executed. Additionally, HiveForce Labs identified **four** different adversaries that were actively carrying out these attacks.

Furthermore, HiveForce Labs identified **Zero-Day** in Google Chrome Fixed with Emergency Update. The threat actors **FIN7 and Wizard Spider** unite to spread Domino Family malware and three other malicious programs

Apart from these threats, there was also an increase in ransomware attacks over the past week. These attacks included **Kadavro Vector Ransomware** and **LockBit Ransomware**. All these attacks were observed to be on the rise, posing a significant threat to users all over the world.



# High Level Statistics

**10**
Attacks Executed

**1**
Vulnerabilities Exploited

**4**
Adversaries in Action

- Kadavro Vector Ransomware
- Crimson RAT
- Zaraza bot
- Dave Loader
- Domino Backdoor
- NewWorldOrder Loader
- Carbanak Backdoor
- Project Nemesis infostealer
- LockBit Ransomware
- QBot

- CVE-2023-2033

- APT 36
- FIN7
- Wizard Spider
- LockBit Gang

# Insights

**APT36** targets Indian educational institutions with Crimson RAT

The First **Chrome zero-day** of 2023 squashed by an emergency Google update

**38** web browsers compromised by new Zaraza Bot malware

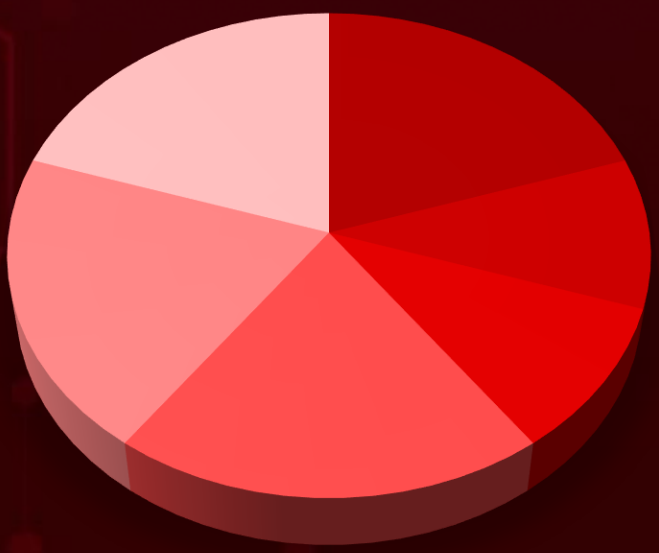
**Double Trouble:** FIN7 and Wizard Spider join forces to spread Domino malware

**Kadavro Vector Ransomware** strikes again, demanding payment in Monero

**QBot** banking Trojan strikes again in a new wave of attacks

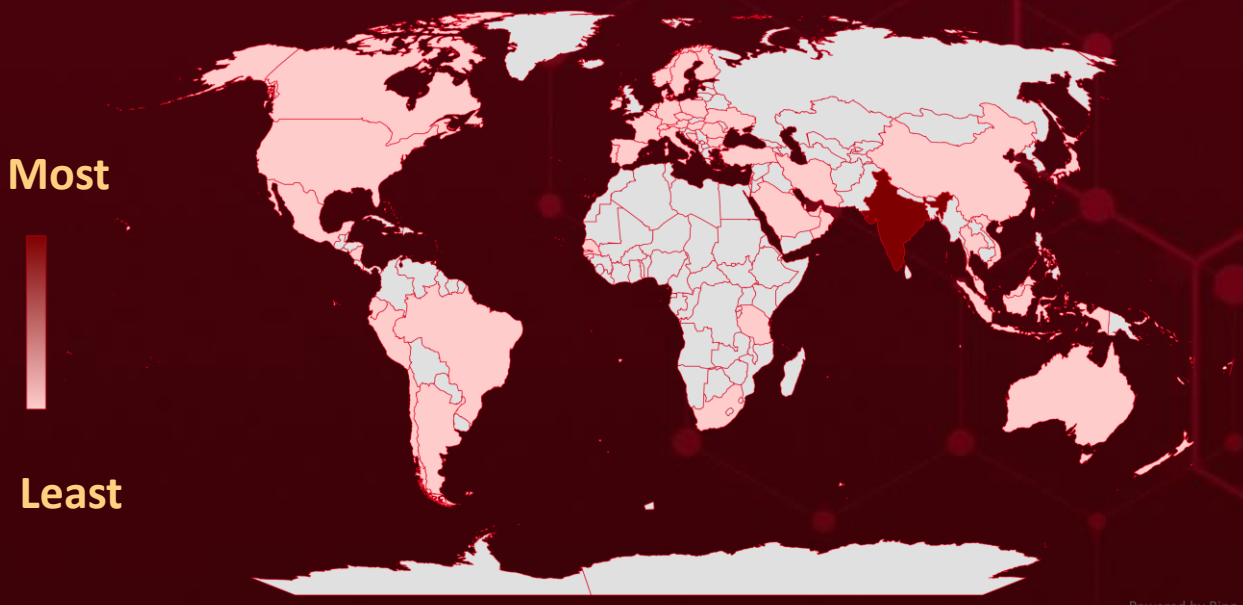
**LockBit strikes!** MacOS under attack

## Threat Distribution



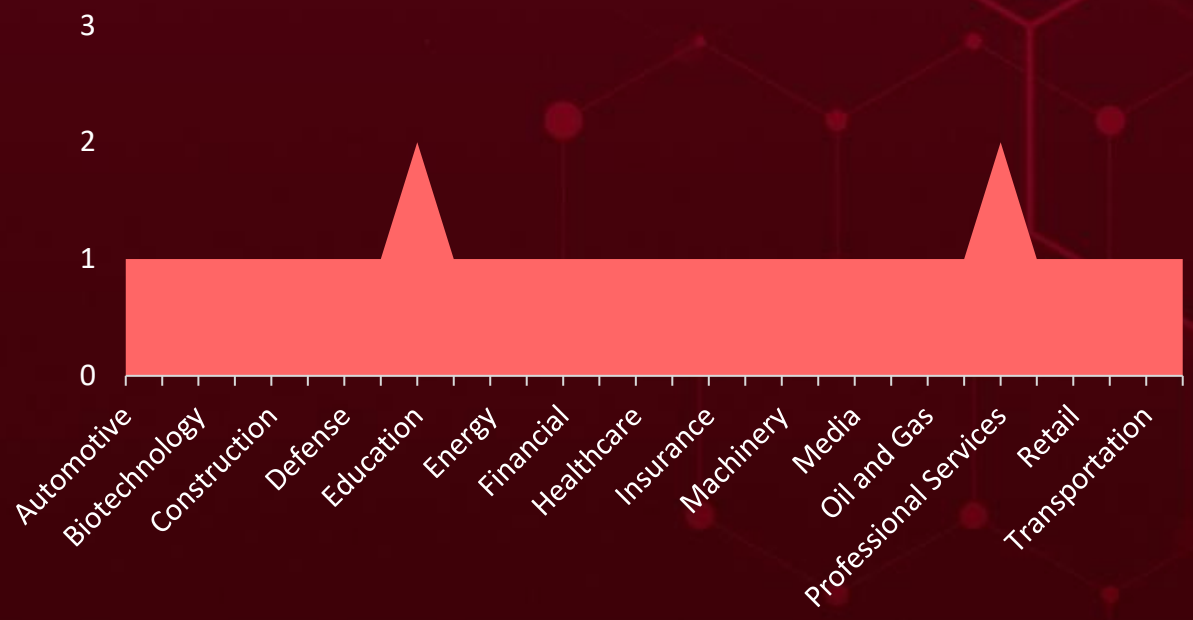
Backdoor Botnet Infostealer Loader Ransomware Trojan

# Targeted Countries




| | Countries | | Countries | | Countries |
|---|---|---|---|---|---|
| | India | | Singapore | | Saudi Arabia |
| | Mauritius | | China | | Senegal |
| | Spain | | Switzerland | | Indonesia |
| | Poland | | Cyprus | | South Africa |
| | Austria | | Turkey | | Iran |
| | United Kingdom | | Czech Republic | | Sweden |
| | Bahrain | | United States | | Ireland |
| | Nicaragua | | Denmark | | Taiwan |
| | Belgium | | Malaysia | | Isle of Man |
| | Australia | | Ecuador | | Thailand |
| | Bosnia and Herzegovina | | Mexico | | Italy |
| | Tanzania | | Finland | | Ukraine |
| | Brazil | | New Zealand | | Japan |
| | Argentina | | France | | United Arab Emirates |
| | Bulgaria | | Norway | | Vietnam |
| | Netherlands | | Germany | | Kuwait |
| | Canada | | Peru | | Lebanon |
| | Oman | | Hong Kong | | |
| | Cayman Islands | | Portugal | | |
| | Puerto Rico | | Hungary | | |
| | Chile | | Qatar | | |
| | | | Romania | | |

# Targeted Industries




# TOP MITRE ATT&CK TTPS

| | | | | |
|---|---|---|---|---|
| **T1027** Obfuscated Files or Information | **T1059** Command and Scripting Interpreter | **T1005** Data from Local System | **T1140** Deobfuscate/ Decode Files or Information | **T1486** Data Encrypted for Impact |
| **T1036** Masquerading | **T1566** Phishing | **T1562** Impair Defenses | **T1497** Virtualization/ Sandbox Evasion | **T1047** Windows Management Instrumentation |
| **T1566.001** Spearphishing Attachment | **T1547** Boot or Logon Autostart Execution | **T1584.005** Botnet | **T1562.001** Disable or Modify Tools | **T1056** Input Capture |
| **T1071** Application Layer Protocol | **T1584** Compromise Infrastructure | **T1102** Web Service | **T1113** Screen Capture | **T1204** User Execution |

# Attacks Executed

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| Kadavro Vector Ransomware | Kadavro Vector is a specific variation of NoCry ransomware. The attackers demand payment in Monero (XMR) cryptocurrency in exchange for the decryption of the files. | Fake Tor Browser Installers | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Ransomware | | Financial loss, unauthorized access, and exfiltration of stolen data | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | 8dc6ff90357e8e2d598bebe3240cefabe22054036ec2e2e91377c7125f8f8b89<br>39308dee3ad1f5ce7ccc3d52b3783db204d12694d6c00ec7ec301ecb73e7c8b6<br>b30ef4dbcc89cd4bf0da3e7787f43e42023ddc2b5f0bb4f24937538e10e17533<br>b7ca2dde7789da13d1b8729cc2ef3d5dc596cbd710a06c17ff6eb4ef2d9d1182 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| Crimson RAT | APT36 is targeting educational institutions and students in the Indian subcontinent by distributing malicious documents disguised as education-themed content to stage the Crimson RAT malware using tactics like OLE embedding. | Phishing emails | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| RAT | | Data Theft, unauthorized access, and infrastructure damage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| APT 36 | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA1 | 516db7998e3bf46858352697c1f103ef456f2e8e<br>842f55579db786e46b20f7a7053861170e1c0c5e<br>87e0ea08713a746d53bef7fb04632bfcd6717fa9 | | |
| Domains | richa-sharma.ddns[.]net<br>cloud-drive[.]store | | |

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 |
|---|---|---|---|
| Zaraza bot | A new credential-stealing malware named Zaraza bot uses Telegram as its command and control, targeting 38 web browsers | Unknown | - |
| TYPE | | IMPACT | AFFECTED PRODUCTS |
| Botnet | | exfiltrating sensitive data for potential identity theft and financial fraud. | - |
| ASSOCIATED ACTOR | | | PATCH LINK |
| - | | | - |
| IOC TYPE | VALUE | | |
| MD5 | 41D5FDA21CF991734793DF190FF078BA | | |
| SHA1 | b50a8e2a7998e17286d2e18d1cf3f7e4e84482c6 | | |
| SHA256 | 2cb42e07dbdfb0227213c50af87b2594ce96889fe623dbd73d228e46572f | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| Dave Loader | Dave Loader is developed by members of the Wizard Spider group. Dave Loader has been utilized this year to load IcedID and Emotet serve as initial access vectors for ransomware attacks. | Phishing or Malvertising | - |
| TYPE | | IMPACT | AFFECTED PRODUCTS |
| Loader | | Gain unauthorized access to a system or network | - |
| ASSOCIATED ACTOR | | | PATCH LINK |
| FIN7 & Wizard Spider | | | - |
| IOC TYPE | VALUE | | |
| SHA256 | de9b3c01991e357a349083f0db6af3e782f15e981e2bf0a16ba618252585923a<br>b14ab379ff43c7382c1aa881b2be39275c1594954746ef58f6a9a3535e8dc1a8<br>dbdfc3ca5afa186c1a9a9c03129773f7bc17fb7988fe0ca40fc3c5bedb201978<br>ce99b4c0d75811ce70610d39b1007f99560e6dea887a451e08916a4f8cf33678 | | |

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 |
|---|---|---|---|
| Domino Backdoor | The Domino Backdoor obtains fundamental system information, which it then transmits to the C2, and receives an AES-encrypted payload in return. | Dave Loader | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Backdoor | | Credential theft and exfiltration of stolen data | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| FIN7 & Wizard Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | de9b3c01991e357a349083f0db6af3e782f15e981e2bf0a16ba618252585923a<br>b14ab379ff43c7382c1aa881b2be39275c1594954746ef58f6a9a3535e8dc1a8<br>dbdfc3ca5afa186c1a9a9c03129773f7bc17fb7988fe0ca40fc3c5bedb201978<br>ce99b4c0d75811ce70610d39b1007f99560e6dea887a451e08916a4f8cf33678<br>e5af0b9f4650dc0193c9884507e6202b04bb87ac5ed261be3f4ecfa3b6911af8 | | |
| IPV4 | 88.119.175[.]124<br>94.158.247[.]72 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| NewWorldOrder Loader | The NewWorldOrder loader, typically used in FIN7's Carbanak attacks was recently employed to distribute the Domino malware. | Unknown | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Loader | | Data loss, unauthorized access, and infrastructure damage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| FIN7 & Wizard Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | f1817665ea2831f775e23cbda27cbeb06d03e6c39bbfad920b50f40712dd37cb<br>51e0512a54640be8e3477363c8d72d893c6edd20399bddf71e95eec3ddfdb42e<br>f4ebd59fb578a0184abf6870fc652210d63e078a35dace0a48c5f273e417c13d<br>92651f9418625e5281b84cccb817e94e6294b36c949b00fcd4046770b87f10e4 | | |

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 |
|---|---|---|---|
| Carbanak Backdoor | The Carbanak Backdoor was loaded using NewWorldOrder Loader samples with the same filename ThunderboltService.exe. FIN7 has been using Carbanak since late 2015. | NewWorldOrder Loader | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Backdoor | | Data loss, unauthorized access, and infrastructure damages | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| FIN7 & Wizard Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA256 | f1817665ea2831f775e23cbda27cbeb06d03e6c39bbfad920b50f40712dd37cb<br>51e0512a54640be8e3477363c8d72d893c6edd20399bddf71e95eec3ddfdb42e | | |
| IPV4 | 178.23.190[.]73 | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| Project Nemesis infostealer | The Domino Loader includes an encrypted payload in its resources, which it decrypts using AES. The decrypted payload is a .NET infostealer identified as "Nemesis Project," which is one of Domino's final payloads. | Domino Loader | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Infostealer | | Data loss, unauthorized access, and infrastructure damage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| FIN7 & Wizard Spider | | | - |
| **IOC TYPE** | **VALUE** | | |
| Domain | es-megadom[.]com | | |
| IPV4 | 45.67.34[.]236 | | |

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 |
|---|---|---|---|
| LockBit Ransomware | LockBit ransomware, known as the oldest ransomware affiliate program, has been discovered on VirusTotal compiled for Apple's macOS arm64 architecture, raising concerns about the ransomware threat on Mac devices. | Ransomware affiliate program | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Ransomware | | Data loss, unauthorized access, and Financial Fraud | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| LockBit Gang | | | - |
| **IOC TYPE** | **VALUE** | | |
| SHA1 | 2d15286d25f0e0938823dcd742bc928e78199b3d<br>864f56b25a34e9532a1175d469715d2f61c56f7f<br>Ef958f3cf201f9323ceae9663d86464021f8e10d | | |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVEs |
|---|---|---|---|
| QBot (also known as QakBot, QuackBot, and Pinkslipbot) | The QBot malware is capable of intercepting traffic and giving operators remote access to the infected system. The Trojan can also download additional malware, such as CobaltStrike or ransomware and turn the victim's computer into a proxy server to facilitate the redirection of traffic. | Malicious PDF attachments in emails | - |
| **TYPE** | | **IMPACT** | **AFFECTED PRODUCTS** |
| Trojan | | Credential theft, data loss, unauthorized access, and infrastructure damage | - |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |
| **IOC TYPE** | **VALUE** | | |
| MD5 | 1FBFE5C1CD26C536FC87C46B46DB754D<br>FD57B3C5D73A4ECD03DF67BA2E48F661<br>28C25753F1ECD5C47D316394C7FCEDE2 | | |
| Domains | cica.com[.]co/stai/stai.php<br>abhishekmeena[.]in/ducs/ducs.php | | |

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-2023-2033 |  | Google Chrome: All versions (before 112.0.5615.121) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:google:google_chrome:-:*:*:*:*:*:*:* | - |
| Google Chrome Type Confusion Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH DETAILS |
| | CWE-843 | T1203:Exploitation for Client Execution; T1068:Exploitation for Privilege Escalation; T1190:Exploit Public-Facing Application; T1588:Obtain Capabilities; T1588.006:Vulnerabilities; T1588.005:Exploits | Upgrade the chromium package to version 112.0.5615.121. https://www.google.com/intl/en/chrome/?standalone=1 |

# Adversaries in Action

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED COUNTRIES |
|---|---|---|---|
|  | Pakistan | Education | India |
| | **MOTIVE** | | |
| | Information theft and espionage | | |
| APT 36(Transparent Tribe, ProjectM, Mythic Leopard, Copper Fieldstone, Earth Karkaddan, STEPPY-KAVACH) | **TARGETED CVEs** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCTS** |
| | - | Crimson RAT | - |
| **TTPs** | | | |
| T1566:Phishing; T1559:Inter-Process Communication; T1547:Boot or Logon Autostart Execution; T1113:Screen Capture; T1102:Web Service; T1127:Trusted Developer Utilities Proxy Execution; T1531:Account Access Removal; T1140:Deobfuscate/Decode Files or Information; T1027:Obfuscated Files or Information | | | |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED COUNTRIES |
|---|---|---|---|
|  | Russia | - | Worldwide |
| | **MOTIVE** | | |
| | Financial crime | | |
| FIN7(aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1) | **TARGETED CVEs** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCTS** |
| | - | Dave Loader, Domino Backdoor, NewWorldOrder Loader, Carbanak Backdoor, Project Nemesis infostealer | - |
| **TTPs** | | | |
| T1047:Windows Management Instrumentation; T1059:Command and Scripting Interpreter; T1129:Shared Modules; T1036:Masquerading; T1497:Virtualization/Sandbox Evasion; T1562:Impair Defenses; T1562.001:Disable or Modify Tools; T1027:Obfuscated Files or Information; T1497.002:User Activity Based Checks; T1564:Hide Artifacts; T1564.003:Hidden Window; T1003:OS Credential Dumping; T1056:Input Capture; T1056.001:Keylogging; T1010:Application Window Discovery; T1057:Process Discovery; T1518:Software Discovery; T1115:Clipboard Data; T1005:Data from Local System; T1071:Application Layer Protocol; T1573:Encrypted Channel; T1518.001:Security Software Discovery | | | |

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED COUNTRIES</th></tr>
<tr><td rowspan="3">  <br><br>Wizard Spider( aka ITG23, Grim Spider, TEMP.MixMaster, Gold Blackburn, Gold Ulrick)</td><td>Russia</td><td rowspan="2">-</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial crime, Financial gain</td></tr>
<tr><td>TARGETED CVEs</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCTS</td></tr>
<tr><td>-</td><td>Dave Loader, Domino Backdoor, NewWorldOrder Loader, Carbanak Backdoor, Project Nemesis infostealer</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">T1047:Windows Management Instrumentation; T1059:Command and Scripting Interpreter; T1129:Shared Modules; T1036:Masquerading; T1497:Virtualization/Sandbox Evasion; T1562:Impair Defenses; T1562.001:Disable or Modify Tools; T1027:Obfuscated Files or Information; T1497.002:User Activity Based Checks; T1564:Hide Artifacts; T1564.003:Hidden Window; T1003:OS Credential Dumping; T1056:Input Capture; T1056.001:Keylogging; T1010:Application Window Discovery; T1057:Process Discovery; T1518:Software Discovery; T1115:Clipboard Data; T1005:Data from Local System; T1071:Application Layer Protocol; T1573:Encrypted Channel; T1518.001:Security Software Discovery</td></tr>
</table>

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED COUNTRIES |
|---|---|---|---|
|  LockBit Gang | Unknown | Automotive, Aviation, Biotechnology, Chemicals, Construction & Engineering, Consumer, Defense, Distributors, Education, Electrical, Energy, Family Services, Financial, Food Products, Healthcare, Hotels, Insurance, IT, Machinery, Marine, Media, Metals & Mining, Oil and Gas, Pharmaceuticals, Professional Services, Real Estate, Retail, Telecommunication, Transportation, Utilities | Argentina, Australia, Austria, Bahrain, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Cayman Islands, Chile, China, Cyprus, Czech Republic, Denmark, Ecuador, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Ireland, Isle of Man, Italy, Japan, Kuwait, Lebanon, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Nicaragua, Norway, Oman, Peru, Poland, Portugal, Puerto Rico, Qatar, Romania, Saudi Arabia, Senegal, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Tanzania, Thailand, Turkey, United Arab Emirates, United Kingdom, United States, Vietnam, Ukraine |
| | **MOTIVE** | | |
| | Financial gain | | |
| | **TARGETED CVEs** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCTS** |
| | - | LockBit Ransomware | - |
| **TTPs** | | | |
| T1486:Data Encrypted for Impact; T1059:Command and Scripting Interpreter; T1195:Supply Chain Compromise; T1553:Subvert Trust Controls; T1553.002:Code Signing; T1566:Phishing; T1566.001:Spearphishing Attachment; T1219:Remote Access Software:T1560:Archive Collected Data; T1027:Obfuscated Files or Information; T1204:User Execution | | | |

# Recommendations

**Security Teams**

This digest can be utilized as a drive to force security teams to prioritize the **one exploited vulnerability** and block the indicators related to the threat actor **APT 36, FIN7, Wizard Spider, LockBit Gang** and malware **Kadavro Vector Ransomware, Crimson RAT, Zaraza bot, Dave Loader, Domino Backdoor, NewWorldOrder Loader, Carbanak Backdoor, Project Nemesis infostealer, LockBit Ransomware, and Qbot.**

**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 **1 exploited vulnerability.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **APT 36, FIN7, Wizard Spider, LockBit Gang** and malware **Kadavro Vector Ransomware, Crimson RAT, Zaraza bot, Dave Loader, Domino Backdoor, NewWorldOrder Loader, Carbanak Backdoor, Project Nemesis infostealer, LockBit Ransomware, and Qbot** in Breach and Attack Simulation(BAS).

# Threat Advisories

Google Chrome Emergency Update Fixes Zero-Day Exploit in the Wild

Kadavro Vector Ransomware spread as a fake Tor browser installer

APT36 targets Indian educational institutions with Crimson RAT

New Zaraza Bot Malware Steals Login Credentials from 38 Web Browsers via Telegram

FIN7 & Wizard Spider team up to disseminate Domino malware

LockBit Ransomware Targets MacOS

New Wave of QBot Attacks Detected via Malicious PDF Attachments

# 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 |
|---|---|---|
| Kadavro Vector Ransomware | SHA256 | 8dc6ff90357e8e2d598bebe3240cefabe22054036ec2e2e91377c7125f8f8b89,39308dee3ad1f5ce7ccc3d52b3783db204d12694d6c00ec7ec301ecb73e7c8b6,b30ef4dbcc89cd4bf0da3e7787f43e42023ddc2b5f0bb4f24937538e10e17533,b7ca2dde7789da13d1b8729cc2ef3d5dc596cbd710a06c17ff6eb4ef2d9d1182,124c17b099d8c09db4bd82b5ef3d41cea61727a480abfd56a943208d858ea8cf,e6e62b3fd2be817c41537b9e3244a40b052e78e826b87c77d1bfdfa1644be199,af19fd4147c2253070e345cfcef86b1236c759911ff6b1ef90955d2e86cb8aa4,8ea5398c46a9a53f15d94a6c627ac591aa13bd2f2ac2cd35c9022c8e4dfa43fe,7694bfd321345364659539de8b4664e5d0cba8bc137b007089c63ec12e32f4d9,a076adcf9a2c8298549c22e5059cc5cd90ddc65abadaec417c3dcc74d9ce484b,2ed272aaa05d80a8504772192d5fc99035e5634e8fc306d0a3e09593c466e969 |
| | Pastebin Address | 124c17b099d8c09db4bd82b5ef3d41cea61727a480abfd56a943208d858ea8cf,e6e62b3fd2be817c41537b9e3244a40b052e78e826b87c77d1bfdfa1644be199,af19fd4147c2253070e345cfcef86b1236c759911ff6b1ef90955d2e86cb8aa4,8ea5398c46a9a53f15d94a6c627ac591aa13bd2f2ac2cd35c9022c8e4dfa43fe,7694bfd321345364659539de8b4664e5d0cba8bc137b007089c63ec12e32f4d9,a076adcf9a2c8298549c22e5059cc5cd90ddc65abadaec417c3dcc74d9ce484b,2ed272aaa05d80a8504772192d5fc99035e5634e8fc306d0a3e09593c466e969 |

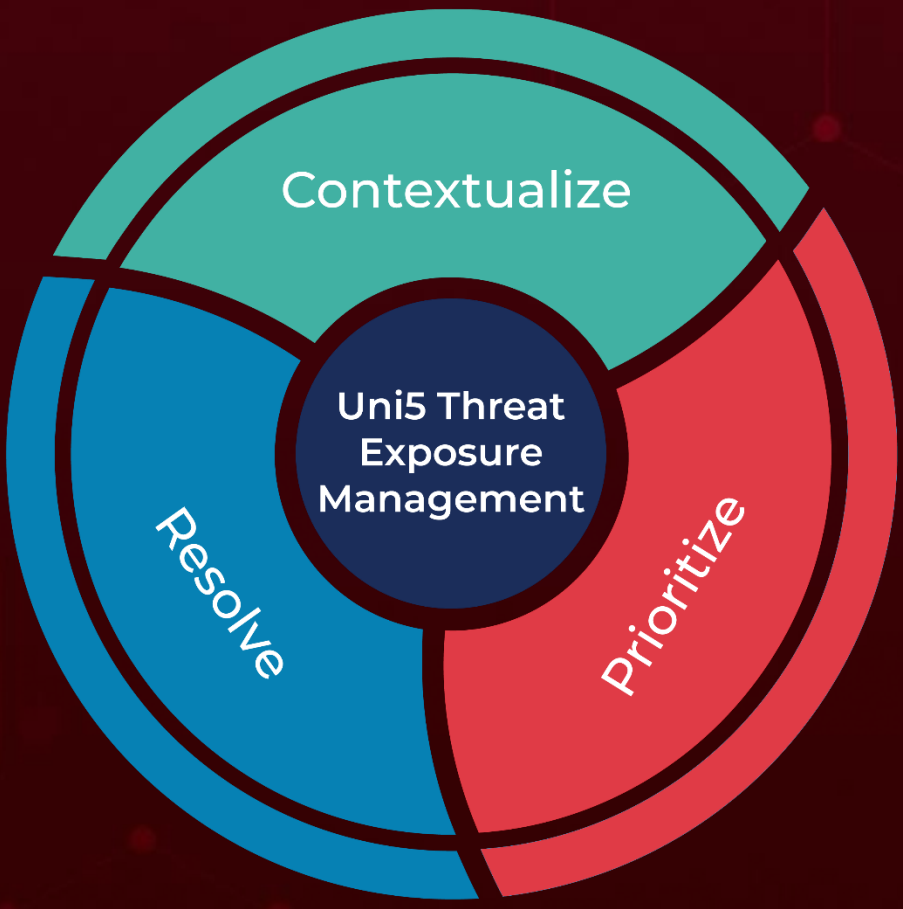
| Attack Name | TYPE | VALUE |
|---|---|---|
| Crimson RAT | Domains | richa-sharma.ddns[.]net<br>cloud-drive[.]store<br>drive-phone[.]online<br>s1.fileditch[.]ch |
| | SHA1 | 738d31ceca78ffd053403d3b2bc15847682899a0<br>9ed39c6a3faab057e6c962f0b2aaab07728c5555<br>af6608755e2708335dc80961a9e634f870aecf3c<br>e000596ad65b2427d7af3313e5748c2e7f37fba7<br>fd46411b315beb36926877e4b021721fcd111d7a<br>516db7998e3bf46858352697c1f103ef456f2e8e<br>842f55579db786e46b20f7a7053861170e1c0c5e<br>87e0ea08713a746d53bef7fb04632bfcd6717fa9<br>911226d78918b303df5110704a8c8bb599bcd403<br>973cb3afc7eb47801ff5d2487d2734ada6b4056f |
| Zaraza bot | MD5 | 41D5FDA21CF991734793DF190FF078BA |
| | SHA1 | b50a8e2a7998e17286d2e18d1cf3f7e4e84482c6 |
| | SHA256 | 2cb42e07dbdfb0227213c50af87b2594ce96889fe623dbd73d<br>228e46572f0125 |
| Dave Loader | SHA256 | de9b3c01991e357a349083f0db6af3e782f15e981e2bf0a16ba<br>618252585923a,<br>b14ab379ff43c7382c1aa881b2be39275c1594954746ef58f6a<br>9a3535e8dc1a8,<br>dbdfc3ca5afa186c1a9a9c03129773f7bc17fb7988fe0ca40fc3c<br>5bedb201978,<br>ce99b4c0d75811ce70610d39b1007f99560e6dea887a451e08<br>916a4f8cf33678 |
| Domino Backdoor | IPV4 | 88.119.175[.]124<br>94.158.247[.]72<br>185.225.17[.]202<br>5.182.37[.]118 |
| | URLs | hxxp://170.130.55[.]250/x64.exe<br>hxxps://upperdunk[.]com/mr64.exe |
| | SHA256 | de9b3c01991e357a349083f0db6af3e782f15e981e2bf0a16ba<br>618252585923a,b14ab379ff43c7382c1aa881b2be39275c159<br>4954746ef58f6a9a3535e8dc1a8,dbdfc3ca5afa186c1a9a9c03<br>129773f7bc17fb7988fe0ca40fc3c5bedb201978,ce99b4c0d75<br>811ce70610d39b1007f99560e6dea887a451e08916a4f8cf33<br>678,f4ebd59fb578a0184abf6870fc652210d63e078a35dace0<br>a48c5f273e417c13d,92651f9418625e5281b84cccb817e94e6<br>294b36c949b00fcd4046770b87f10e4,e5af0b9f4650dc0193c9<br>884507e6202b04bb87ac5ed261be3f4ecfa3b6911af8 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| NewWorldOrder Loader | SHA256 | f1817665ea2831f775e23cbda27cbeb06d03e6c39bbfad920b50f40712dd37cb,51e0512a54640be8e3477363c8d72d893c6edd20399bddf71e95eec3ddfdb42e,f4ebd59fb578a0184abf6870fc652210d63e078a35dace0a48c5f273e417c13d,92651f9418625e5281b84cccb817e94e6294b36c949b00fcd4046770b87f10e4 |
| Carbanak Backdoor | IPV4 | 178.23.190[.]73 |
| | SHA256 | f1817665ea2831f775e23cbda27cbeb06d03e6c39bbfad920b50f40712dd37cb,51e0512a54640be8e3477363c8d72d893c6edd20399bddf71e95eec3ddfdb42e |
| Project Nemesis infostealer | IPV4 | 45.67.34[.]236 |
| | Domain | es-megadom[.]com |
| LockBit Ransomware | SHA1 | 2d15286d25f0e0938823dcd742bc928e78199b3d,<br>864f56b25a34e9532a1175d469715d2f61c56f7f,<br>ef958f3cf201f9323ceae9663d86464021f8e10d |
| QBot (also known as QakBot, QuackBot, and Pinkslipbot) | MD5 | 253E43124F66F4FAF23F9671BBBA3D98<br>39FD8E69EB4CA6DA43B3BE015C2D8B7D<br>299FC65A2EECF5B9EF06F167575CC9E2<br>A6120562EB673552A61F7EEB577C05F8<br>1FBFE5C1CD26C536FC87C46B46DB754D<br>FD57B3C5D73A4ECD03DF67BA2E48F661<br>28C25753F1ECD5C47D316394C7FCEDE2 |
| | Domain | cica.com[.]co/stai/stai.php<br>abhishekmeena[.]in/ducs/ducs.php<br>rosewoodlaminates[.]com/hea/yWY9SJ4VOH<br>agtendelperu[.]com/FPu0Fa/EpN5Xvh<br>capitalperurrhh[.]com/vQ1iQg/u6oL8xlJ<br>centerkick[.]com/IC5EQ8/2v6u6vKQwk8<br>chimpcity[.]com/h7e/p5FuepRZjx<br>graficalevi.com[.]br/0p6P/R94icuyQ<br>kmphi[.]com/FWovmB/8oZ0BOV5HqEX<br>propertynear.co[.]uk/QyYWyp/XRgRWEdFv<br>theshirtsummit[.]com/MwBGSm/lGP5mGh |

# 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

**April 24, 2023 . 7:00 AM**



More at www.hivepro.com