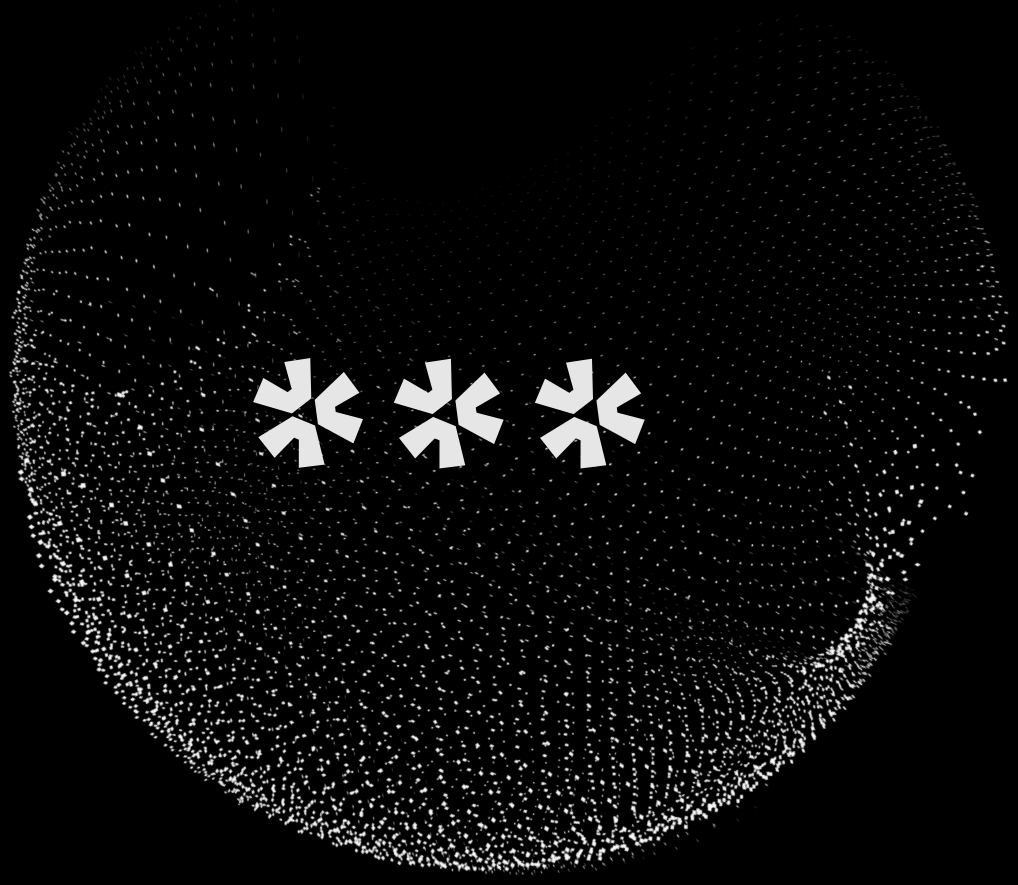
elixicode



11/06/2024

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

“

The threat landscape is a dynamic battlefield. Threat intelligence equips you with real-time insights to navigate this ever-changing terrain.

”

- Unknown

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.

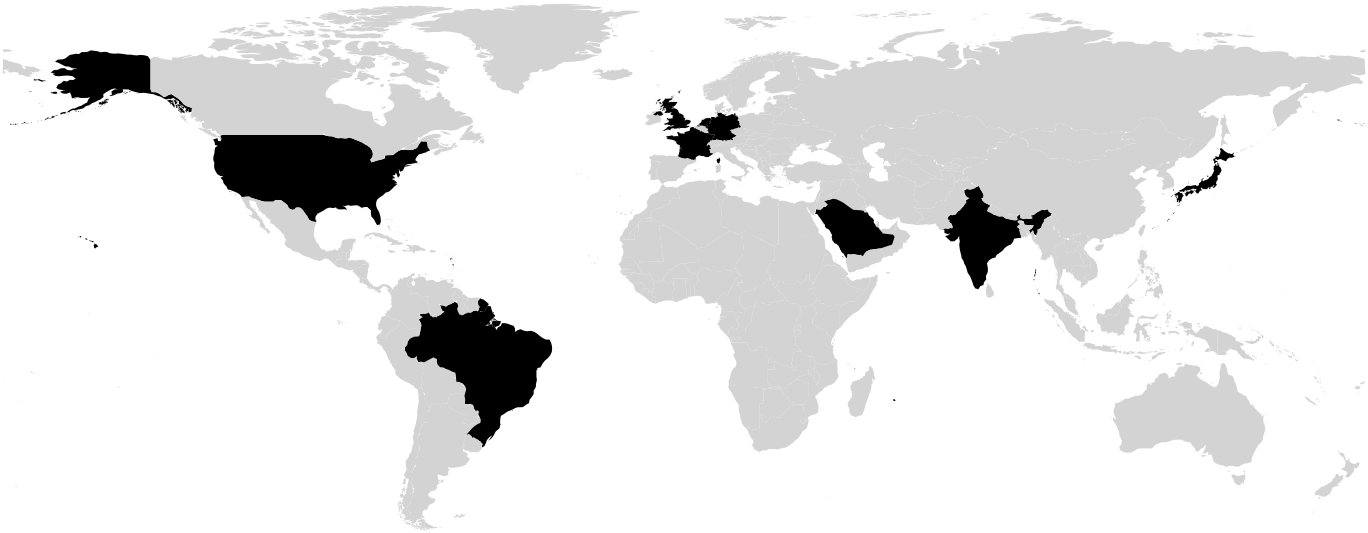
Join us on this journey of proactive security. Follow us on X and access your free weekly Threat Intel Report today!

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 **France**

3 **Germany**

4 **India**

5 **Japan**

6 **Brazil**

7 **United Kingdom**

8 **Saudi Arabia**

9 **Korea, Republic of**

10 **Netherlands**

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

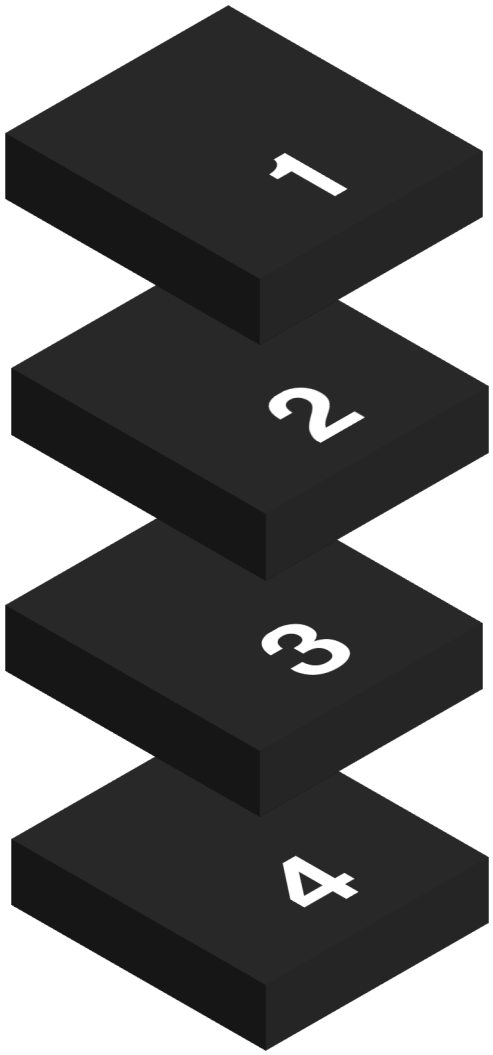
Communication

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

4

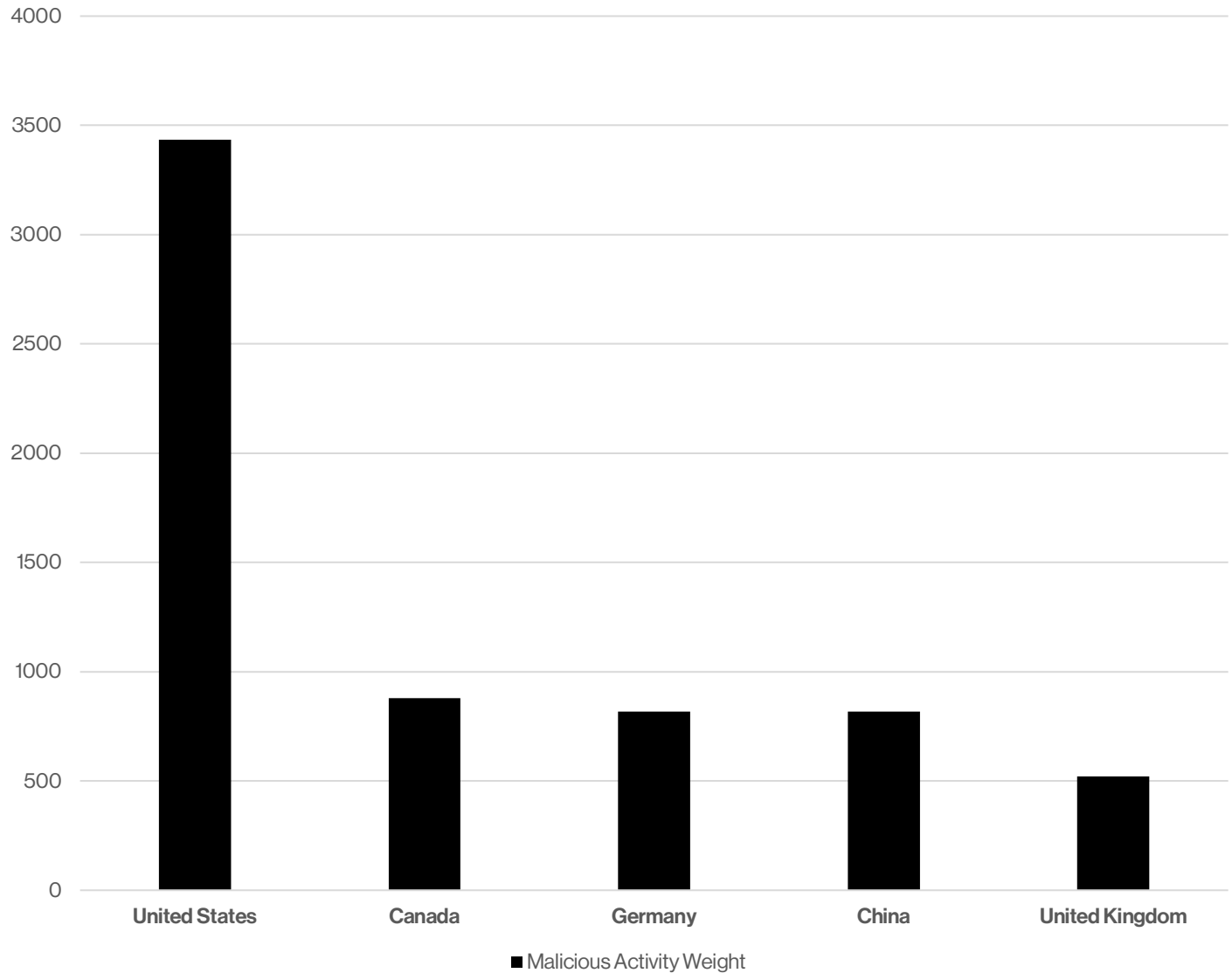
Government

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	**Snowflake Data Breach Impacts Ticketmaster and Other Organizations**
	Description	The access was possible because the demo account was not behind Okta or Multi-Factor Authentication (MFA), unlike Snowflake's corporate and production systems, the company said. In a separate knowledge base article, the company warned of "an increase in cyber threat activity targeting some of our customers' accounts", once again underlining that credential stuffing was to blame, and not a vulnerability, misconfiguration, or Snowflake system compromise. "Throughout the course of our ongoing investigation, we have promptly informed the limited number of customers who we believe may have been impacted," the company said.

2	Title	**Ticketmaster Confirms Data Breach**
	Description	Last Friday, Live Nation filed a data breach disclosure notice with the US Securities and Exchange Commission (SEC), noting that there was "unauthorized activity within a third-party cloud database environment containing company data" on May 20, and that "a criminal threat actor offered what it alleged to be company user data for sale via the Dark Web" on May 27. However, the events giant didn't confirm the mind-boggling number of records (560 million) that ShinyHunters claimed to have, nor did it reveal details on what type of data the breach contains.

3	Title	**Cryptojacking: 'Commando Cat' Cryptojacks Docker Containers**
	Description	An attack campaign named “Commando Cat” was observed abusing Docker remote API servers to deploy cryptocurrency miners. The naming of the campaign was used to signify the use of the Commando open-source project to deploy benign containers on demand.

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	**Ransomware Attack Hits London Hospitals**
	Description	A ransomware attack that hit pathology services provider Synnovis on Monday and impacted several major NHS hospitals in London has now been linked to the Qilin ransomware operation. Ciaran Martin, the inaugural CEO of the UK's National Cyber Security Centre (NCSC), said today that the Qilin gang is likely responsible for the incident. The attack has resulted in Synnovis being locked out of its systems and is causing ongoing service disruptions at Guy's and St Thomas' NHS Foundation Trust, King's College Hospital NHS Foundation Trust, and various primary care providers across south east London.
2	Title	**Frontier Communications Data Breach: 750K Customers Impacted**
	Description	However, the fact that it was forced to shut down its systems suggested that a ransomware group might have been responsible. This was confirmed on June 1, when the RansomHub ransomware gang added Frontier Communications to its Tor-based leak site, claiming the theft of 5GB of data, including the names, addresses, email addresses, dates of birth, phone numbers, and Social Security numbers of over two million people. According to a data breach notice filed by the company with the Maine Attorney General's Office this week, however, 751,895 individuals were affected by the incident.

3	Title	**TikTok Hack Targets 'High-Profile' Users Via DMs**
	Description	In January 2021, Check Point detailed a flaw in TikTok that could have potentially enabled an attacker to build a database of the app's users and their associated phone numbers for malicious future activity. Then in September 2022, Microsoft uncovered a one-click exploit affecting TikTok's Android app that could let attackers take over accounts when victims clicked on a specially crafted link. Another issue disclosed by Imperva over a year ago could have allowed attackers to monitor users' activity and access sensitive information on both mobile and desktop devices.

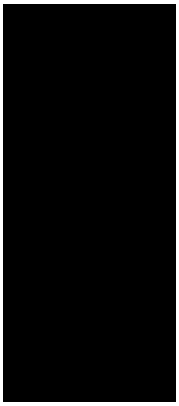
Must–Read Cybersecurity News

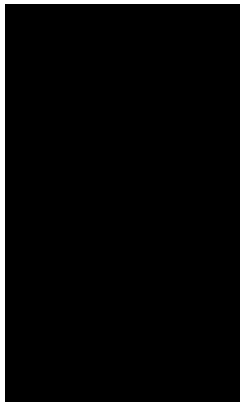
Staying ahead of the curve in cybersecurity demands constant vigilance. This section tackles the top 3 cybersecurity news stories currently dominating the headlines, ranked in descending order of their heat and potential impact.

1	Title	**TikTok Fixes Zero-Day Bug Used To Hijack High-Profile**
	Description	Over the past week, attackers have hijacked high-profile TikTok accounts belonging to multiple companies and celebrities, exploiting a zero-day vulnerability in the social media's direct messages feature. Zero-day vulnerabilities are security flaws with no official patch or public information detailing the underlying weakness. After being compromised, user accounts belonging to Sony, CNN, and others had to be taken down to prevent abuse.

2	Title	**Attacks Surge On Check Point VPN Zero-Day**
	Description	Check Point published an advisory regarding a critical vulnerability, CVE-2024-24919, which has since seen a surge in exploitation attempts. The vulnerability, rated with a CVSS score of 8.6, allows attackers to access sensitive information on the Security Gateway, potentially leading to lateral movement and domain admin privileges. CVE-2024-24919–involves sending a crafted POST request to the server, which runs as root.

3	Title	**Critical PHP Remote Code Execution Flaw Let Attackers Inject Malicious Script**
	Description	There are two scenarios of exploitation: running PHP under CGI mode and Exposing the PHP binary along with the

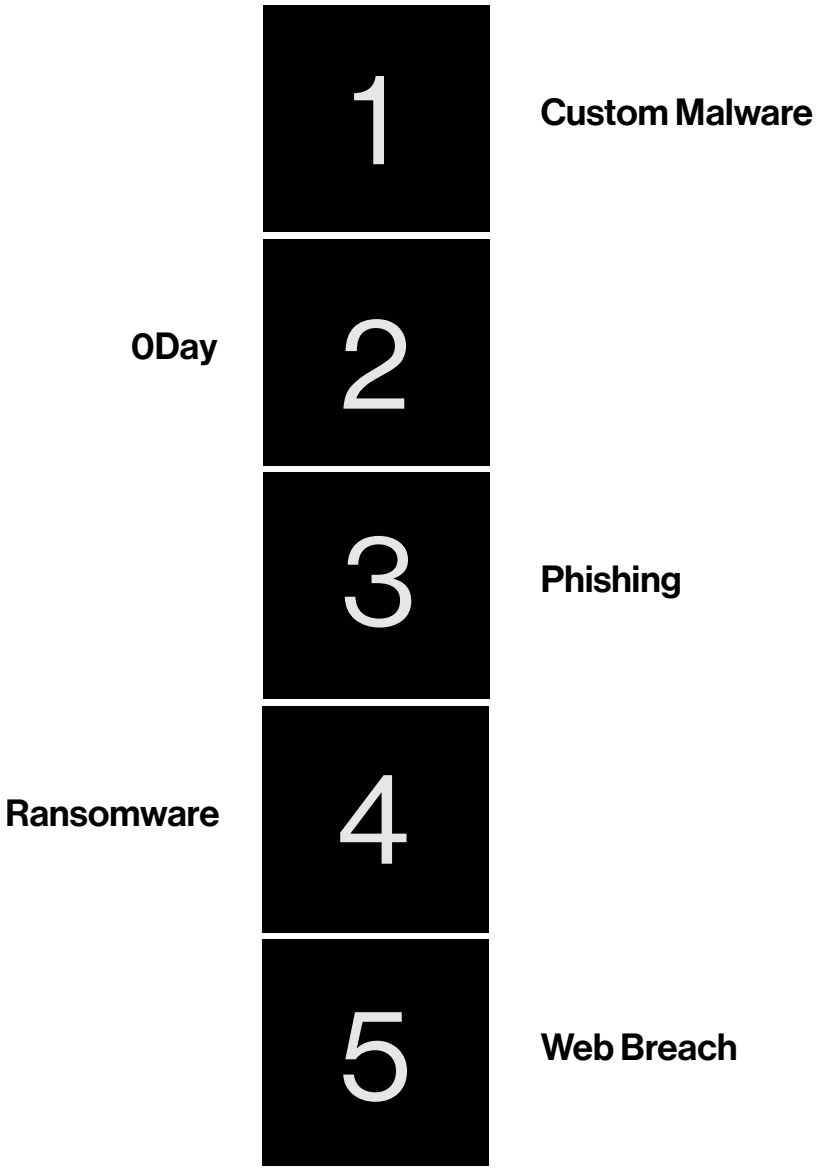




default XAMPP configuration. The first scenario of running PHP under CGI mode involves the configuring of the Action directive to map corresponding HTTP requests to a PHP-CGI executable binary in the Apache HTTP server. This exploitation scenario is direct and affects common configurations, which includes AddHandler cgi-script .phpAction cgi-script "/cgi-bin/php-cgi.exe"or FilesMatch ".php$"> SetHandler application/x-httpd-php-cgi

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	**TA0004**
	Tactic	**Privilege Escalation**
	Description	The adversary is trying to gain higher-level permissions.
	Reference	https://attack.mitre.org/tactics/TA0004/

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	**T1059**
	Sub-technique ID	**T1059.003**
	Technique	**Command and Scripting Interpreter**
	Sub-technique	**Windows Command Shell**
	Description	Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as SSH.
	Technique Reference	https://attack.mitre.org/techniques/T1059/
	Sub-technique Reference	https://attack.mitre.org/techniques/T1059/003/

2		
	Technique ID	**T1003**
	Sub-technique ID	**T1003.001**
	Technique	**OS Credential Dumping**
	Sub-technique	**LSASS Memory**
	Description	Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct Lateral Movement using Use Alternate Authentication Material.
	Technique Reference	https://attack.mitre.org/techniques/T1003/
	Sub-technique Reference	https://attack.mitre.org/techniques/T1003/001/

3		
	Technique ID	**T1021**
	Sub-technique ID	**T1021.001**
	Technique	**Remote Services**
	Sub-technique	**Remote Desktop Protocol**
	Description	Adversaries may use Valid Accounts to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user.
	Technique Reference	https://attack.mitre.org/techniques/T1021/
	Sub-technique Reference	https://attack.mitre.org/techniques/T1021/001/

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-2024-24919
Information disclosure on Check Point Security Gateway enabled with remote access VPN or Mobile Access Software Blades.

2

CVE-2018-20062
A vulnerability in VulNoneCms V1.3. which allows remote attackers to execute arbitrary PHP code via crafted use of the filter parameter.

3

CVE-2019-9082
A vulnerability in ThinkPHP before 3.2.4, as used in Open Source BMS v1.1.1 and other products, allows Remote Command Execution.

4

CVE-2024-21683
This High severity RCE (Remote Code Execution) vulnerability was introduced in version 5.2 of Confluence Data Center and Server.

5

CVE-2024-4577
In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, which may allow RCE.

6

CVE-2024-37364
Ariane Allegro Scenario Player through 2024-03-05, allows physically proximate attackers to obtain sensitive information.

Exploitation Prevalence

7.9%	4.7%	4.7%	4.7%	3.9%	3.9%
CVE-2024-24919	**CVE-2018-20062**	**CVE-2019-9082**	**CVE-2024-21683**	**CVE-2024-4577**	**CVE-2024-37364**

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. banker
3. AgentTesla
4. Mirai
5. Remcos
6. WannaCry
7. GuLoader
8. AsyncRAT
9. PureLogStealer
10. XWorm

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	Spyware
4	Stealer
5	Evasion
6	Trojan
7	Discovery
8	Ransomware
9	Miner
10	Backdoor

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.

	unknown.exe
	XClient.exe
	build.exe
	Request for Quotation (RFQ#196).zip

Top 5 Most Common Malware Extensions

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

1010 1010	.exe
1010 1010	.pdf
1010 1010	.bin
1010 1010	.zip
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.

	.2.exe
	.bat.exe
	.pdf.exe
	.scr.exe
	.1.zip
	.xlam.xlsx
	.0.exe
	.1.exe
	.5.exe
	.exe.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	N/A
	Malware Type	Miner
	MD5	223fcf873dd157649dc30053926e4aeb
	SHA1	1370b553d2046ce4b4ad48f34f39ca9af57e246b
	SHA256	2712cfc84e57a8c2c3637bc69d65c1741fcb7a600c78709bbe3d47c5f76a4293

2	Malware Family	WannaCry
	Malware Type	Trojan
	MD5	d69dc6569b385c0467185d002e252d89
	SHA1	25938a66cce0078c76a15f351cbd19c8fcc2b081
	SHA256	80239619c4ca44380c6269873a5b6b695585ccfcf278e0f2c72698658a3a6fd8

3	Malware Family	N/A
	Malware Type	Dropper
	MD5	013144b4ec92ddbec4d81f8e4bc6ff29
	SHA1	9f43a3450f8193c67e07793e97abd244d3d0e3af
	SHA256	2e3698eac0e8a7fa4feb3ab475ead44a198096052edbf9f83d9a304bc4a502b7

4	Malware Family	N/A
	Malware Type	N/A
	MD5	7fe352e22b099ffe1f308a9786e14a8d
	SHA1	31d06e58776725a2698b08a51c2868d6fc3cc461
	SHA256	fd01c4cc2bafdaae4201afa6e288a744b006997f3c13ab621d4102d563e05882

5	Malware Family	Emotet
	Malware Type	BOT
	MD5	f260e94242a6c9382eb754912c8f04d2
	SHA1	d1509589aa404f8a9d7e058389d995639d064aa2
	SHA256	36201d4f760ade0fc6de622e4ca9598f126798fa2f06bff9826e89248efb0adc

6	Malware Family	AgentTesla
	Malware Type	Loader
	MD5	cb95734e59b6b649c53ebae76634a05c
	SHA1	2211f611f66a45c94079c99d9e43bf9c1309c498
	SHA256	73c5c4b12646631dbf1e8adf10b52b8635b34d02d753d3fe829bd41210f547f0

7	Malware Family	N/A
	Malware Type	N/A
	MD5	69f76735b9213bdaf23b6b9e4c2c1934
	SHA1	9fb40afe1ab8879fe6bb34c92d8c8fec8c7612e9
	SHA256	05667aebb491a808847858de4af20b4798d23f17fc82084b8f6dd05e2643b44e

8	Malware Family	Kovter
	Malware Type	Trojan
	MD5	b44a8dbe40cf3d75a23d5b991246249b
	SHA1	78f70912abd3599935dd15d12428b41bee81e452
	SHA256	e93ea2c9e689a35ef77e597a4cf34409f9c02dd74790716eae060304995d6289

9	Malware Family	PrivateLoader
	Malware Type	Dropper
	MD5	4ecac60bcb0ebc8f268ea8cae2cc46ec
	SHA1	0e0f083c10b3a828bff4b90c3f62d3f292691f99
	SHA256	7aa2680b83656ff7cbfe453c3b0e9b874cbe9b8b0d19ff26317b35672f8405d6

05

Domains Briefing

PUBLIC

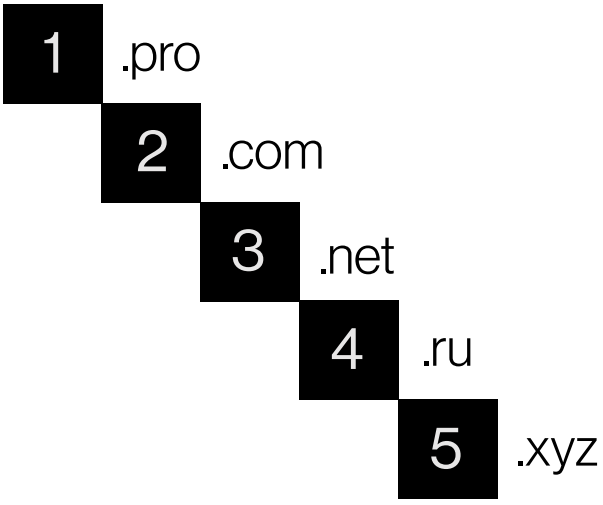
Top 5 Malicious Domains to Avoid at All Costs

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	nnfems[.]com	GoDaddy.com, LLC
2	www.pentagrid[.]ch	N/A
3	url.us.m.mimecastprotect[.]com	MarkMonitor, Inc.
4	censys[.]com	Cloudflare, Inc.
5	eumostwanted[.]eu	Easy by Europlanet

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
pricekaboom[.]com	pickaboo.com
universalmovies[.]top	universalmovies.it
shopnow321[.]online	shopno1.online
innovativebuildingsolutions[.]in	innovatebuildingsolutions.com
atjehupdate[.]com	athomupdate.com
www.mermod[.]swiss	mso.swiss
qr-in[.]com	qrinc.com
carliente[.]com	charlieintel.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://u44898889.ct.sendgrid[.]net/ls/click?upn=u001.iNlWQGPxkAjLQcVbcGEDqmFkVRmKvyDAEqnwMo6hHjmnm0gMV8suMSwHduUnR5ZUfDILsRCgY2qMOzozibTAG5wiP2httt-2FRJrEmsQ8C70YaUC9YQ-2FPW3X7ADBv1sttWGiwlBsgqiRGKJ4abHG4W39MJCAM7QQWpc7H3toVpQQlmebg5IKA9TAgknzmnr-2F36zTwGwjDgiO0221FvRYrwJpAsXZqdDF18OFE1WDU95FTQgu1BotbXE3OFGBkUXwVDurWx_yRTbqPeWhJT-2FNHFsn9pSpbpVyrasoLyq3JkD8aHr2dk7NpDjl0E9KE6pMnsYzAtXmik3zZ8yt79QEFr1s3Be-2FoeIPx-2FRJ1ly3l38XALiJCpWhvPqZ4cSPIeA3ZSQy9t5HsOdNiBU6Px6Lwu6-2FlYhfpMWd2yoD27KBxAQU7TQEP9kndCOQMBn4QtqK0wogOE4k1YqNUTrz6r-2BZ8-2FDfCEAg0Yh1zrgh2exabL2egc4MP7MYf9ut6RGLmmRXJKVfki-2FYUPWBk9SO9P1E-2BaqLpl5qJYvDN2JLBKK6h7J-2FPoPqHBY-2F7HQSuFSzNqWvQjYMcaeBJDUCDHmuvApb7AM1zWcPD1t22p9eOq2Ek-2FL9gy40v9ZUFG70MlVj-2FC5Cei5te5eLF-2B2wc-2BV3gJOIhX718LcI7Oia16bAmU-2FkiYFRR1Khu-2F9do09-2BbwpIRDzGyV-2FmkyexRsSGV-2FOcbzTHtqzPHQ9npXgc5sEdISNzkmhn29Nr9GS2f-2BE9G1uNPKx-2BhvwciZVN0J84pwZKoECQWZ9uYJN8k1WadqOChAy5jf98ZvirHyBNeyhmA029j90ZFysFZ3Ltz8-2BXvmr1xOM-2Fx9EA-2F0Y0ftR2UkbQol3mYLIVrJpNyIu3tKag4GKcg4WrgE0xTWB-2BOkGvipSmA-2F6xEFwirIRq3YNlJXn74ZQzKES1kQJ4XDf0I8V-2BZ-2FINux4DCKU2lLa-2FBKs4Rxa9Z0PFz3JtTZ6KDdHjuiASC5vgAa2uCoxVuJQGxSBPDkbNvFPw-2Frg53bwKmTGC-2B9zHAjSU-2Fs9Bu-2F-2BFsFgpPDepWO06QgQ-2BmRHTzdtEvCUPDjyzApP-

	2BTJIcpTIrXVzPtZUUAX7sfYhnywsZ6uyrv65HOAJFfCI1jPRpMwAKcf45w0v72-2Bb-2FJS6r6n7
3	http://ln[.]run/qDLvL
4	https://www.partner-ads[.]com/dk/klikbanner.php?partnerid=8112&bannerid=34504&htmlurl=https://goo.su/kpPKg
5	https://tracking.vipacademia[.]com/tracking/click?d=QK6KMFYOU_Jl56p_h16egEGM-1g9zCxDVHrhC86SPZrQmSj0KnV1uaZxc7z9LuEiLHtCQOC9FJ1hxmXl5P3ZeV5RLeQGwltMRr05tv5wl4AvMV7BcdQycq6l-Mg-zJ5y3lR-hE7UCBuOAH-PKTcX39cvMWFQQ-beP6HtNTTo9AiRFvmeGoFHE9U9hGGSUePO_5PLoQqvVFiJ8bAt9B_IsqO1HWbXEascE_HmF0URkd2MaMG7OqnPpuxsl2l_tVdHtA2

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	39.4%

2	Hosting Provider	Amazon.com, Inc.
	Hosting Location	United States
	Activity Weight	20.0%

3	Hosting Provider	Google LLC
	Hosting Location	United States
	Activity Weight	14.3%

4	Hosting Provider	Cloudflare, Inc.
	Hosting Location	Canada
	Activity Weight	11.7%

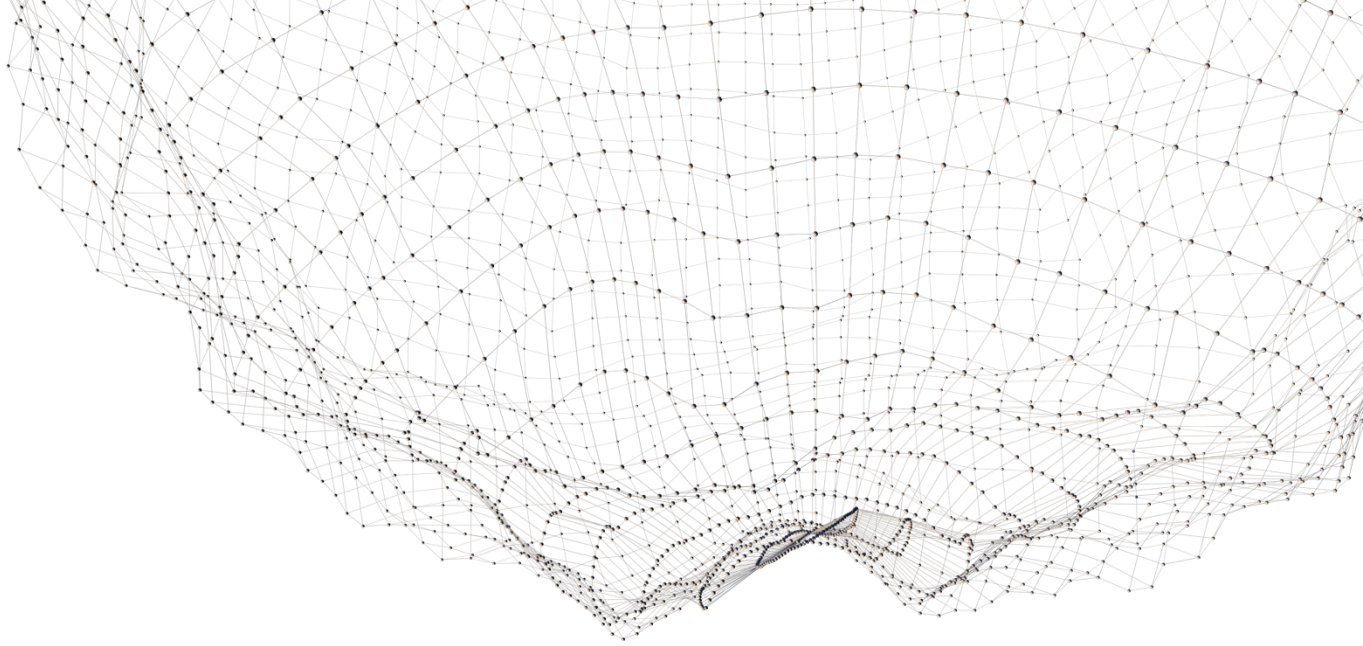
07

IP Address Briefing

Top 13 Malicious IP Addresses

Knowledge is power in the fight against cybercrime! This section exposes the top 13 malicious IP addresses currently posing a significant threat, ranked by their prevalence and malicious activity.

#	IP Address	Country	ISP
1	91.189.91[.]42	United States	Canonical Group Limited
2	91.189.91[.]43	United States	Canonical Group Limited
3	149.154.167[.]99	United Kingdom	Telegram Messenger Inc
4	185.125.190[.]26	United Kingdom	Canonical Group Limited
5	34.149.87[.]45	United States	Google LLC
6	89.105.201[.]183	Netherlands	NovoServe B.V.
7	116.202.190[.]18	Germany	Hetzner Online GmbH
8	103.149.87[.]198	Cambodia	4S TECHNOLOGY TRADING SERVICES COMPANY LIMITED
9	93.123.39[.]193	Bulgaria	Sircrosar Limited
10	77.91.77[.]122	Germany	WAIcore Hosting LTD.
11	117.220.144[.]68	India	National Internet Backbone
12	77.91.77[.]81	Germany	WAIcore Hosting LTD.
13	94.232.249[.]46	Syrian Arab Republic	Syrian Telecommunication Private Closed Joint Stock Company



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.

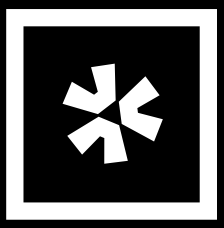
Bolster Network Security:

- **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