nccgroup

FOX IT
part of nccgroup

Threat Monitor

Annual Report 2023

nccgroup.com

FOREWORD

In this year's Annual Cyber Threat Monitor Report, we take a look back at the key events that shaped the cyber threat landscape in 2023, as well as looking ahead at the year to come, sharing insights from our Cyber Threat Intelligence team here at NCC Group.

2023 appeared to show signs that the international community beginning to take the threats from cyber adversaries more seriously.

We saw several examples of coordinated law enforcement action against criminal groups including key ransomware operators and individuals believed to be acting on behalf of foreign intelligence services. There was also consensus on the issue of ransomware, in that governments around the world have showed a united front against ransom payments and intelligence sharing through The International Counter Ransomware Initiative, which introduced several measures that offer a real opportunity to fight back against the pervasive threat from ransomware operators.

However, despite this, we saw the highest volume of ransomware victims NCC Group has ever recorded with an 84% increase in 2023 alone. The sheer volume of attacks and different types of victims proves that no organisation is safe.

Notably, ransomware operators employed new and innovative techniques to maximize their profits, targeting big software creators and managed service providers. So, even if an organisation does not perceive a direct threat from ransomware, it should consider the potential impact on its supply chain.

The ongoing threat to critical national infrastructure across the globe by hacktivists and Foreign Intelligence Services continued in 2023, following on from multiple geo-political conflicts in the Middle East, Eastern Europe, and Asia. National Cyber Security Centres in multiple countries have highlighted this threat and it is something we are monitoring as a priority moving in to 2024.

With those few things in mind, here we give further insight into what was a challenging 2023, and what organistions should be focusing on in the year ahead.

Matt Hull

Global Head of
Threat Intelligence

CONTENT

SECTION 01

CRITICAL EVENTS TIMELINE

10th Jan
Ransomware

Royal Mail attack

Royal Mail suffered 6 weeks of disruption to international postal services, affecting 11,500 Post Office branches.

This was due to a LockBit affiliate driven ransomware attack, with Royal Mail refusing to pay the ransom.

30th Jan
Hacktivism

Killnet targets NATO countries supporting Ukraine

Pro-Russian Hacktivist group, Killnet, launched DDoS attacks against US healthcare organisations and public healthcare sectors.

This followed claims the group had successfully compromised US Healthcare organisations. The motivation is believed to be the retaliation against countries in support of Ukraine, with DDoS attacks also focused on other NATO countries.

7th Mar
Malware

Emotet returns with new evasion techniques

Emotet was observed returning after a period of hiatus, with new evasion techniques, allowing it to continue to send malicious spam to victims, as well as steal credentials and email addresses, whilst enabling lateral movement and download further malware.

It has been observed being used by Ransomware groups to distribute their ransomware payloads.

2nd Feb
Ransomware

GoAnywhere MFT Zero-Day exploited by CL0P

Remote Code Injection flaw, CVE-2023-0669, on exposed administrative consoles of GoAnywhere secure web file transfer solution was shared by Fortra.

Reports at the time indicated that it had been actively exploited by threat actors, and later shown to be the case that CL0P ransomware group was using this flaw in a spate of ransomware attacks.

14th Mar
Surveillance

Russian state-sponsored TA targets EU diplomatic entities and systems

Nobelium, aka APT29 and Cozy Bear, targeted European diplomatic missions and systems sharing sensitive political information, aiding the Ukrainian government, and helping Ukrainian citizens flee.

This group is affiliated with the Foreign Intelligence Service of the Russian Federation (FVR) and was targeting Polish representatives of the Ministry of Foreign Affairs visiting the US with a spear-phishing campaign compromising the official EU electronic document exchange system, LegisWrite.

8th Aug
Police Force: Data Leak

FOI request leads to acci-dental PII data leak

In response to a Freedom of Information (FOI) request made to the Police Service of Northern Ireland, a spreadsheet detailing the locations and names of serving employees was mistakenly made public and posted online, putting these employees at risk.

Police forces in Norfolk and Suffolk also confirmed FOI requests led to inadvertently sharing too much Personally Identifiable Information (PII) publicly, whilst Cumbria Police blamed human error for the publication of the names and salaries of all its officers online.

31st Aug
Malware Infamous Chisel

Ukraine Military Devices targeted by Russian GRU

NCSC and its Five Eyes partners issue a report associating Infamous Chisel Malware targeting Ukrainian military Android devices, with the threat actor, Sandworm.

The malware allows for data exfiltration and remote access.

The campaign is believed to be part of the Russian war efforts against Ukraine.

11th Jul
Breach

Microsoft China Storm-0558

Using forged authentication tokens, Microsoft revealed that Customer email accounts were accessed using Outlook Web Access (OWA) Exchange Online.

China based threat actor, Storm-0558 is believed responsible, using the access to email accounts to gather useful intelligence.

31st May
Ransomware

Move-IT Managed File Transfer vulnerability in mass Cl0p exploitation

Progress released a security advisory regarding a Zero-Day vulnerability, CVE-2023-34362, in their managed file transfer (MFT) software package, which had been used to exfiltrate data.

Ransomware group CL0P was seen to be leveraging this flaw, alongside other File Transfer vulnerabilities, to steal data to demand ransom payments.

23rd May
Barracuda

Zero Day Vulnerability Replace, don't patch, vulnerable devices

Barracuda announced a zero-day vulnerability in their Email Security Gateway, CVE-2023-2868, which had been exploited in the wild, the threat actor believed to be the Chinese state affiliated UNC4841, leveraging the flaw for espionage.

The threat actor quickly adapted to containment and remediation efforts, leaving Barracuda to take the unusual step of recommending customers replace their existing appliances with new ones, rather than rely on more typical remediation efforts.

14th Apr
Papercut: Ransomware

Zero-Day actively exploited by Russian threat actors

Print Management Software maker, Papercut, announced Remote Code Execution (RCE) vulnerabilities in Papercut NG and Papercut MF, which could be levered without authentication in this critically rated CVE.

A user account data flaw affecting Papercut NG and Papercut MF was also discovered, and both were known to be exploited by threat actors. Papercut has 100+ million customers worldwide. Groups such as LockBit then leveraged this flaw in ransomware attacks.

29th Mar
Supply Chain Attack

3CX Voice Over Internet Protocol (VOIP) desktop client compromised

North Korean threat actors expected to be responsible for the compromise, which was used to go on to comprise 3CX customers critical infrastructure organisations within the energy sector.

A trojanised version of the legitimate 3CX software was used to compromise their customers. What set this attack apart is that the attack was the result of an earlier supply chain attack, with a 3CX employee downloading malware infected software package.

20th Sept
FBI & CISA Advisory

Law Enforcement – Snatch Ransomware

The FBI and CISA released an advisory warning that Snatch threat actor group were targeting a wide range of Critical National Infrastructure (CNI) sectors for ransomware attacks.

Sectors targeted included the Defence Industrial Base (DIB), Food and Agriculture as well as Information Technology sectors.

27 Sept
Law Enforcement

Dual Ransomware Advisory

The US Federal Bureau of Investigation (FBI) shared a Private Industry alert warning of an increasing trend of dual ransomware, where victims were targeted with more than one ransomware attack in close succession, with threat actors using different types of ransomware in each instance.

Also noted was an increased use of wiper malware to destroy data, amongst other tactics to pressure victims to pay ransom.

27th Sept
Law Enforcement

US and Japanese warn of Chinese exploitation of Cisco Router Firmware

China remains active in its offensive cyber capabilities, warned US and Japanese security agencies as organisations in both countries were targeted by People's Republic of China-linked threat actors, BlackTech. Government, Industrial, Technology, Media and Telecommunication organisations were amongst US and Japanese targets, with attackers leveraging flaws in Cisco routers.

The group breaches network devices for international subsidiaries to then pivot to corporate headquarters.

7th Oct
Ransomware

Caesars Casino

Hackers exfiltrated data from the hotel and casino giant. They paid $US 15,000,000 after negotiating on the ransom. The threat actor suspected to be responsible is Scattered Spider, aka UNC3944.

7th Oct
Geopolitics

Hamas attack on Israel

Palestinian group, Hamas, officially designated in many countries as a terrorist organisation, launched an armed assault against Israel.

1,200 civilians were killed in the attacks making this one of the deadliest attack in Israel's history. Hostages were also taken. 2 days later, the Israeli government announced a complete siege of Gaza, as a result of which over 23,000 Palestinians have since been killed.

10th Oct
23andMe: Data Breach

Genetic Company hacked, and genetic ancestry data leaked

A successful credential stuffing attack allowed a threat actor to directly access 14,000 23andMe customer records, stealing genetic ancestry information and, in some cases, health related detail based on the genetics. Some of the stolen detail was leaked online and the criminals offered the records for sale, putting at risk particular groups.

Using the access to these accounts allowed the threat actor to pivot from there to scrape some detail from 6.9 million customers.

12th Oct
Ransomware

MGM Casino

MGM shared details of a ransomware attack, which included the theft of customer data, and cost to the business in the region of $US 100,000,000.

BlackCat, aka AlphV subgroup of Scattered Spider, took responsibility for the attack, in which the casino refused to pay the ransom.

12th Dec
Hack

Kyivstar Telco company disclosed records destroyed by Russian state affiliated TA

Russian threat actor, Sandstorm, believed responsible for an attack which disrupted Ukraine's largest mobile network operator so severely, that its customer base of half the population of Ukraine was left without services for days.

This also meant they would not receive alerts warning of Russian attacks, therefore endangering life. The attack wiped out 'almost everything', leaving infrastructure decimated.

SECTION 02

INCIDENTS OF NOTE

Hybrid Warfare: Gaza conflict

Throughout the year, the Russia and Ukraine conflict continued. However, the 7th October 2023 saw the Islamic Resistance Movement (Hamas) launch a surprise military operation against Israel. The cyber threat landscape has seen an interesting mirroring of the Russia-Ukraine conflict with hacktivism at the forefront of the cyber threat.

Mostly targeted against Israeli infrastructure, the activity has typically impacted the Availability vector of the CIA triad through Denial of Service (DoS) attacks. Furthermore, for the greatest impact, adversaries have been targeting Critical National Infrastructure sectors such as Energy and Defence, Telecommunications and Government to have the largest impact for their respective side.

The adversarial groups have also had a keen interest and relative success rate with specific targeting of Industrial Control Systems (ICS), in particularly SCADA.

Companies targeted through digital supply chain: File sharing platforms targeted

Throughout 2023, file sharing platforms were exploited across the globe to compromise organisations using them for data extortion and ransomware attacks.

Fortra's GoAnywhere MFT software was targeted early in the year through a zero-day vulnerability tracked as CVE-2023-0669, which leveraged remote command execution to deploy ransomware to the userbase.

CL0P managed to successfully breach 130 companies and exposed millions of individual's private data using this vulnerability. This flaw was patched in version 7.1.2.

Furthermore, in June 2023, MOVEit was exploited through additional zero-day vulnerabilities tracked as CVE-2023-35708 and CVE-2023-34362.

This attack had far-reaching consequences, including organisations that had supply chain usage of the tool.

This attack has been documented as the biggest data theft of 2023, with over 2,000 organisations compromised and the data theft impacting 62 million individuals. Patches are available for these vulnerabilities and should be applied.

Supply chains continue to be breached: Capita Breach

In March 2023, Capita, an outsourcing company suffered a data breach which impacted 90 organisations.

Capita suffered an unauthorised intrusion into their Microsoft 365 applications and had Black Basta ransomware deployed to 0.1% of their server estate.

This was reduced due to the intervention of Capita to stop movement. However, the reputational damage and financial impact has been costly for the company as they suffered direct cyber incident costs of around £25m. The groups share price dropped 12% showing the reputational damage of the attack starting to show in public markets.

The costs continue to mount for the company too, as they lost £67.9m for the first six months to June 2023 compared to a profit of £100,000 a year earlier.

The company attributed these losses to the fall out of the cyber incident and cannot determine the size of the fine yet.

This attack shows the real impact that supply chains can have on organisations and proves the need to hold third parties to the same security standards as your own organisation, which might include standards such as ISO27001.

Data compromise exposes data for hundreds of millions of individuals: KidSecurity app

In September 2023, a tracking app for parents to know where their children are, KidSecurity, was found to have not configured authentication for their Elasticsearch and Logstash collections.

The app with over 1,000,000 downloads from the Google Play store inadvertently left user activity logs publicly available to the internet for over a month. The instance contained over 300 million records with private data including 21,000 phone numbers and 31,000 email addresses.

This exposure also showed payment details including the first six and last four digits of card numbers, expiry dates and the issuing bank. There have been indications that threat actors have leveraged this misconfiguration to leak the data. Open instances of Elasticsearch are often leveraged by attackers to exploit vulnerabilities.

Ransomware re-encryption after failed negotiations: Henry Schein ransomware and data breach

In October 2023, healthcare solutions giant Henry Schein suffered from re-encryption of their files after negotiations stalled with the ransomware group Alphv. The group claimed to have 35TB of sensitive data.

The re-encryption happened just as the company got back to operating capabilities, so this was a big setback for the company and caused a lack of availability for its applications and ecommerce platform which triggered another two weeks of operational disruption.This breach included 35,000,000 records.

Ransomware halted physical delivery: Royal Mail hit by LockBit

In January, Royal Mail discovered a cyberattack which halted their international shipping services due to what they referred to as, “severe service disruption.”

It later surfaced that the threat group responsible for the attack was LockBit, who announced their role in a post published on a Russian-speaking hacking site. Royal Mail were able to re-establish most of their international shipping services by the 3rd of February on Twitter, and declared that they were fully operational on the 21st of February 2023.

On the 23rd of February, LockBit leaked 44GB of data stolen from Royal Mail, as they refused to pay the £66 million ransom due to it being ‘an absurd amount of money.’

The leaked data included files relating to “various parts of Royal Mail’s business…technical information, contracts with third-party suppliers, human resource and staff disciplinary records, details of salaries and overtime payments, and even one staff member’s Covid-19 vaccination records.”

The ransom has since lowered to £33m, but Royal Mail have shown no signs of giving in to the threat groups demands.

This is an excellent example of the real-world implications of cybercrime, notably where operational disruption is concerned, with the impact extending beyond the victim itself. UK residents were forced to use alternative shipping solutions for their international exports, also highlighting the impact on customer confidence.

SECTION 03

LAW ENFORCEMENT INTERVENTIONS

TrickBot:

Trickbot is a banking trojan which started off as a derivative of the Dyre banking trojan in 2016 before evolving independent features which turned it into a flexible and modular piece of malware, enabling cybercriminals to deploy multiple payloads including malware.

Joint sanctions between the United Kingdom and the United States were levied against 11 named individuals believed to have been involved in the development of the TrickBot trojan. Additionally, two individuals have been arrested and faced charges relating to their involvement with the banking trojan, a Latvian national, Alla Witte, plead guilty to conspiracy to commit computer fraud for their involvement with the group, and in June 2023 was sentenced to 32 months imprisonment.

Additionally, Russian national Vladimir Dunaev, was arrested in South Korea in September 2021 and was extradited to the United States; he plead guilty to committing computer fraud and identity theft as well as conspiracy to commit wire fraud and bank fraud, and faces up to a maximum of 35 years in prison upon his scheduled sentencing on 20 March 2024.

Sanctions against North Korea:

In May, the US Treasury Department's Office of Foreign Assets Control (OFAC) levied sanctions against four corporate, government, and academic entities as well as one individual for their involvement in international fraud for the purposes of raising funds for the North Korean regime.

Thousands of workers hide their identity to be hired as IT professionals overseas in order to generate revenue for the government through receiving foreign salaries and funnelling them back to Pyongyang.

Some of these workers receive salaries in excess of a quarter of a million dollars, and while this may not be applicable for every one of the illicit IT workers, the economy of scale through utilising thousands of agents means the Kim regime is able to generate significant funds.

US Secretary of State, Anthony Blinken, summarises the issue as:

"The DPRK conducts malicious cyber activities and deploys information technology (IT) workers abroad who fraudulently obtain employment to generate revenue that supports the Kim regime . . . The DPRK's extensive illicit cyber and IT worker operations threaten international security by financing the DPRK regime and its dangerous activities, including its unlawful weapons of mass destruction (WMD) and ballistic missile programs."

BreachForums and Pompompurin

US authorities in March arrested the threat actor responsible for successfully hacking the FBI in 2021. Conor Brian Fitzpatrick, known online by his alias Pompompurin, and is also connected to the FBI's InfraGard network breach in 2022, the 2022 Twitter data leak, the 2021 Robinhood hack, as well as being the owner of BreachForums.

BreachForums rose to take the place of RaidForums after its own takedown at the hands of the FBI in 2022 and has been host to such data as PII of roughly 170,000 individuals affected by the DC Health Link breach in March 2023.

Only 20 at the time of his arrest, Fitzpatrick was charged with three crimes: conspiracy to commit access device fraud; solicitation for the purpose of offering access devices; and possession of child pornography.

Held on a $300,000 bond paid by his parents, Fitzpatrick has since pled guilty to all three charges and faces up to a maximum of 40 years behind bars.

Ukrainian phishing ring busted

Ukrainian cyber authorities apprehended members of a phishing ring responsible for stealing over £3 million/160 million Ukrainian hryvnia from over one thousand victims spread across Poland, Spain, France, Portugal, Czechia, and other European nations.

Joint raids were conducted on over 30 locations, resulting in the seizing of computer equipment, mobile phones, and numerous SIM cards used as part of numerous phishing campaigns.

The perpetrators of these campaigns created over 100 different phishing sites to trick victims into thinking they could purchase cheap goods, upon which the scammers would then use the payment card details for further fraudulent campaigns.

In addition to the phishing sites themselves, the group employed scammers in call centres based in Lviv and Vinnytsia for the purposes of adding legitimacy to the fake online stores through talking to victims and encouraging them to complete purchases.

This operation was conducted in collaboration with authorities from Czechia and resulted in two arrests made within Ukraine, as well as 10 more in undisclosed countries in Europe.

The suspected leaders face charges on fraud and creating criminal organisations and could face up to 12 years in jail if successfully prosecuted.

Spanish authorities arrest 40 members of the Trinitarios group

Authorities in Spain arrested 40 members of the notorious Trinitarios crime group in May.

The group was responsible for carrying out numerous fraud campaigns, facilitated by initial phishing and smishing attacks with which they gained banking and payment card details of victims, used to generate approximately €700,000 from over 300,000 victims.

Some of the proceeds were used to pay the legal fee of members who were already incarcerated, bought drugs for resale, as well as to purchase property in the Dominican Republic.

13 homes located across Spain in Madrid, Seville, and Guadalajara, were raided as part of the campaign to arrest the gang members, resulting in the seizure of computer equipment and cash, as well as tools for conventional crimes such as lock picks.

Amongst the 40 individuals arrested, there are thought to be two hackers who were primarily responsible for carrying out phishing and smishing attacks, as well as 15 others who are charged with crimes such as bank fraud and identity theft, typical crimes resulting from falling victim to a phishing attack.

This case shows how the gap between cybercrime and conventional crime is narrowing as the two fields merge.

LockBit affiliate arrested

A Russian national was arrested and charged in June for his role as an affiliate of the LockBit Ransomware-as-a-Service (RaaS) group.

Ruslan Astamirov is accused of at least five attacks between 2020 and early 2023 against victims across the globe, including in the United States.

He faces charges of conspiring to commit wire fraud and conspiring to intentionally damage protected computers and to transmit ransom demands, and faces up to a maximum of 25 years in prison.

This second LockBit arrest in six months prompted the U.S. Attorney Philip R. Sellinger for the District of New Jersey to say;

“The LockBit conspirators and any other ransomware perpetrators cannot hide behind imagined online anonymity.

We will continue to work tirelessly with all our law enforcement partners to identify ransomware perpetrators and bring them to justice.”

6,500 arrests plus nearly a billion seized

Following its initial compromise by European law enforcement agencies in 2020, further efforts have targeted the userbase of EncroChat.

The encrypted communications platform which ran on a specially hardened version of the Android operating system offered users self-destruct features, panic wipe capabilities, 24/7 customer support, and more for a one-time payment of €1,000 and €1,500 for a 6 month subscription.

More than 6,500 arrests have since been made, including of 197 high-value targets. This was done through analysing over 100 million conversations between approximately 60,000 users of the platform.

Through utilising this data, law enforcement agencies across Europe were able, in addition to the thousands of arrests, seize 270 tons of narcotics, 971 vehicles, 271 properties, 923 weapons, 68 explosives, 40 planes, 83 boats, as well as €740 million in cash in addition to freezing a further €154 million.

Europol states that a third of EncroChat users were members of organised crime groups, a third were drug traffickers, while the rest were included money launderers, murderers, and firearms traffickers.

This campaign sent shockwaves through OCGs (Organised Criminal Groups) across Europe, and further highlighted the intersection between conventional criminal activity and cyber-enabled crimes.

Man indicted after acting as malicious insider against water treatment facility

July saw the indictment Rambler Gallo, a former employee of a Massachusetts based company operating at the Discovery Bay Water Treatment Facility in California, after his alleged attack on the facility in January 2021.

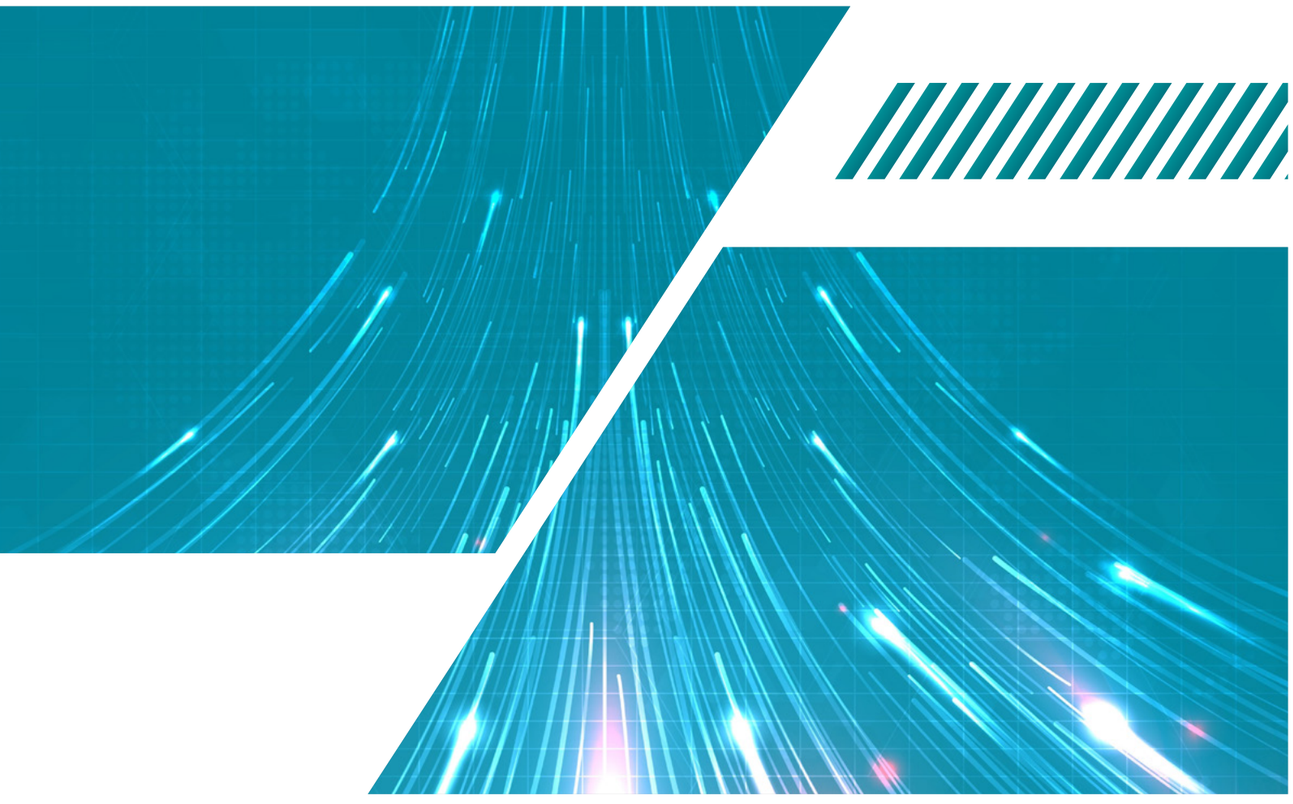
Gallo, the former Instrumentation and Control Tech at the facility, is alleged to have installed software on his own private computer as well on the private internal network of his employer, and, upon resignation from the company in January 2021, exploiting his remote access to uninstall software which was the main hub of the network and which was responsible for protecting the entire water treatment system including filtration, chemical levels, and water pressure.

He faces up to 10 years behind bars and up to $240k for the charge of transmitting a program, information, code, and command to cause damage to a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i).

This Discovery Bay facility attack, as well as the similar attack on the water system of Oldsmar in early 2021, likely contributed to the March 2023 decision of the Biden administration to make the conducting of cyber security audits on public water systems mandatory.

SECTION 04

INCIDENT RESPONSE FINDINGS



Our Incident Response data represents cases handled by our CIRT Team when responding to NCC clients. In 2023, the Financials sector observed the greatest percentage of incidents raised (15%), closely followed by Industrials (14%) and Government (14%).

This reflected a shift in the top-three targeted sectors in 2022, from Government (18%), Industrials and Financials in joint second (13%) and Technology and Consumer Cyclicals (11%) in joint third.

Over the last two years, the data suggests that Financials and Industrials remain of consistent interest to threat actors, with a growth of 2% in incident response cases for the Financials sector between 2022 and 2023.

This is likely a combination of the potential for financial gain understood by cybercriminals where targeting these sectors successfully, as well as the continued need for sufficient cyber security hygiene to combat ever growing cyber threats.

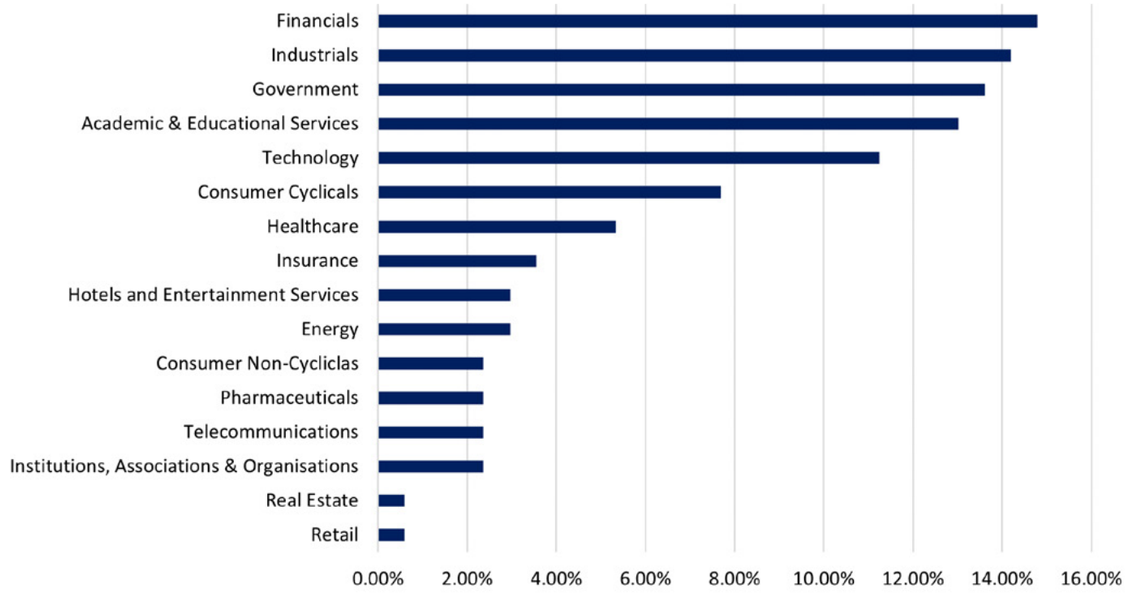


Figure 1: Percentage of CIRT Cases by Sectors Impacted

Analysis of attack categories found that most incidents concerned Unauthorised Access (36%), Phishing (16%) and Malicious Code (15%).

Where the top-targeted sector was concerned, Financials, most attacks were related to Unauthorised Access (5%) and Phishing (5%).

Remaining aware of possible signs of authorised access such as unusual activity on devices, as well as ensuring appropriate phishing training and awareness can support organisations to prevent or minimise potential attacks.

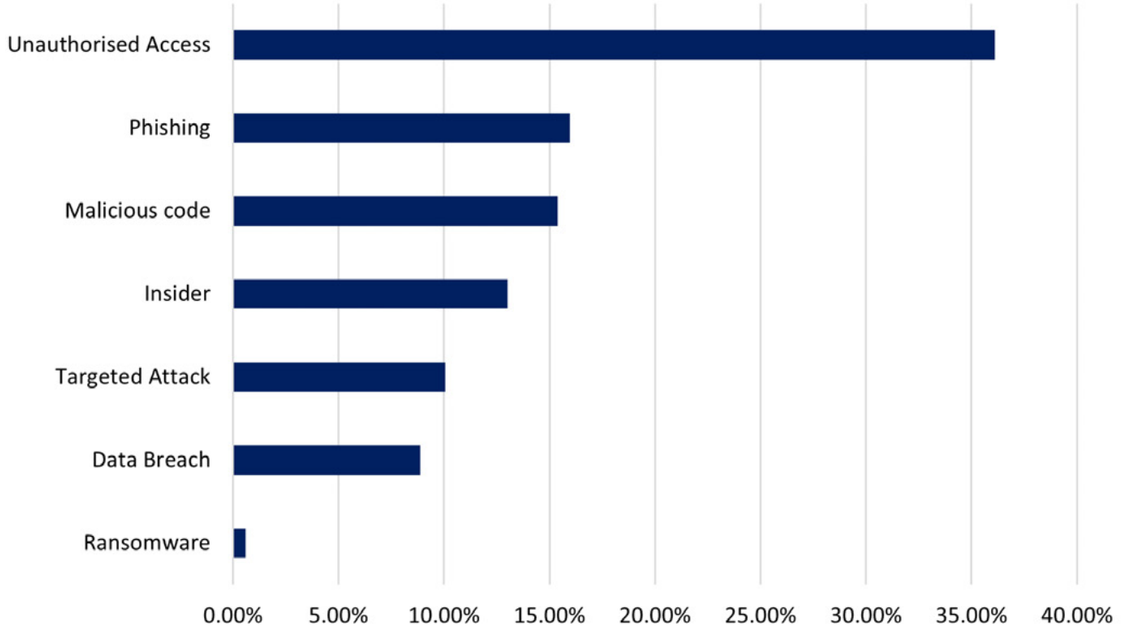


Figure 2: CIRT Cases by Attack Type 2023

SECTION 05

SOC FINDINGS

Data collated from our Global Security Operations Centre (SOC) reported 3493 true positive incidents across the European and APAC SOCs. 2023 saw a 36% increase from the 2559 true positive cases observed in 2022, 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 NCCs 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.

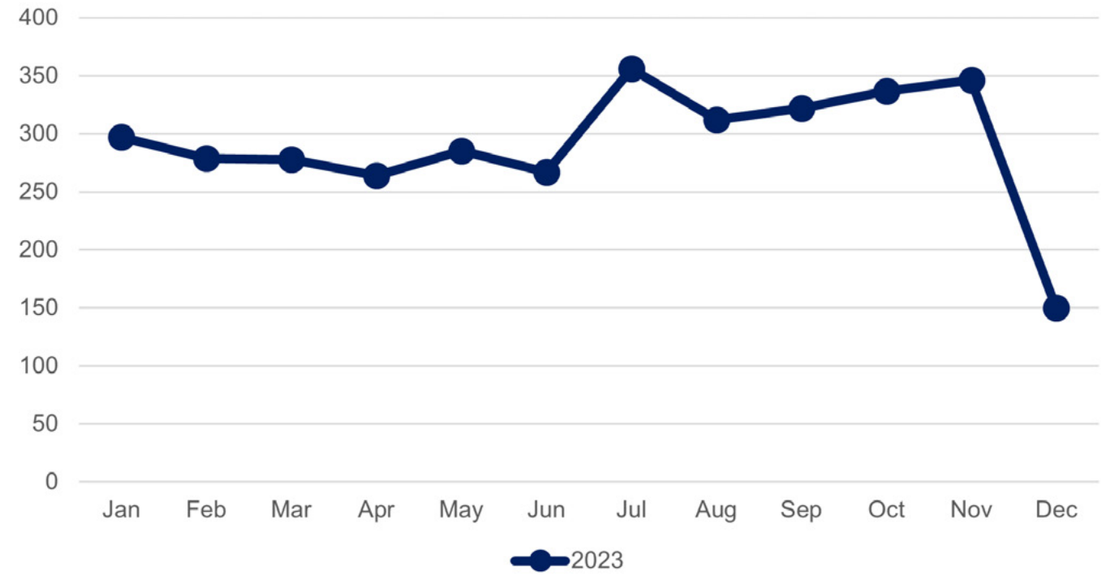


Figure 3: Month-by-Month Count of Incidents Raised in the SOC (2023)

July recorded the greatest number of tickets raised with 356 in total, followed by November in second place with 336.

Comparing with the figures for 2022 (see Figure 4) we instead saw a steady growth for the period January-May with a peak in May with 297 tickets raised.

This was followed by a drop in June with 175 and a growth spurt again for the period June – September; with the highest number of tickets recorded for 2022 being in September or a total of 350.

However, this peak was again followed by a rapid decline for the period October – December, ending the year with 192 tickets raised in December.

As seen in Figure 3, we observe a much steadier flow of tickets raised in 2023 for the period January – June. After which, we notice the peak to 356 tickets raised in July, followed by a slight decrease to 312 in August then we see a steady increase for the period September - November.

Similar to the previous two years, the month of December tends to mark some of the lowest ticket activity recorded throughout the year as whole. In 2023, we observe that the lowest number of tickets raised was in fact in December with a total of 150.

It is, however, difficult to pinpoint a root cause for the spike in July and November activity as a number of variables may be at play, from client security practices to a growth in cybercrime activity.

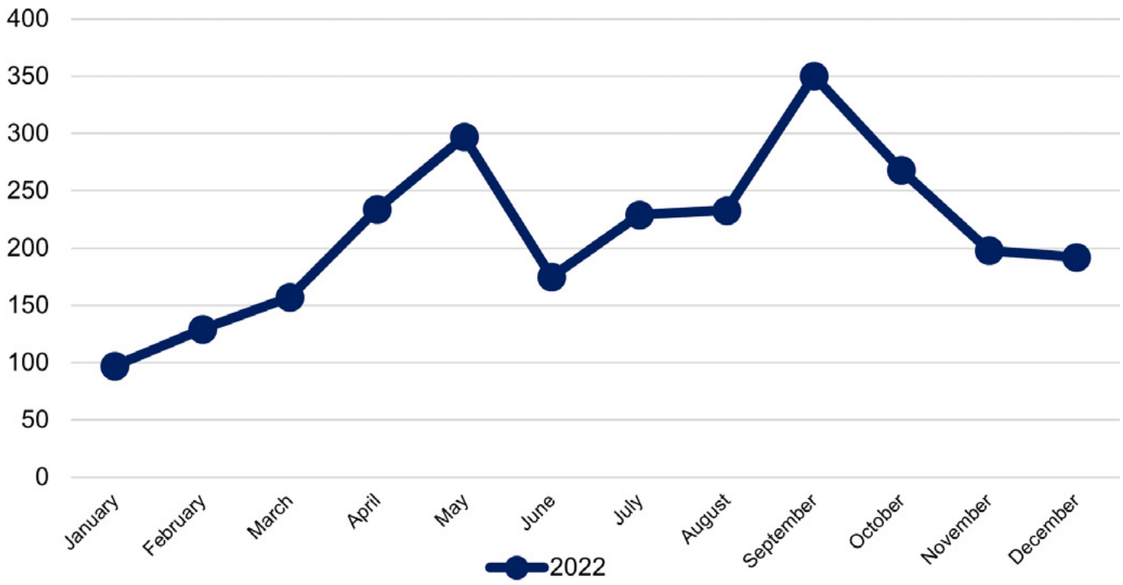


Figure 4: Month-by-Month Count of Incidents Raised in the SOC (2022)

Next, we dissect the number of cases raised by true positive category, captured in Figure 5, and notice the following; overall, 1263 incidents were mitigated (36%), and 1574 (45%) required no action, hence, the vast majority (82% or 2837) did not need to be escalated, with no further action needed.

Finally, 588 cases were escalated to the client (17%).

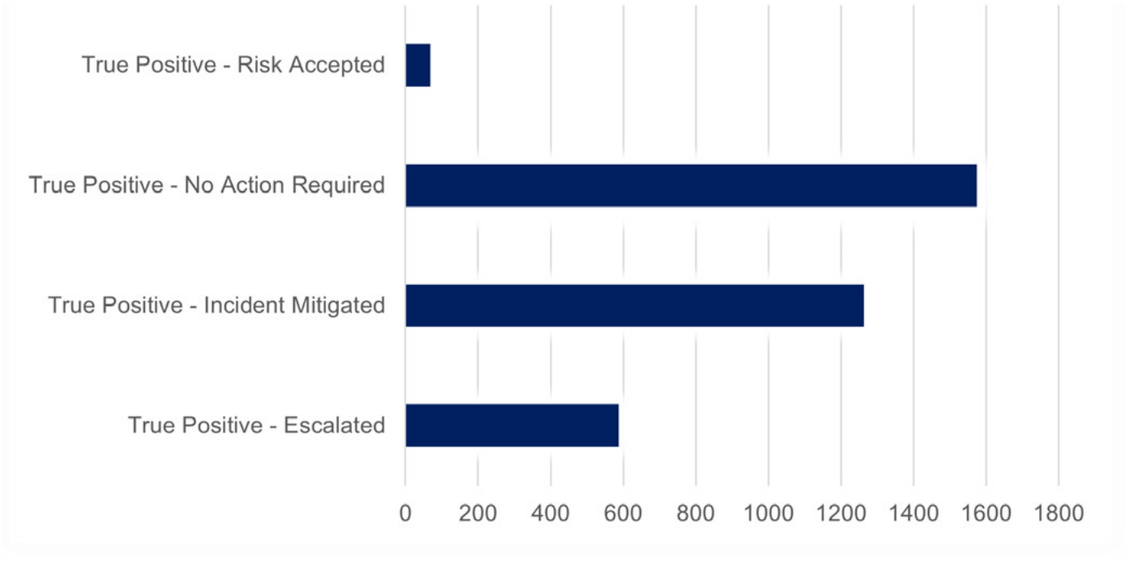


Figure 5: Number of Cases by True Positive Category (2023)

While analysing incidents by sector (Figure 6), we notice that NCC Group's clients within Academic & Educational Services were most susceptible to incidents with a total of 810 recorded.

Again, this is likely to be influenced by NCC Group's client base as a whole. With that in mind, it is worth mentioning that Academic & Educational Services was also ranked as the most targeted sector in 2022 with 657 incidents.

Year-on-year, the number of incidents recorded for the sector has experienced an increase of 23%. Interestingly, the sector was also the top target in 2021 with 255 incidents recorded at the time.

Given the overall number of tickets recorded in the period 2021 – 2023 for Academic & Educational Services, there is a high possibility that this would continue to be the case in 2024, so we would strongly recommend that clients within the sector stay vigilant and ensure best security practices are followed.

The remaining targets within the top five for 2023 are actually the same sectors as in 2022 with the differences being; the higher number of incidents recorded year-on-year as well as a shift in Technology's position from fifth in 2022 to third in 2023, which means that Financials and Energy moved to fourth and fifth respectively.

With regards to the figures, all sectors have experienced an increase in incidents raised.

However, we notice that Technology and Energy's sectors have experienced the highest increases with 161% (from 217) and 95% (from 261) respectively. Finally, Industrials and Financials' targeting increased by 46% (from 439) and 20% (from 435) respectively.

We would highly recommend that clients operating within these sectors review their defensive mechanisms.

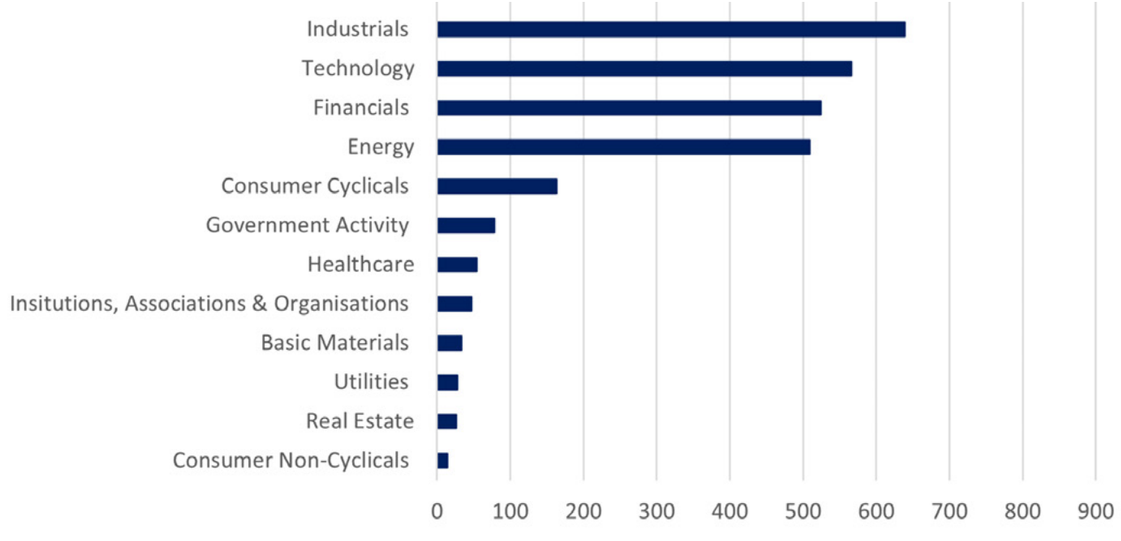


Figure 6: SOC Tickets' Raised according to Sector (2023)

SECTION 06

RANSOMWARE THREAT LANDSCAPE

With 2023 concluded, the following provides an analysis of the ransomware threat landscape with year-on-year comparisons and trend predictions for 2024, 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.

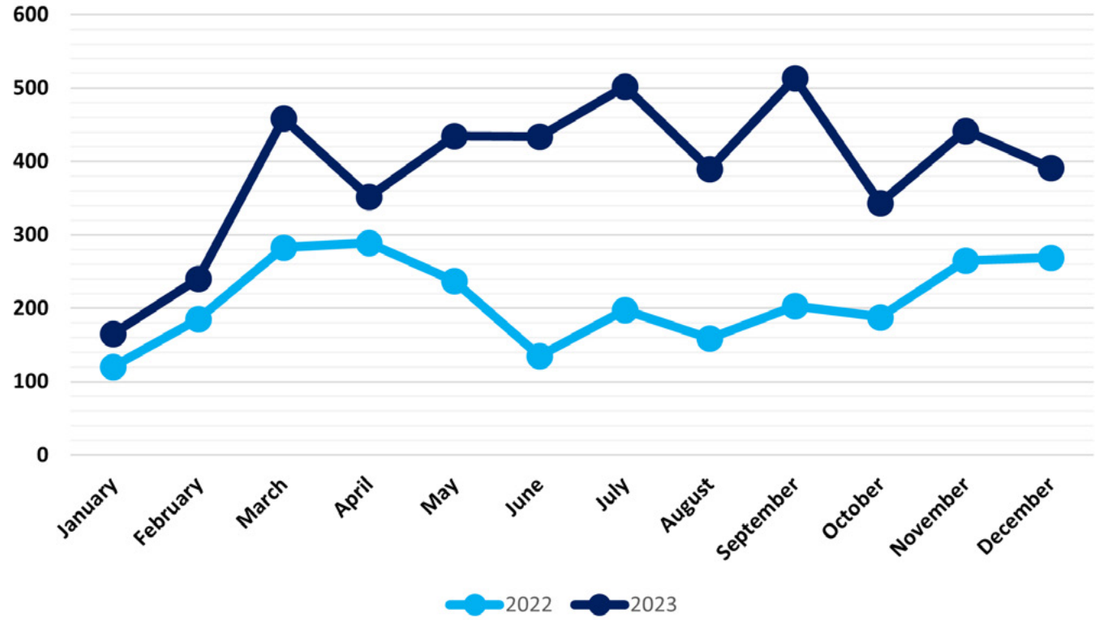


Figure 7: Global Ransomware Attacks by Month

First and foremost, an interesting observation to note is that from 2021-2022 there was in fact a miniscule 5% decrease in ransomware cases year-on-year, from 2667 to 2531 incidents, which contrasts heavily with our findings for 2022-2023 where there was a huge 84% increase from 2531 to 4667.

As is easily interpretable from Figure 7, and as we have referred to throughout the year, 2023's monthly totals consistently surpassed those of 2022, when there was a far more sporadic distribution between 2021 and 2022. To highlight how significant 2023's comparative increases were, the mean number of attacks for 2021 was 222, for 2022 it was 211, and for 2023 was a huge 389.

There is a whole host of potential explanations for this huge contrast between 2021/2022 and 2023. From a general heightened understanding of the profit that double extortion ransomware can amass for threat actors, to an increased accessibility of ransomware distributions for affiliates to utilise with the growing number of Ransomware-as-a-Service (RaaS) offerings.

While these are all valid and likely contribute in some way, NCC Group strongly consider the frequent uptick of new players in 2023's ransomware threat landscape to be pushing this figure up further, with an additional 3 arriving in December alone (Hunters, DragonForce and WereWolves).

Corroborating the above statement regarding the increasing availability of a plethora of ransomware variants is an interesting case that took place in September of 2023.

A ransomware threat actor accessed one of Symantec's client's environments and attempted to deploy LockBit ransomware, however, the client was able to detect and block LockBit's variant before the impact stage.

With a demonstration of tenacity, the threat actor instead tried to deploy a much newer variant; 3AM (the first observation of which was very possibly this same incident), which was instead successful, although it was still subsequently blocked after just three machines were affected.

This is a quintessential example of threat actors having a pool of variants to choose from, making their attacks far more persistent and difficult to block, and thereby potentially increasing the overall ransomware cases across the year.

If this develops into a trend and is not a one off incident, the standard approach for proactive security measures may not end at simply knowing which groups are targeting a specific sector and region and defending accordingly. Instead, it may have to include a holistic view of the whole ransomware threat landscape with constant IoC ingestion for every emerging group, to avoid successful "second attempts."

This occurrence does also raise an intriguing question regarding the loyalty of affiliates to their ransomware groups, as this instance implies that the usage of them is somewhat interchangeable.

Another curious case that took place in 2023 involved a ransomware attack on a university in the UK, where the threat actors emailed students and staff detailing the data that they had stolen, likely in an attempt to get the victims to apply more pressure on the university.

This has aptly been referred to as another triple-extortion technique, as it is yet another way to tighten the threat actor's grip on the victim; first there was the addition of DDoS to the attacks, then the withholding of victim names and only revealing them after their 'time had run out,' and now there is this. Irrespective of whether or not this technique will be repeated, we are certain of one thing; ransomware groups will continue to innovate in their extortive techniques in an effort to continuously increase their success rates.

As such, we reiterate the importance for organisations to remain vigilant and consistently enhance their defensive mechanisms.

If this influx of new threat actors continues in 2024, we can expect a similar increase in ransomware cases from 2023-2024, and perhaps an even larger one if the arrival of new ransomware groups occurs exponentially.

As our findings for the year highlight, double extortion ransomware is showing no signs of slowing down and its popularity, scope, and impact, are heightening on at least a yearly basis. So, unless we have finally reached a plateau which is unlikely at this point, and if there is a similar increase for 2023-2024 as there was from 2022-2023, the number of ransomware cases could even double by the end of the year.

As our findings for the year highlight, double extortion ransomware is showing no signs of slowing down and its popularity, scope, and impact, are heightening on at least a yearly basis.

Sectors

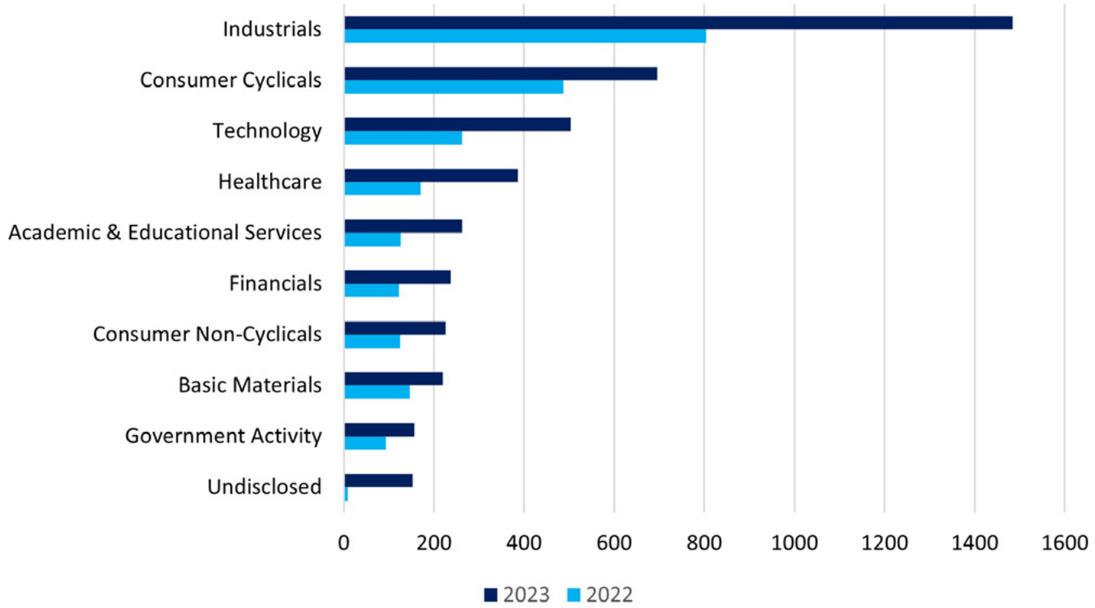


Figure 8: Most Targeted Sectors 2022 vs 2023

Sectoral targeting in 2023 was largely similar to that of the previous year although, as previously mentioned, 2023 was the most active year to a significant degree.

The most targeted sector for 2023 was as is to be expected Industrials with 1484 attacks (32% of year's total)

The most targeted sector for 2023 was as is to be expected, Industrials with 1484 attacks (32% of year's total), followed by Consumer Cyclicals with 695 (15%) and finally Technology with 503 (11%).

Figure 8 is perhaps one of the most effective visualisations to portray the explosiveness of 2023 when contrasted with 2022; although they largely shared the same most targeted sectors, in terms of absolute figures 2023 was much busier.

The activity in Industrials has almost doubled from the 804 attacks witnessed in 2022; a huge 85% increase. Consumer Cyclicals saw a less radical increase, but an increase nonetheless, from 487 hack & leak ransomware cases in 2022 (a 43% rise).

Finally, Technology was another sector with a drastic rise in attack numbers, again almost doubling from 263 hack & leak cases (a huge 91% increase).

Proportionally speaking, Industrials stayed the same, accounting for 32% of victims in both 2022 and 2023.

Conversely, Consumer Cyclicals exhibited a 5% proportional decrease from 2022 and Technology experienced a 6% proportional decrease.

Industrials

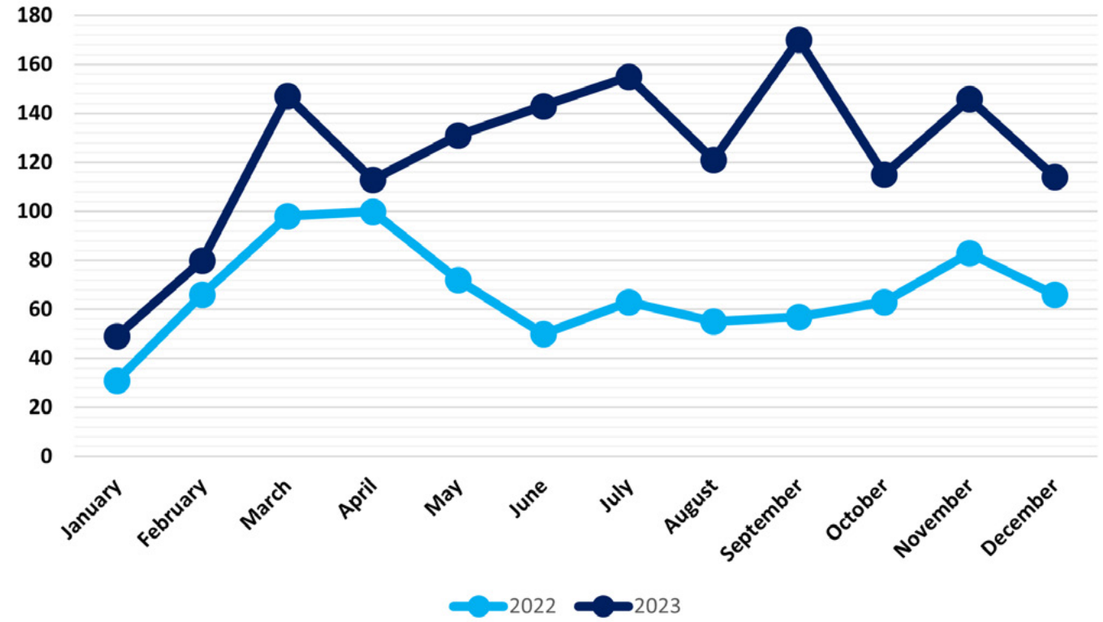


Figure 9: Total Industrials Victims Month-by-Month 2022 vs 2023

As mentioned above, ransomware cases in the Industrials sector almost doubled from 2022-2023 from 804 to 1484, but despite that the total ransomware cases shot up by 84% over the two years, the sector remained at 32% overall weighting of attacks.

This notably contrasts with Consumer Cyclicals and Technology which, although experienced increases in total figures, exhibited 5% and 6% relative decreases respectively.

This alone goes to show the attractiveness of the Industrials sector, and Figure 9 highlights that year-on-year there has been a consistently sustained interest, dwarfing its 2022 totals.

When we compare Figure 9 with Figure 7, it is possible to observe a striking similarity between the two graphs, especially, where 2023 is concerned.

This highlights the correlation between the overall total of ransomware attacks and the number of cases within Industrials, which brings us to our next point that was mentioned in our 2022 Threat Monitor.

As the Industrials sector is so heavily targeted within the ransomware threat landscape, the frequency of cases within is highly reactive to overall threat actor activity for that month, once more illustrating the significance of this sector.

This sector is often the most targeted for a number of reasons. Firstly, industries within, such as Professional & Commercial Services are likely an attractive target to TA's due to the vast quantities of PII that they store.

Firms that operate on a consultancy basis tend to serve a vast number of clients yearly, and thus have consistent access to huge amounts of client data making them both an attractive and lucrative target from a TA's perspective. Other industries within the sector share some commonalities which make them attractive to TA's.

One example is the cost of operational disruption (especially for those organisations that have tight production lines), another being the expanded attack surface due to sector-wide issues like IT/OT convergence.

Industries

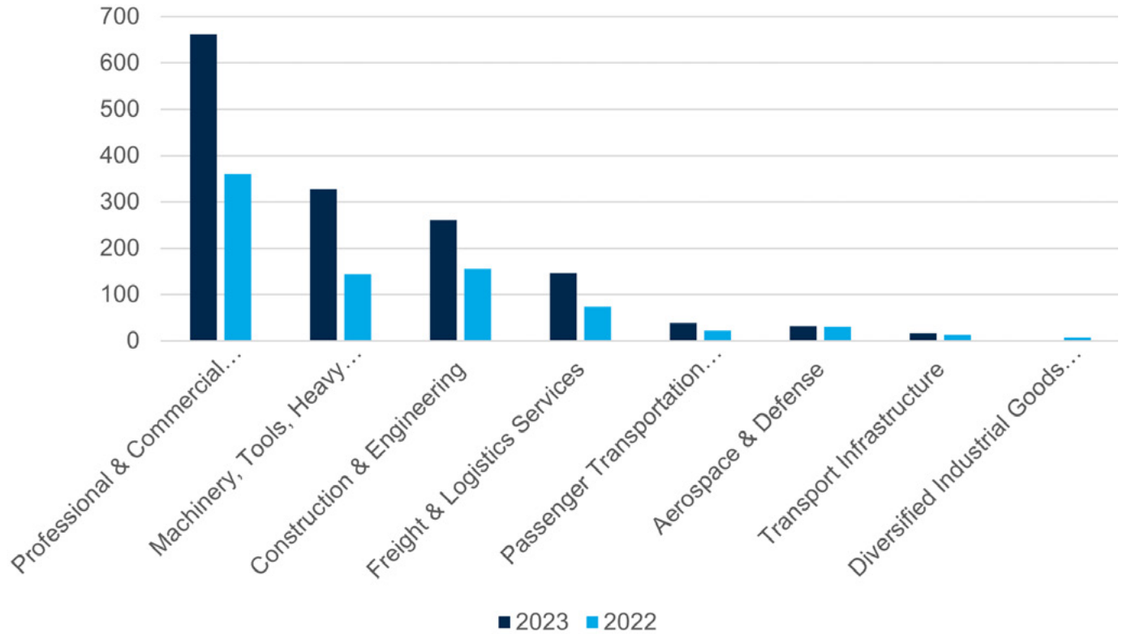


Figure 10: Most Targeted Industries in Industrials 2022 vs 2023

Similar to the observations for 2021-2022, the most targeted industries within the sector have remained largely the same between 2022 and 2023, with only a few minor differences, and of course, the expected discrepancy in total figures.

The most targeted industries within the sector have remained largely the same between 2022 and 2023.

In first place, we have Professional & Commercial Services with 662, which is 45% of the total figure, followed by Machinery,

Tools, Heavy Vehicles, Trains & Ships with 327 or 22% of the total, and finally Construction & Engineering is in third place with 260 cases which is 18% of the total.

Consumer Cyclicals

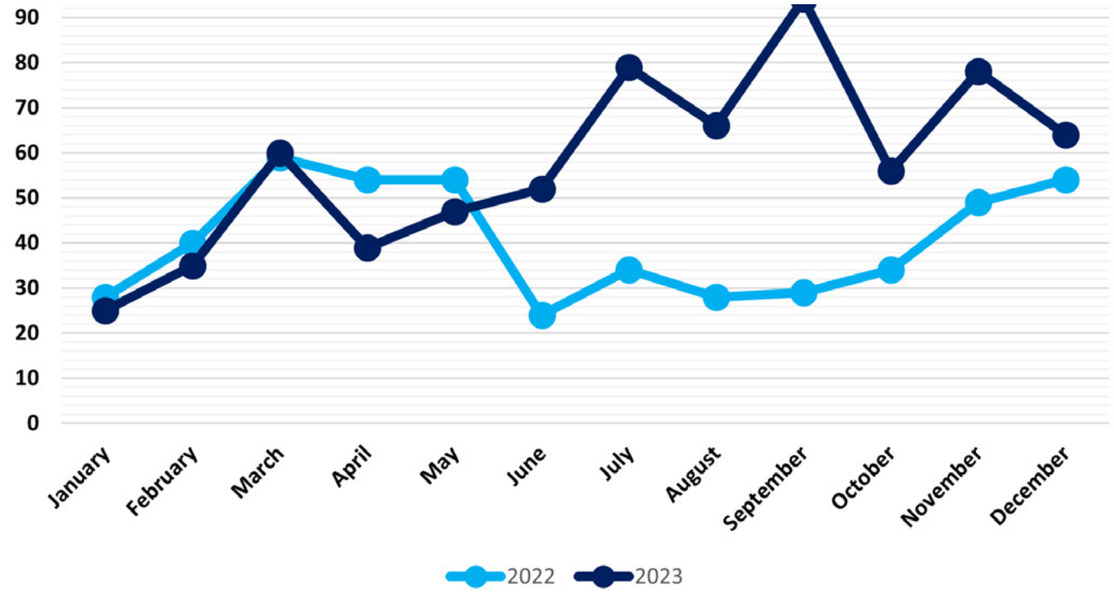


Figure 11: Total Consumer Cyclicals Victims Month-by-Month 2022 vs 2023

Consumer Cyclicals experienced a less explosive increase from 2022 to 2023 when compared to 2021 and 2022. Furthermore, the sector saw a 5% relative decrease when totalling its contribution to all ransomware cases in 2023, implying that for that year Consumer Cyclicals was less of a focus for threat actors.

It is possible that this is because of the heightened threat actor interest in the Industrials sector, causing Consumer Cyclicals to be less targeted.

As can be seen in Figure 11, the apparent cause of the increase in absolute figures in 2023 is a heightened interest in the sector from June onwards, which consistently surpasses that of the previous year.

However, this is again directly proportional to the overall threat actor activity within the year, so this does not necessarily indicate a specific focus on Consumer Cyclicals in the latter half of the year. Consumer Cyclicals will likely continue to be heavily targeted for the foreseeable future due to the nature of the industries existing within.

Organisations operating within Hotels & Entertainment Services as well as various retailers will be targeted for very similar reasons; their constant influx of new clientele and thus their access to payment details and information, alongside other PII such as email addresses and sometimes home addresses.

Contrastingly, organisations under the manufacturing umbrella (such as Automobiles & Auto Parts and Homebuilding & Construction Supplies) are more likely to be targeted due to their need for operational uptime which, once disturbed, can cause major profit losses which incentivises ransom payments.

Industries

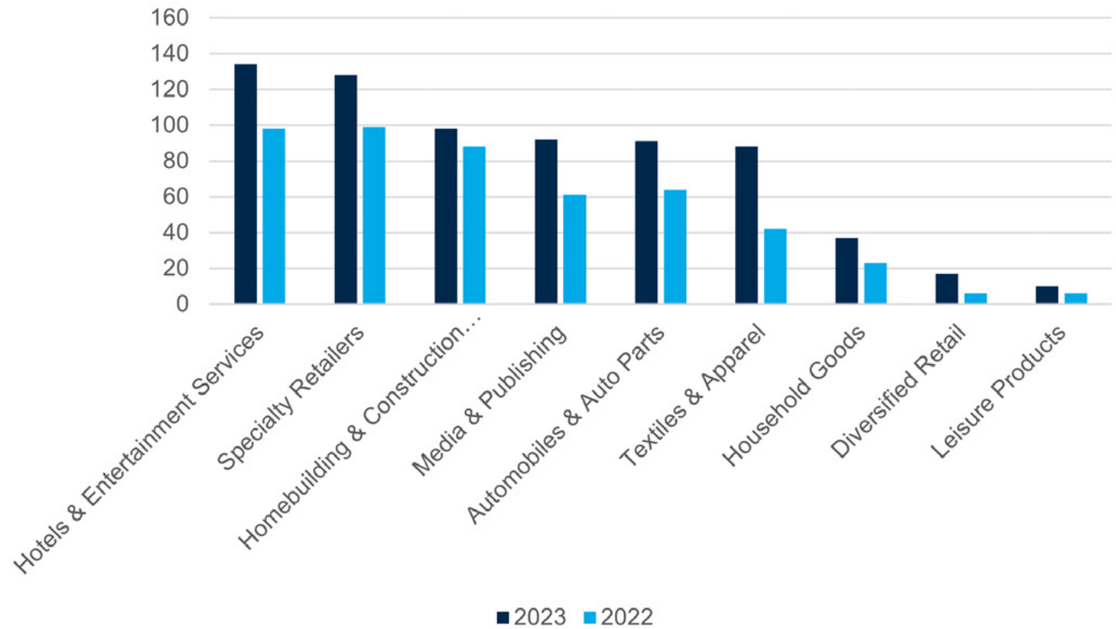


Figure 12: Most Targeted Industries in Consumer Cyclicals 2022 vs 2023

As is to be expected based on the provided justifications for threat actors favouring these sectors, the most targeted have remained largely the same with just a few minor fluctuations.

In first place we have Hotels & Entertainment Services with 134 attacks (19% of the total), followed by Specialty Retailers with 128 cases (18% of the total), and finally followed by Homebuilding & Construction Supplies in third place with 98 cases (14% of the total).

NCC Group do not foresee a major shift in the top three most targeted industries within this sector in 2024 due to their attractiveness to extortive threat actors.

Technology

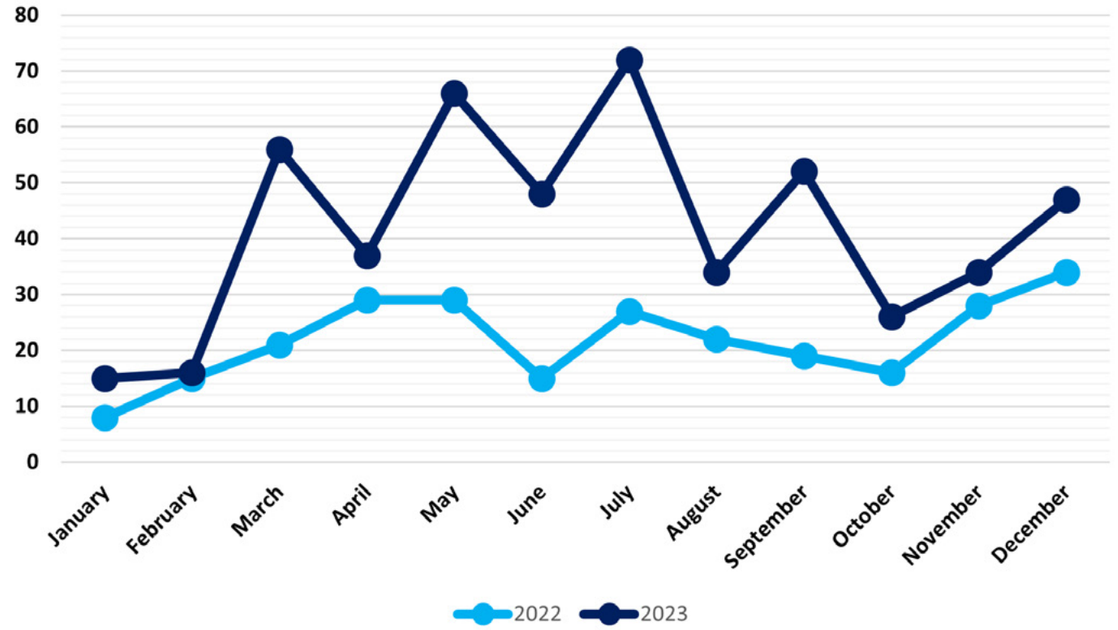


Figure 13: Total Technology Victims Month-by-Month 2022 vs 2023

Finally, we come to our third most targeted sector for 2023; Technology. As touched on previously, this sector also experienced a massive increase in terms of absolute figures, from 263 cases in 2022 to 503 in 2023, which is almost double (91% increase) and is in fact the largest year-on-year increase in our top sectors.

With that being said, it also interestingly experienced a 6% proportional decrease when compared to its weighting in 2022, which is also the largest in our top three, again an intriguing observation.

This is possibly linked to the rise in the number of ransomware groups in 2023, whom still heavily target Technology, contributing to the rise in total figures, but will still have the majority of their resources aimed at the Industrials sector.

Furthermore, there is a blatant pattern that has presented itself in 2023's figures; for the majority of the year there has been a significant increase, then a drop, followed by another increase, starting from February, and persisting until October.

Perhaps, this pattern arises as a result of the effort that is required to effectively breach a Technology organisation; particularly Software & IT Services, which is by far the most targeted industry within.

Although they may be attractive targets, they are arguably more likely to have stronger security postures, and performing further supply chain compromises after initial access may necessitate a more sustained effort, causing the subsequent drop after the rise.

There are a number of factors contributing to the consistently high attack volumes within the Technology sector, and in particular the Software & IT Services industry; the storage of IP in the form of source code for example, which are attractive targets for extortive threat actors.

Perhaps the most significant however, is the heightened potential for supply chain attacks.

Perhaps the most significant however, is the heightened potential for supply chain attacks, specifically where managed service providers are concerned, where a threat actor can hit a myriad of organisations with just one compromise, as mentioned above.

We predict that Technology will continue to be a prominent target in 2024 as it has been the third most targeted sector for two years now, which is unlikely to alter.

Industries

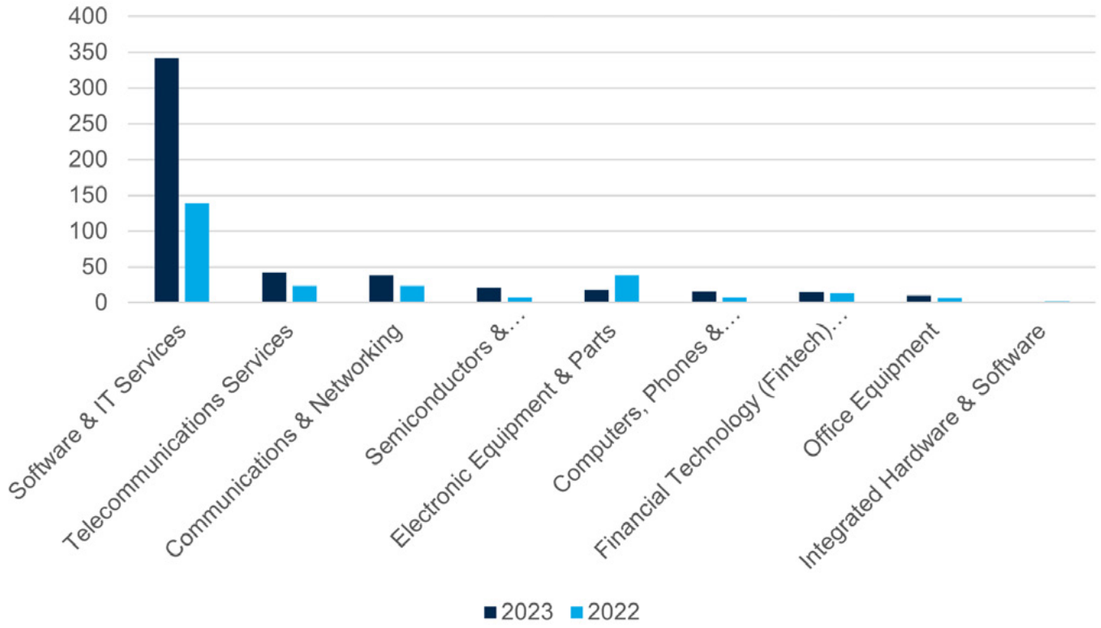


Figure 14: Most Targeted Industries in Technology 2022 vs 2023

Software & IT Services as the most targeted industry within the Technology sector to a large degree with 342 attacks, which accounts for a huge 68% of all attacks within, which is also a 146% increase year-on-year.

Secondly, we have Telecommunications Services with 42 cases in 2023, which accounts for 8% of all ransomware attacks in the year. Finally, Communications & Networking is in third place with just 38 attacks, also contributing 8%.

SECTION 07

THREAT ACTORS

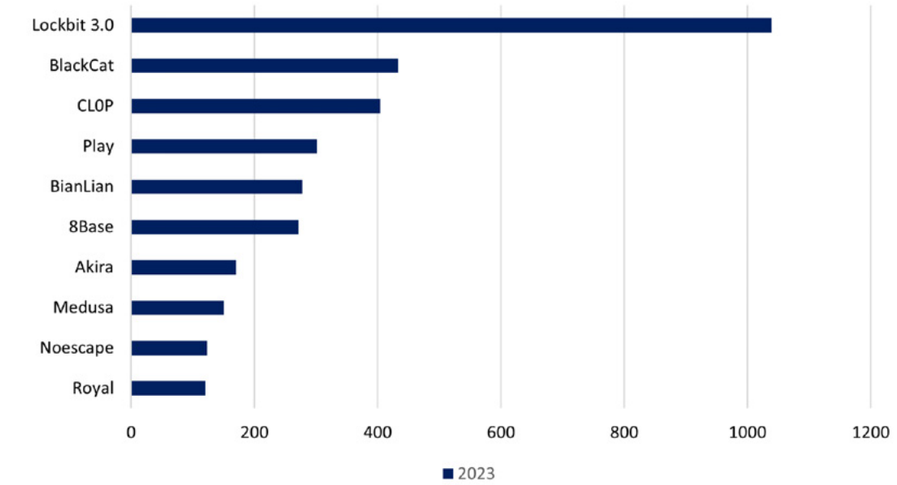


Figure 15: Top 10 Most Active Threat Actors in 2023

2023 was an eventful year for ransomware operators, witnessing a large increase in activity over 2022.

Threat actors have continued to mix up their Tactics, Techniques, and Procedures (TTPs) as companies around the world have continued to respond to the ransomware threat. We have seen the steady and consistent activity levels of groups such as LockBit 3.0, often one of the most active TAs of each month.

We have also observed groups fluctuate in their activity levels, and thus rise and fall in the ranks of the most active threat actors, and we have seen new groups rise to prominence and prior groups fall off the map.

5 groups were present in the top 10 most active TAs list for 2022 and maintained this prominence into 2023, though some like CL0P are notable for changing their position from 10th most active group in 2022 with only 57 attacks to 3rd most active group in 2023 with 404 attacks, an increase of over 700%.

The scale of the increase in activity is notable; the 10th most active group of 2023, Royal with 120 attacks, would have been 5th most active in 2022 should LockBit 2.0 and 3.0 be counted together, or 6th most active should they be counted separately.

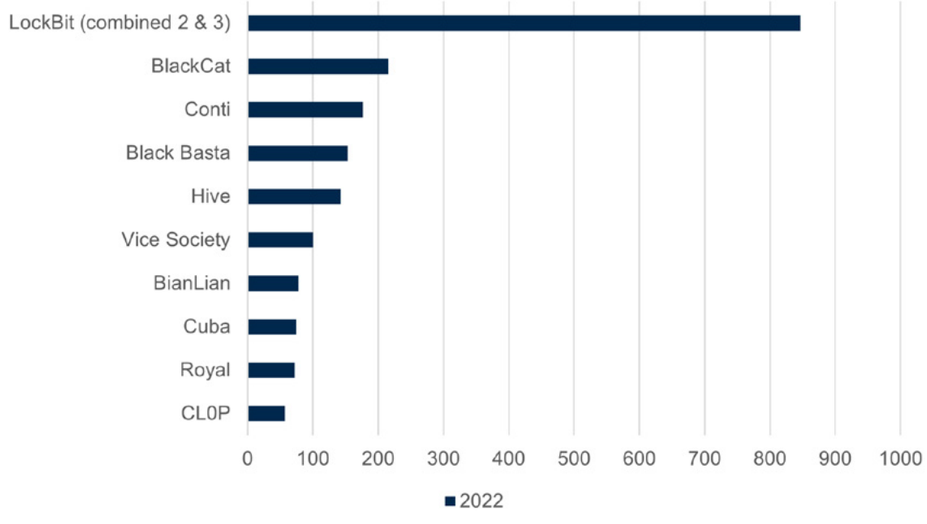


Figure 16: Top 10 Most Active Threat Actors in 2022

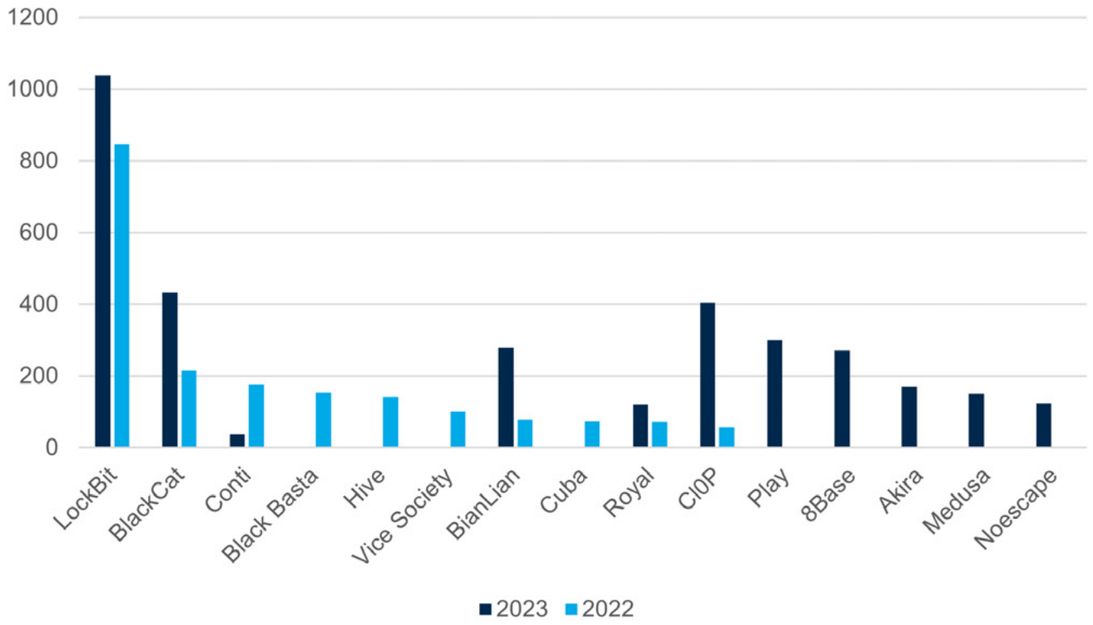


Figure 17: Most Active Threat Actors 2022 vs 2023

Of the groups amongst the 10 most active last year in 2022, only Conti and LockBit 2.0, after undergoing their transition to LockBit 3.0, were not active in 2023.

This is contrary to 2022 when we reported only 50% of 2021's 10 most prolific actors staying active throughout 2022.

We actually see included in the 10 most active threat groups of 2023, three groups which weren't around at all in 2022 and so have burst onto the scene, these being; 8base, Akira, and Noescape.

Further to seeing fresh groups in the 10 most active for the year, 2023 also saw a nearly 20% rise in threat actors, climbing from 55 threat groups in 2022 to 64 in 2023.

LockBit 3.0

LockBit is once again the most prominent ransomware group of 2023, as they were in 2022. 2023 saw their activity levels jump over 20% from 846 total attacks for LockBit 2.0 and 3.0 (465 and 381 attacks respectively) combined in 2022, to 1039 attacks for LockBit 3.0 in 2023.

LockBit 3.0's 2023 activity is nearly 250% that of the second most active threat group for the year, BlackCat, which themselves saw a 200% increase in activity since last year.

This shows how dominant LockBit has been in the ransomware space, that other threat groups can double or more their 2022 activity levels and still not be anywhere near LockBit's level of activity. LockBit has consistently been at the top of the rankings of most active monthly threat groups, only being not the most active three times throughout the year in March, June, and August when they were the second most active threat group.

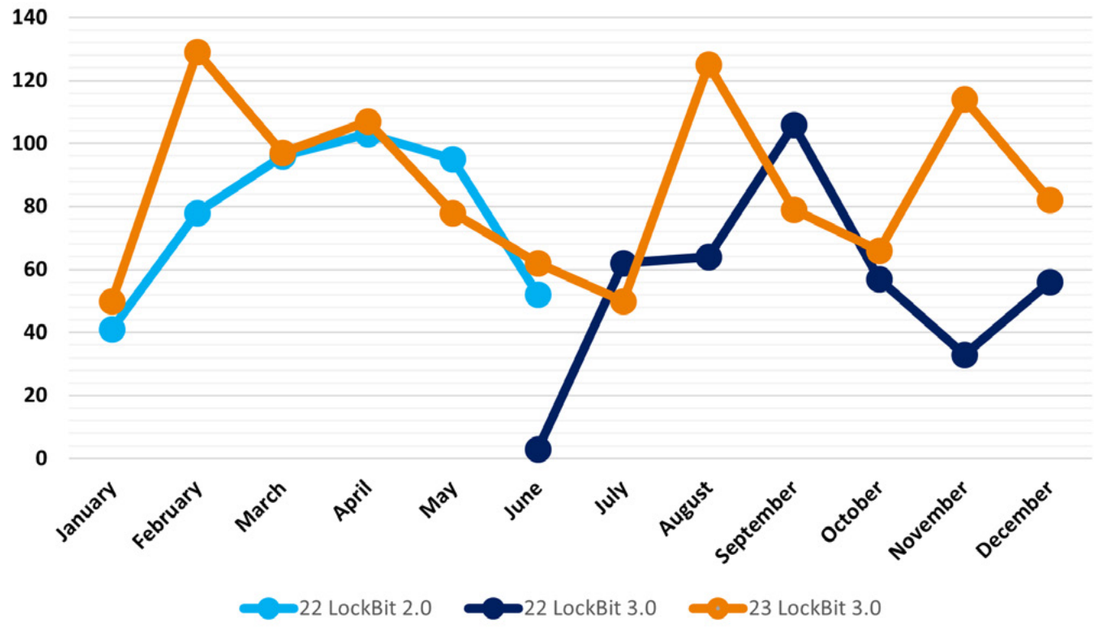


Figure 18: Total LockBit (2.0 & 3.0) Attacks Month-on-Month 2022 vs 2023

2022 saw LockBit (2.0 and 3.0 combine) represent 44% of all ransomware activity for the year.

2023 saw that proportional share decrease, despite the increase in real-terms attacks, to just under 32% of the total ransomware activity for the year, a 28% decrease in their share of responsibility since last year.

As their real-terms attacks have continued to increase though, we can put this down to other groups emerging onto the ransomware scene, and existing groups ramping up their activity levels, as opposed to indicating that LockBit were in any sort of overall decline.

One notable event, which LockBit were involved in, occurred toward the end of the year, concerned the disruption of the NoEscape and BlackCat/ALPHV's .onion sites.

Chatter online indicates that NoEscape may have pulled an exit scam, stealing potentially millions of dollars in ransom payments and shutting down the group's infrastructure, while BlackCat claimed their outage was caused by hardware failure, there is also the distinct, though unconfirmed, possibility that it was linked to law enforcement efforts.

LockBit seized upon the moment, and their operation's manager LockBitSupp, has now started to recruit affiliates from NoEscape and BlackCat to join LockBit's efforts.

It is unconfirmed who, or how many, affiliates from BlackCat and NoEscape moved to LockBit, though one victim of BlackCat, the German Energy Agency dena[.]de, has been seen on LockBit's victim list.

This wouldn't be the first time a rival threat group has ceased operations and its affiliates have joined LockBit. In 2021, the BlackMatter ransomware group was shut down and some of its affiliates joined LockBit whilst others joined with affiliates from DarkSide to form BlackCat/ALPHV.

It remains to be seen how the landscape will react to this shake up, and NCC Group will continue monitoring the situation in order to stay abreast of any updates.

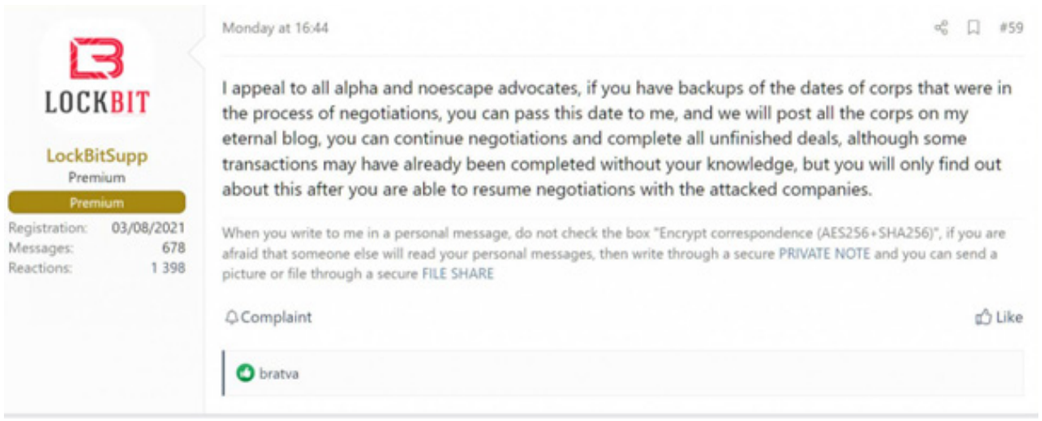


Figure 19: LockBitSupp Recruitment Post

Sectors Targeted

LockBit's targeting of different business sectors remained similar to that displayed in 2022 with the focus being on Industrials, Consumer Cyclicals, and Technology. Industrials, with 361 total attacks over the course of the year, accounts for 35% of LockBit's total attacks.

Consumer Cyclicals, with 165 total attacks throughout 2023, accounts for 16% of LockBit's activity. Technology, regularly amongst the top three targeted sectors of the year, received 95 attacks, or 9% of the group's total.

Industries Targeted

As far as specifically targeted industries, the focus for LockBit remains the same as 2022 with Professional & Commercial Services receiving the brunt of their efforts.

Their second most targeted industry is Machinery, Tools, Heavy Vehicles, Trains & Ships, while last year's second most targeted is this year's third, Construction & Engineering.

Professional & Commercial Services received a total of 148 attacks, or 14% of LockBit's total efforts. Machinery, Tools, Heavy Vehicles, Trains & Ships received 85 attacks, representing 8 % of LockBit's efforts, while Construction & Engineering received a total of 68 attacks: just under 7% of the group's annual total.

Blackcat

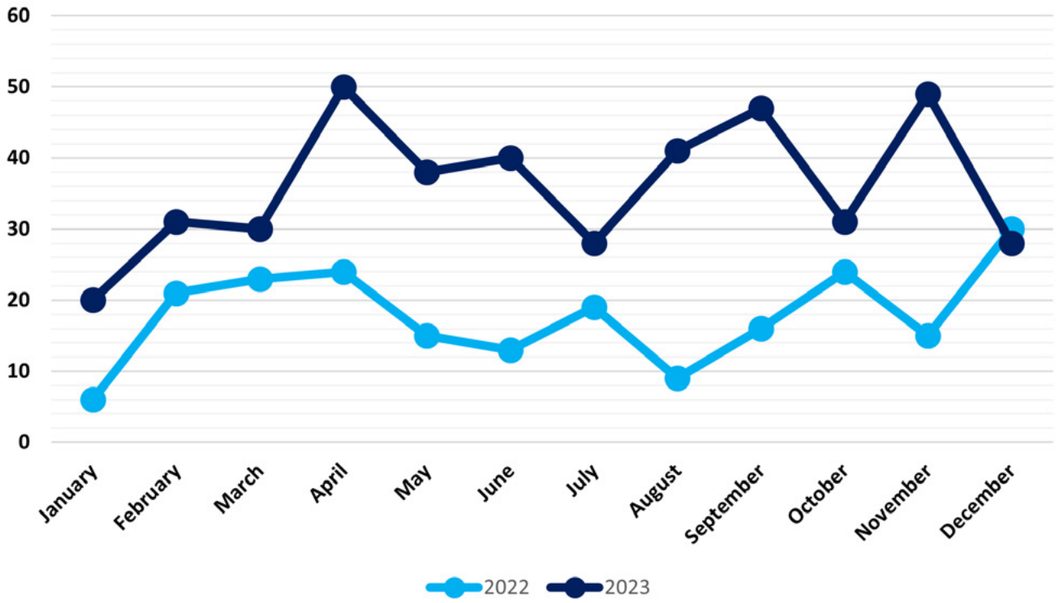


Figure 20: Total BlackCat Attacks Month-on-Month 2022 vs 2023

Following on from their activity levels in 2022, BlackCat/ALPHV remains the second most active ransomware threat group of 2023 (when considering LockBit 2.0 and LockBit 3.0 as one evolved entity instead of two separate ones).

Their activity spiked over 100% from their activity levels last year, rising from 215 attacks in 2022 to 433 attacks in 2023.

This more than doubling of attacks in real terms also represents an increase in BlackCat's proportional share in the total ransomware attack volume, though only minorly from 8.5% share of the total in 2022 to just over 9% of the total in 2023.

BlackCat displayed a consistently high activity level throughout 2023, only missing being in the top three most active threat groups in four months of the year, though in those four months they were the fourth most active threat group.

Though not as dominant, and with attack volumes still less than half of, LockBit BlackCat have shown a consistent level of activity throughout the year until experiencing a dip in activity in December.

This can likely be attributed to the temporary disruption which BlackCat/ALPHV's leak site experienced in early December.

There has been much speculation about what caused the 5-day disruption with some speculating that it is the result of law enforcement interventions, whilst the operators at BlackCat maintain it was simply a hardware issue which is in the process of being solved.

Members of BlackCat have had a turbulent career in cybercrime: affiliates of the DarkSide group formed BlackMatter upon DarkSide's disbandment; affiliates of BlackMatter helped to form BlackCat/ALPHV in early 2022; and now LockBit 3.0 has started to poach some affiliates of BlackCat and even displaying some of BlackCat's victims on their leak site (see LockBit section above).

Sectors Targeted

BlackCat's 2023 distribution of focus amongst business sectors is only slightly different to what was seen in 2022. Industrials remain the most targeted sector with 142 attacks representing 33% of the group's total activity.

The second most targeted sector is, once again, Consumer Cyclicals with 64 attacks representing 15% of the group's 2023 activity. The third most targeted sector in 2023, taking the place of 2022's Technology sector, is the Healthcare sector which received 53 attacks, or 12% of their total activity for the year.

Industries Targeted

The specifics of targeted industries within overall sectors have also undergone a shift since 2022. The most targeted industry remains Professional & Commercial Services with 77 attacks, 18% of the group's yearly total.

The second most targeted industry is Healthcare Providers & Services with 34 attacks, less than half the total of those levied against Professional & Commercial Services, representing 8% of the group's total. The third most targeted industry for BlackCat in 2023 was Software & IT Services, the industry which was in joint-second position in 2022.

This industry was attacked by BlackCat 31 times in 2023, 7% of their total activity for the year.

CL0P

Figure 21: Total CL0P Attacks Month-on-Month 2022 vs 2023

For a long time CL0P has been present in the threat landscape, but their activity was particularly notable in 2023 where being the third most active threat actor over the course of the year and, in some instances, the most prominent actor of the month.

With a huge 609% increase from just 57 attacks in 2022, which was 2% of the year's total, to a much more impactful 404 cases in 2023, which is 9% of the total; CL0P have evidently stepped up their game.

Despite being completely inactive for 33% of the year (0 attacks), and conducting just 5 attacks or less per month for another 42%, they have still managed to come in third relying on their campaigns carried out in March, June, and July (and also the months in which the group was in first position).

Interestingly, as the readers of our Monthly Threat Pulse will be aware, these seemingly random spikes that can be observed in Figure 21 are in fact representative of CL0P's bespoke modus operandi (MO) which distinguishes them from the majority of other threat actors in the ransomware threat landscape.

Between the GoAnywhere MFT vulnerability (CVE-2023-0669), exploited by them on the 3rd of February, and which significantly boosted their March figures, and the MOVEit Transfer vulnerability (CVE-2023-34362) exploited on the 31st of May, affecting their June and July figures, we can begin to outline their MO.

CL0P favours identifying a weak spot in organisational supply chains (preferably facilitating file transfer / storage), developing an exploit, and subsequently performing mass-exploitation over the following month/s, and the numbers show that this is indeed highly effective.

Going forward, we can expect this activity to persist as it has evidently proven to be profitable for the ransomware group, particularly in June and July with the collective victim count of 261 likely enabling them to have their subsequent four-month break.

Therefore, it is prudent for organisations of any sector to consider their third-party security posture and the exploitability of their supply chain, to avoid becoming a victim of CL0P's likely future excursion into the supply chain.

Sectors Targeted

In 2023, CL0P's most targeted sectors were Industrials with 108 attacks (27% of their total for the year), followed by Technology with 80 (20% of the total), and finally Financials in third with 67 (17% of the total).

Note that, unlike other threat actors in the ransomware threat landscape, CL0P's targeted sectors are likely more circumstantial than those of other groups, as their victims will be those organisations that use the device that they are targeting.

In this case, Industrials will certainly be the most targeted due to the sheer quantity of varying industries that reside within, meaning a greater percentage of organisations using these devices will exist within the Industrials sector.

Industries Targeted

In terms of CL0Ps most targeted industries, in first is Professional & Commercial Services with 67 cases (16% of their total for the year), followed by Software & IT Services in second with 61 (15% of the total), and finally Banking Services with 33 (8% of the total).

SECTION 08

REGIONS

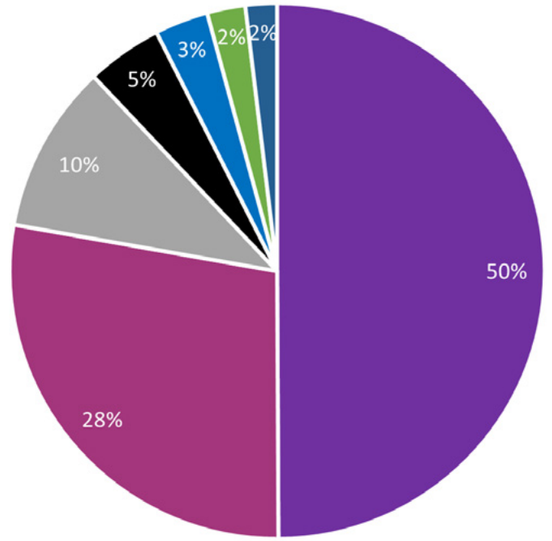
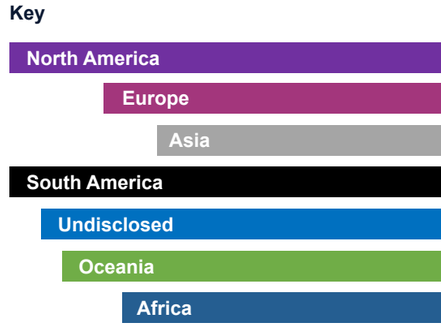


Figure 22: Total Victims by Region in 2023



There are no deviations from the norm with regard to the most targeted regions in 2023, with North America, Europe and Asia occupying more than 80% of the pie chart, with the rest being fairly evenly split between South America, Undisclosed, Oceania and Africa.

As can be seen in Figure 22, North America was the most targeted region in 2023, accounting for 2330 attacks (or 50%), followed by Europe with 1300 (28%), and in third we have Asia with 475 attacks (or 10%).

As can be seen in Figure 22, North America was the most targeted region in 2023.

Threat actors likely perceive these regions as wealthier which thereby increases their targeting, consistently making these three regions the most targeted.

Notably, in 2022 the distribution of attacks between North America and Europe was less disparate with them contributing 44% and 35% respectively, showing that interest in the former has seemingly increased in 2023.

In fact, relatively speaking, North America's targeting increased by 6%, even with the sizeable 84% increase in overall ransomware attacks in 2023.

As a result, Europe's targeting decreased by 7% and Asia's decreased by 1%.

As for the remaining regions; South America experienced 214 cases (15%), Undisclosed had 151 cases (3%) which accounts for those hacked organisations whose names were not disclosed by the threat actors and therefore the regions unidentifiable.

Oceania suffered 108 attacks (2%), and finally Africa saw 89 (2%).

Contrasting the situation with the top three, these regions have stayed largely consistent with 2022, proportionately speaking, where South America contributed 5%, Oceania 3%, Africa 2%, and finally just 9 undisclosed attacks (0%) as this was a new technique at the time.

Something to extrapolate from this data is that the extortive methodology of keeping victim names redacted does not seem to have been a passing fancy and must be proving effective in pressuring victims, as it now accounts for 3% of the year's total.

We expect this extortion technique to persist in 2024 and, if other threat actors begin to adopt it, we could even see it increasing by 2024's close.

SECTION 09

VULNERABILITY LANDSCAPE

Exploiting vulnerabilities are a proven point of entry for threat actors. In this section we highlight critical vulnerabilities that have been published during 2023 and enable readers to gain insights into the dynamics of the vulnerability landscape.

According to NIST, 2023 saw a total of 29,065 vulnerabilities disclosed across the year compared to 25,083 in 2022 an increase of 3,982 in a year.

As the corporate world settles into a hybrid and remote working environment, the top three MITRE techniques exploited are exploitation of remote services, exploitation of public facing applications and the exploitation for privilege escalation.

Additionally, of the disclosed vulnerabilities, less than 1% of them were continually exploited in the wild according to Qualys. With the increase in remote work and AI seen this year, 3 in 4 security professionals also believe that the cyber risk of organizations has increased.

Furthermore, the reliance on supply chain security is also high on the agenda for organisations with 8 in 10 saying there is an ever-increasing dependency on good security postures of those in their supply chains according to SoSafe.

Managed File Transfer platforms are a way for organisations to securely share files and data with other parties.

They are usually more secure than other methods including the File Transfer Protocol (FTP) and email. Additionally, they are usually hosted in the cloud so are scalable and efficient. These platforms are used by organisations to share a variety of documentation including contracts for new hires and for suppliers and clients.

Therefore, these platforms have a vast array of data traversing them and could be seen as valuable to malicious actors. In 2023, the vulnerabilities disclosed showed exactly this with data sharing enabling platforms including MFT platforms such as GoAnywhere and MOVEit and print management solution PaperCut NG featuring in the Qualys top exploited vulnerabilities with CVE-2023-0669, CVE-2023-34362 and CVE-2023-27350 respectively.

Furthermore, the top ten exploited vulnerabilities of 2023 were all from the year apart from CVE-2022-41328 which is a Fortinet FortiOS vulnerability from a previous year still heavily exploited in the wild sitting at number 3 in the list.

In addition, SentinelOne continue to see Fortinet FortiOS & FortiProxy (CVE-2018-13379), Microsoft Exchange Server (CVE-2021-34473, CVE-2021-31207, CVE-2021-34523) and Atlassian Confluence Server & Data Centre (CVE-2021-26084, CVE-2022-26134) among other historic vulnerabilities being routinely abused throughout 2023.

This shows that organisations are not implementing sufficient mitigation or remediation efforts to secure their digital estate from historic vulnerabilities and shows the importance of an effective patch management programme to mitigate this threat.

2023 saw the rise of Artificial Intelligence (AI) and Machine Learning (ML) with OpenAI's ChatGPT becoming widely adopted in the mainstream. This presents a variety of opportunities and challenges for both malicious actors and defenders of digital estates. The UK's National Cyber Security Centre (NCSC) believes it has great potential but needs to be built on secure foundations.

The fast rise of the technology has created a new vulnerability in adversarial attacks. NCSC say there are several methods for this attack including data poisoning. Additionally, AI presents an opportunity to get ahead of the vulnerability before they are found because AI can spot insecure coding practices.

However, AI can be used maliciously to develop better phishing and malware capabilities.

In 2019, 80% of cyber security decision-makers expected AI to increase the scale and speed of attacks and 66% expected attacks to evolve to “conduct attacks that no human could conceive of”.

In 2023, security experts say this is already happening with AI-enabled cyberattacks being an issue that organisations are unable to cope with.

Those that leverage generative AI models such as ChatGPT need to be aware of the trustworthy nature of the coding packages it outputs as it can be leveraged to spread malicious packages into developer’s environments through data poisoning.

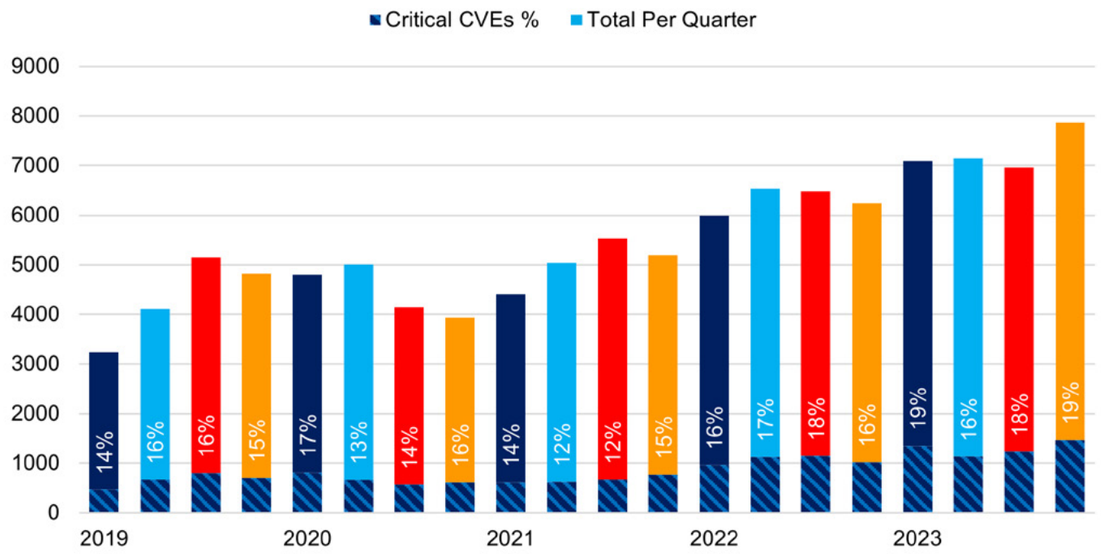


Figure 23: Vulnerability Disclosures per Quarter 2019-2023

Figure 23 demonstrates that NCC Groups 2022 prediction that there would be an increase in vulnerability disclosures was correct.

2023 saw a substantial increase in vulnerability disclosures and was a record year compared to 2022 where the number of vulnerabilities disclosed per quarter increased substantially up 38.5% on average, beginning a continuous upwards trajectory seen in 2022.

However, on average, per quarter the number of critical vulnerabilities disclosed was down 12%.

This average is heavily weighted towards a high number of vulnerabilities during Q2 of 2023 (7150 vulnerabilities) and the lowest number of critical vulnerabilities being disclosed at 1132.

If the anomaly of Q2 is excluded, then critical vulnerabilities as a percentage of disclosed vulnerabilities remains in a decline at 9% compared to 2022. It is noteworthy, that given the substantial increase in vulnerability disclosures, the number of critical vulnerabilities being disclosed were still at record levels with an average of 1295 critical disclosures per quarter, up 21% year on year.

The stable trend of vulnerability disclosures in previous years seems to have come to an end.

With the innovative security measure of BugBounty programmes being adopted by organisations to find vulnerabilities in their software and hardware before adversaries, it encourages the ethical disclosure of security vulnerabilities by security researchers to vendors giving them chance to patch before exploitation occurs by malicious actors, enhancing their security posture.

Additionally, the known exploited vulnerabilities have stayed level with the previous years (2020-2023) excluding the spike during the remote working shift during the COVID-19 pandemic (see Figure 24) and prime opportunity to target the less secure home worker.

However, it would be reasonable to assume that malicious actors will not disclose the vulnerabilities they are utilising to enable greater success on their objectives.

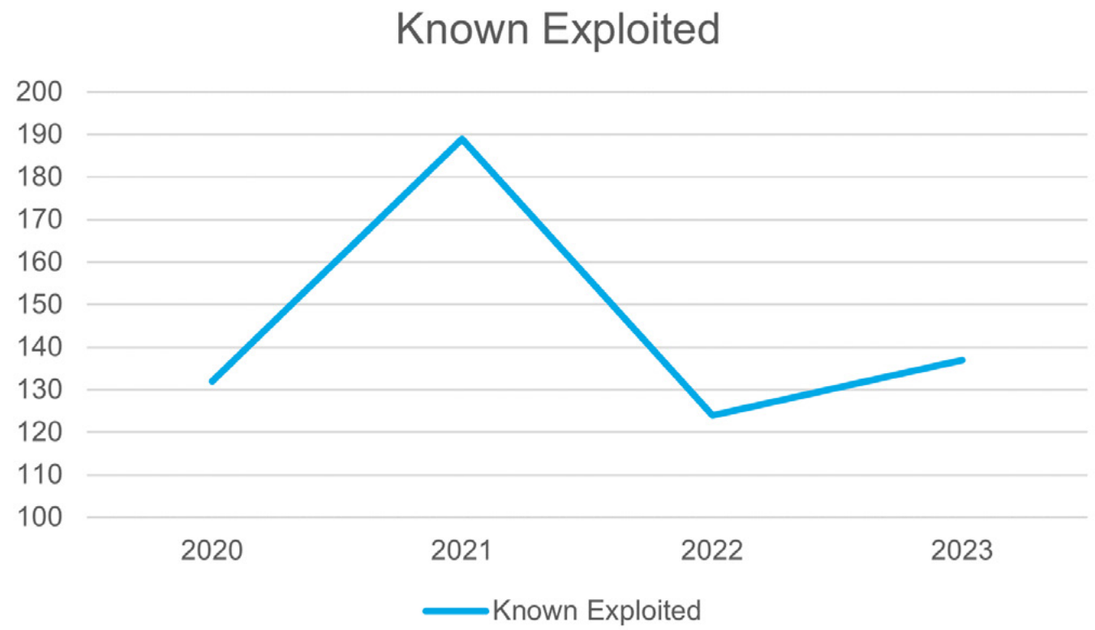


Figure 24: Known Exploited Vulnerabilities

Looking forward into 2024, it is highly likely the number of vulnerability disclosures will continue its upwards trajectory year over year given the increase in BugBounty initiatives, and with global governments understanding that increased disclosure could see increased exploitation attempts, given greater awareness.

Additionally, generative AI will keep evolving and help organisations improve their security posture whilst also being leveraged by malicious actors to enhance their capabilities.

Historic vulnerabilities will also continue to be abused by adversaries as it is common knowledge that not all organisations have an efficient patch management programme in place to successfully mitigate the threats these historic vulnerabilities pose. Therefore, organisations should enforce an actionable and appropriate patch management programme to mitigate the risks posed by disclosed vulnerabilities and ensure they are consuming and actioning relevant threat intelligence from mature intelligence functions, be that internal or third-party providers, to allow for a proactive approach to their security posture.

SECTION 10

GLOBAL CONFLICTS

In 2023, two key global conflicts saw cyber capabilities work alongside kinetic warfare. Notably, Russia's ongoing invasion of Ukraine and the Israeli-Palestinian conflict.

Russian Invasion of Ukraine

Increased Attacks, Reduced Impact

In 2023, cyber-attacks against Ukrainian infrastructure continued to be high; however, their sophistication and overall impact reduced.

In H1 2023, Ukraine's State Service of Special Communications and Information Protection of Ukraine (SSSCIP) identified a 123% increase in registered incidents from H2 2022, however, the growth of critical incidents had severely decreased (-81%), and the ratio of high-level critical incidents improved.

During this period, attackers appeared to place greater emphasis on the likes of spray and pray and phishing approaches versus sophisticated techniques.

With reduced innovation with respect to the technology used and the methods employed, as well as an increasingly opportunistic rather than strategic approach, Ukraine's defence has grown stronger. Furthermore, Ukraine's ability to bolster its security defences should not be understated.

Prior hostilities between Ukraine and Russia, as well as international and domestic support, have allowed Ukraine to anticipate and build resilience against Russian capabilities, contributing to their success in 2023.

Ongoing cooperation with international bodies such as the NATO Cooperative Cyber Defence Centre or Excellence (CCDCOE), as well as private companies such as Microsoft, Google, Amazon, and ESET, continue to fortify their defence.

Although cyber-attacks have not been the leading attack method in this war, and have not met previous conceptions of Russia's reputation as a prolific cyber actor, they have certainly become part of the broader military strategy on both sides.

As the war continues to unfold, it is likely that we will continue to observe the exploitation of cyber powers alongside kinetic warfare against both Ukrainian and Russian infrastructure.

Influence and Information Operations

Particular emphasis was placed on Russian influence and information operations against Ukraine. Notably, espionage, surveillance and intelligence gathering targeted the Ukrainian civic sector with law enforcement a key interest.

The likely suspected objective here being to ascertain information gathered by Ukraine, which could be used to identify Russian war crimes. Such evidence could assist in criminal proceedings against Russian individuals and companies engaged in the war.

Advanced Persistent Threat groups (APTs), notably the Russian Federal Security Service (FSB), the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), and the Foreign Intelligence Service of the Russian Federation (SVR), were identified as likely responsible.

The threat actors would often revisit previously targeted victims, leveraging information accessed to conduct further operations.

In addition, the SSCIP and CERT-UA found Russian information operations also heavily consisted of disinformation campaigns, identifying the Media sector as a key target, where targeting resources and or accounts.

Disinformation campaigns support Russia to undermine the truth, sow discord, and limit access to timely and accurate information. By influencing public opinion, Russia continues its attempts to undermine confidence in Ukrainian policies and government, and to destabilise international support for Ukraine.

This is of course not new, as we have historically observed Russia engage in widespread disinformation campaigns, and we are likely to observe this as the war continues into 2024.

Disruption and Hacktivism

Distributed Denial of Service (DDoS) attacks were prevalent throughout 2023. From January to March alone, DDoS accounted for 87.5% of all cyberattacks recorded by the CyberPeace Institute.

From January to March alone, DDoS accounted for 87.5% of all cyberattacks recorded by the CyberPeace Institute.

Whilst differing cyber threat actors are engaged in DDoS, hacktivists on both sides, such as Russia's Killnet and Ukraine's IT Army have remained active.

Notable events include KillNets' DDoS attacks against US hospitals in response to Western support for Ukraine, as well as their reported targeting of NATO websites. Likewise, in collaboration with groups such as Anonymous Sudan, believed to be part of Killnet, Killnet threatened to target critical banking infrastructure SWIFT, in response to increased Western aid to Ukraine.

In the opposing corner, the IT Army of Ukraine disrupted Russian Internet providers in territories occupied by Russia, "Miranda-media", "Krimtelekom" and "MirTelekom".

Over the last two years, hacktivism has underscored the increasing prevalence of non-traditional actors participating in cyberwarfare, and war more generally.

Whilst this has taken the shape of both state-backed and non-state-backed hacktivism, the latter has been notably evident in both sides of the war.

Concerns regarding whether these groups may have a greater appetite for attacks than known state groups continue to be raised.

Destructive Operations

In addition to the above, destructive attacks were also observed in 2023, predominantly conducted by the Russian APT group Sandworm. These attacks seek to eradicate targeted infrastructure to ensure maximum chaos and destabilisation.

In December 2023, Ukraine's largest telecommunications provider Kyivstar was targeted, destroying the core of the telecoms operator. The Solnstsepek group, who are believed to be linked to Sandworm, subsequently claimed the events.

This concerned one of the most destructive cyber-attacks conducted by Russia against Ukraine since the onset of the war, which as a result, left an estimated 25 million subscribers without internet connection.

The threat actors are reported to have been on the network since May 2023, demonstrating how APTs can often remain in systems undiscovered until the moment of attack.

The events are being emphasised as a warning to the West that no one is untouchable, and thus of potential threats to come.

Global Impact

Whilst much of the events were concentrated in Ukraine and Russia, the international nature of the war has led to spill over effects also reflected by cyber activity. Countries seen to support Ukraine have continued to feel the wrath of Russian threat actors.

For example, Microsoft observed Cadet Blizzard targeting Latin American and European companies, particularly NATO countries, providing military support to Ukraine.

In addition, Russia's disinformation campaigns seek to garner support for the state beyond its borders where spreading a pro-Russian narrative at international scale. This has included narratives of Western Russophobia, Ukrainian Nazi ideology and the negative impact of Ukrainian refugees in Europe spread via fake social media accounts.

Overall, the international impact will likely see the continued targeting of Ukrainian supporters, NATO countries, and the spread of disinformation to boost Russian backing.

Summary

Overall, in 2023, cyber-attacks have remained an important tool alongside kinetic warfare for both Ukraine and Russia.

As part of the broader military strategy, they support operations in the physical world where enhancing disruptive and destructive capabilities, as well as driving key information and influence operations.

Russia's cyberattacks remained persistent, and although their overall impact often not critical, nor their levels of sophistication high, nonetheless the attacks on Kyivstar served as a stark reminder that detrimental attacks remain a possibility.

That said, Ukraine's defence efforts remain strong, and with continued collaboration with international partners, the public and private sectors, the country will continue to reinforce its cyber security strategy.

Going forward, an understanding of the key APTs and hacktivist groups should support their defence measures.

Israeli-Palestinian Conflict

The ongoing war between Israel and Palestine has predominantly shed light on hacktivist activities, although debate as to whether nation states are already involved has been raised.

Certainly, there is the possibility that APTs may adopt a more proactive role in cyber activity the longer the war unfolds. Groups such as Cyber Avengers, Cyber Toufan and Killnet have been prominent where targeting Israeli infrastructure, demonstrating the international element of the hacktivist community, notably given the latter.

Equally, pro-Israeli hacktivists have also been observed targeting Palestinian infrastructure, such as Predatory Sparrow.

Similar to Russia-Ukraine, we are observing increasingly non-traditional actors adopt their position in war and provides food for thought where considering the types of threat actors we may increasingly see in future conflicts.

SECTION 11

THREAT SPOTLIGHT

Ducks & Loaders: Life after Qakbot?

Law enforcement operations can have a severe and abrupt impact on the threat landscape, putting pressure on threat actors to expand and adapt their toolsets to minimize business interruption. Operation Duck Hunt in 2023 that knocked an extremely prolific loader malware family, Qakbot, off its throne is one of such changes.

This shift in landscape tends to attract the attention of certain threat intelligence analysts; and so, due to Qakbot's popularity and its subsequent downfall, these certain threat intelligence analysts at NCC Group became interested in proactively monitoring potential increases in the usage of similar loaders.

Should Qakbot's departure from the playing field have left a vacuum, which competitor would rise up to the challenge now that the tool's infrastructure has been seized? And so, while law enforcement silently toiled to disrupt, we silently turned to digging.

Loader malware is a pivotal, expensive, and powerful entry vector that secures its place in the victim's systems. Loaders serve a wide range of other malware operators (including other loaders), making sure that initial stages of crime run smoothly, making them high priority investigation targets.

After all, from the defending perspective, one would much rather close off the entry points for malicious activity as early as possible instead of dealing with the fallout within the core systems.

Our research preemptively started with a close investigation of the Pikabot loader, a trojan that emerged in May 2023 that was deemed a likely match for Qakbot.

The new addition to the loader market exhibited multiple resemblances to Qakbot from the beginning of its career. The eerily similar way both loaders were spreading during their respective campaigns by what is thought to be one specific affiliate by the security research community.

This annual Spotlight would like to take you for a fly-by through our investigation of the loader landscape step by step, starting with getting cozy with our new malware friend Pikabot, continuing to the tall grass hunt for more specimen like it, and the woes of collecting malware data from the Wild Wide Web.

Pikabot overview

Before embarking on looking for traces of Qakbot's competitor activity, we had to get up close and friendly with our potential targets in order to understand how they tick and how to go about looking for more.

Pikabot is a new loader type malware that emerged in early 2023. In its early stages, the loader's purpose was fetching additional malware. Like Qakbot, the loader consists of three main modular components. The loader component is used to drop secondary payloads on infected systems and downloads the malicious DLL.

The code injector is used to decrypt and inject the core module. Finally, the core module is responsible for communicating with the C2 servers; retrieving and injecting malicious payloads from the C2; executing remote commands and code injection. In recent campaigns Cobalt Strike has been used to facilitate the further compromise of the infected system and network.

Pikabot shares similarities with Qakbot including the distribution methods, campaigns, and malware behavior. E-mail thread hijacking is used to attempt to lure the target to interact with a password protected ZIP file.

When this happens, curl is used to download Pikabot, which collects some basic level information like the current user and system network details.

Anti-analysis analysis and main components

One of the fascinating and frustrating things about new malware is keeping up with its changelog.

Pikabot has been undergoing many frequent and rapid changes in the past year, from improving obfuscation techniques being used to the actual processes executed, improving the anti-analysis and detection evasion of the malware.

The frequency of changes could be attributed both to the craftiness of the threat actors always on the lookout for the best methods of avoiding detection, but also to the fact that Pikabot is a relatively new malware.

Regardless of the driver, the steady output of changes complicates tracking any malware, boosting Pikabot's evasion portfolio.

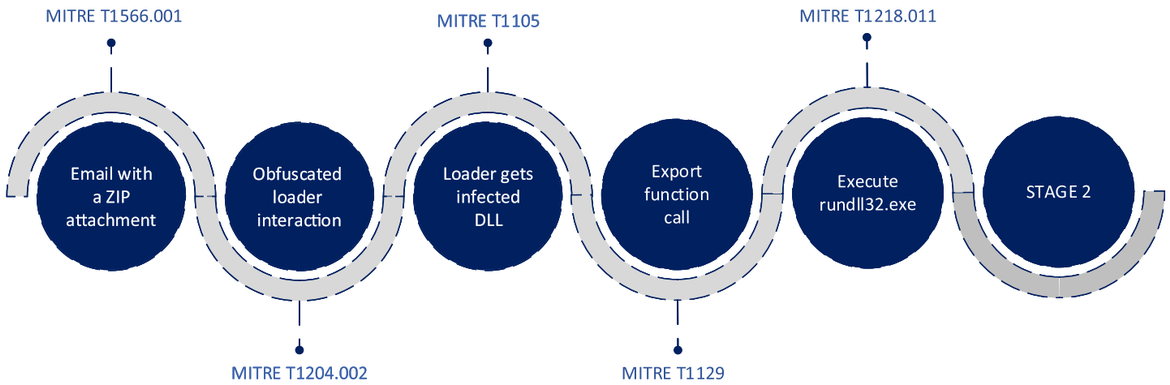


Figure 25: 1 Pikabot Infection Chain

The core module injector

The core module usually contains anti-analysis code, specifically anti-debug and some virtual machine or sandbox checks, as well as flags for checking the user's language to avoid infecting victims in Commonwealth of Independent States (CIS) countries, depending on the operator.

The main functionalities are decrypting, injecting, and executing the core module. Later versions of the malware spawn a legitimate looking SearchProtocolHost.exe process to inject the core module.

In even newer samples, SearchFilterHost.exe is used instead.

The loader

Pikabot's two-step infection chain would usually start with a ZIP attachment to an e-mail, that in most cases holds a JavaScript file (the loader itself) that would execute the second stage upon interaction.

The type of loader differs and can be presented as HTA, IMG, PDF or LNK files, which slightly changes the upcoming steps, but the main goal remains the same: getting a malicious DLL and executing it.

In most cases, the loader downloads the malicious DLL from an external server using the curl command. Next, the loader executes the resulting DLL using rundll32.exe, usually by calling one of its export functions. The name of the export function changes and might be Crash, Enter, vips, Excpt, or something else entirely.

The core module

Unsurprisingly, the core module holds the very center of the malware chocolate egg: the main malicious functions of the loader.

After another round of anti-analysis checks has verified that it is safe to begin operations, the core module will start gathering victim information.

Each victim gets assigned its own ID after which an array of specifications on the user and computer are queried in order to adjust the next steps.

In newer versions of the malware, the following processes are spawned to collect more information:

```
whoami.exe /all

ipconfig.exe /all

netstat.exe -aon
```

The gathered data is encrypted and subsequently sent to a C2 server. The core module, safely nested in the victim system, can then start receiving target specific commands from the threat actor and, for example, begin dropping other malware.

Earlier infections show Pikabot successfully ferrying penetration testing frameworks and other big malware into the victim systems like Cobalt Strike, IcedID, and DarkGate.

The Hunt

After having gotten up close and familiar with Pikabot, we added it to our malware portfolio and turned our sights to the next stage: collecting data on the various loaders' activities in the timeframe between Qakbot's downfall and present time.

Our targets of choice, in addition to Pikabot, were Danabot and DarkGate; solid and popular competitors that had their own breakthroughs and an eventful 2023.

In order to build a reliable landscape picture, we could not rely on internal data only.No analyst team is an island, and cybersecurity's strength lies in its collective community. The array of sources plugged into the sample collection stage included:

- Desk research and previous publications.
- Crowdsourcing YARA rules for the malware families within scope.
- Developing additional YARA rules for Pikabot specifically.
- Performing retrohunts using the outputs above.
- Verifying all Pikabot samples manually.

The downside of multi-source hunting for entire entities like full active malware does, however, come at a potential cost of loss of accuracy. Whatever visibility we might gain could be compromised by noise or improperly set searches. To circumvent this and retain control over the process, NCC Group analysts created multiple additional YARA rules to hunt for Pikabot as a starting point.

If set up correctly, hunt progression would show the following: a decrease in Qakbot's activity, an increase in the usage of Pikabot, and subsequent increases in other loader popularity.

We focused on the most tangible indicators of a malware's activity: capture samples themselves (the most coveted clue), and command & control IOCs that could be attributed to a specific malware family.

Packed samples (malware obfuscated by means of being compressed by other software) did not make it into our analysis due to having to hunt for the various packers used, and out of concern for introducing data duplications.

Tally-ho!

The hunt culminated in 3 graphs for us to dissect: one focusing solely on the sample sightings, and two outlining the C&C numbers.

Finding one: confirmation

The unsurprising but not unwelcome first find among the collected numbers: the Qakbot's takedown is not shy about showing itself through a glaring lack of samples and Qakbot related infrastructure IOCs in the collected findings.

Qakbot was observed decreasing activity and working on their internal infrastructure during the summer months.

This may account for the odd dip in IOCs following May, though it is also unknown how long Operation Duck Hunt was active for, and what kind of effects covert interference might have on these results.

Figures 26 and 27 show Qakbot's dominance and subsequent downfall during Operation Duck Hunt.

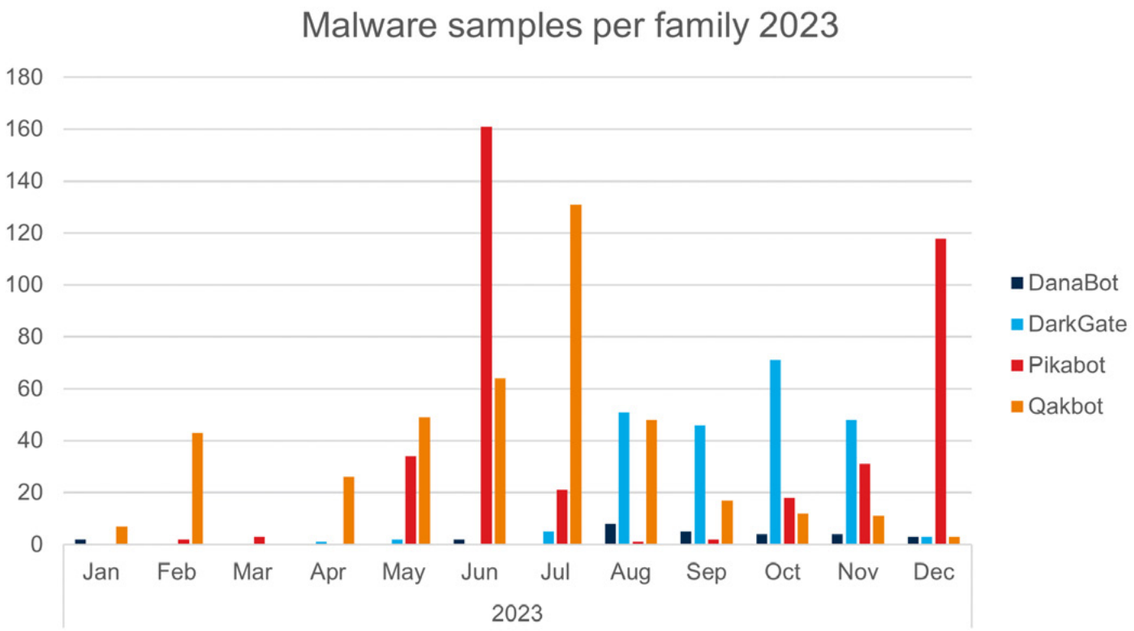


Figure 26: Retrohunt Results for 2023

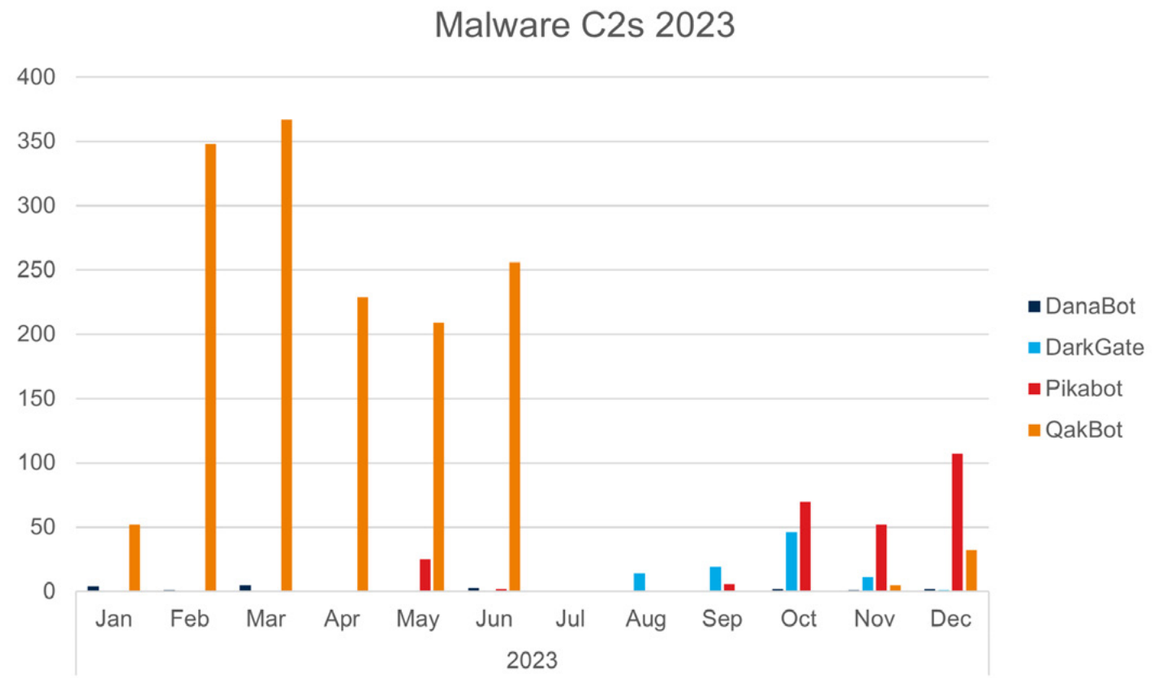


Figure 27: Command & Control Servers for 2023

Finding two: coronation

As for the alleged competitors, Pikabot emerges as the current market leader according to our data. Congratulations, Pikabot!

Finding three: peaks and valleys

Sudden ebbs and rises in the data graphs may seem jagged at a glance, but most tend to have a logical explanation: we simply do not expect smooth progression from malware tracking due to the nature of collecting samples and indicators.

As new versions of malware are pushed by the threat actors, detection on the defending side needs time to improve and develop, a process not represented by a smooth and gradual line.

For 'commercial' malware (i.e. advertised and distributed through underground forums and chatter as opposed to kept in smaller teams), this is further intensified since more operators could potentially make use of the updated malware versions, resulting in higher detection (sharper rise) on the graphs simply due to higher numbers involved in the attacks that will then get detected.

Correlations between the developments we currently know of within the presented malware families and their detection numbers indicate a change-detection lag of ca 3 weeks.

For the collected samples (Figure 26), the peaks in May and November correlate neatly with Pikabot's technical evolution steps and new features added. Danabot upgraded to version 3 in July, moving the detection ticks upwards the next month.

Some sharp increases and decreases may have other internal explanations requiring us to corroborate sources. DarkGate related IOCs taper off quite aggressively after their October peak, though there are no conclusive reasons for this.

One hypothesis is the noted difficulty in crypting DarkGate – obfuscating the malware so that it may be delivered to target systems undetected – on underground forums.

This issue came to light in December 2023, which resulted in the DarkGate's developer offering to crypt the malware for customers at the cost of USD 5000 and recommending a crypting service costing upwards of an impressive USD 10000.

These additional costs to an otherwise very expensive malware (a monthly license easily costs USD 15000) may have influenced the ongoing operations and sourcing of additional customers.

Several threat intelligence providers have observed and reported on small-scale campaigns involving Qakbot in December, indicating the project may be severely hamstrung but perhaps not down for the count.

As no arrests were made it is possible that the development team behind Qakbot were able to set up their infrastructure and resume operations.

If this were the case, it would account for the November and December uptick in samples and IOCs seen in figures 26 and 28.

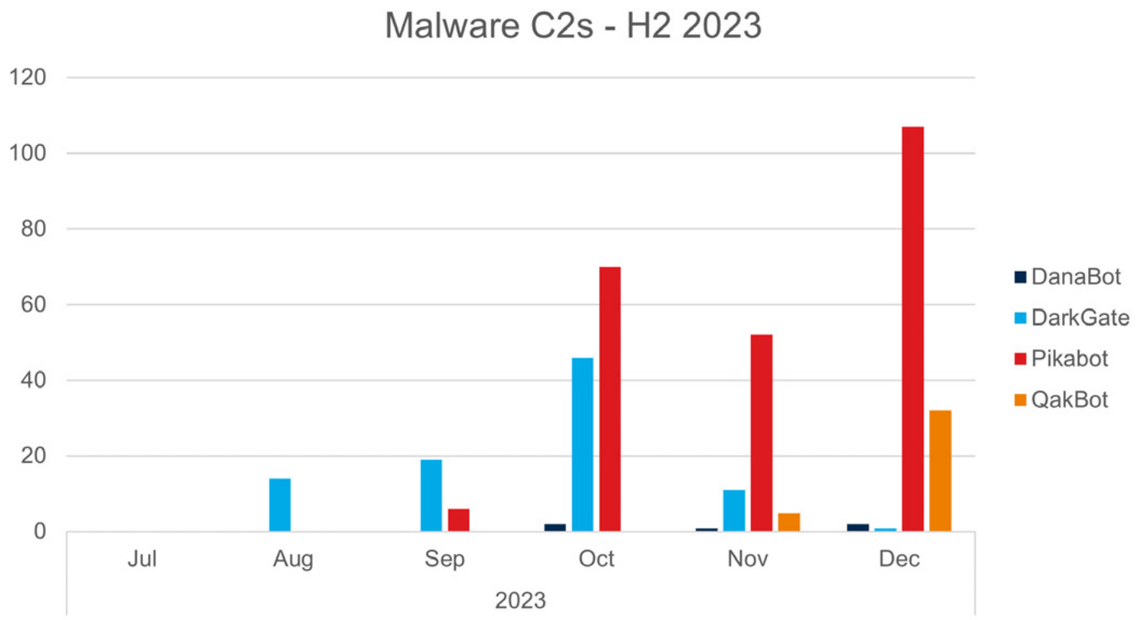


Figure 28: Command & Control Servers for H2 2023

The danger of statistics

As much as we would love our findings to be irrefutable, there is always a risk with using increasingly large datasets collected from third party sources to make trend explanations and predictions.

Ultimately, confidence scores assigned to C&C related IOCs or reliability of YARA rules developed by someone else will always decrease reliability of findings – in addition to the fact that investigated targets are criminal tools developed in a notoriously non-transparent setting. In order to keep the results as tightly controlled as possible, we have set the following hard criteria to minimize noise:

- Public YARA rules used to hunt for samples were selected from the sets with proven accuracy and a low false positive rate.
- C&C selection was based on a confidence threshold with a high score (75 to 100) assigned by the submitters.

Unfortunately, even imposing constraints and reducing scope does not entirely remove the risk of duplicates if the same infection was captured using different methods that could potentially result in multiple entries describing the same event from different angles.

Wrap-up

2023 has been a turbulent and exciting year in the loader microcosm. Like avid birdwatchers, threat analysts have keenly observed new families rise and develop, taking their place among the names in our monitoring.

For the recipients of the report, unfortunately, this means that new threats have grown and settled into the landscape within an impressive timeline.

Despite Qakbot's dramatic downfall, it would seem there is not one specific competitor that has shown alarming levels of activity to fill the vacuum of its absence. On the contrary, several strong players ended up developing new toolsets and capabilities, providing a steady increase in the loader market. Regardless of the internal drivers that acted as catalysts for the developer teams behind DarkGate, Danabot, and Pikabot to push their products to the public, the result is the same: it would seem we have traded Qakbot for at least three worthy challengers that have taken the last two quarters of the 2023 by storm.

Diversity in the choice of tooling allows multiple threat actors to pick the instruments for the job with more ease.And so, we go excitedly into 2024 armed with the knowledge that the hunt has just begun.

Further research into the activity relating to other loaders may further illuminate the dynamics of the current landscape.

About us

NCC Group is a global cyber and software resilience business, operating across multiple sectors, geographies and technologies.

As society's dependence on the connected environment and associated technologies increases, we use our global expertise to enable organisations to assess, develop and manage their cyber resilience posture to confidently take advantage of the opportunities that sustain their business growth.

With circa 2,400 colleagues, we have a significant market presence in the UK, Europe and North America, and a growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

+44 (0)161 209 5200
response@nccgroup.com
www.nccgroup.com