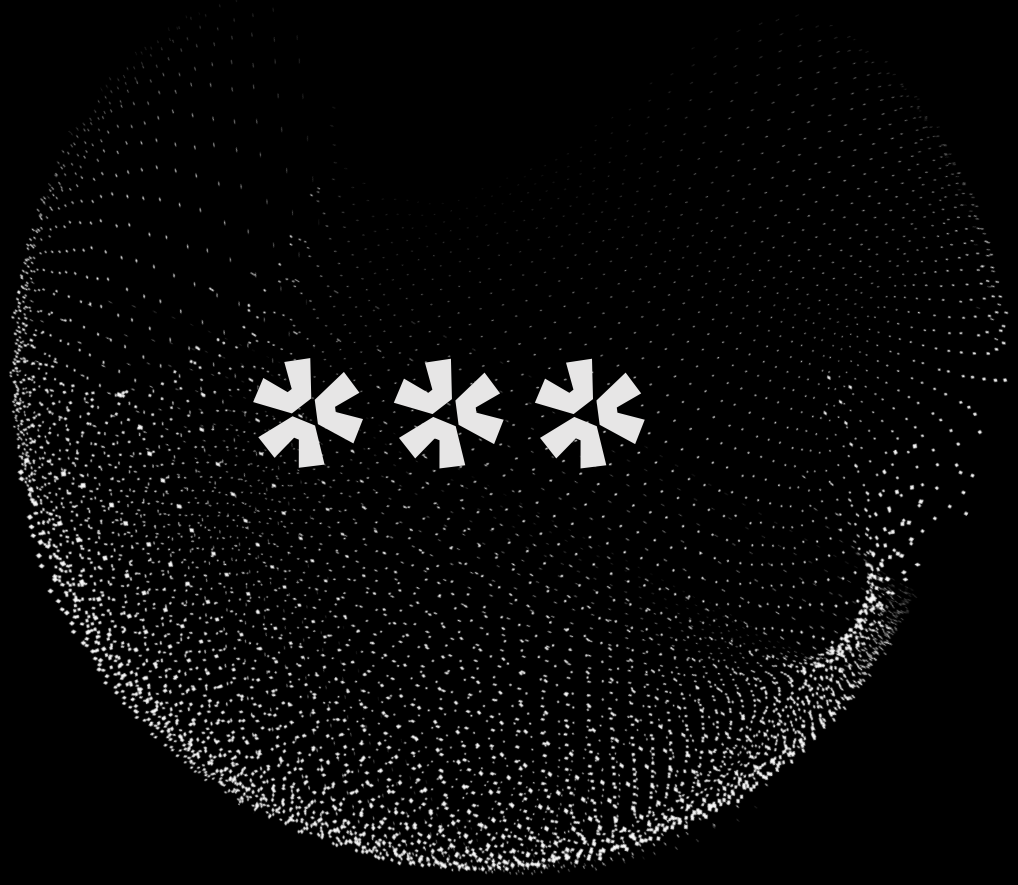
elixicode



09/07/2024

Threat Intel Report

# Foresighting The Future, Fortifying Now

Stay one step ahead of cybersecurity threats with Elixicode's forward-thinking approach. Our weekly report equips you with actionable insights and proactive measures to build robust defenses against emerging threats.

**PUBLIC**

# Table of Contents

“

Building a global threat intelligence network empowers us to identify and track cybercrime across borders, disrupting their operations.

”

- International Law Expert

# Unveiling the Future of Threats: Your Guide to Proactive Security

In today's digital landscape, foresight isn't just a luxury, it's a necessity. Cyber threats evolve at lightning speed, demanding proactive action to fortify your defenses. At Elixicode, we believe knowledge is power, and that's why we're launching this weekly Threat Intel Report, exclusively available for free on our X (previously Twitter) page.

This report, published every week, serves as your essential guide to the latest threats, aligning with our motto of "Foresighting the future, Fortifying Now". We delve deep into malware trends, malicious domains, emerging vulnerabilities, and even country-specific threat landscapes, empowering you to take preventive measures and stay ahead of the curve.

**Why should you make "Foresighting the future, Fortifying Now" a reality?**

- **Actionable insights:** Each report is curated by our expert analysts, providing concise and practical steps you can take to mitigate specific threats.
- **Stay ahead of the curve:** We track emerging threats and trends, keeping you informed about the latest developments in the cybercrime world.
- **Community-driven security:** By sharing this knowledge, we collectively raise the bar for cyber defense, making everyone safer.

**Elixicode's commitment to the community:**

This report is more than just information; it's our contribution to building a stronger, more secure digital world. We believe that by empowering individuals and organizations with knowledge, we can collectively combat cybercrime and create a safer online environment.

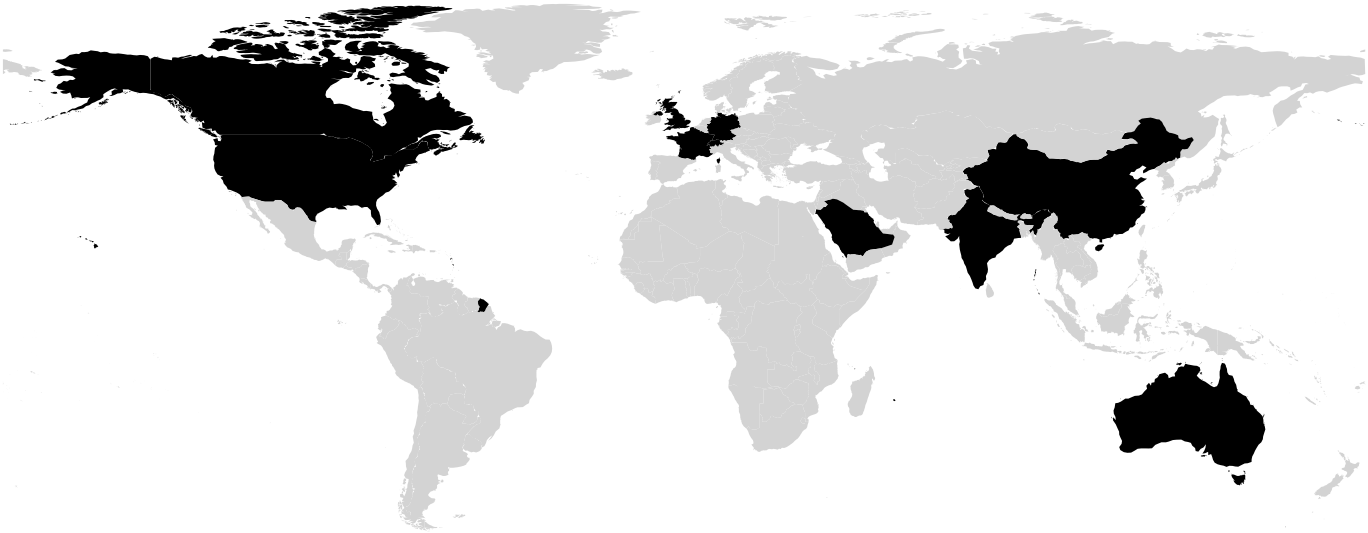
**Join us on this journey of proactive security. Follow us on X and access your free weekly Threat Intel Report today!**

01

# Geopolitical Briefing

# Top 10 Cybersecurity Battlegrounds

This map visualizes the top 10 most active countries in the global cybersecurity landscape, highlighting both their roles as destinations and sources of cyberattacks. The countries are ranked in descending order of activity, revealing the leading players in this increasingly dynamic arena. This visualization provides a valuable overview of the global cybersecurity landscape, enabling you to identify key areas of concern and strategic priorities.



1. **United States**
2. **Germany**
3. **India**
4. **Canada**
5. **Saudi Arabia**
6. **France**
7. **Switzerland**
8. **Australia**
9. **China**
10. **United Kingdom**

# The Industries Cybercriminals Favor Most

The ever-evolving cyber threat landscape constantly targets specific industries, exploiting vulnerabilities and seeking valuable data. This section reveals the top 4 most targeted industries in order of attack frequency and severity. By analyzing attack trends and industry-specific vulnerabilities, we gain valuable insights into the motivations and methods of cybercriminals.

1

### Technology

Innovation stifled by stolen ideas, development hampered by cyberattacks, supply chains exploited.

2

### Finance and insurance

Financial fraud skyrockets, sensitive data exposed, market manipulation disrupts economies.

3

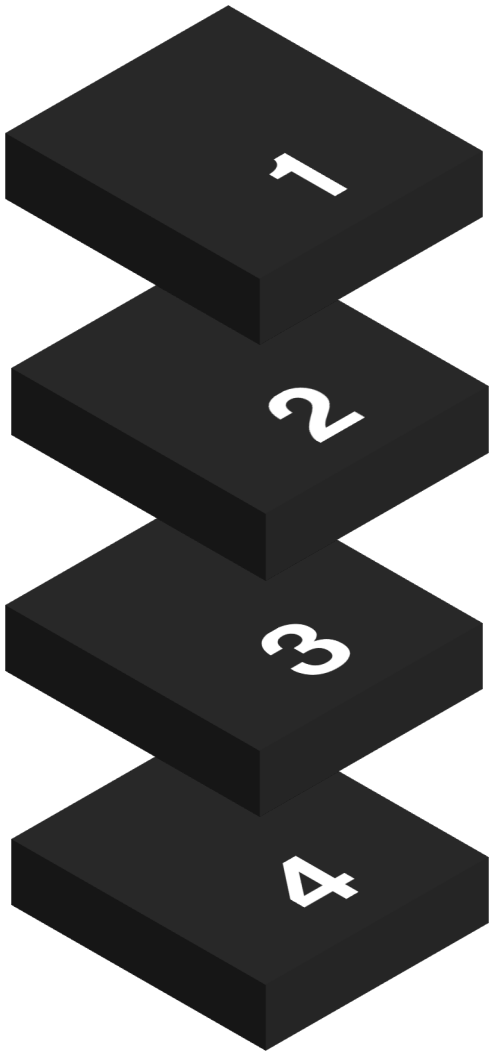
### Communication

Networks disrupted, online privacy invaded, freedom of expression curtailed.

4

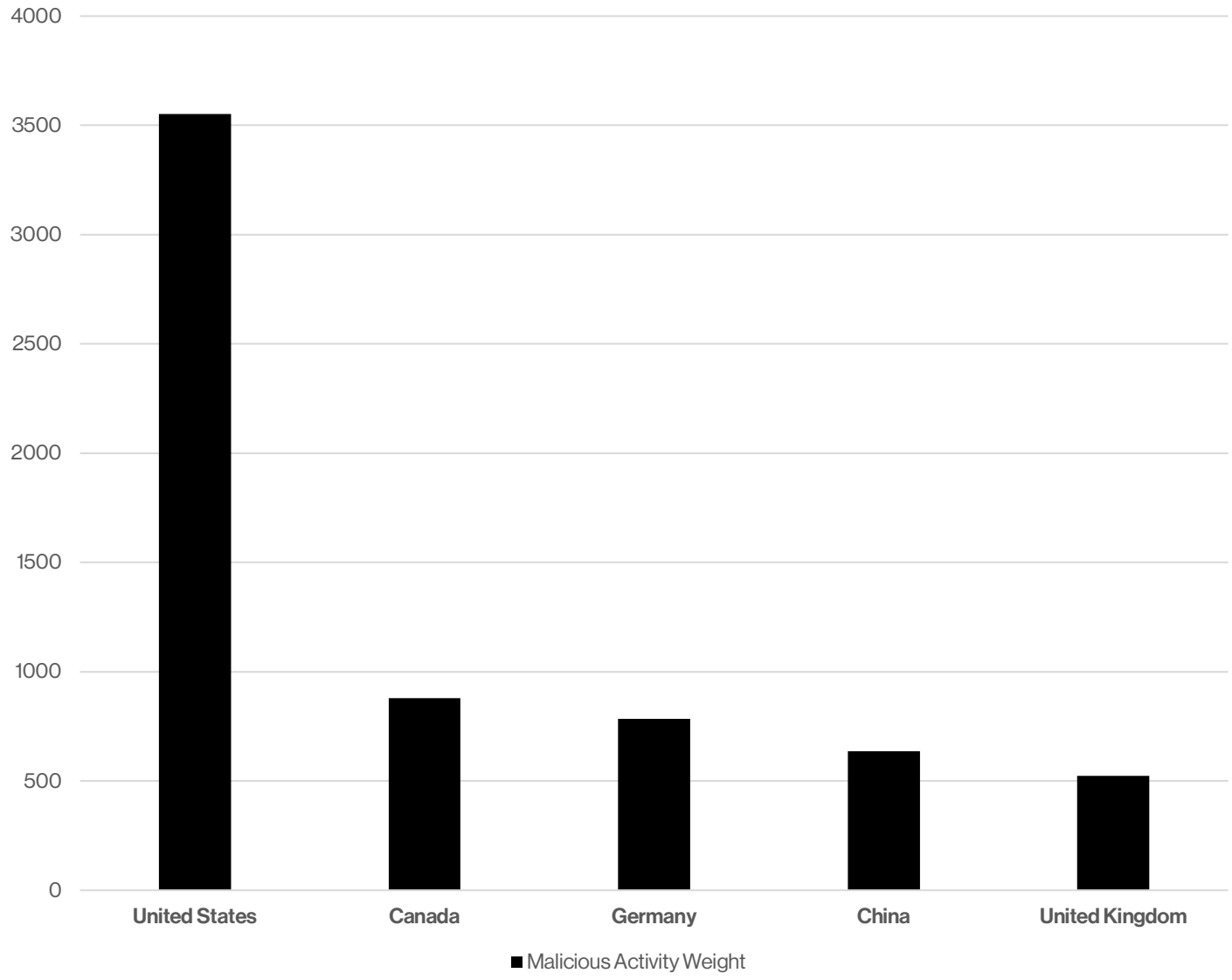
### Government

Classified intel exposed, public trust undermined through disinformation campaigns.



# Tracing the Source

Delving into the shadowy world of cybercrime, this section pinpoints the top 5 countries hosting the most malicious IP addresses ranked in descending order of prevalence. Understanding these hotspots allows us to track emerging threats, identify potential attack vectors, and collaborate with international partners to disrupt malicious activity.



02

# Cyberattacks Briefing

PUBLIC

# Top 3 Breach Stories Heating Up the News Cycle

In the fast-paced world of cybersecurity, data breaches constantly capture our attention. This section sheds light on the top 3 data breaches currently dominating the news cycle. From large-scale corporate compromises to targeted attacks on vulnerable sectors, these incidents highlight the ever-present threat of cybercrime. By analyzing the details of these breaches, we gain valuable insights into attack methods, data vulnerabilities, and the evolving techniques cybercriminals employ.

| | | |
|---|---|---|
| 1 | Title | **Hackers Expose 33M Twitter User Phone Numbers** |
| | Description | Cloud communications provider Twilio has revealed that unidentified threat actors took advantage of an unauthenticated endpoint in Authy to identify data associated with Authy accounts, including users' cell phone numbers. The company said it took steps to secure the endpoint to no longer accept unauthenticated requests. The development comes days after an online persona named ShinyHunters published on BreachForums a database comprising 33 million phone numbers allegedly pulled from Authy accounts. Authy, owned by Twilio since 2015, is a popular two-factor authentication (2FA) app that adds an additional layer of account security. |

| | | |
|---|---|---|
| 2 | Title | **Hackers Leak 39,000 Ticketmaster Tickets** |
| | Description | Ticketmaster later confirmed that its data breach was stolen from their Snowflake account. At the time, the threat actors demanded that Ticketmaster pay them $500,000 so that the data would not be leaked or sold to other threat actors. However, a week ago, the same threat actors leaked 166,000 Taylor Swift ticket barcodes, demanding a higher $2 million extortion demand. Ticketmaster responded by saying that the data is useless as their anti-fraud measures constantly rotate to unique mobile barcodes. "Ticketmaster's SafeTix technology protects tickets by automatically refreshing a new and unique barcode every few seconds so it cannot be stolen or copied," Ticketmaster told BleepingComputer. |

| | | |
|---|---|---|
| 3 | Title | **Affirm Says Evolve Bank Data Breach Also Compromised Some Of Its Customers** |
| | Description | Affirm shares customer data with Evolve as required to issue Affirm Cards, a debit card that lets you pay for purchases over time. "On June 25, 2024, Evolve Bank & Trust ("Evolve"), the third-party issuer of the Affirm Card, notified Affirm (the Company) that Evolve had experienced a cybersecurity incident whereby a third party gained unauthorized access to personal information and financial information ("Personal Information") of Evolve retail banking customers and the customers of its financial technology partners," reads the 8-K filing. |

# Top 3 Attacks Shaking the Headlines

Navigating the ever-changing landscape of cyber threats can be overwhelming. This section dissects the top 3 cyber-attacks currently captivating the news, ranked in descending order of recency and potential impact.

| | | |
|---|---|---|
| 1 | Title | **CloudSorcerer Malware Targets Russian Government** |
| | Description | CloudSorcerer communicates with its cloud services through APIs, using authentication tokens, and employs GitHub as its initial C2 server. Despite similarities to the CloudWizard APT reported in 2023, CloudSorcerer's malware code is entirely different, Kaspersky said, suggesting it is a new actor utilizing a similar method of engaging with public cloud services. Additional advanced functionalities are executed based on specific command IDs, such as creating or deleting tasks, managing services and performing network operations. The C2 module sets up an initial connection to the C2 server, starting with a GitHub page, and can alternatively use a photo hosting server on my.mail. |

| | | |
|---|---|---|
| 2 | Title | **Patelco Credit Union Shuts Down Following Ransomware Attack** |
| | Description | It offers a wide range of financial services, including checking and savings accounts, loans, credit cards, investment services, and insurance plans. The California-based not-for-profit organization serves over 400,000 members through 37 branches in the Bay Area, Sacramento, and San Jose. In a status update about service outages that started on June 29, 2024, Patelco said it experienced a ransomware attack that day. "On June 29, 2024, Patelco Credit Union experienced a ransomware attack," informed Patelco. "Unfortunately, this incident has required us to proactively shut down some of our day-to-day banking systems in order to contain and remediate the issue.". |

| | | |
|---|---|---|
| 3 | Title | **New Ransomware Targets Windows and VMware ESXi** |
| | Description | A new ransomware-as-a-service (RaaS) called Eldorado emerged in March and comes with locker variants for VMware ESXi and Windows. The gang has already claimed 16 victims, most of them in the U.S., in real estate, educational, healthcare, and manufacturing sectors. Researchers at cybersecurity company Group-IB monitored the Eldorados activity and noticed its operators promoting the malicious service on RAMP forums and seeking skilled affiliates to join the program. Eldorado also runs a data leak site that lists victims but it was down at the time of writing. |

# Must-Read Cybersecurity News

Staying ahead of the curve in cybersecurity demands constant vigilance. This section tackles the top 3 cybersecurity news stories currently dominating the headlines, ranked in descending order of their heat and potential impact.

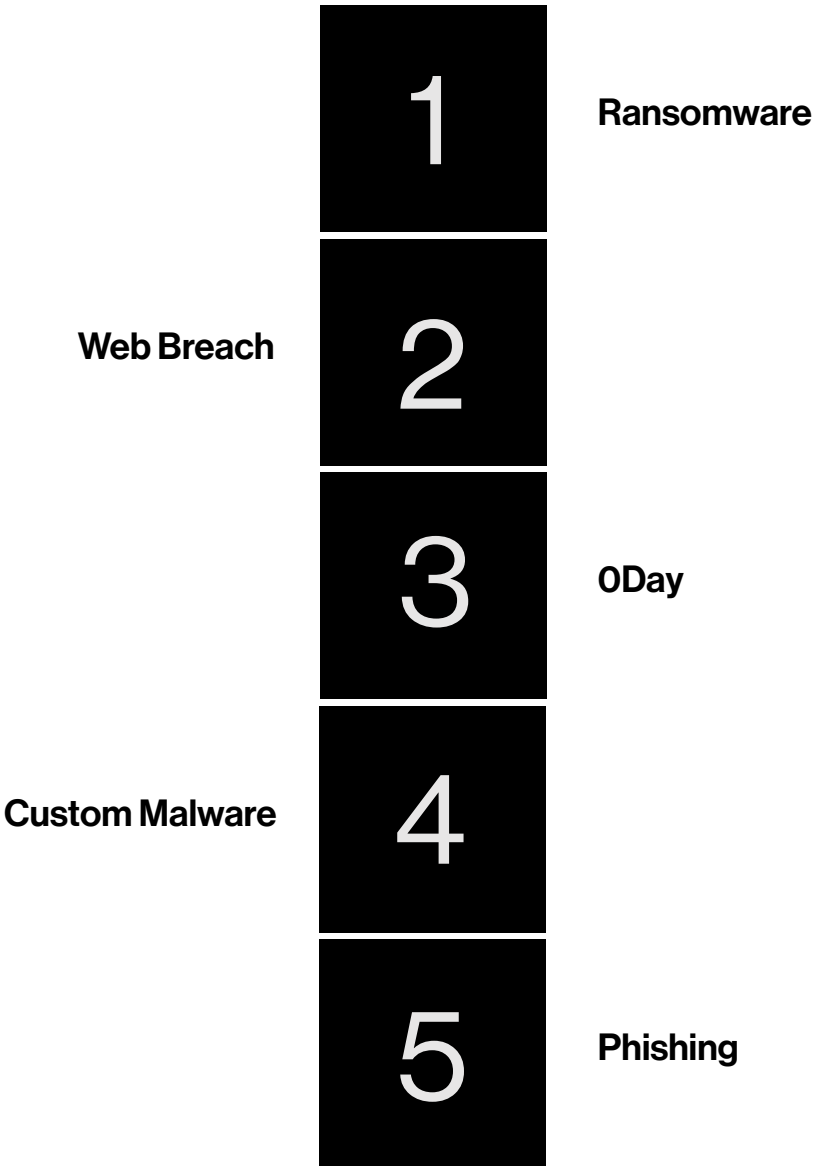
| | | |
|---|---|---|
| 1 | Title | **Suse Linux Security Advisory** |
| | Description | • CVE-2024-33870<br>• CVE-2024-29510<br>• CVE-2024-24791<br>• CVE-2024-33869 |

| | | |
|---|---|---|
| 2 | Title | **Hackers Exploiting Remote Code Execution Vulnerabilities** |
| | Description | This vulnerability affects HFS version 3 before 0.52.10 on Linux, UNIX, and macOS systems, allowing remote authenticated users with upload permissions to execute OS commands due to the use of execSync instead of spawnSync in the child_process Module of Node.js. The vulnerability arises because HFS uses a shell to execute the df command, which attackers can exploit to run arbitrary commands on the host system. The update addresses the issue by replacing execSync with spawnSync in the child_process module, thereby preventing the execution of arbitrary commands via the shell. |

| | | |
|---|---|---|
| 3 | Title | **Mt. Gox Begins Repaying Bitcoin To Creditors a Decade After Exchange's Collapse** |
| | Description | Gox, the Japanese bitcoin exchange that collapsed into bankruptcy a decade ago, on Friday said the company has begun to make payments in bitcoin and in bitcoin cash to some of its creditors. The announcement added that repayments to other users of the hacked exchange would be "promptly made" if they meet certain conditions, including undergoing account verification, as well as subscribing to one of the designated digital asset exchanges through which the bankruptcy estate is facilitating disbursements in digital tokens. "We ask eligible rehabilitation creditors to wait for a while," continues the statement. |

## Ranking the Top 5 Cyberattack Methods

In the ever-shifting arena of cybersecurity, knowing your enemy is crucial. This section ranks the top 5 types of cyberattacks currently plaguing the digital world, listed in descending order of their prevalence. From the widespread reach of malware to the targeted precision of phishing campaigns, understanding these diverse attack methods empowers us to bolster our defenses and make informed decisions.



# Top 3 MITRE ATT&CK Tactics in Action

Gain crucial insights into the tactics cybercriminals employ by exploring the top 3 MITRE ATT&CK tactics observed in real-world attacks, ranked in order of observed prevalence.

| | | |
|---|---|---|
| 1 | MITRE ID | **TA0040** |
| | Tactic | **Impact** |
| | Description | The adversary is trying to manipulate, interrupt, or destroy your systems and data. |
| | Reference | https://attack.mitre.org/tactics/TA0040/ |

| | | |
|---|---|---|
| 2 | MITRE ID | **TA0002** |
| | Tactic | **Execution** |
| | Description | The adversary is trying to run malicious code. |
| | Reference | https://attack.mitre.org/tactics/TA0002/ |

| | | |
|---|---|---|
| 3 | MITRE ID | **TA0003** |
| | Tactic | **Persistence** |
| | Description | The adversary is trying to maintain their foothold. |
| | Reference | https://attack.mitre.org/tactics/TA0003/ |

# Most Observed MITRE Techniques

This section dives deeper into the tactics discussed previously, highlighting the top 3 most utilized MITRE ATT&CK techniques and sub-techniques observed in real-world attacks, ranked in order of prevalence. Gain insights into attackers' preferred methods and sub-techniques for achieving their goals, empowering you to prioritize and tune your security measures effectively.

| 1 | | |
|---|---|---|
| | Technique ID | **T1083** |
| | Sub-technique ID | **N/A** |
| | Technique | **File and Directory Discovery** |
| | Sub-technique | **N/A** |
| | Description | Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. |
| | Technique Reference | https://attack.mitre.org/techniques/T1083/ |
| | Sub-technique Reference | N/A |

| 2 | | |
|---|---|---|
| | Technique ID | **T1190** |
| | Sub-technique ID | **N/A** |
| | Technique | **Exploit Public-Facing Application** |
| | Sub-technique | **N/A** |
| | Description | Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration. |
| | Technique Reference | https://attack.mitre.org/techniques/T1190/ |
| | Sub-technique Reference | N/A |

| 3 | | |
|---|---|---|
| | Technique ID | **T1039** |
| | Sub-technique ID | **N/A** |
| | Technique | **Data from Network Shared Drive** |
| | Sub-technique | **N/A** |
| | Description | Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within cmd may be used to gather information. |
| | Technique Reference | https://attack.mitre.org/techniques/T1039/ |
| | Sub-technique Reference | N/A |

03

# Vulnerability Briefing

PUBLIC

# Most Exploited Vulnerabilities

Beware these weak spots! This section reveals the top 6 CVEs currently exploited in active cyberattacks, ranked based on their frequency of exploitation in real-world attacks. Understanding these critical vulnerabilities empowers you to patch your systems swiftly and stay ahead of cyber threats.

1

**CVE-2024-20399**
A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands as root.

2

**CVE-2024-23692**
Rejetto HTTP File Server, up to and including version 2.3m, is vulnerable to a template injection vulnerability.

3

**CVE-2024-6387**
A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd).

4

**CVE-2023-2071**
Rockwell Automation FactoryTalk View Machine Edition allows unauthenticated remote code execution via crafted malicious packets.

5

**CVE-2023-29464**
FactoryTalk Linx, in the Rockwell Automation PanelView Plus, allows an unauthenticated threat actor to read data from memory via crafted malicious packets.

6

**CVE-2024-6071**
PTC Creo Elements/Direct License Server unauthenticated remote arbitrary OS commands execution.

## Exploitation Prevalence

| 9.1% | 5.7% | 4.5% | 4.5% | 4.5% | 4.5% |
|---|---|---|---|---|---|
| **CVE-2024-20399** | **CVE-2024-23692** | **CVE-2024-6387** | **CVE-2023-2071** | **CVE-2023-29464** | **CVE-2024-6071** |

# 04
# Malware Briefing

## Unveiling the Top 10 Malware Families on the Prowl

In the ongoing battle against malicious software, staying vigilant is key. This section sheds light on the top 10 malware families actively posing a threat organized in order of activity. By leveraging this intelligence, you can fortify your defenses, deter cyberattacks, and contribute to a more secure digital environment for all.

1. xmrig
2. AgentTesla
3. AsyncRAT
4. Mirai
5. Remcos
6. GuLoader
7. RedLine
8. XWorm
9. Lumma
10. Stealc

## Unveiling the Top 10 Malware Types

This section dives deeper into the top 10 malware types currently plaguing the digital world, ranked by their prevalence. Understanding the diverse functionalities and goals of these threats empowers you to make informed decisions.

| | |
|---|---|
| 1 | Persistence |
| 2 | Upx |
| 3 | Stealer |
| 4 | Evasion |
| 5 | Spyware |
| 6 | Trojan |
| 7 | Miner |
| 8 | Discovery |
| 9 | Rat |
| 10 | Ransomware |

## Most Common Malware File Names for Enhanced Detection

Don't let deceptive file names fool you! This section sheds light on the most common file names used by malware, empowering you to strengthen your detection and prevention systems. By understanding the naming conventions and tactics employed by attackers, you can improve your ability to identify malicious files before they can compromise your systems. This valuable knowledge allows you to refine your security filters, educate users on suspicious file names, and proactively mitigate potential threats.

| | |
|---|---|
| | testsh-main.zip |
| | RobloxPlayerInstaller.exe |
| | 1.exe |
| | wannaCry.exe |

## Top 5 Most Common Malware Extensions

Remember, even a seemingly harmless extension can harbor hidden dangers.

| | |
|---|---|
| 1010 1010 | .exe |
| 1010 1010 | .zip |
| 1010 1010 | .bat |
| 1010 1010 | .pdf |
| 1010 1010 | .elf |

# Identifying Malware Hidden in Double Extensions

Cybercriminals are constantly innovating their tactics, and double extensions represent a cunning attempt to bypass user and system defenses. This section exposes the most common double extensions used by malware, equipping cybersecurity specialists with crucial knowledge to detect and thwart these deceptive threats. By understanding the logic behind these extensions and the types of malwares they often disguise, specialists can refine detection filters, educate users on spotting suspicious files, and proactively identify potential compromise attempts.

| | |
|---|---|
| | .dll.dll |
| | .dll.exe |
| | .scr.exe |
| | .2.exe |
| | .pdf.exe |
| | .0.exe |
| | .ppc.elf |
| | .4.exe |
| | .txt.jar |
| | .5.exe |

# Top 9 Active Malware Variants

Unveiling the top 9 hashes of the most active malware variants, this valuable resource empowers you to strengthen your threat detection and prevention capabilities. Hashes provide a unique fingerprint for each file, enabling you to accurately identify known malicious variants before they can execute and harm your systems.

| | | |
|---|---|---|
| 1 | Malware Family | hacktool |
| | Malware Type | Miner |
| | MD5 | 93204e8e3ecb258439133f9e3c2e25fc |
| | SHA1 | 0f3d7047924de2958882efeb60654cf99621d22e |
| | SHA256 | 6a40699ad6e5bcc4aacc1023d48c1a97341434c633ecc2e5ded7d01ceb50fd1c |

| | | |
|---|---|---|
| 2 | Malware Family | WannaCry |
| | Malware Type | Ransomware |
| | MD5 | 84c82835a5d21bbcf75a61706d8ab549 |
| | SHA1 | 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467 |
| | SHA256 | ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa |

| | | |
|---|---|---|
| 3 | Malware Family | N/A |
| | Malware Type | Trojan |
| | MD5 | 15d1285b7f081a6595bd2509af67d0a5 |
| | SHA1 | a2bb676c493335defd494f3ca6bc5863c826a65c |
| | SHA256 | 6834c9d484470975d26f840c3dd61eb4eec7c82b796a72c308d238592af4048b |

| | | |
|---|---|---|
| 4 | Malware Family | N/A |
| | Malware Type | PUA |
| | MD5 | e927148af4298e8d1ca02d175218b9bc |
| | SHA1 | 18224fd3b2108160e3905f6ebce75d0b88529b42 |
| | SHA256 | 7175d0071e3fefe19009a280a0cd3e43ecf3936ff5a06d0a2ca616f5d0d6a3cf |

| | | |
|---|---|---|
| 5 | Malware Family | N/A |
| | Malware Type | N/A |
| | MD5 | fd4bf565af2154c5651a5d34bf993660 |
| | SHA1 | 4419971b7bf4fd32393707a5c18c66b19ffb46a0 |
| | SHA256 | d0ec7df89e17c336e054aeb8dc433226fceff8dfc7d35f4f56dec398a6c1677e |

| | | |
|---|---|---|
| 6 | Malware Family | N/A |
| | Malware Type | N/A |
| | MD5 | 8a1dbacf6988044e94bde41ec40d0702 |
| | SHA1 | be704c499e3add1a48d5c837d85ac887900c7b8f |
| | SHA256 | 67f4136ef474ee986914c002a076cfefd5eb763cf479c080b7befffc48bb79ce |

| | | |
|---|---|---|
| 7 | Malware Family | N/A |
| | Malware Type | N/A |
| | MD5 | 80648041f66086247d8654ab3183feb9 |
| | SHA1 | e9f86c788c481f82a2c1cee12738fb8638e5abd0 |
| | SHA256 | 156b0e9a1fe964d47d28f6824a338f586b8a9e75b3e0a88811c570c0c2f6f174 |

| | | |
|---|---|---|
| 8 | Malware Family | hacktool |
| | Malware Type | Downloader |
| | MD5 | a0f4dea92c2045c7da2664345e4e5edf |
| | SHA1 | 65b0a50e15806582dc219e62dc69537e6fdb393b |
| | SHA256 | ece5d03dbc48cc6126fb1757b3951b9aedfad5a007ebddd4e5f98eb1ff230946 |

| | | |
|---|---|---|
| 9 | Malware Family | N/A |
| | Malware Type | RAT |
| | MD5 | dd96882c5f8176276cf4c89b48c0812f |
| | SHA1 | a2cc6c07197e0e52b330be9ab0a25b701f707850 |
| | SHA256 | af6b8a5712b7a3b3061cbb969a689ecf331f3527a402fb38ab7523843ec02e19 |

05

# Domains Briefing

PUBLIC

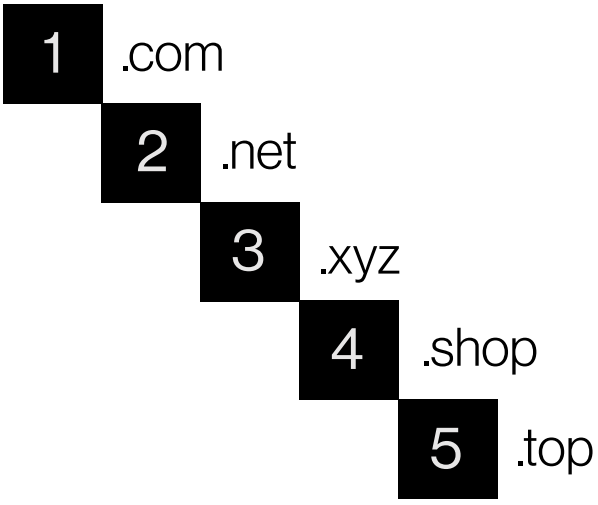
## Top 5 Malicious Domains to Avoid at All Costs

Tread carefully in the digital wilderness! This section exposes the top 5 most prevalent malicious domains observed in the wild, ranked by their frequency of luring unsuspecting users.

| # | Domain | Registrar |
|---|---|---|
| 1 | json[.]gp | N/A |
| 2 | n[.]tdi | N/A |
| 3 | 3[.]td | N/A |
| 4 | getwave[.]gg | N/A |
| 5 | hop[.]fyi | Squarespace Domains II LLC |

## Top 5 TLDs of Malicious Domains

This section reveals the top 5 TLDs most frequently used by malicious domains ranked in order of prevalence, empowering you to identify potential threats beyond the usual suspects.



# Exposing Malicious Domains Disguised as Legitimate Websites

Navigating the digital world requires eagle eyes! This section delves into the malicious domains utilizing typosquatting tactics, ranked by their prevalence. These domains prey on users' misspellings, leading them to phishing sites, malware traps, or data-stealing scams. By understanding these deceptive tactics, you gain valuable insights into how attackers exploit human error.

| Malicious Domain | Brand Targeted |
|---|---|
| gebeus[.]ru | getbus.ru |
| gofastup[.]top | gofast4.top |
| pcapi-server[.]com | pairserver.com |
| whatismyipaddressnow[.]co | whatismyipaddress.com |
| wingtransfer[.]com | wetransfer.com |
| mussangroup[.]com | masangroup.com |
| maanalaw[.]com | mangaclaw.com |

06

# URL Briefing

PUBLIC

# Top 5 Malicious URLs Lurking Online

This section exposes the top 5 malicious URLs currently posing a threat, ranked by their prevalence. These deceptive links often hide malware, phishing scams, or data-stealing attempts behind seemingly harmless facades. By understanding these digital pitfalls, you can navigate the online world with caution and make informed decisions about where you click.

| # | Malicious URL |
|---|---|
| 1 | http://ip-api[.]com/line/?fields=hosting |
| 2 | https://getwave[.]gg/ |
| 3 | https://github[.]com/Dfmaaa/MEMZ-virus |
| 4 | https://u4041592.ct.sendgrid[.]net/ls/click?upn=u001.HwvKDDUOH-2FsSEvMYmw1tppEzGPuRcsSEN-2FAvdwfLzzz9S8aAEpo-2FCkKMTSNroyst4cAg7fmKqk-2BXpAldaJdsVhazspBukcGU2rXKMLs60LQtBJrf-2FJdu7cEbTRGqV3LmEEBI8oe29WfBnZqIdZ3e0Q-3D-3DJVwp_g4mmm0p0L4-2BAfZooz6wMJwPd1KTnF-2F1EeKuhFaBtNgo62D9kdkj5eF0sGUgcGM79wFTTu8cJaw8pGMiEFNE-2F-2BPzyYP1upBXDH3LjBiRqrMBRqnnovqxGUfO9NPWK7R0Ii6zugVJ3GqkhNcEMi-2F7SJYbzO6oh2y-2F7xnRJ4LzF6r9GdOOz5ZynFZ-2BRKZTtw6iNokIZanr7qFI0LrUX1p3FjQ-3D-3D |
| 5 | https://hr.economictimes.indiatimes[.]com/etl.php?url=https://hr.economictimes.indiatimes.com/etl.php?url=//www.assurancehongkong.com#Wlondonops@riyadbank.com//5wgkjeu0ci455/%2F/bG9uZG9ub3BzQHJpeWFkYmFuay5jb20= |

# Identifying Hosting Providers Housing Most Malicious URLs

Knowing where threats originate empowers proactive defense! This section sheds light on the top 4 web hosting service providers abused for hosting most of the malicious URLs tracked, ranked by their prevalence.

| | | |
|---|---|---|
| 1 | Hosting Provider | Cloudflare, Inc. |
| | Hosting Location | Canada |
| | Activity Weight | 51.5% |

| | | |
|---|---|---|
| 2 | Hosting Provider | Microsoft Corporation |
| | Hosting Location | United Arab Emirates |
| | Activity Weight | 24.2% |

| | | |
|---|---|---|
| 3 | Hosting Provider | Google LLC |
| | Hosting Location | France |
| | Activity Weight | 13.6% |

| | | |
|---|---|---|
| 4 | Hosting Provider | Cloudflare London, LLC |
| | Hosting Location | United States |
| | Activity Weight | 3.3% |

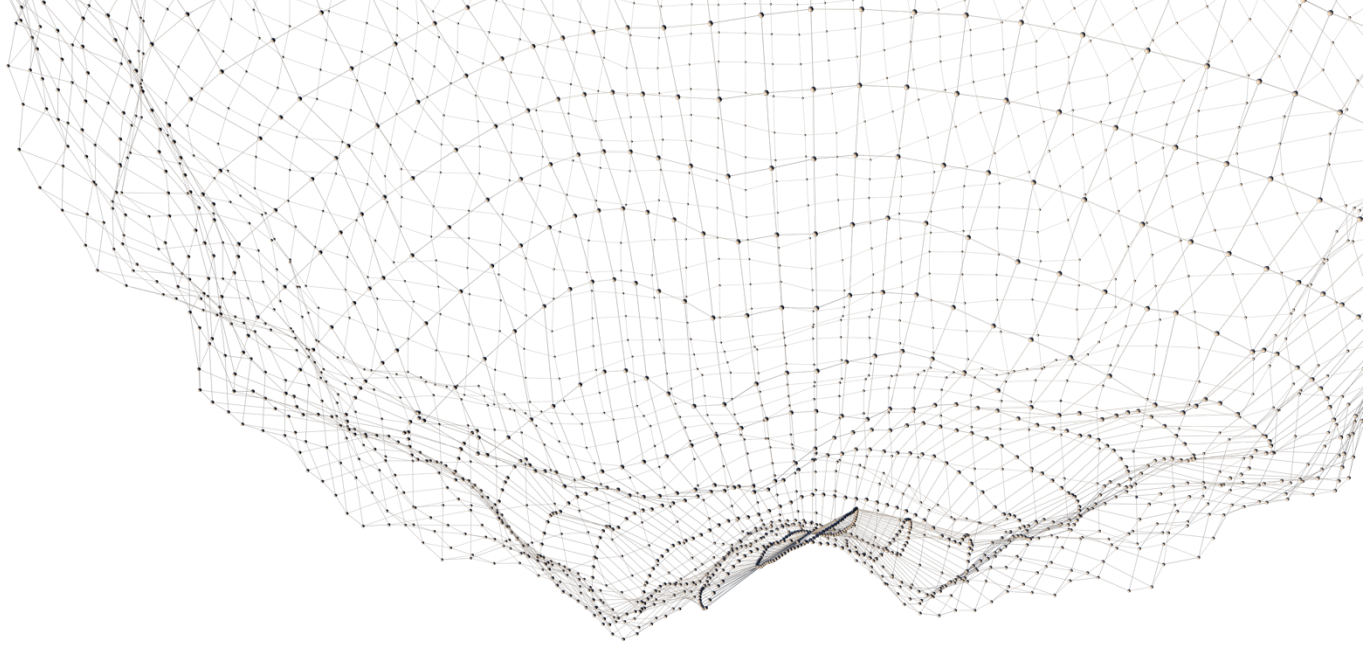
07

# IP Address Briefing

# Top 15 Malicious IP Addresses

Knowledge is power in the fight against cybercrime! This section exposes the top 15 malicious IP addresses currently posing a significant threat, ranked by their prevalence and malicious activity.

| # | IP Address | Country | ISP |
|---|---|---|---|
| 1 | 77.91.77[.]81 | Germany | WAIcore Hosting LTD. |
| 2 | 178.237.33[.]50 | Netherlands | Schuberg Philis B.V. |
| 3 | 77.91.77[.]82 | Germany | WAIcore Hosting LTD. |
| 4 | 85.28.47[.]30 | Russian Federation | N/A |
| 5 | 13.248.169[.]48 | Canada | Amazon.com, Inc. |
| 6 | 185.172.128[.]90 | Germany | TNSECURITY LTD |
| 7 | 185.172.128[.]69 | Germany | TNSECURITY LTD |
| 8 | 195.133.13[.]231 | Russian Federation | JSC "RetnNet" |
| 9 | 94.100.180[.]31 | Russian Federation | LLC VK |
| 10 | 35.186.221[.]100 | United States | Google LLC |
| 11 | 76.223.67[.]189 | United States | Amazon.com, Inc. |
| 12 | 35.190.52[.]58 | United States | Google LLC |
| 13 | 111.10.231[.]151 | China | China Mobile Communications Group Co., Ltd. |
| 14 | 208.91.112[.]55 | United States | Fortinet Inc. |
| 15 | 92.60.39[.]76 | Germany | netcup GmbH |



08

# Putting Intel into Practice

# Proactive Defense Moves for a Secure Future

This section empowers you to transform intelligence into actionable steps, fortifying your defenses against the evolving threat landscape. Here's how:

**Strengthen Your Perimeter:**

- **Identify critical assets:** Align geo-targeting insights with your infrastructure footprint to prioritize protection efforts.
- **Refine industry-specific mitigation strategies:** Adapt existing security controls based on targeted industries in your sector.
- **Enhance threat actor monitoring:** Track activities of malicious actors linked to high-risk countries.

**Patch, Harden, Repeat:**

- **Patch promptly:** Prioritize patching critically exploited vulnerabilities, following vendor recommendations.
- **Harden configurations:** Implement security best practices to reduce attack surface vulnerabilities.
- **Conduct vulnerability assessments:** Regularly scan systems for emerging exposures and address them proactively.

**Shield Your Systems:**

- **Deploy endpoint protection:** Utilize endpoint detection and response (EDR) solutions to identify and mitigate malware infections.
- **Block malicious domains and URLs:** Leverage threat intelligence feeds and URL filtering solutions.
- **Educate users:** Train employees on phishing awareness and safe browsing practices.

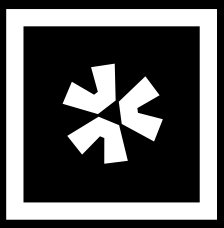
**Bolster Network Security:**

- **Implement IP reputation filtering:** Block traffic originating from known malicious IP addresses.
- **Monitor network activity:** Analyze logs for suspicious inbound and outbound traffic.
- **Strengthen firewall rules:** Refine access control lists to restrict inbound connections from high-risk countries or ISPs.

**Remember:**

- **Stay informed:** Continuously monitor evolving threats and update your defenses accordingly.
- **Prioritize based on risk:** Allocate resources strategically, focusing on vulnerabilities and threats most likely to impact your organization.
- **Invest in people and processes:** Empower your team with relevant training and implement robust security policies.

By applying these proactive measures, you can leverage threat intelligence to create a resilient security posture, proactively mitigating risks and securing your future.



# elixicode

Cybersecurity with innovation and creativity

www.elixicode.com

https://twitter.com/Elixicode
https://www.linkedin.com/company/elixicode
https://www.youtube.com/@Elixicode

PUBLIC