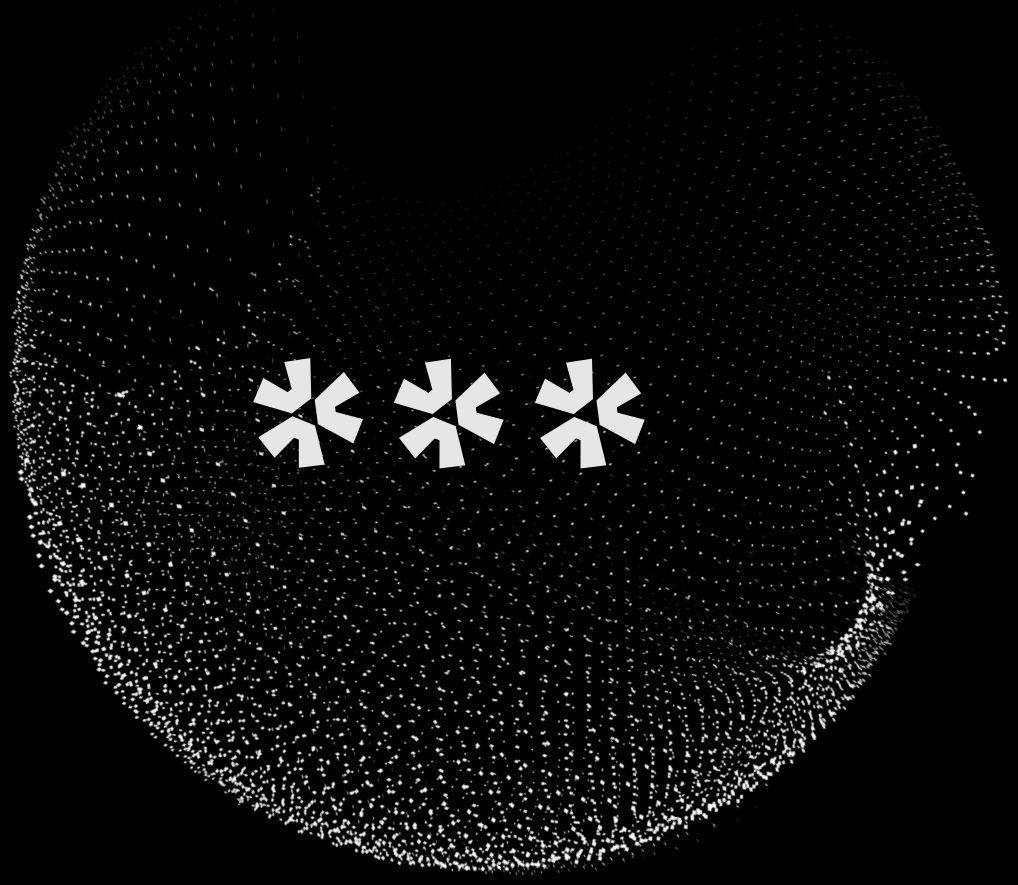
elixicode



20/05/2024

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.

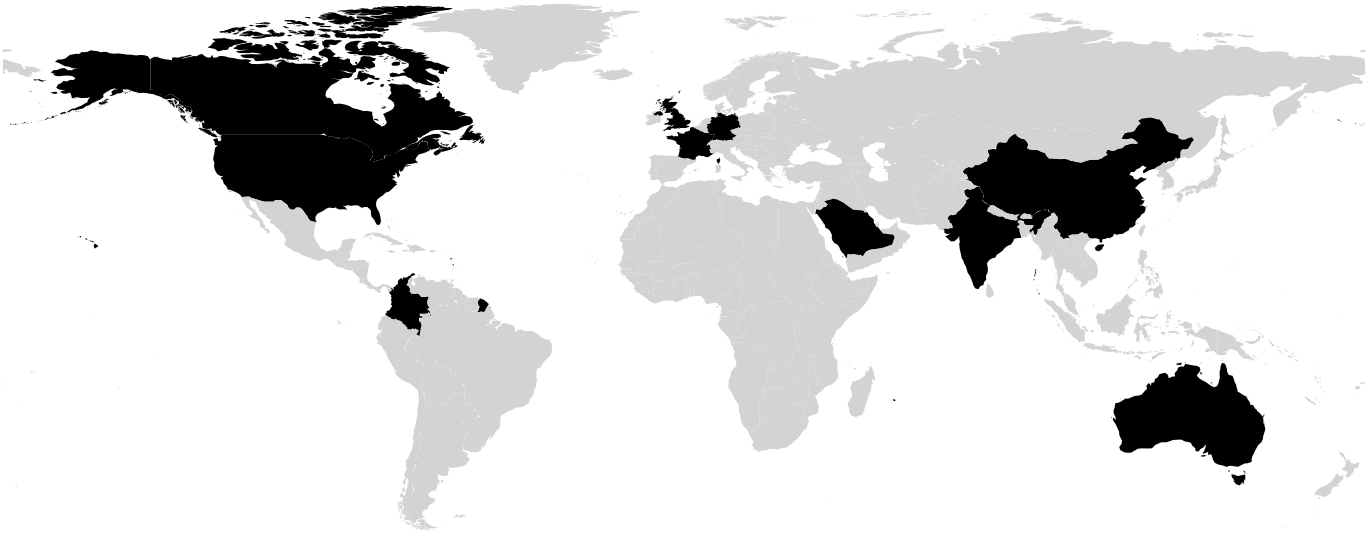
Join us on this journey of proactive security. Follow us on X and access your free weekly Threat Intel Report today!

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

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

Government

Classified intel exposed, public trust undermined through disinformation campaigns.

3

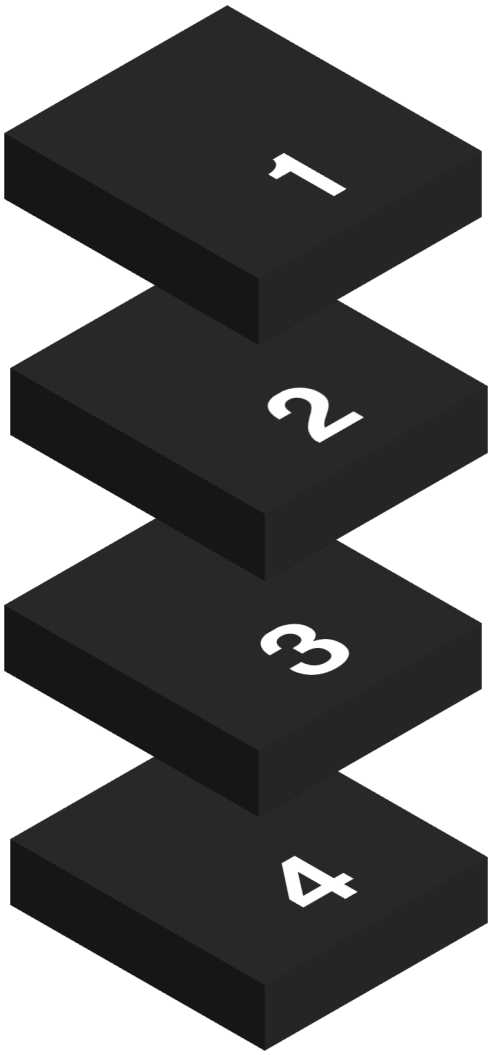
Finance and insurance

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

4

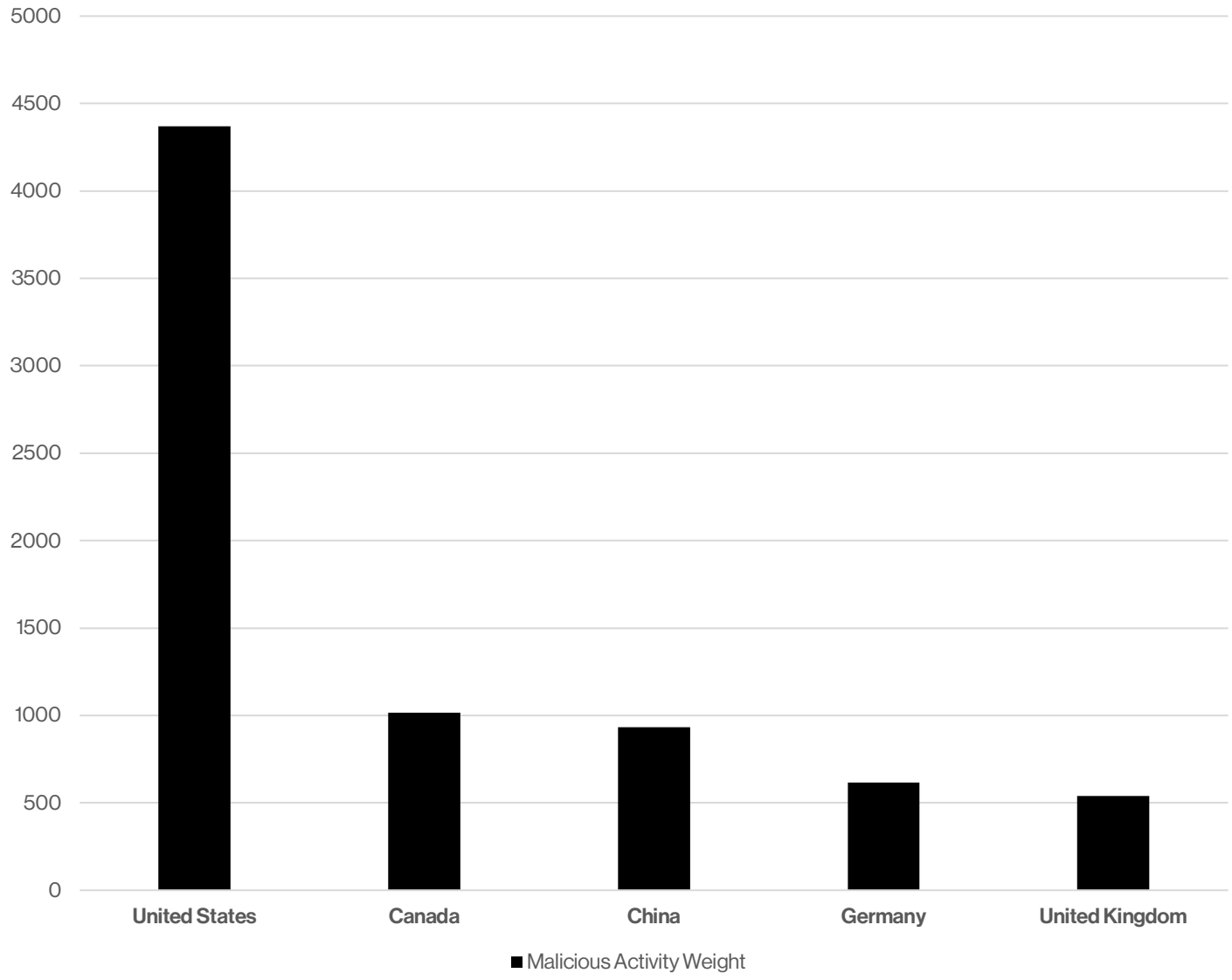
Communication

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



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	**Nissan Data Breach Impacts 53,000 Employees**
	Description	Nissan notes that it is not aware of the exposed data having been misused. To mitigate the risk of this data exposure, though, Nissan enclosed instructions for letter recipients on how they can enroll in a free-of-charge 24-month credit monitoring and identity theft protection service through Experian. Nissan has been the target of several security incidents over the past few years, which affected various divisions of the Japanese car manufacturer. In early December 2023, Nissan Oceania (Australia and New Zealand) announced an investigation into a cyberattack and potential data breach.

2	Title	**Black Basta Ransomware Strikes 500+ Organizations Worldwide**
	Description	CISA and the FBI said that Black Basta ransomware affiliates breached over 500 organizations between April 2022 and May 2024. In a joint report published in collaboration with the Department of Health and Human Services (HHS) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), the two federal agencies added that the gang also encrypted and stole data from at least 12 out of 16 critical infrastructure sectors.

3	Title	**BreachForums Seized Once Again, What Is Next?**
	Description	On March 21, 2023, the new administrator announced the decision to shut BreachForums down. Another forum administrator going by the name "Baphomet" then took over. According to BleepingComputer, the FBI has also seized the site's Telegram channel, with law enforcement sending messages to the channel on behalf of the forum's operator "Baphomet". BreachForums was in use just last week for a big name breach when a cybercriminal put up for sale breached customer data taken from Dell between 2017-2024.

Top 2 Attacks Shaking the Headlines

Navigating the ever-changing landscape of cyber threats can be overwhelming. This section dissects the top 2 cyber-attacks currently captivating the news, ranked in descending order of recency and potential impact.

1	Title	**Sugargh0St Rat Attacking Organizations & Individuals In Ai Research**
	Description	The operation, linked to a threat cluster known as UNK_SweetSpecter, went after businesses, universities, and government agencies. Attack Method: Emails with AI-themed baitUNK_SweetSpecter's campaign in May 2024 used a free email account to send emails with AI-themed traps to people who might be victims.

2	Title	**Windows Quick Assist Abused In Black Basta Ransomware Attacks**
	Description	In most of the observed batch script variations, the credentials are immediately exfiltrated to the threat actor's server via a Secure Copy command (SCP)," Rapid7 added. "In at least one other observed script variant, credentials are saved to an archive and must be manually retrieved." To block these social engineering attacks, Microsoft advises network defenders to block or uninstall Quick Assist and similar remote monitoring and management tools if they're not used and to train employees to recognize tech support scams. Those targeted in these attacks should only allow others to connect to their device if they contacted their IT support personnel or Microsoft Support.

Must-Read Cybersecurity News

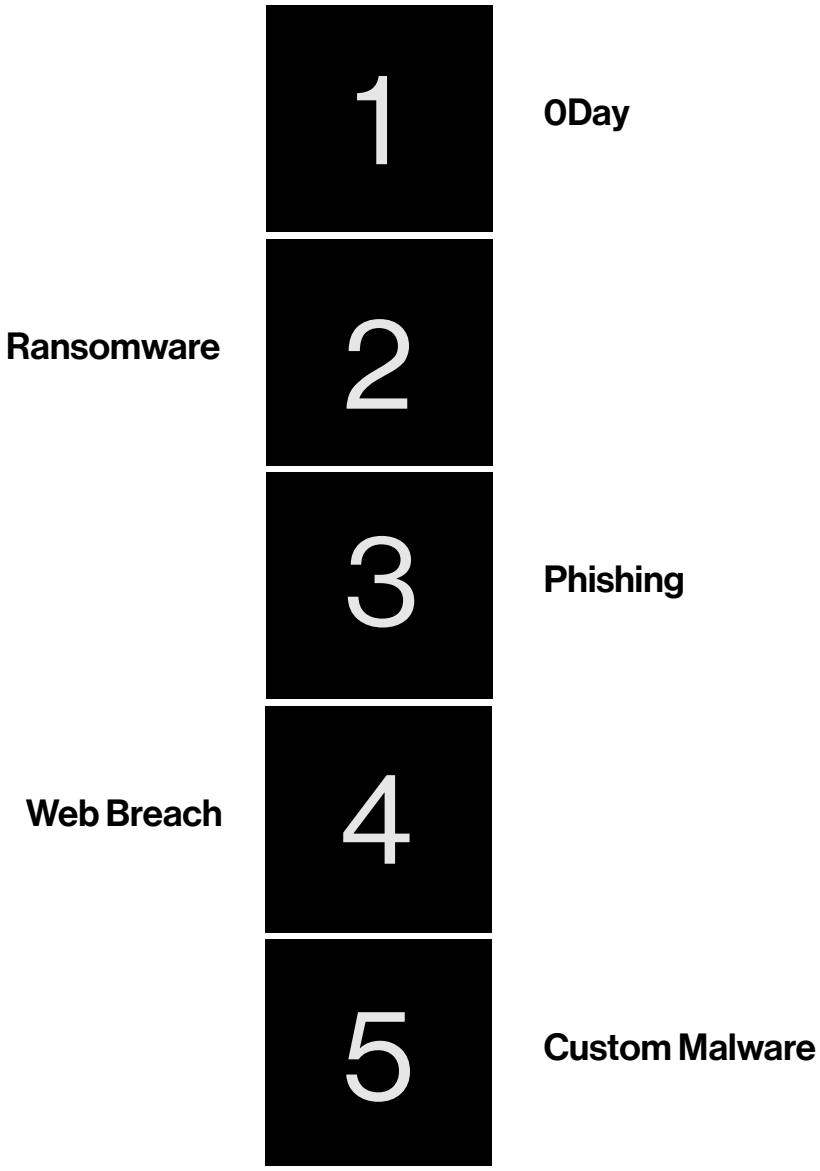
Staying ahead of the curve in cybersecurity demands constant vigilance. This section tackles the top 2 cybersecurity news stories currently dominating the headlines, ranked in descending order of their heat and potential impact.

1	Title	**Mozilla Thunderbird: Security Vulnerabilities Fixed In Thunderbird 115.11**
	Description	• CVE-2024-4769 • CVE-2024-4777 • CVE-2024-4767 • CVE-2024-4767

2	Title	**Ebury Botnet Infects 400,000 Linux Servers**
	Description	"When the known_hosts file contains hashed information, the perpetrators try to brute force its content," reads ESET's detailed report."Out of 4.8 million known_hosts entries collected by Ebury operators, about two million had their hostname hashed. 40% (about 800,000) of those hashed hostnames were guessed or brute forced. ", and where possible, the attackers may also exploit known vulnerabilities in the software running on the servers to gain further access or elevate their privileges.

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	**TA0008**
	Tactic	**Lateral Movement**
	Description	The adversary is trying to move through your environment.
	Reference	https://attack.mitre.org/tactics/TA0008/

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	**T1204**
	Sub-technique ID	**T1204.002**
	Technique	**User Execution**
	Sub-technique	**Malicious File**
	Description	An adversary may rely upon a user opening a malicious file in order to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. This user action will typically be observed as follow-on behavior from Spearphishing Attachment. Adversaries may use several types of files that require a user to execute them, including .doc, .pdf, .xls, .rtf, .scr, .exe, .lnk, .pif, and .cpl.
	Technique Reference	https://attack.mitre.org/techniques/T1204/
	Sub-technique Reference	https://attack.mitre.org/techniques/T1204/002/

2		
	Technique ID	**T1106**
	Sub-technique ID	**N/A**
	Technique	**Native API**
	Sub-technique	**N/A**
	Description	Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations.
	Technique Reference	https://attack.mitre.org/techniques/T1106/
	Sub-technique Reference	N/A

3		
	Technique ID	**T1140**
	Sub-technique ID	**N/A**
	Technique	**Deobfuscate/Decode Files or Information**
	Sub-technique	**N/A**
	Description	Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system.
	Technique Reference	https://attack.mitre.org/techniques/T1140/
	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-2024-4761
Out of bounds write in V8 in Google Chrome prior to 124.0.6367.207 via a crafted HTML page.

2

CVE-2024-4671
Use after free in Visuals in Google Chrome prior to 124.0.6367.201 potentially allowing a sandbox escape via a crafted HTML page.

3

CVE-2024-30051
Windows DWM Core Library Elevation of Privilege Vulnerability.

4

CVE-2024-30040
Windows MSHTML Platform Security Feature Bypass Vulnerability.

5

CVE-2024-4947
Type Confusion in V8 in Google Chrome prior to 125.0.6422.60 that allows for RCE within a sandbox via a crafted HTML page.

6

CVE-2024-30044
Microsoft SharePoint Server Remote Code Execution Vulnerability.

Exploitation Prevalence

4.2%	4.0%	3.5%	3.3%	2.6%	2.0%
CVE-2024-4761	**CVE-2024-4671**	**CVE-2024-30051**	**CVE-2024-30040**	**CVE-2024-4947**	**CVE-2024-30044**

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. PureLogStealer
4. Mirai
5. Remcos
6. GuLoader
7. WannaCry
8. AsyncRAT
9. FormBook
10. RisePro

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

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.

	asih.exe
	launcher.exe
	freeflag.docm

Top 5 Most Common Malware Extensions

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

1010 1010	.exe
1010 1010	.zip
1010 1010	.pdf
1010 1010	.elf
1010 1010	.xls

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
	.pdf.exe
	.scr.exe
	.0.exe
	.xla.xlsx
	.bat.exe
	.6.exe
	.doc.rtf
	.1.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	Ransomware
	MD5	b89051e8cf348e69c0943b540af3b99c
	SHA1	50200e338cb5df75077c6144884bf0ff6bf7cc7a
	SHA256	2e0a0e7e5d510f4274cd22ca2ed10f4bcca932a8cb2a756a47c13fb36a5fb58d

2	Malware Family	Meterpreter
	Malware Type	Backdoor
	MD5	f427a819c67044acdf8f414120b812c5
	SHA1	cf529be783bded68cf3daa09aba68a07a27b9f9f
	SHA256	fba8b4330afcb3f4639c70af022ee87152270e417a2e34600f87376da01dec16

3	Malware Family	GootLoader
	Malware Type	Loader
	MD5	54ec9e1d29608f6d5e3090e90ac38a15
	SHA1	06e376d1778623aafa5ffec261b8e8be10a48ddd
	SHA256	a23dd0d4665be9c9064bfd377abd005651c1cdb9238c8d798283ac9caa638f91

4	Malware Family	N/A
	Malware Type	Trojan
	MD5	d9f38d365b7710b2ce6f5110ab51b090
	SHA1	a99bf69be60de3a70a52863832b2a3e6a49d1da4
	SHA256	2ec6ee841febd37853ac022b3b06f587cf4dd7fdbf2f5d3932122a9715218790

5	Malware Family	N/A
	Malware Type	Dropper
	MD5	c3c51348ef1eda5bfeff8f37caf6d9bd
	SHA1	088ae0858d9c3cfebccd68d9efc308add9de5e08
	SHA256	dce7ae032573aebe5bb028531c1e92d4f4c2428127720c699262421e3adcb431

6	Malware Family	N/A
	Malware Type	Dropper
	MD5	9b163fdc7af0bd5f7c265c25073823ea
	SHA1	a1617b652f24afb7b037da2047736126dc02c59a
	SHA256	94c67f62bb61c23330e28207f1fb8bc390da0b4caa0e217cf201a505c8c81a0c

7	Malware Family	BlackSuit
	Malware Type	Ransomware
	MD5	e3b085bf28df48a7a6dd82951c3fc230
	SHA1	d97c2076e1631e8e9d700956ed6c572eb06e128d
	SHA256	22c923e3278b0a1df89b782cebb153d66204f2aa51a0e89a36e2de21fa25afc5

8	Malware Family	CobaltStrike
	Malware Type	RAT
	MD5	4ea278e24ead1d95ebe3e2751b29a83e
	SHA1	6a59659d489e228da7625a8e85fd207fe72d7134
	SHA256	9f30efab15c2b9c9261f1204c9cf62ae8d017dc498a2b1ea5ae6e96619ee0283

9	Malware Family	N/A
	Malware Type	Dropper
	MD5	1ebed34934afd950c8861ecc0a65f866
	SHA1	d5e4f3762932a6a388b4eb35c70a0333f21165ea
	SHA256	41644ece96af2c710a353ce39a500929a87b96182e2d0e0cf0bde6fc27f554bb

05

Domains Briefing

PUBLIC

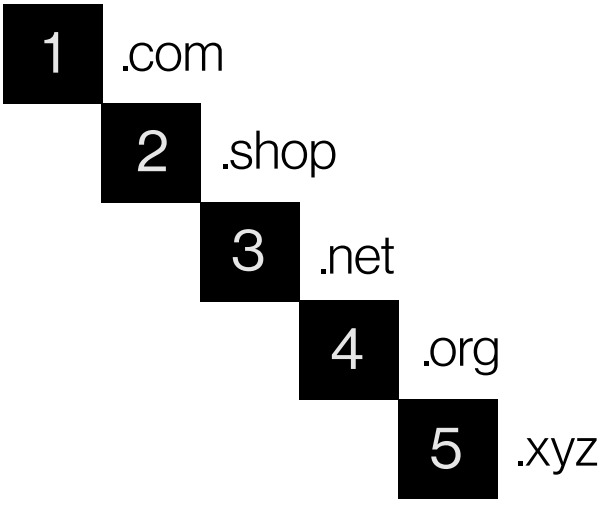
Top 5 Malicious Domains to Avoid at All Costs

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	dokdo[.]in	Uniregistrar Corp
2	url.us.m.mimecastprotect[.]com	MarkMonitor, Inc.
3	bitly[.]cx	CentralNic Ltd
4	www.amera.co[.]uk	123-Reg Limited t/a 123-reg
5	tezadlar[.]az	N/A

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
twomancake[.]com	twomance.com
breachforums[.]st	breachforums.vc
pasted[.]to	paste.to
qeintechnologies[.]com	qttechnologies.com
www.gattosat[.]icu	g-tst.icu
kino2[.]top	kinox.top
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	http://geoplugin[.]net/json.gp
3	https://assets-usa.mkt.dynamics[.]com/fc8d85f7-6213-ef11-9f85-00224832232e/digitalassets/standaloneforms/469b3461-6b13-ef11-9f88-7c1e5213cab3
4	https://atom-distinct-glazer.glitch[.]me/#aW5mb0BhamlsLmNvbQ==
5	https://bonzi-buddy.updatestar[.]com/en

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	34.1%

2	Hosting Provider	Amazon.com, Inc.
	Hosting Location	United States
	Activity Weight	23.3%

3	Hosting Provider	Microsoft Corporation
	Hosting Location	United Arab Emirates
	Activity Weight	16.4%

4	Hosting Provider	Cloudflare, Inc.
	Hosting Location	Canada
	Activity Weight	13.0%

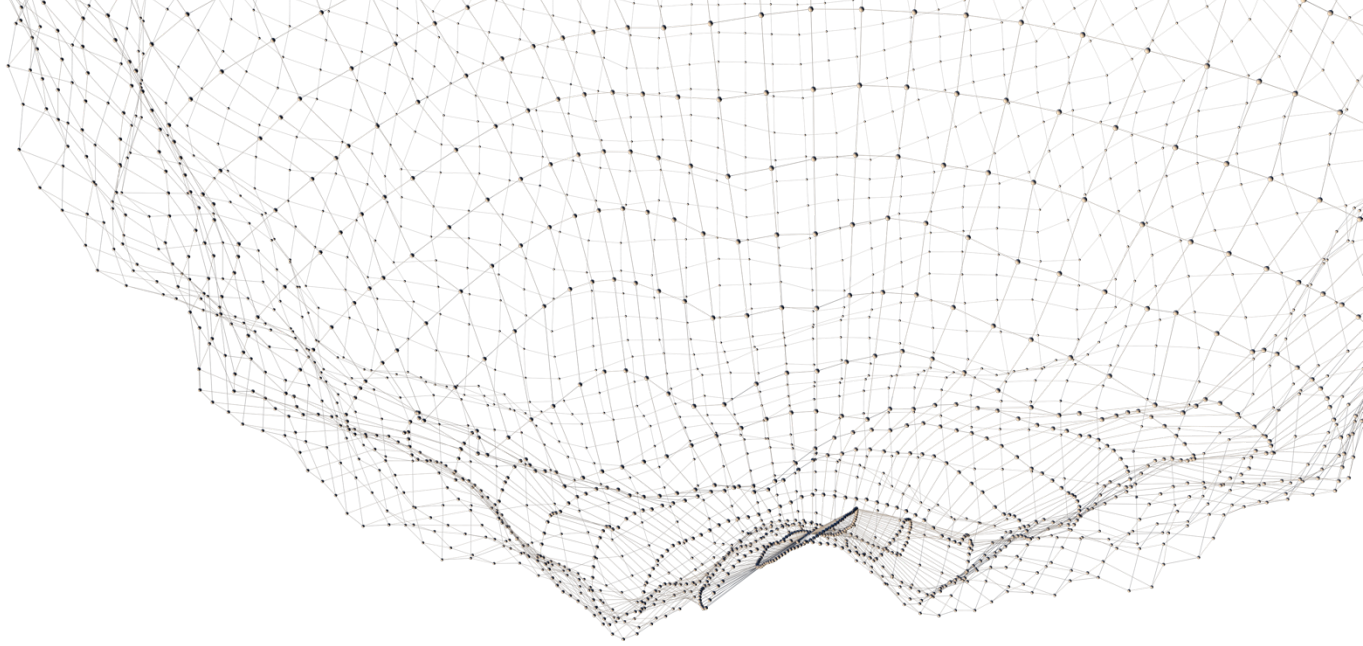
07

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	3.33.130[.]190	Canada	Amazon.com, Inc.
2	199.59.243[.]225	United States	Amazon.com, Inc.
3	76.223.67[.]189	United States	Amazon.com, Inc.
4	185.234.216[.]64	Russian Federation	Chang Way Technologies Co. Limited
5	159.89.102[.]253	Germany	DigitalOcean, LLC
6	103.235.46[.]40	Hong Kong	Beijing Baidu Netcom Science and Technology Co., Ltd.
7	45.141.85[.]179	Russian Federation	Media Land LLC
8	85.107.228[.]217	Türkiye	Turk Telekomunikasyon Anonim Sirketi
9	92.205.15[.]157	Germany	Host Europe GmbH
10	94.156.8[.]244	Türkiye	SUNUCUN BILGI ILETISIM TEKNOLOJILERI VE TICARET LIMITED SIRKETI
11	185.241.208[.]23	Germany	1337 Services GmbH
12	206.238.196[.]53	Singapore	N/A
13	147.45.47[.]115	Russian Federation	Karina Rashkovska
14	171.38.43[.]209	China	CHINA UNICOM China169 Backbone
15	193.17.183[.]196	Spain	NEAR IP, S.L.



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.

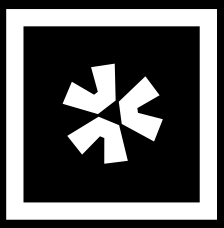
Bolster Network Security:

- **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