nccgroup

People powered tech-enabled cyber security

Cyber Threat Intelligence

Annual Report 2024

FOX IT
part of nccgroup

Contents

Foreword

Reflecting on the cyber security landscape of 2024, it is evident that the challenges organisations faced were unprecedented in scale and complexity. Last year was marked by a series of high-impact cyber incidents that tested the resilience of businesses and institutions worldwide. From crippling ransomware attacks to sophisticated nation-state espionage campaigns, the financial and operational repercussions underscored the urgent need for stronger defences and more strategic responses.

This annual report provides a detailed analysis of the pivotal events that shaped the cyber security environment in 2024. By exploring key incidents—from the exploitation of zero-day vulnerabilities to global law enforcement efforts dismantling cybercriminal networks—we aim to equip organisations with the insights needed to fortify their operations against similar threats in the future.

Looking to the future, the challenges posed by cyber threat actors are set to escalate, with consequences that may feel like science fiction but are all too real. Cybercriminals and nation-state actors are capitalising on the growing integration of technology into every aspect of our lives. This seamless connectivity, while transformative, presents attackers with increasing opportunities to disrupt systems, steal data, and create chaos at an unprecedented scale.

Third-party compromises are expected to remain a critical concern. The next major breach could send devastating ripple effects across supply chains. In parallel, the rapid advances in artificial intelligence (AI) are giving rise to a new generation of cybercriminal tactics. With AI-driven tools, phishing schemes are becoming more convincing, while generative AI, deepfake technology, and advanced language models make detecting attacks significantly harder.

Cloud vulnerabilities and insecure APIs continue to threaten sensitive business data and critical systems. A single misconfiguration in the cloud could expose entire networks, while poorly secured APIs remain an entry point for attackers to infiltrate systems. These persistent issues emphasise the importance of maintaining robust security hygiene in rapidly evolving technological environments.

Meanwhile, the proliferation of Internet of Things (IoT) devices presents a mounting risk. From smart appliances to city-wide IoT systems, these devices often lack adequate security, making them prime targets for attackers. Cybercriminals have already hijacked IoT devices to build massive botnets, and as these technologies become integral to critical infrastructure, their potential to disrupt operations and expose sensitive data will only grow.

Even ransomware —a long-standing cyber threat— continues to evolve. While traditional attacks focused on encrypting data, many attackers now prioritise data theft, which is faster, easier, and more profitable. Stolen information can be leveraged for extortion, fraud, identity theft, or even future breaches, making it a highly valuable commodity in the hands of cybercriminals.

The geopolitical dimension of cyber security also makes for an ever-changing threat landscape. Nation-state actors are intensifying their efforts to compromise critical infrastructure, including energy, healthcare, and telecommunications. Sophisticated campaigns, such as those by Volt Typhoon, have already highlighted the fragility of these sectors. The use of “pre-positioning”—where adversaries covertly infiltrate systems in preparation for future sabotage or disruption—is a stark reminder of the hidden vulnerabilities that could be activated during times of geopolitical tension or conflict.

In response to these threats, NCC Group remains committed to strengthening its threat intelligence capabilities. Through collaboration with international partners and leveraging cutting-edge technologies, we aim to help our clients not only understand the evolving threat landscape but also act decisively to mitigate risks.

As we publish this report, the cyber security challenges ahead demand that businesses, governments, and individuals stay vigilant and proactive. By understanding the risks and acting today, we can collectively work towards a more secure digital future.

Thank you for your continued trust in us as we navigate these challenges together.

Sincerely,

Matt Hull

Global Head of Threat Intelligence

Section 1

Timeline of Critical Incidents

The timeline below provides insights into cyber incidents observed across 2024. This encompasses everything from ransomware attacks and nation-state targeting, to law enforcement and government activity.

11/01/24

Chinese threat actors, UNC5221, were suspected of exploiting zero-day vulnerabilities in Ivanti Connect Secure VPN and Ivanti Policy Secure gateway. CVE-2023-46805 and CVE-2024-21887, affect all supported versions of the Ivanti Connect Secure VPN and Policy Secure Gateway. Their exploitation allows attackers to bypass authentication and execute arbitrary commands with elevated privileges. The nation-state group used advanced methods to maintain persistence and evade detection, including custom malware and deception of Ivanti's Integrity Checker Tool.

07/02/24

The Cyber Security and Infrastructure Security Agency (CISA), National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) issued an advisory on Volt Typhoon, regarding their compromise of US critical infrastructure networks. The advisory highlighted that Volt Typhoon is pre-positioning itself on IT networks to enable disruptive or destructive cyberattacks in the event of a major crisis or conflict with the United States.

Volt Typhoon has targeted multiple critical infrastructure sectors, including Communications, Energy, Transportation Systems, and Water and Wastewater Systems, across the US and its territories, including Guam. The group's activities are not consistent with traditional cyber espionage but instead are focused on enabling lateral movement to operational technology (OT) assets to disrupt functions.

20/02/24

Operation Cronos was initiated by the UK's National Crime Agency (NCA), in collaboration with US and EU agencies, and aimed to dismantle the infrastructure supporting LockBit ransomware. The operation dismantled over 30 servers essential to LockBit's infrastructure. This included servers to host malware and coordinate ransom negotiations, as well as vital backend systems. Authorities arrested multiple individuals from developers to affiliates who executed attacks. Seized decryption keys were distributed to victims, allowing them to recover data without paying ransoms.

28/02/24

Change Healthcare, a subsidiary of the UnitedHealth Group, suffered a significant ransomware attack by the ALPHV/Blackcat group. The attackers claimed to have stolen 6 terabytes of sensitive data from the company. The breach disrupted Change Healthcare's systems, which serve as a critical intermediary for medical and insurance data processing. Following the breach, the company engaged cyber security experts from Mandiant and Palo Alto to investigate the attack.

05/03/24

The personal information of up to 43 million citizens was compromised in a data breach at France Travail, a French government department responsible for assisting unemployed individuals. The breach exposed names, dates of birth, social security numbers, email addresses, postal addresses, and phone numbers. The incident, which occurred between February 6 and March 5, was investigated by the Cybercrime Brigade of the Paris Judicial Police Department.

The breach raised concerns about identity theft and fraud, as the stolen data could be linked to other breaches to create larger profiles on individuals. French citizens were advised to be vigilant against phishing attempts and ensure that their passwords are strong. This breach follows a previous incident last year that affected 10 million citizens and is considered the worst-ever data breach in France. The attack coincides with DDoS attacks on French government departments, claimed by the pro-Russia Anonymous Sudan group.

06/04/24

A major cyber incident targeted several key maritime ports and vessels, deploying sophisticated ransomware and malicious software that disrupted port operations and manipulated Automatic Identification Systems (AIS) on ships. This led to substantial delays, misrouted cargo, and increased risk of collisions.

The financial impact was severe, with estimated losses exceeding $500 million, including direct operational disruptions and indirect costs like insurance claims and ransom payments. Major ports in Europe, Asia, and North America, including the Port of Rotterdam and the Port of Singapore, experienced extensive delays and operational shutdowns.

Sensitive data, such as cargo manifests and crew details, were compromised, posing risks of identity theft and espionage. The incident highlighted the urgent need for enhanced cyber security measures in the maritime industry, which relies heavily on outdated systems and lacks robust cyber security protocols.

02/05/24

The second phase of Operation Cronos involved intense international efforts, including sanctions and legal actions against key actors. Notably, a Russian national, identified as the developer and administrator of LockBit, was sanctioned by the United Kingdom, United States, and Australia.

The sanctions, including asset freezes and travel bans, were imposed by the UK Foreign Commonwealth and Development offices, the US Department of the Treasury's OFAC, and the Australian Department of Foreign Affairs and Trade. A US Indictment was unsealed against this individual for his role in LockBit's creation.

12/05/24

The healthcare communication platform ConnectOnCall experienced a significant data breach, compromising the personal information of 900,000 patients and healthcare providers.

The breach involved unauthorised access to the platform between February 16 and May 12, 2024. Exposed data includes names, phone numbers, medical record numbers, dates of birth, and details related to health conditions, treatments, and prescriptions. ConnectOnCall promptly secured its systems, took the platform offline, and enlisted external cyber security specialists to investigate and enhance security measures.

27/05/24

Operation Endgame was a significant international effort led by France, Germany, and the Netherlands, supported by Eurojust. This also involved Denmark, the UK and US, as well as Armenia, Bulgaria, Lithuania, Portugal, Romania, Switzerland, and Ukraine. The operation targeted botnet infrastructure used for deploying malware, including ransomware, affecting millions globally.

Authorities disrupted over 100 servers and seized more than 2000 domains linked to malware distribution, particularly targeting "dropper" malware families like IceID, Smokeloaded, Pikabot, and Bumblebee. Endgame's impact extended beyond the immediate takedown, with authorities arresting suspects in Ukraine and Armenia, and issuing arrest warrants for eight individuals in Germany.

03/06/24

The ransomware attack on Synnovis impacted healthcare services across multiple London hospitals. Synnovis provides essential pathology services to Guy's and St. Thomas' NHS Foundation Trust and King's College Hospital NHS Trust, as well as general practitioners across six London boroughs.

The attack disrupted IT systems that handle blood tests and other diagnostics, creating severe delays in patient care. As a result, critical incidents were declared in some hospitals due to resource strain, and some non-urgent procedures were cancelled or rescheduled. Blood transfusion systems were notably affected, with emergency protocols in place to reserve blood only for essential transfusions.

19/06/24

The BlackSuit ransomware attack on CDK Global caused a massive disruption to car dealerships across North America, prompting a critical outage that forced CDK to shut down its IT systems.

This resulted in dealerships being unable to process sales, manage inventory, or provide customer service, leading to significant operational challenges. CDK Global initiated negotiations with BlackSuit to avoid leaking data. The attack affected major dealership groups such as Penske Automotive and Sonic Automotive, which had to rely on manual operations.

12/07/24

AT&T reported a major data breach affecting the call and SMS logs of approximately 109 million customers. The breach targeted AT&T's data stored on the Snowflake cloud platform, where attackers accessed logs from multiple timeframes. These logs contained metadata such as phone numbers, call durations, and cell sited IDs. The breach raised significant security concerns due to the sensitive nature of the communications data involved, despite the lack of direct personal identifiers.

After discovering the breach, AT&T collaborated with the FBI and the US Department of Justice (DoJ) to delay public disclosure, citing potential risks to national security and public safety.

06/08/24

Ransomware targeted the Paris Olympics, affecting IT systems at the Reunion des Musees Nationaux, which manages nearly 40 museums, including Olympic venues like the Grand Palais. Although the attackers encrypted some data and demanded a ransom, quick action by cyber security teams prevented significant disruptions to Olympic events. French authorities, aided by the pre-event security enhancements from the French cyber security agency, were prepared for such attacks and had implemented robust defenses, including penetration tests and awareness initiatives. The attack was one of over 68 attempted breaches recorded since the Olympic games started.

26/09/24

The Texas-based UMC health system suffered a ransomware attack that severely impacted its operations. The incident led the hospital to temporarily shut down its IT system to prevent further compromise, which disrupted patient services and forced the diversion of emergency patients.

Initially, many patients were rerouted, though the emergency center eventually resumed ambulance intake, with limited patient diversions still in place. UMC's 30 clinics across Texas and New Mexico remained operational, although certain services like radiology were impacted and required downtime.

01/10/24

The third phase of Operation Cronos targeting LockBit was coordinated by Europol, Eurojust, and law enforcement from 12 countries. This operation led to significant seizures and arrests. Key actions included the arrest of a suspected LockBit developer in France and two individuals in the UK linked to LockBit affiliates. Spanish authorities seized nine servers and arrested a hosting service administrator.

Additionally, the US, UK, and Australia imposed sanctions on individuals tied to LockBit and Evil Corp. Europol's Joint Cybercrime Action Taskforce played a central role, providing analytical support, crypto-tracing expertise, and coordinating technical operations.

07/10/24

The BidenCash marketplace leaked over 1.2 million payment card details on a cybercrime forum. The leaked data included card numbers, expiration dates, CVV numbers, and other personal information, such as names and addresses. This leak was part of a promotional strategy by BidenCash to advertise their services. The compromised cards were primarily from the US, India, and Brazil.

28/10/24

Operation Magnus targeted two major infostealer malware families: RedLine and META. This operation was led by US agencies including the FBI and IRS Criminal Investigation, in partnership with Europol, Eurojust, and law enforcement in Belgium and the Netherlands. These infostealers capture sensitive data, such as login credentials, financial information, and cryptocurrency account details, which are then sold on dark web forums.

The operation disrupted the infrastructure supporting these malware families, including seizing domains, servers, and telegram channels linked to their administrator. One of the key figures, Maxim Rudometov, a Russian national, was charged for his role in the development and operation of RedLine. He faces charges related to fraud and money laundering.

31/10/24

Operation Serengeti led by INTERPOL and AFRIPOL between September and October 2024, targeted cybercriminals across 19 African countries. The operation resulted in the arrest of 1,006 suspects and the dismantling of 134,089 malicious infrastructures. The operation focused on various cybercrimes, including ransomware, business email compromise (BEC), digital extortion, and online scams. It identified over 35,000 victims and linked cases to nearly $193 million in financial losses worldwide.

13/11/24

The FBI and CISA issued a joint statement revealing a cyber espionage campaign by the People's Republic of China (PRC) targeting commercial telecommunications infrastructure. PRC-affiliated actors compromised networks at multiple telecommunications companies, enabling the theft of customer call records, compromising private communications in government, and copying information subject to US law enforcement requests.

The FBI and CISA have provided technical assistance, sharing information with potential victims, and working to strengthen cyber defences across the commercial communications sector. They encourage any organisation that believes it might be a victim to contact their local FBI Field Office or CISA.

01/12/24

PIH Health faced a major disruption due to a ransomware attack that compromised part of its network. In response, the healthcare provider shut down its entire network as a precaution, affecting critical communication systems, including phone lines, voice messages and internet services across its hospital.

PIH Health engaged third-party cyber forensic specialists to assist with the investigation and recovery efforts. The ransomware virus was isolated, and work is ongoing to securely restore affected systems.

04/12/24

Law enforcement agencies successfully demolished sophisticated Russian money laundering networks in a large worldwide investigation known as "Operation Destabilise." The investigation focused on two major Russian-language networks, Smart and TGR, which facilitated the laundering of billions of dollars for cybercriminals, drug traffickers, and sanctioned Russian leaders.

The operation resulted in 84 arrests, the confiscation of more than £20 million in cash and cryptocurrency, and the suspension of operations in 30 countries. The networks exploited bitcoin exchanges to transfer illicit payments without crossing physical borders, having a substantial influence on global cybercrime and money laundering activities.

04/12/24

Reports confirm a two-year campaign in which Russian cyber-espionage group Turla hijacked the infrastructure of the Pakistani threat actor Storm-0156 to conduct their own attacks. By taking over the Pakistani group's servers, Turla was able to launch covert operations against already compromised targets, making their activities harder to detect. This tactic of hijacking other hackers' infrastructure is a sophisticated method that allows Turla to mask their operations and exploit the existing access and tools of other threat actors.

08/12/24

Threat actors successfully hacked the US Treasury Department by exploiting a remote support platform used by the federal agency. According to a letter obtained by the New York Times, the incident has been attributed to a Chinese state-sponsored Advanced Persistent Threat (APT) actor. BeyondTrust's investigation revealed two zero-day vulnerabilities, CVE-2024-12356 and CVE-2024-12686, which enabled the threat actors to breach and take control of Remote Support SaaS instances.

As the Treasury Department was a customer of one of these compromised instances, the attackers were able to access agency computers and remotely steal documents.

18/12/24

Mark Sokolovsky, a 28-year-old Ukrainian national, has been sentenced to 60 months in federal prison for his role in operating the Raccoon Infostealer malware. Sokolovsky conspired to run Raccoon Infostealer as a malware-as-a-service (MaaS), allowing cybercriminals to lease access to the malware for approximately $200 per month, paid in cryptocurrency. This malware was used to steal personal data, including login credentials and financial information, then used for financial crimes or sold on cybercrime forums.

25/12/24

4.45GB of data leaked from Cisco's DevHub platform, following an earlier breach in October. This incident was caused by a misconfiguration that made certain files publicly accessible. The leaked data, posted online by the hacker known as IntelBroker, included Java binaries, source code, cloud server disk images, cryptographic signatures, and internal project archives.

Cisco emphasised that its internal systems and enterprise environments remain secure, and that no sensitive customer information such as personally identifiable information (PII) or financial data was exposed. The company has since corrected the configuration error and enhanced its security measures to prevent similar incidents in the future.

Section 2

15%

Global ransomware attacks increased by 15% in 2024

27%

Industrials accounted for 27% of ransomware attacks in 2024

10%

LockBit was responsible for 10% of attacks in 2024

Ransomware Key Statistics

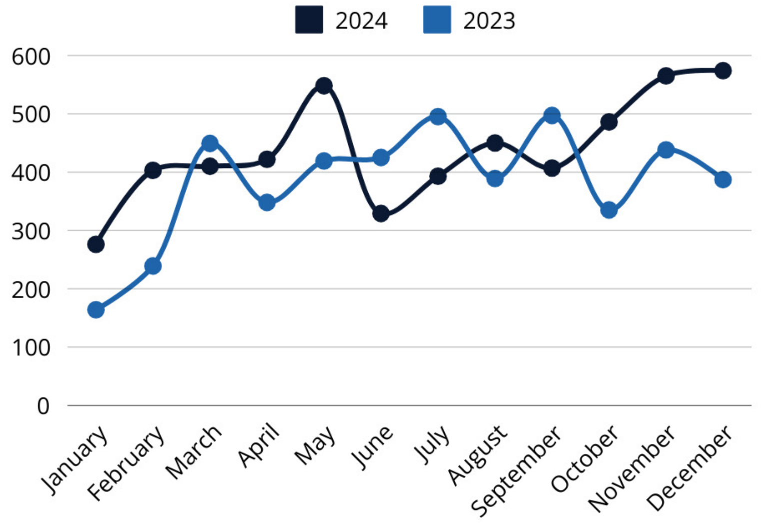


Figure 1 Number of Ransomware Attacks 2023 vs 2024

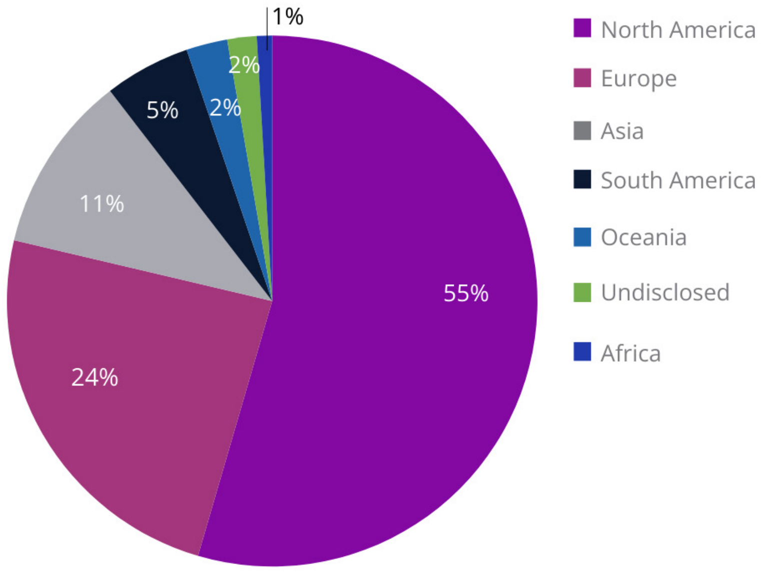


Figure 2 Number of Ransomware Attacks by Region 2024

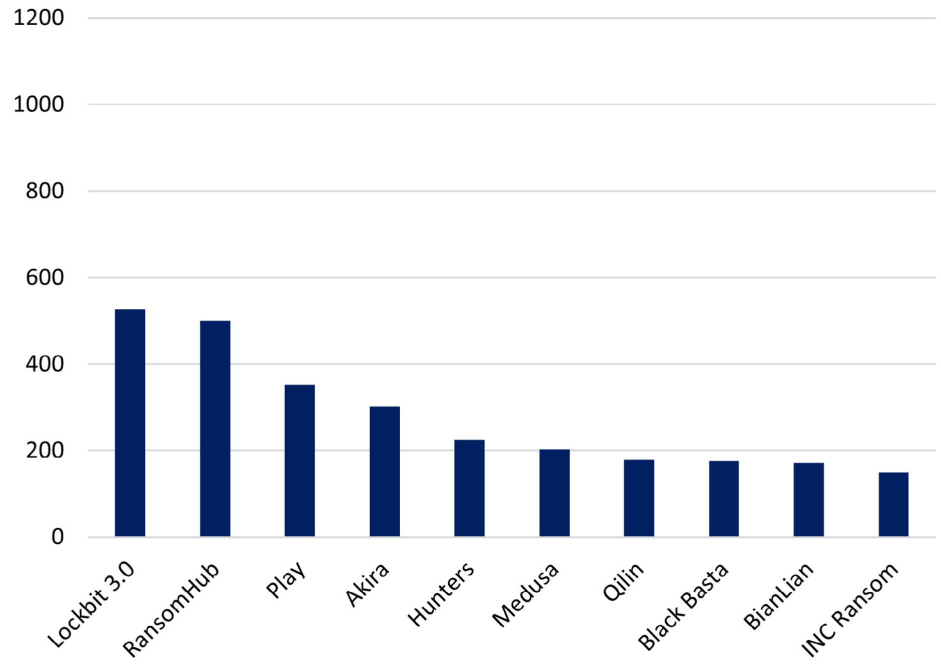


Figure 3 Top 10 Threat Actors 2024

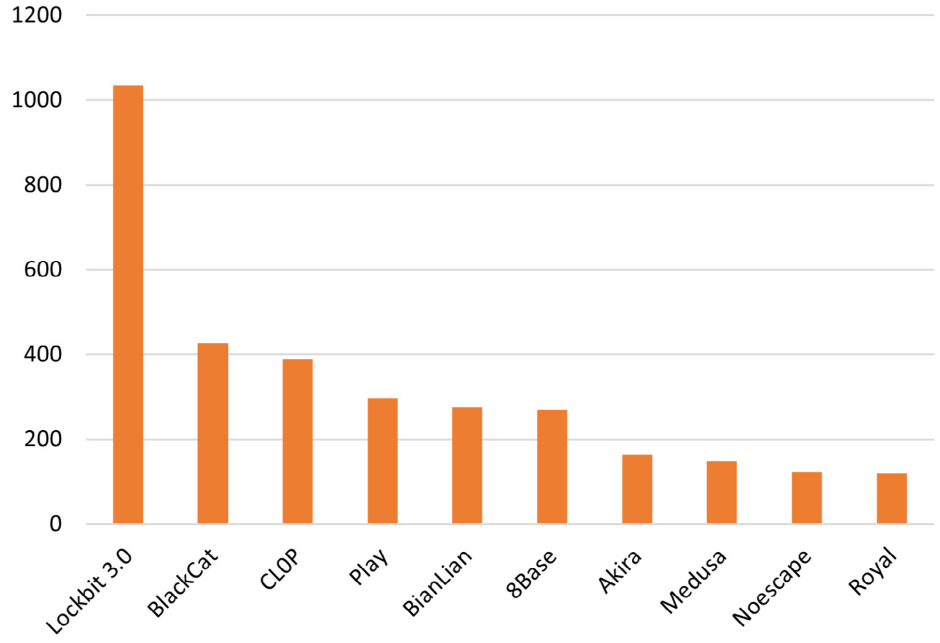


Figure 4 Top 10 Threats Actors 2023

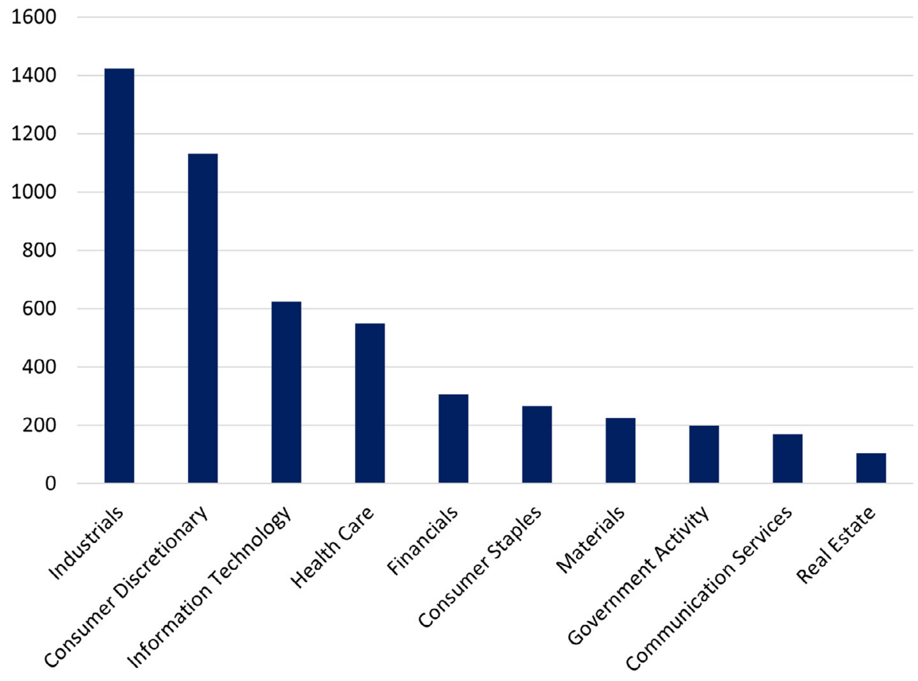


Figure 5 Top 10 Targeted Sectors 2024

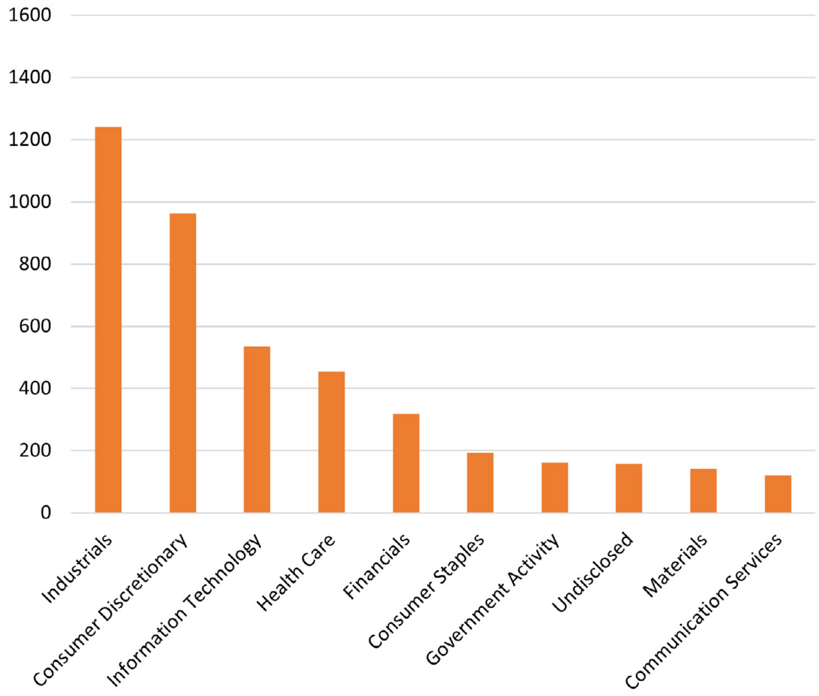


Figure 6 Top 10 Targeted Sectors 2023

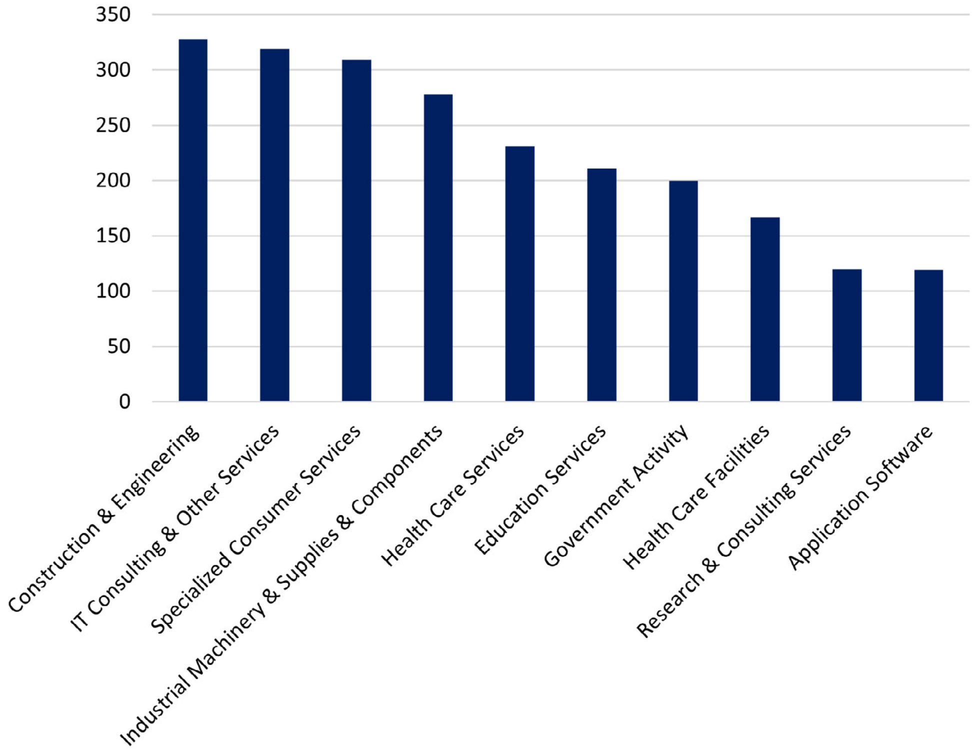


Figure 7 Top 10 Ransomware Attacks by Sub-Industry 2024

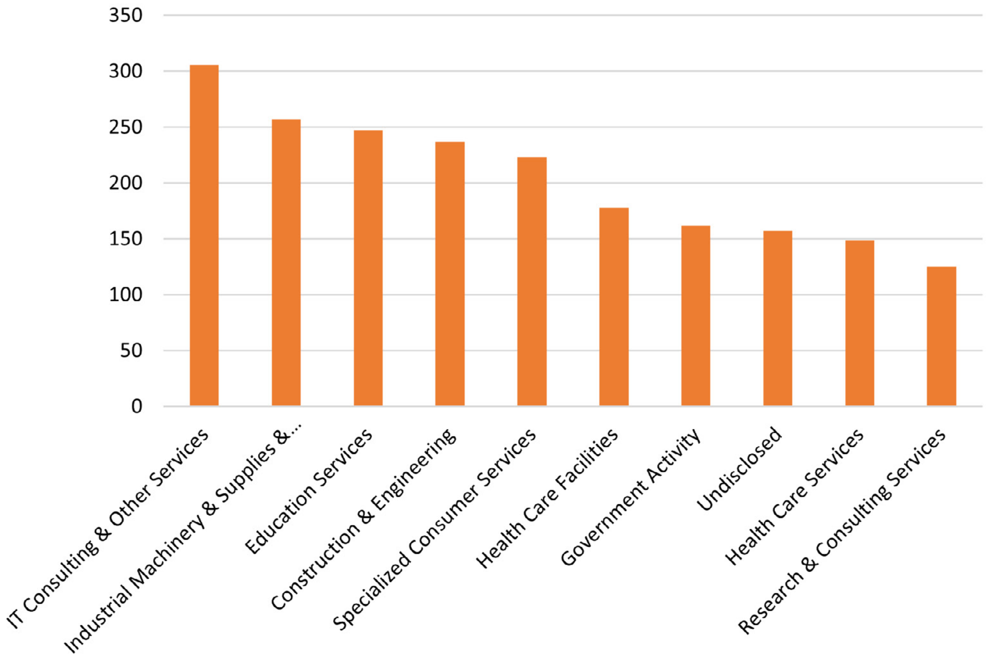
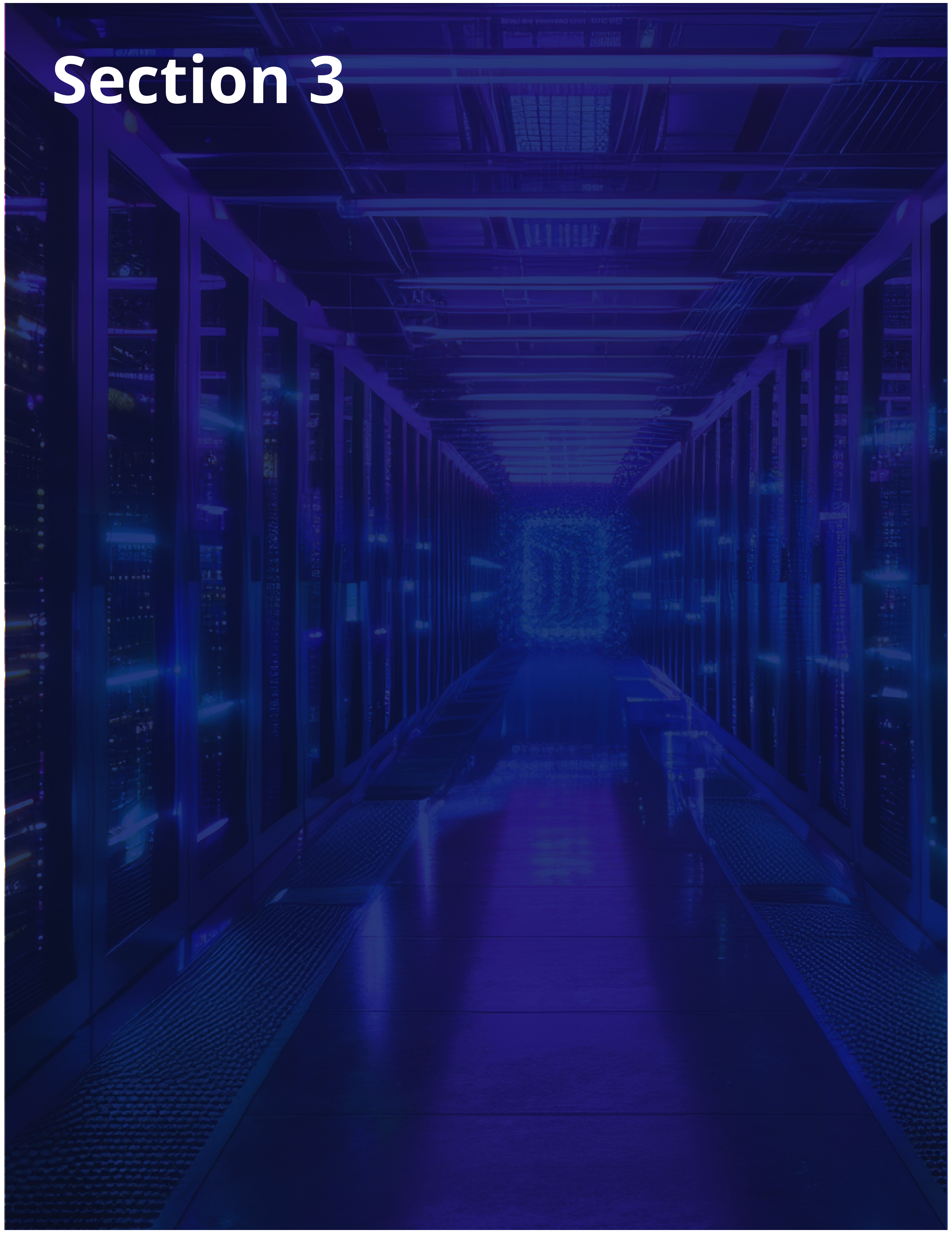


Figure 8 Top 10 Ransomware Attacks by Sub-Industry 2023



Section 3

Ransomware Statistical Trends 2024

2024 saw a major shift in the number of attacks per month within the ransomware threat landscape. 5263 attacks were recorded, an increase of 15% from 2023. This surge was particularly noticeable in the latter half of 2024, with November and December experiencing the highest monthly attacks, 565 and 574 respectively. This differs from previous observations in which December normally sees a decrease in ransomware attacks around the holiday season.

All regions experienced an increase in ransomware attacks in 2024. North America remains the most targeted region with 2869 attacks, up 25% from 2023. Asia observed 571 attacks, a 23% increase from 2023, and South America 276, an increase of 29%. Europe, Oceania and Africa saw modest increases alike, which are further detailed in the regional section below.

LockBit remained the most prominent threat actor of the year, although the group's activity declined from 1034 attacks in 2023 down to 526 in 2024. New actors such as RansomHub rose up the rankings, contributing to the overall increase in attacks. Other notable actors like Play and Akira saw an increase in their activity, with Akira nearly doubling their attacks from 164 in 2023 to 303 in 2024. Lastly, Funksec, a new group which emerged as the top threat actor for December 2024, will be one to watch in 2025.

Several factors contributed to the increase in ransomware attacks in 2024, in which exploited vulnerabilities and compromised credentials were among the top causes. In addition, geopolitical tensions heightened the risk of ransomware being used as a tool to achieve political goals. Moreover, attacks have become more profitable due to increasing cryptocurrency values further escalating these threats. A rise in Ransomware-as-a-Service (RaaS) platforms has also made it easier for attackers to launch attacks, whilst law enforcement action led to the emergence of new threat actors. In 2023, we recorded 62 threat actors which increased to 94 in 2024.

Industrials Remains the Top Ransomed Sector

The industrials' sector was the most targeted, up from 1240 attacks in 2023 to 1424 in 2024, an increase of 15%. This sector is a key component of the global economy, making it a prime target for threat actors. The attacks on the sector have been disruptive, affecting critical infrastructure and causing significant operational downtime.

Many industrial organisations still rely on legacy systems that may not be adequately updated or patched. These outdated systems often have vulnerabilities which threat actors exploit to gain information or infiltrate the system and drop ransomware programs. Fog ransomware was observed to be targeting virtual environments and backup systems that are critical to industrial operations. It can encrypt machine files and delete backups to disrupt operational continuity. Helldown also leveraged tools from LockBit's leaked builder to actively target the manufacturing sector and proceed with dual extortion tactics.[1]

In addition to vulnerabilities posed by legacy systems, the convergence of Operational Technology (OT) and Information Technology (IT) in industrial environments has expanded the attack surface.[2] While IT systems are typically more secure, OT systems may lack the same level of protection which provides an entry point for various threat actors specialising in the sector. For instance, BlackSuit, formerly known as Royal, rebranded and enhanced its capabilities to target industrial organisations more effectively to cause significant operational disruption. Furthermore, the sector's reliance on interconnected supply chains makes it particularly vulnerable to ransomware attacks, in which one successful attack can have a cascading effect on others within the supply chain, significantly increasing its impact.

The industrial sector must acknowledge the changing landscape of cyber threats and take proactive measures to protect its operations. Organisations can better fight against sophisticated threats by investing in legacy system modernisation, enhanced cyber security measures, and employee training. This comprehensive approach will reduce the dangers posed by ransomware and other cyberattacks, assuring the resilience and continuation of vital industrial operations.

RansomHub Becomes the Most Active Threat Actor

RansomHub emerged as the most active threat actor following the attempted takedown of LockBit 3.0. Early in H1 2024, LockBit continued to be the dominant player within the ransomware landscape. However, law enforcement operations, notably Operation Cronos, which took down their infrastructure and revealed the identity of their lead operator, caused a significant drop in activity by the end of H2 2024.[3]

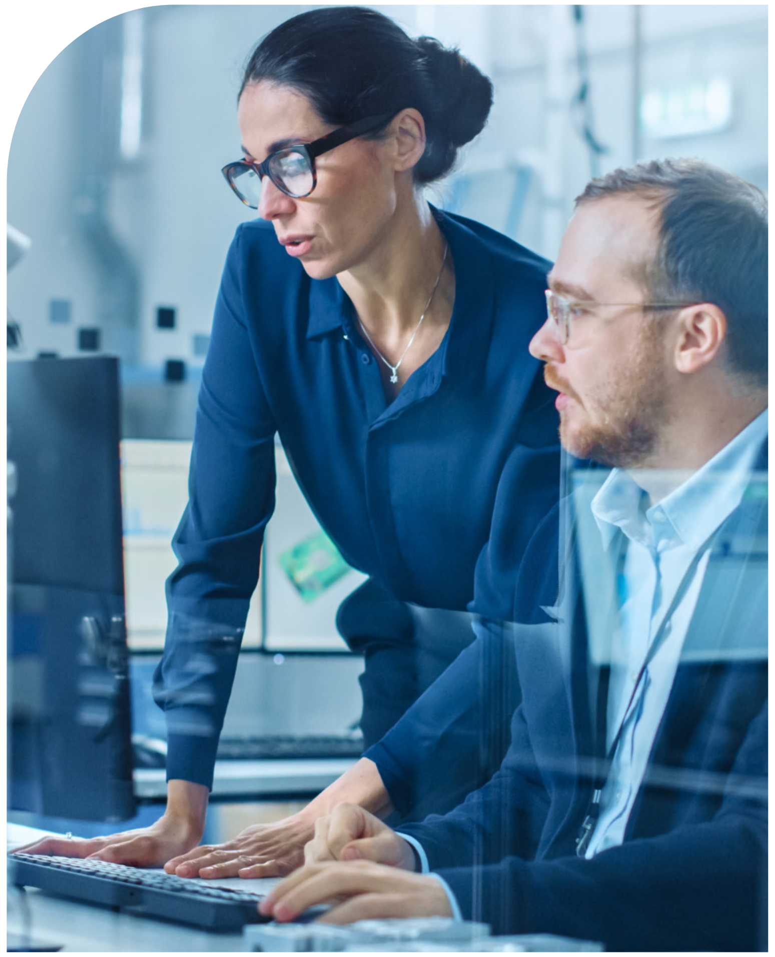
These efforts opened a vacuum in the ransomware landscape which caused many affiliates to either find another operator or create their own variant. RansomHub emerged as a top destination for high level affiliates of LockBit and ALPHV.

Descended from previously prominent variants like Knight and Cyclops, RansomHub's reputation and technical expertise opened the door for experienced LockBit affiliates to begin conducting attacks with RansomHub.[4]

This trend is reflected by the data in H1 2024, where LockBit held 433 victims compared to RansomHub with 123. In H2 2024, RansomHub numbers grew to 378 victims, surpassing LockBit with only 93. These numbers follow law enforcements' efforts against LockBit, likely influencing the decline. Equally, the authenticity of these numbers remains in question, where it is suspected LockBit artificially inflated their numbers following the takedown.

Overall, RansomHub's emergence can be attributed to the dynamic between RaaS and law enforcement operations. Targeting major players has forced affiliates to find the next best operator who can provide them with the best software and commission.

This trend is expected to continue with increased activity by major RaaS operators like RansomHub, along with the emergence of more variants. Law enforcement operations will continue; however, affiliates will create or join other ransomware operators where major players are targeted.



Regional Ransomware Trends

North America (2689 attacks) and the European Union (1272 attacks) continued to see the greatest number of attacks, in line with our observations since 2021. The data also indicated a 23% rise in attacks in Asia, a 29% increase in South America, and a 22% uptick in Oceania, when compared to 2023. High payouts, geopolitical pressures, and a thriving RaaS ecosystem are potential factors which explain the multi-regional increase.

2024 was on pace to be a record year for ransom payments, further buoyed by increasing cryptocurrency values.[5] 2024 also saw a record $75 million ransom payment to the Dark Angels group. The financial incentive to conduct attacks has drawn in more operators and affiliates who look to increase their operations on a global scale. Moreover, organisations in Asia, South America, and Oceania have also been undergoing rapid digitisation, increasing the risk of threat actors looking to exploit weak cyber security measures.

Geopolitical factors are also likely at play. States such as the Democratic People's Republic of Korea (DPRK), who invest significantly into financially motivated cybercrime, made over $1.34 billion, a 103% increase from 2023's $660.50 million.[6] Moreover, the Russia-Ukraine war and tensions in the South China Sea have placed organisations in the crossfire of threat actors, blurring the lines between state-sponsored and criminal activities.[7] Ransomware operators can be leveraged as a geopolitical tool by targeting CNI and simultaneously funding regimes, whilst averting kinetic military operations.[8]

The increased number of ransomware operators, and possibly affiliates, has created a thriving RaaS ecosystem allowing threat actors to increase attack volume on organisations outside of the EU and NA. High payouts and nation-states who support ransomware operations against geopolitical competitors have allowed ransomware threat actors to enjoy an environment with more sophisticated resources. This has also lowered their risk of being apprehended.

Conclusion

In 2025, we expect to see a continued increase in attack numbers, in line with the incline observed since 2021. Attacks are highly likely to be directed at sectors like industrials, who have historically been vulnerable to ransomware attacks. Law enforcement operations will continue to target major operators. However, the thriving RaaS ecosystem will allow affiliates to easily change their operator and continue conducting attacks under a different ransom group name. Growing use of AI and machine learning to assist with attacks, and defence strategies will significantly reshape the cyber security landscape. Basic security foundations must be implemented by organisations to ensure a proactive defence against ransomware. Integrating technological and automated solutions alike, such as AI-assisted measures, should also be considered to facilitate the process where possible.

Section 4

Law Enforcement Targeting Ransomware

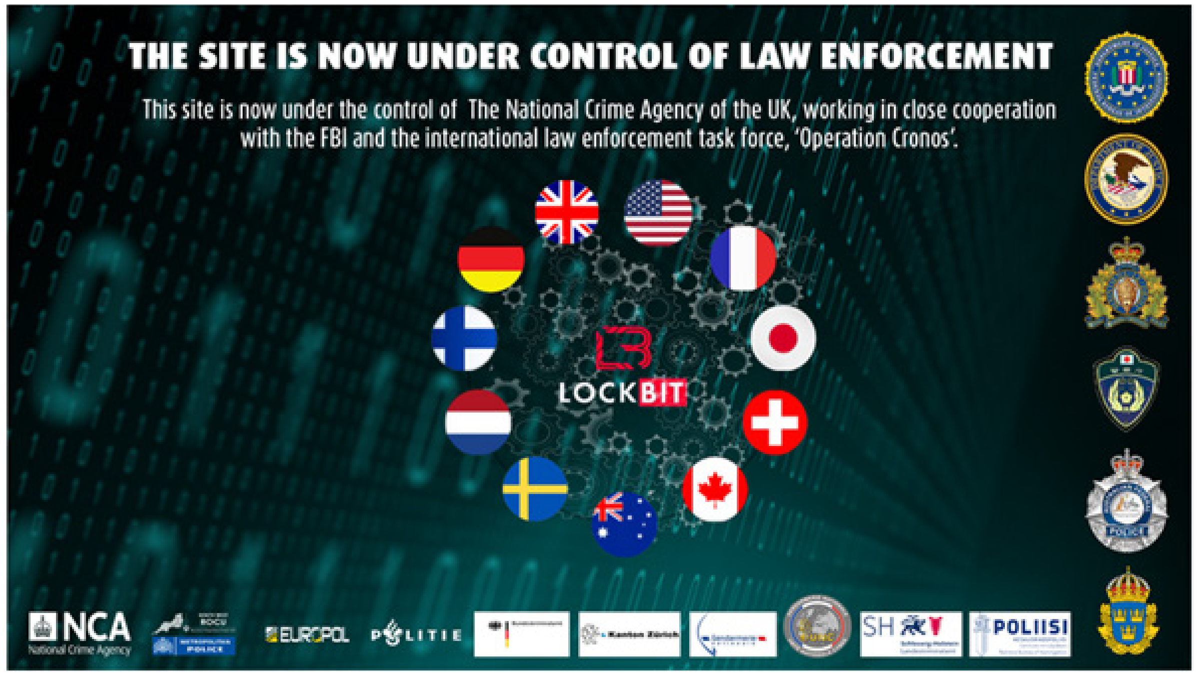
Despite multiple successes in 2024, in the form of arrests, convictions, charges, and infrastructure takedowns, it has sometimes felt like law enforcement are playing a game of whack-a-mole. Disruptions are often temporary, with recently targeted actors re-emerging shortly after.

LockBit

In operation since late 2019, LockBit have already gone through multiple stages of evolution and have proven resilient to law enforcement interventions. In February 2024, the UK's NCA, alongside international partners, conducted Operation Cronos.

This internationally collaborative effort seized control of LockBit's primary administration environment which enabled the group's affiliates to build and conduct their own attacks.

Equally, it targeted LockBit's dark web leak site where they hosted and threatened to publish their victims' information. This was co-opted by the NCA to post information pertaining to LockBit's operations, their source code, and intelligence from their systems regarding their services, affiliates, and past activity.[9]



THE SITE IS NOW UNDER CONTROL OF LAW ENFORCEMENT

This site is now under the control of The National Crime Agency of the UK, working in close cooperation with the FBI and the international law enforcement task force, 'Operation Cronos'.

Figure 9 Notice on LockBit's leak site stating control had been taken by the NCA

LockBit were however back in operation 5 days later, stating that only servers running PHP were lost and backup systems unaffected. The group posted details about their breach and their plans to reinforce their infrastructure to avoid future hacks.

They created a new leak site with a countdown to releasing victim information. LockBit offered up a reward bounty for anybody able to find and report to LockBit, a vulnerability in the latest PHP version. It should be noted that some of the victims posted on their new leak site were previous LockBit victims, leading to speculation that the group was scrambling to 'save face'.[10]

Shortly after the commencement of Operation Cronos in February, LockBit member Mikhail Vasilev was sentenced to four years in prison and ordered to pay $860k in restitution to their Canadian victims. Although arrested in November 2022, it wasn't until February 2024 that he pled guilty to eight criminal charges, including cyber extortion and weapons offenses. The timing of the guilty plea and sentencing was an additional win for law enforcement.[11]

Despite these setbacks, NCC Group reported in the May edition of the Threat Pulse that LockBit was the most active ransomware group, with 176 reported victims.

It should be noted that these figures were obtained from LockBit's dark web leak site and are based off LockBit's own reporting. Given the suspicion that they were artificially inflating their numbers with previously targeted victims, these figures were observed with a degree of scepticism.

May of 2024 saw the UK, US, and Australia join in sanctioning Dmitry Yuryevich Khoroshev, a Russian national and accused leader of LockBit, who operated under the name LockBitSupp.[12] Despite sanctions, there were no arrests, and LockBit continues to be active. The group has shown resilience and adaptability in the past, and it would be unwise to discount them from a revival in the future. In fact, we may observe the group's resurgence in 2025.

A recent warning in December 2024 by the alleged group leader, LockBitSupp, announced the return of LockBit 4.0 in the new year. A dark web post stated that we should anticipate new ransomware activity from February 3rd, 2025. This information is to be taken with a pinch of salt, as LockBit may be looking to maintain its notoriety. The takedown of ransomware groups is nonetheless a constant game of cat and mouse, it would therefore be unsurprising should the group re-emerge under a fourth edition.

ALPHV / BlackCat

ALPHV/BlackCat's dark website was shut down less than two weeks after the NCA disrupted LockBit's infrastructure, with a banner stating it was seized by law enforcement. The NCA, however, stated that it had no connection to BlackCat going offline.[13]

It is likely that this was an exit scam using the smokescreen of law enforcement to cover their tracks, though it is possible that the group was spooked by the disruption of LockBit. Additionally, BlackCat had recently received a payout of over $20 million from Optum, a unit within UnitedHealth's Change Healthcare; it is possible that the group disappeared to avoid sharing the prize with affiliates.[14]

Despite going offline at the start of the year, it appears that ALPHV/BlackCat have returned under a new name, Cicada3301. Cicada3301 has been active since June 2024, only a few months after BlackCat's exit scam. The group shares multiple characteristics with BlackCat, namely that the strain is written in Rust. Cicada3301 is not an exact BlackCat clone, but it is believed that the developers of the Cicada3301 toolset had either seen BlackCat's code base or were the same developers themselves.[15]

Scattered Spider

Scattered Spider experienced a series of arrests in 2024 alike. In November, four US citizens were indicted by the US Justice Department for their roles in Scattered Spider.[16] The charges included conspiracy, aggravated identity theft and conspiracy to commit wire fraud, resulting in up to 25 years of prison time.
The high-profile arrests and charges are said to demonstrate an aggressive response to financial crime, in a continued effort by law enforcement to tackle cybercrime.

This included a 19-year-old Florida man charged with wire fraud and aggravated identity theft earlier in January 2024, as part of a campaign to use SIM-swapping techniques to steal cryptocurrency. The individual was accused of stealing circa £800k from at least 5 victims between August 2022 and March 2023, and of being a member of Scattered Spider.[17] A fifth individual, Tyler Robert Buchanan from Scotland[18] , was also included in the indictments, and arrested earlier in June under suspicion of being the leader of Scattered Spider.

REvil

Possibly the most interesting law enforcement activity of 2024 is the prison sentencing of four REvil ransomware members in Russia. Legal punishment of cybercriminals is exceedingly rare in Russia, a jurisdiction where many feel safe from prosecution and extradition. However, in a rare show of cooperation, Russia's FSB, upon request from American authorities, executed a series of arrests in 2022.

Authorities seized millions in multiple currencies including Rubles, USD, Euros, and cryptocurrency, as well as computer equipment and luxury vehicles.[19] The four members who were sentenced in October 2024, received between 4 to 6 years for their role in the group's malicious activities.[20]

Law Enforcement Impact

Takedowns impact the ransomware landscape by removing or disrupting some of the biggest players. This has a knock-on effect with affiliates moving to work with other RaaS providers, surviving members trying to revive their group, or banding together to form a new threat group. This migration of talent can imbue groups with the skills they may have previously lacked and boost their performance.

Law enforcement interventions against cybercriminals can sometimes feel like a game of whack-a-mole, with defenders and security teams playing catch up to attackers. As evidenced by LockBit's many iterations up to LockBit 3.0, law enforcement interventions are not always permanent fixes.

However, by disrupting the landscape even just for a time, it does serve as a reprieve for organisations which otherwise would have been targeted. There is also the added benefit of law enforcement agencies gaining access to decryption keys through their interventions, which can help existing victims recover their data.

Given so many ransomware groups are in uncooperative jurisdictions, it is difficult to have a lasting impact on specific groups but rather the landscape as a whole. This is achieved by disrupting as many groups and as much infrastructure as possible, and by providing existing victims with decryption keys when they are recovered.

RansomHub have been the most prevalent group each month since July 2024 and, given the scale of their activity when compared to other groups, seem likely to continue in this top spot for the foreseeable future. Being the most active group is a double-edged sword, however, with a target from law enforcement naturally on their back.

Ransomware is also being used by more threat actors than before, including nation-states and hacktivists, as highlighted in the nation-state section below. We expect to see a swathe of new actors emerge onto the ransomware scene in 2025. Equally, nation-states may work with existing ransomware groups, which helps to conceal their activity. Though these groups likely won't supersede groups whose sole focus is ransomware, they do have the potential to shake up the ransomware landscape.

Law enforcement interventions against cyber threat groups are difficult campaigns to set up. They frequently require international collaboration and dedicated investigative work to establish priority targets and identify and compromise crucial infrastructure. Knowing this, it is imperative that organisations do not rely solely on law enforcement to help them defend against threat groups.

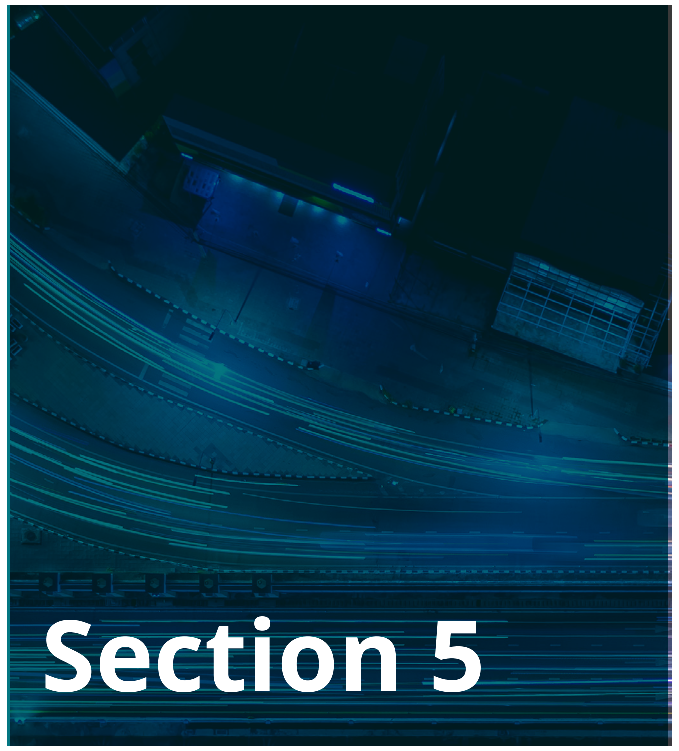
Rather, it is recommended to take charge and pre-emptively secure infrastructure, establish back-ups to minimise damage, and train staff to recognise and respond to threats.

What does this mean for organisations?

For organisations, ongoing takedowns could see ransomware actors update and evolve their tactics, techniques and procedures (TTPs) at a faster rate, to support more effective evasion techniques. The development of existing tactics can aid groups in avoiding detection, rendering group attribution more difficult. If attribution is not possible, then threat actors are likely to avoid arrest. Organisations should anticipate an evolution in attack behaviours, as threat actors naturally will want to avoid legal implications. This could manifest as changes to tactics within existing groups, or the rise of new groups where rebranding completely.

As changes may render the threat landscape increasingly difficult to keep up with, it is pivotal that businesses adopt key cyber security practices within their organisations to ensure a robust defence. Ensuring that basic security fundamentals are upheld will ensure effective defence overall, despite changes to threat actor behaviours. Consistency in their implementation across all areas of the organisation alike will be crucial to minimise risk.

Going forward, businesses should continue to aggressively apply cyber security best practices to ensure their best efforts at protection.



Section 5

What have Nation-States been up to?

Threat actor groups and campaigns tracked as Advanced Persistent Threats (APTs) are typically understood as nation-state-sponsored resources. APTs are typically utilised to progress a country's longer-term strategic interests. Being tied to nation-state motivations and goals, the APT threat landscape is strongly influenced by geopolitical factors.

APT capabilities can support a wide range of nation-state goals including, but not exclusive to:

- Collection of signals intelligence (i.e. compromise of diplomatic communication channels)
- Identification and suppression of domestic opposition (i.e. state surveillance)
- Accelerated progress towards technological or economic goals (i.e. IP theft)
- Undermining competitors (i.e. political and social unrest through influence operations)
- Supporting current or planned kinetic military activity (i.e. hybrid warfare activities).
- Income generation (i.e. theft of financial assets)

Geopolitically, 2024 represents a period of global instability driven by ongoing military conflict in Europe and the Middle East and coincided with significant global election cycles and challenging economic conditions. Domestic and international divisions, often exacerbated by cyber-enabled influence operations, have impacted stability, and further entrenched the perceived divide between US-led 'Western' global systems and ideology, and alternatives presented by Russian and Chinese interests. Global efforts to consolidate support among allies, particularly in the Global South, have intensified. In this environment, an urgency for information and strategic advantage drives increased demand for APT activity, whilst simultaneously the practical impact of their discovery and attribution is reduced by the poor quality of existing relations. Sustained tensions at the current level also drive the accelerated development of cyber-warfare tactics and cyber-enabled preparations for future conflict, as this potential becomes a less unlikely future scenario.

Four nations stand out as being particularly adversarial towards both public and private industry in the West: China, Russia, North Korea, and Iran.

China

Throughout 2024, China has consistently formed a focal point for global geopolitical tensions; including conflict over non-competitive trade practices and the use of tariffs, protectionism towards advanced technology and supply chains, and increasingly confident assessments of China's support of Russia's war in Ukraine.

This year, China's stability has also been undermined by slowing economic growth, Taiwan's election of a President who is publicly defiant towards Beijing, and ongoing challenges to China's maritime claims in the South China Sea. In the final months of 2024, China's presence and tone on the international stage has notably shifted toward demonstrations of its capability as a global leader, particularly around the Global South, coinciding with the power void observed in the interim period before then US President Elect Donald Trump took office.

The following examples of notable cyber activity highlight Chinese APT activities towards mass intelligence gathering and the development of their offensive cyber capabilities.

Chinese APTs of Interest

A series of Chinese APTs, tracked as Volt Typhoon, Salt Typhoon, and Flax Typhoon by Microsoft, have attracted significant attention, following public reporting of their sophisticated campaigns targeting communications and IT infrastructure around the globe.

Whilst not the only reported example, Volt Typhoon's activities have been the primary public source of concern regarding a shift in Chinese activities. Volt Typhoon's observed targeting and behaviour is assessed as inconsistent with traditional espionage, and consistent with pre-positioning in US critical infrastructure. The targeting of US communications infrastructure, including Guam (a US military hub in the Pacific), has been inferred as China seeking to pre-position for disruption and leverage in the event of a crisis in the Asian Pacific region. Severing or impacting American lines of communications, even temporarily, would benefit China tactically and strategically, should they proceed with the stated goal of invading Taiwan.[21,22]

Salt Typhoon's reported compromise of multiple US telecommunications providers, including AT&T, Verizon, and T-Mobile, continues to attract political, media and law enforcement attention. The full impact of the campaign continues to be investigated and reported.[23]

Finally, Flax Typhoon has expanded its usual targeting of Taiwan to global organisations. The group exploits public-facing servers and leverages known vulnerabilities to compromise IoT devices and build botnets which are used for C2 purposes, and which have been observed launching attacks, exfiltrating data, and scanning for additional vulnerabilities.[24]

Targeting of China's Regional Strategic Rivals

Entities and countries affiliated with the Association of Southeast Asian Nations (ASEANS) were targeted for espionage in the run-up to and during the ASEAN-Australian Special Summit in March.[25] Chinese APT Stately Taurus, aka Mustang Panda, created two separate malware packages for the campaign, both of which were re-purposed legitimate packages from reputable publishers.

Delivered via phishing campaigns, the malware was designed to connect to attacker-controlled C2 infrastructure to receive further instructions and to deliver the PUBLOAD malware, a downloader known to be used by Mustang Panda.[26] This campaign helps to highlight the focus China places on regional intelligence gathering to best position China for a wide range of strategic goals; including and not exclusive to their sovereign claims over Taiwan, contested maritime claims in the South China Sea, regional US-influence and military presence and economic competition. Even strategic partners such as Myanmar, which has recently experienced a wave of financial and political support from Beijing, are considered valid targets for intelligence gathering.[27]

APT41

APT41 were observed conducting a global espionage campaign against a range of industries around since at least early 2023.[28] Media and entertainment industry victims were in Asia (focused on Taiwan and Thailand), while all bar one of the shipping and logistics industry victims were located in Europe or the Middle East (mainly UK, Italy, Spain and Turkey). The automotive and technology industries were also targeted. Victims outside of Asia largely represent multinational organisations with operations around the globe, and so the extent of the attacks has the potential to spread beyond the immediate regions of targeting.[29]

This campaign utilised custom tools such as AntsWord and BlueBeam, used for persistence, and a novel tool seen for the first time, DustTrap, used for decrypting malicious payloads.[30] DustTrap is executed in memory to minimise forensic traces, and further obfuscates APT41's malicious activity by using compromised Google Workspace accounts to communicate with APT41 controlled infrastructure, disguising malicious activity with legitimate traffic.[31]

i-SOON

On 16 February, a post was made to GitHub containing approximately 500 documents leaked from Chinese company i-SOON (also known as Anxun). The leak, suspected to have been made by a disgruntled employee, includes documents indicating the conducting of cyber espionage campaigns commissioned by multiple Chinese government agencies against foreign governments[32]; including India, Thailand, Vietnam, South Korea, and NATO countries including the United Kingdom.[33]

This Shanghai-based technology company advertises cyber security training, anti-fraud, blockchain forensics, public security, and enterprise security solutions. The leak provides an insight into Chinese private sector companies acting as an APT-for-hire for the Chinese state. i-SOON, and companies like it, are also encouraged to proactively breach victims in the hope that they can find an interested client.[34] In addition to the military and Ministry of Public Security, leaked content indicates i-Soon also undertook activities for another Chinese cyber security company, Chengdu 404, which have also been assessed as being a façade for APT41.[35] The leak includes tactical insights such as i-SOON's reliance on basic methods like phishing to make up for their difficulty in procuring malware.

Russia

Geopolitical tensions around Russia have remained focused on the continuing war against Ukraine. High losses, Ukrainian incursions into Russia, and signs of economic strain create domestic pressures which drive Putin to demonstrate strong leadership internally. In addition, faced with continued international support of Ukraine and successive relaxing of tactical restrictions, it has been necessary for Russia to aggressively pursue measures to undermine Ukrainian defences, promote instability and division amongst Ukraine's allies, and expand its own support.

The following examples of notable Russian nation-state-sponsored cyber activity highlight how maintaining effective offensive cyber-capabilities in the third year of a military conflict (against highly motivated and increasingly capable defenders) has created the ideal conditions for a dynamic, constantly evolving Russian threat. Hybrid warfare tactics are supported by intelligence collection against Ukraine, NATO members and their supporters.

Broader influence campaigns notably focused on international elections. In contrast to other nation-states, the demands of supporting an active military conflict is inferred to result in the prioritisation of campaigns which have shorter-term (at times more reactive) goals. The involvement of hacktivism on both sides complicates the threat landscape.

Evolving Malware

Now approaching three years of war in Ukraine, Russian APTs appear to have moved away from a reliance on destructive wiper malware: now favouring spearphishing attacks, used to deliver malware, harvest credentials from unwitting victims, and in some cases, extort victims. Agent Tesla, Remos, Smokeloader, Snake Keylogger, and Guloader were found to be some of the most prevalent malware delivered via these phishing campaigns.[36]

Gamareddon

Whilst Russia's Gamareddon remains the most active group in Ukraine, their activity has expanded to include NATO countries friendly to Ukraine, including Bulgaria, Latvia, Lithuania, and Poland.[37,38] This group, believed to operate out of the occupied Crimean Peninsula orders from the Federal Security Service (FSB), primarily attacks government targets and favour spearphishing.[39] In recent years, Gamareddon have improved technically and now largely utilise custom malware.[40] Some of these tools, developed in PowerShell, focus on data theft; from email clients, instant messaging apps such as Telegram and Signal, as well as web apps running within browsers.[41]

APT29

APT29 also evolved their tactics in 2024, leveraging increasing adoption of cloud-based solutions. This approach is well suited to APT29, which has traditionally been known for conducting supply chain attacks, such as 2019's Solar Winds attack. In addition to their traditional method of establishing initial access using phishing campaigns, APT29 have been observed accessing networks using brute force and password spraying attacks. Once initial access has been gained, they have exploited the dormant accounts of former employees not affected by systemwide password resets to establish persistence, as well as using stolen access tokens and exploiting misconfigurations to enrol their own, attacker-controlled, devices in the victim's cloud environments.[42]

Further tactics they have recently adopted include exploiting service accounts and residential proxies. Service accounts are used to run and manage applications and services and, as there is no human involved, can be susceptible to compromise due to their inability to implement MFA.

Depending on the applications or services they're managing, service accounts can hold elevated privileges over other accounts, and so pose a significant threat to an organisation should they become compromised. Residential proxies are used to obfuscate APT29's traffic by making it appear to originate from an IP within ranges used by ISPs for residential broadband customers. This can help negate network defences which are reliant on IP addresses as indicators of compromise.[43]

APT29 have further been spotted reusing iOS and Chrome exploits developed by both NSO Group and Intellexa in a campaign against Mongolian government departments which succeeded in compromising websites for the Mongolian cabinet, as well as Ministry of Foreign Affairs. After compromise, these sites directed users to attacker-controlled sites where CVE-2023-41993, CVE-2024-5274, and CVE-2024-4671 could be exploited. Exploits used in this campaign share the exact same trigger as one previously used by Intellexa, indicating a strong connection between the authors or providers of both exploits. Though currently unclear how APT29 gained knowledge of this exploit, it is possible that they were purchased from the surveillance firms.[44]

Global Elections

One of the biggest focuses for Russian influence operations in 2024 has been global elections: both attempting to influence outcomes and more generally to exacerbate social unrest and political divisions. Russia is accused of creating and spreading videos faked with AI to hurt the presidential campaign of Kamala Harris and her running mate Tim Walz, as well as paying companies millions of dollars to produce pro-Russian content in the run up to the American election.[45] Outside of the American elections, APT28 was observed to have targeted the German Social Democratic Party executive, with APT29 suspected of breaching the email accounts at Microsoft and some of their customers, reportedly including the UK Home Office.[46,47]

Iran

In 2024, geopolitical tensions around Iran have remained focused on its opposition to Israel's military activity against Hamas. Whilst in the background international efforts to slow and prevent Iran's development of nuclear capabilities continue. Historically, Iran has preferred to project power and influence indirectly; relying heavily on influence networks and militia groups across the region, which include Hamas and Hezbollah. In addition to supporting these groups against Israel, Iran made direct attacks against Israel in April and October and has yet to respond to Israel's October retaliation. Iran is understood to have armed both regional militia groups, and Russia against Ukraine. The implications for their weapons stockpiles are not known.

As 2024 ends, Iran's inability/unwillingness to oppose militarily the rapid removal of the Syrian regime is the clearest indicator of how Iran has been weakened by Israel's activities, supported by the US and their allies. Iran is resourceful and highly motivated; declines in their traditional modes of regional influence have coincided with investments in their global relations, for example with Russia and China. This has provided platforms to undermine the narrative of their isolation, and both increase international concerns over Israel's activities in Gaza and undermine the US and their allies.

The following examples of notable Iranian nation-state-sponsored cyber activity highlight how Iran is also embracing their cyber-capabilities tactically and strategically, as an opportunity to overcome the limitations of their more traditional methods of influence.

Initial Access Brokers

Pioneer Kitten has been observed acting as initial access brokers (IABs) for profit-driven ransomware gangs. This is an evolution of previously witnessed behaviour where Iranian TAs sought to monetise their access to victim environments on underground markets, specifically to Russian-speaking OCGs. Now though, they are believed to have been directly collaborating with ransomware affiliates in exchange for a cut of the proceeds for assistance with providing initial access.

Pioneer Kitten is suspected of having collaborated with ransomware groups such as ALPHV/BlackCat, RansomHouse, and NoEscape, and have been observed exploiting CVEs such CVE-2024-3400, as well as older vulnerabilities in Citrix and F5 BIG-IPs, reinforcing the need for organisations to patch and update their hardware, software, and firmware in a timely manner.[48]

Expansion of Targeting

Iranian APTs have continued to target US and Israeli organisations in critical sectors such as energy, finance, and government, both private and public. Since 2023, APT Cotton Sandstorm, also known as Emennet Pasargad, have been developing their tradecraft, including attempts to harvest content from IP cameras in Isreal following October 7th, as well as the use of AI. The group was seen targeting the 2024 Olympics, having compromised a French commercial dynamic display provider.[49]

The FBI has assessed the group's recent activity to include both computer intrusion activity as well as exaggerated or false claims of network accesses or stolen data to amplify the psychological effects of their operations.[50]

Influence Operations

In August, US officials reported that they had observed Iran targeting both the US public and Presidential campaigns with 'increasingly aggressive' influence operations and cyber operations.[51]

OpenAI made additional reporting in relation to attempts to use ChatGPT to create fake content in support of disinformation campaigns attributed to Iranian influence operation tracked as Storm-2035.[52] Google reported phishing campaigns by APT42, which is linked to Iran's Islamic Revolutionary Guard Corps, against a large number of individuals who influence US and Israeli defence and foreign policy. Whilst almost two thirds of known targets were regionally located in Israel and the US, targets within Iran and also the UK were highlighted. Tactically, APT42 abused legitimate services such as Google Drive, Dropbox and OneDrive to host malware, phishing pages, and malicious redirects.[53]

North Korea

North Korea, also known as Democratic People's Republic of Korea (DPRK), have remained focused on their traditional goals of opposing South Korea and the US interests, developing nuclear weapon capabilities, and acquiring illicit funds to achieve these goals.

Since June, these goals came together as North Korea expanded its relationship with Russia. International state visits were followed by the implementation of a mutual defence pact, then the reported deployment of North Korean troops to areas of Russia attacked by Ukrainian forces. Intelligence reporting has provided the international community with increasing confidence that developments have included an exchange of North Korean weapons for Russian advanced technology necessary for the development of nuclear weapons.

The following examples of notable nation-state-sponsored cyber activity highlight how North Korea continue to adapt their techniques and targeting to maintain the flow of illicit funds and information.

Dual objectives of espionage assets

Stonefly, an APT under control of the Reconnaissance General Bureau (RGB), also known as Andariel, Onyx Sleet and APT45, have traditionally focused on espionage campaigns against US interests, and government departments in Taiwan, China, and South Korea. However, recent targeting of US private entities lacking obvious intelligence value has been inferred to represent a shift towards, or additional role in, financially motivated campaigns, potentially ransomware attacks.[54,55]

A joint advisory by the US, UK and Republic of Korea including the FBI, Republic of Korea's National Intelligence Service (NIS) and National Cyber Security Centre (NCSC), issued in July, highlights that despite the above reported activity, the group remains a significant global espionage threat to sectors including defence, aerospace, nuclear and engineering. It reports that the campaign seeks to obtain 'sensitive and classified technical information and intellectual property to advance the regime's military and nuclear programs and ambitions'.[56]

The group is known to gain initial access through spear phishing campaigns and the exploitation of known vulnerabilities, and once in, use established system discovery and enumeration techniques, before establishing persistence by deploying webshells and scheduled tasks. The group uses a mix of publicly available tools as well as modified and custom malware.[57]

Insider Threat

2024 has seen regular reporting in relation to US and US-allied based companies, with IT professionals who have subsequently been identified as covert North Korean assets posing as western remote workers. Whilst employed, these assets are reported to have been involved in data extraction and espionage activities. On discovery, the companies have been subjected to extortion over breached data. The salaries of these assets and ransom payments are suspected to be another means by which the North Korean regime acquire illicit funds.[58,59,60]

Looking Ahead

Likely in response to the shifting and volatile geopolitical landscape, 2024 has been a year of evolution for APTs from all the above nations. Looking forward into 2025 this trend is expected to continue, with the following themes capable of driving new trends.

Inauguration of US President-Elect Donald Trump

Whilst Donald Trump is almost defined by his unpredictability, significant domestic, foreign and defence policy changes in the US are anticipated during his second term in office, beginning on 20th January.

Nation-state activity in 2025 will be heavily influenced by his administration's stance towards the Russia-Ukraine conflict, Israel, China (over their economic activities and Taiwan), North Korea and Iran's nuclear weapons ambitions, and most recently, regime change in Syria. Trump's less ideologically driven approach provides an opportunity for Russia and China to benefit from a more transactional approach towards Ukraine and Taiwan. Whilst an anticipated aggressive stance on trade and tariffs risk exacerbating tensions linked to the global economy and relations with China more generally.

Perceived acts of aggression towards US interests risk triggering impulsive retaliatory responses; for Russia in particular, this may drive a trend towards reduced targeting of US entities and an increased focus on European and Asian-Pacific regions. For China in particular, who place such value on gaining advantage through intelligence gathering, increasing demand for cyber-espionage activities should be expected as we enter this new geopolitical chapter.

Pressures to End the War in Ukraine

Ukraine, Russia, NATO, and European countries start 2025 preparing for the potential scenario of the US leveraging its resources and influence to force an end to the Russia-Ukraine conflict, prioritising speed over geopolitical security. The interim period is likely to continue the current trend of increased intensity whilst both sides seek to secure as many gains as possible in anticipation of the need to leverage all their advantages in future peace negotiations.

The realities of these pressures risk unintended escalations towards the worst-case scenarios of the use of nuclear weapons and widening of the conflict, triggering a direct NATO response.

Under these pressures, Russian APT activities (offensive, intelligence focused or influence-driven) are anticipated to occur at capacity levels, and potentially be expanded by financially motivated cyber-crime groups. Multiple recent reports of Russian cyber-crime enforcement activity would be consistent with a play book Putin has used historically against Russian oligarchs; to compel control of their activities (and profits).

Chinese Opportunities for Taiwan

Chinese APTs, with the pressure of President Xi's desired 2027 date for a Taiwan invasion, are likely to continue targeting critical infrastructure of American and adversarial Pacific nations, particularly with pre-positioning attacks to exploit network access in the event of crises and not for immediate goals. Any perceived lack of commitment of the Trump administration to intervening in Taiwan, has the potential to incentivise China to accelerate their plans and/or test boundaries. Aggressive cyber- espionage activity towards US government (and those of their allies and influencers) involvement in regional foreign and defence policy would be expected to be at increased risk.

The Impact of Regime Change in Syria

The rebel offensive which led to Syrian President Bashar al-Assad being provided with sanctuary in Russia, whilst rebel forces took control of the government and expanded their control of the country, has triggered a regional geopolitical shift. Iran and Russia's failure to intervene provides an indication of the impact of Russia's continued war in Ukraine, and Israel's military response to Hamas' attack over the last 14 months.

Coming out of a 13-year civil war, which occurred in the context of over 50 years of violent oppression by the Assad family, delivering stability within the country will be a significant and long-term challenge.
The challenge will be increased by the strategic value Syria plays both regionally and globally, and the interference from domestic and external forces which should be anticipated. Particularly for Russia and Iran, who will seek to minimise the strategic losses incurred, expansion and development of their cyber-capabilities is an obvious means by which they can attempt to continue to pursue their strategic goals through increasingly limited means.

Iran will face domestic and international pressures to respond in ways which range from ensuring their survival through achievement of a nuclear deterrent, to attempting a reset of its foreign relations through diplomacy and nuclear decommissioning. Cyber-capabilities can be expected to form a key part of the current regime's strategy to suppress domestic opposition and the risk of Syrian events inspiring an Iranian uprising, and to use espionage and offensive cyber-capabilities to strengthen its current position. Disruption to Iran's abilities to support its proxies, Hamas and Hezbollah, has the potential to lead to a transfer of knowledge and skills for its cyber-capabilities from Iran, potentially in collaboration with Russia, and even China.

Section 6

Key Thematic Research Areas 2024

Throughout 2024, we focused on digging deeper into the emerging cyber security trends impacting the threat landscape. Our focus in Q2 (April to June) was artificial intelligence (AI), followed by misinformation, disinformation and malinformation in Q3 (July to September). The themes remain prominent to the cyber security conversation, with AI continuously developing and information validity an ongoing concern.

Artificial Intelligence (AI)

AI continues to evolve with the introduction of generative tools such as ChatGPT, CoPilot, Adobe Firefly, Google Gemini and MetaGPT skyrocketing the public interest into what AI can and cannot do. Equally, an interest in how this can be leveraged by malicious cyber adversaries and defensive security teams is evident.

As a brief reminder, AI develops methods for computers to execute tasks typically associated with human intelligence, including data analysis, pattern and behaviour identification, or making recommendations. Machine Learning (ML) is a notable subset of AI which permits machines to extract knowledge from data and learn from the insights to make its own decisions.

Defensive and Malicious Use of AI

Both defenders and malicious threat actors see AI as a powerful tool that can be used in various ways to facilitate achieving specific tasks and goals. From a defender's point of view, AI can automate and speed up the threat detection and analysis process by removing the need to manually update the rulesets based on previous findings, as it can learn from its own experience and update continuously. This results in fewer missed true positives or incorrectly raised false positives but also reduces "alert fatigue", when an analyst misses a true positive due to faltering focus. Overall, if a human operator is required, they are more likely to make better decisions.

The various ways in which threat actors could use AI are captured below:

- Craft a more convincing phishing email
- Facilitate writing malware packages
- Enable malicious network scanning
- Launch BEC campaigns
- Impersonate an individual's voice using deep fakes which can then be used to launch vishing attacks

NCC Group's Threat Intelligence Team explored how AI used by cybercriminals can bring risks as well as advantages to the criminal scene. Notably, AI's ability to streamline existing operations could lead to greater operational efficiency, reduced operational costs, and a potential for larger financial gains for threat actors. However, the use of AI simultaneously introduces complexities, potential pitfalls, and a rather steep learning curve for the average beginner. The development and deployment of truly AI-driven operations and attacks still requires a high level of expertise and resources which may not be achievable for an entry level attacker.

Most use cases observed thus far have predominantly built on existing techniques by enhancing them through greater speed and precision than a human operator would be able to achieve.

It is important to note that while the benefits of utilising AI to achieve threat actors' goals and objectives quickly and efficiently might seem great at face value, the complexity it introduces through cost, time, and expertise needed will impact which threat actors are able to truly benefit from AI in the future. Subsequently, this could impact the overall availability and reliance on AI-driven tools during attack planning and attack execution as well as the number of attacks in which AI is successfully utilised.

AI-powered Malware

This year, we also considered advances in AI-powered malware which relies on machine learning techniques to improve its sophistication and continuously learn from its surroundings. Such adaptability in real-time makes it more difficult to predict and prevent future attacks. AI-powered malware would be able to avoid traditional signature-based detection techniques by mimicking regular network traffic patterns or legitimate program behaviour.

We reviewed the Moris Worm II as an example, which was developed by researchers to exploit vulnerabilities in AI-enabled systems, such as ChatGPT, Gemini Pro, LLaVa. The worm can replicate, propagate and perform malicious activity related to spamming and exfiltrating personal data. Functions included data exfiltration from emails and flooding users with spam, and the ability to craft convincing phishing emails. The research highlights how AI-powered malware could present a threat in the future as malicious cyber adversaries could, depending on their sophistication, create worms of such capability alike.

NCC Group's AI/ML Security Testing Offerings

NCC Group uses AI to support clients in identifying security weaknesses as well as enhancing their cyber security posture. We have captured below how NCC Group can support clients with the following offerings:

- Red Teaming (Penetration Testing) – aim to evaluate the resilience of the client's AI/ML components, helping to safeguard them against cyber threats, with a focus on examining data integrity, model reliability, and resistance to adversarial attacks in AI systems. This intelligence-led approach provides visibility into how the client's defences perform against real world scenarios, without the added consequences of legitimate targeting.

- Secure Development Lifecycle Testing (SDL) – NCC Group experts work alongside the client to analyse the existing SDL policies and processes and how these relate to AI/ML alongside reviewing the AI/ML pipeline. This could translate to application code review, DevOps security assessments, or custom consulting to fit the client's specific needs.
- AI/ML Threat Modelling – NCC Group's security consultants work alongside the subject matter experts (SMEs) in the client's organisation to collaborate on a range of offerings including, but not limited to, application attack surface analyses, application threat modelling, and application security architecture reviews to ensure the application's security. This enables NCC consultants to gain an intimate understanding of the client's unique security landscape and provide bespoke recommendations to strengthen their security defences and minimise any potential impact from the cyber threats they may be exposed to.

Use of AI in Threat Intelligence

There has been a lot said on the use of AI by malicious actors to exploit companies and individuals. The discussion of how AI can be leveraged in a meaningful way to enhance threat intelligence is notably sparser. It is not arguable that AI is powerful; it is an excellent replacement for a human in many repeatable and well-defined tasks. However, what is arguable is the suitability of AI in a multitude of other cases. The rising popularity of LLMs and renewed public interest has driven a global increase in the number of "AI-powered" solutions, many of which claim to hold the secret for detecting and stopping emerging threats. How can they do this?

In any successful AI integration, the primary aim is to reduce human involvement, while staying accurate and increasing the value that can be gained from operation at scale. It is good when humans can't do a task either, due to a limitation of brain power or social collaboration. It is less good when identifying or investigating known unknowns and unknown unknowns. AI can only respond to what it knows, it cannot address novelty in the meaningful way threat intelligence needs it to. In such cases, AI can be a hindrance more than a help.

LLMs (think ChatGPT and LLAMA) can help immensely with:

- Summarisations - large numbers of reports can be fed about a particular threat actor and LLMs will either be far better than humans at summarising it, or they will hallucinate. It can be difficult to tell when it is hallucinating.
- Retrieval Augmented Generation - by augmenting what an LLM knows with proprietary knowledge, it can respond to user queries and reference specific knowledge in the process (you can think of a chat bot which can answer questions about a meeting or document content by giving it access to the recording or document).
- Named Entity Recognition - LLMs perform well at identifying named entities (e.g. USA, NCC Group PLC, Stuxnet, and Black Basta) from text, allowing analysts to quickly extract them from large reports.
- Extracting relationships - LLMs can also extract relationships between these entities and can extract them into structured formats such as STIX, which machines can read and process at scale.

One example would be an LLM which can extract the MITRE ATT&CK TTPs associated with a particular threat actor in a set of reports and summarise this alongside a STIX representation of the information.

The field of AI, however, is wider than just LLMs. In many cases, an LLM may not be suitable at all, since they are expensive to train and are prone to hallucinations. Hallucinations are a huge problem in threat intelligence, since the credibility of the information being shared is of the upmost importance. In many cases, the integration of other AI methods can prove more successful for well-defined tasks. Natural language generation, for example, is well-established and less error-prone than LLMs, but when integrated into document templates with pre-defined structures, it can be used to rapidly produce real-time intelligence from machine-readable formats such as STIX and MISP. This can be used to produce (for example) real-time threat actor profiles from the latest intelligence, or incident executive summaries from a timeline stored in a case-handling system.

Other areas of AI out-perform LLMs often in their defined domains:

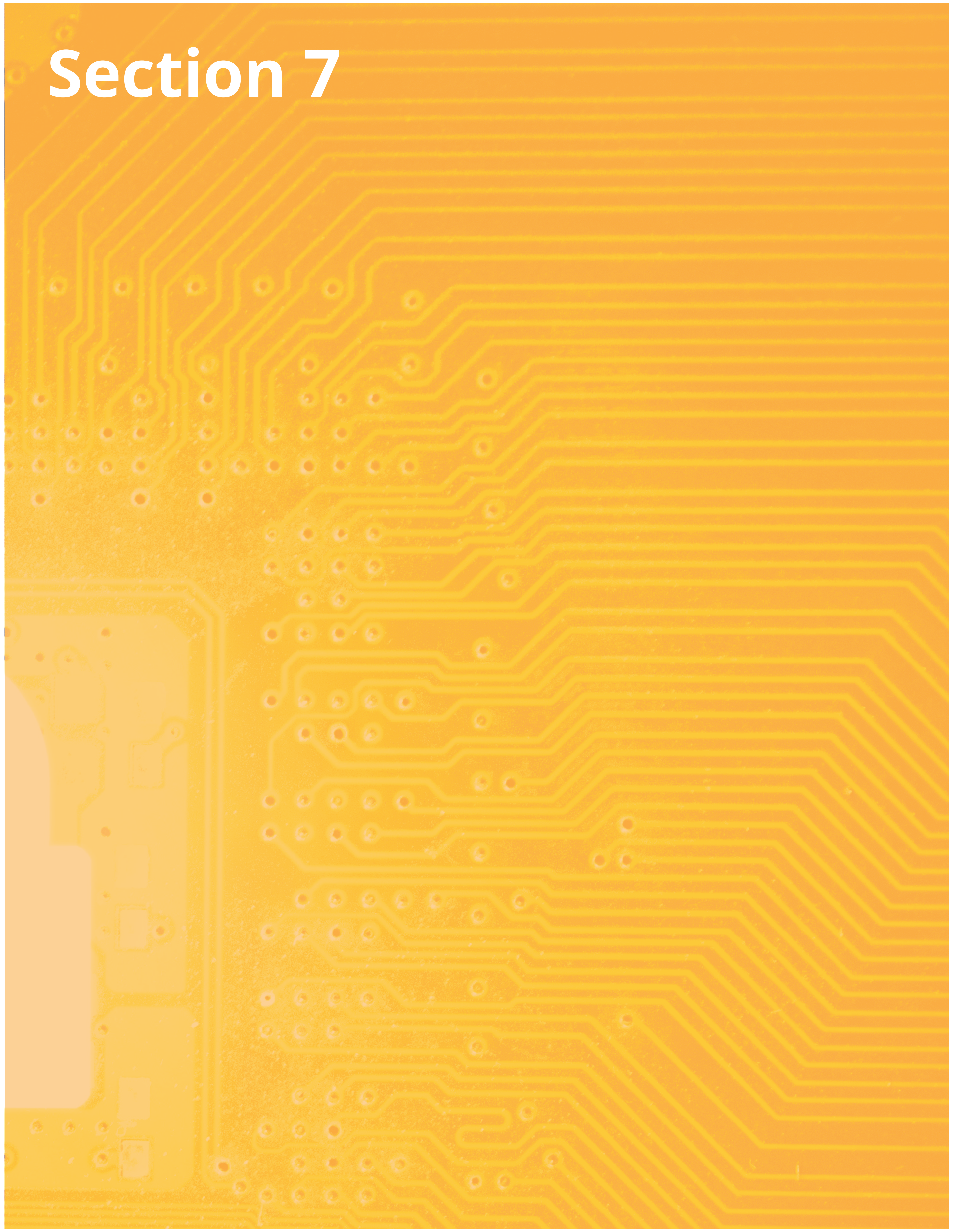
- Named entity recognition
- Pattern recognition in machine-readable data
- Data and event classification
- Activity clustering

In all cases, AI is a support tool. It is widely feared that AI will replace threat intelligence analysts and consultants. This is unlikely to be true, but a human with AI will. Using it in the correct way, with purpose and deliberate effort, can give organisations a step up, putting them ahead of threat actors in a meaningful way.

Future Considerations AI

As outlined throughout Q2, AI can be used offensively and defensively in cyber security and has the potential to significantly enhance capabilities on both sides of the spectrum. Defenders using AI-driven tools and techniques can achieve better decision making via enhanced threat detection and analysis, while also reducing the alert fatigue. From an offensive perspective, cyber adversaries can benefit from streamlined operations and reduced costs, however, they may require resources and time which may not be available to a novice attacker.

As AI is ever evolving, it is highly likely that we will observe further advances as well as increased sophistication in both defensive and offensive applications. This makes it crucial for organisations to remain well informed and ensure a proactive cyber security approach.



Section 7

Misinformation, Disinformation and Malinformation

Threat actors have significantly increased their efforts in misinformation, disinformation, and malinformation to conduct influence operation campaigns, which are often aligned with strategic geopolitical interests. In 2024, these themes were of growing interest, and more so as multiple global events from the year, notably the Olympic Games and global elections, fortified potential threats from these three categories.

From July through to September, we captured the theme of misinformation, disinformation, and malinformation. This focused in-depth on the three types of false or misleading information which can not only negatively impact individuals, groups, organisations, and countries, but can be utilised by threat actors maliciously. Below is a brief reminder of what each term represents:

- Misinformation - false information, which is not intended to cause harm.
- Disinformation - false information which is deliberately created and circulate to cause harm or manipulate.
- Malinformation - information which is used out of context or selectively to cause harm or manipulate.

Olympic Games

Developments in AI and the extensive use of social media have helped to drive improvements in the output of malicious actors, such as increasing the plausibility and persuasiveness of their misinformation and disinformation campaigns. Additionally, social media is consumed by a diverse audience of all ages, meaning that information is reaching a much broader cross section of the population. In 2024, we saw malicious cyber adversaries conduct online influence campaigns to sway opinions relating to global elections and the Olympic Games.

Regarding the Olympics, the Russian state was highly critical, likely as a response to the participation ban imposed on their athletes due to Russia's 2022 invasion of Ukraine. Some of the malicious activity observed in 2024 included:

- A film titled "Olympics Has Fallen", attributed to the Russian-sponsored group, Storm-1679. The film's plot provides a negative critique of the International Olympics Committee (IOC) leadership team.[61]
- A disinformation campaign aiming to undermine France. A video went viral featuring an actor appearing as French President Emmanuel Macron, portraying Paris as filthy, dirty, rubbish-strewn and overrun with rats.[62]

This highlighted how large-scale sporting events, such as the Olympics, provide malicious actors with both a global audience and the opportunity to engage in high-stake disinformation campaigns, while the world is watching. Having a substantial audience ensures maximum exposure to encourage disorder and fear around the event through influence operations. Thus, putting the security of such events at risk now and in the future.

Global Elections and the Malicious focus on the US Election

2024 was also an important year for global elections with almost half the global population participating in general and state elections across 50+ countries.[63] Some of these included the European Elections for MEPs in June 2024, the UK General Election in July 2024, and most recently the US Presidential Election in November 2024.

As elections encourage and require healthy debate, this also created the opportunity for malicious cyber adversaries to influence the public's opinion in line with their own strategic objectives. Disinformation campaigns, for example, could confuse voters about the overall voting process, requirements, or even the value of casting your vote at all and could suppress voter turnout. Some of the disinformation cases that have been observed throughout the US election include:

- Aiming to reinstate Putin's friend[64] and ally, Trump. The democratic party was maligned, and vice-president Kamala Harris also denigrated. Existing divisive issues, such as immigration, were reinvigorated.[65]
- In September 2024, the DOJ seized 32 internet domains associated with the Russian disinformation campaign, known as 'Doppelganger'.[66] The companies were urged by Putin to use tactics such as cybersquatting, fabricated influencers, and fake profiles on social media, to promote their false narratives, using generative AI as the means to fabricate content.
- On 27th September 2024, three Iranian nationals were charged with material support for terrorism, computer fraud, wire fraud and identity theft, for hacking into the campaign of an unnamed presidential candidate. However, it was indicated that it was Trump's campaign, with emails and documents leaked to the media.[67]

UK Riots

In light of the UK riots, which originated in Southport and took place in July 2024, we discussed the impact of misinformation, disinformation, and malinformation in the context of cyberterrorism. At the core of the unrest was the reignition of existing tensions in the UK around asylum seekers, immigration, and islamophobia, with online channels quickly being flooded with disinformation and misinformation.

The spread of disinformation represents a move from cybercrime towards cyber-enabled crime, as we have witnessed online disinformation influence offline harm. The Southport riots serve as an example on how information online can fuel offline behaviours, which could have dangerous and violent outcomes. Overall, such events serve as a reminder to always ensure the validity of information. For the public, it is important to consume information critically, especially when dealing with sensitive information.

Mitigations and Recommendations

Recommendations to limit the impact of misinformation, disinformation, and malinformation include:

- Easy access to facts, to allow the public to check information and form their own opinion. Platforms such as USAFacts provide facts and statistics regarding the federal budget, immigration, healthcare, and the environment, to present accurate information from which to make informed voting decisions.
- Training election workers to recognise and handle AI-generated content and deepfakes.
- As generative AI and targeted social media campaigns make it easier for disinformation to spread at large scale, affecting voters across the political spectrum, providing voters with access to unbiased facts and reliable news sources would help to preserve the integrity of the electoral process.

Future Considerations

Having observed how the spread of disinformation and misinformation has intensified during 2024, we are confident that similar global events will continue to draw the attention of malicious adversaries. Advances in AI have increased threat actors' ability to produce credible content more efficiently and make their campaigns more believable. Audiences consuming the material are unable to easily distinguish between tampered and real information. Furthermore, large-scale events capture a substantial audience, and this provides malicious actors with the opportunity to propagate their message with maximum exposure. Heading into 2025, we should remain vigilant to potential influence campaigns and look to consume information critically.

Section 8

Vulnerability Threat Landscape

The exploitation of vulnerabilities is one of the most frequently used initial access vectors for threat actors. In this section, we review some of the vulnerabilities exploited on a mass scale in 2024, helping readers to gain insights into the vulnerability threat landscape from the last 12 months, and supporting them to better understand and anticipate likely threats.

NCC Group predicted that the number of vulnerability disclosures would continue to rise year on year, due to the increase in BugBounty initiatives, as well as changes in vulnerability disclosure processes, leading to a potential increase in exploitation as a result.[68] Generative AI was predicted to enhance the capabilities of malicious actors, whilst inefficient patch management programmes amongst many organisations would allow these same actors to exploit historic vulnerabilities.

Vulnerability Disclosure Counts Increase in 2024

This forecasted trend has been borne out by the number of vulnerabilities disclosed in 2024, with 40,287 reported for 2024, compared with 29,066 in 2023, an increase of 11,221.[69]

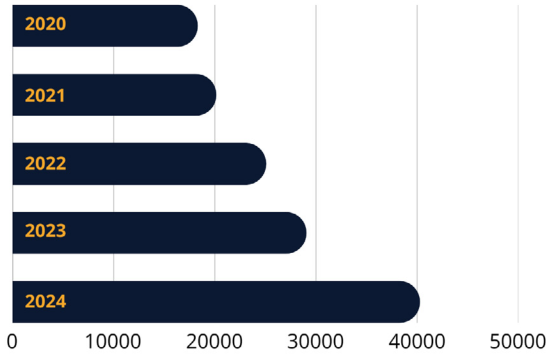


Figure 10 Vulnerability disclosure by year 2020-2024

A review of the number of reported Common Vulnerabilities and Exposures (CVEs) from the start of 2024 until mid-July 2024 by Qualys found that 0.91% of disclosed vulnerabilities had been weaponised and exploited in the wild.[70] This is an increase on the 0.77% of vulnerabilities seen weaponised or exploited last year, but illustrates the small number of CVEs which are known to be exploited. Furthermore, it is also this small proportion which is the most dangerous, and those which organisations should be aware of and take steps to protect themselves from. In addition, there is increasing evidence that it is taking threat actors increasingly shorter time from discovering vulnerabilities to exploitation.

Zero-days become more prevalent

Zero-days are becoming more prevalent. In 2023, Mandiant suggested that 70% of the exploited vulnerabilities they interrogated were leveraged as zero-days, and 30% were n-days, which are vulnerabilities first exploited after patches are released.[71] The UK's National Cyber Security Centre (NCSC) and international partners backs up these findings, suggesting more zero-days were exploited in 2023 than in 2022, suggesting an increase. In 2024, this remained to be true, with an increased use of zero-days.[72]

Time-to-Exploit sharply decreasing time for remediation

In addition to the increased zero-day usage in widely exploited vulnerabilities in 2023, the average Time-to-Exploit (TTE), defined as the average time it takes threat actors to exploit a vulnerability before or after a patch is available, has fallen significantly. In 2018-2019, the average TTE was 63 days, 32 days in 2021-2022 and in 2023, this dropped to an average of 5 days.[73] Rapid 7 has tracked TTE since 2020 and has noted a similar trend in declining timeframe between vulnerabilities becoming publicly know, and exploitation.[74]

The average TTE is 22 days, but the median is just one day, for all CVEs they considered between 2020 up to February 2024. Forecasts suggested that this would be the same in 2024 and potentially increase to even faster exploitation times in 2025, according to Mandiant.[75] Whilst these figures represent averages, it does point to a shifting landscape for organisations with regards to vulnerability management, requiring ever faster reaction to help mitigate vulnerabilities.

Researchers have indicated that mass exploitation is now the primary attack vector for ransomware and nation-state threat actors pursuing espionage.[76]

This is speculated to be due to the prevalence of vulnerable edge devices, or the increased instance of mass exploitation.[77] Exploited network edge devices as the source of mass exploitation events almost doubled in 2023, with network perimeter technologies exploited in 36% of the widely exploited vulnerabilities, according to Rapid 7. Attackers target these devices and services as they are accessible online and make for good initial access points. Whilst similar figures for 2024 are not available, indications so far suggest that vulnerable edge devices continue to be increasingly part of the reason for increased numbers of mass exploitation events in 2024.[78]

Defining Mass Exploitation

This vulnerability report aims to highlight some of the CVEs disclosed in 2024 which were known to be widely exploited. We consider mass exploitation as those vulnerabilities which affect many different types of organisations globally, impacting different sectors and locations. 2023 saw more mass compromise events arising from zero-days than from n-days.[79]

From 2023 and into early 2024, 53% of new widespread vulnerabilities were zero-days, compared with 43% in 2022, according to Rapid 7's 2024 Attack Intelligence report.[80] The report also states that they have seen a change in attacker behaviour, whereby widely exploited vulnerabilities were exploited by many attackers making multiple exploitation attempts at many targets. Increasingly, mass compromise events stemmed from single attackers executing complex zero-day attacks.

This would indicate that we should include vulnerabilities exploited by single threat actors as well those exploited by many.

Quantifying Mass Exploitation

How do we know which have been widely exploited? CISA publishes details of vulnerabilities that are known to have been exploited or are being actively exploited in the wild, in its Known Exploited Vulnerabilities (KEV) database.[81] Here, active exploitation is defined as: 'a vulnerability under active exploitation is one for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner.'

This will not encompass all exploited vulnerabilities; however, to be included in this list, vulnerabilities must have an assigned CVE ID, be under active exploitation, and have clear and actionable remediation advice available to organisations.

For 2024, the counts of vulnerabilities captured in the KEV database comes to 185.[82] Research by BitSight found that in 2023, 35.3% of 1 million global organisations they reviewed had a CVE listed in KEV, meaning that over a third of these organisations had a vulnerability known to be exploited by threat actors.[83]

Almost 25% had 5+ and 10% had more than 10 of the vulnerabilities in KEV, which highlights the prevalence of these exploited vulnerabilities globally, and the need for defenders to prioritise vulnerability management.[84] This is particularly pertinent as the same research indicates that for vulnerabilities listed in KEV, these are addressed within 6 months on average, whilst those not in KEV take an average of 1.7 years.

Details of CVEs widely exploited in 2024

Ivanti Connect Secure and Policy Secure Gateways

In February 2024, CISA raised an alert related to Ivanti Connect Secure and Policy Secure Gateways, warning of its mass exploitation by threat actors.[85] Ivanti had disclosed two zero-day vulnerabilities in their Connect Secure VPN gateway appliances, CVE-2023-46805 and CVE-2022-21887.[86] Exploitation of these could lead to authentication bypass and command injection, with subsequent compromise of victim networks. An estimate from Volexity suggests that 1,700 compromised, indiscriminately targeted, Ivanti Secure VPN devices had been discovered globally.[87] In addition, they report that their victims varied greatly in size and spanned the globe and covered many industrial verticals including governments, telecommunication companies and defence contractors. Multiple threat actors were seen to attempt exploitation. The same month, two more vulnerabilities affecting Ivanti Connect Secure and Policy Secure gateways were disclosed, CVE-2024-21888 and CVE-2024-21893, a server-side request forgery (SSRF), which Mandiant revealed had been exploited by a China-nexus espionage driven adversary.

Flaws in JetBrains' TeamCity

CVE-2024-27198 and CVE-2024-27199 flaws in JetBrains' TeamCity are both authentication bypass vulnerabilities in its web component, announced in March 2024.[88] CVE-2024-27198 allows remote unauthenticated attackers to entirely compromise vulnerable TeamCity servers. DarkTrace estimates that 30,000 organisations globally use TeamCity for automation, build testing and deployment processes for software projects.[89]

There was also evidence that this vulnerability was being exploited by ransomware groups and shortly after disclosure, there were attacks on several organisations in the financial sector. CrowdStrike also tracked multiple instances of exploitation, as did ShadowServer, and one estimate suggested that there were 1,700 exposed TeamCity instances of which 1,442 showed evidence of attempted exploitation.[90]

Cisco Firewall

The UK's National Cyber Security Centre (NCSC) issued an advisory in April 2024, warning organisations of the active exploitation of vulnerabilities in Cisco Firewall platforms running Adaptive Security Appliance (ASA) Software or Cisco Firepower Threat Defense (FTD) software.[91] A response from Cisco indicated that attacks targeting these devices were intended to implant malware, execute commands and potentially exfiltrate sensitive data from compromised devices.[92] CVE-2024-20353 and CVE-2024-20359 had been exploited by threat actors targeting government and critical national infrastructure worldwide.[93]

ConnectWise

Vulnerabilities CVE-2024-1708 and CVE-2024-1709 were disclosed in February 2024, by ConnectWise relating to their ScreenConnect remote desktop including on-premise customers.[94] CVE-2024-1798 is a path traversal vulnerability and CVE-2024-1709 is an authentication bypass flaw, which could be exploited by threat actors to gain remote access to more than 10,000 servers controlling 100,000s of endpoints, according to one estimate.[95] Also suggested was that Initial Access Brokers (IABs) were commoditising these vulnerabilities, gaining access to be sold on to give access to ransomware groups. The ShadowServer Foundation saw evidence of 643 IPs being attacked at the time of reporting in February 2024.[96]

Palo Alto's PAN-OS

The GlobalProtect feature of Palo Alto's PAN-OS was identified as having an unauthenticated remote code execution vulnerability in April 2024, which allows an attacker to execute code with root privileges on the firewall.[97] CVE-2024-3400 started as a zero-day exploit, which it suspected was being exploited by a nation-state threat actor, who was moving through victim networks, stealing sensitive credentials and files.[98] Censys estimates suggest 143,000+ GlobalProtect publicly-facing devices worldwide, which gives an indication of the potential scale of the opportunity for threat actors.[99]

Fortinet FortiManager

CVE-2024-47575[100], a missing authentication flaw in Fortinet FortiManager was disclosed in October 2024. This flaw allows for an unauthorised remote threat actor using a compromised device to execute arbitrary code or commands on other FortiManager devices.[101] They could then gain access to sensitive files or take control of the affected system.[102] Mandiant was part of the investigative team and revealed that there had been evidence of mass exploitation, as 50+ devices had been compromised across various industries.[103]

Older CVEs will Continue to be Exploited

Older vulnerabilities were also weaponised in 2024, which is not unusual, but has been seen to be used to a greater extent, with over 10% of CVEs identified prior to 2024 being weaponised, according to Qualys' research.[104]

Whilst this review is to consider vulnerabilities under mass exploitation in 2024, it is worth remembering that older vulnerabilities remain an ongoing threat, particularly those affecting remote services and public-facing applications. Thus, this has served as a reminder for defenders to stay abreast of patching vulnerabilities, both new and old.

Threat Intelligence Alert Subscription

NCC group provide a regular Threat Intelligence Alerting Service, which provides customers with details of emerging threats, including critical vulnerabilities being actively exploited. The aim of these alerts is to furnish our customer base with intelligence to allow for situational awareness and prompt patching prioritisation and mitigation activities. This is available as part of our NCC Group MXDR Services or by subscribing to our Threat Intelligence Services.

Section 9

NCC Group Customer Impact: Unravelling the Breach 2024

One of the most effective ways to understand the dynamic threat landscape is to look internally at our security operations services that identify, alert, and respond to suspicious activity. This concerns NCC Group's Security Operations Centre (SOC) team, as well as our Digital Forensics and Incident Response (DFIR) services, who deal directly with our client base and thus can provide an evidenced-based understanding of attacks from 2024.

The below case studies present an ever-dynamic threat landscape characterised by varying attack types. These examples also reflect some of the attacks repeatedly highlighted as a threat to organisations, such as phishing, the exploitation of zero-day CVEs, and ransomware, thus re-affirming their existence and relentless nature.

In addition, these case studies provide insight into how the SOC, DFIR, and NCC Group as a whole, are able to support our customers with incident readiness, response management and response recovery throughout 2024.

Managed Extended Detection and Response

Throughout 2024, NCC Group's SOC service monitored the security of NCC Group's clients, identifying, alerting and responding to suspicious activity. Enriched with Threat Intelligence, in collaboration with Incident Response, the SOC delivered a robust security monitoring program to defend against malicious activity. This year, we are including case studies to illustrate real-world scenarios of cyber threats and applicable solutions.

Case #1: SocGholish Infection Resulting in Lateral Movement and Multi-User, Multi-Host Compromise

The NCC Group's SOC responded to multiple alerts indicating a SocGholish malware infection. The initial access vector was identified as a malicious Update.js file, which was downloaded by a user, likely as part of a fraudulent software update scheme. Following the initial compromise, the threat actor leveraged the infection to execute lateral movement within the network, resulting in the compromise of multiple user accounts and host systems.

Based on the analysis conducted by the NCC Group's SOC, the attack was attributed to SocGholish malware. Key indicators supporting this conclusion include:

- Malware Artifacts: The infection involved the deployment of the well-known Update.js file, a signature component commonly associated with SocGholish campaigns.
- Behavioural Analysis: Observed commands demonstrated patterns of Python script execution, aligning with publicly documented SocGholish activity.
- Persistence Techniques: The infection leveraged persistence mechanisms consistent with known SocGholish tactics, further corroborating its attribution.

A comprehensive investigation was undertaken in collaboration with the NCC DFIR team and the client to address the incident. Compromised hosts were isolated and affected user accounts were disabled to prevent further unauthorised activity.

The client was promptly contacted, and they confirmed that the activity was indeed malicious. As part of the remediation process, the identified malicious files were added to Microsoft Defender's block list, and persistence mechanisms implemented by the threat actor were removed from the affected hosts. IP addresses associated with the threat actor's C2 communication and remote access activities were blocked in Microsoft Defender. Furthermore, the client was advised to apply similar blocks on their network devices. These measures ensured effective containment and threat mitigation while DFIR conducted their investigation.

The incident, although detected, could have been identified earlier in the cyber kill chain to minimise potential impact. Mitigating actions were promptly implemented on the affected hosts and user accounts, significantly reducing the risk of the malware and threat actor causing further damage. Following the investigation conducted by DFIR, it was recommended that the client rebuild the compromised hosts and proceed in alignment with DFIR's guidance.

Collaboration with the detection engineering team resulted in the creation and deployment of enhanced detection rules designed to identify the initial SocGholish infection, the observed Python commands and activity, and the lateral movement tactics employed by the threat actor. These improvements aim to bolster the NCC Group SOC detection and response against similar threats in the future.

Case #2: Compromised Student VPN Account Acquired on the Dark Web leading to Akira Ransomware

A notorious financially motivated ransomware group compromise affected an education institution, with initial access gained via a compromised student VPN account that was sold on the Dark Web. This allowed the threat actor to successfully connect and move laterally within the university network to deploy ransomware at a large scale and exfiltrate data.

The attack was attributed to the Akira threat actor group after TTPs for Akira ransomware were discovered. These TTPs included Akira's encryptor 'w.exe' being dropped into the user's program data directory, an attempt to delete shadow copies via PowerShell, and a text file titled 'akira_readme.txt' being dropped onto systems as the ransom note.

The NCC Group SOC performed a full investigation while liaising with NCC Group's DFIR team. The initial compromised host was isolated upon discovery and proactive searching was conducted by the SOC Team to identify and isolate any newly compromised hosts because of successful lateral movement. The responsible binaries were added to the Defender indicators list to block the execution of any further malicious files.

While the NCC Group's SOC limited the attack via host isolation and blocking of malicious binaries, the speed at which the ransomware propagated across the network resulted in the incident being handed over to the NCC Group DFIR team, who were deployed on-site to assist with the response to the attack, with the network being disconnected from the internet to contain the attack while the threat was eradicated.

Case #3: Insider Threat Exploits GitHub to Spread Impacket Malware via Compromised Accounts

NCC Group's SOC identified early warning signs of malicious activity stemming from behaviours typically associated with discovery and reconnaissance. This led analysts to identify a compromise within a financial institution. The threat actor initially gained access through an internal user's credentials, leveraging their Windows 365 workstation as a launchpad for the attack. From this foothold, the attacker orchestrated a series of malicious actions, including deploying DLL files across multiple hosts. These files later revealed themselves as part of beaconing activity.
The campaign escalated as the threat actor exploited repositories in the customer's GitHub environment, ultimately enabling them to establish connections, move laterally through the pension fund's network, deploy malware, and exfiltrate sensitive data.

A deep dive into the incident identified the culprits as the FalconForce red team, whose distinctive TTPs were uncovered during the investigation. Among these was their signature DLL process injection method: a malicious DLL was stealthily dropped into the user's AppData directory and executed via the trusted, signed process SrcUpdateMgr.dll. Adding to the complexity, they employed a "Living-off-the-land" tactic using rundll32.exe to establish outbound connections across internal and external IPs, facilitating seamless lateral movement within the network.

NCC Group launched a comprehensive investigation, working closely with the customer's Security Team via a bridge call.

Although the initial compromised user account had been overlooked by the customer, SOC analysts quickly identified signs of lateral movement, hands-on-keyboard activity, and the deployment of Impacket malware. Swift action followed: three compromised hosts were isolated, and proactive searches uncovered one additional compromised host as the attacker's lateral movement persisted. Microsoft Defender's automatic intervention further mitigated the threat by locking three compromised accounts.

Despite the attacker's sophisticated methods, the combined efforts of NCC Group and the customer's Security Team successfully contained the attack. Host isolations and automated account blocks by Microsoft Defender halted the breach in its tracks.
The collaborative response not only neutralised the threat but also uncovered a critical detail: this incident was part of a planned Tiber test; a simulated attack designed to mimic real-world adversaries and evaluate the customer's cyber security defences.

Digital Forensics and Incident Response

NCC Group's DFIR team offers continuous support to proactively mitigate against security incidents, and 2024 was no different. In 2024, DFIR responded to global incidents, provided ongoing support and mitigation advice to fortify organisations' security posture. In this year's annual report, we share several case studies that illustrate some of the cybercriminal activity organisations are faced with, and how NCC Group has supported incident response.

The following case studies highlight the dynamism of the present threat landscape, with examples covering search engine poisoning (SEO), ransomware, BEC phishing and CVE exploitation.

Digital evidence is critical to understanding the modern threat landscape. Digital fingerprints from a security incident support examination, investigations, analysis, response, and more, as depicted above. With this data, NCC Group's DFIR have successfully assisted in moments of crisis and in preparation for potential, future, disasters, and will continue to do so into 2025. Incorporating DFIR lowers the potential impact of an incident to your business and reinforces overall security maturity to the organisation.

Case #1: Ransomware Threat actor Targeting Automotive Customer

As ever, ransomware remains an ongoing threat to organisations, as threat actors continue to seek to extort victims for financial gain. In one incident, NCC Group provided incident response support to a large automotive company that was experiencing a ransomware attack across multiple domains. Here, access was gained through an external facing Remote Desktop Web Access service. Notably, attribution was not possible in this scenario due to common tools and techniques being used to conduct the attack. Where typically a custom ransomware is used, which aids in attribution, BitLocker was the encryption method deployed. Data was exfiltrated from the estate but to date, has not been released publicly.

Upon NCC Group being engaged, it was identified that the threat actor was still active within the environment and was attempting lateral movement to multiple domains. Upon initial triage the recommendation was quickly made to isolate all domains from the internet to prevent the threat actor from encrypting additional domains. Forensic analysis began to identify the initial access vector, tooling and techniques deployed to facilitate the creation of an eradication plan. Upon implementation of the eradication plan, NCC Group confirmed the threat actor had been successfully removed from the estate and security improvement work was undertaken by the customer, with NCC Group guidance.

In summary, the investigation and subsequent eradication plan allowed the customer to bring the network back up and resume operational processes. A security improvement plan was also created and provided to ensure the customer's security posture is improved going forward.

Ransomware persists in the threat landscape, and this is reflected not only by this case study but also in NCC Group's Threat Intelligence Team's coverage of ransomware. Both reflect the persistent threat and the importance of implementing sufficient mitigations for a robust defence. These stretch from phishing training and awareness, a common initial access vector to ransomware attacks, to network segmentation to prevent the spread of the ransomware across the estate. Interestingly, in this case, the use of common tools and techniques to conceal the ransomware strain and render attribution difficult speaks to the savviness of threat actors and the evolution of tactics to enhance their success, both of which we should anticipate in 2025.

Case #2: Business Email Compromise Utilising Infrastructure to Further Phishing Campaign

NCC Group was contacted to investigate a Business Email Compromise (BEC) compromise which had impacted a major Political Party. BEC occurs when a threat actor accesses a work email account to trick someone into transferring money, or to steal valuable (or sensitive) data. In this incident, the victim received an email from a known third party who had been compromised. They had observed that several emails had been sent out which looked legitimate but were malicious in nature. Analysis quickly established the user had interacted with a phishing link from a genuine third party resulting in the user providing their credentials to access a document.

Due to the nature of the correspondence between the two parties this would not have been uncommon and appeared genuine to the user. Collaboration with local law enforcement quickly established that this specific phishing campaign had been observed within the legal profession and was currently being furthered via user interaction within the community.

Importantly, the compromised credentials allowed the attacker to exfiltrate the user's mailbox, establishing a list of contacts. The application 'eM Client' was also installed, which is a desktop email client that can allow an attacker to have persistent access to the mailbox and exfiltrate emails.

The compromised credentials also allowed the threat actor to gain access to the infrastructure, in this case, SharePoint, enabling the threat actor to upload malicious documents. The threat actor then replicated the phishing campaign via the compromised user's account, sending phishing emails to the user's contacts. Due to the swift communication between the user and his contacts, it was quickly established that the account had been compromised, and steps were taken to block and reset the user account, locking out the threat actors' access to the infrastructure.

Further steps were then taken to remove the malicious documents from the SharePoint ensuring the outgoing phishing campaign was halted. It was noted during the investigation that the originating phishing campaign was still active, and communication was then established between the victim and the legal company from which the initial phishing email was received. DFIR advised to purge the malicious documents from their SharePoint and reset the user access. Due to the swift actions of all, the incident was quickly resolved.

Case #3: Ivanti Zero-day affected a Wholesale Provider

Threat actors continue to exploit zero-day vulnerabilities to initiate attacks, underscoring the importance of rapid patching. NCC Group was engaged to provide incident response support to a wholesale provider who was impacted by the CVE-2023-46805 and CVE-2024-21887 zero-day vulnerabilities, affecting their unpatched Ivanti Connect Secure (ICS) VPNs.

- CVE-2023-46085 concerns an authentication bypass vulnerability in the web component of ICS (9.x, 22.x) and IPS which enables a remote attacker to access restricted resources by bypassing control checks.
- CVE-2024-21887 a command injection vulnerability in web components of ICS (9.x, 22.x) and IPS which allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.[105]

An alert was raised for both CVE's, alongside multiple others, by NCSC, warning of their exploitation in February 2024.

In this instance, although attribution was not possible in this scenario, the web shell component identified in this incident was known as WIREFIRE or GIFTEDVISITOR - an indicator of compromise seen during the Ivanti VPN zero-day time frame in early 2024. Due to Ivanti encrypting many system files, including underlying operating system log files, upon engagement, NCC Group had to decrypt the Ivanti VPN images before conducting analysis.

The Ivanti integrity checker was deployed on the VPN appliances to determine any file modifications. It was identified that two VPN appliances in the estate had file modifications related to malware deployment. Additionally, a web shell was dropped within the visits.py file, part of cav-0.1-py3.6.egg, providing backdoor access to the appliances. The wholesale provider immediately applied the workaround and rebuilt the two affected VPN appliances. Simultaneously, NCC Group triaged domain controller logs and found no evidence of lateral movement.

NCC Group Impact

NCC Group continue to support customers to defend and respond to threats so that organisations may continue to operate as normal. Our case studies offer insights into some of the activity from the year, depicting an active and dynamic threat landscape. Whilst we only provide a snippet of activity dealt with by the SOC and DFIR, they reflect some of the more prominent threat types highlighted across the cyber security community, such as ransomware, BEC, phishing and CVE exploitation, which remain key threats to organisational security.

In addition, these provide an understanding as to how NCC Group approaches incident response. Notably, having such insights can also support the threat intelligence function with primary data to better understand and analyse threat actor activity. Collaboration is critical to a successful threat intelligence function and as such, data identified from the SOC and DFIR services is pivotal to boosting our understanding of the threat landscape.

Online Exposure Monitoring (OXM) Service: Case Studies

In the early stages of an attack, long before it hits a victim organisation, threat actors undertake reconnaissance. Here, they focus on identifying their target's external infrastructure, leaked credentials, attack vectors, any sensitive data and much more, in the hopes of identifying information that can aid them in launching an attack. This information is extremely valuable to threat actors. At NCC Group we know this because this is the information we gather to support our red teams.

NCC Group launched the Online Exposure Monitoring (OXM) service to replicate this reconnaissance activity. This Threat Intelligence service ensures continuous surveillance of an organisation's digital presence across the clear, deep, and dark web, identifying leaked credentials, sensitive data brokerage, communications to and from the Tor network, potential phishing websites, and much more to stay one step ahead of threat actors.

Case #1: Identifying a Dark Web Forum Conversation

One of the many capabilities of the DarkIQ platform is the ability to track conversations on Dark Web forums and chatrooms based on an organisation's attributes, which vary from brand names, patent numbers, filenames, project names and many other examples.

To leverage this function, NCC Group's analysts perform a hands-on dark web threat hunt on a weekly basis to monitor all mentions of their clients in the digital space. In one recent instance, one of our analysts identified a suspicious conversation on the Russian underground forum, "RAMP", where a threat actor claimed to have breached a managed service provider, giving them access to the sensitive information of their client base. One of these client organisations was an OXM customer.

Our analyst proceeded to map out the timeline of the event, actors that were involved, potential aliases on other forums and marketplaces, and, critically assessed the validity of the claim. Within an hour of identification, the client was made aware of the potential threat and was advised to contact the managed service provider directly to verify the legitimacy of the claim and deduce the nature of the client's data that the provider is privy to. This is a quintessential example of the service's strength where exploring online spaces you may not consider, lack the time to monitor, or are simply unaware of, in order to identify emerging threats to your organisation.

Case #2: Detecting a Ransomware Data Leak Site (DLS) Posting

One of the most devastating cyber events that an organisation can experience is a double extortion ransomware attack; the operational downtime and thus loss of revenue, sensitive data exfiltration, reputational damage and, of course, significant regulatory fines, can cripple any organisation, irrespective of maturity.

In such cases, organisations frequently turn to NCC Group for their expertise. In one case, a client's data was encrypted, with potential data exfiltrated. As such, they purchased the OXM service to ensure that they would be notified of any DLS postings in a timely fashion. This would allow them to kick-start their disaster recovery process as efficiently and effectively as possible.

Due to the critical nature of ransomware attacks, the DarkIQ platform scans ransomware group data leak sites for client data on an hourly basis. Predictably, within a few months of the client's profile being created, NCC Group spotted the listing within an hour of it being posted and informed the client immediately, thereby initiating their internal processes in a timely fashion, demonstrating maturity and trustworthiness to their own customers.

Efficiency is what OXM ultimately strives to bring to clients. It acts as a security camera outside of their organisation, flagging concerns before disaster strikes, but also minimises impact when the bomb has already been detonated.

However, in cases such as this, NCC Group's assistance does not stop there. Included in some of the higher tiers of the service are Support Tokens, which can be redeemed to purchase numerous intelligence products, ranging from malware analysis to threat landscape assessments.

In this case, the client asked NCC Group to download a sample of the stolen data and analyse it to determine the nature of it and thus the potential impact on their organisation. NCC Group provided them with regular updates on their ongoing research and were able to identify Personally Identifiable Information (PII) in what appeared to be HR databases, but no Intellectual Property (IP) or credentials. This, once again, allowed the client to gauge the incident's impact, as well as informing their subsequent decision-making process.

Case #3:
Dark Web Traffic Probing Remote Access and VPN Hosts

As mentioned in the above sections, one functionality of the DarkIQ platform is the indexing of dark web traffic, which allows us to see when the Tor network is interacting with client infrastructure. While sometimes these may be benign, there are instances when threat actors could be probing for security weaknesses, installing malware following initial access, beaconing to previously installed malware, or exfiltrating sensitive data. By identifying these network events, the customer can further investigate the affected host to determine the nature of the connections and whether there has been any impact on their organisation.

One such case took place in mid-2024, when NCC Group uncovered dark web traffic incrementally contacting client remote access and VPN infrastructure, spanning from December of 2023 up until May 2024, with the most significant activity taking place in March. This activity consisted of significant data transfers out of the organisation and sizeable quantities of individual connections throughout the month. NCC Group assessed that these hosts could have been targeted for initial access with valid credentials that were ascertained prior. Furthermore, the incremental nature of the traffic could have hinted at an attempt to evade detection due to data transfer limits.

Following this finding, NCC Group worked closely with the customer to investigate the traffic and undertake the necessary mitigations, ensuring that there had been no prior impact and that such instances would be sure to have limited implications in the future.

Summary

As demonstrated in these case studies, the OXM service provides organisations with sorely needed insights into their online exposure, allowing them to identify a threat before it evolves into a serious incident. While the traditional approach of cyber security (in a nutshell; detection and response) remains entirely essential to secure systems and data, it is a common misconception that this is all you need to have in place to achieve a competitive security posture.

However, SOCs and incident response teams only account for roughly 33% of the widely referenced cyber kill chain, while the other 66% can be covered via the implementation of online exposure monitoring, as demonstrated in Figure 11.

Therefore, if organisations wish to significantly reduce the ever-increasing cost and impact of cyber incidents, it is imperative to have a combination of online exposure monitoring and detection and response functions in place.

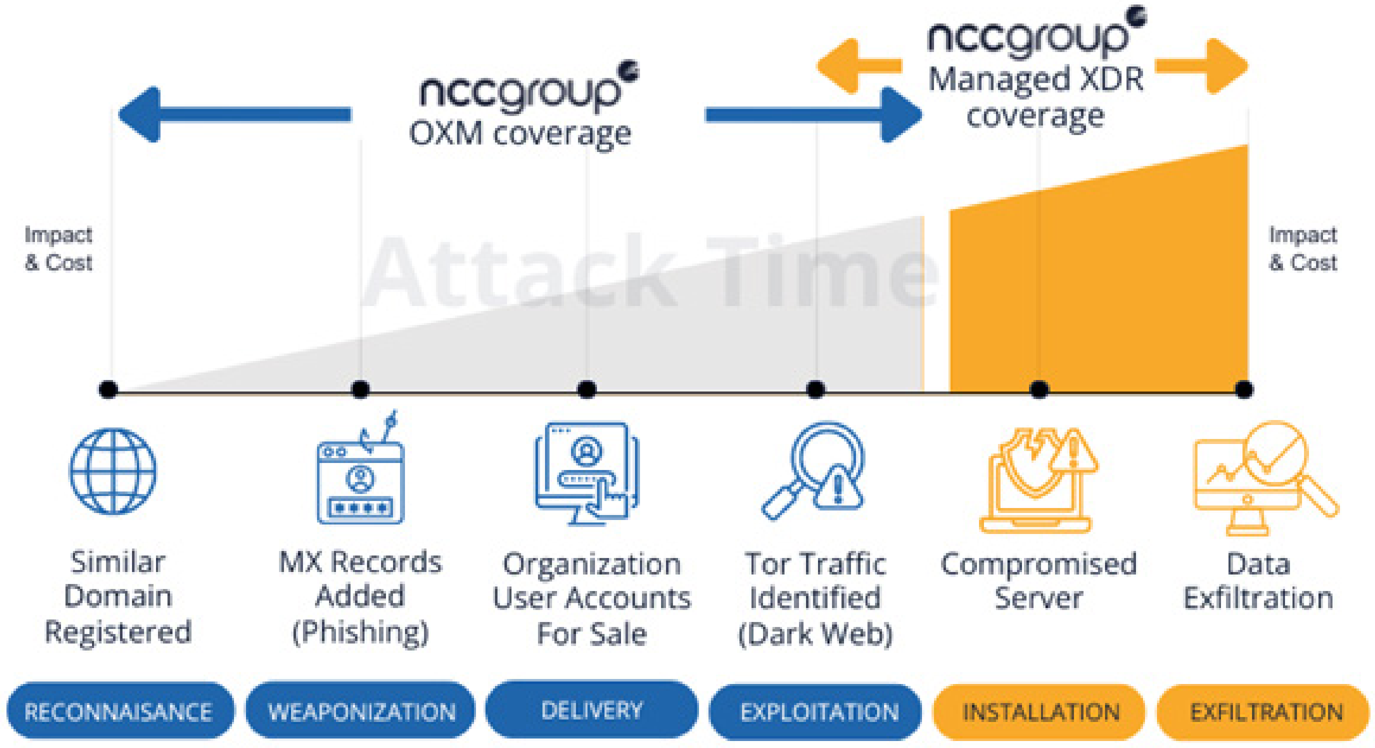


Figure 11: Lockheed Martin Cyber Kill Chain X the OXM Service

Get in Touch Regarding the OXM Service

If any of the above sounds like something your organisation would benefit from, please get in touch.

nccgroup

People powered tech-enabled cyber security

FOX IT
part of nccgroup