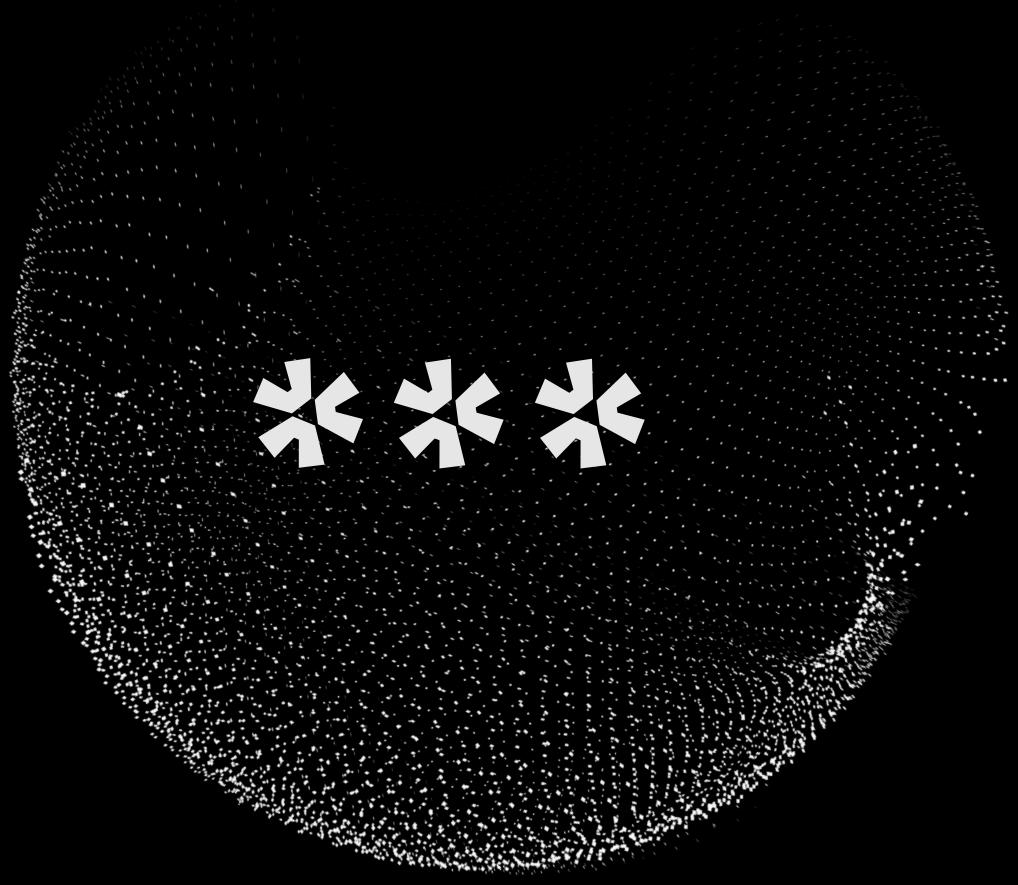
elixicode



18/06/2024

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

“

Don't underestimate the power of seemingly insignificant data points. Threat intelligence connects the dots, revealing the bigger picture.

”

- 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.

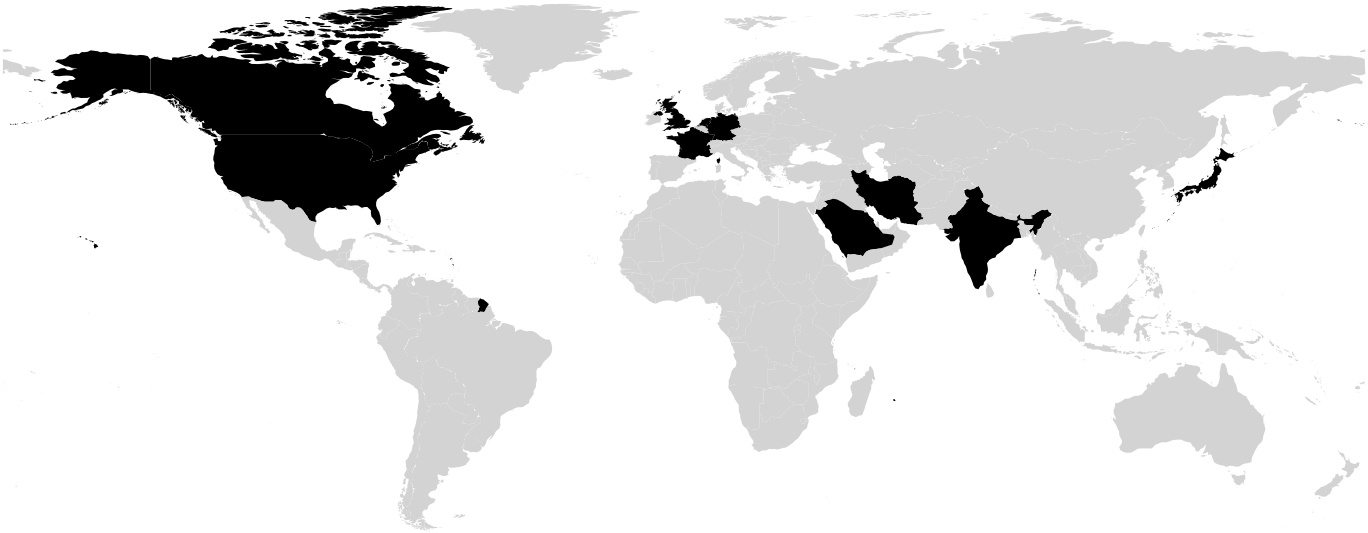
Join us on this journey of proactive security. Follow us on X and access your free weekly Threat Intel Report today!

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. **Germany**
3. **France**
4. **Netherlands**
5. **India**
6. **Saudi Arabia**
7. **United Kingdom**
8. **Canada**
9. **Iran**
10. **Japan**

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

Communication

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

3

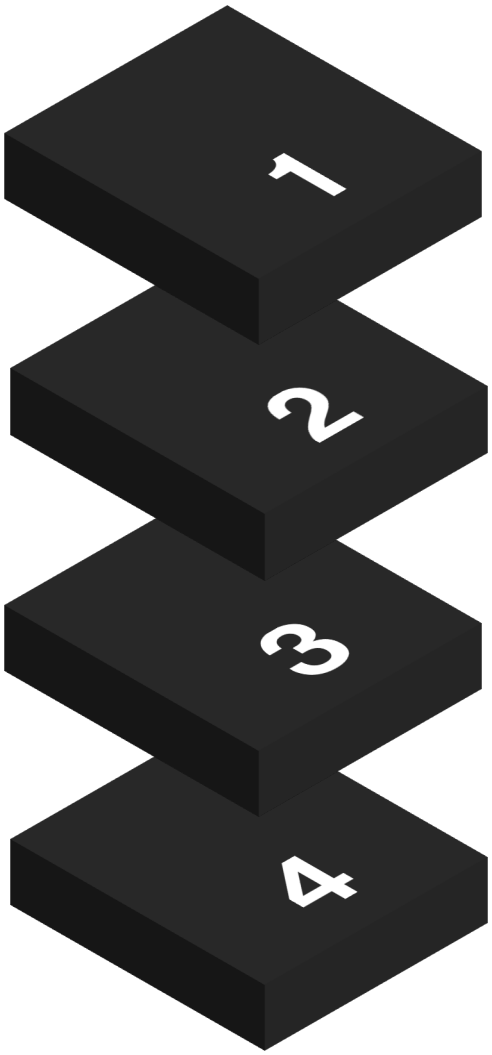
Finance and insurance

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

4

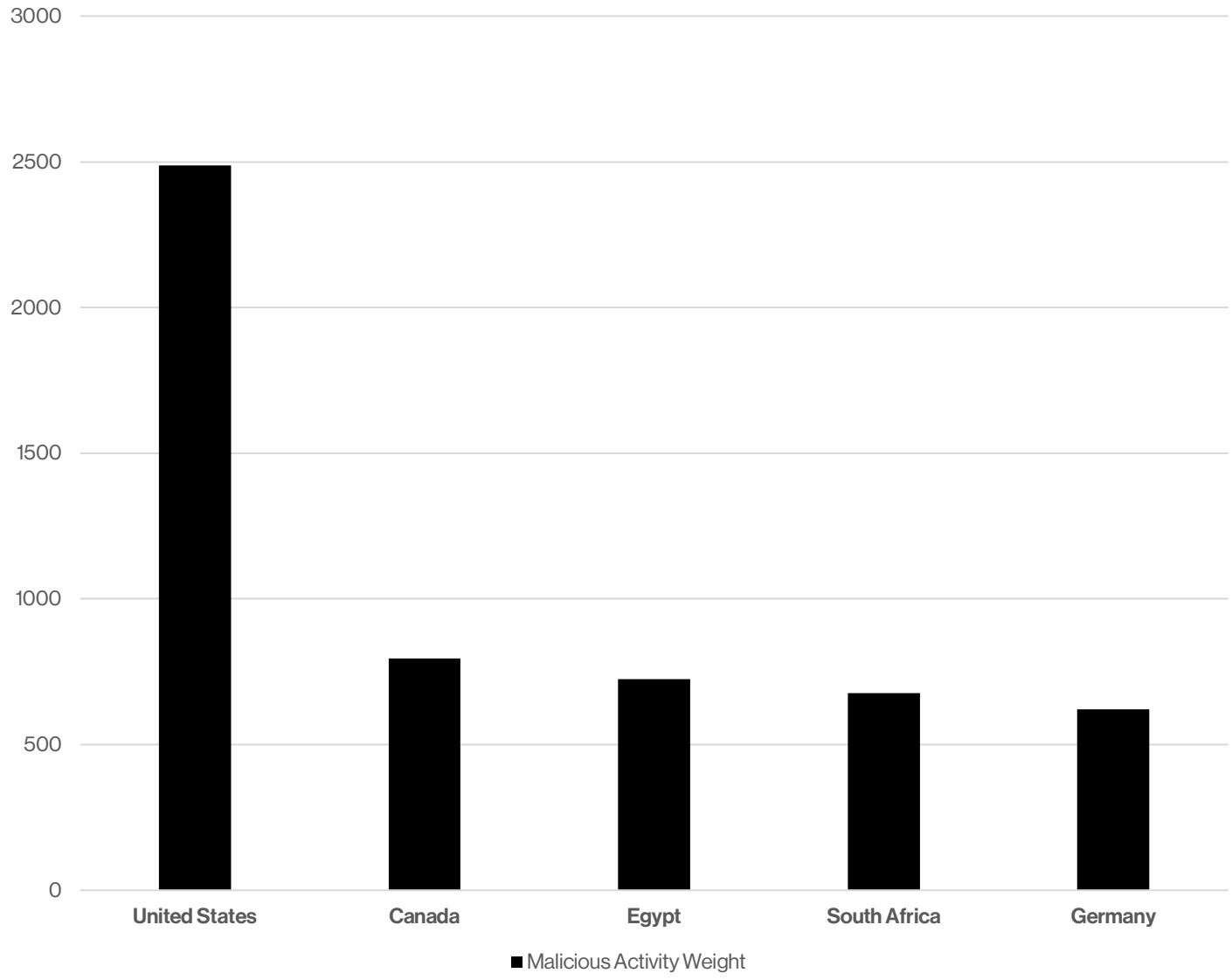
Government

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	**“23AndMe” Data Breach Under Joint Investigation In Two Countries**
	Description	Privacy authorities in Canada and the United Kingdom have launched a joint investigation to assess the scope of sensitive customer information exposed in last year's 23andMe data breach. The Privacy Commissioner of Canada and The Information Commissioner's Office (ICO) will also look into whether the company had adequate safeguards to secure customer data stored on its systems. The joint investigation will also examine if 23andMe alerted affected individuals and the privacy regulators as required by Canadian and UK privacy and data protection laws. In the wrong hands, an individual's genetic information could be misused for surveillance or discrimination.

2	Title	**Snowflake Attacks: Mandiant Links Data Breaches To Infostealer**
	Description	Let's review the facts: two large organizations announced that they suffered a data breach, identifying unauthorized activity within a third-party cloud database environment. Snowflake did publish a warning with CISA, indicating a "recent increase in cyber threat activity targeting customer accounts on its cloud data platform." Snowflake issued a recommendation for users to query the database logs for unusual activity and conduct further analysis to prevent unauthorized user access.

3	Title	**Chinese Hackers Breach 20,000 Fortigate Systems Worldwide**
	Description	The Dutch intelligence services and the NCSC consider it likely that the state actor could potentially expand his access to hundreds of victims worldwide and carry out additional actions such as stealing data. At least 20,000 Fortigate systems breached Since February. The Dutch military intelligence service has discovered that the Chinese threat group obtained access to at least 20,000 FortiGate systems worldwide in 2022 and 2023 over a span of a few months, at least two months before Fortinet disclosed the CVE-2022-42475 vulnerability. The MIVD believes the Chinese hackers still have access to many victims because the Coathanger malware is difficult to detect as it intercepts system calls to avoid revealing its presence.

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	**Chinese Hackers Compromised 20K Fortigate Systems Worldwide**
	Description	The Military Intelligence and Security Service (MIVD) and the General Intelligence and Security Service (AIVD) have released a security advisory stating that Chinese state actors have been abusing vulnerabilities in edge devices to gain additional capabilities and activities. 20K FortiGate Systems Compromised. According to the reports shared with Cyber Security News, the COATHANGER malware campaign was further investigated, which revealed that the threat actor had gained access to at least 20,000 FortiGate systems worldwide, including dozens of governments, international organizations, and a large number of companies within the defense industry.

2	Title	**Ransomware Group May Have Exploited Windows Vulnerability As Zero-Day**
	Description	A known ransomware group may have exploited a recently patched Windows privilege escalation vulnerability before Microsoft released a fix, Symantec reported on Wednesday. The flaw in question, tracked as CVE-2024-26169 and classified as 'important', has been described as a Windows error reporting service privilege escalation vulnerability that can allow an attacker to obtain System privileges. However, Broadcom's Symantec says it has found evidence suggesting that the Black Basta ransomware group (aka Cardinal, Storm-1811 and UNC4393) may have actually exploited this vulnerability as a zero-day.

3	Title	**London Hospitals Cancel Over 800 Operations After Ransomware Attack**
	Description	Ongoing service disruptions at Guy's and St Thomas' NHS Foundation Trust, King's College Hospital NHS Foundation Trust, and primary care providers across South East London result from Synnovis being locked out of its systems by a June 3 attack linked to the Qilin ransomware operation. While memos issued by hospital officials revealed this "ongoing critical incident" has had a "major impact" on their procedures and operations.

Must-Read Cybersecurity News

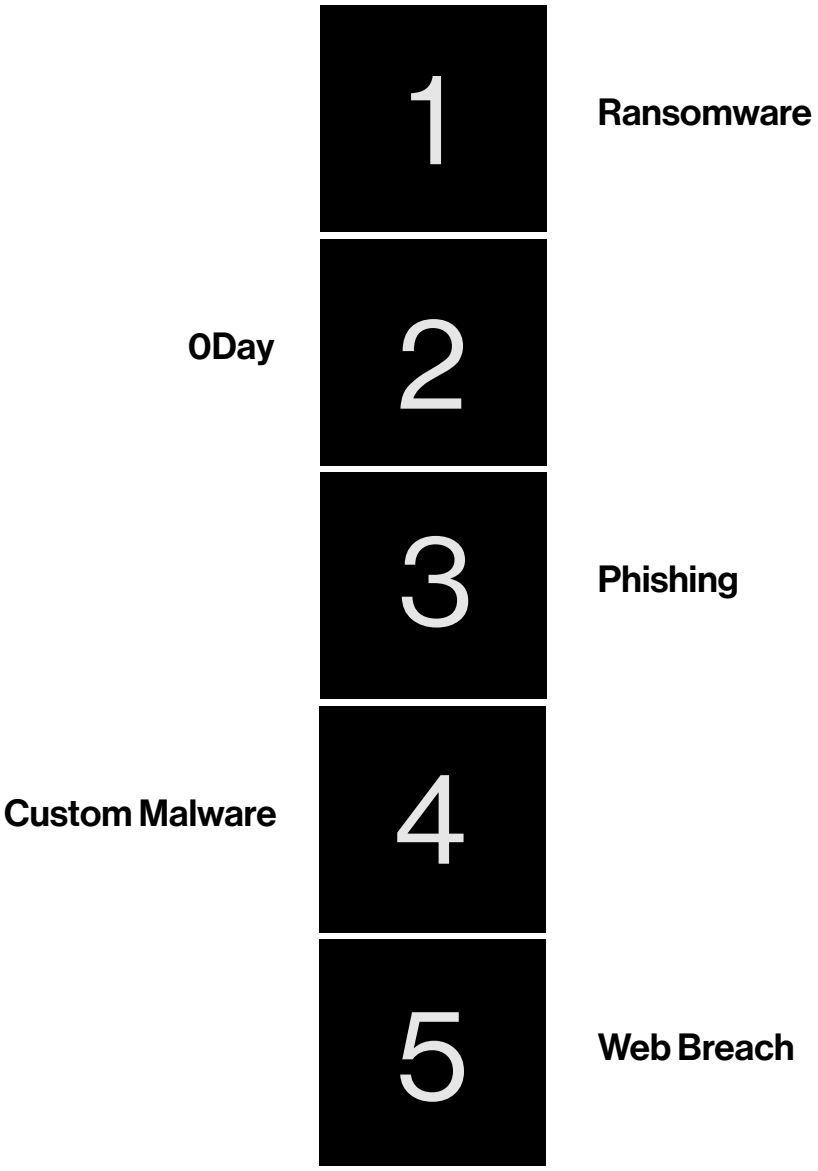
Staying ahead of the curve in cybersecurity demands constant vigilance. This section tackles the top 2 cybersecurity news stories currently dominating the headlines, ranked in descending order of their heat and potential impact.

1	Title	**VMware Player Vulnerabilities**
	Description	VMWare Player Vulnerabilities: • (CVE-2024-22269) • (CVE-2024-22270) • (CVE-2024-22268) • (CVE-2024-22267)

2	Title	**Veeam Auth Bypass Exploit Available, Patch Now**
	Description	The post showcased that the flaw is practically more straightforward to exploit than the vendor's bulletin suggested. Critical authentication bypass CVE-2024-29855, rated 9.0 as per CVSS v3.1 ("critical"), is an authentication bypass vulnerability impacting Veeam Recovery Orchestrator (VRO) versions 7.0.0.337 and 7.1.0.205 and older. The flaw allows unauthenticated attackers to log in to the Veeam Recovery Orchestrator web UI with administrative 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	**TA0004**
	Tactic	**Privilege Escalation**
	Description	The adversary is trying to gain higher-level permissions.
	Reference	https://attack.mitre.org/tactics/TA0004/

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-2024-4577
PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, 8.3.* before 8.3.8, vulnerability that could be used to run arbitrary PHP code on the server, etc.

2

CVE-2024-30080
Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability.

3

CVE-2024-26169
Windows Error Reporting Service Elevation of Privilege Vulnerability.

4

CVE-2024-4610
Use After Free vulnerability in Arm Ltd Bifrost GPU Kernel Driver, Arm Ltd Valhall GPU Kernel Driver.

5

CVE-2023-50868
The Closest Encloser Proof aspect of the DNS protocol allows remote attackers to cause a denial of service via DNSSEC responses.

6

CVE-2024-30103
Microsoft Outlook Remote Code Execution Vulnerability.

Exploitation Prevalence

2.7%	2.5%	2.5%	2.5%	2.5%	2.5%
CVE-2024-4577	**CVE-2024-30080**	**CVE-2024-26169**	**CVE-2024-4610**	**CVE-2023-50868**	**CVE-2024-30103**

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	N/A
2	AgentTesla
3	AsyncRAT
4	WannaCry
5	RedLine
6	GuLoader
7	DCRat
8	XWorm
9	Remcos
10	Formbook

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

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.

	SolaraBootstrapper.exe
	test.exe
	Server.exe
	Client-built.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	.pdf
1010 1010	.elf
1010 1010	.rar

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.

	.0.zip
	.2.exe
	.pdf.exe
	.scr.exe
	.5.exe
	.xlam.xlsx
	.bat.exe
	.doc.rtf
	.0.exe
	.6.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	N/A
	Malware Type	Stealer
	MD5	a048795fdaf5b6d844960e1c45c3a442
	SHA1	8a0e147897b62398a6e9bcabcfa87a088ee76a3b
	SHA256	40c5ec744bcf776a3e885a2a88e49ff092155211e8e08ea9576fc98f781f6fc5

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

4	Malware Family	Lumma
	Malware Type	Dropper
	MD5	543e80dbd2fa8ddf8cebccc1099b4609
	SHA1	dae57bb7f0ef4e045e0da446ac8e8f546e341147
	SHA256	52e7510e97f558788067937c97a268ad4951d22f8b94d87855bcb3dd4d6e6708

5	Malware Family	RedLine
	Malware Type	Stealer
	MD5	6e1166af854364a8668e80049abf4cca
	SHA1	0832bab61321ec1b2998e7dc99b807c5d51ba5b7
	SHA256	b1309d691e19475051caa2f1346d2f7a23706bca559852d8c420f3f8fbcb557f

6	Malware Family	N/A
	Malware Type	Dropper
	MD5	af8e86c5d4198549f6375df9378f983c
	SHA1	7ab5ed449b891bd4899fba62d027a2cc26a05e6f
	SHA256	7570a7a6830ade05dcf862d5862f12f12445dbd3c0ad7433d90872849e11c267

7	Malware Family	AsyncRAT
	Malware Type	Hacktool
	MD5	f192b4e9cf07850041e19ea07cd984e3
	SHA1	061a917e9691648e00a7f91ff82ae1c0e8da248b
	SHA256	515b7bd886b37d24fa02bb3d9b1ecf31f887bb46834787771722236d40c565c7

8	Malware Family	RisePro
	Malware Type	Backdoor
	MD5	a053de60d84cf6a5a7e258c551383c4f
	SHA1	f0e2a41497547fe914c77aac099f36eb5f79d7e7
	SHA256	e5d62ab8315f16292765038ccf6c4f46d69b6c9ca988d89211ac1d590c57e35d

9	Malware Family	AgentTesla
	Malware Type	Rat
	MD5	0c0a41c08e05cc17ec190a8325122ff1
	SHA1	d626dadb8389d7d3a2ef8a4d55ea1e93012344df
	SHA256	dc2e8a0f43a7ba9dc6ccf14dfda7e6ddd366d137cf774e221b09165ca6b414a8

05

Domains Briefing

PUBLIC

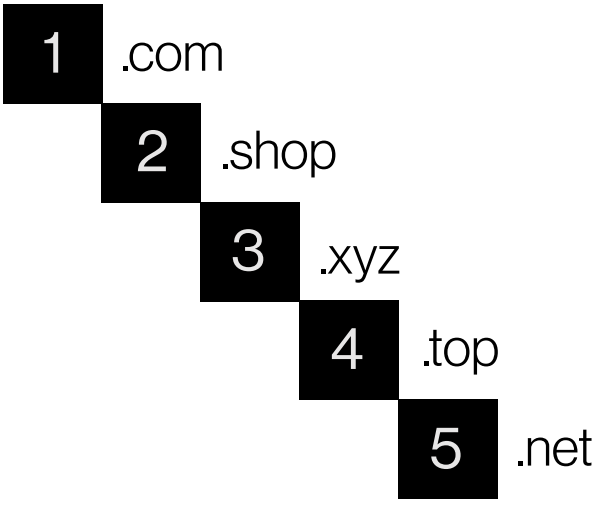
Top 5 Malicious Domains to Avoid at All Costs

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	ninext[.]ng	N/A
2	www.otsi-usa[.]net	Hostopia Canada Corp
3	Binarly[.]io	Key-Systems GmbH
4	aguasazuis.com[.]br	N/A
5	melliobrien[.]com	Key-Systems GmbH

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
whatismyipaddressnow[.]co	whatismyipaddress.com
ftp.normagroup.com[.]tr	normagroup.com
www.johnson[.]health	johnson.ca
bashupload[.]com	biaupload.com
universalmovies[.]top	universalmovies.it
smsmail[.]net	samsmail.net
telegram-gh[.]org	telegram.org
kraitnaa[.]com	karinaa.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	https://ipinfo[.]io/
2	https://melliobrien[.]com/
3	http://185.172.128[.]93/sh
4	https://taxconnect.co[.]in/bulletins/
5	https://nimb[.]ws/yu06mxW

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	50.9%

2	Hosting Provider	Amazon.com, Inc.
	Hosting Location	Ireland
	Activity Weight	15.9%

3	Hosting Provider	Microsoft Corporation
	Hosting Location	United Arab Emirates
	Activity Weight	11.1%

4	Hosting Provider	Google LLC
	Hosting Location	Germany
	Activity Weight	10.8%

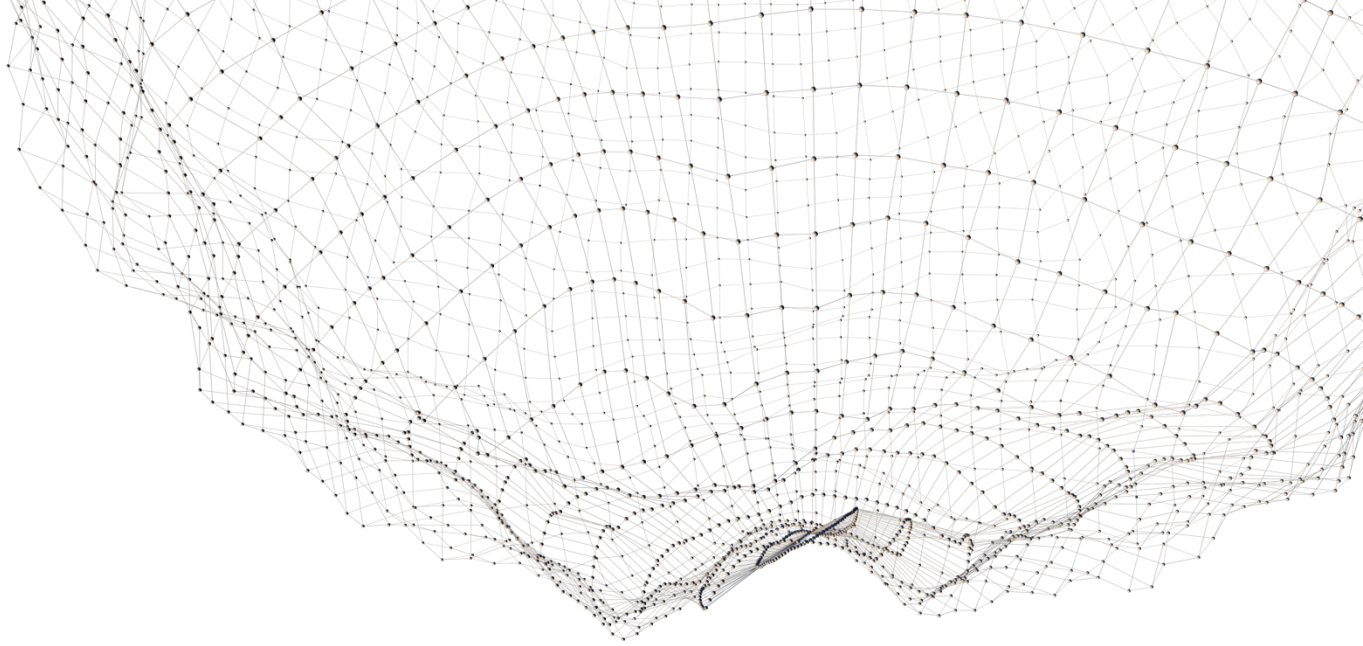
07

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	91.189.91[.]42	United States	Canonical Group Limited
2	91.189.91[.]43	United States	Canonical Group Limited
3	3.33.130[.]190	Canada	Amazon.com, Inc.
4	94.156.8[.]80	Türkiye	SUNUCUN BILGI ILETISIM TEKNOLOJILERI VE TICARET LIMITED SIRKETI
5	89.105.201[.]183	Netherlands	NovoServe B.V.
6	185.125.190[.]26	United Kingdom	Canonical Group Limited
7	45.131.111[.]98	Germany	Ferdinand Zink trading as Tube-Hosting
8	149.154.167[.]99	United Kingdom	Telegram Messenger Inc
9	89.190.156[.]145	Netherlands	Alsycon B.V.
10	194.59.31[.]219	Macao	MARKAHOST TELEKOMUNIKASYON VE TICARET LIMITED SIRKETI
11	147.45.47[.]126	Russian Federation	Karina Rashkovska
12	195.201.251[.]58	Germany	Hetzner Online GmbH
13	103.167.88[.]191	Viet Nam	JOBKEY JOINT STOCK COMPANY
14	54.171.230[.]55	Ireland	Amazon.com, Inc.
15	185.172.128[.]93	Germany	TNSECURITY LTD



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.

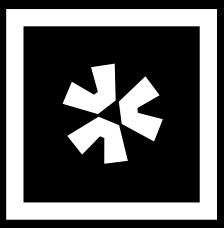
Bolster Network Security:

- **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