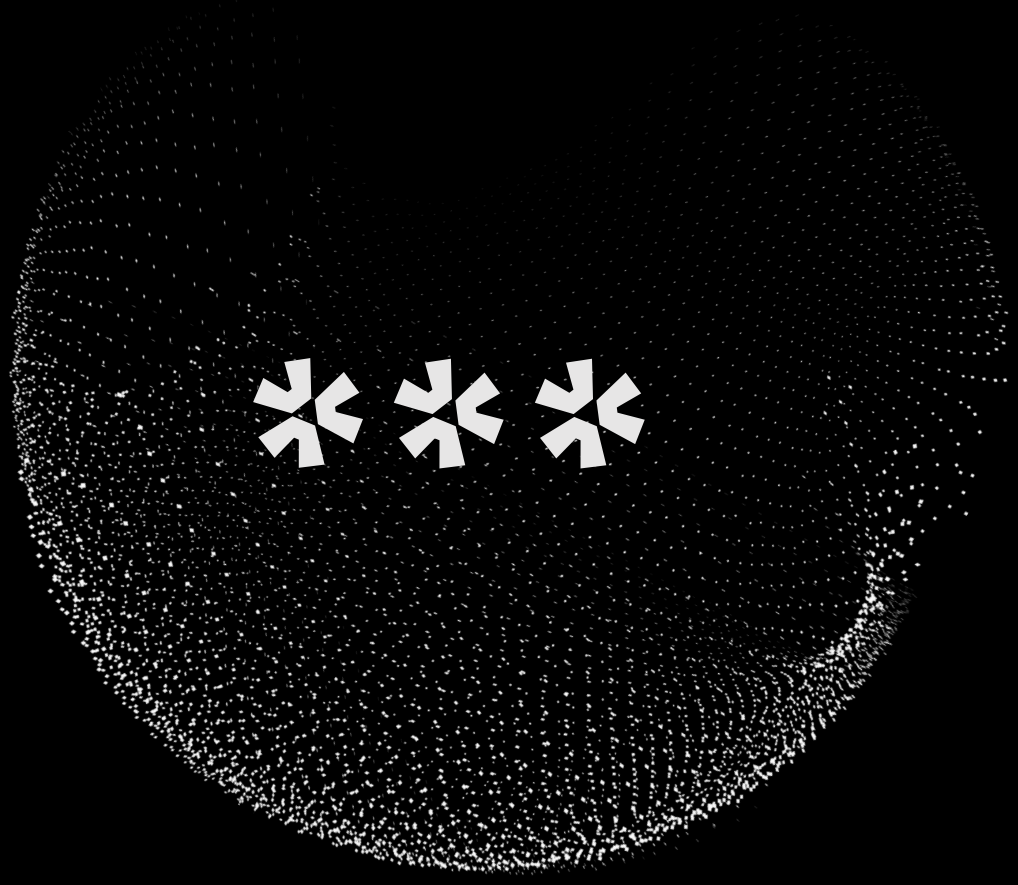
elixicode



28/05/2024

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

PUBLIC

“

Threat intelligence is an underutilized weapon in the fight against cybercrime. Its full potential is yet to be realized.

”

- World Economic Forum

PUBLIC

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!

PUBLIC

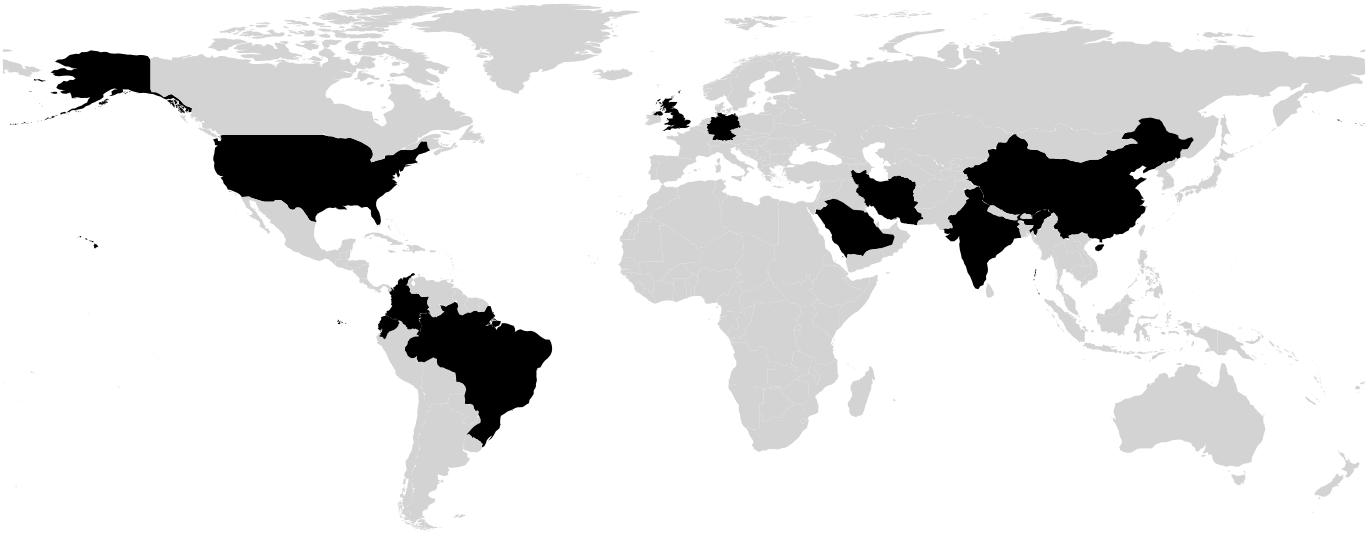
01

Geopolitical Briefing

PUBLIC

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. **China**
4. **Saudi Arabia**
5. **Iran**
6. **India**
7. **Colombia**
8. **United Kingdom**
9. **Brazil**
10. **Ecuador**

PUBLIC

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

Government

Classified intel exposed, public trust undermined through disinformation campaigns.

2

Technology

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

3

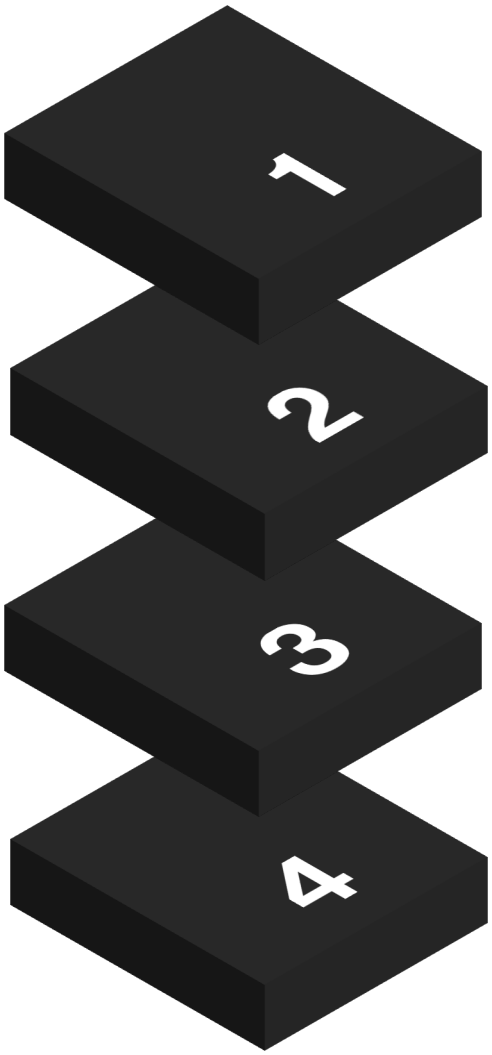
Finance and insurance

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

4

Communication

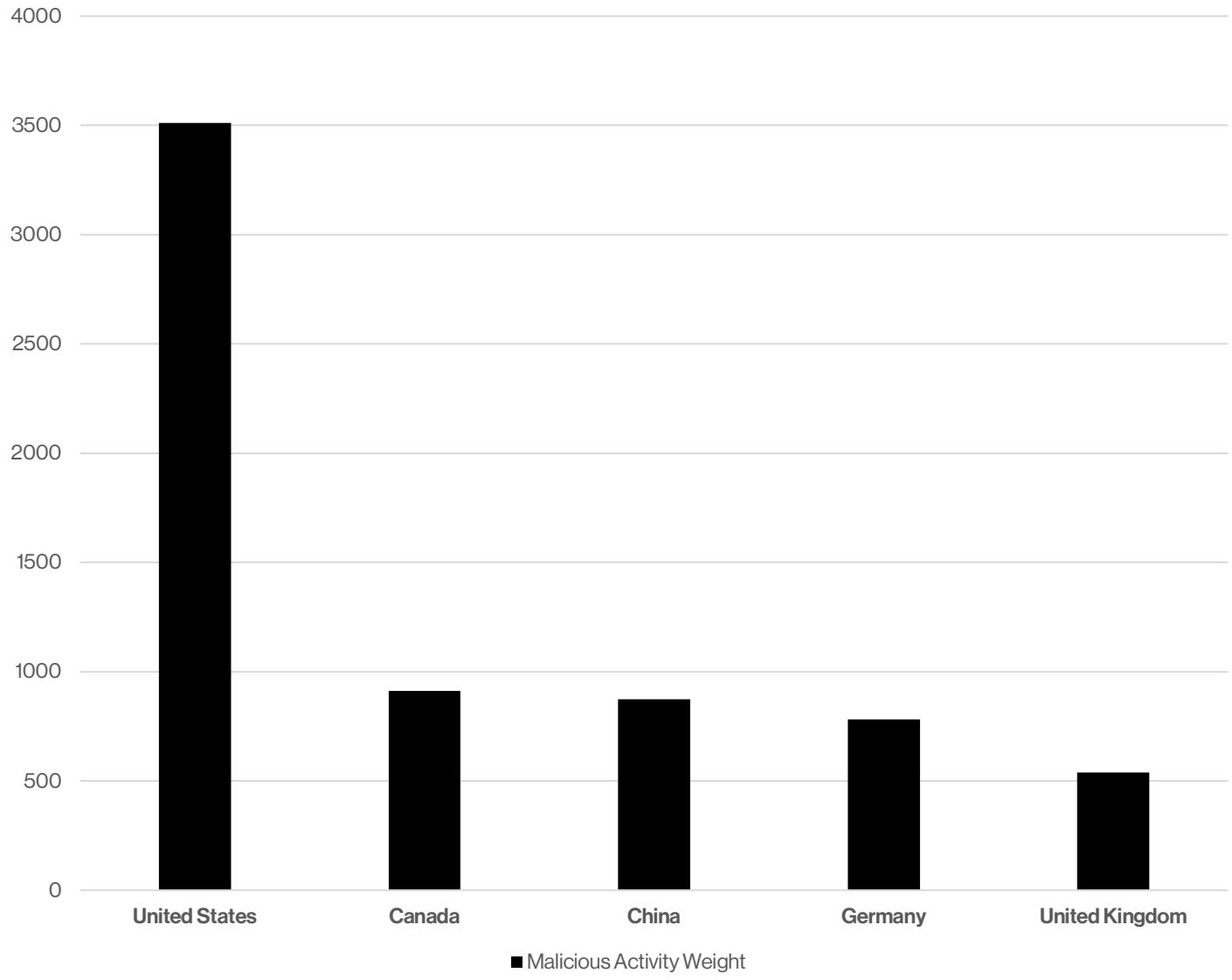
Networks disrupted, online privacy invaded, freedom of expression curtailed.



PUBLIC

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.



PUBLIC

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	**Data Breach Impacts Healthcare Provider**
	Description	San Antonio-based healthcare provider El Centro Del Barrio (which operates as CentroMed) is informing 400,000 patients that their personal and protected health information was compromised in a recent cyberattack. The data breach was discovered on May 1, 2024, after a threat actor gained access to the organization's network on April 30, CentroMed said in an incident notice (PDF) on its website. "While in our IT network, the unauthorized party accessed and/or acquired files that contain information pertaining to CentroMed's current and former patients," the healthcare provider said.

2	Title	**OmniVision Says Personal Information Stolen In Ransomware Attack**
	Description	The California-based imaging sensors manufacturer OmniVision is warning of a data breach after the company suffered a Cactus ransomware attack last year. OmniVision, a subsidiary of the Chinese Will Semiconductor, designs and develops imaging sensors for smartphones, laptops, webcams, automotive, medical imaging systems, and others. In 2023, the company employed 2,200 people and reported an annual revenue of $1.4 billion. On Friday, OmniVision informed the authorities in California of a security breach incident that lasted between September 4 and September 30, 2023.

PUBLIC

3	Title	**Intercontinental Exchange To Pay $10M Sec Penalty Over VPN Breach**
	Description	When it comes to cybersecurity, especially events at critical market intermediaries, every second counts and four days can be an eternity. ICE discovered the incident on April 15, 2021, after a third party informed it of a potential system intrusion linked to an unknown vulnerability in its virtual private network (VPN). Breached by suspected state hackers. "Sophisticated threat actors, believed to be nation-state actors, installed a webshell code onto a compromised VPN device in an attempt to harvest information passing through that device".

PUBLIC

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	**Vulnerability In Popular Logging Utility Fluent Bit**
	Description	It impacts versions from 2.0.7 through 3.0.3, with fixes available in version 3.0.4. The issue relates to a case of memory corruption in Fluent Bit's built-in HTTP server that could allow for DoS, information leakage, or remote code execution. Specifically, it relates to sending maliciously crafted requests to the monitoring API through endpoints such as “/api/v1/traces” and “/api/v1/trace”."Regardless of whether or not any traces are configured, it is still possible for any user with access to this API endpoint to query it," security researcher Jimi Sebree said.

2	Title	**Hackers Backdoor Courtroom Video Recording Software**
	Description	"Cybersecurity company Rapid7 investigated this supply chain incident (now tracked as CVE-2024-4978) and found that the S2W Talon threat intelligence group first spotted the trojanized JAVS installer in early April and linked it to the Rustdoor/GateDoor malware. While analyzing one incident linked to CVE-2024-4978 on May 10, Rapid7 found that the malware sends system information to its command-and-control (C2) server after it gets installed and launched.

PUBLIC

3	Title	**Chinese Hackers Using ORB Proxy Networks For Stealthy Cyber Attacks**
	Description	Unlike traditional botnets, ORBs can be a hybrid of both, offering threat actors a constantly evolving infrastructure that's difficult to track by reporting details of the framework developed by Mandiant to map these ORBs, allowing defenders to identify potential infiltration attempts. One such network, ORB3 (also known as SPACEHOP), has been linked to the well-known Chinese APT (Advanced Persistent Threat) groups APT5 and APT15. At the same time, SPACEHOP is believed to be used for tasks like initial reconnaissance and vulnerability exploitation.

PUBLIC

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.

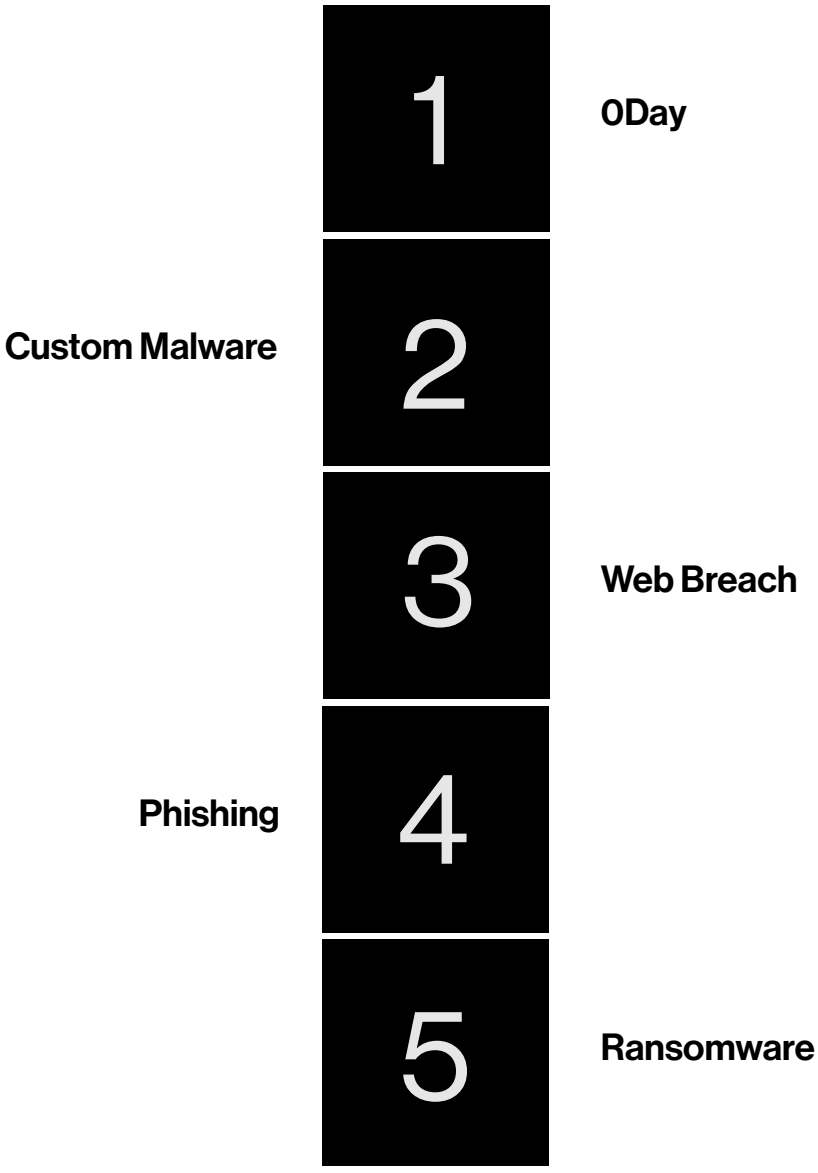
1	Title	**Debian Chromium Security Update**
	Description	• CVE-2024-5157 • CVE-2024-5158 • CVE-2024-5160 • CVE-2024-5159

2	Title	**SUSE Linux Security Advisory**
	Description	• CVE-2024-5160 • CVE-2024-5159 • CVE-2024-5157 • CVE-2024-5158

PUBLIC

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.



PUBLIC

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/

PUBLIC

Most Observed MITRE Techniques

This section dives deeper into the tactics discussed previously, highlighting the top 1 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	**T1070**
	Sub-technique ID	**T1070.003**
	Technique	**Indicator Removal**
	Sub-technique	**Clear Command History**
	Description	In addition to clearing system logs, an adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.
	Technique Reference	https://attack.mitre.org/techniques/T1070/
	Sub-technique Reference	https://attack.mitre.org/techniques/T1070/003/

PUBLIC

03

Vulnerability Briefing

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-2024-4978
Justice AV Solutions Viewer Setup 8.3.7.250-1 contains a malicious binary when executed and is signed with an unexpected authenticode signature.

2

CVE-2024-4323
A memory corruption vulnerability in Fluent Bit versions 2.0.7 thru 3.0.3 which may lead to DOS, info disclosure or RCE.

3

CVE-2024-4947
Type Confusion in V8 in Google Chrome prior to 125.0.6422.60 allows to execute arbitrary code inside a sandbox via a crafted HTML page.

4

CVE-2024-4761
Out of bounds memory write in V8 in Google Chrome prior to 124.0.6367.207 via a crafted HTML page.

5

CVE-2024-4985
An authentication bypass vulnerability in the GitHub Enterprise Server (GHES).

6

CVE-2024-5274
Type confusion in V8.

Exploitation Prevalence

3.6%	3.6%	3.2%	2.8%	2.8%	2.4%
CVE-2024-4978	**CVE-2024-4323**	**CVE-2024-4947**	**CVE-2024-4761**	**CVE-2024-4985**	**CVE-2024-5274**

PUBLIC

04
Malware Briefing

PUBLIC

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. Mirai
4. Remcos
5. DCRat
6. Vidar
7. XWorm
8. AsyncRAT
9. GuLoader
10. RedLine

PUBLIC

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	Spyware
6	Stealer
7	Discovery
8	Miner
9	Ransomware
10	Android

PUBLIC

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
	svchost.exe
	New Text Document.bin.exe
	AnyDesk.exe

Top 5 Most Common Malware Extensions

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

1010 1010	.exe
1010 1010	.pdf
1010 1010	.apk
1010 1010	.elf
1010 1010	.zip

PUBLIC

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.

	.bin.exe
	.2.exe
	.pdf.exe
	.scr.exe
	.0.exe
	.bat.exe
	.com.exe
	..exe
	.3.exe
	.pdf.lzh

PUBLIC

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	Formbook
	Malware Type	Stealer
	MD5	0b0d247aa1f24c2f5867b3bf29f69450
	SHA1	48de9f34226fd7f637e2379365be035af5c0df1a
	SHA256	a6e7292e734c3a15cfa654bba8dea72a2f55f1c24cf6bbdc2fd7e63887e9315a

3	Malware Family	AsyncRAT
	Malware Type	Injector
	MD5	9211293fdf6164567c9c0557cf200057
	SHA1	cef794bc498b0b4ffea444c8f0bd002f0ad717bc
	SHA256	4f9ae5b89c89e5c79c53db694d4d67e2d9b3c47c7389c8c3899dedbc9e92be76

PUBLIC

4	Malware Family	DCRat
	Malware Type	Rat
	MD5	a0fc62e3b7ee3716781698677ef0a315
	SHA1	679ee9e6c503af58943768fac7801a0c85149728
	SHA256	13cc97185f7caa3a67fb2f2325ae2741db7f880eeab103799cd3a2747056ccbc

5	Malware Family	DCRat
	Malware Type	Rat
	MD5	2b249a7350b1cc720a1b86d5521a8095
	SHA1	c40c7bc6676c50e9b7453936d3eb2fc1c718e6dc
	SHA256	a016313bc090d337a66dcefc7cc18a889f5c1cfc721185fa9ad7038159efb728

6	Malware Family	DCRat
	Malware Type	Rat
	MD5	3f3906f8ced4518fe1f773cc8539c00a
	SHA1	5910cb6fac241a38403053e54091c1260ac99b76
	SHA256	77c5f17e97ac13be2f3b9f632d2a1cea5a17b598b533840d2996985d218445fe

PUBLIC

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

8	Malware Family	Revenge
	Malware Type	Ransomware
	MD5	d9da18def2eac42f378b14ef96af89f0
	SHA1	1b6045264b241e4a24d538366a350bd86e384cc2
	SHA256	eedb5b73023cb3e8f55ba5166a064facac13621503b25d43cb92fe179d7b5431

9	Malware Family	DCRat
	Malware Type	Rat
	MD5	a452777147dc02f5d8ccacfc0502ac7c
	SHA1	da8810335c641f55872b90a6ea7f178a0875721c
	SHA256	c1fb621cbb84ba538603cae73960db7969ec4bde877e5692241c82ea25bdf644

PUBLIC

05

Domains Briefing

PUBLIC

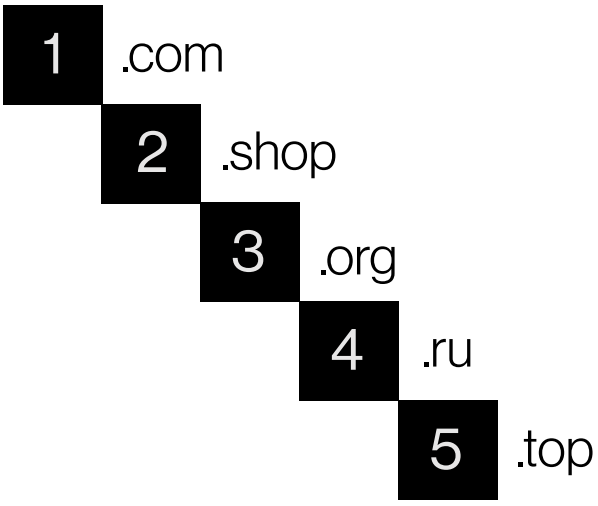
Top 5 Malicious Domains to Avoid at All Costs

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	getpdf[.]pw	N/A
2	url.us.m.mimecastprotect[.]com	MarkMonitor, Inc.
3	bzsqycdkiis.nrgwebservers[.]com	ENOM, INC.
4	survivalconstitution[.]com	GoDaddy.com, LLC
5	www.ericdaigle[.]ca	Gandi Services Inc., Gandi SAS

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.



PUBLIC

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
qr-in[.]com	qrinc.com
isols[.]co	isotls.com
pricekaboom[.]com	pickaboo.com
ryosx[.]cc	rydox.cc
tonybabb[.]com	tonybai.com

PUBLIC

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://www.bostonreview[.]net/articles/
3	https://googleweblight[.]com/i?u=https://humdrum-artistic-peripheral.glitch.me#YldGc2RlVnlhMmx6ZEdGdWFVQmhhbWxzYzJFdVkyOXQ=
4	http://bzsqycdkiis.nrgwebservers[.]com/
5	https://approvedfax.blogspot[.]com/2024/05/blog-post.html

PUBLIC

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	48.0%

2	Hosting Provider	Amazon.com, Inc.
	Hosting Location	United States
	Activity Weight	19.8%

3	Hosting Provider	Microsoft Corporation
	Hosting Location	United Arab Emirates
	Activity Weight	14.1%

4	Hosting Provider	Google LLC
	Hosting Location	France
	Activity Weight	8.6%

PUBLIC

07

IP Address Briefing

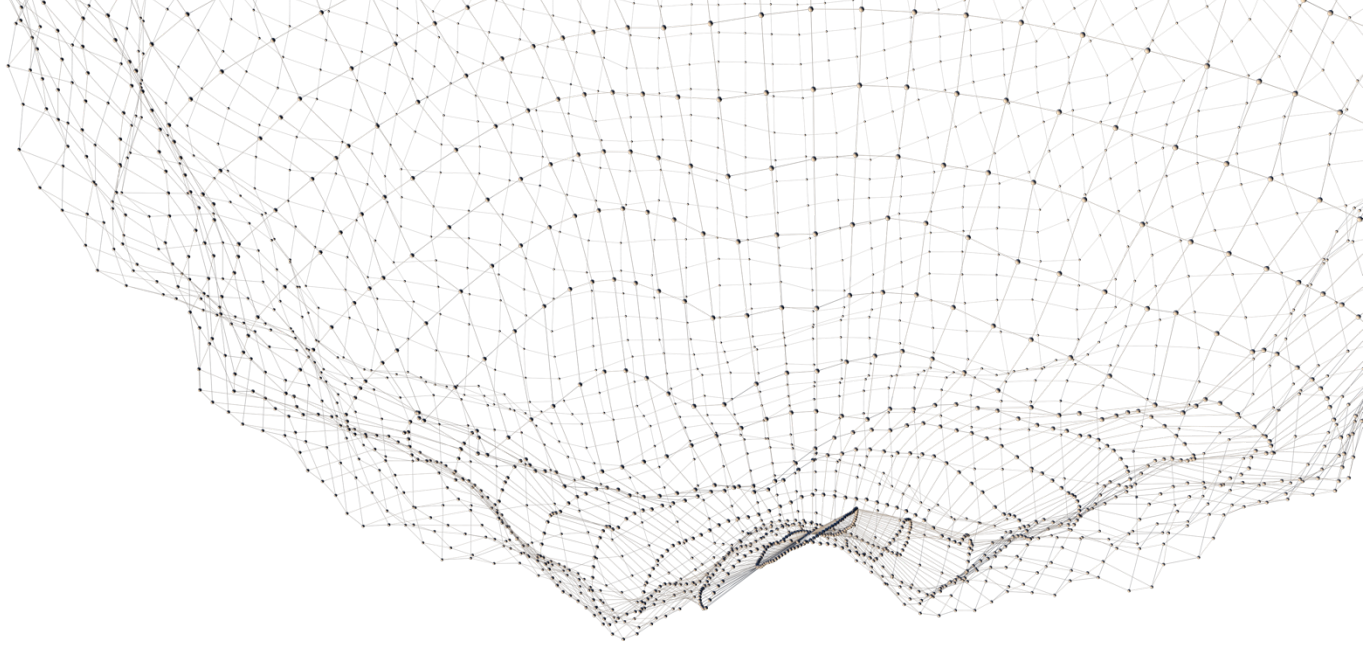
PUBLIC

Top 10 Malicious IP Addresses

Knowledge is power in the fight against cybercrime! This section exposes the top 10 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	185.125.190[.]26	United Kingdom	Canonical Group Limited
4	149.154.167[.]220	United Kingdom	Telegram Messenger Inc
5	5.42.96[.]64	Russian Federation	CJSC Kolomna-Sviaz TV
6	65.109.242[.]59	Finland	Hetzner Online GmbH
7	20.117.108[.]240	United Kingdom	Microsoft Corporation
8	45.140.147[.]81	Netherlands	STARK INDUSTRIES SOLUTIONS LTD
9	89.111.173[.]112	Russian Federation	"Domain names registrar REG.RU", Ltd
10	69.165.74[.]70	Germany	LLC Baxet

PUBLIC



08

Putting Intel into Practice

PUBLIC

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.

PUBLIC

Bolster Network Security:

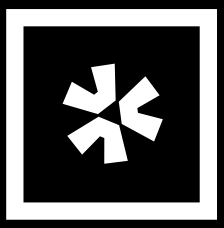
- **Implement IP reputation filtering:** Block traffic originating from known malicious IP addresses.
- **Monitor network activity:** Analyze logs for suspicious inbound and outbound traffic.
- **Strengthen firewall rules:** Refine access control lists to restrict inbound connections from high-risk countries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

PUBLIC



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