Threat Intelligence Assessment

June 2024

Ellen Hallam

Senior Threat Intelligence Analyst

Ellen.Hallam@bytes.co.uk

Intelligence Cut-off Date: **28th June 2024**
Disseminated: 1st JULY 2024

Contents

INTRODUCTION

This Threat Intelligence Assessment consists of a "Fact" section, take from various Open Sources, to explain the issue being discussed and is usually followed by an Analyst comment section, adding more detail and an Analyst Assessment section, with suggestions on what the occurrence means for us and what we might see next. Although sometimes, it is not possible, or necessary to have an analyst comment or assessment section. The monthly threat assessment seeks to summarise:

1. What key themes we are seeing
2. What threat actors are doing
3. What the new and emerging threats are this month
4. What the key risks to businesses are
5. Any *relevant* critical vulnerabilities and exploits (as vulnerabilities are *technically* not within the remit of threat intelligence)
6. The report is often structured around Geopolitical events, as natural categories, as the Cyber domain, Geopolitics and Disinformation are all interconnected.

This is currently in the "experimental" phase, so feedback would be useful.

The Probability Yardstick

To quantify language, we use the Probability Yardstick, from the Professional Head of Intelligence Assessment. It is a tool used by the UK Government to standardise the way we describe probability and has been used to ensure consistency across the different thematic areas and threats when providing assessments on how *likely* something is to occur. The yardstick is attached for information.

Professional Head of Intelligence Assessment

Probability Yardstick

Probability range	Judgement terms	Fraction range
> 0 - ≤ ≈5%	***Remote chance***	> 0 - ≤ ≈1/20
≈10% - ≈20%	***Highly unlikely***	≈1/10 - ≈1/5
≈25% - ≈35%	***Unlikely***	≈1/4 - ≈1/3
≈40% - < 50%	***Realistic possibility***	≈2/5 - < 1/2
≈55% - ≈75%	***Likely*** or ***Probably***	≈5/9 - ≈3/4
≈80% - ≈90%	***Highly likely***	≈4/5 - ≈9/10
≥ ≈95% - < 100%	***Almost certain***	≥ ≈19/20 - < 1

≈ approximately ≥ is more than or equal to ≤ is less than or equal to > is more than < is less than

THREAT TRENDS ANALYTICAL OVERVIEW:

June's Threats are significantly influenced by the geopolitical landscape, due to the number of upcoming elections and ongoing conflicts in Russia and Palestine.

Cyber events are closely linked to geopolitical trends and the volume of high-profile elections, in particular the UK, US, France and European Union Parliamentary elections.

The EU elections took place in June and the French and UK elections are due to take place this month, with US elections due by the end of the year.

The Olympics is also posing a significant threat to France, with regards to threats, but also physical threats from the Islamic State and al Qaeda.

Advanced Persistent Threats are targeting countries, not only with cyber-attacks, but also with disinformation campaigns, in an attempt to influence the electorate.

Third-party attacks have been prevalent this month, as Synnovis, a pathology services provider was targeted, to impact the NHS. Snowflake, the cloud storage provider, was also targeted by threat actors.

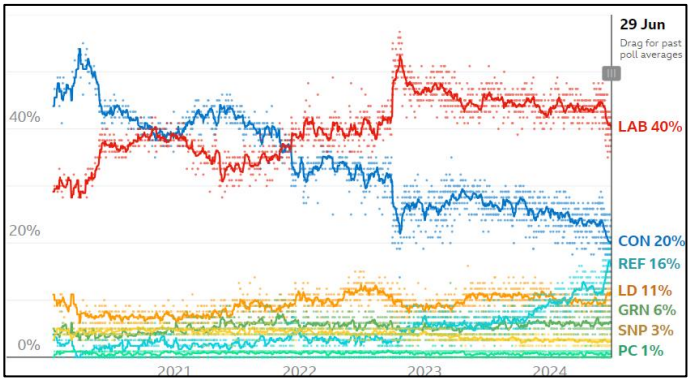
MONTHLY STATISTICS

- 75% of new Vulnerabilities are exploited within 19 days | Help Net Security
- Skybox Security's report revealed that over 30,000 new vulnerabilities emerged in 2023, with a new vulnerability surfacing every 17 minutes and averaging 600 per week. | Skybox
- 1 in 3 breaches go undetected | Help Net Security
- There have been 435 posts within the month of June | RansomWatch
- There have been 2577 posts within the year of 2024 | RansomWatch
- 97% of FTSE 100 firms suffered supply chain breaches last year | ITPro

GEOPOLITICAL THREAT TRENDS OVERVIEW:

UK

UK General Election



The UK General Election is due to take place on Thursday 4th July. The poll, taken from the BBC, shows party popularity over the last 4 years. The poll suggests the election outcome will be a comfortable win for Labour, with the Conservatives set to lose this election, after 14 years of leading the country[1].

There are numerous Cyber threats to the election with disinformation being spread and cyber-attacks being orchestrated by state-backed groups, criminals and hackers. The NCSC is tackling the risks of cyber interference at the election, by launching a person internet protection (PIP) service for high-risk individuals' and their personal devices, protecting them from cyber threats[2]. The NCSC is also working with international partners to protect civil society groups from transnational repressions and cyber threats, offering guidance and support. This can be found here: Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society | CISA.

Analyst Comment:

The UK's dispersed paper-based voting system makes significant interference difficult. However, changing the outcome of an election is a desirable effect for another nation, especially a hostile one. There is concern over the subtleties of election interference, after the Cambridge Analytica scandal in 2016 was believed to have influenced the Brexit referendum. The scandal involved the misuse of the Facebook data of 87 million people being used for advertising during elections. Although the Information Commissioner stated that Cambridge Analytica was "not involved" with the outcome of the Brexit referendum, it raises significant concerns about privacy and data use, alongside what can influence the outcome of an election[3].

Analyst Assessment:

It is almost certain that Russian, Chinese and North Korean affiliated organisations, whether nation-backed, or part of an anti-West hacking group, will be attempting to assert influence over the outcome of the election and destabilise the UK. Cyber-attacks and disinformation are highly likely to be the most prominent methods and recent advances in technology have increased the credibility of deepfake video and audios, which are almost certain to influence voters with false information. The UK has already sanctioned China for cyber-attacks on UK infrastructure by Chinese-backed threat actors, so cyber-attacks on key UK infrastructure are highly likely to continue.

Recommendations:

1. Check the source of everything you read to do with the election. Is it from a reputable source?
2. Consider what your organisation can do to support the NCSC in raising awareness of disinformation campaigns and both the benefits and challenges of AI.

[1] UK election poll tracker | The Economist
[2] https://www.ncsc.gov.uk/pdfs/news/ncsc-support-those-high-risk-cyber-attacks-ahead-election.pdf
[3] Cambridge Analytica 'not involved' in Brexit referendum, says watchdog - BBC News

Scattered Spider ringleader arrest

The alleged ringleader of the Scattered Spider cybercrime group, a 22-year-old man from the United Kingdom, was arrested in Spain. The arrest was the result of an investigation that began in May 2023 after the FBI's Los Angeles branch requested information on the man. The suspect was arrested at Palma airport on 31st May as he tried to board a private flight to Naples[4].

Analyst Comment:

Scattered Spider is suspected of hacking into Twilio, LastPass, DoorDash, Mailchimp, and nearly 130 other organisations over the past two years. The group is known for its SIM-swapping attacks and ransomware campaigns. The suspect allegedly had control of Bitcoins worth $27 million[5]. Some members of the group have reportedly aligned their activities with the RansomHub ransomware group, which is a spinoff of the ALPHV/BlackCat group[6]. The recruitment drive appears to be an effort to capitalise on the situation caused by the collapse of the ALPHV/BlackCat Ransomware as a Service (RaaS) operation, which left affiliates without payment infrastructure.

Analyst assessment:

Although a win for law enforcement, It is highly unlikely the arrest of one individual will cause great impact to Scattered Spider, due to its diffused structure and continual evolution of tactics. Scattered Spider is highly unlikely to be tightly organised, which means individuals within the group can adapt or get new roles without effort or disruption.

Law enforcement arrests are almost certain to sow distrust within the group, especially as trust and anonymity play vital roles in being in a hacker organisation. Irrespective, it is almost certain Scattered Spider will continue to be a threat.

An ALPHV/Blackcat/Scattered Spider joint operation is highly likely to pose a significant threat to the Cyber world. Recruitment of some of the best black hat hackers, combined with a successful malware variant, skilful social engineering tactics and a plethora of data exfiltration tactics could mean the new collective is capable of successfully targeting critical infrastructure and other much larger organisations and holding them to ransom.

Recommendations:

1. Does your organisation know which threat actors are most likely to target them? Once you have identified this, Mitre Att&ck is one of the techniques which can be used to conduct analysis on how threat actors might attack your organisation and can help you "blue team" to identify what measure you can input to prevent threat actors from accessing your environment.

2. How good is your security posture? Have you got a risk assessment in place? Consider how prepared your organisation is and what you might do if you experience a ransomware attack.

[4] Scattered Spider Boss Cuffed in Spain Boarding a Flight to Italy (darkreading.com)
[5] Scattered Spider arrest in Spain unlikely to stop cybercrime group | CSO Online
[6] Alleged Scattered Spider ringleader taken down in Spain after law enforcement crackdown | ITPro

Billiceray school Cyber attack

The Billericay School in Essex, UK, suffered a significant cyber-attack during half term. The school's systems were compromised despite having industry-standard firewalls, firmware, and malware security in place. The attack resulted in all the school's IT systems being compromised and inaccessible due to a complex encryption. The names, addresses, and medical notes of children may have been accessed by criminals and contact details of parents and carers could also have been obtained.

The school was closed to several year groups on certain days. The head teacher, Patrick Berry, stated that they were doing all they could to strengthen their defences against cybercrime. The school was working with Action Fraud to investigate the cyber-attack[7].

Analyst Comment:

The Information Commissioner's Office reported 347 cyber incidents in the education and childcare sector in 2023, a 55% increase from 2022[8].

Analyst Assessment:

Threat actors are highly likely to target Education for the sensitive information stored. It is almost certain cyber-attacks on educational institutions will continue to rise, as Incidents like this also suggest it likely that normal security measures, such as firewalls, firmware and malware security are no longer enough to mitigate against the threats posed by ransomware actors.

[7] https://www.bbc.co.uk/news/articles/c2vv141pv8po

[8] https://www.nprillinois.org/2024-03-11/one-reason-school-cyberattacks-are-on-the-rise-schools-are-easy-targets-for-hackers

NHS & Synnovis fall out

The Synnovis cyber-attack was a significant incident that affected several hospitals in London. The attack occurred on 3rd June, with Qilin, a Russian-affiliated ransomware group targeting Synnovis, a pathology services provider[9]. The attack resulted in all of Synnovis' IT systems being compromised and inaccessible due to a complex encryption[10]. This led to interruptions to many pathology services, with the attack being declared as a critical incident, with operations cancelled and emergency patients diverted elsewhere. The Qilin gang have demanded $50 million in ransom, in exchange for a decryption key. Synnovis is working with investigators to identify what happened and what information the ransomware gang has. Kings College Hospital, Guy's hospital and St Thomas' hospital were all affected, causing severe O Positive and O Negative blood shortages.

Analyst Comment:

The FBI, NCA, and NCSC are investigating the incidents, with efforts to remove leaked data and track down the criminals, despite the challenges posed by Qilin's potential ties to Russia[11].
This is another supply chain attack, showing an emerging TTP from threat actors, who research their intended victim and identify the organisations in their infrastructure who may be a more viable target.

Qilin have shared almost 400Gb of private information on their dark website[12]. A spokesperson for QIlin, speaking to The Register, stated that their goal was to "cause a healthcare crisis at London Hospitals." They targeted companies whose management was directly, or indirectly affiliated with the political elites of a particular country, through politically motivated attacks[13]. They are known for targeting the healthcare and education sectors not because of politics but because of the reliance these sectors have on uptime and the sensitivity of the data they hold, and some experts suggest they are more opportunistic[14].

Analyst Assessment:

Since the Wannacry attack in 2018 and the Covid-19 pandemic, the NHS has had more funding, but smaller, less wealthy organisations are far less likely to have funds available to afford to spend more on a suitable level of Cyber security. Events like this, which are well-publicised and high impact, make attacks like this almost certain to continue, as they provide threat actors with lucrative targets for extortion, by endangering patient lives.

Recommendations:

There are many ways Organisations can look to mitigate the risk posed by Ransomware. Knowledge of threats, what they target and how they target infrastructure is invaluable, as is having a suitable SOC, to catch-and prevent breach attempts as they happen. Things to consider include:

- Creating an Asset inventory. You can use this to identify all third-party services and vendors you work with to enable you to see the data they have access to.

[9] Cyber-attack on London hospitals declared critical incident - BBC News
[10] Cyber Attack Information Centre | Synnovis
[11] UK and US cops put Qilin ransomware crims in the crosshairs • The Register

[12] https://www.independent.co.uk/news/uk/nhs-data-london-bbc-national-crime-agency-b2568028.html
[13] https://www.independent.co.uk/news/uk/nhs-data-london-bbc-national-crime-agency-b2568028.html
[14] https://www.theregister.com/2024/06/20/qilin_our_plan_was_to/

- Creating a Risk register. Rank and prioritise your risks. Not all third parties present the same level of risk, so you can prioritise these, based on the sensitivity of the data they handle and their level of access to your systems.
- Ensuring employees have the highest level of training and awareness on risks to the business, especially phishing links, as these are among the most common initial access vectors.
- Ensuring you have an Incident Management Plan, which will help you to respond to security incidents, including those that involve third parties.
- Looking to define and track metrics too, to measure the effectiveness of your third-party practices. You could use automated tools to monitor this.
- Ensuring you are continuously testing and monitoring security controls, using Penetration Testing as well as Red and Blue Teaming to continually appraise your security measures.

Election interference through Tiktok

The BBC conducted a project to investigate the content promoted by social media algorithms and found that young voters on TikTok are being exposed to misleading and divisive content[15]. Fake videos involve party-leaders, misinformation and clips littered with abusive comments. The content is being shared by many people, from students and political activities to comedians and anonymous bot-like accounts. Videos include unfounded rumours about Rishi Sunak and Sir Keir Starmer and misleading claims about Sunak's national service pledge for 18-year-olds, suggesting young people will be sent to war zones, which have amassed thousands of views. Although some videos are described as satirical, or parodies in captions, it is clear users are confused about which claims are factual. Tiktok told the BBC it is increasing investment in countering misinformation for the UK General election, by adding fact-checking experts to existing resources and employing AI-labelling technology. The investigation was part of a project assessing what content is promoted to different types of people.

Analyst Comment:

Social Media is by far the best way to reach voters, especially young voters, who tend to access the platform more than their older counterparts. Disinformation has always been around in some form or other, for example, with some newspapers taking a more right-wing, or more left-wing slant on events. However, the issues here arise with the sheer volume of content available and subtle deviation from the truth, meaning small nuances are believed and not questioned. This highlights the importance of media literacy and critical thinking when engaging with content on social media platforms. It's always good to verify information from multiple reliable sources before believing or sharing it.

Analyst Assessment:

Election interference is almost certain to continue until both the US and UK elections have passed. It is difficult to assess how successful interference will be, as it is difficult to quantitively measure how likely the electorate is to be influenced and how significantly this will impact the results of an election.

Recommendations:

1. Fact-check and correlate your sources.
2. Trust your senses – if something doesn't feel right, it's probably not.
3. Keep up with mainstream news, from known and trusted news providers.

[15] https://www.bbc.co.uk/news/articles/c1ww6vz1l81o

Snowflake attack

The Snowflake attack was a significant cybersecurity incident that targeted customers of the cloud storage provider, Snowflake Inc. Details are still emerging, but as many as 165 customers have been compromised, including companies like Ticketmaster and Advanced Auto Parts, were among the first identified victims. Others include QuoteWizard and Live Nation[16].

The attackers obtained login credentials through information-stealing malware. These credentials were primarily obtained from multiple infostealer malware campaigns that infected non-Snowflake owned systems[17].

The attackers exported a significant volume of customer data from the respective Snowflake customer instances, including full names, addresses, phone numbers and partial credit card numbers for 560 million Ticketmaster customers.

None of the affected accounts used Multifactor Authentication (MFA), which requires users to provide a one-time password or additional means of authentication, besides a password.

The group conducting the attacks, UNC5537, began to extort many of the victim's directly, and is actively selling stolen data on the dark web.

Analyst Comment:

UNC5537 are a threat actor group identified by Mandiant. It is important to note Snowflakes' enterprise environment has not been breached, but instead, customer credentials have been compromised.

Analyst assessment:

There is a realistic possibility that UNC5537 are not a new group, but a mix of individuals from other threat groups rebranded, as this has occurred in the past. The attack appears more sophisticated and systematic in comparison to other attacks, with multiple customer breaches, indicating a likely level of sophistication and organisation.

It is likely that this incident will affect trust between third parties and likely Snowflake, as well as breached customers, may face regulatory and legal fines for customer's whose data was compromised, alongside the cost of implementing enhanced security measures.

Recommendations:

This incident underscores the importance of robust cybersecurity measures, including the use of multifactor authentication and regular monitoring of systems for signs of unauthorised access. It's also a reminder of the potential risks associated with third-party vendors and the need for businesses to carefully manage and monitor these relationships.

The Snowflake attack has several potential long-term consequences for both Snowflake and its customers:

[16] https://www.yahoo.com/news/snowflake-breach-tells-us-passwords-080019489.html
[17] https://arstechnica.com/information-technology/2024/06/hackers-steal-significant-volume-of-data-from-hundreds-of-snowflake-customers/

US

Copycop Russia - US elections

CopyCop is a network of websites that uses large language models (LLMs) to rewrite and publish stories on a range of contentious issues[18][1]. The operation involves plagiarising, translating, and editing content from legitimate mainstream media outlets[19]. By employing prompt engineering techniques, the network tailors this content to resonate with specific audiences, injecting political bias that aligns with its strategic objectives. This network is reportedly linked to Russia and its activities are seen as a form of propaganda. CopyCop seek to target divisive issues with a Pro-Russian stance.

CopyCop churned out 19,000 deceptive posts in a month[20]. The content from CopyCop is also amplified by well-known Russian state-sponsored actors such as Doppelgänger and Portal Kombat. Also, it boosts material from other Russian influence operations like the Foundation to Battle Injustice and InfoRos, suggesting a highly coordinated effort[21].

Analyst Comment:

Please note that there's also a tool named CopyCop which is unrelated and used for creating compliant marketing copies.

AI is rapidly speeding up the rate in which influence actors like CopyCop can manipulate emerging narratives when targeting specific audiences for a political purpose[22].

Russia's ongoing disinformation campaigns are not just aimed at the US, although they seek to damage President Joe Biden and the Democrats to weaken U.S. military aid to Ukraine and support for NATO. France and the UK are also targets, and there have been reports on Russia's involvement with the Belarus General election. Despite automation, the network has made operational security mistakes, including leaving AI prompts in published articles. These were not subtle. More than 90 French articles, for instance, were altered with the following instruction in English: "Please rewrite this article taking a conservative stance against the liberal policies of the Macron administration in favour of working-class French citizens[23]."

Analyst Assessment:

It is likely CopyCop is a Russia government-aligned influence network, despite CopyCop taking steps to actively mask their origin.

It is likely the spread of disinformation will distort public understanding of important issues. This is likely to lead to polarisation, meaning people struggle to find common ground. In the long term, there is a realistic possible this can cause a threat to democracy

It is likely to erode trust in legitimate news sources, as people may begin to struggle to distinguish between real and fake news.

[18] https://ground.news/article/a-russia-linked-network-uses-ai-to-rewrite-real-news-stories
[19] https://www.recordedfuture.com/russia-linked-copycop-uses-llms-to-weaponize-influence-content-at-scale
[20] A Russia-linked network uses AI to rewrite real news stories (economist.com)
[21] Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale (recordedfuture.com)
[22] Russia's 2024 election interference has already begun (nbcnews.com)
[23] A Russia-linked network uses AI to rewrite real news stories (economist.com)

It is almost certain that pro-Russia propaganda campaigns are now common across all major social media platforms, with efforts to exploit US societal divisions.

Disinformation is a significant risk to the world over, as the fine line between fact and truth is becoming increasingly blurred due to influence operators highly likely seeking to evolve their tactics to persuade audiences. This is almost certain to continue, and worsen, as the US election approaches.

Note: The analyst has not used "misinformation, as the distinction between ***misinformation*** *and* ***disinformation*** *lies in intent:*

1. ***Misinformation****: This term refers to* ***false information*** *that spreads* ***unintentionally****, regardless of whether the sharer knows it's wrong.*
2. ***Disinformation****: On the other hand, disinformation is* ***deliberately deceptive false information****. It's created with the* ***intent to mislead*** *others, often covertly.*

Recommendations:

It's important for individuals and institutions to be aware of these potential implications and to take steps to promote media literacy, fact-checking, and critical thinking. It's also crucial for tech companies and policymakers to work together to address the challenges posed by AI-powered disinformation networks.

Countering foreign disinformation campaigns effectively requires a multi-faceted approach. As an organisation, you can:

1. Promote news literacy to help people distinguish between real and fake news.
2. Invest in tools to identify fake news and avoid supporting organisations who profit from fake news.
3. Support high-quality journalism to build trust.
4. Improve your organisations online accountability.
5. Continue to build Government-Private sector partnerships
6. Leverage knowledge from other countries and organisations.

EUROPEAN UNION

Parliamentary elections summary:

The Centre-Right European People's Party (EPP) remains the largest group, with hard-right groups also gaining seats. The centre-left Socialists and Democrats (S&D) and the liberal Renew Europe group secured 403 lawmakers - around 56% of all seats - between them. They sit in groups based on political affiliations, which are important for parliamentary debates and EU funding. There may need to be some changes in group alignments before the parliament reconvenes, especially among hard-right groups[24].

The European Union elections have caused President Macron, who was re-elected on the 24th April 2022, beating Right-Wing Marine Le Pen, has called an election in France, which will happen on the 30th June and 7th July. This election will elect the 577 members of the National Assembly, the lower house of the French parliament.

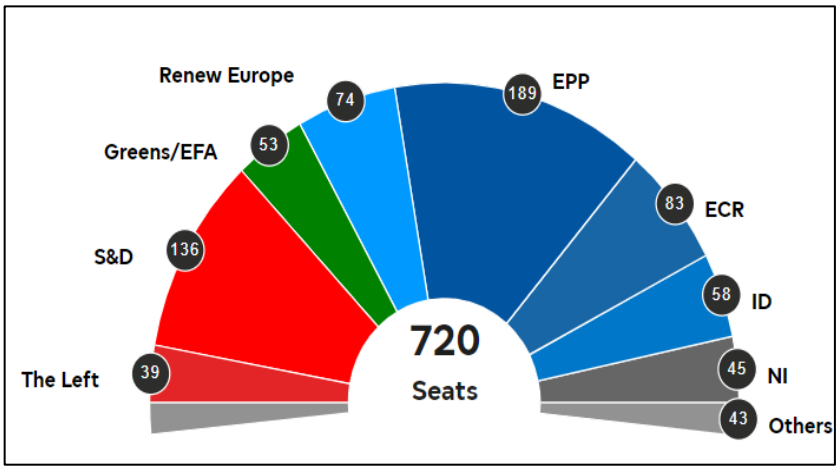


Figure 1: European Parliament 2024-2029 Provisional results

Analyst Comment:

The EU parliament writes legislation and oversees the bloc's annual budget, which totalled EUR 185.6 billion in 2023. It also approves candidates for some of the top positions within the wider EU bureaucracy, such as President of the European Commission. Due to sluggish post-pandemic economic growth and concerns over security, Eurosceptic parties (those opposed to increasing the powers of the EU) made significant electoral gains. At the same time, the main centre-right alliance won a large number of seats, maintaining its historical dominance of parliament. In the cyber realm, the EU election represented a key target for state-backed threat actors, particularly Russian-linked groups. The campaign season was already impacted by several online influence campaigns, and there were digital disruptions on the days of voting[25].

Analyst Assessment:

The main sources of Cyber threats to the election highly likely originated in anti-Western countries, like China, Iran and Russia. It is highly likely the aim of cyber interference was to disrupt the voting process, influence public opinion and undermine the legitimacy of the election.

[24] European election 2024: Live results and analysis (reuters.com)
[25] zerofox.com/advisories/23678/

IRELAND

Critical Infrastructure Cyber attacks

In June 2024, Ireland experienced several cyber-attacks, as part of orchestrated attacks on EU member states. The NCSC became aware of a series of low impact DDoS attacks targeting several websites in Ireland. This included the voting registration site, voter.ie, although the impact was minimal[26].

Like other EU states, Russian-based hackers have targeted several Irish websites in the lead-up to the local and European elections. The attacks aimed to disrupt online services and influence public opinion. The hackers employed various tactics, including distributed denial-of-service (DDoS) attacks and phishing schemes[27].

The attacks did not significantly disrupt the functioning of the websites due to the preparedness of the victims.

Analyst Comment:

The websites of the Houses of the Oireachtas, Transport for Ireland and Irish Rail were also impacted.

Analyst Assessment:

The hacker group, HackNet is believed to be linked to Russian Intelligence and have also targeted other EU countries.

It is likely Ireland, and the EU may be less at risk, due to the upcoming US/UK General elections, which is highly likely to switch focus away from Ireland and the EU, over to the UK until 4th July and then the US until the election finishes.

[26] https://www.rte.ie/news/2024/0608/1453744-irish-websites-cyberattacks/
[27] https://www.hlb.ie/hlb-cyber-news-insights-june-2024/

FRANCE:

Threats to the Paris Olympics

The Paris Olympics, which will run from 26th July to 11th August 2024, are already being targeted by both physical and cyber threats:

Physical threats: French security authorities foiled a plan to attack football events during the Olympics. An 18-year-old man from Chechnya was arrested on suspicion of planning an attack targeting soccer events that would be held in the city of Saint-Etienne. The planned attack was to target spectators and police forces. The suspect wanted to attack the Olympic events "to die and become a martyr"[28].

Islamic State: Islamic State Supporters are continuing to promote unmanned aerial vehicle (UAV) attacks targeting sporting events for the Union of the European Football Associations (UEFA) Championships, which have been happening throughout June, and the Olympics.

Cyber Threats: The 2024 Paris Olympic Games are facing an “unprecedented level” of cyber threats. Organisers have partnered with major technology companies and government agencies to mitigate these threats. The Olympic Games have long been a target for cyberattacks by organised crime groups as well as state and non-state actors given the global and high-profile nature of the events[29]

Olympics with Disinformation: Researchers at Microsoft have observed Russian threat actors, including “Storm-1679” and “Storm-1099”, ramp up disinformation campaigns to target France. The campaign aims to besmirch the International Olympic Committee (IOC) while creating an impression of potential violence disrupting the international event. Storm-1679 released a feature-length film, Olympics Has Fallen, using artificial intelligence (AI) to impersonate Tom Cruise and discredit the IOC. Additionally, Storm-1679 has been disseminating false videos to incite fear of violence at the Games, while Storm-1099 has amplified anti-Olympics messaging through multiple fake news sites[30].

Russia has been targeting Americans travelling to the Paris Olympics with fake CIA videos, which is part of a broad disinformation campaign[31].

Analyst Comment:

The French Government has raised the Country’s terrorism threat assessment system (Vigipirate) to the highest level and security is therefore at the highest possible level, to mitigate the probability and impact of an attack.

Analyst Assessment:

Heighted security measures are highly likely to reduce the risk (likelihood and impact) of a violent extremist, or terrorist attack, especially from Islamic State and Al Qaeda supporters, who almost certainly intend to target the Paris Olympics.

Reports of arrests and foiled attack are almost certain to have a psychological impact on attendees, meaning further reassurance and constant security presence, across the city, will be required 24/7.

[28] https://apnews.com/article/paris-olympics-st-etienne-foiled-plot-b802119bfa66922c774573acdac37247
[29] https://apnews.com/article/paris-olympics-st-etienne-foiled-plot-b802119bfa66922c774573acdac37247
[30] How Russia is trying to disrupt the 2024 Paris Olympic Games - Microsoft On the Issues
[31] https://www.msn.com/en-us/news/world/russia-targets-americans-traveling-to-paris-olympics-with-fake-cia-video/ar-BB1ox4Ss

Event Organisers will almost certainly be observing online forums and messaging applications used al-Qaeda and IS to identify potential attack vectors and suggest targets (although, judging by recent IS publicity campaigns, most famous landmarks, including Big Ben are being listed as targets.)

It is highly likely that hacktivists, or criminal groups seeking attention to profit, will cause the majority of disruptions for the Olympics, likely seeing to exploit the pressure facing Paris, as host city, to extort ransomware payments from organisations in the government, hospitality, transportation, logistics or healthcare industries.

Olympic-themed phishing lures and scams will almost certainly target businesses and people attending the games.

State actors will likely use espionage and influence operations and there is a realistic possibility these will make use of Olympic-themed lures, or infrastructure to gather information on targets. The Iranian Government is likely to conduct Distributed Denial of Service attacks, website defacement and potential wiper malware, disguised as ransomware. However, it is also likely Geopolitical developments could shift the threat landscape to make a significant event more likely, such as France aiding Ukraine in resisting Russia, with lethal aid, which could trigger an escalation.

RUSSIA/UKRAINE

Russia prepares a Proxy War against NATO

Russian attacks on Ukrainian positions near the strategically important town of Chasiv Yar continue relentlessly. These assaults disrupt troop rotations and supply deliveries for Ukrainian forces[32]. This comes after Western Countries promised more weapons supply to Ukraine over the past weeks.

Russia has targeted Kharkiv to divert Ukrainian forces from Donetsk and create a buffer zone against cross-border attacks. In the past 24 hours, they launched 42 glide bombs in the Kharkiv region, to strike civilian targets, including buildings and energy infrastructure.

The International Criminal Court issued arrest warrants for former Russian Defence Minister Sergei Shoigu and military chief of staff Gen. Valery Gerasimov for alleged war crimes related to attacks on civilians[33].

Lieutenant General Igor Kolesnikov and Retired Major General Vyacheslav Kruglov wrote in the monthly Ministry of Defence of the Russian Federation magazine that Russia is preparing a new proxy war against NATO.

There have also been reports of an incident involving an oil storage depot in Belgorod, a Russian city just north of Ukraine. According to these reports, Russia accused Ukraine of attacking the depot with two Ukrainian helicopters. Ukraine's top security official, Oleksiy Danilov, denied that Ukrainian forces were behind the attack[34]. The incident has reportedly affected peace talks.

In a separate incident, Ukrainian drones reportedly targeted the Novoshakhtinsky petroleum plant in the Rostov region and an oil depot in the Starooskolsky city district of the Belgorod region. The Novoshakhtinsky petroleum plant is the largest supplier of petroleum products in the south of Russia and the only oil refinery in the Rostov region[35].

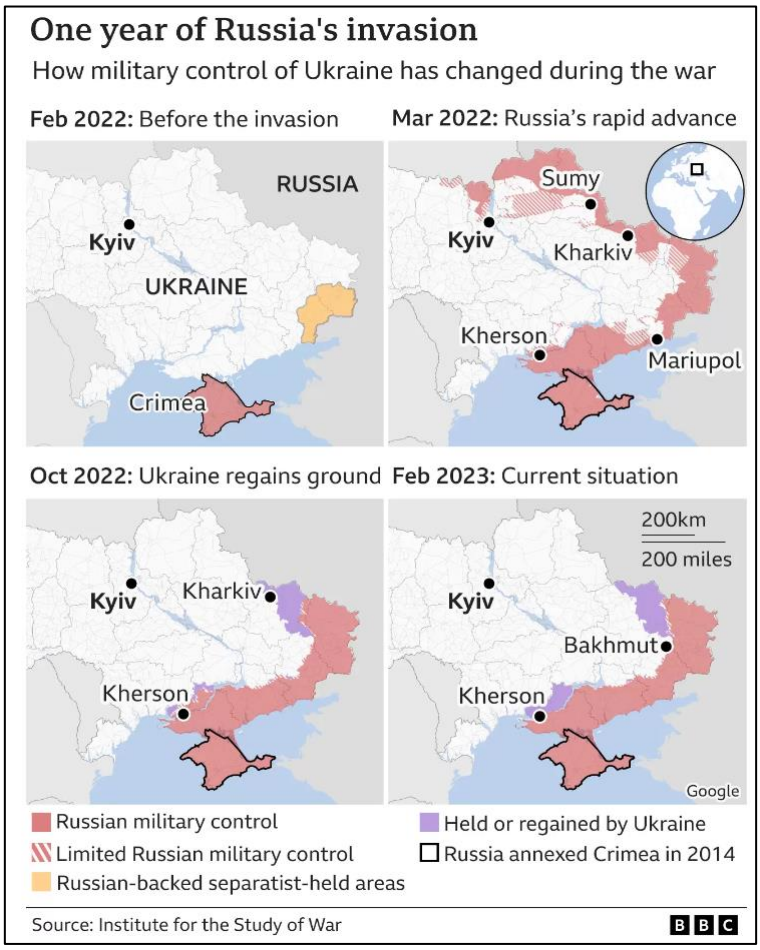
The Department of Treasury (USDT) has issued more than 300 additional sanctions against Russia and entities enabling sanctions evasion. This also targets economic interests in Turkey and China to discourage countries from engaging in commerce with Russia. Russia in turn will continue to exploit US economic measures to promote and speed up de-dollarisation.

Analyst Comment:

Putin initially aimed to quickly take Kyiv and depose Ukraine's government but faced humiliating retreats and failed to achieve a swift victory. The war has become a protracted conflict, with a front line of 850km, resulting in limited territorial gains and heavy casualties. Despite military setbacks and international sanctions, Putin maintains control in Russia, but his international authority has been damaged[36].

The image below, also taken from the BBC, shows the state of territory controlled by Russia and Ukraine and how this has changed over the last 1.5 years of war:

[32] Russia keeps up pressure on the front line as Ukraine gets a boost from Western military aid | AP News
[33] https://apnews.com/article/russia-ukraine-war-donetsk-73646205f876a1819b07ab5bc0742ad9
[34] https://www.bbc.com/news/world-europe-60952125
[35] https://www.bbc.com/news/world-europe-60952125
[36] Has Putin's war failed and what does Russia want from Ukraine? - BBC News



Analyst Assessment:

The article is almost certain to indicate Russia's perception that it is under constant attack from the US and NATO. This is almost certain to drive Russia's foreign policy aims and objectives.

It is highly likely Russia are targeting Ukraine's electricity supply to weaken morale and hinder Ukraine's weapon industry.

Russia's increased offensive on the front line is highly likely to capitalise on their military advantage before Western weapons reach Ukraine's front line and even the capability of Ukraine.

It is highly likely, with more weaponry and equipment, Ukraine will be able to push Russian troops back towards Russia, which is likely to explain why Russia is so opposed to further Western intervention.

CHINA

Tensions between the US and mainland China remained a key concern.

China's military presence in the South China Sea, technological advancements, and trade tensions contributed to geopolitical strains[37].

Empire Dragon, a Chinese influence network, tried to hijack hashtags related to the Tiananmen Square massacre anniversary with content about George Floyd's death anniversary. The aim was to distract from anti-CCP sentiment and target the US. The operation was poorly executed and used YouTube videos with controversial clips.

China's Change 6 mission's success has been overshadowed by a misinformation campaign questioning NASA's Apollo moon landing. The US and China are in a space exploration race, with China planning a crewed lunar mission by 2030 and the US aiming for a 2026 moon landing with Artemis 3. Chinese social media is rife with conspiracy theories about the US moon landing, gaining traction among millions of followers[38].

President Biden and President Xi held a call to manage tensions, discussing cooperation on climate change and narcotics, but disagreed on Taiwan and economic issues. Biden reaffirmed support for Taiwan and freedom of navigation in the South China Sea, while Xi warned against US interference, viewing it as a "red line." Xi criticized US sanctions on China, stating they suppress China's economy and technology, and warned against suppressing China's development. Upcoming diplomatic events, including Taiwan's presidential inauguration, could impact US-China relations[39].

Analyst comment:

Tensions with China and the US have been strained, due to both countries competing for global influence, in areas like trade, technology and military power[40]. Trade tensions, tariffs and disputes over intellectual property rights have strained relations. The US is concerned over China' Military expansion in the South China Sea, as well as its support for Russia over the Ukraine conflict. China continues to view US support for Taiwan as a challenge to its sovereignty and disinformation campaigns continue to fuel distrust.

Analyst Assessment:

The spread of misinformation could likely harm US-China space diplomacy and international relations, highlighting the need for accurate information and cooperation.

The spread of disinformation and influence operations, especially using the highly politicised George Floyd incident, in almost certain to create significant anti-Chinese sentiment, which is highly likely to further impact the already strained relationship between the US and China.

[37] https://www.spglobal.com/en/research-insights/market-insights/geopolitical-risk
[38] 'Americans didn't land on the Moon': How China is fuelling misinformation war against US - Times of India (indiatimes.com)
[39] Biden and Xi discuss US-China cooperation and conflict - BBC News
[40] https://apnews.com/article/us-china-blinken-wang-yi-8c1c453df3afbd6ec87ced0c8d618064

NORTH KOREA

Moonstone Sleet new targeting

A newly identified North Korean APT, labelled Moonstone Sleet, by Microsoft, has expanded its distribution of malicious node package manager (npm) code to public repositories, posing a threat to the software supply chain by poisoning open-source code repositories, such as Github[41].

Analyst Comment:

Moonstone Sleet is a North Korean threat actor that Microsoft has recently identified. It combines techniques used by other North Korean threat actors with unique attack methodologies to engage in financial and cyberespionage operations.

Moonstone sleet sets up fake companies and job opportunities to engage with targets, uses trojanised versions of legitimate tools, creates a malicious game, (DeTankWar) and deploys custom ransomware, called FakePenny.

Moonstone Sleet initially overlapped TTPs with another North Korean group, known as Diamond Sleet, but has since established itself as a threat actor with its own infrastructure[42].

Analyst Assessment:

Moonstone Sleet 's quick expansion of techniques is insightful, but indicative of the growing risk to third-party and the software supply chain, as third-party attacks affect all users of the compromised software and can have widespread consequences for government, critical infrastructure, and private sector software customers.

North Korea is highly likely to target any organisation which provides financial gain or enables espionage. They are highly likely to continue to target organisations in the software, information technology, education and defence industrial sectors.

[41] North Korea's Moonstone Sleet Widens Distribution of Malicious Code (darkreading.com)
[42] https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

PAKISTAN

Terror Attacks in Jammu and Kashmir, India

A series of terror attacks in India's Jammu and Kashmir territory killed 12 people and injured dozens between June 8 and 11, 2024. The attacks targeted Hindu pilgrims and security forces and were blamed on Pakistan-backed militants. The violence came after India's election and amid claims of reduced militancy in the region. Further attacks and protests are possible[43].

Meanwhile, Cisco has identified Operation Celestial Force, a campaign by Pakistani-Nexus threat actors, active since at least 2018, targeting individuals in the Indian subcontinent with malware like GravityRAT and HeavyLift.

Malware is delivered through spear phishing and social engineering, to Windows, Mac or Android, via malicious documents and links on social media. Originally a Windows-based malware, GravityRAT expanded to Android devices around 2019, with continuous capability enhancements[44].

The adversary group uses two malware families, GravityRAT and HeavyLift, to spy on defence, government, and technology targets. The attackers use a tool called GravityAdmin to control the malware campaigns and steal data from the victims.

Analyst Comment:

The Kashmir conflict is a territorial dispute primarily between India and Pakistan, with additional involvement from China. The conflict is deeply rooted in society, dating back to the partition of India in 1947, where both India and Pakistan claimed both Jammu and Kashmir. The conflict escalated into three wars between India and Pakistan, along with other armed skirmishes. Tensions persist, with violence flaring up periodically, when something changes. Both sides now have nuclear capability.

Analyst Assessment:

The two sides currently exist in a fragile ceasefire, albeit with frequent terror attacks. This is highly likely to continue, unless something significant disrupts this. There is a realistic possibility, the targeting of Indian organisations, by Pakistani cyber hackers would change the status quo and cause a geopolitical disaster.

Recommendations:

1. Educate users on Cyber hygiene
2. Implement defence-in-depth models to protect against targeted attacks
3. Consider suitable tooling to support with protecting against threats.

[43] Jammu and Kashmir: 10 Hindu pilgrims killed in bus attack in Reasi - BBC News
[44] Operation Celestial Force employs mobile and desktop malware to target Indian entities (talosintelligence.com)

ISRAEL/GAZA

Humanitarian situation worsens

A UN report that accuses both Israeli and Palestinian groups of committing war crimes in Gaza. The report lists the specific crimes that each side is allegedly responsible for, such as starvation, murder, torture, and hostage-taking. The document also discusses the strategic implications of the report, such as the difficulty of peace talks and the impact on global public opinion[45].

Analyst Comment:

As of the latest reports, the situation in Gaza remains dire. The UN's World Food Programme warns of food and water shortages due to the Israeli siege. Gaza's only power station has run out of fuel, and the territory relies on generators. However, Israel maintains that its blockade will continue until Israeli hostages are released. Additionally, heavy fighting persists in Jabalia (northern Gaza) and Rafah (southern Gaza), with Palestinian fighters resisting Israeli troops. Overcrowding in UN facilities poses health risks for the displaced population[46].

There have been two ceasefire resolutions offered; the latest, 2735, proposes a comprehensive three-phase ceasefire deal, which includes an immediate ceasefire, hostage release and humanitarian assistance.

Furthermore, Arid Viper, a Hamas-linked APT group, has been observed targeting users across Egypt and Palestine with AridSpy Android spyware distributed via Trojanised messaging apps, which collect data and can be used by threat actors to conduct targeted surveillance, track physical movements and monitor communications, posing a personal security risk.

Analyst Assessment:

Although there have been calls for a ceasefire across the world, it is highly unlikely Israel will consent to a ceasefire until all Israeli hostages have been returned to Israel and equally unlikely Hamas will return the hostages until Israel agrees to a ceasefire. The rest of the world is almost certainly going to have to continue supporting Gaza with crucial humanitarian aid.

The ability of Iranian threat actors to record audio and take pictures is highly likely to enhance their capability for espionage, potentially enabling blackmail, extortion, or further infiltration into sensitive networks and/or personal lives.

[45] Israel, Hamas accused of war crimes in new UN report - BBC News
[46] https://www.bbc.com/news/live/world-middle-east-67073970

IRAN

Emerald Divide Influence Network Exploits Disagreements

Emerald Divide targets the Israeli-Palestinian conflict and promotes a pro-Palestinian agenda. The operation uses a small network of online accounts to spread disinformation and propaganda, create divisions among different groups, undermine the credibility of Israeli leaders, and encourage actions such as protests or boycotts. Emerald Divide uses techniques such as amplifying existing narratives, motivating to act, and dividing communities to achieve its goals.

Emerald Divide uses modern digital tools such as AI-generated deepfakes and a network of strategically operated social media accounts. These accounts target diverse and often opposing audiences, effectively stoking societal divisions and encouraging physical actions such as protests and the spreading of anti-government messages.

The operation also involves serious cybersecurity threats like the harvesting of personally identifiable information and doxing Israeli officials. Its continued evolution and adaptability make it a persistent security threat, with future operations likely focusing on exploiting other contentious issues within Israeli society[47].

Analyst Comment:

Emerald Divide harvests personally identifiable information and engages in doxing of Israeli officials[48].

Analyst assessment:

As with any other sophisticated Disinformation/Influence campaign, the primary goal of Emerald Divide is almost certainly to manipulate Israeli society by amplifying ideological divisions and diminishing trust in the Israeli government.

The current political situation is almost certain to enable Iran to capitalise and rapidly adapt to on strong emotional reactions to the Israel-Hamas conflict.

There is a realistic possibility leveraging AI-generated deepfakes and a network of strategically operated social media accounts will encourage and insight physical actions, such as protests and spreading anti-government messages.

Recommendations:

1. Governments, technology firms, and security researchers should collaborate to dismantle the campaign's infrastructure.
2. Public awareness and education are vital in preventing unwitting engagement with Emerald Divide.

[47] https://www.recordedfuture.com/iran-aligned-emerald-divide-influence-campaign-evolves-to-exploit-israel-hamas-conflict
[48] Iran-Aligned Emerald Divide Influence Campaign Evolves to Exploit Israel-Hamas Conflict | Recorded Future

RANSOMWARE ROUNDUP

LockBit summary

The LockBit ransomware gang recently claimed responsibility for a cyberattack on the United States Federal Reserve. They alleged to have stolen 33 terabytes of sensitive banking data, including "juicy banking information containing Americans' banking secrets." However, it turns out that the threat actor hit an individual bank, Evolve Bank and Trust and not the Fed itself[49].

The FBI has acquired over 7,000 decryption keys and is offering them to past victims for free. This is part of an international operation that disrupted the ransomware network in 2024, but the group is still active and demanding ransoms from new victims.

Analyst Comment:

Lockbit has faced significant disruptions due to international law enforcement efforts.

Cybersecurity experts like Dominic Alvieri and Thomas Richards expressed scepticism about LockBit's claims, noting the lack of proof and the group's history of dishonesty[50].

LockBit 3.0 criticised the Federal Reserve's negotiators, who only offered them $50,000, and demanded a new one within 48 hours.

LockBit has extorted up to USD 1 billion in ransoms from over 7,000 attacks worldwide. Their most recent large-scale attack is an attack on the Indonesian Government, putting a $8million ransom on return of the data, which Indonesia are refusing to pay[51].

Analyst Assessment:

Despite law enforcement efforts, LockBit remains active and is likely to continue to target victims and leak stolen data whilst regrouping after the February International Law Enforcement takedown.

The FBI's call to action and provision of decryption keys almost certainly represents crucial steps in combating ransomware and assisting affected organisations in recovering their data without paying the ransom payment.

There is a realistic possibility that there was circular reporting at play in this instance, as Lockbit's reference to "America's banking secrets," was wrongly interpreted by someone as referring to the Federal Reserve, when this was not the case.

LockBit's attack on the Indonesian Government this month, suggesting LockBit are trying to overcome law enforcement involvement and regain their international standing as a prolific ransomware group.

Recommendations:

This serves as an interesting lesson in being cautious about making assumptions, especially where Ransomware groups are concerned. They are often known to lie to extort money and are often unreliable when ransoms have been paid, only returning some, or fragmented data.

[49] https://nsaneforums.com/news/security-privacy-news/lockbit-lied-stolen-data-is-from-a-bank-not-us-federal-reserve-r23935/

[50] Ransomware gang claims cyber-attack on Federal Reserve | Tom's Guide (tomsguide.com)

[5151] LockBit in $8M Indonesia ransom demand | Cybernews

Other notable events:

- **The NCSC** has published recommendations on maintaining a strengthened cyber posture, reporting a Cyber Incident, Phishing attacks, BEC compromise and reporting a scam[52].

- **CISA recommends Small to Medium Businesses adopt Single Sign-on**. The study identified financial and non-financial barriers, including high costs, bundled services, and technical challenges. SSO enhances cybersecurity by centralizing identity management, yet SMBs often perceive it as non-essential due to misaligned views on its benefits and costs. CISA recommended vendors unbundle SSO services and offer tailored, affordable options for SMBs. To facilitate adoption, SMBs should evaluate needs, consider cloud-based solutions, and start with pilot programs. The Government and non-profits are encouraged to support SMBs with education, buyer's guides, financial incentives, and free consulting services to mitigate costs and promote better security practices[53].

- **Santander:** The Santander cyber-attack was a significant cybersecurity incident that affected millions of customers and employees of the bank[54],[55]. The attack affected all Santander staff and approximately 30 million customers[1]. The bank, which employs 200,000 people worldwide, including around 20,000 in the UK, confirmed that data had been stolen. The attackers, known as the ShinyHunters group, obtained confidential information belonging to millions of Santander staff and customers.

- **23andMe:** a genetic testing company, exposed the personal data of millions of users. The hacker, Golem1234, used credential stuffing to access user profiles and steal data. British and Canadian authorities are investigating the breach and its implications for data protection.

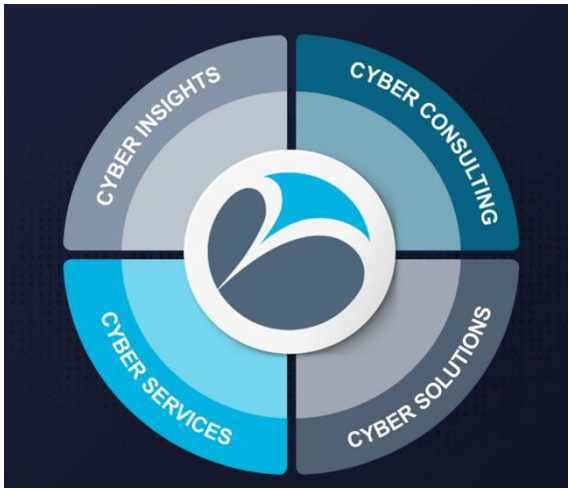
- **CDK global**: A software provider for the automotive industry fell victim of a ransomware attack by the BlackSuit Ransomware gang. They demanded a large ransom and exploited a second vulnerability during the recovery process.

- **Dreamwall Akira:** Akira ransomware is a relatively new threat that has demonstrated aggressive targeting, particularly in the U.S. health sector. Akira threat actors gain initial access through a virtual private network (VPN) service lacking multifactor authentication (MFA).Known Cisco vulnerabilities (such as CVE-2020-3259 and CVE-2023-20269) are exploited 2. Dreamwall, a Belgium-based digital signage company, fell victim to Akira RW. The attackers encrypted over 1,000 devices and demanded a 20-bitcoin ransom (approximately $1 million).The attack affected Dreamwall's clients, including airports, shopping malls, and cinemas.

- **Heras.co.uk** Lockbit ransomware attack: Heras.co.uk, a UK-based fencing company, suffered a Lockbit ransomware attack that encrypted its files and stole its data. The attackers demanded a ransom of 11 bitcoins (about $550,000) and threatened to leak the data if not paid.

[53] https://www.ncsc.gov.uk/guidance/maintaining-a-sustainable-strengthened-cyber-security-posture?utm_source=substack&utm_medium=email
[54] https://www.bbc.co.uk/news/articles/c6ppv06e3n8o
[55] https://www.techradar.com/pro/security/santander-hit-by-massive-hack-all-staff-and-30-million-customers-affected

Bytes Software Services



Bytes Security Division act as an independent, trusted advisor. Our customers benefit from a wealth of knowledge and 25 years' experience in the industry.

Bytes uniquely brings together cyber consultancy, solution specialists, pro-services, support and managed services under one roof.

The security team is technical-led, and expertly positioned to support the delivery of an end-to-end and integrated methodology to cyber security, covering compliance, risk and technology solutions.

Our consultative approach enables our team to fully understand our customers challenges and business goals, ensuring we deliver innovative and relevant security solutions.

Bytes Security Mission is to reduce our customer's cyber risk, protect their brand and safeguard their data. We are agnostic, but opinionated.

AUDIT & ADVISORY	STRATEGY	ASSURANCE
Payments & PCI DSS	ISF Security Healthcheck & Benchmarking	Penetration Testing
Data privacy services	Cyber strategy & cyber resilience	
ISO 27001 advisory services		
Cyber / information / technology security frameworks	vCISO service	Digital Forensics, Threat Intelligence & Incident Management
Cyber Essentials & Cyber Essentials Plus	Project & 3rd party security reviews	
Digital footprint, risk & threat assessment		

[Cyber Security Portfolio | Bytes]