Quorum Cyber

Threat Intelligence Intelligence Outlook 2023

TLP Status: Green

Prepared by: Jack Alexander & Craig Watt

Reviewed by: James Allman-Talbot

+44 333 444 0041

quorumcyber.com

Verdant, 2 Redheughs Rigg, Edinburgh, United Kingdom, EH12 9DQ

Microsoft Solutions Partner

Table of Contents

Document Control

Revision History

Version	Date	Summary of Changes
0.1	15/01/2023	Initial report
0.2	06/02/2023	Draft one
0.3	13/02/2023	Draft two
0.4	15/02/2023	Draft three
1.0	23/02/2023	Completed report
1.1	23/02/2023	PDF Formatting

Related Documents

The following documents are either referenced within, or are related to, the content of this document:

Document Name	Date	Version
-	-	-

Executive Summary

- Ransomware-as-a-Service (RaaS) increased in prevalence throughout the 2022 calendar year. The use of the RaaS model is highly likely to continue this trajectory due to the commercial availability and low cost of the service.
- The ongoing conflict between Russia and Ukraine has resulted in economic instability and has created the perfect conditions for cyber threat actors to capitalise on the situation. The military conflict will almost certainly remain highly significant as the 2023 calendar year progresses due to the scope and potential international implications of the war. While the front lines of the ground war will likely see limited movements until the spring due to adverse weather conditions, the cyber battlefield will remain unaffected. Additionally, new patriotic hacktivist groups have been formed on both sides since the start of the conflict, with the aims of disrupting each other and those supporting their efforts.
- Oil and gas companies were targeted by several hacktivist attacks throughout 2022. This is a trend that is likely to continue into 2023. In Europe, activist group Just Stop Oil conducted an online protest against the expansion into the Rosebank oil field. This protest was limited in nature but there is a realistic possibility that it could be the catalyst for increasingly serious campaigns throughout 2023 and beyond as protests pivot into cyberspace.

Introduction

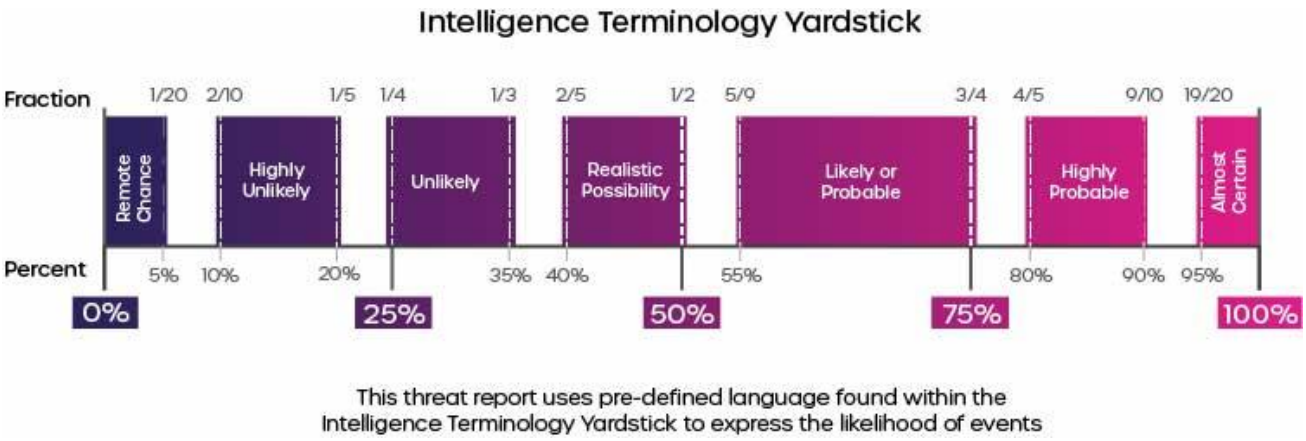
This report has been written by Quorum Cyber's Threat Intelligence team to provide a high-level cyber threat overview about developing threats and how they are likely to evolve over the calendar year. Included within this report are our assessments on traditional cyber threats, such as phishing and ransomware, which are undertaken by cybercriminals, geopolitical considerations from external nation threats, such as Russia, China, and Iran, and developing threat trends detected by our intelligence team.

Additionally, sector-specific threats and areas of developing concern have been highlighted for multiple different industries, including those involved in financial, healthcare, defence and aerospace, housing, education, the public sector and energy.

The inclusion of these sectors has been chosen so that appropriate mitigation steps can be implemented to reduce the threat of compromise by malicious cyber threat actors.

Intelligence Cut-off Date (ICoD): 06/02/2023 10:00 GMT

The following intelligence report has been written using the 'Intelligence Terminology Yardstick'. The likelihood of events corresponds with pre-defined language found in the table below to remove areas of uncertainty.



This threat report uses pre-defined language found within the Intelligence Terminology Yardstick to express the likelihood of events

Malware Threats

Malware continues to be a threat to all online users and as time advances, so too does their sophistication. It's likely that 2023 will be the year of Malware-as-a-Service (MaaS) as threat actors including hacktivists and those without sufficient tooling or infrastructure use these services to further their goals. RaaS makes it easier than ever for threat actors to gain access to ransomware and phishing tools without requiring comprehensive technical skills in how to use them.

Malware-as-a-Service

MaaS offers a simple interface and pre-built infrastructure for threat actors who do not possess their own. This is highly beneficial for the threat actor as it allows them to conduct their aims without committing substantial time, expertise and resources to the development of their own malware. A prominent service is Robin Banks, a Phishing-as-a-Service (PhaaS) that, as the name suggests, has historically targeted the financial sector but is now increasingly being used as a common service targeting all sectors. Robin Banks remerged in early November 2022 after a four-month absence and is actively being used in attacks across the cyber landscape.

In conjunction with PhaaS, RaaS has grown over the previous year with December ransomware statistics reporting that all five of the most active ransomware strains use RaaS models[1]. Prolific RaaS based ransomwares include, but are not limited to:

- LockBit Ransomware[2]
- Conti Ransomware[3]
- Pysa Ransomware[4]
- Black Basta Ransomware[5]
- Nevada Ransomware[6]

RaaS model services are highly likely to continue being the most used ransomwares in 2023 due to their commercial availability, with some licences being sold for as little as $66[7]. Furthermore, the widely reported lucrative nature of ransomware is only fuelling criminal ambitions, driven by financial incentives.

The current global situation in the wake of 2022 regarding conflict, healthcare and the cost of living has cultured the perfect environment for criminals to exploit. Furthermore, intelligence suggests that nation states are developing and distributing RaaS to portray state activities as criminal activities, thus creating deniability.

All is not bad news, however. Recent activity by law enforcement has led to the disruption of multiple MaaS including Hive, Conti and Raccoon.

Ransomware

Despite the growth of RaaS modelled organisations, the level of reported ransomware attacks has seen an overall decrease in activity since March 2022. There is a realistic possibility that this drop is due to increased law enforcement activity and the adoption and investment of effective endpoint detection and response (EDR) solutions by more

[1] https://therecord.media/ransomware-tracker-the-latest-figures/
[2] https://www.kaspersky.com/resource-center/threats/lockbit-ransomware
[3] https://flashpoint.io/blog/history-of-conti-ransomware/#:~:text=Conti%20operates%20using%20a%20Ransomware,second%20stage%20of%20the%20attack.
[4] https://www.cybereason.com/blog/research/threat-analysis-report-inside-the-destructive-pysa-ransomware
[5] https://www.quorumcyber.com/threat-intelligence/black-basta-ransomware-breakdown/
[6] https://www.quorumcyber.com/threat-intelligence/nevada-ransomware-report/
[7] https://securityintelligence.com/articles/cyber-crime-cheap/

businesses. It remains unclear if this trend will continue throughout 2023, however, by making security conscious decisions, businesses can more effectively and proactively defend against the ransomware threat. Security conscious recommendations can be found at the end of this report.

Of note, on 2nd February 2023, it was reported that 42 clients of the London software trader ION Cleared Derivatives incurred a ransomware attack[8]. The attack was linked to the LockBit ransomware group. At the time of the release of this report, the incident remained in the investigation phase and analysis to assess the extent of the impact on trading. Such supply-chain attacks can lead to devastating consequences for any industry sector, such as finance.

Finally, due to the increasing likelihood of a global financial recession, it is expected that ransomware attacks will peak in the 2023 calendar year[9], a factor which must be kept firmly in mind within the context of the security posture for all sectors.

DDoS Threat

A distributed denial of service (DDoS) is an attack that aims to disrupt the normal flow of traffic to a targeted service. They operate by overwhelming the target with a flood of network traffic provided by a botnet[10]. In 2022, Russian state-sponsored threat actor Killnet conducted multiple DDoS attacks against European and US organisations that were almost certainly in retaliation for continued western support for Ukraine in the ongoing conflict[11]. Killnet attacks often occur in conjunction with changes in western policies that negatively affect Russia, or during shipments of aid to Ukraine. Targets of Killnet DDoS include:

- US airport infrastructure[12]
- US government state departments
- Royal family website
- British Army website (unconfirmed)
- European Parliament[13].

DDoS attacks are often conducted by state-sponsored threat actors to disrupt Critical National Infrastructure (CNI) of a rival. However, criminal groups are now monetising this tactic by issuing ransom demands to cease an attack and allow normal traffic to continue.[14].

Targeted DDoS attacks will almost certainly continue into 2023 while international geopolitical tensions remain frayed. Due to the likely connection between DDoS attacks and state-sponsored threat groups, attacks of this nature are highly likely to be those considered to be in the public sector or CNI. These include:

- Defence & Aerospace
- Government agencies
- Energy sector
- Education sector
- Healthcare services
- Financial sector.

[8] https://www.infosecurity-magazine.com/news/city-of-london-high-alert/
[9] Cybersecurity Trends: IBM's Predictions for 2023 (securityintelligence.com)
[10] https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-botnet/
[11] https://www.hackread.com/pro-russian-killnet-uk-ddos-attacks/
[12] https://therecord.media/coverage-of-killnet-ddos-attacks-plays-into-attackers-hands-experts-say/
[13] https://www.hackread.com/killnet-european-parliament-ddos-attack/
[14] https://www.cloudflare.com/en-gb/learning/ddos/ransom-ddos-attack/

2022 Geopolitical Considerations

2022 was a turbulent year for geopolitical stability. Long considered to pose the greatest threat to western security, Russia, China and Iran often found themselves front page news for the wrong reasons. Reasons include international invasions, revolutionary uprisings and state censorship.

Starting with Russia, 2022 witnessed the nation enacting in the largest sovereign invasion in Europe since the Second World War. After months of military build-up and training exercises along their neighbour's border, the long anticipated Russian invasion of Ukraine commenced on 24th February resulting in severe international sanctions.

Ukraine is often considered to be the breadbasket of Europe, due to the nation's large wheat grain exports on which many European, Middle Eastern and African (EMEA) nations depend[15]. Disruption to this source of grain, as a direct result of the invasion, had considerable impact on reliable global food supply[16], resulting in steep inflation across the world[17].

In addition to the conflict affecting international food security, it has also led to a significant energy crisis in Europe and further afield. In retaliation to the waves of economic sanctions imposed by the European Union (EU), Russia threatened their oil and gas supplies, leading to record high energy prices[18].

The economic instability resulting from the resource crisis has created the perfect conditions for threat actors to take advantage. While media attention was focused on conflict events on land, in the air and at sea, the hybrid cyber war was in full force and affected many western organisations and critical infrastructure.

Highlighted below are key cyber events highly likely conducted by Russian state-sponsored threat actors in 2022:

- Killnet DDoS attacks targeting western CNI
- Wiper malware attack on European satellite infrastructure to counter Ukraine communications[19].

In China, the government's zero-Covid policy ended in civil unrest after the nation became one of the last to maintain strict covid restrictions[20]. The end of the controversial policy came to fruition after rare protests against the Chinese Communist Party (CCP) in the nation's economic capital Shanghai. The FIFA World Cup added to Chinese frustrations, as millions watching saw stadiums packed with football supporters not wearing face masks.

In August, China-US political relations were strained as House of Representatives Speaker Nancy Pelosi visited Chinese claimed Taiwan. The visit, meant to reassure Taiwan of continued US support, was met with condemnation from China and resulted in largescale Chinese military exercises off the Taiwanese coast, prompting fears of a crisis in the region.

In Iran, nationwide anti-regime protests erupted after the death of Mahsa Amini while she was in the custody of the Iranian Guidance Patrol, also known as the Morality Police. Starting on 16th September, the protests had spread to all major cities across Iran. The protests have also led to multiple sectors calling for strikes, including Iran's most important industry, oil[21]. The walkout of oil workers will be extremely concerning for the regime's government, as the striking of oil workers in the 1979 Iranian Revolution[22] was a key turning point that led to the collapse of the old Iranian monarchy, and the rise of the current religious government.

[15] https://www.wilsoncenter.org/blog-post/forty-percent-world-food-programs-wheat-supplies-come-ukraine
[16] https://www.goldmansachs.com/insights/pages/the-war-in-ukraine-stokes-global-food-inflation.html
[17] https://www.nytimes.com/2022/10/19/business/europe-food-prices-inflation.html
[18] https://www.bbc.co.uk/news/58888451
[19] https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack/
[20] https://www.bbc.co.uk/news/world-asia-china-63855508
[21] https://www.iranintl.com/en/202212175612
[22] https://en.wikipedia.org/wiki/Iranian_Revolution

Geopolitical Considerations – Russia

Russia will almost certainly remain on the front pages of the majority of news outlets for the duration of 2023 due to the scope and potential international implications of the Russa-Ukraine war. While the front lines of the ground war will likely see limited movements until spring due to adverse weather conditions, the cyber battlefield will remain unaffected.

As mentioned earlier in this report, the LockBit group was linked with the ransomware attack on multiple clients of the software company ION Cleared Derivatives. The reported links between the group and the Russian state have led to the conclusion that there remains a possibility that this ransomware attack could be a result of Russian retaliation against UK-imposed financial sanctions.

Russian DDoS

During the conflict, Russia has utilised two main methods of cyber-attack: wiper malware and DDoS.

In a recent report from Russia's largest Internet Service Provider (ISP), Rostelecom, 2022 was a record-breaking year for DDoS attacks targeting Russia, Ukraine and nations assisting both sides of the conflict. In 2023, this trend will almost certainly continue due to threat actors, such as Killnet, operating under the influence of the Russian government, targeting western organisations when support for Ukraine is publicised.

Russian Wiper Malware

Wiper malware in 2023 will likely affect organisations who directly support Ukrainian military efforts, CNI of those nations that provide Ukraine with weapons, and states that actively impose economic sanctions on Russia as a consequence of the war. Examples of wipers that have been used by Russian-aligned threat actors since the start of the conflict so far are:

Wiper Malware	Associated Ransomware	Target Operating System	Code Language
WhisperGate	Yes	Windows	C++ / .NET
HermeticWiper	Yes	Windows	C / Assembly
IsaacWiper	No	Windows	C / C++ / Assembly
DesertBlade	No	Windows	Golang
ACIDRAIN	No	Linux (MIPS)	C
CaddyWiper	No	Windows	C
DoubleZero	No	Windows	.NET
AwfulShred	No	Linux	Bash
SoloShred	No	Solaris	Bash

It is highly likely that wiper malware will continue to be a mainstay of Russian state-sponsored cyber aggression during the remainder of the conflict. Additionally, western countries and organisations that are seen to support Ukraine are

highly likely to be a desired target of third-party attacks. For example, previously mentioned state-sponsored threat actor, Killnet, has openly targeted organisations in both the US and UK.

Western organisations most likely to be targeted by Russian state-sponsored threat actors in 2023 are those involved in the support of Ukrainian aid and those who contribute to western CNI such as the energy, financial, defence and health sectors. Adding weight to this assessment of continuing Russian wiper activity, reporting indicates recent use of a new wiper variant name, 'NikoWiper'; a report on this developing activity is available on the Quorum Cyber online TI page[23].

Russian Spear Phishing

The National Cyber Security Centre (NCSC) released an advisory on 26th January 2023[24] pertaining to two Advanced Persistent Threat (APT) groups that are expected to enhance their spear-phishing attack efforts against organisations and individuals in the UK throughout the 2023 calendar year. Of particular relevance to this section is the fact that one of these groups was detected to be Russia-based SEABORGIUM (Callisto Group/TA446/COLDRIVER/TAG-53).

Throughout the 2022 calendar year, the threat groups were detected to have targeted a variety of industry sectors and individuals including the education and defence sectors, government, non-governmental organisations (NGOs), politicians, journalists and activists. The threat group is known to implement typical spear-phishing techniques in which a specific individual or group will be targeted with information known to be of interest to them.

The use of the spear-phishing attack vector is common amongst established threat actor groups. However, what is significant regarding SEABORGIUM is that they are evolving the process associated with these attacks, leading to increasingly sophisticated attack efforts. As such, organisations and individuals ought to maintain an elevated level of vigilance and follow the recommended defence strategies outlined by the NCSC.

A full report on SEABORGIUM is available on the Quorum Cyber Threat Intelligence page online[25].

[23] https://www.quorumcyber.com/threat-intelligence/
[24] SEABORGIUM and TA453 continue their respective... - NCSC.GOV.UK
[25] https://www.quorumcyber.com/threat-intelligence/advanced-persistent-threat-groups-continue-their-respective-spear-phishing-campaigns-against-targets-of-interest/

Geopolitical Considerations – China

2023 is shaping up to be a key year for China. The nation has set out an ambitious plan of achieving 70% self-sufficiency in high-tech research and production by 2025. The plan has been dubbed "Made in China 2025" and seeks to ensure China's dominance in global tech manufacturing. For years China has been at the forefront of high-tech manufacturing but has lagged behind in the research and development of home-grown technology. Alarmingly, one of the historically reported methods to promote this research expansion is the widespread theft of Intellectual Property (IP) from western tech companies, most notably from the communications, military and medical sectors.

With 2025 fast approaching, it is assessed that 2023 will continue to witness multiple espionage attempts by Chinese state-sponsored groups to fulfil their goal of 70% self-sufficiency. Two of the most notorious groups filling this role are APT10, operating since at least 2006[26], and HAFNIUM[27], operating since early 2021. Both groups use a multitude of exploitive measures to achieve their aim of IP theft, but most commonly use dedicated spyware or the choreographed exploitation of zero-day and known vulnerabilities.

Common Chinese Spyware

Both APT10 and HAFNIUM have been reported to deploy spyware variants, known as China Chopper and Tarrask, to infiltrate western organisations and exfiltrate sensitive research data. In 2023, the deployment of such spyware by these two groups is highly likely to continue to further state ambitions.

China Chopper[28] is a simple and easy-to-use text-based post exploitation tool that can provide an attacker with a backdoor into a network. The malware, just 4 kilobytes in size, has been seen in wide operational use and was even used in the notorious Microsoft Exchange Server attacks in 2021.

Tarrask[29] is a spyware specifically designed to avoid digital defences and maintain persistence on an infected system/network by generating covert scheduled tasks. Despite the intended digital defence evasion, the latest versions of Microsoft Defender have built-in detections to identify and alert a user to its presence.

[26] https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations
[27] https://attack.mitre.org/groups/G0125/
[28] https://attack.mitre.org/software/S0020/
[29] https://attack.mitre.org/software/S1011/

Geopolitical Considerations – Iran

At the start of 2023, two major geopolitical considerations confront the Iranian political landscape. These are the ongoing nationwide unrest and protests against the government after the death of Mahsa Amini while in police custody, and the supply of military hardware to Russia for use in Ukraine[30]. Both examples garnered attention and condemnation from around the world and have the potential to threaten the nation's global standing.

While the Iranian government attempts to quash unrest, hacktivists, both national and international, are likely to conduct online activities against the regime in support of their own cause.

The primary objective for the Iranian government while these events unfold is likely to be the preservation of power and control of the state. It is therefore a realistic possibility that international cyber-attacks originating from Iran will be lower than normal while resources are used to combat internal unrest. However, when protest activities begin to decline, it is highly likely that international targeting will continue, particularly against rival Israeli and Middle Eastern agencies.

As mentioned previously in the Russian geopolitical considerations section, the NCSC recently released an advisory reporting that an Iranian state-sponsored threat group, known as APT42 (Charming Kitten), is expected to enhance their spear-phishing attack efforts against organisations and individuals in the UK throughout the 2023 calendar year. APT42 are known to actively target sectors across the UK, but key targets include academia, defence and governmental organisations. A full report on APT42 is available on the Quorum Cyber Threat Intelligence page online[31].

[30] https://www.bbc.co.uk/news/world-europe-63921007
[31] https://www.quorumcyber.com/threat-intelligence/advanced-persistent-threat-groups-continue-their-respective-spear-phishing-campaigns-against-targets-of-interest/

Hacktivism

Hacktivist activities most commonly occur against organisations involved in areas of cultural, political and social friction, such as those invested in the production of fossil fuels, have poor working conditions, and those who distribute military hardware.

Oil and gas companies have been targeted in several instances of hacktivism during 2022, a trend that is likely to continue into 2023. In Central and South America, hacktivist group Guacamaya successfully hacked agencies and organisations linked to the sector[32].

These included, but were not limited to, mining and oil companies in Brazil, Venezuela and Colombia, and the Guatemalan Ministry of Energy.

The aim of these attacks is to steal email data and to publish it to one of two dedicated hacktivism publishing sites, Distributed Denial of Secrets[33], or Extractivist Leaks[34]. Once the stolen data has been published, any credentials can be used for initial access in future cyber-attacks.

In the UK and Europe, activist group Just Stop Oil conducted an online protest against the expansion into the Rosebank oil field[35] on 25th October 2022. The protest itself was limited in nature but there is a realistic possibility that it could be the catalyst for increasingly serious campaigns in 2023 and beyond. Should Just Stop Oil commit to expanding their online activist activities then there is a realistic possibility it is likely that their actions may increase in intensity to match those already implanted by their South American counterparts, Guacamaya.

In Ukraine and Russia, new patriotic hacktivist groups have been formed on both sides since the start of the conflict with the aim of disrupting each other and those supporting their efforts. These campaigns have been widely effective for both sides and have included the use of DDoS and wiper malware. While the conflict continues there are no signs of associated hacktivist efforts slowing, and therefore they will almost certainly continue throughout 2023.

Likely target sectors for hacktivism activities in 2023:

- Energy sector organisations involved in the production and use of fossil fuels.
- Government agencies involved in social and international issues.
- Defence contractors.

[32] https://www.vice.com/en/article/5d39i3/meet-the-environmental-hacktivists-trying-to-sabotage-mining-companies
[33] https://ddosecrets.com/index.php?search=extractivist&title=Special%3ASearch&wprov=acrw1
[34] https://enlacehacktivista.org/index.php?title=Extractivist_Leaks/es
[35] https://www.offshore-energy.biz/equinor-facing-protests-over-one-of-the-biggest-new-oil-and-gas-projects-in-uk/

Financial Sector

The financial sector contains an abundance of critically sensitive data that naturally makes it an attractive target for both cybercriminals and nation-state threat actors. Cybercriminal networks almost certainly view those within the financial sector as a prime target due to the vast amounts of customer banking credential data potentially available for exploitation. Furthermore, nation-state threat actors, and especially those with economic sanctions imposed on them by the UK and US, will almost certainly seek the disruption of UK finance as recompense. Of note, nation-states under UK economic sanctions which possess capable cyber offensive capabilities include Russia, Iran and North Korea.

Throughout the calendar year of 2022, organisations within the financial sector experienced cyber-attacks from multiple attack vectors including but not limited to[36]:

- Banking Trojans (Xenomorph, Sova & Gootkit)
- Data Breaches (Raccoon Stealer, Redline Stealer & Vidar)
- Phishing (23.6% of phishing attacks occurred against financial organisations in Q1 of 2022[37])
- Ransomware.

By the end of Q4 2022, a total of fifty-five ransomware data leaks were reported in the financial sector globally. The sector in general was ranked as eleventh in terms of affected industries by ransomware attacks, globally[38], with the LockBit ransomware gang reportedly responsible for approximately 40% of all ransomware data leaks against financial institutions. The trend of high-volume LockBit ransomware attacks against financial institutions is expected to continue into the 2023 calendar year, especially due to the dissolving of rival groups such as Conti beginning in June 2022, and the FBI's disruption of Hive[39].

As of Q4 2022, finance organisations had experienced 566 data breaches, correlating to 254 million leaked records. This was ranked as the second highest number of data breaches, compared to the cross-sector ranking. A total of 57% of these breaches were attributed to "general hacking" methods and 6.5% were attributed to skimming attacks.[40]

A consistent level of interest in fraudulent money transfers was observed throughout the 2022 calendar year, an interest that has by speculation been attributed to the emergence of digital money transfers and cryptocurrency methods. However, both the US and the EU implemented strict anti-money laundering laws, thereby increasing potential sanctions. This could impact the threat landscape as it pertains to financial organisations heading into 2023.

Listed as one of the sector's most active threats, the notorious banking trojan, Emotet, was absent from the cyber threat landscape during the first half of 2022. However, a re-emergence was recently observed in November 2022 in the form of a largescale malware spam ("malspam") campaign. Cyber security researchers following this re-emergence have noted that the main targets are located in multiple western nations and this is likely to continue to increase the scale of the current campaigns into the 2023 calendar year[41].

In addition, the aptly named financial targeting PhaaS platform, Robin Banks, has resurfaced after a four-month absence in 2022 and seems poised to continue targeting those in the sector during 2023. Past victims of their phishing spam include Lloyds Bank, Citibank and Bank of America[42].

[36] https://flashpoint.io/blog/risk-intelligence-year-in-review-financial/
[37] https://www.egress.com/blog/phishing/phishing-statistics-round-up
[38] https://flashpoint.io/blog/risk-intelligence-year-in-review-financial/
[39] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant
[40] https://flashpoint.io/blog/risk-intelligence-year-in-review-financial/
[41] https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return
[42] https://www.quorumcyber.com/threat-intelligence/robin-banks-phishing-service-targets-financial-sector/

Healthcare Sector

The volume of detected cyber-attacks against the healthcare sector has significantly increased in recent years[43], an increase that was documented at 94% from 2020 to 2021[44]. However, this was likely due to the Covid-19 pandemic. A substantial portion of such attacks have been attributed to threat actors associated with eCrime[45], almost certainly motivated by financial gain. The increased volume of attacks was specifically noted and documented throughout the latter half of 2022, and it is more than reasonable to conclude that such a trajectory will likely continue as the 2023 calendar year progresses.

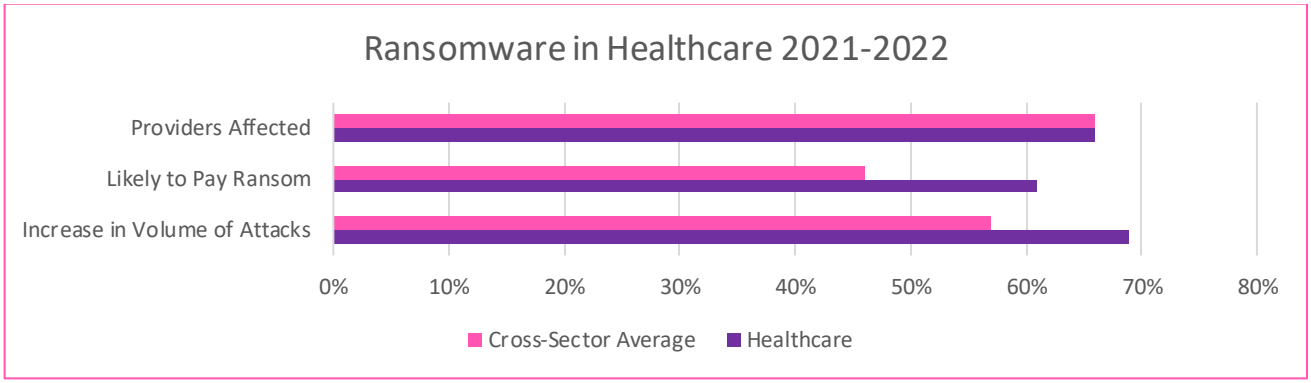


Figure 1: Ransomware statistics affecting healthcare organisations compared with cross-sector average 2021-2022.

Despite the threat of ransomware, 99% of healthcare sector organisations reportedly recovered at least a portion of the encrypted data[46], highlighting resilience and potential backtracking of ransomware threats[47].

Phobos ransomware is widely used to target those in the sector, however, there is a realistic possibility that its affiliates will swap to the RaaS providers such as LockBit, ALPHV and AvosLoker in 2023, as these provide threat actors with more substantial resources, allowing for more attacks. This is due to the very nature of eCrime adversarial groups, as they always seek the most efficient manner of exploiting a target organisation to generate the greatest revenue, as the final objective[48].

Several nation-state APT groups actively target the healthcare sector, including Nemesis Kitten, Unknown Panda and Cyborg Spider. Due to the innovation of these threat actor groups, as well as the resources at their disposal, it is likely that these groups will target organisations with greater sophistication than their cybercriminal counterparts.

As is the case for all industry sectors, due to the increasing likelihood of a global financial recession, it is expected that ransomware attacks will peak in the 2023 calendar year[49], a factor which should be kept firmly in mind within the context of the security posture of healthcare sector organisations.

[43] https://expertinsights.com/insights/healthcare-cyber-attack-statistics/
[44] https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
[45] https://www.helpnetsecurity.com/2021/05/25/healthcare-related-ecrime/
[46] https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
[47] https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor/
[48] https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/
[49] Cybersecurity Trends: IBM's Predictions for 2023 (securityintelligence.com)

Defence & Aerospace Sector

The Defence & Aerospace sector is home to some of the most advanced cyber systems in the world which can provide their customers with an advantage on the geopolitical world stage. Therefore, the sector is a highly desirable target for both cybercriminals driven by financial gain, and also sophisticated nation-states who seek to exfiltrate data from these advanced systems to give them a strategic edge over their international rivals.

A consistent number of attacks have been observed against the aerospace industry throughout the previous three-year period (52 attacks in 2020, 48 attacks in 2021 and 50 attacks reported by the end of Q3 in 2022).

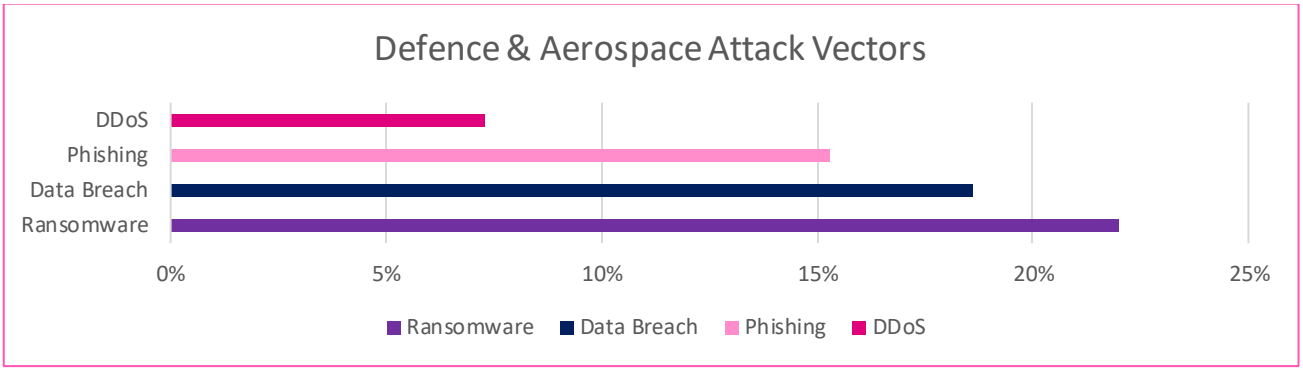


Figure 2: Common attack vectors affecting the defence & aerospace sector from 2020 – 2022 (listed by the percentage of reported incidents).

As with other sectors, defence and aerospace organisations commonly depend on a complex network of highly distributed supply chains. This dependency increases the potential attack surface presented to threat actors and requires strong mitigation strategies to prevent potential attacks.

Multiple nation-states with sophisticated cyber capabilities almost certainly view the disruption and infiltration of the western defence and aerospace sector as a high priority. These states include Russia, China, Iran and North Korea. Additionally, these nations can extend their objectives through state-aligned APT groups[50]. It is likely that these nation-state threat actors target defence and aerospace organisations to develop a competitive advantage for their native companies or to support the modernisation of their military infrastructure[51].

It has been reported that the following factors will contribute to this trend:

- Threat actors targeting defence technologies to counter an adversary's capabilities, or to create disruptions within hostile territory, as seen in Ukraine
- The growth of the global arms and defence trade, motivating nations to utilise cyber espionage methods to steal intellectual property and to reduce the financial costs of their own research
- Multiple advanced threat actors are currently operating within the sector with the aim of cyber espionage including APT28 (Fancy Bear), APT35 (Charming Kitten) and the Equation Group.

Ransomware will likely continue to be a major threat to the sector, deployed both for its financial gain, but also for data exfiltration and disruption. Additionally, wiper malware mostly used by Russia will likely pose a significant threat, especially to organisations directly supporting the defence of Ukraine.

[50] https://www.welivesecurity.com/wp-content/uploads/2022/11/eset_apt_activity_report_t22022.pdf
[51] https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf

Housing Sector

Housing associations are highly desirable targets for cybercriminal groups due to the large amounts of sensitive customer data they hold, including legal, financial, and personal information. Recent trends have indicated that, of the wide array of attack vectors available to threat actors, ransomware attacks have appeared to have progressed to the greatest levels of prevalence. It is highly likely that this is due to the previously mentioned abundance of valuable data[52]. Housing association organisations are likely to suffer various consequences following a successful cyber-attack, including threat actors accessing organisational data, loss of service and resulting reputational damage[53].

Research-based trends have illustrated that housing associations are at the greatest risk of incurring cyber-attacks via the following three attack vectors:

- Phishing campaigns
- Ransomware attacks
- Credential leaks.

As in most sectors, phishing campaigns remain as the foremost risk facing housing associations since this attack method is associated with a low financial cost, convenience of utilisation and the way such attacks can spread between network environments. In 2022, it was reported that phishing emails accounted for 83% of cyber-attacks[54].

Due to the nature of the data in the possession of housing organisations, it is expected that ransomware groups will continue to focus their attack efforts within this industry sector. The most commonly reported ransomware activity, dating back to Q3 2022, correlated to the following ransomware groups[55], as outlined in *Figure 3*:

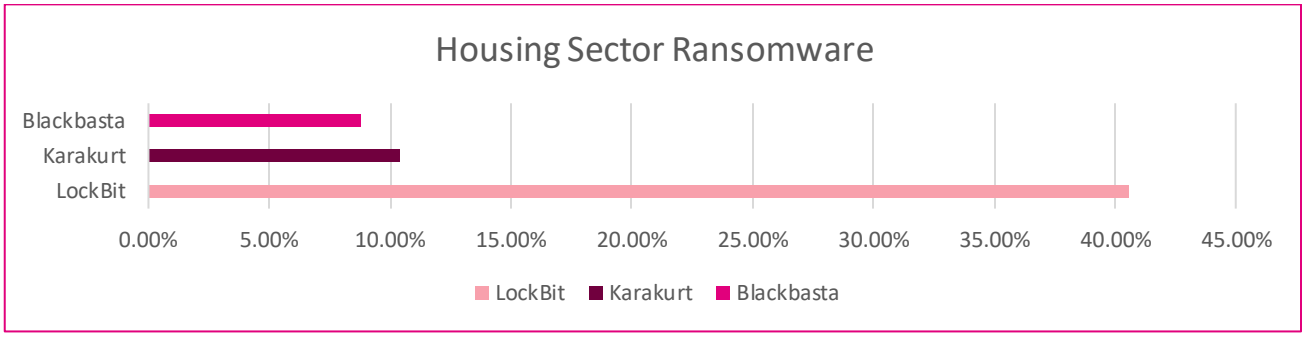


Figure 3: Common ransomware groups operating within the housing sector throughout Q3 and Q4 of 2022 (listed by percentage of reported attacks).

Much like the previous year, ransomware attacks in 2023 will likely present the most consequential attacks to the sector, as continued targeting will inevitably occur. However, despite this unfortunate assessment, there are positive developments to mention. Most notably, the notorious ransomware gang, Hive, which frequently targeted the sector in 2022, but since January 2023 has been infiltrated and disrupted by Europol and the FBI.

[52] https://www.securityhq.com/blog/elevated-risk-of-cyber-threats-for-housing-sector/
[53] https://www.mazars.co.uk/Home/Industries/Public-Social-Sector/Transforming-your-organisation/Horizon-Scanning/Cyber-security-and-the-housing-sector
[54] https://www.ncsc.gov.uk/report/weekly-threat-report-1st-april-2022
[55] https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-and-black-basta-are-the-most-active-raas-groups-as-victim-count-rises-ransomware-in-q2-and-q3-2022

Education Sector

Cyber-attacks targeting the education sector are becoming more common due to the large amounts of sensitive data and lack of defensive resources[56]. Cybercriminals are also almost certainly aware of the increased publicity that comes with targeting the sector as attacks often make the local news and articles are popular on technology news sites. This publicity can be used to drive further sales of RaaS platforms, thus leading to higher revenue for the associated threat group and additional attacks against the sector.

APT group Vice Society has become notorious for targeting the education sector. The group uses multiple ransomwares to achieve their financial aims, including HelloKitty, Zeppelin and a new variant strain named PolyVice[57]. A full report on Vice Society can be found on the Threat Intelligence section of Quorum Cyber's website[58]. Vice Society has targeted organisations across the globe, historically in the US, UK, Spain, France, Brazil, Germany and Italy.

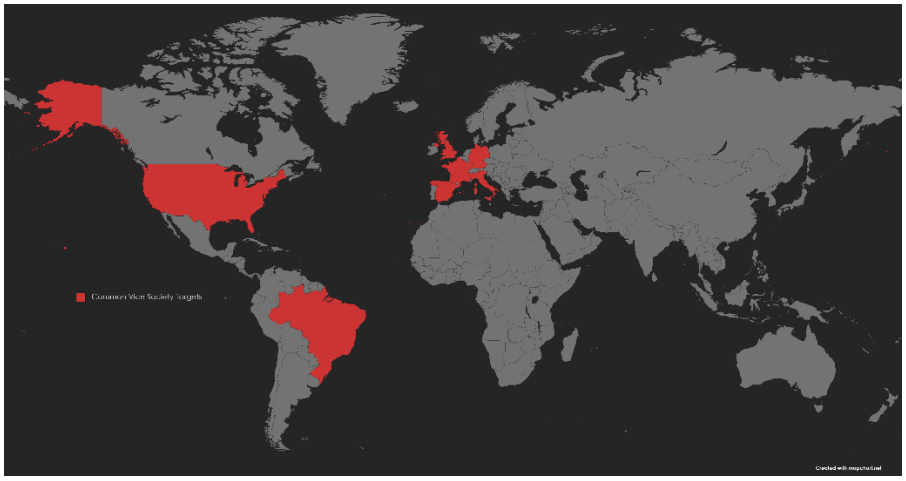


Figure 4: Historic Vice Society target locations

Higher education organisations are likely to be a target for cyber espionage and spyware, stealware and ransomware used as cover for data exfiltration. China has a history of such activities and will likely seek to continue these attacks during 2023 to further develop the Chinese education system and to exploit captured sensitive information.

[56] https://www.intelligentciso.com/2023/01/17/combatting-the-ongoing-issue-of-cyberattacks-to-the-education-sector/
[57] https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/
[58] https://www.quorumcyber.com/threat-intelligence/vice-society-attempts-to-extort-uk-school-by-posting-sensitive-files/

Public Sector

The public sector is one of the most common targets for cyber exploitation in the UK. This is likely due to complexity and, unfortunately, the lack of sufficient resources to maintain all aspects of the public estate. In 2022, UK councils were reportedly hit with up to 10,000 malicious cyber instances, daily[59]. Of these attacks, phishing campaigns, DDoS attacks and ransomware attacks stand out as the most prevalent and had the greatest impact.

Phishing

Phishing remains one of the largest, if not the largest, online threats facing UK councils and the wider public sector, with three-quarters (75%) stating that it was the most common type of attack that had been attempted against them[60] in the first half of 2022. This high percentage is likely due to the low cost associated with this attack vector, its spreadable nature and ease of implementation. For UK councils and the public sector, phishing provides the potential for lateral movement between connected systems outside of the initial attack vector.

DDoS

As reported by the risk management firm, Gallagher, DDoS attacks against UK councils were the second most reported cyber-attack type, accounting for 6% of malicious cyber instances in the first half of 2022. It is likely this trend will continue throughout 2023.

Ransomware

Public sector organisations remained a prime target for opportunistic threat actors seeking to deliver ransomware payloads in 2022. This is likely due to the previously mentioned insufficient funding to maintain a strong security posture over all endpoints and a cyber security aware workforce. Furthermore, due to the UK's support for Ukraine, Russian based threat actors, such as LockBit, are more likely to target the UK's CNI as it is unlikely to be challenged by Russian authorities[61].

In a recent and widely publicised attack, LockBit 3.0 was used to attack the Royal Mail, causing significant disruption to international services[62]. While the Royal Mail is now privately owned, it still demonstrates the targeting of UK CNI. LockBit 3.0 emerged as the most prolific ransomware in circulation in the latter months of 2022, accounting for over a third of all reported ransomware attacks globally. Ransomware attacks such as this will almost certainly continue during 2023 due to the potential for financial gain and by those who wish to disrupt the UK's CNI.

[59] https://www.openaccessgovernment.org/uk-councils-keeping-local-authorities-residents-safe-secure/147197/
[60] https://www.ajg.com/uk/news-and-insights/2022/august/uk-councils-hit-by-10000-cyber-attacks/
[61] https://news.sky.com/story/royal-mail-cyber-attack-carried-out-by-russian-linked-ransomware-gang-12785685
[62] https://www.bleepingcomputer.com/news/security/royal-mail-halts-international-services-after-cyberattack/

Energy Sector

Throughout 2022, energy sector organisations across the US and Europe remained extremely attractive targets for both criminal groups and nation-state threat actors due to their potential for financial leverage and involvement with CNI. Soaring fuel prices, driven by the ongoing conflict in Ukraine, and the subsequent rise in energy demand almost certainly put the energy sector within the crosshairs as malicious adversaries likely deemed the entities within the sector to be more willing to make ransom payments to ensure the smooth running of CNI. Russia, North Korea, Iran and China were assessed to be the greatest threats to the energy sector due to their resources, proven capability and intent to cause harm to western CNI and energy suppliers.

Since the invasion of Ukraine, Russian activity surrounding the energy sector significantly increased. This was almost certainly due to the western sanctions against the Russian state and the known dependency of European energy demands, historically provided by Russian oil and gas. Hours before the invasion of Ukraine, Russia enacted a wiper malware attack on the VIASAT European communication satellite network, resulting in multiple accounts of disruption across the region. The wiper malware used in the VIASAT attack was Acid Rain and has since been commonly attributed to the Russian APT, APT28 (Fancy Bear)[63]. Russian wiper malware attacks were prolific during 2022 and are likely to continue this trajectory throughout 2023.

Threat actors originating from China have also been linked to emerging activity towards energy sector organisations. Almost certainly due to China's ambition of becoming a global superpower, a mainstay of Chinese cyber aggression is to covertly compromise western energy, technology, and financial firms to exfiltrate data, thereby accelerating the development of their own associated sectors. The trend of China-based threat actors targeting energy sector organisations is likely to continue into 2023.

Iran also has the capability to threaten western energy sectors, should the geopolitical need arise. Despite this capability, current Iranian intentions are to limit the impact of western imposed sanctions, therefore, Iran is unlikely to conduct significant international cyber campaigns as this would only exacerbate sanctions on their own oil and gas industries.

North Korea, and by extension, the North Korean state-sponsored threat group Lazarus, has a recent history of targeting the energy sector as highlighted on 14th September 2022 in the Quorum Cyber Threat Intelligence report[64]. Targeted attacks of western finance and energy sector infrastructure, for monitory and intellectual property gain, will almost certainly continue in 2023 based on the North Korean government's requirement for additional unconventional funding, while international sanctions prevent regular cash flow.

Additionally, cybercriminals such as BlackCat ransomware group have gained notoriety for their sophistication, innovation and targeting of European energy organisations, including the oil port of Rotterdam-Antwerp and the Italian Energy Agency[65]. While this group has primarily targeted European energy companies thus far, there is a realistic possibility that they will expand and begin targeting other international firms, potentially in the UK and US. Based on the current energy crisis, it is highly likely that ransomware groups will continue to target companies within the energy sector throughout 2023.

Credential leaks may occur via multiple means, such as third-party attacks, insider threats or phishing scams. Once details have been leaked, a malicious actor can then use legitimate credentials to access a secure system and perform an opportunistic attack, delivering malware with minimal resistance. As the 2023 calendar year progresses the sale of energy sector credentials will almost certainly continue to be of high interest for any threat actor group due to the financial opportunities connected to their access.

[63] https://attack.mitre.org/groups/G0007/
[64] https://www.quorumcyber.com/threat-intelligence/energy-sector-targeted-by-lazarus/
[65] https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/