bfore.ai

PreCrime Landscape Report

September 2022

Bfore.ai
Predictive Cyber Security
Quarterly Threat Intelligence Reporting

Contents

PreCrime Landscape Report Q3

Bfore.Ai Data Overview

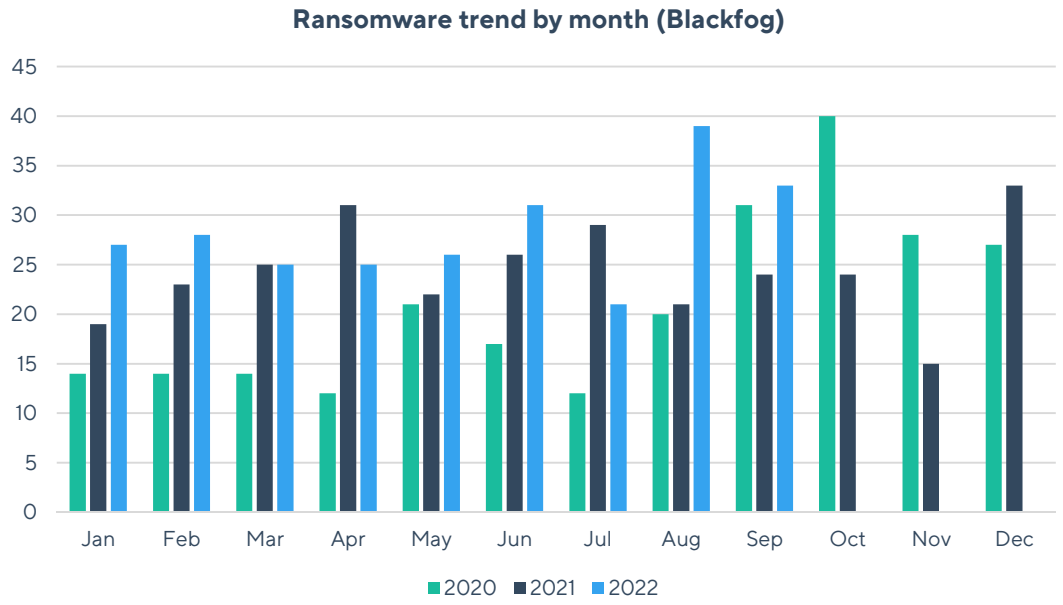
How efficient is Bfore.ai in detecting malicious domains?

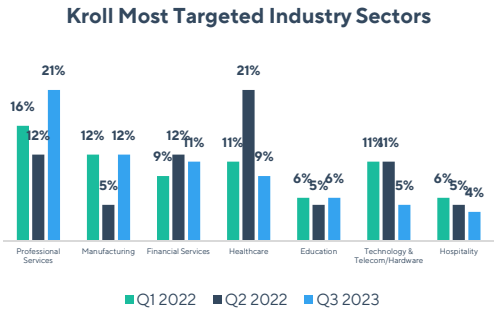
801,762
Malicious Domains Detected Q3 2022

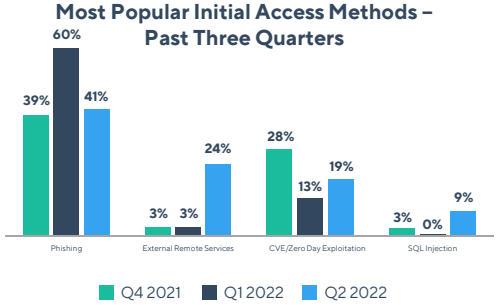
Phishing
Main Threats from detected domains

Financial
Industry most targeted from detected domains

The months of July, August, and September have shown increased recorded data breaches, phishing malware, and ransomware attacks. Threat actors are consistently evolving their capabilities, with double and triple extortion being a more commonly used tactic, along with MFA fatigue and voice phishing.



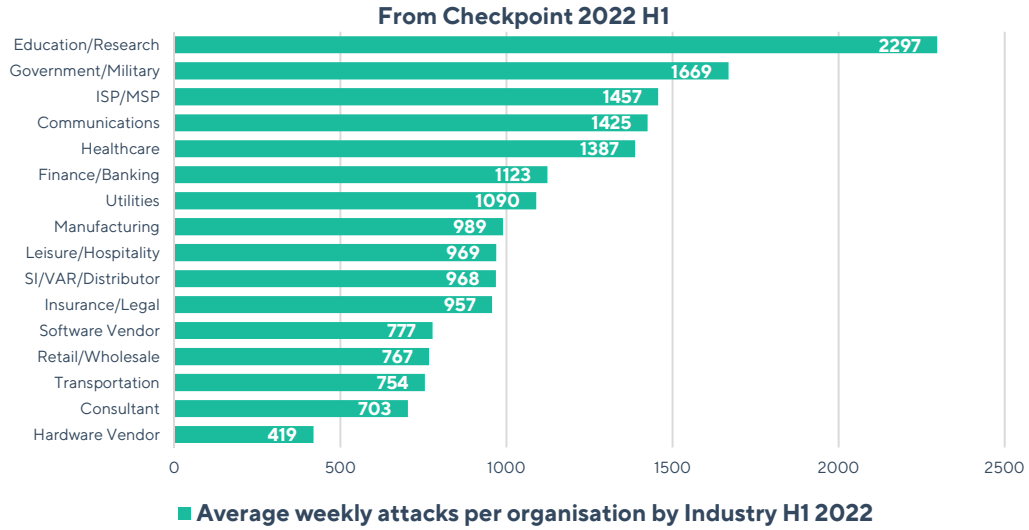




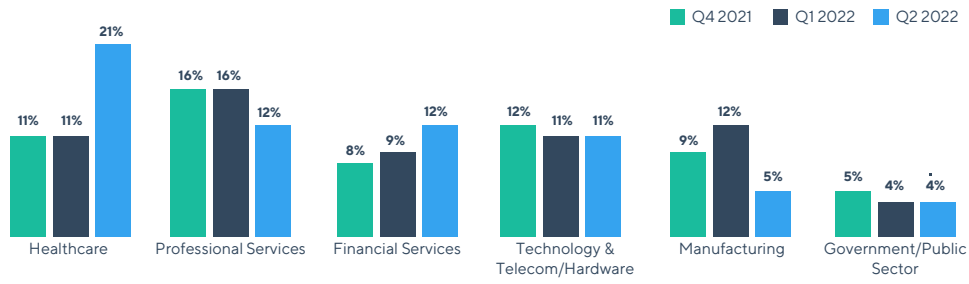
Data Breaches Overview

Cyber Breaches in Q3

Companies are continuously experiencing more data breaches with ever-increasing costs. According to the Identity Theft Resource Center's 2021 Data Breach Report, there were 1,862 data breaches in 2021, surpassing the 1,108 recorded in 2020 . In terms of costs, IBM found that the average cost of a data breach increased by 12.7% from 2020 (USD 3.86 million) and 2.6% from 2021 (USD 4.24 million), with average costs now at USD 4.35 million in 2022. The healthcare industry has also seen an increase in attacks over the past year as the graphs below by Kroll and CheckPoint demonstrate. Healthcare has been the most expensive industry for 12 years running, with costs reaching a record high of USD 10.10 million in 2022. The healthcare industry is an incredibly appealing target for threat actors due to the importance of keeping their systems working. Financial organizations experience the second highest costs, averaging USD 5.97 million, followed by pharmaceuticals at USD 5.01 million, technology at USD 4.97 million, and energy at USD 4.72 million.



Graph 1: Checkpoints 2022 Mid-year report 'Cyber Attack Trends'



Graph 2: Kroll Q2 Threat Landscape

1

Data Breaches

July

Marriott Confirms 20 GB Data Breach

Impact:
Hackers stole 20 gigabytes of sensitive data from Marriott International. The stolen data included internal business documents, flight information, and corporate credit card numbers.

Initial Access method:
Social engineering attack, where an employee was tricked into granting an anonymous hacking group access. The hacking group's access was limited to that single employee's computer.

Neopets Data Breach Exposes Data on 69 Million Accounts

Impact:
A hacker leaked data of 69 million Neopets users, which they put for sale in an online forum. Personal data, including name, email address, date of birth, zip code, and more, as well as 460 MB of compressed source code for the Neopets website, were leaked.

Initial Access method:
Attackers had access to the Neopets IT systems from January 3, 2021 until July 19, 2022.

Mangatoon Data Breach Exposed 23M Accounts

Impact:
- Twenty-three million user accounts on the comic reading app Mangatoon were exposed by the well-known hacker, pompompurin.
- Names, email addresses, genders, social media account information, auth tokens from social logins, and salted MD5 password hashes were leaked

Initial Access method:
- Breach of an Elasticsearch database with weak credentials.

Hacker Posts Data on 5.4 Million Twitter Users For Sale

Impact:
Contact information for 5.4 million Twitter accounts, including phone numbers and email addresses, was sold on a Dark Web forum for the asking price of 30,000 USD by a hacker using the alias 'devil'.

Initial Access method:
The hacker exploited a vulnerability to scrape the data from Twitter, wherein if an email address or phone number was submitted to Twitter's systems, it would tell the person the submitted email addresses or phone number and the Twitter account with which it was associated.

1 Billion Chinese Citizens' Data Stolen

Impact:
A Chinese database from the Shanghai National Police (SHGA), including sensitive data of 1 billion Chinese citizens, claims to have been stolen by a hacker under the alias 'ChinaDan'. The hacker offered to sell the data, including names, addresses, birthplace, national ID numbers, mobile numbers, and criminal records, for 10 bitcoins (approximately $200,000). This event could be considered the largest data leak ever[2].

Initial Access method:
The enormous data theft occurred because of an error in a Shanghai police database, which allowed anyone to access the data without requiring a password[2].

August

130+ Companies Compromised in 0ktapus Phishing Breach

Impact:
A months-long phishing campaign has been revealed that has compromised at least 130 companies, including Cloudflare, Doordash, Mailchimp, and Twilio by threat actors who have been given the moniker '0ktapus'.

Initial Access method:
0ktapus executed their attack by sending a text message to victims with a link that would direct them to a fake page imitating the authentication service Okta, where the victims would then enter their login credentials, giving the attackers access to their account[3].

[2] Insider, ThreatPost
[3] 0ktapus Phishing Breach

Cyberattack resulted in closure of 7/11 stores in Denmark

Impact:
One hundred seventy-five 7/11 stores were forced to close for a period of X days in Denmark after a ransomware attack by an unknown hacker disrupted stores' payment and checkout systems[4].

Initial Access method:
Unknown

Cisco hacked by Yanluowang ransomware gang, 2.8GB allegedly stolen

Impact:
- Cisco was attacked by the Yanluowang ransomware group.
- Allegedly 2.8GB of data was stolen.

Initial Access method:
They gained access by using an employee's stolen credentials after hijacking that employee's personal Google account containing credentials synced from their browser[5].

Patients are Sent Elsewhere After $10M Ransomware Attack on French Hospital

Impact:
A French hospital was targeted by a $10 million ransomware attack causing the hospital's IT system to stop functioning. As a result staff are now working with limited resources and all non-critical services were directed elsewhere[6].

Initial Access method:
The suspected LockBit 3.0 ransomware was used.

[4] BleepingComputer, Link2
[5] BleepingComputer, The Hacker News
[6] France24

Malicious Chrome Extensions May Impact Over 1.4 Million Users

Impact:
The malicious extensions include, Netflix Party, Netflix Party 2, FlipShope, Screenshotting, and AutoBuy Flash Sales and have impacted 1.4 million users[7].

Initial Access method:
Malicious google chrome extensions are mimicking the appearance of popular extensions but they redirect users to phishing sites that insert affiliate IDs into the cookies of eCommerce sites and track the users' browser history. Every website the victim visits is then sent to servers owned by the extension creator so that they can insert code into eCommerce websites being visited. By doing this, the attacker modifies cookies on the eCommerce site so that the extension author receives the affiliate payment for any items purchased.

The British National Health Service (NHS) has suffered a major services outage

Impact:
The United Kingdom's National Health Service (NHS) 111 emergency services have been affected by a cyberattack that hit the systems of Advanced, a British managed services provider (MSP), leading to a major outage of a computer system that is used to coordinate services for patients[8] [9].

Initial Access method:
Unknown

September

Lapsus$-Affiliated Hacker Compromises Uber

Impact:
The hacker accessed several other employee accounts and gained elevated permissions to a number of tools, including G-Suite and Slack, where they posted a message to a company-wide Slack channel and reconfigured Uber's OpenDNS to display a graphic image to employees on some internal sites. The hack resulted in some confidential information being accessed, including all vulnerability reports[10].

Initial Access method:
A threat actor, 'teapots2022', believed to be affiliated with Lapsus$ hacked Uber by using an Uber EXT contractor's stolen credentials in an MFA fatigue attack where the contractor was flooded with two-factor authentication (2FA) login requests until one of them was accepted.

[7] Zdnet
[8] Acronis
[9] BleepingComputer
[10] The Cyber Wire

Hacker Breaches Rockstar Games, Leaks GTA6 Footage

Impact:
The same attacker who hacked Uber (teapotuberhacker) also claimed to have leaked footage of an upcoming game produced by Rockstar Games, Grand Theft Auto 6.

Initial Access method:
The hacker acquired the footage after gaining access to the company's Slack.

Instagram Phishing Campaign

Impact:
Thousands of Instagram users were targeted, where their name, email, phone number, and Instagram password were stolen, leaving their accounts vulnerable.

Initial Access method:
An Instagram phishing campaign has been revealed in which threat actors sent fake emails to thousands of Instagram users requiring them to fill out a form to claim a verification badge (blue badge), which is highly coveted[11].

Cyberattacks linked to Iran have been disrupting Albania's government systems

Impact:
Albania's government systems have been disrupted and forced to shut down as a result of multiple cyberattacks linked to Iran, resulting in the diplomatic ties between Iran and Albania being cut.

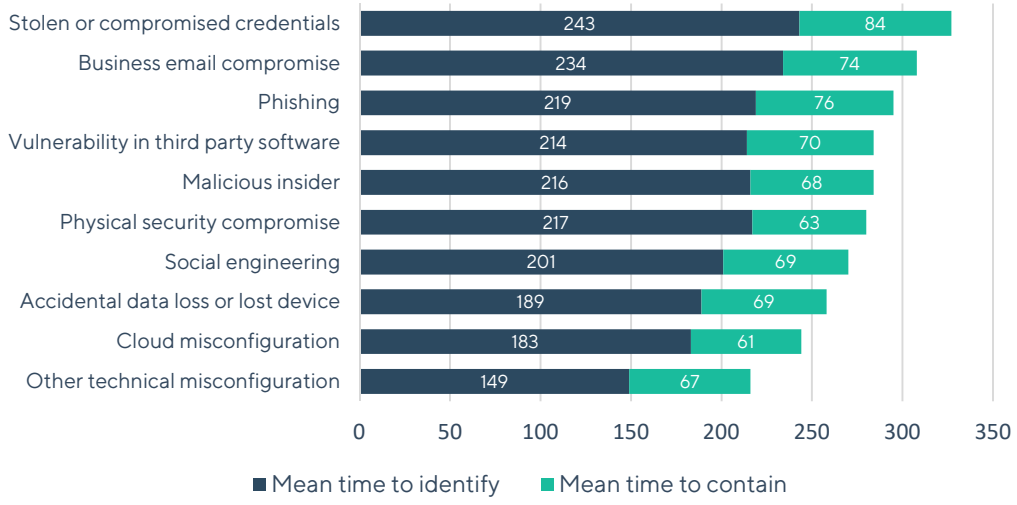
Initial Access method:
Unknown

[11] BleepingComputer

Initial Attacks Vectors

In 2021 and the first half of 2022, the most common initial attack vector for data breaches was stolen or compromised credentials (19%) followed by phishing (16%), cloud misconfiguration (15%), and vulnerability in third-party software (13%). In terms of costs, the costliest initial attack vector in 2022 on average was phishing at USD 4.91 million, followed by business email compromise at USD 4.89 million (6% of breaches), vulnerability in third-party software at USD 4.55 million and compromised credentials at USD 4.50 million.

IBM: Average time to identify and contain a data breach by initial attack vector 2022 H1



In Q3

Source: IBM Cost of a Data Breach Report 2022

These trends reflect cybercriminals' continued focus on compromising people as opposed to gaining access to systems through technical vulnerabilities[12]. Weak controls, and other poor cyber hygiene practices continue to be a popular initial attack vector, with human error contributing to 95% of cyberattacks, according to an IBM Threat Intelligence survey.

[12]https://www.proofpoint.com/uk/newsroom/press-releases/proofpoints-2022-state-phish-report-reveals-email-based-attacks-dominated

Social Engineering

Phishing and Malicious domains 2022

In Q2, APWG recorded the worst quarter for phishing attacks ever recorded in Q2 with over 1 million phishing attacks. This number has quadrupled since 2020, when APWG observed between 68,000 and 94,000 attacks per month. Interisle consulting group also found that phishing increased by 61% in the period 1 May 2020 through 30 April 2021. Email conversation hijacking has also been increasingly used by cybercriminals with a 270% increase in 2021[13]. In these attacks cyber criminals hack into accounts and hijack ongoing conversations in order to send phishing emails that seem more believable as the message comes as part of an ongoing thread.

Phishing against social media websites (15.3% of attacks) and cryptocurrency targets (6.5% of attacks) have both seen an increase, and are now more prevalent than attacks against online games, government sites, and telecom services combined[14].

Finally, smishing and vishing attacks have seen a huge increase in volume (70% more since Q1)[15]. Additionally, hybrid vishing attacks have increased greatly. In these attacks cybercriminals first reach out to victims via email wherein they don't include malicious links or attachments, but phone numbers that the victim is instructed to call. These attacks are seemingly being deployed as more people are becoming aware of the threat of links or attachments in emails, making these types of attacks seem less suspicious.

The Cybercrime Information Center found that the most used TLDs from May to June 2022 were as follows[16].

Top 10 TLDs by Phishing Domains (Cybercrime Information Center):

Rank	TLD	Domains in TLD	Phishing Domains
1	com	159,523,887	86,925
2	cn	8,125,667	20,554
3	ml	5,882,344	14,228
4	tk	5,503,716	11,449
5	xyz	4,187,298	7,054
6	shop	1,057,174	6,817
7	ga	8,030,092	6,807
8	cf	5,756,243	6,769
9	top	1,759,256	6,704
10	gq	4,666,405	6,075

Source: Cybercrime information center

With the majority of phishing domains registered with the following

[13]https://blog.barracuda.com/2022/03/16/spear-phishing-report-social-engineering-and-growing-complexity-of-attacks/
[14]https://www.interisle.net/PhishingLandscape2022.html
[15]https://www.helpnetsecurity.com/2022/09/26/phishing-activity-trends-2022/?web_view=true
[16]https://cybercrimeinfocenter.squarespace.com/phishing-activity-numbers-may-july-2022

Top 10 Domain Registrars by Phishing Domains (Cybercrime Information Center)

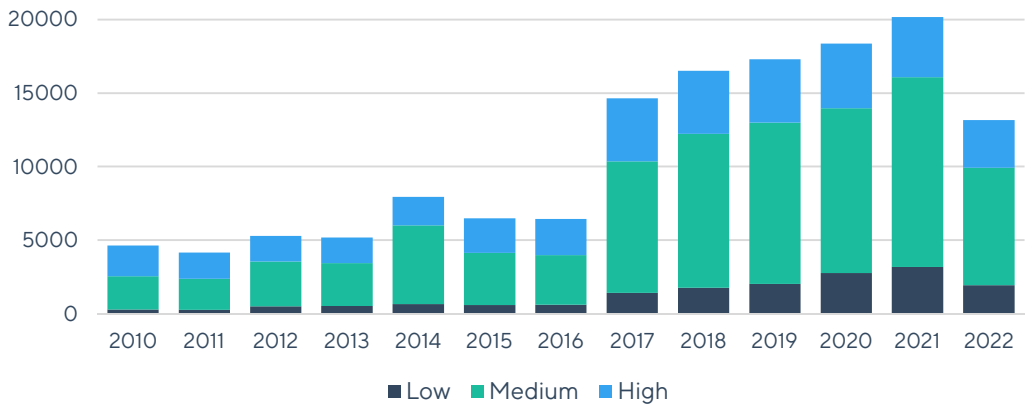
Rank	Registrar	Registrar IANA_ID	gTLD Domains under Management	Phishing Domains
1	GoDaddy.com, LLC	146	66,205,047	15,248
2	NameSilo, LLC	1479	4,532,558	13,371
3	NameCheap, Inc.	1068	13,993,839	11,586
4	PDR Ltd. d/b/a PublicDomainRegistry.com	303	4,902,630	9,276
5	ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED	3775	1,604,281	6,279
6	Hosting Concepts B.V. d/b/a Registrar.eu	1647	1,706,275	5,303
7	Wix.com Ltd.	3817	2,435,808	5,303
8	Alibaba Cloud Computing Ltd. d/b/a HiChina (www.net.cn)	1599	3,057,716	4,668
9	Porkbun LLC	1861	931,876	4,025
10	OwnRegistrar, Inc.	1250	688,866	3,927

Source: Cybercrime information center

Vulnerabilities

The number of new vulnerabilities reported over the past few years has steadily increased. From 14,000 new vulnerabilities reported in 2017 to over over 20,000 vulnerabilities in 2021 and now more than 13,000 new vulnerabilities thus far in 2022.

CVSS Severity Distribution over time (National Vulnerability Database)



Source: CVSS severity distribution over time. nvd.nist.gov

1

The proliferation of vulnerabilities and the speed at which threat actors are weaponizing these vulnerabilities is putting organizations at higher risk of data breaches.

Some of the most exploited vulnerabilities remain similar to those seen in 2021:
Log4Shell CVE-2021-44228

Known as: Log4Shell

Affects:
Apache's Log4j library (an open-source logging framework that is incorporated into thousands of products worldwide)

Exploitation method:
A threat actor can exploit this vulnerability by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows a cyber actor to take full control over the system.

Impact:
Ability to steal information, launch ransomware, or conduct other malicious activity

[1]

Proxylogon CVE-2021-26855, CVE-2021-26858, CVE-2021-26857, CVE-2021-27065

Known as: ProxyLogon

Affects:
Microsoft Exchange email servers

Exploitation method:
- CVE-2021-26855 allows an external attacker to evade the MS Exchange authentication process and impersonate any user.
- CVE-2021-26857: A hostile actor can exploit this vulnerability in conjunction with stolen credentials or the previously known SSRF vulnerability to execute arbitrary commands on a vulnerable Exchange Server in the SYSTEM security context.
- CVE-2021-26858 & CVE-2021-27065: are both post-authentication arbitrary file write vulnerabilities that allow an authorized user to write files to any path on a vulnerable Exchange Server.

Impact:
Allows attackers to bypass authentication, impersonate administrators and gain persistent access to files, mailboxes, and credentials stored on the servers.

ProxyShell CVE-2021-34523, CVE-2021-34473, CVE-2021-31207

Known as: ProxyShell

Affects: Microsoft Exchange email servers

Attackers generally target Exchange Servers to gain a foothold in a company's network in order to obtain access to sensitive information, as well as deliver ransomware and malware. Attackers use online scanners such as Metasploit module and Nmap script to find and exploit vulnerable Exchange Servers, making it easy for them to exploit these servers.

Exploitation method:

These vulnerabilities reside within the Microsoft Client Access Service (CAS), which typically runs on port 443 in Microsoft Internet Information Services (IIS). CAS is commonly exposed to the internet to enable users to access their email via mobile devices and web browsers.

- CVE-2021-34473 Microsoft Exchange Server Remote Code Execution Vulnerability. The attacker can force the vulnerable server to make requests to internal resources on his behalf. No authentication is needed in this case since the requests are made by the endpoints to the backend servers.
- CVE-2021-34523 Microsoft Exchange Server Elevation of Privilege Vulnerability. Grants privileged management role.
- CVE-2021-31207 Microsoft Exchange Server Security Feature Bypass Vulnerability. Allows an attacker to export mailbox content to a path and extension of their choosing even though it should only be letting them export in certain mail extensions.

Impact:

Successful exploitation of these vulnerabilities in combination enables a remote actor to execute arbitrary code[17] [18].

[17] https://blog.qualys.com/vulnerabilities-threat-research/2022/05/06/cisa-alert-top-15-routinely-exploited-vulnerabilities

[18] https://resources.infosecinstitute.com/topic/most-dangerous-vulnerabilities-exploited/

Malware

Cybersecurity vendor Akamai determined that the number of domains associated with malware or ransomware saw a 3% increase in Q2 compared to Q1[19]. Checkpoint found that the malicious file types most used for malware were .EXE and .PDF file types, where the majority of malware domains were registered under GoDaddy and under the TLD com. The top malware families in the beginning of 2022 include, Emotet, Formbook and AgentTesla.

Top 10 Domain Registrars by Malware Domains (Cybercrime Information Center)

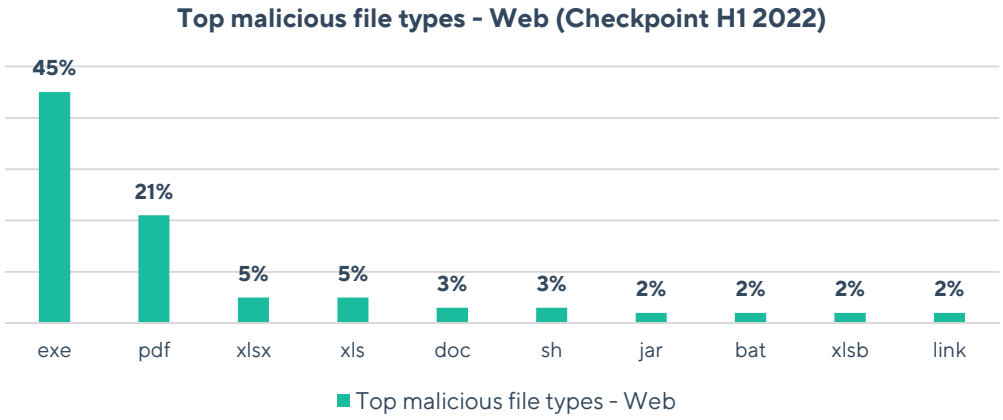
Rank	IANA_ID	Registrar	Total Malware Domains ▼
1	146	GoDaddy.com, LLC	2,799
2	303	PDR Ltd. d/b/a PublicDomainRegistry.com	1,562
3	1923	Gname.com Pte. Ltd.	1,232
4	1068	NameCheap, Inc.	1,165
5	1479	NameSilo, LLC	1,026
6	472	Dynadot, LLC	540
7	69	Tucows Domains Inc.	476
8	48	eNom, LLC	433
9	420	Alibaba Cloud Computing (Beijing) Co., Ltd.	314
10	955	Launchpad.com Inc.	20

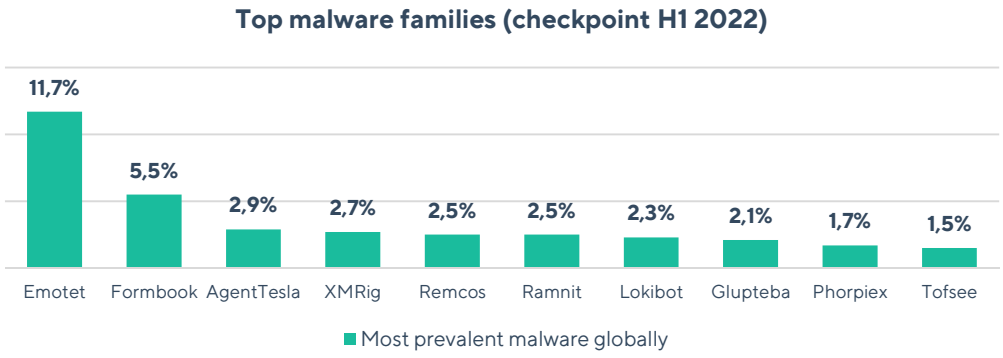
Top 10 TLDs by Phishing Domains (Cybercrime Information Center):

Rank	TLD	Total Malware Domains ▼
1	com	11,803
2	net	986
3	br	839
4	ru	670
5	org	651
6	in	524
7	ml	417
8	cloud	320
9	xyz	310
10	pl	258

Source: Cybercrime information center

[19] https://www.dnsfilter.com/newsroom/dns-data-shows-increased-malicious-domain-activity





Source: Checkpoints 2022 Mid-year report 'Cyber Attack Trends'

Emotet:

Type of malware: Trojan

First recorded: 2014

Attribution: Hacker group Mealybug

Distribution method: malicious email campaigns.

Spreads through malspam (spam emails containing malware), often impersonating familiar and trusted brands such as PayPal or DHL, to trick users.

Purpose/Impact:

- Used to download and install other malware: Trickbot, QakBot and Ryuk
- The malware is used to steal bank logins, financial data, and Bitcoin wallets.
- Emotet has compromised individuals, companies, and government entities across the US and Europe. But with Emotet being used to download and deliver other malware, the target list is potentially even bigger.

Formbook:

Type of malware: Infostealer trojan

First recorded: 2016

Attribution: This malware is commonly used by hackers with low programming knowledge and technical literacy.

Distribution method: Malicious email campaigns.

Usually via shipping-related and business-related email campaigns containing various file attachments. The most observed attachments include PDFs, DOC or EXE, or ZIP, RAR, ACE, and ISO files.

Purpose/Impact:

- Formbook harvests credentials from web browsers, collects screenshots, monitors and logs keystrokes, and is capable of downloading and executing files.
- Targets individuals and organizations worldwide using Windows systems.
- Sold as a malware-as-a-service (MaaS) on cyber criminal forums. Popular due to its ease of operation, stealing and evasion capabilities.

Agentesla:

Type of malware: Password stealer spyware

First recorded: 2014

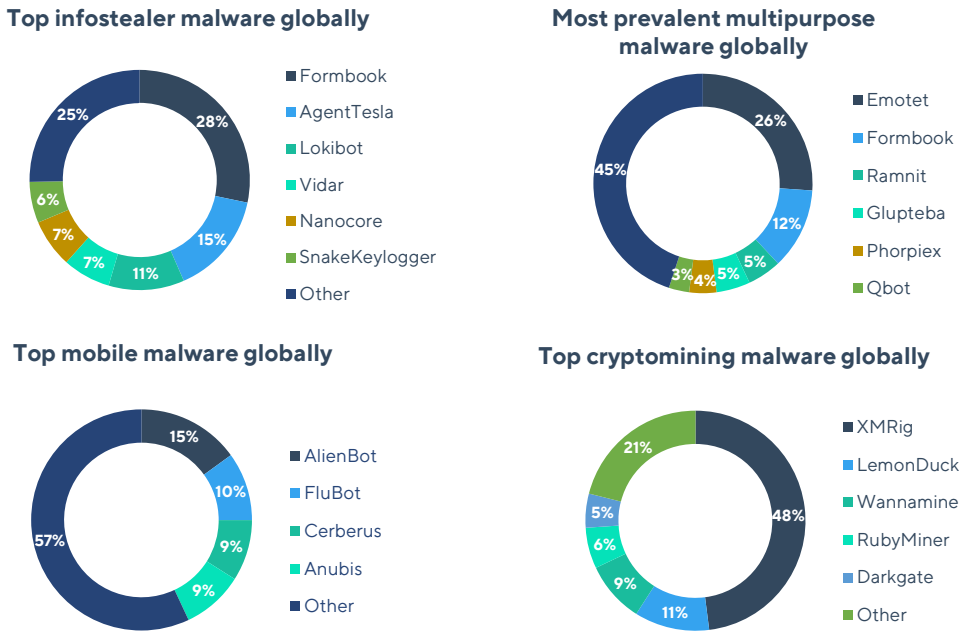
Attribution: It is thought that Agent Tesla spyware has originated in Turkey.

Distribution method: Malicious email campaigns.

Usually delivered to victims in malicious documents or links. Upon visiting a link a contaminated document is downloaded onto the victims computer. If the victim opens the document it triggers the download of the spyware which saves itself in the “%temp%” folder before automatically executing.

Purpose/Impact:

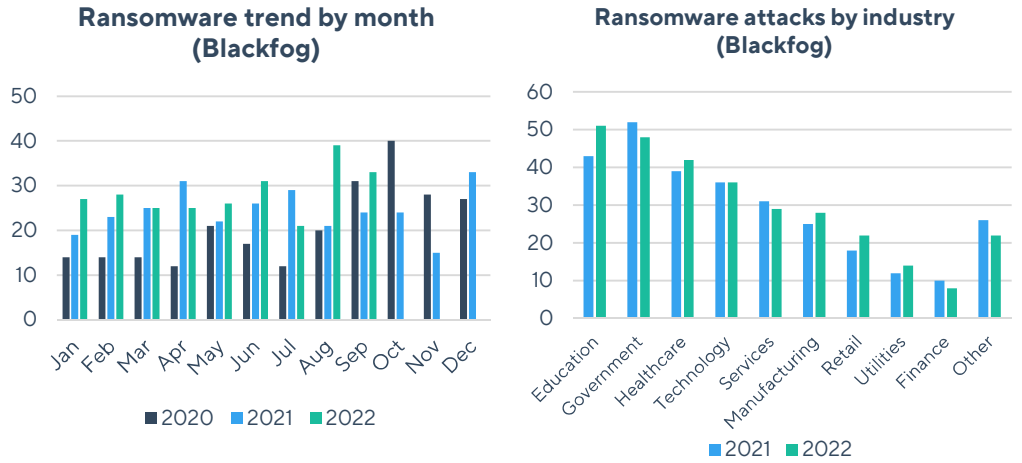
- Used to spy on victims, allowing the hacker to see everything that the victim is typing in supported programs and web-browsers.
- The malware is being marketed and sold on their website and has become extremely popular in the hacker community.
- The malware and associated email campaigns targets users worldwide from a wide variety of businesses.



Source: Checkpoints 2022 Mid-year report 'Cyber Attack Trends'

Ransomware

The first half of 2022 has seen an uptick in the amount of ransomware deployed. According to a Verizon report, ransomware increased with an almost 13% in 2021, a rise as big as the past five years combined[20]. In Q3 ransomware attacks generally increased with a huge increase in August compared to previous years. Additionally, the most targeted industries were education, government and healthcare.



The State of Ransomware in 2022

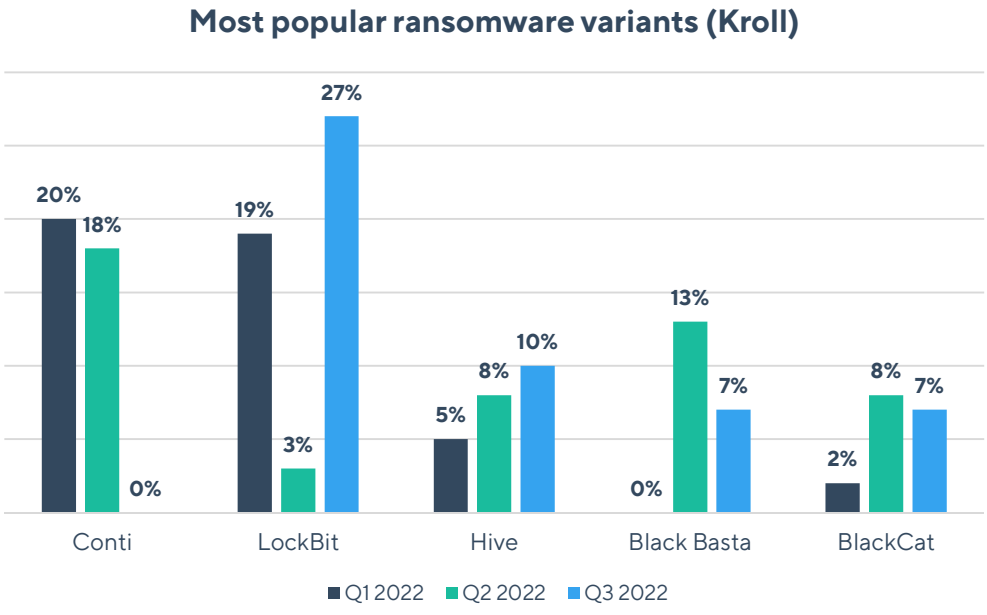
Source: Blackfog.

[20] https://arcticwolf.com/resources/blog/verizon-dbir-2022/

Some of the most recent innovations in ransomware attacks include double and triple extortion. Double extortion attacks occur when cybercriminals exfiltrate the data before they encrypt it, so when the victim is reluctant to pay the ransom, the attacker threatens to release the stolen data on the dark web, potentially exposing customer information and the organization's confidential data. In triple extortion, cybercriminals encrypt and exfiltrate the data and threaten to release it if the ransom does not get paid, while also contacting and threatening individuals who could be impacted by the data's release to pay a fee or risk that their private information gets exposed[21].

Additionally, some ransomware groups have started to employ a successful strategy wherein they solely rely on threatening to leak data without encrypting any files. More ransomware groups may decide to employ this strategy in the future.

- New groups detected in July: BianLian, Yanluowang, 0mega, Cheers, and RedAlert.
- New groups detected in August: D0nut, IceFire, DAIXIN, and Bl00dy. Unusually[22] [23]
- New groups detected in September: Sparta and Royal



Kroll Q3 Threat Landscape Report

[21] https://arcticwolf.com/resources/blog/dangers-of-double-and-triple-extortion/
[22] https://www.blackfog.com/the-state-of-ransomware-in-2022/#August
[23] https://www.malwarebytes.com/blog/threat-intelligence/2022/09/ransomware-review-august-2022

LockBit:

First seen: 2019

Attribution: Speculated to be Russian. LockBit's public communications include a broadly anti-Western political view, with indications of Russian origins with global affiliates.

About:

- LockBit's family of ransomware programs is self-spreading, and mainly deployed against high valuable victims who have the ability to pay a large ransom such as enterprises and government organizations.
- LockBit functions as ransomware-as-a-service (RaaS).
- LockBit 3.0 can encrypt and exfiltrate all the files on an infected device, allowing the attacker to hold the victim's data hostage until the requested ransom is paid[24].

Access to target network:

- LockBit primarily gains initial access to target networks through phishing campaigns, purchased access, unpatched vulnerabilities, insider access, and zero-day exploits.

Conti group:

First seen: 2020

Attribution: Speculated to be a Russia-based cybercrime group under the pseudonym Wizard Spider

About:

- Conti was very successful and popular group with around 600 campaigns in 2021 and a total revenue of around $2.7 billion in cryptocurrency.
- When Conti publicly stated their support for Russia in the Russia/Ukraine conflict in February 2022, a presumably former member of the group started leaking and exposing huge amounts of information about the group and their method of operation. The group has since gone off the grid.[25]

Access to target network:

- Conti ransomware was often delivered to victims through malicious links and excel sheets in email campaigns that contained TrickBot malware.
- Alternatively, Conti actors used Stolen or weak Remote Desktop Protocol (RDP) credentials, fake phone calls, fake software, and unpatched vulnerabilities to gain initial access to different networks.

[24] https://www.blackberry.com/us/en/solutions/endpoint-security/ransomwareprotection/lockbit#:~:text=The%20LockBit%20gang%20maintains%20a,part%20of%20their%20business%20model.
[25] https://cyberint.com/blog/research/contileaks/

Black Cat (aka ALPHV and Noberus):

First seen: 2021

Attribution: Coreid (aka FIN7, Carbanak, or Carbon Spider). Is said to be a rebranded successor of DarkSide and BlackMatter.

About:

- The threat actors use the double extortion technique and run a ransomware-as-a-service (RaaS) operation, wherein the core developers enlist the help of affiliates in carrying out attacks in exchange for a cut of the illicit proceeds.
- ALPHV is one of the first strains programmed in Rust, a trend which has since been adopted by other families in recent months in order to develop and distribute cross-platform malware[28].

Distribution method:

- The malware gains initial access to targeted systems using compromised user credentials[29].

[26] https://heimdalsecurity.com/blog/what-is-conti-ransomware/
[27] https://www.bleepingcomputer.com/news/security/google-says-former-conti-ransomware-members-now-attack-ukraine/
[28] https://thehackernews.com/2022/09/blackcat-ransomware-attackers-spotted.html
[29] https://www.cisecurity.org/insights/blog/breaking-down-the-blackcat-ransomware-operation

Black Basta:

First seen: 2022

Attribution: Unkown

About:

- The ransomware group cooperates with QuakBot (Qbot) malware operators to distribute ransomware.
- Different ransomware variants within the Black Basta group, making them capable of impacting Windows, Linux, and ESXi VM images.
- The ransomware group uses the double extortion technique[30].
- Black Basta has mainly targeted victims in North America followed by Europe and the Asia-Pacific[31].

Distribution method:

- Black Basta mainly uses Malspam (pshishing) and Insiders to gain access to different networks[32].

Hive:

First seen: 2021

Attribution: Unkown

About:

- The threat actor is known to run a ransomware-as-a-service (RaaS) operation, where the developers work on the ransomware, and they have affiliates to conduct the attacks.
- Hive ransomware has been used to target a wide range of businesses and critical infrastructure sectors.

Distribution method:

- Hive ransomware's initial access method is dependent on the affiliate.
- Hive actors have previously gained access to a victim networks through unpatched vulnerabilities, by distributing phishing emails with malicious attachments, and through single factor logins via Remote Desktop Protocol (RDP), virtual private networks (VPNs), and other remote network connection protocols.

[30] https://www.picussecurity.com/resource/black-basta-ransomware-gang
[31] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta
[32] https://cyberint.com/blog/research/blackbasta/

Upcoming quarter/ Recommendations:

Phishing attacks tend to increase around holiday seasons. With black Friday, thanksgiving and christmas coming up, expect to see an increase in social engineering attacks promoting 'good deals' for customers to save money.

With the trends in phishing, malware and ransomware attacks continuously increasing, expect to see those trends continue to rise.

Be prepared for an extended period of heightened risk as the war in Ukraine continues to pose threats towards Western organisations and businesses. Additionally, the heightened risk can cause fatigue in cyber security professionals, therefore, businesses must ensure that there are enough professionals in the team so they are not overworked as stressed employees equal a higher probability of mistakes occurring.

The growing appearance of deepfake attacks is significantly reshaping the threat landscape for organizations and enterprises, financial institutions, celebrities, political figures, and ordinary people. Expect to see attacks using deepfake become increasingly sophisticated.

1

Sources

[1]

[2] Insider, ThreatPost

[3] Oktapus Phishing Breach

[4] BleepingComputer, Link2

[5] BleepingComputer, The Hacker News

[6] France24

[7] Zdnet

[8] Acronis

[9] BleepingComputer

[10] The Cyber Wire

[11] BleepingComputer

[12] https://www.proofpoint.com/uk/newsroom/press-releases/proofpoints-2022-state-phish-report-reveals-email-based-attacks-dominated

[13] https://blog.barracuda.com/2022/03/16/spear-phishing-report-social-engineering-and-growing-complexity-of-attacks/

[14] https://www.interisle.net/PhishingLandscape2022.html

[15] https://www.helpnetsecurity.com/2022/09/26/phishing-activity-trends-2022/?web_view=true

[16] https://cybercrimeinfocenter.squarespace.com/phishing-activity-numbers-may-july-2022

[17] https://blog.qualys.com/vulnerabilities-threat-research/2022/05/06/cisa-alert-top-15-routinely-exploited-vulnerabilities

[18] https://resources.infosecinstitute.com/topic/most-dangerous-vulnerabilities-exploited/

[19] https://www.dnsfilter.com/newsroom/dns-data-shows-increased-malicious-domain-activity

[20] https://arcticwolf.com/resources/blog/verizon-dbir-2022/

[21] https://arcticwolf.com/resources/blog/dangers-of-double-and-triple-extortion/

[22] https://www.blackfog.com/the-state-of-ransomware-in-2022/#August

[23] https://www.malwarebytes.com/blog/threat-intelligence/2022/09/ransomware-review-august-2022

[24] https://www.blackberry.com/us/en/solutions/endpoint-security/ransomwareprotection/lockbit#:~:text=The%20LockBit%20gang%20maintains%20a,part%20of%20their%20business%20model.

[25] https://cyberint.com/blog/research/contileaks/

[26] https://heimdalsecurity.com/blog/what-is-conti-ransomware/

[27] https://www.bleepingcomputer.com/news/security/google-says-former-conti-ransomware-members-now-attack-ukraine/

[28] https://thehackernews.com/2022/09/blackcat-ransomware-attackers-spotted.html

[29] https://www.cisecurity.org/insights/blog/breaking-down-the-blackcat-ransomware-operation

[30] https://www.picussecurity.com/resource/black-basta-ransomware-gang

[31] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

[32] https://cyberint.com/blog/research/blackbasta/

Follow Us