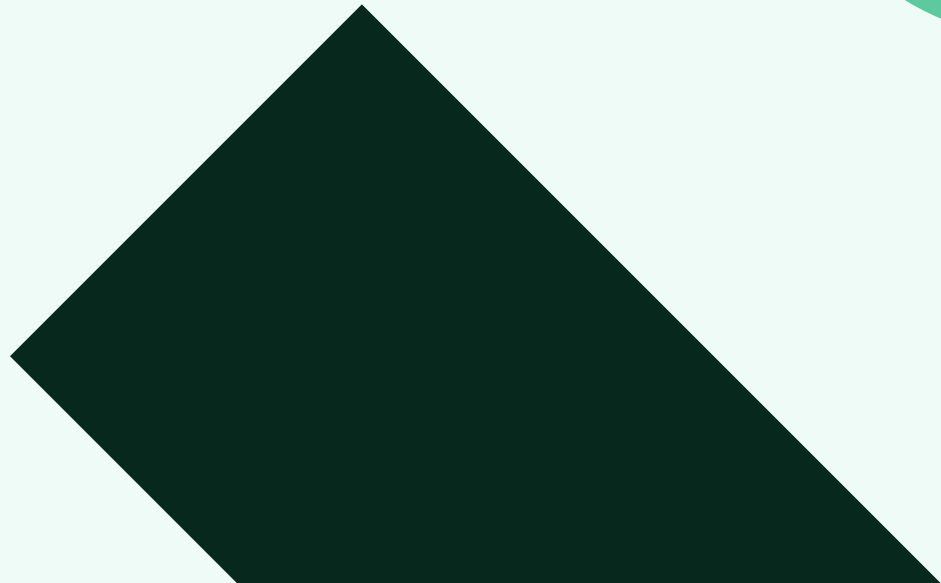


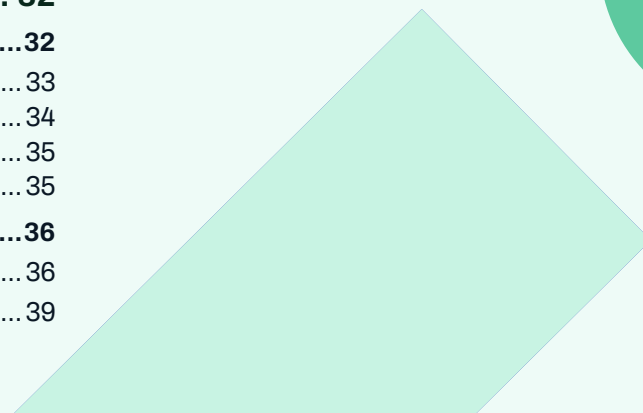
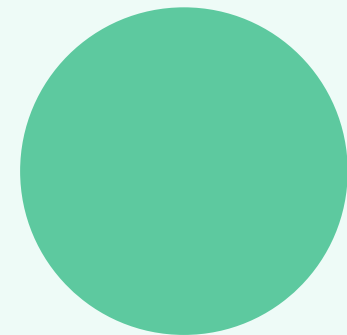
# Cyber Threat Landscape

European Mid Market 2025



# Table of Contents

Foreword.....	3	<b>Battlegrounds 2025 .....</b>	<b>40</b>
<b>Executive Summary.....</b>	<b>4</b>	<b>Identity and Cloud.....</b>	<b>40</b>
<b>Introduction.....</b>	<b>9</b>	<b>Mobile .....</b>	<b>41</b>
<b>Scope.....</b>	<b>9</b>	<b>MacOS .....</b>	<b>42</b>
<b>Thematic Threats 2025 .....</b>	<b>11</b>	<b>Linux .....</b>	<b>43</b>
<b>Financial Crime .....</b>	<b>11</b>	<b>Key Vectors .....</b>	<b>44</b>
Ransomware .....	11	Phishing.....	44
Resource Jacking.....	20	Attacker in the Middle / MFA.....	46
<b>APT / Espionage .....</b>	<b>21</b>	Business Account compromise.....	46
Russia.....	21	Malspam.....	47
China .....	23	Infrastructure Service Exploitation.....	48
DPRK.....	25	Supply Chain .....	49
Iran .....	27	Legitimate Tooling.....	51
State Ransomware .....	27	Malware.....	53
Cloud .....	28	<b>Conclusion .....</b>	<b>55</b>
Hacktivism .....	28		
DDoS Capability .....	30		
<b>'Other' Threats .....</b>	<b>31</b>		
Hack and Leak.....	31		
Anarchistic DDoS .....	31		
<b>Key Drivers 2025 .....</b>	<b>32</b>		
<b>Changing Geopolitical Forces.....</b>	<b>32</b>		
The US presidential election.....	33		
Russia/Ukraine .....	34		
China/Taiwan .....	35		
Cryptocurrency .....	35		
<b>Emerging Technology.....</b>	<b>36</b>		
Artificial Intelligence.....	36		
Quantum Computing .....	39		

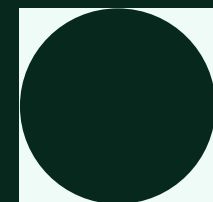


# Foreword

“ The passing of a calendar year is a relatively arbitrary milestone when considering development of cyber threats that a.) have been under active development and evolution for a number of years and b.) are responsive to events and activities that we, as industry, blue teams, and government agencies, undertake. Therefore, the purpose of this report is not to offer a set of predictions for how a threat may materialise in 2025, but articulate the threat, forecast what the key battlegrounds will be in cyberspace, and illuminate where continual advances and evolutions of the threat will manifest in the short term (12-month period).

This assessment, in the context of the European mid-market, has been put together using what we see in the Threat Intelligence team at WithSecure and will provide stakeholders with insight intended to support counter-threat operations and help WithSecure in its mission to build and sustain digital trust, confidence and equity.”

**Tim West,**  
Director, Threat Intelligence & Outreach



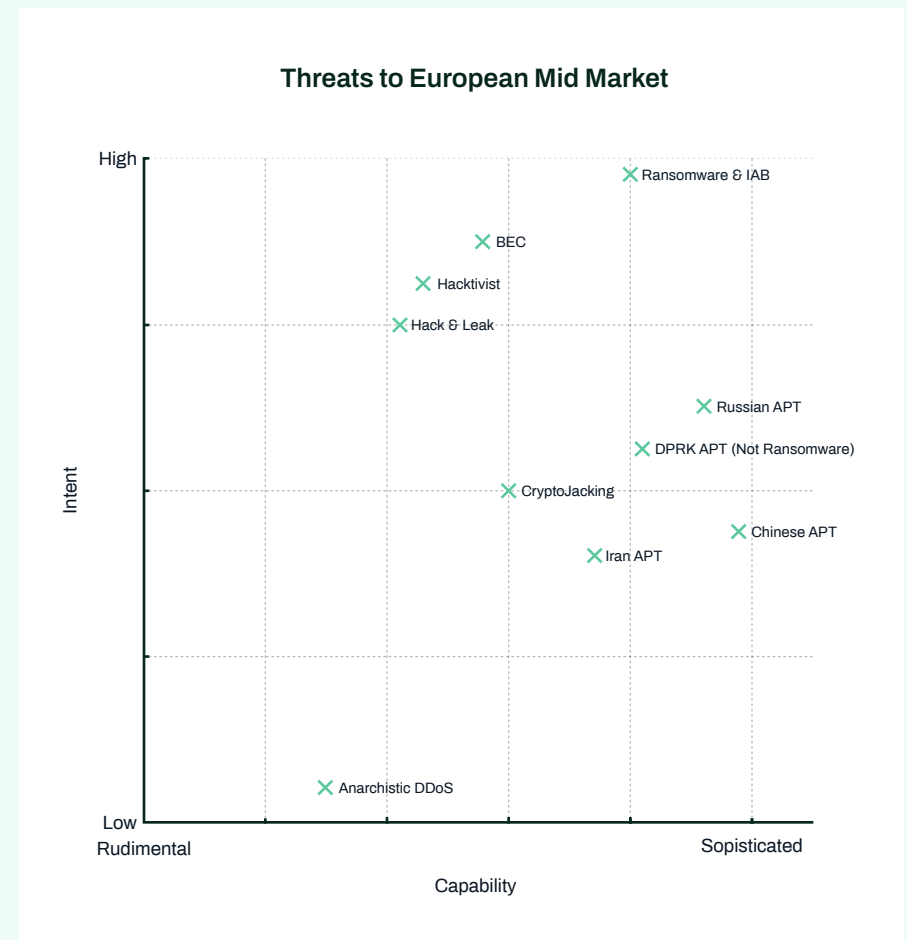
# Executive Summary

2024 presented a tumultuous geopolitical, technological and economic landscape, greatly impacting the cyber ecosystem and threat landscape. This report will forecast the landscape of 'cyber-dependent crime', and the Computer Network Attack/Exploitation (CNA/E) threats facing the European mid-market into 2025.

The following chart depicts the state threats to the European Mid-market industry. Predominantly the biggest threat will come from financially motivated actors such as **Ransomware** actors, however **Business Email Compromise (BEC)** actors, **Hacktivists** IABs and to a lesser extent, **Russian APT** actors will wield significant intent towards the European Mid-market. This is a generalist picture, assessing systemic threats to the mid-market of Europe. It will not be applicable to an individual organisation.

State-sponsored actors / APTs retain a disproportionate amount of 'cyber security column inches', however this is not proportionate to the threat most organisations in the European mid-market will face.

Threat is calculated as a function of Capability x Intent, where intent is defined by the amount of effort a threat is willing to spend targeting an arbitrary organisation in the European mid-market. Organisational impact will vary between actors' objectives (i.e. destructive attacks impact more than DDoS), the above graph positioning should not be conflated with the risk to European mid-market that each actor type poses.



# Key Battlegrounds

The following table depicts the change in where the cyber security battlegrounds will be from 2024 to 2025. The emboldened ones depict where these will be key into 2025, despite their direction of change.

# Key Themes 2025

The following are likely to represent the key themes for network defenders throughout 2025.

## Cloud adoption

The more Cloud becomes an intrinsic part of the fabric of organisational networks, the more we see the evolution from cloud-aware to cloud-astute threat actors. The use of legitimate tooling and functionality to complete illegitimate tasks will be a key theme that network defenders will have to grapple with in 2025 – continuing from 2024. We have started to observe known cloud services used as nodes in attacks, not only limited to C2 infrastructure. As organisations have become increasingly de-perimeterised it has catalysed the infostealer industry and theft of identity/authentication material activities will continue to be a key trend. The adoption of modern architecture, particularly when functionality is fluid as it is in cloud, will somewhat undermine years of behavioural and user training from non-cyber savvy users. Actors will increasingly exploit cloud environments which try to hide their complexity from users who are becoming increasingly accustomed to repeatedly (and arbitrarily) authenticating to different services.

Battlegrounds	Trend
<b>Windows</b>	↓
<b>Cloud</b>	↑
MacOS	↗
Linux	→
Mobile	→
<b>In code</b>	↑
<b>In browser</b>	↗
Security tooling	→
<b>At user (social engineering)</b>	↗
In macro / In document	↓
<b>Identity</b>	↗

## Novel Social Engineering

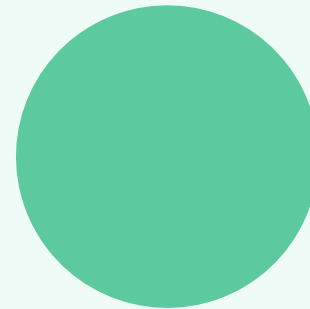
For many actors, particularly those who have flexible target profiles, it is easier and faster to bypass intrusion prevention systems through social engineering, rather than technological means. The gap between malicious elements (i.e. malware) and the initial contact technique is bridged by social engineering techniques. WithSecure observed a rise in novel, multi-step social engineering attacks that have been extremely successfully proliferating malware, and this rise will likely increase into 2025. We will likely continue to observe a paradigm shift from “pushing” a malicious item (binary, link etc) to a victim, to careful prepositioning that socially engineers a victim to “pull” a malicious element from the attacker. Furthermore, we can increasingly expect alternate messaging services to be an increasing vector of inbound malspam.

## Emerging software supply chain threats

An increasing number of poisoned software packages are being discovered in open-source software libraries. This provides a novel way of executing code that bypasses application whitelisting and many anti-malware scans. It is increasingly being used to propagate infostealers to development teams. This also applies to malicious browser plugins. Browsers often store authentication material and are increasingly acting as workstations in SaaS environments.

## More advanced identity attacks

As the adoption of Cloud services continue to increase, malware-less and identity-focused attacks will reinvigorate social engineering campaigns deploying more novel and innovative techniques. Attacker in The Middle (AiTM) techniques will also almost certainly increase in proportion with adoption of Cloud services and multi-factor authentication. Infostealer malware will remain extremely active and multifunctional, able to steal authentication material from a wide range of sources.



## Edge service / Infrastructure exploitation

Exploitation of edge and infrastructure service will be a common theme in 2025. Vendors appear to be struggling with both the vulnerability remediation process and a bruising operational tempo. Vulnerabilities are often both severe and rudimentary, meaning a broad spectrum of actors have the capability to exploit them with drastic effect. Issues are often compounded by an inability to deploy proprietary security tooling on such inherently vulnerable infrastructure.

## Artificial Intelligence (AI) penetration

While there are still some fundamental capability ceilings in place on generally available AI, it is still an extremely useful tool for nefarious actors.



It will likely enable increases in the number of actors able to meet a 'minimum viable standard' to cause harm in cyberspace. An increase in the number of able actors and increase in efficiency of existing intrusion sets will almost certainly increase the threat to a typical European mid-market organisation faces.



In its current state, AI will probably not revolutionise the sophistication of the most capable intrusion sets, but it will offer a great efficiency boost (i.e. increasing the number of vulnerabilities a capable bug hunter is able to detect), whilst offering large productivity boosts to social engineering techniques.



Currently AI likely provides an equal-or-greater opportunity to network defenders, who will have better access to advanced defensive AI capability, however this balance can easily be redressed if irresponsible decisions are taken on the use of AI by information technology leaders.



AI will amplify both known, and unknown security risks.

## Key Drivers

The following are the key drivers identified in this report that will almost certainly impact the threat landscape and alter the assessment in this report, but are too unpredictable to assess with sufficient confidence:

### Geopolitical Events

Following a heavy anti-incumbent wave of national elections, 2025 will likely see an increasingly fractured geopolitical environment. The following list of possible geopolitical events that will shape the cyber ecosystem might include, but will not be limited to:



The fallout from the incoming US regime, particularly trade policy and foreign aid commitments to NATO, and Ukraine.



How the conflict between Israel and Hamas and events with Iran will develop.



How China's claim over Taiwan will proceed.

### Artificial Intelligence Reasoning

Artificial Intelligence is under rapid development and public models are frequently being updated with new features. These features are often relatively cosmetic, increasing efficiency and performance that sit under the same capability ceiling as preceding models. A true breakthrough in Agentic AI1 will impact the landscape wider than is currently assessed in this report.

### Artificial Intelligence Regulation

While there are many ways to 'jailbreak' large language models, Trust and Security teams at commercial AI providers will be critical when seeking to combat misuse of Generic AI capabilities. Regulation will be key in positively managing the ways that AI will be a disruptor to economy and society in 2025.



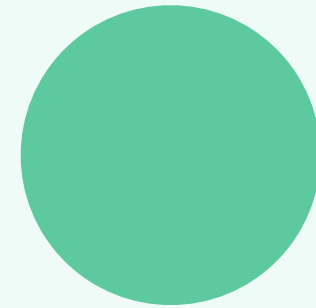
# Introduction

## Scope

This report will be prepared, where possible, through the lens of the European mid-market. Cyber does not always respect borders and often we must refer to incidents and events that fall outside of a geographic profile in order to make proper assessment.

Throughout this report, threat is calculated through a function of Capability x Intent that an entity may wield towards organisations within the European mid-market. Readers should note that while organisations may be targeted (deliberately or incidentally) as a result of geography within which they sit, they are seldom targeted because of the size or position they sit within the market. Assessing intent is more straightforward when considering opportunistic and financially motivated threat actors, however it is challenging to generalise a threat when considering niche, or specialised organisations that fall within the European mid-market. It is important that these organisations are able to calculate their own threat model based on their own unique profile.

This report will focus on 'cyber-dependent crime', not 'cyber-enabled crime'. Cyber-enabled crime defines where more traditional criminal objectives are achieved using techniques that may also be utilised in offensive cyber operations. For example, establishing a lookalike domain in order to socially engineer an individual to steal credit card information. Such activity is out of scope for this report. This report will focus on cybercrime where it refers to "Computer Network Exploitation" (CNE) or "Computer Network Attacks" (CNA) seeking to undermine the confidentiality, integrity or availability of information and information systems. Fraud, scams and child sexual exploitation (CSE), while illegal and often occurring within cyberspace, are out of scope for this report.



Information operations and misinformation are forms of mass social engineering. This will also not be covered in this report as threats in this space do not represent a cyber security risk to organisations.

### This report will be structured into three main sections:



**Key battlegrounds** - Technology and attacker TTPs are constantly evolving based on adoption of different architectures, and adoption of trending and successful vectors. This section of the report will forecast the state of the threat to environments and the trending vectors employed by threats in 2025.



**Key drivers** - The threat landscape is evolving and is driven and influenced by a myriad of external factors such as emerging technology or geopolitical events. These are often almost impossible to foresee, and therefore it is inappropriate to attempt to prescribe all possible threat scenarios stemming from these. This report will instead highlight and describe these key drivers that will impact upon the threat landscape in 2025.



**Thematic threats** - Covering significant financial, governmental, ideologist or political intrusion sets.

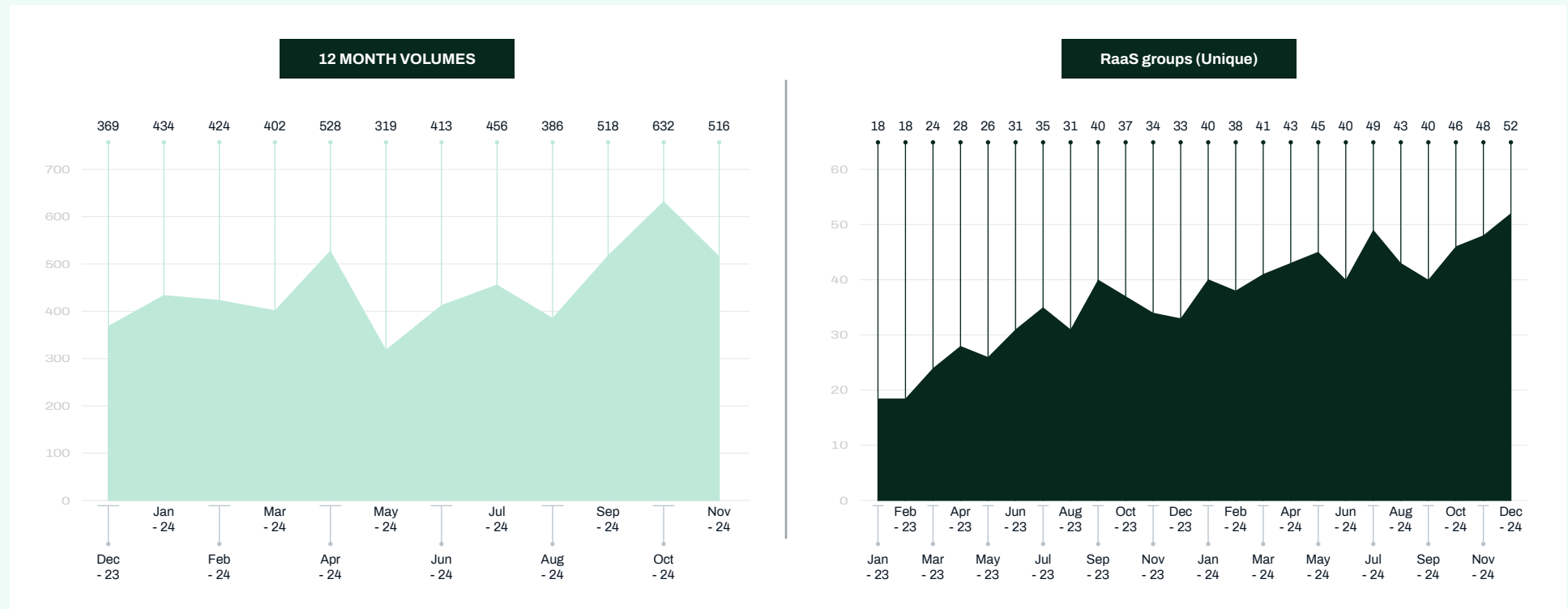
The purpose of this report is to forecast threat into 2025, and while they will be referred to, this report will not re-explain the vectors that can be considered 'status-quo'. Instead, detail will be reserved for where the threat will change and evolve into 2025.

# Thematic Threats 2025

## Financial Crime

## Ransomware

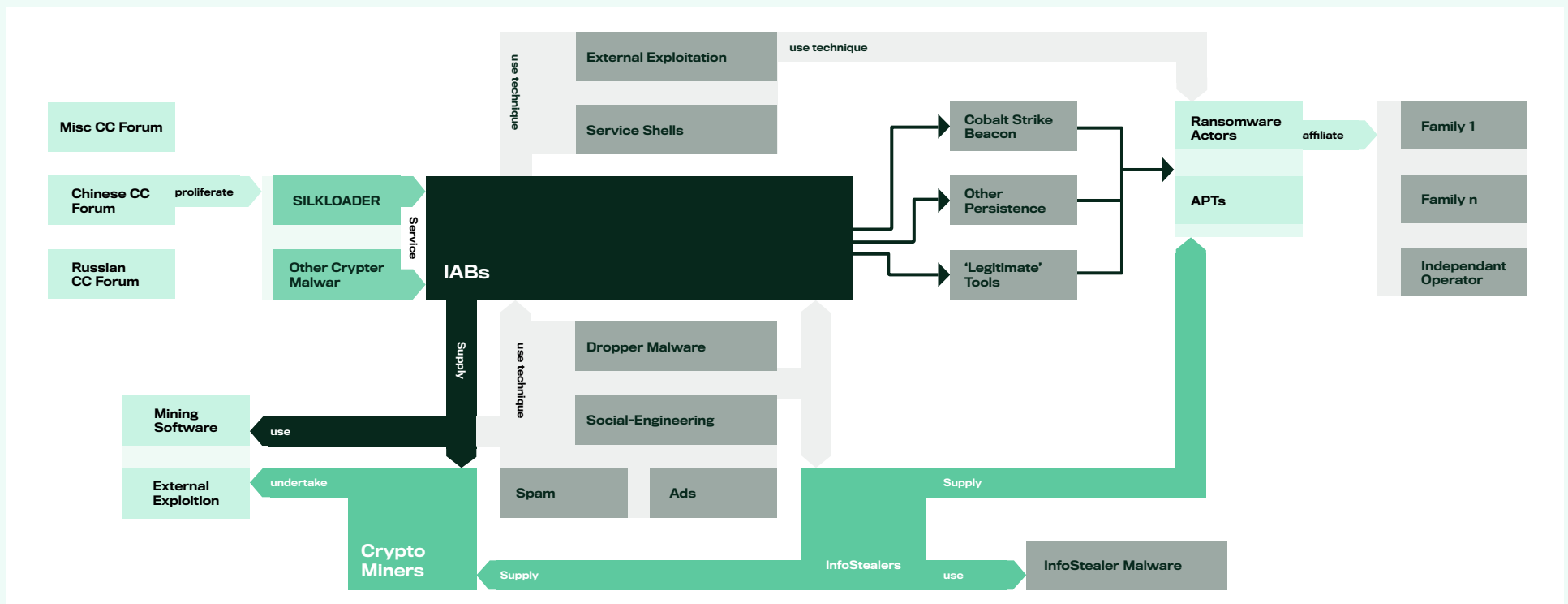
Throughout 2024, the Ransomware landscape was disrupted by a number of key events. These events curtailed the rate of ransomware attacks throughout quarter three (Q3) of 2024, however the ransomware ecosystem showed signs of recovery in Q4. Volumes over October, November and December presented much higher numbers than previously seen throughout 2024 and the number of unique, active ransomware brands has been increasing towards the end of 2024.



## Architecture of a RaaS collective

WithSecure's understanding on the architecture of a Ransomware as a Service architecture is not likely to change significantly in 2025. The cybercrime architecture will largely be defined by an 'as-a-service' industry. Efforts by law enforcement in 2024, and into 2025 (expected) may drive some actors to operate in a way that obscures the full impact of their actions, for example, affiliates may choose to utilise many different ransomware families. While there are some ransomware actors that operating a full end-to-end kill chain (not using service provisions) under a consistent ransomware brand, this will probably remain less common than ransomware affiliates heavily utilising the 'as-a-service' model defined in this section.

It is highly likely that the number of active ransomware groups will continue to rise into 2025. This is likely a result of two key factors: the availability of leaked or open-source ransomware 'builder' code, and the desire to obfuscate the significance of any affiliates. It is likely that many of the most productive ransomware affiliates will continue or expand working to multiple different ransomware brands. The following diagram details the as-a-service architecture of cyber-crime intrusion sets. While it was developed towards the end of 2023, it will still almost certainly be relevant in 2025:



## Initial Access Brokers

Initial access brokers are at the centre of the as-a-service model. They are very difficult to attribute and are a key driver in the marked increases of ransomware productivity.

Many of the more capable initial access brokers have industrialised initial access across vulnerabilities and repositories of stolen identities. IABs will invest effort in compromising companies of the European mid-market regardless of their profile (sector, size etc) as these factors do not impact upon their business model.

WithSecure have observed IABs operating with both state-sponsored APT attacks and ransomware operators.

## Nationalities

Eastern Europe and Russia are heavily cited as the source of most ransomware attacks. This attribution is often due to the execution guardrails found in ransomware binaries that prevent detonation if deployed upon computers with Cyrillic characters, and the abundance of Russian language cybercrime forums. This is still common, although probably less and less the default. Ransomware operations are being launched from all over the world and many affiliates operate in Europe and North America.

In 2024, there have been examples of affiliates being arrested in the US and Europe, and there are also ransomware groups primarily operating out of countries that do not have an extradition treaty with the US and Europe. For example, RA World (first seen in summer 2023) are a ransomware group we believe overlap with DEV-0401 / EMPORER DRAGONFLY, a China-domiciled intrusion set. WithSecure have also observed 'Phalcon' ransomware, highly likely operated by Iranian actors. North Korea (DPRK) is a clear exception when considering state-sponsored CNE/CNA (Computer Network Exploitation / Attack) events as their intrusion sets also operate with a revenue generation mandate. There are examples of ransomware families that are directly developed by DPRK; however, these have not been observed for a long time. It is far more likely that actors operating out of DPRK are likely utilizing established ransomware-as-a-service models to undertake their attacks. WithSecure Threat Intelligence has observed overlap between infrastructure used in intrusions orchestrated by DPRK and those of more 'traditional' ransomware affiliates.

There is almost certainty a significant number of unreported independent 'small game hunters' who capitalize on leaked ransomware source code and disposable email addresses to launch attacks without relying on established extortion infrastructure.

## Law Enforcement Impact

Law enforcement impact throughout 2024 was effective in at least temporarily impacting the efficacy of the wider ransomware landscape. It is likely that law enforcement agencies will seek to replicate this success into 2025. It is therefore possible that successful counter-ransomware action in 2025 will continue, and LEAs will continue to target ransomware affiliates. It is highly likely that such operations would positively impact the ransomware landscape, however in order to drive lasting and significant change, there first needs to be a concerted, multi-lateral governmental initiative.

Op Cronos was probably the most successful and impactful LEA counter-ransomware operational in history, and at the time of writing the report there are signs that the ransomware industry is recovering from the impact. As private industry alone does not possess the mandate to fundamentally counter ransomware actors (only really being able to respond to events and not target affiliates directly), it is therefore possible that things will get worse before lasting action can be taken against ransomware actors targeting European small / medium sized enterprises.

## Victimology

The following data is limited to multi-point of extortion groups who are operating a leak site which is parseable. In this section we will be looking at victim leak sites. This dataset is probably the best and most consistent source we have that enables us to understand the landscape, but the data collected here is not fallible,

### **There are several variables that impact and skew this dataset:**

- It is attacker led, and some attackers may be incentivized to post incorrect data.
- It is fluid, and victims are added and removed frequently.
- Extortion success is another key factor, if the amount of paying victims greatly increases, 'total' ransomware numbers may also appear to decrease.

With this said, we can draw some insight from this data with sensible assumptions – and recognizing the data isn't perfect, it does provide a decent gauge on the ransomware landscape.

### **The assumptions the industry typically abide by are:**

- There is a roughly relatively consistent month-on-month victim payment rate,
- Actor posts do contain an element of truth.

Since 2022, the proportion of small (0-200 employees) victims has increased year on year, from 50% in 2022, to approximately 62% in 2024. While medium sized businesses (200-1000 employees) proportions

remained relatively consistent, large (1,000-5,000 employees) and very large (5,000+ employees) organisations have represented a smaller and smaller percentage of victims.



It is possible that the continued reduction of large and extra-large victims on a ransomware breach site is in part due to a greater ability to meet the demands of extortionists. It is almost certain this comes as a result of a better ability to mitigate cyber risk, through the ability to deploy dedicated teams, products and services with cyber insurance and detailed recovery processes. Small and medium sized enterprises are therefore far more susceptible to ransomware impact, impact that also poses a more existential risk to the mid-market.

## Ransomware threats to Europe

Ransomware impacts the United States far more than it does the Europe. This is not likely to be an intentional choice by ransomware actors (although there may be some exception to this), it is more likely to be broadly representative of the volume of connected infrastructure that can be targeted.

The baseline of European vs global victims is approximately 21%. The following table depicts ransomware variants with a victim count of 10 or more that disproportionately target European organisations.



This demonstrates that there are probably some ransomware brands whose affiliates do operate with a European preference. These brands are not the most prolific in the ransomware ecosystem.



## Payment rates in 2025

“WithSecure do not participate in ransomware negotiations or payments to as part of its incident response service, therefore WithSecure Threat Intelligence must rely on third party reporting to make assessment on payment rates in 2025.”

The ransomware threat to organisations is more understood in 2024 and therefore well-resourced organisations are increasingly prepared to mitigate the risks that ransomware poses. As the adoption of cyber insurance increases, and as protective security tooling and recovery capabilities become more democratised, payment rates will likely drop into 2025. Throughout 2024, it is likely that payment rates have been decreasing, although there is a wide disparity in reporting as to the extent to which the rates have been in decline. It is likely this drop will continue into 2025.

This will likely not reflect a reduction in total monies being paid to ransomware actors. Payment numbers will probably increase in line with attack frequencies, and frequency of attacks will almost certainly not reduce without significant intervention by competent, authoritative organisations – this is unlikely to happen in 2025.



## Techniques Tactics and Procedures

It is unlikely that high level tactics, techniques and procedures used by ransomware actors will significantly change into 2025. The following table depicts the initial access techniques we will see ransomware affiliates deploying into 2025. All of the noted TTPs, and how they are likely to manifest into 2025 are further explored in this document:

T1566.002	Phishing: Spearphishing Link
T1133	External Remote Services
T1190	Exploit Public-Facing Application
T1078	Valid Accounts
T1566.002	Spearphishing Link
T1566.001	Spearphishing Attachment
T1566.003	Spearphishing via Service

## Cloud Infrastructure Awareness

Ransomware targets architectures in proportion to the usage of the architecture in industry. Windows based ransomware is the most common, and Mac / Linux ransomware variants do exist, but are much less common. Cloud awareness and targeting by ransomware actors will increase broadly in proportion with the adoption of Cloud architectures by organisations. This section does not refer to on premise hosted cloud infrastructure (i.e. ESXi services) as these have long been targeted by ransomware actors.

Cloud-aware ransomware actors often target cloud data storage as a means to either access sensitive data or prevent recovery from “offline” data storages. Cloud service providers have somewhat mitigated these risks, such as defining time periods between deletion requests and data removal, however in many cases the effectiveness of these controls is dependent on configuration of the service and may not be enabled by default. As increasing cloud adoption continues throughout 2025, ransomware actors will have little choice but to continue their development of cloud TTPs. There is active development in cloud attack techniques by offensive security researchers, and it is likely that many of these techniques will be adopted by malign actors. This said, cloud-native attacks observed in the wild almost always rely on exploitation of legitimate functionality, insecure identities and poorly configured environments<sup>2,3</sup>. More in-depth, academic cloud attacks documented by security researchers are often remediated by CSPs prior to their publication, however they do serve to demonstrate that there almost certainly exists a large number of possible attack paths that are not yet known. It is likely that these will be targeted by more capable threat actors, although this probably encompasses a smaller subset of ransomware actors.

Cyber-hygiene in cloud architecture is different from traditional on-premise architecture. Patch and vulnerability management is outsourced by definition, so configuration and posture management is critical<sup>4</sup>. It is almost certain that ransomware actors in 2025 will target misconfigurations, rather than vulnerability exploitation. This will likely impact smaller to medium sized organisations disproportionately, as cloud complexity is often obfuscated from a user and SME's often do not have dedicated infrastructure teams capable of ensuring robust posture management.

Throughout 2025 it is likely that we will see further development of tooling designed to improve the efficiency of actors completing set tasks in specific environments. These tools will almost certainly be primarily focussed on data destruction, encryption and/or exfiltration. Ransomware actors will almost certainly seek to utilise legitimate services to support various stages of their attacks. Cloud native functionality designed to sync data across tenants [i.e. Azure Storage Explorer] has been observed in ransomware exfiltration efforts. Illicit use of such functionality is almost certainly harder for security tooling to detect. This may be due to the unavailability of relevant logs, or the high false-positive rates associated with heuristic detections.

## Hybrid services

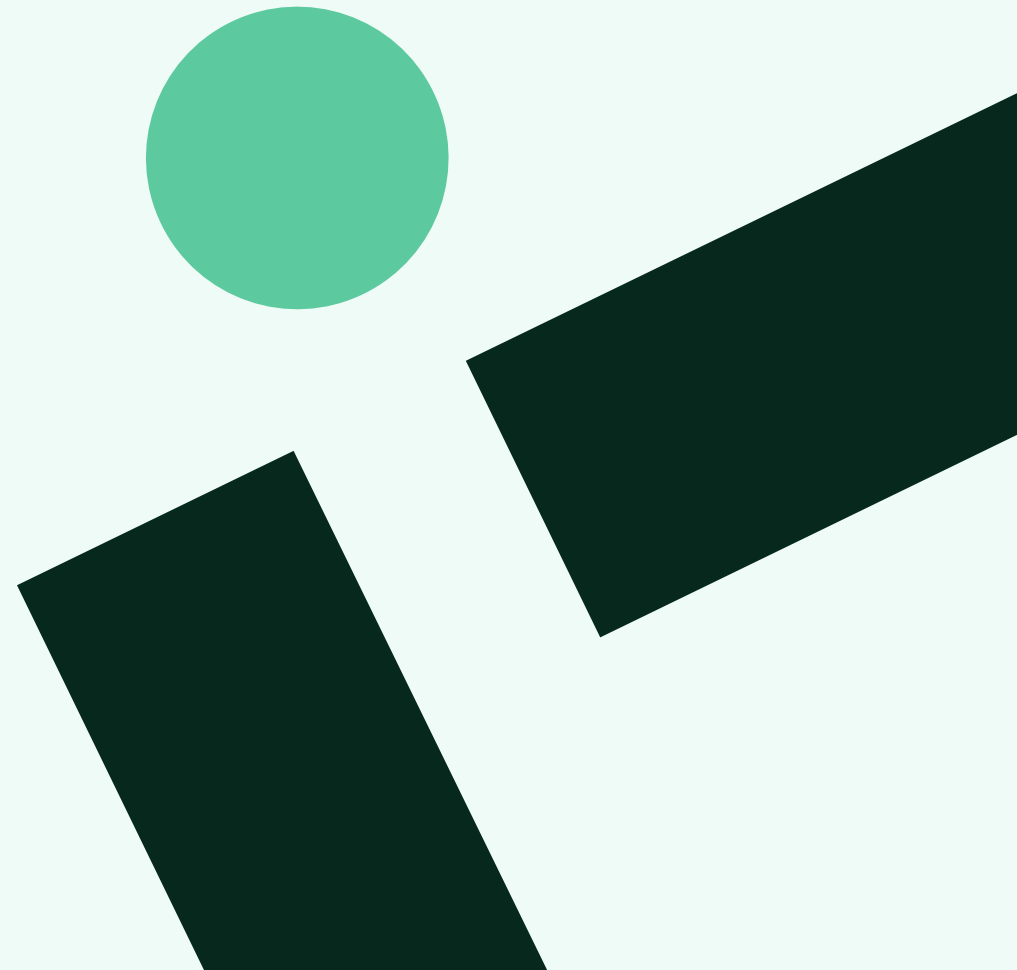
Ransomware actors will continue to target vulnerable cloud-based applications in 2025. Identity is likely to be the primary attack vector for such services, driving the high volume of infostealing malware campaigns that will continue into 2025. High value data repositories will be actively targeted, such as cloud-storage services and managed file transfer services. We have seen mass exploitation campaigns specifically targeting these services throughout 2024 [Snowflake, Cleo] and these will continue to be viewed as attractive targets to ransomware actors in 2025.

## 'Smash and grab' attacks

Many ransomware actors are pursuing more cost/time efficient attacks. This likely comes as actors do not foresee a contraction in their targeting pipeline, however, do recognise that organisations may be capable of recovery without meeting the demands of the attackers (i.e. the supply of victims high, but extortion success is difficult to predict). Instead of committing significant time and effort targeting an entire network, a smaller part of a can be targeted at a greater speed. This is a successful tactic as data theft, rather than data encryption is now likely to be a more attractive extortion lever for ransomware actors. Actors working to Akira have been observed in late 2024 launching high frequency, high speed attacks against on-premises virtual infrastructure (ESXi). This also enables ransomware actors to maximise the number of potential victims from a single exploit that may be patched rapidly after its first deployment.

## Legitimate services

Ransomware related actors increasingly utilise legitimate services across the entirety of their attack paths. This is detailed in [Legitimate Tooling](#) and will not be duplicated here.



## Resource Jacking

Resource jacking is a largely unreported threat vector. This is almost certainly because the impact of resource jacking attacks are often relatively low. Resource jacking is almost always utilised to 'mine' cryptocurrency. For the purposes of this report, we will explore two different versions of 'cryptomining', 1.) using stolen cloud resources, and 2.) the use of distributed computing through compromised hardware. The separation is important because cloud resource bills can seriously impact a small organisation, whereas very often a cryptominers installed 'on-premise' is only discovered following investigation into a separate intrusion.

### Cloud resource jacking

The most impactful form of resource jacking attack comes when cloud instances are deployed, typically through the compromise of a cloud administrator account, or through exploitation of poor cloud security configuration. Actors will then create new cloud instances, or scale up existing services, to deploy cryptominers. This can result in a very large compute bill from the cloud service provider. It is likely that CSPs are now more aware of the vectors described in this section and there is more mitigation in place. This said, CSPs seem to retain little responsibility for stolen compute resources and therefore very large bills can cause significant impact to European mid-market organisations.

## Hardware Exploitation

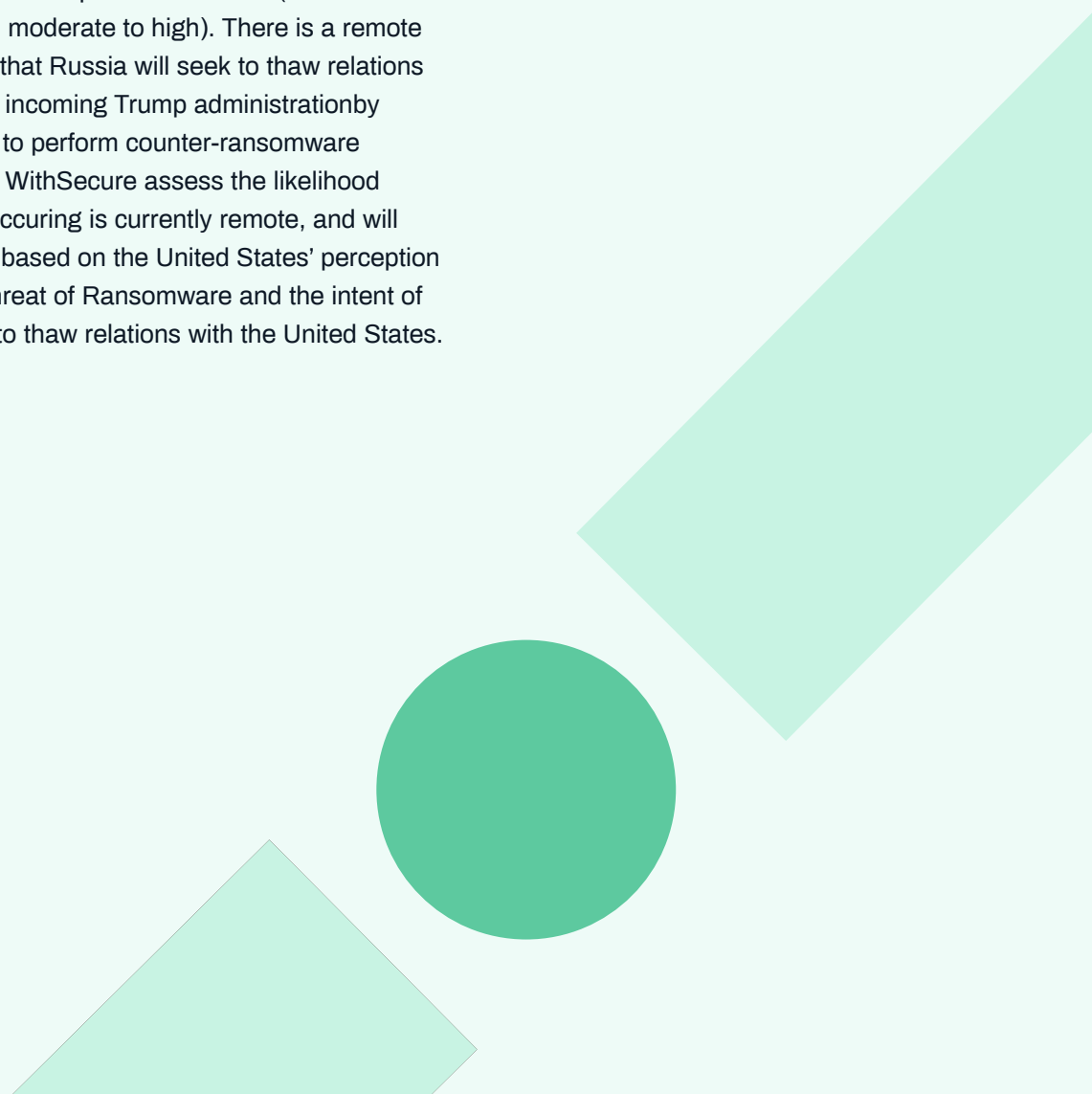
Where state-sponsored, ransomware and hacktivist actors are frequently reported to have exploited vulnerabilities in Internet connected devices, it is possible that actually the most prolific actors exploiting these vulnerabilities are cryptominers. WithSecure Incident Response often discover cryptomining malware when working on an incident response engagements<sup>5</sup>. There are a number of active malicious internet crawlers at any one time, and it is highly likely that a large proportion of these will seek to deploy cryptomining software<sup>6</sup>. It is almost certain that Cryptominers will actively intend to cause as little impact upon a victim as possible in order to maintain persistence for as long as possible. While the threat from this kind of cryptomining operator is high (calculated by capability x intent), the risk is very low due to the small impact caused. There is unlikely to be a marked change to this threat as we transition from 2024 into 2025.

# APT / Espionage

## Russia

Russian state threats are highly capable and active in cyberspace. Throughout 2025, Russian state aperture will primarily remain focussed around the conflict in Ukraine, launching espionage and destructive attacks with the intention of weakening Ukrainian resolve. Alongside this, 2024 was touted the year of the election, and often did not favour incumbent governments. Throughout 2025 Russia will also seek to utilise cyber for intelligence and information gathering following the regime changes in many countries. Russia will almost certainly seek to capitalise on the installation of governments sympathetic to Russia, seeking to stoke nationalistic sentiments with a view to a.) advancing Russia's position and ambitions on the international stage and b.) undermine cooperation between European Union and NATO countries. It is possible Russia will seek to cement its territorial gains in Ukraine with a resolution to the conflict, although activity in cyberspace supporting this objective will probably not greatly change the current systemic

threat the European mid-market (which remains moderate to high). There is a remote chance that Russia will seek to thaw relations with the incoming Trump administration by offering to perform counter-ransomware actions. WithSecure assess the likelihood of this occurring is currently remote, and will change based on the United States' perception of the threat of Ransomware and the intent of Russia to thaw relations with the United States.



Throughout 2024 there was much commentary detailing an assessed risk of Russian pre-positioning within western critical national infrastructure, which would be leveraged in the event of a conflict with Russia. This is a complex assessment, however if true, it is unlikely that Russia would seek to leverage such access to launch destructive attacks against European critical national infrastructure in 2025. There have been notable events throughout 2024 where (almost certainly) Russian state sponsored actors targeted undersea internet cables. While this will impact in cyberspace, such attacks are out of scope for this report.

As is noted in the [Hacktivism](#) section, Russian state actors have a precedent in utilising false-flag techniques to achieve its objectives. False-ransomware and false-hacktivism threats may be realised by the European mid-market throughout 2025, however it is likely this will either materialise within the sphere of a conflict (almost certainly Ukraine), or in response to a significant geopolitical event.

Heading into 2025, Russia remains a significant threat to the European mid-market and will actively seek to compromise organisations that will further its intelligence / espionage requirements. The risk to the European mid-market from Russian APT is likely lower than the risk from ransomware due mainly to a smaller destructive footprint that most espionage operations leave.

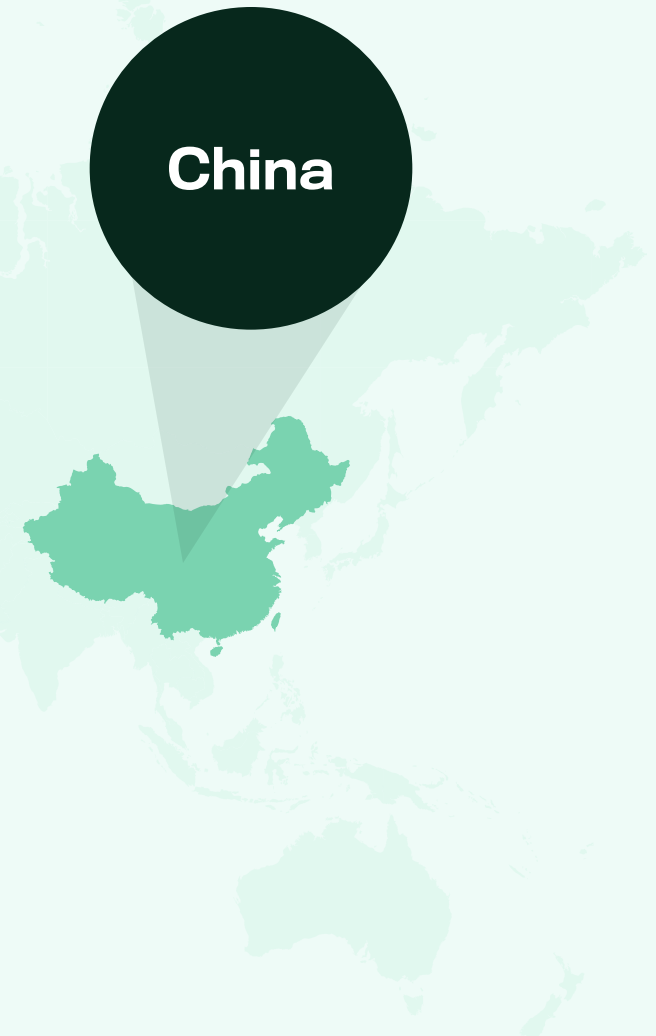


# China

China probably operates the most well human-resourced intelligence apparatus on the planet, and this almost certainly extends into cyberspace. This gives the Peoples Republic of China (PRC) the ability to conduct highly extensive operations with an extremely broad scope and scale. As this is coupled with a highly capable and well-resourced infrastructure, China is often stated to be the biggest cyber threat to western Governments.

Information gathering operations, and pre-positioning activity often do not have an immediate and tangible impact upon victim organisations. Therefore while international relations with China remain relatively stable, there is less cyber risk associated with PRC to the European mid-market than to the networks of government and infrastructure organisations of countries that PRC will consider adversarial.

PRC actors are known to target critical national infrastructure, including but not limited to, communications, energy, military, government, water and waste. CISA<sup>7</sup> has commented that the “most active and persistent” activity it is observing is not consistent with traditional espionage activity and is more likely pre-positioning for destructive and disruptive action. China will almost certainly see the United States as its main international rival, however it almost certain that this activity is not only limited to the United States (US), and European agencies and organisations have been and will be targeted. Seeking to quantify the threat to the mid-market (calculated by revenue and/or employee counts) is difficult as the targeting aperture of China will be focussed on the function of its victims and how well they align with Chinese strategic goals.

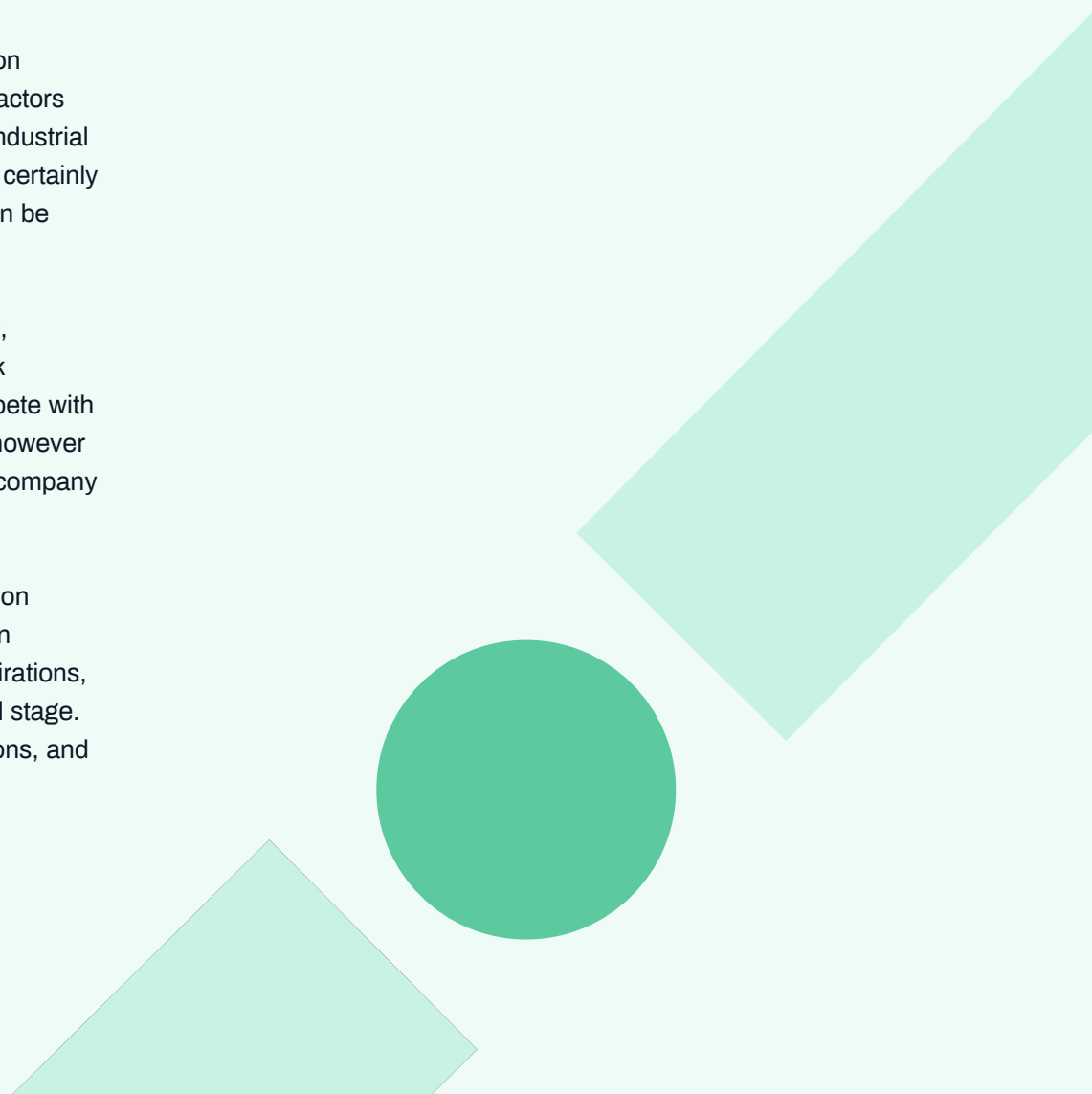


State intrusion sets are known to employ highly stealthy tactics in their attacks making them very difficult to detect. Crucially, PRC APTs are notoriously persistent, and it is often very difficult to fully expel from a network, even once they are detected. Throughout 2025, PRC will almost certainly continue deploying zero-day, n-day and known exploits against internet connected infrastructure and will continue to industrialise the collection of such exploits.

The compromise of routing equipment will contribute to Chinese obfuscation networks which obscure attacker traffic to and from victim networks. PRC actors are often observed targeting network appliances, such as firewalls on an industrial scale, often exfiltrating configuration and user information. This will almost certainly have been done with a view to decrypt sensitive information which can then be utilised in further operations.

China's aspirations in cyberspace will not only be limited to pre-positioning, espionage and information gathering. It is almost certain that they will seek continue to steal IP (intellectual property) in key industries in order to compete with western industry R&D efforts. There is often no immediate impact of this, however it often results in the erosion of the competitive advantage of a product or company in a marketplace.

Like Russia, Chinese state sponsored actors will seek to conduct information operations with a view to influence voting intentions and public sentiment in strategically important countries. This will be done to support strategic aspirations, particularly within the Chinese nine-dash line<sup>8</sup>, but also on the international stage. Geopolitical events will shape Chinese information and espionage operations, and this is explored further in the [Geopolitical](#) section of this report.



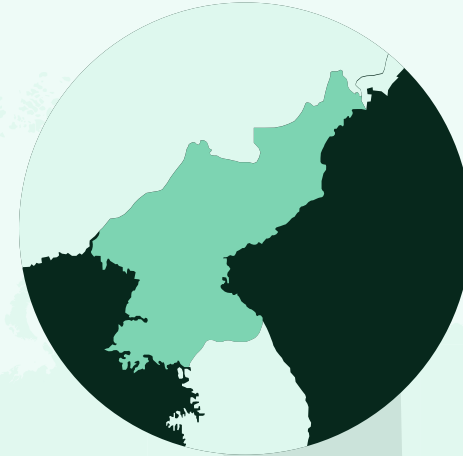


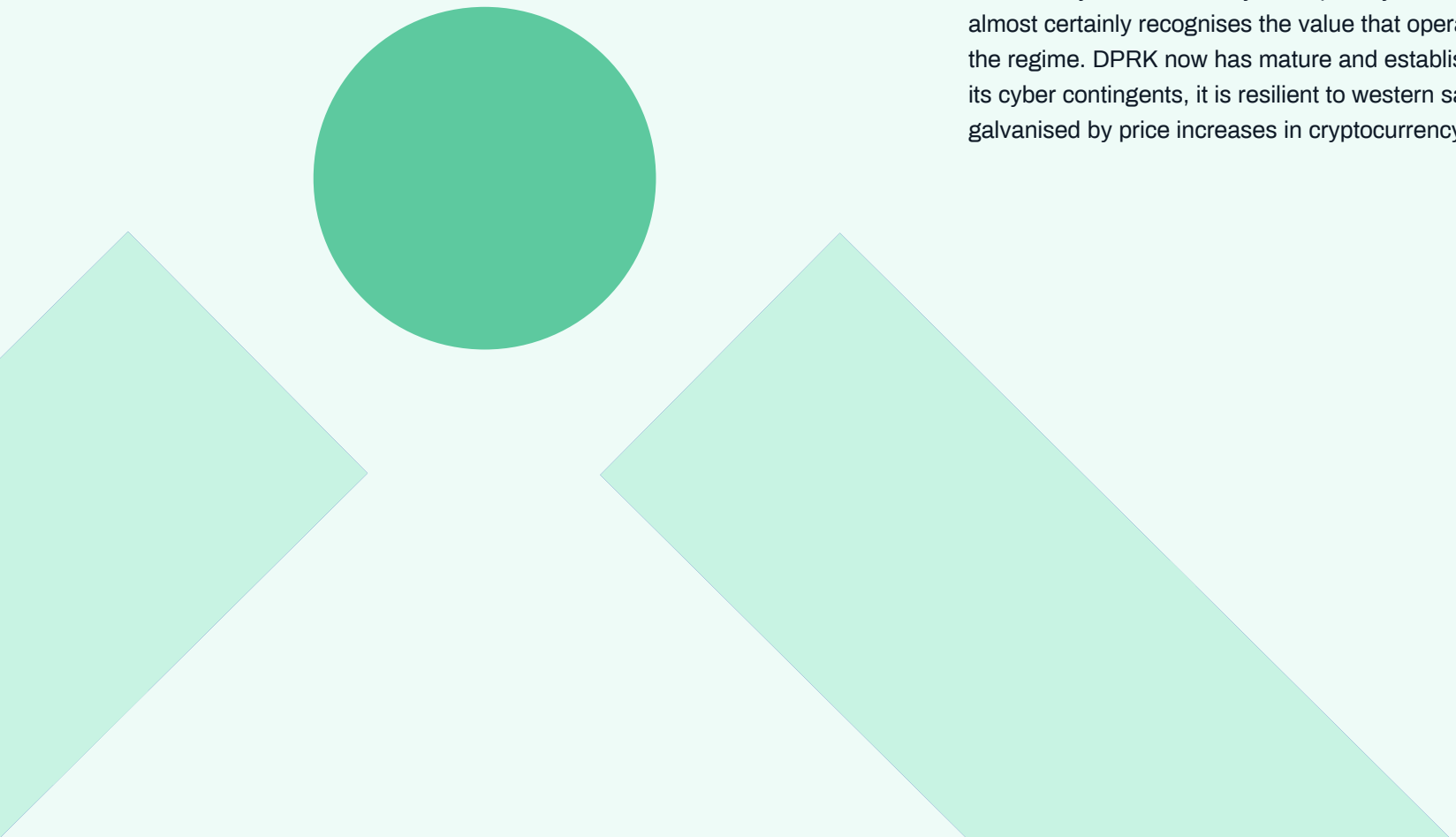
## DPRK

Democratic People's Republic of Korea (DPRK) typically deploys its capability in cyberspace in support of its economic need and geopolitical objectives.

DPRK's geopolitical focus will remain in-region, and it will deem the Republic of Korea (ROK / South Korea) as its primary adversary. DPRK will utilise a significant proportion of its offensive cyber capability to support its espionage operations against ROK. It is also likely DPRK will seek to launch information operations that will attempt to undermine RoK's government and/or foment civil unrest. DPRK's espionage aperture may expand beyond South Korea in 2025, likely in support of tactical requirements (military, healthcare etc). DPRK is a heavily sanctioned, and isolated country, and its recent deployment of troops to Ukraine is almost certainly in a mercenary capacity<sup>9</sup> - possibly as a way to attain technology, funding and other resources from Russia.

The main threat from DPRK to the European mid-market is through DPRKs extensive revenue generation operations. Organisations dealing in, or holding, cryptocurrency assets will almost certainly continue to be directly or indirectly targeted by DPRK actors. DPRK is known to deploy innovative TTPs when seeking to target cryptocurrency entities. It is highly likely they will continue to actively develop macOS malware, representing one of the main threats to the MacOS ecosystem. DPRK APTs will also see software supply chain attacks as a productive way to deploy crypto-specific infostealers. Both of these TTPs offer DPRK an effective way to broadly target organisations and individuals within a specific (Web3 and Cryptocurrency) industry.





DPRK actors are highly likely to be active participants within cyber-criminal networks (including ransomware). As with other cyber criminals, DPRK actors will seek to deploy social engineering techniques to gain access to a company's network and will almost certainly seek to deploy generative AI, particularly deepfakes, to achieve this. Unlike most other criminal groups, DPRK have the capacity, resources, infrastructure and patience to conduct longer term, complex operations<sup>10</sup> against large, 'hard' targets with well-resourced cyber security teams. One such example of this was the injection of IT workers into dozens of 'Fortune 100' organisations.

It is unlikely that DPRK's cyber capability is waning as we head into 2025, it almost certainly recognises the value that operations in cyberspace bring to the regime. DPRK now has mature and established educational pathways into its cyber contingents, it is resilient to western sanctions and is likely to feel galvanised by price increases in cryptocurrency.

## Iran

Iran's main focus in cyberspace in 2025 will probably remain on events surrounding Israel and Hamas. Israel is a capable and active force in cyberspace and Iran will almost certainly view Israel as a priority threat. Towards the end of 2024, Iran and Israel tensions escalated into kinetic action, and it is highly likely that cyber activity on both sides will have complemented this. Iran's primary focus will probably remain 'in-region' (Middle East), targeting governments, telecommunications, military advantage and high interest individuals (including dissident journalists). Iranian state-sponsored activity has also been observed overlapping with Ransomware operations, detailed in the following section. Iran likely presents a moderate to low systemic threat to the European mid-market in 2025.

## State Ransomware

Ransomware has become so prolific that its usefulness cannot simply be limited to financial gain. The cyber security industry has many examples of state-sponsored destructive attacks masquerading as ransomware. This is currently not a likely or realistic threat model for most organizations operating away from the sphere of conflict in Eastern Europe, however this threat model could change in line with increasing geopolitical tensions. Private organizations not headquartered in Ukraine have been impacted by a Russian-state 'ransomware' campaign - Prestige. Microsoft have detailed organizations in Poland, and WithSecure have detected Prestige related implants in Estonian networks. While WithSecure Threat Intelligence has observed state-operated ransomware events targeting small European organizations, it is likely that this will only be a significant threat to organizations operating in the sphere of an armed conflict. This may expand to a wider set of organizations within the European mid-market in the event of escalation between Iran/Israel and if China/Taiwan. In these events organizations may need to revisit this threat model.

North Korea (DPRK) is an exception when considering state-sponsored CNE/CNA (Computer Network Exploitation / Attack) events, as their intrusion sets also operate with a revenue generation mandate. There are examples of ransomware families that are directly developed by DPRK; however, these have not been observed for a long time. It is far more likely that actors operating out of DPRK are utilizing established ransomware-as-a-service models to undertake their attacks. WithSecure has detected overlap in infrastructure used in intrusions orchestrated by DPRK, and intrusions by ransomware affiliates. This is a model also employed by some Iranian state-sponsored actors, who are more likely 'moonlighting' with ransomware operations.

## Cloud

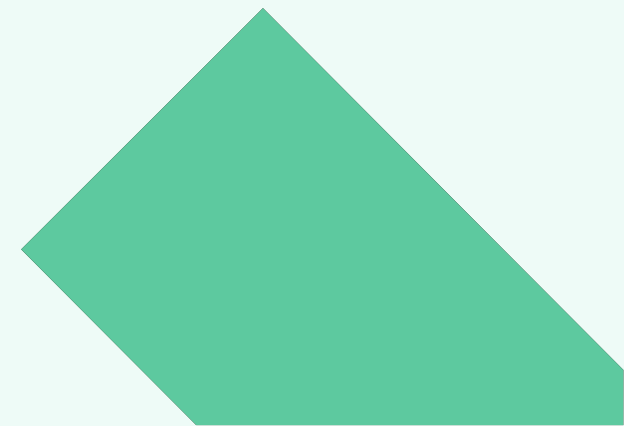
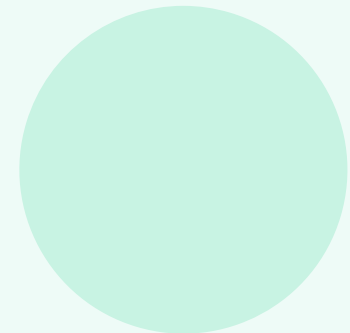
It is almost certain that every adversarial nation listed above will have the capability to target the cloud services of a victim. As with other actor types, is also highly likely that state-sponsored APTs will view this vector as an attractive one due to a relative lack of understanding by users, insecure default settings, a lack of logging and few EDR solutions, and an abundance of compromised identities as their disposal.

There are no significant documented events that suggest there is a systematic threat to resources in the cloud via the compromise of the underlying 'host' infrastructure. This said, it is likely that advanced nation states have the capability to achieve this. China have demonstrated their willingness and ability to target backbone services (ISPs / Telecommunications) and it is unlikely that they will view the CSPs as materially different to this established targeting profile. It is unlikely that even a small number of criminal organizations will be able to conduct such operations on hygienic systems [remotely targeting 'guest' infrastructure by laterally moving from 'host' infrastructure] without significant help.

## Hacktivism

Pro-Russian hacktivist collectives remain a threat to organisations across Europe. It is not clear how any (possible) peace negotiations will influence their operations in 2025. In the event that the EU 'step-up' their military support to Ukraine (perhaps in order to fill a deficit that may be left by the US), it is likely that European organisations will face an increased hacktivist threat which would predominantly come in the form of DDoS attacks, and sporadic wiper events.

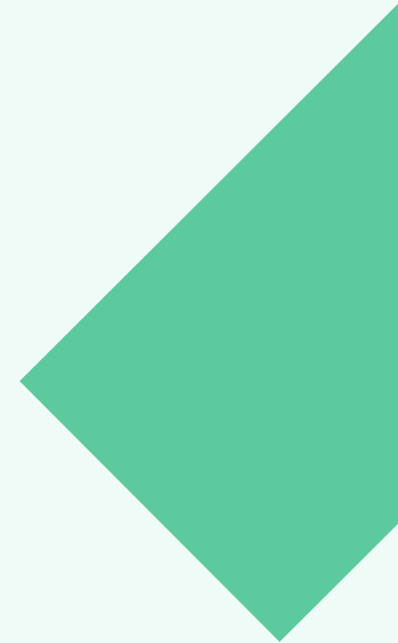
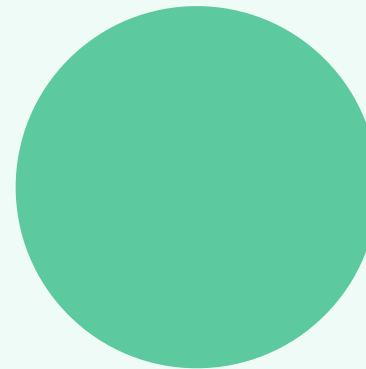
Hacktivist collectives by default will largely respond to geopolitical events, while still maintaining a relatively regular attack cadence. DDoS attacks are launched on a daily basis by hacktivists. It is common for pro-Russian hacktivists to change targeted countries on a daily basis (although in parallel, Ukraine is targeted daily). Targets are often minor business, transport hubs, or regional governmental functions<sup>11</sup>. It is likely that lightweight reconnaissance is done to ascertain whether a particular technology is in use by the potential victim, or whether DDoS protection is in place before DDoS targets are chosen. This often results in smaller 'mid-market' organisations and local governments being impacted.



As noted, there are also more distinct hacktivist events that align with major geopolitical events. This often results in a more concerted (and broadly impactful) DDoS attack. Hacktivist activity surrounding the Romanian election in late 2024 appeared particularly choreographed, just as attacks on French governmental targets were during their parliamentary election in mid-2024. A new government in the United States will change foreign policy relating to Russia (influencing European policy), and this will influence the hacktivist threat – one way or another.

Throughout 2024, as events further developed surrounding Israel, Palestine, and Iran, new hacktivist collectives emerged. Hacktivists focussed on the middle east are localised and primarily direct offensive attacks from Iran towards Israel (or Israeli companies) and vice-versa. If kinetic activity intensifies between Iran and Israel, cyber activity will almost certainly follow suit. Israel military activity in Palestine following a Hamas terrorist attack on October 7th 2023, has garnered a lot of international attention with multiple claims of human rights abuses against Israel. These events somewhat spilled into the political zeitgeist of Europe, to the extent where they have disrupted sporting events<sup>5</sup>. It is likely that hacktivist events will also expand beyond this geographical sphere. European organisations who are seen to take a strong stance on either side of the conflict or are seen to deal with Israeli military or government, will face an increased hacktivist threat. As is the case with pro-Russian hacktivist groups, this will likely come in the form of DDoS attacks and wiper events.

Hacktivist groups will also seek to compromise and disrupt SCADA/ICS systems. Hacktivist actively typically utilises unsophisticated attack technique and tactics and they will be reliant on targeting internet-facing, poorly secured systems.



## DDoS Capability

DDoS actors and hacktivists use a mixture of readily available 'stresser' services, and proprietary botnets. These are mainly made up of networks of inherently vulnerable SOHO (Small Office / Home Office) or IoT (Internet of Things) devices (although enterprise endpoints are occasionally included as part of large DDoS botnets). These make particularly attractive targets for 'bot herders' due to weak default configurations and a general lack of security monitoring and patching. Cloud services are also targeted and utilised in DDoS attacks, including but not limited to: Jupyter, Hadoop, HugeGraph.

There is an expectation that the number of IoT devices will rise to 30-40 billion in 2025<sup>12</sup>. The EU Cyber Resilience Act came into force towards the end of 2024, and mandates better cyber security standards on IoT devices. This will limit proliferation of vulnerable devices, however bot herders are unlikely to be deterred as there will be no shortage of vulnerable devices outside the European Union. Exploitation of IoT / SOHO devices will continue into 2025, particularly as many vulnerabilities exploited by bot herders are old, for example, a vulnerability exploited in mid-2024 in D-Link routers was first released in 2014.



# 'Other' Threats

## Hack and Leak

Hack and leak operators are defined by actors who perform data theft, or data leak operations. Often, they do not have any apparent motive and simply seek to leak data. Many actors will seek to sell the data to other actors, who probably then will attempt to exploit this data to extort a victim or launch further attacks. The actors demonstrate lower sophistication than other actors. They will almost exclusively target vulnerabilities on a speculative basis. This means that although they can cause tangible impact on their victims, they can be considered low threats to the European mid-market.

## Anarchistic DDoS

Non-ideologically motivated DDoS, where it does not align with other actors' objectives (I.e. as part of a ransomware extortion demand) can be considered 'Anarchistic'. This defines actors who may have personal vendettas against an organisation or services, want to gain notoriety, or perhaps simply are "bored". These actors pose a low threat to the European mid-market, however they do cause sporadic impact, often minor disruptions.

# Key Drivers 2025

## Changing Geopolitical Forces

Geopolitical forces significantly shape the cyber threat landscape. Major powers all retain and deploy offensive cyber capability. Geopolitical and state actions (in and out of cyberspace) set the tone for other threats that may not be operating under the direct control of a state.

APT groups typically operate directly to further the strategic objectives of a nation-state. These threats, despite an asymmetrically large media footprint, are not usually the biggest risk to the vast majority of mid-market organisations. This being said, geopolitical analysis should not be overlooked as previously noted, these forces influence the macro cyber environment more than is often recognised. For example, as economic difficulties directly catalyse increasing cybercrime activity<sup>12</sup>, the continued fallout from Russia's illegal invasion of Ukraine and resulting energy crises and economic depression will almost certainly have driven actors towards active participation in the cybercrime ecosystem.

This in itself has a significant economic impact – if cybercrime were an economy, by GDP, it would be the third largest in the world<sup>3</sup>.

2024 was significant due to the number of elections held in countries around the world. Five of the Seven G7 countries held national elections, with the remaining two (Canada, Italy) holding regional elections. 17 countries in Africa held general, presidential or parliamentary elections, as did other international powers, such as the European Union and India. While Russia, and North Korea also held elections, it is almost certain these were demonstrative only.



## The US presidential election

At the time of writing this report, Donald Trump has been elected as the next president of the United States. There are still a number of weeks until he is handed power, and there is still uncertainty on allegiance of the House of Representatives, which would either enable, or check the Trump government's ambitions. It is likely Trump will pursue an 'America First' agenda and adopt a more isolationist stance. This may impact Europe economically as trade barriers and tariffs are introduced or increased on imports to the EU's largest trading partner. Trade barriers may be viewed as hostile by China, leading some commentators to speculate a trade war is possible. We do not yet know what trade or tariff stance the US will take on imports from China, however it will highly likely galvanise Chinese state activity in cyberspace.

Throughout recent years, European and US law enforcement cooperation has been a key driver in numerous successful actions against cyber-criminal networks and individuals. It is unlikely that a new Trump administration will significantly change this cooperation, particularly as the US remains the most targeted country by ransomware and other criminal actors.

# Russia/Ukraine

Upon Russia's invasion of Ukraine in 2022, rising prices of oil exacerbated economic pressures caused by stimulus packages in response to the Covid-19 pandemic, triggering a cost-of-living crisis across many countries.

Donald Trump has claimed he will be able to bring about a swift end to the war in Ukraine in a way that will probably involve threatening to withdraw aid if Ukraine do not concede on some of their territorial losses. WithSecure has not allocated analyst time to assessing the full potential likelihood or impact of this, but it is unlikely it will, in the short term, mean a reduction of cyber activity in and around Ukraine. It would remain highly likely that in this event, attacks will enter a new phase in 2025. Offensive Russian cyber activity in Ukraine has changed through 2022 (a focus on dismantling infrastructure), 2023 (securing footholds and seeking feedback on kinetic actions) and 2024 (espionage, military & CNI targeting). It is almost certain that since 2022, these operations have spilled into surrounding European countries. In the event of ceasefire negotiations, it is unlikely that the threat from Russian state, and state aligned actors to European countries in the periphery of, and supportive to, Ukraine will change.

## European support / NATO

Defence spending has increased across Europe since the invasion of Ukraine by Russia in 2022<sup>4</sup>. Countries not reaching their 2% commitment have constantly been criticised by incoming president Trump who likely holds the view that the US is carrying a disproportionate 'load' when referring to the defence of Europe. The extent to which the US maintains or withdraws military support to European defence is unknown (although it remains improbable that the US will totally renege from their NATO collective defence obligations in 2025), however it is possible that a weakened (or perceived weakened) NATO may drive Russian aggression in the region which in turn would drive an increase in cyber activity.

# China/Taiwan

Many political commentators have noted that appeasement of Russia in their territorial ambitions may set a precedent that China may seek to exploit in their ambitions to expand their territory within the 'nine dash line' – an area that encompasses Taiwan. Trump's statements relating to the imposition of high tariffs threaten a trade war with China and therefore there is a realistic possibility that US/China relations will sour somewhat. All this said, it is not possible to make any assessment with adequate confidence as to how events surrounding Taiwan will develop in 2025.

## Cryptocurrency

Since Donald Trump was elected as the next US president, the price of Bitcoin has reached an all-time high, with additional value of 41% (at the time of writing) added to the price from the previous month. Cryptocurrency is favoured by cybercriminals due its decentralised nature and a lack of regulation. While Bitcoin is seen as one of the more 'legitimate' cryptocurrencies, and other, more privacy focussed coins have not experienced the same boost as Bitcoin (such as Monero) it is likely the rise of the price will galvanise financially motivated actors who will seek to defraud, scam or steal Bitcoin from victims.

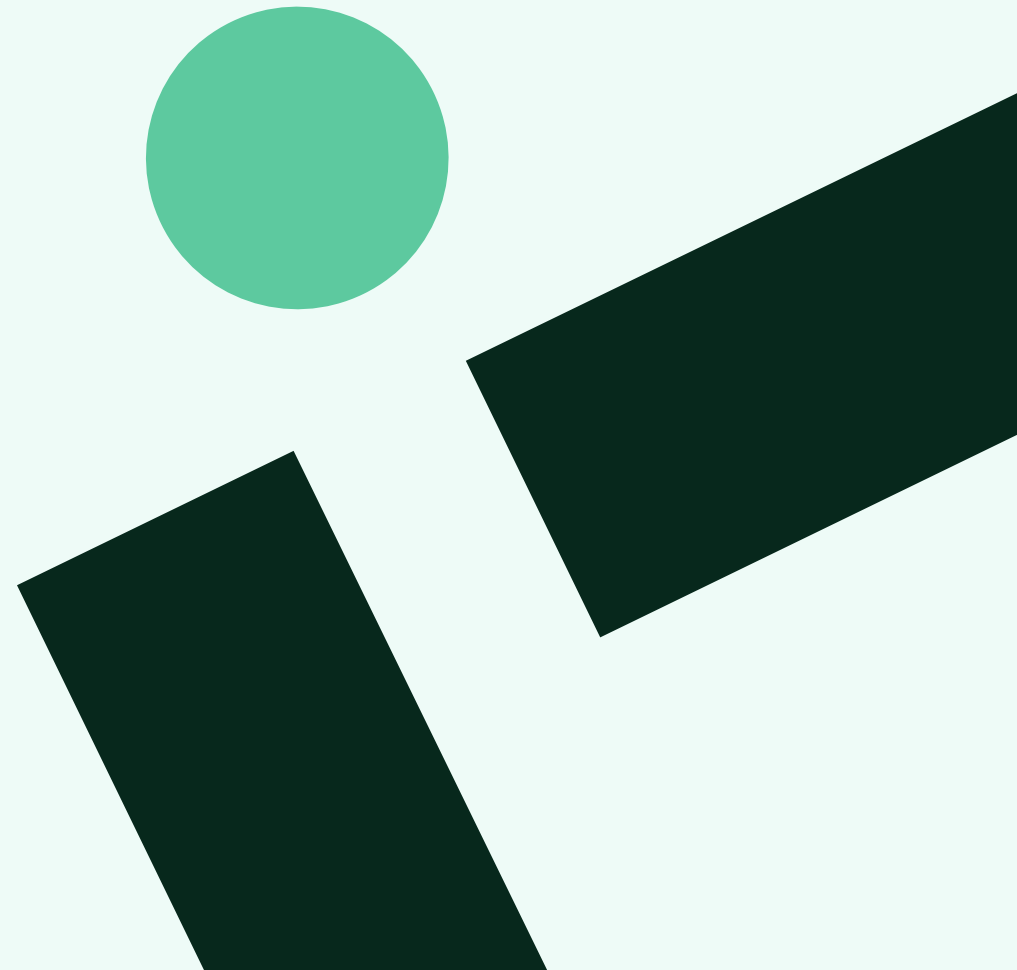
Criminals who may hold bitcoin (perhaps as payment from successful extortion attempts) will now have access to increased resources. Resources that, in many cases, are already substantial. It is possible that the increased price in Bitcoin will somewhat galvanise the underground cybercriminal market, and financially motivated threat actors. As with any attack against consumer "banking", key battlegrounds will continue to be centred around a victim's identity and authentication material. This assessment is predicated upon the value of Bitcoin, a notoriously volatile asset, holding or growing.

# Emerging Technology

## Artificial Intelligence

Artificial intelligence is advancing rapidly and becoming increasingly available to the general public<sup>13</sup>. New and improved models are being released with increasing frequency, continually improving both output accuracy and quality. From a conceptual perspective there are currently some fundamental limitations which mean Artificial General Intelligence (AGI) has not yet been achieved, which is somewhat curtailing the current impact of artificial intelligence. True AI reasoning is not yet possible, meaning a human (in this case, an attacker) needs to remain 'in the loop'. Despite this, there will almost certainly be a marked capability boost that will assist good and malign actors alike.

Many commercially available Large Language Models and Generative AI (genAI) services contain guardrails that prevent harmful or illegal content from being created. This being said, there are many open-source models available, giving actors the opportunity to deploy malicious and unregulated generative AI<sup>14</sup>. Because deploying a private model is not as simple, capable, or cheap as using commercial genAI solutions, threat actors are seeking to circumvent the guardrails put in place by the genAI services. It is relatively simple to do so, and security researchers and cyber-criminals alike are freely sharing how-to guides to 'jailbreak' generative AI capability. This demonstrates a nascent but increasing rate of adoption of freely available AI services by criminals.



## Lowering the bar

In its current state, and also likely with the next iterations of models, Generative AI presents an extremely useful tool for threat actors, but it is unlikely to drastically revolutionise cyber-attacks in 2025. Instead, it will probably supplement and enhance actors who will be able to achieve broadly what they currently achieve, more cheaply and more efficiently. The impact it will have on the cybercrime landscape should not be understated however, as the gaps between the most capable and least capable actors will narrow. The rate of capability advances in AI lowers the ability to forecast longer term with high confidence.

The advent of AI has not changed the fact that ransomware is a primary threat to the European mid-market. In the short term, an increase in the sheer number of criminal actors capable of operating somewhat effectively in this space may be more damaging on the whole than the AI led development of new and highly advanced attack-techniques. These may come but will almost certainly be pioneered by highly capable state-sponsored intrusion sets, likely operating to a far more specific victim profile than the European mid-market.

Artificial intelligence will bring benefit to attacker and defender alike; therefore, its impact on the cyber landscape will be an economy, offering and unequal set benefits and drawbacks to the network defence mission. Legitimate enterprise will have better access to more capable AI, and therefore throughout 2025, AI will probably drive a net positive for network defenders and legitimate cyber security functions, so long as it is democratised and available to those without large IT budgets.

## Geopolitical Implications

The European Union note that “embracing AI technology will likely determine the path of the EU's future economic development”. This view is almost certainly shared by other economies, making access to the technology and materials that underpin AI a key geopolitical battleground<sup>15</sup>. Regulation around AI will be a key topic of discussion in 2025, as authorities will be under pressure not to ‘over-regulate’ its use and deployment in order to unlock more economic potential. Of course, looser regulation can leave a technology more open to abuse.

## Attacks against AI

WithSecure Consulting are at the forefront of research into both attacks against AI/LLMs, and attacks using AI/LLMs. As it is still a relatively nascent capability this research is relevant to the threat outlook in 2025<sup>16</sup>.

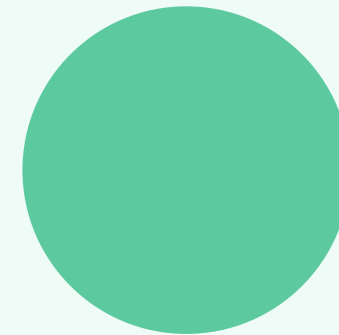
## Agentic AI

Agentic AI is a method of allowing artificial intelligence to act independently in order to achieve its set goals. Agentic workflow adoption by organisations will almost certainly rise into 2025, which will in turn increase the risk of prompt injection attacks, which goes unsolved in even the latest OpenAI o1 models. If jailbroken, these workflows can of course also be misused by actors with malign intent. It is highly likely that there will be a high level of intent by actors, however there will be limits to how it can be deployed 'in anger'. At the time of writing the report Anthropic has released a beta capability called 'computer use' which seeks to emulate a human using a computer.

This has led to speculation regarding the use of agentic AI in operating command and control functionality. In reality this capability is ineffective in its current form and would possibly even present a higher detection rate than other command and control methods. As with other AI concepts, if Agentic AI can get out of its current 'prototype/research' state, workflows will offer some benefit to malign actors, just as it will to legitimate users, but it is unlikely that there will be a significant increase in threat as a result. AI is under rapid development and as the capability increases it is possible this assessment will change.

## Deepfake technology

Deepfake technology is already being deployed by fraudsters and scammers, and as noted, this is out of scope for this report as these are not computer network exploitation/attack techniques. This being said, it has been noted that with the prevalence of social engineering techniques, deepfake technology will possibly be seen as a viable way to optimise and enhance social engineering elements of a computer network intrusion.



## Quantum Computing

Quantum computing has long been touted as a transformative technology that will greatly undermine some of the encryption standards that are critical to information system security and authentication processes. Theoretically, quantum computers can also weaken symmetric encryption (although increasing key lengths may offer sufficient mitigation in the short term). There is little doubt that quantum computing will seriously impact the security landscape when it does become generally available, although it is unlikely to represent a significant and direct threat in 2025. Organisations will be, and have been, instructed to start preparing for a post-quantum world, where quantum resistant encryption techniques will need to be deployed. Many Cloud Service Providers (CSPs) are already adding quantum resistant encryption methods to their offering. There is also speculation that some governmental organisations are engaging in 'collect now, process later', although we do not have evidence of this at WithSecure. Quantum computing is advancing, and Google have demonstrated some new capability with their Willow processor, and while it is almost certain this will not be a threat to the European mid-market in 2025, many organisations should begin future-proofing.

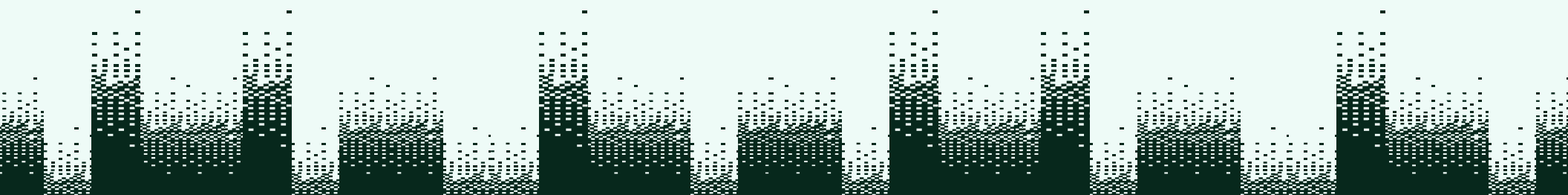
# Battlegrounds 2025

## Identity and Cloud

The more cloud becomes an intrinsic part of the fabric of organisational networks, the more we see the evolution from cloud-aware to cloud-astute threat actors. The use of legitimate tooling and functionality to complete illegitimate tasks will be a key theme that network defenders will have to grapple with in 2025 – continuing from 2024. We have started to observe known cloud services used as nodes in attacks, not only limited to C2 infrastructure. As organisations have become increasingly 'de-perimeterized' it has catalysed the infostealer industry and theft of identity/authentication material activities will continue to be a key trend, although this does not mean mass edge service exploitation will cease in 2025.

Major Cloud Service Providers (CSPs) are resourced enough to employ their own full time incident response capability. This makes it extremely difficult to conduct assessment on the threat to Cloud infrastructure providers, particularly if seeking clarification as to whether an absence of evidence regarding compromises of underlying cloud infrastructure systems can be interpreted as evidence of absence. An key issue with cloud technology is that service users often do not have visibility into specific data residency, vulnerabilities or incidents involving the underlying infrastructure and systems that underpin 'aaS' services.

Because cloud computing represents such a large paradigm shift in the information system architecture of global business, there specific paragraphs throughout this report that will not be duplicated in this section. Readers should refer to these sections for a more granular understanding of the cloud threat surface, contextualised by the threat type.





# Mobile

Mobile devices are now the personal computing device of choice for individuals. For this reason, the targeting of mobile devices has long been an effective way to target personal banking. There are also numerous examples of sophisticated, highly targeted attacks against individuals of intelligence value.

Apple iOS devices automatically push security updates to user devices and applications must be downloaded from the official app store, only after attaining approval following rigorous scrutiny from Apple. Therefore, in order to target iOS devices attacks often require very specific expertise in order to discover and exploit zero-day vulnerabilities. Private intelligence companies have been known to purchase such '0-click' [no user interaction] vulnerabilities for \$1million US dollars. Because these exploits are so high value, and as they often become mitigated shortly after discovery by researchers, they are not often deployed widely. For this reason, it is unlikely that threats specific to Apple iOS devices are a significant threat to the European mid-market enterprise as a whole, however there could of course be specific exceptions to this for individuals and individual organisations.

There is a higher threat to Android devices, this is because the environment is far less restrictive for application developers. Mobile malware reported on in the public domain predominantly targets sensitive information, with a view to accessing bank and cryptocurrency accounts. This makes it a threat to individuals and small business owners. Android mobile banking malware is far more common in South America than Europe and it is highly likely this is due to cultural practises and differing controls imposed by a banking sector. Targeting mobile devices isn't a particularly viable vector for ransomware actors but organisational resources are often accessible through such a device. Therefore, mobile malware will be a moderate to low threat for European mid-market, where adequate controls and policies are in place.

It has long been predicted that as mobile device adoption sharply rises, mobile threats will also. This has not transpired as expected, in part due to effective security restrictions put in place across mobile environments, but also as targeting endpoints is still a more viable way of gaining a foothold when seeking to compromise a network. It is highly unlikely that the mobile threat to the European mid-market in 2025 will be materially different from 2024.

## MacOS

Infostealers are the primary threat to MacOS users, and multiple MacOS Infostealer Malware as a Service (MaaS) providers are proliferating these infostealers. There is very little ransomware that specifically targets MacOS, and there is no indication that known MacOS ransomware variants are credible threats to the European mid-market. This is likely because MacOS has a lower share of the enterprise market, where ransomware makes the highest profits. There are also no MacOS servers, which is where ransomware is typically targeted for the greatest effect.

Because the Apple silicon processor architecture is shared between desktop and mobile Apple devices, it is possible that a single malicious application could be effective across multiple hardware platforms. At present however, there are very few known instances of iOS/mobile device malware, and this is unlikely to change into 2025.

MacOS market share is unlikely to change drastically in the next 0-5 years. The current major usage trend which hardware and software suppliers are betting on is LLMs, and it appears that Apple have stated that they are investigating on-device LLMs running on custom hardware. This could be an attractive solution to some users, but custom hardware is expensive, and so the price of Apple devices relative to their competition is unlikely to fall. As such, there is no reason to expect a sudden change in demand or market share.

With current geopolitical turmoil and the possibility of a trade war between the US and China, the price of all computer hardware could rise unpredictably, along with the prices of cloud services which do still run on hardware, like any other software. However, there is no reason to believe that Apple is any more exposed to that threat than any other manufacturer. Adoption of hybrid and cloud services is likely to continue, which allows users and organizations to choose the local device based upon personal preference rather than software compatibility. This could lead to more users choosing MacOS devices as they will be compatible with cloud business applications. However, it could also reduce the need to invest in endpoint hardware, moving the corporate device market further towards budget/thin client devices, and away from premium hardware such as Macs.

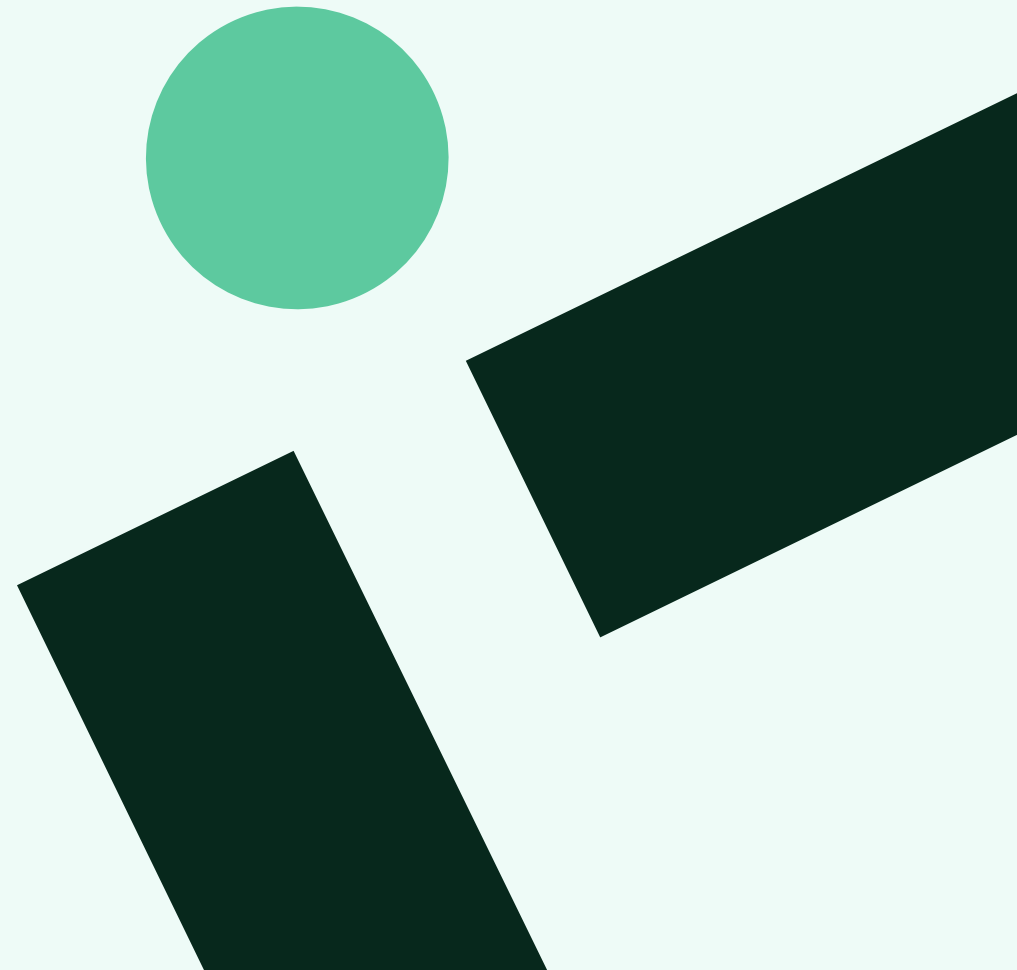
As cloud adoption continues to grow, attacks against cloud services and identity are also going to grow in popularity. As such, the off-device threat is likely to continue to grow for the users of all operating system including MacOS. The move towards MFA and cloud identity solutions means that in enterprise environments standalone infostealers will be less viable, however this is likely to lead to more social engineering attacks as attackers who have stolen credentials try to get through MFA protections.

# Linux

Similar to MacOS, there are no major signals that suggest that the market share of Unix will drastically change into 2025. A Unix-based OS, Linux is typically deployed less as endpoints/workstations than Windows/MacOS and therefore is mainly targeted in its capacity as a server, or host for 'on-premise' software services.

Criminal actors are Linux-capable, and many ransomware actors do have access to Linux specific ransomware executables.

Linux is a popular operating system for cloud computing services as it is cheap to deploy, and flexible in its usage. This applies for both 'host' and 'guest' cloud services. As cloud services become ever ubiquitous, there may be an increased intent against targeting 'host' services with a view to compromise information or the environment of the 'tenant' or 'guest' but it is unlikely that this will be commonplace in 2025. It is probably a capability currently only reserved for the most advanced nation state actors.



# Key Vectors

## Phishing

Phishing is the most common method of social engineering. Defined in the scope of this report as an electronic message that may be transferred over different mediums (although typically this is email) to harvest authentication material or sensitive information from a victim.

Social engineering will remain a significant threat to all organizations in 2025. Very few technical controls can be applied to defend against social engineering attacks. This is possible through anomaly detection and key phrase detection, and it will become less challenging as LLM implementations mature. However, the most capable arbiter of whether a message is business as usual, or a social engineering attack will often be the user.

By 2027 the number of email users will increase 9% to 4.9 billion<sup>17</sup>, with a similar increase in the number of emails received per day to 410 billion. This is a 3% per year future increase, matching the 3% per year increase since 2018. As such in 2025, email will be the primary phishing vector. This said, alternative messaging formats are increasing in popularity with threat actors and the European mid-market should be conscious of the phishing threat through messaging platforms such as Microsoft Teams.

The number of SMS sent per year in the UK was shown to have dropped by 80% from 151 billion to 36 billion between 2012 and 2022<sup>18</sup>. However, while the number of SMS sent may have dropped, it is very likely that the number of SMS capable devices has increased and is unlikely to fall in the medium term. As such, SMS will remain a viable phishing medium, until such a time as it is no longer used by victims as an MFA vector, or communication channel. It is possible IP based mobile communication may emerge as a successor to SMS attacks, however this will almost certainly require a better way to bind real-world to telephonic identity (which is currently phone numbers).

According to Ofcom, use of “online communication services”, which in this context means instant messaging excluding email, increased 1,300% from 100 billion messages per year to 1.3 trillion messages per year between 2012 and 2022, with a sustained growth rate of about 10% per year since 2018. If growth rate continues in the medium term there could be a greater than 50% increase in use of 3rd party messaging in the next 5 years. As such, it is likely that phishing via 3<sup>rd</sup> party messaging platforms will also increase.

There is no reason to believe that abuse of URLs or attachments as malicious payloads will decrease in the short term. The types of malicious payload being delivered typically reflect the most common victim environments (operating system, hardware, software) and the user environment market share/demographic does not change rapidly. There are likely to be brief spikes as new exploits relating to certain environments are discovered and heavily targeted, but these are unlikely to have long term effects on payloads.

## Phishing with AI

The UK NCSC assess the impact of AI over the next two years (2024-2026) will be tangible but not revolutionary, WithSecure Threat Intelligence concur with this assessment:

	Highly capable state threat actors	Capable state actors, commercial companies selling to states, organised cyber crime groups	Less-skilled hackers-for-hire, opportunistic cyber criminals, hacktivists
<b>Intent</b>	High	High	Opportunistic
<b>Capability</b>	Highly skilled in AI and cyber, well resourced	Skilled in cyber, some resource constraints	Novice cyber skills, limited resource
<b>Reconnaissance</b>	Moderate uplift	Moderate uplift	Uplift
<b>Social engineering, phishing, passwords</b>	Uplift	Uplift	Significant uplift (from low base)

## Attacker in the Middle / MFA

Attacker in the Middle (AiTM) is a technique actors use to intercept, or engineer, messages between a legitimate user and a legitimate service to capture credentials, sessions or Multi Factor Authentication (MFA) tokens. This technique is the most effective way of bypassing MFA controls and is likely to be a primary attack vector that the European mid-market will face in 2025.

At the same time, basic credential phishing emails may become less prevalent as a proportion of all identity attacks (particularly AiTM) if effective MFA becomes the default and there is a reduced reliance on credentials, however it should be noted that usernames and passwords are no longer the only authentication method employed in organizations.

MFA is still largely optional, is not in place in many authentication processes, and does not mitigate for open session theft. Use of passkey authentication is low but increasing, with adoption reported to have increased by 400%<sup>19</sup> in 2024. Use of Passkeys is likely to push down the number of credential theft attacks but may just lead to more malware and social engineering attacks. AiTM attacks which specifically target passkey authentication have already been demonstrated by researchers<sup>20</sup> but are not commonplace “in the wild”.

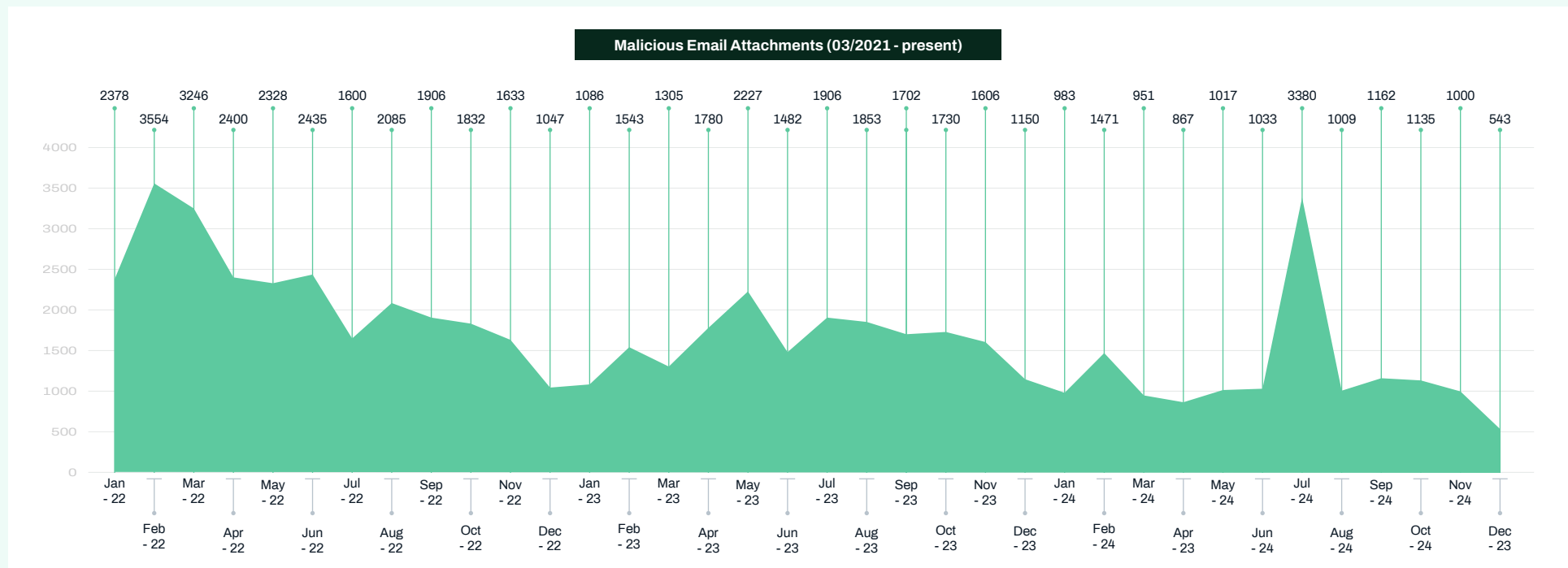
## Business Account compromise

Business Account Compromise (BAC) attacks are a form of phishing attack which takes advantage of existing trust relationships. Business Email Compromise (BEC) attacks are a type of BAC. BAC occurs when attackers gain access to a messaging account used by a business entity and use it to target the normal correspondents of that account with further phishing messages. Once they have access to a mailbox, actors will seek to modify invoices with erroneous account details, diverting legitimate payments. BEC/BAC attacks can be just as lucrative as ransomware operations, with frequent reports of organisations incurring eight figure losses.

As messaging based antimalware controls improve, Business Account Compromise (BAC) attacks will become even more valuable to attackers. This is particularly the case for pure social engineering-based attacks where there are no technical indicators that could be used to identify the legitimacy of a message by the recipient's messaging system. For this reason, BAC is a very high threat to the European Mid-market into 2025 as it will continue to present a cheap and technically unsophisticated way to extract extremely large sums from victims.

# Malspam

As email and malware protection technology and controls have advanced, actors are increasingly utilising more social engineering techniques to deliver malware rather than attaching the malware to the email itself.



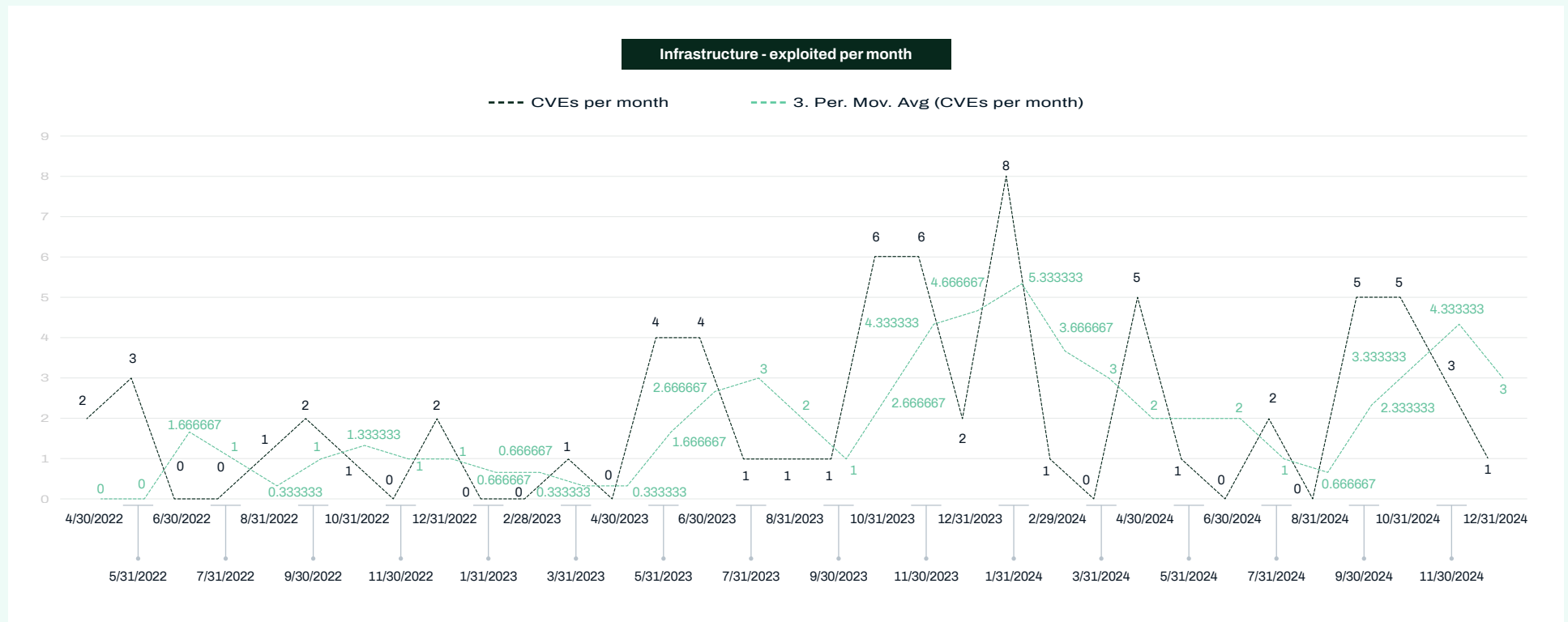
This may take the form of benign email attachments that seek to redirect victims one or more times before the final payload is retrieved. In general, separation of malicious elements and initial message from the attacker is designed to prevent email security tooling from being able to successfully scrutinise malign objectives of an email, however it relies on social engineering tactics to be effective. This concept is particularly stark in malware campaigns that have been dominating the infostealer space in the second half of 2024.

Actors are deploying more novel 'click to fix' or 'fake CAPTCHA' style lures – demonstrating the need for actors to deploy more creative social engineering techniques – which are often successful. For this reason, it is almost certain that the threat from broad messaging-based malware campaigns is low to organisations with adequate security tooling, however messaging services will be utilised to engage the European mid-market in social engineering campaigns that may end with infections of the very same malware.

# Infrastructure Service Exploitation

Edge and Infrastructure services are defined as the services that are internet facing, designed to facilitate ingress/egress of users, data or instructions. Infrastructure devices can also be considered as the networking hardware that underpins IP infrastructure. Throughout 2024, Edge/Infrastructure vulnerabilities was cited as the top initial access vector, where a vector is known.

In 2024 WithSecure Threat Intelligence released assessment into the threat posed from actors capable of exploiting vulnerabilities in edge services, often en-masse. The research found that since 2022 and through 2024 the number of actively exploited infrastructure vulnerabilities has increased, on average each year. While the volume of exploited vulnerabilities peaked in early 2024, a higher frequency of such exploitation campaigns can now be considered the new normal going into 2025.





The threat from infrastructure exploitation is so severe that as of December 2024, the United States is reportedly considering a ban for a particular brand of routing equipment, TP-Link. This is almost certainly due to the number of security vulnerabilities present in the devices, a perceived low level of cooperation with security researchers, and poor response to remediating these issues<sup>21</sup>.

There are numerous commentators who have raised concerns over code quality issues in many enterprise infrastructure services. Where this is coupled with a number of threat actors and security researchers actively conducting vulnerability research into such devices, there is almost certainly a very broad threat surface, and a number of actors with the capability and intent to exploit it.

Infrastructure targeting is often indiscriminate and a part of the kill chain for financially motivated threat actors. This is therefore a significant threat to the European mid-market.

## Supply Chain

The 2020 SolarWinds incident brought the supply-chain threat to the forefront of public consciousness. Since then, there have been a number of impactful supply-chain attacks, mostly targeting the build process of legitimate software which is then distributed, signed as legitimate software, to users. Another form of supply chain attack would be to target outsourced services in a way that impacts upon 'downstream' organisations. A striking example of this is the 2023 MOVEit campaign, where managed file transfer services were targeted en-masse, leading to the theft of data from hundreds of organisations globally. This particular attack was conducted by a ransomware collective, who will continue in 2025 to target externally facing services such as file transfer solutions.

## Service providers

The targeting of service providers (including [cloud service providers](#)) is an effective way to target an organisation. Generally, there is a low threat to a 'typical' European mid-market organisation from the highly precise targeting of specific service providers in order to compromise a victim. Compromises of CSPs (in cases such as Microsoft, discovered January 2024) are typically reserved for the most capable threat actors. This said, there are many examples of small / medium sized enterprises being impacted as collateral through 'non-targeted' supply chain attacks. Two such examples are the 2023 compromise of identity provider Okta and a campaign targeting a vulnerability in the remote management tool ScreenConnect. The latter impacting many WithSecure customers as an opportunistic attack. Threat actors targeted vulnerabilities in ScreenConnect remote management tooling, used by managed service providers, and deployed malware downstream.

There is an inherent level of trust between service providers and their customers, and it is almost certain that there are inherent vulnerabilities in products of service providers (including SaaS services) that will be exploited in 2025. While it is not possible to predict with adequate confidence which specific products will be exploited in 2025 we can state with high confidence that the threat from supply chain attackers to the European mid-market is high.

## Software Supply Chain

Towards the second half of 2024, WithSecure Threat Intelligence has noted a rise in reporting relating to poisoned software supply chains. Using pseudo-watering hole style attacks, actors are targeting developers and to a smaller extent, specific industries by pre-positioning software libraries that may be imported and executed by developers.

This provides a way for attackers to run malicious code in a way that both bypasses some anti-malware tooling and application allowlisting. Furthermore, it provides a way to target high-privilege users (developers) and development environments relatively indiscriminately.

There are many examples of malicious software packages being discovered in open-source repositories – namely PyPi and NPM, and it is almost certain that more will be discovered in 2025. Such payloads often contain infostealer elements, seeking credentials and environment keys. This means the full impact of this threat may not yet be fully understood as it is extremely difficult to ratify subsequent impact stemming from use of the stolen material back to the malicious package. The Log4j vulnerability in 2021 was a stark reminder that many organisations do not have a robust handle on what vulnerable (or malicious) open-source software libraries are present in enterprise software. It is therefore likely the software supply chain threat for the European mid-market will be significant in 2025.

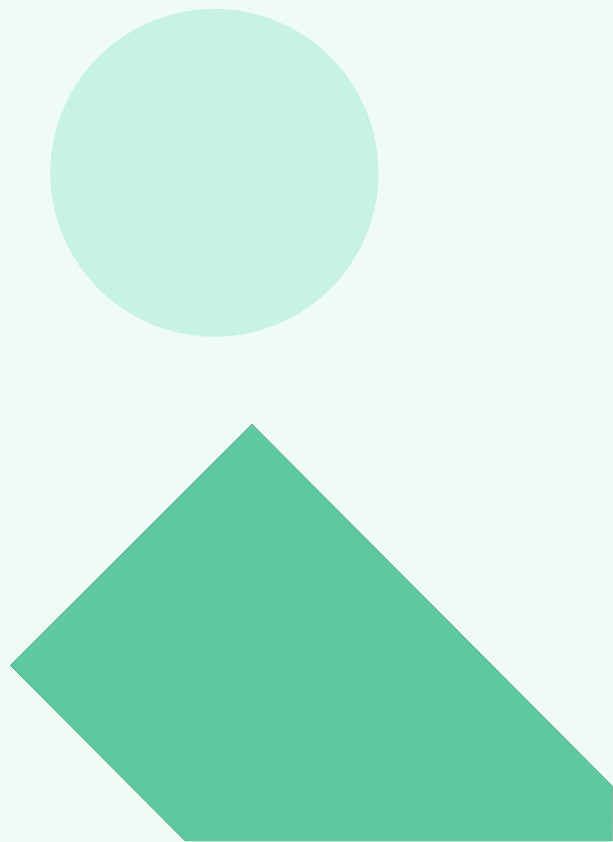
## Legitimate Tooling

Throughout 2024, WithSecure Threat Intelligence noted an increasing use of more diverse legitimate tooling for illegitimate purposes. This is not a new tactic malicious actors use; actors have long exploited poor abuse response functions in content delivery services (such as Cloudflare) to host and obfuscate the infrastructure they deploy. Legitimate Remote Management and Monitoring (RMM) tooling is now used very frequently in ransomware deployments. This will continue into 2025, almost certainly due to the fact that it is legitimately used. While an RMM tool achieves the same tasks as remote access trojans, it can bypass anti-malware security tooling, works well with the common “IT support” lure, and even comes ‘out of the box’ in some Windows versions.

## Cloud services

This tactic is likely to expand into 2025 as compromised or newly established infrastructure on common Cloud services will begin to replace many newly registered domains or ‘raw IP’ based virtual infrastructure. This presents a challenge for network defenders as it undermines malicious domain detection based on the attributes of that domain. It is far harder for a human analyst to identify a malicious URL that sits as part of known, used, and legitimate infrastructure<sup>22</sup>. Cloud Service Providers (CSPs) instruct users to explicitly trust their storage infrastructure, which is problematic when compromised or malicious, but trusted, instances of such services are utilised in attacks. This tactic has been observed since at least 2018, however in general, as cloud adoption increases, misuse of these same services also will<sup>23,24,25</sup>. It is almost certain that this vector will be somewhat mitigated by in-house trust and security capability for the major CSPs, however it does represent another example of involuntary outsourcing of cyber security visibility and capability.

As cloud services become more prevalent in the mid-market into 2025, threat actors will increasingly utilise the capability that this affords them on a network to perform other elicited tasks. Rather than introduce erroneous tooling (such as RClone/MEGAsync) ransomware actors have been observed utilising native cloud capability, in one example: Azure Storage Explorer<sup>26</sup> to exfiltrate data to attacker-controlled tenants. This principle can be extended to a number of legitimate cloud service functionality and while this presents effective and stealthy capabilities to threat actors, this will remain a viable and increasingly popular attack vector.



## Outsourcing control

A relatively new way of targeting an organisation, is through targeting their Cloud Service Provider. This was realised in 2024 when organisations were impacted through the compromise of Microsoft by a Russian intrusion set. Victims are almost entirely unable to mitigate this risk in isolation, and in some cases, did not have a contract value high enough that allowed them access to logs in order to audit who had accessed their own data<sup>27</sup>. While this presents an alarming issue for certain organisations and should serve as a reminder that utilisation of cloud services does somewhat outsource control, it is unlikely to represent a systemic threat to the European mid-market in 2025. This is because actors who are able to bring this level of capability to bear are almost certainly more concerned with specific objectives, targeting specific organisations. Organisations in the European mid-market who may be targeted by such actors are outliers and should employ their own threat modelling processes to mitigate this.

## Social Engineering

There has been a concerted and consistent effort to train users in understanding and recognising unsafe actions or social engineering (i.e. recognising a phishing email). While this is an issue that still persists, the successes in this area are predicated on the fact that users have an adequate (even if still extremely limited) understanding of the workings of a modern operating system. As we continue a move to Cloud services and the complexity is hidden from a user, this user-education effort is somewhat undermined. Users who now may be able to recognise password phishing emails, may not be able to define or recognise consent phishing. This will increase the ability for actors to perform social engineering attacks as Cloud services are increasingly adopted in 2025 and beyond.

## Vulnerable Drivers and AV tools

Deploying legitimate, yet inherently vulnerable drivers with a view to disabling security tooling is referred to as a Bring Your Own Vulnerable Driver (BYOVD) attack. This was a common vector through 2024 by ransomware actors seeking to tamper with EDR products. Legitimate and free rootkit removal tools were also deployed to stop EDR services. This poses a challenge for security tooling as such drivers were often signed, legitimate pieces of software, meaning that detection is often reliant on heuristic measures which may not be as comprehensive as other high fidelity detection logic.



## Malware

### Infostealers

This report has noted the emergence of infostealers as a primary malware threat, catalysed by off-premises services shifting a key battleground to the identity. Infostealers are readily available to criminals, often being “licensed” for a relatively nominal monthly fee. Infostealers are under active development with regular developments in stealth and functionality.

Infostealer actors have frequently demonstrated progressive and innovative ways of infecting a victim computer, from novel social engineering techniques to watering hole style infections (explored under the header [‘Watering hole’ Style Attacks](#)).

WithSecure has noticed frequent and successful infostealer malware infections across its customers. It is highly likely that most enterprise EDR/EPP is capable enough to detect and prevent most infostealer activity, however this is often reliant on full EDR/EPP coverage, and complete ‘alert’ actioning. It is often very difficult to associate an incident (i.e. Ransomware event) with an initial credential-theft event, therefore it is difficult to apply a broad brush quantification to the impact of the theft of authentication material.

## In-browser

Browser attacks are increasingly common as they are a.) a valuable store of sensitive material, and b.) are increasingly used as the interface with a SaaS (thin client) environment. Browser plugins can exist outside of the purview of security tooling and have the ability to access and perform a number of malign tasks such as the collection of sensitive data, installing malware or redirecting users. As an extension of the [software supply chain](#) principle, browser extensions can also be installed from untrustworthy repositories, giving threat actors the opportunity to deploy malicious executable elements that may bypass controls such as application whitelisting.

## Social Engineering

Security tooling has been under active development for many years and is increasingly capable at countering known and common initial access techniques. This leaves actors with two main options to circumvent security tooling 1.) seek to disable or bypass security tooling, 2.) employ social engineering techniques.

When considering initial access, the traditional status-quo was delivery through malspam. This is largely ineffective as advances in email security tooling and years of user awareness training has curtailed the ability of such email attachments to reach the end user. It is likely that in 2025 we will continue to observe a paradigm shift from “pushing” a malicious item (binary, link etc) to a victim, to careful prepositioning that socially engineers a victim to “pull” a malicious element from the attacker. These can be considered as akin to ‘watering hole’ style attacks, in that victims are shepherded towards pre-established, malign resources.

## ‘Watering hole’ Style Attacks

Threat actors have been observed by WithSecure deploying webpages masquerading as download pages for free or open-source software. Potential victims are then routed to these webpages using a variety of methods including, but not limited to: fake job postings, malicious ads, forum / video comments, or through the use search engine optimisation.

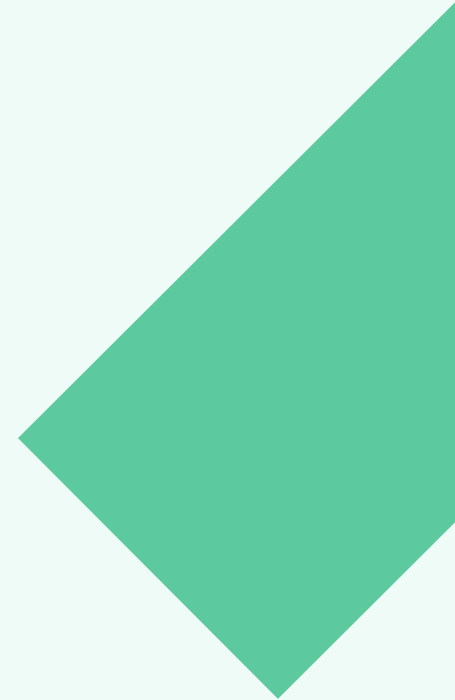
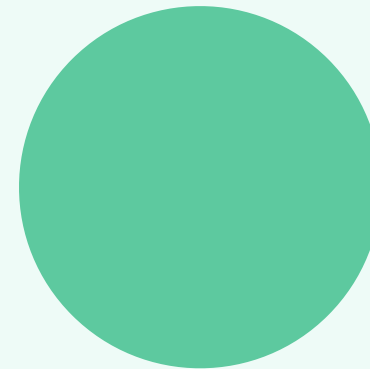
Software supply chain is a concerning malware proliferation tactic that we can consider to be ‘Watering hole’ style, covered in detail in the section [Supply Chain](#). Actors have been observed attempting to coerce victims to unwittingly run such code through typo squatting package names, or by suggesting code additions or fixes on collaborative coding platforms/forums.

# Conclusion

Cyberspace was extremely tumultuous in 2024, and the way that threats operate and manifest is consistently changing and evolving. These changes and evolutions are driven by stimuli surrounding political, economic, ideological and technological factors. As we move into 2025, all of these factors almost certainly will have changed and advanced from the environment in which we currently sit in December 2024.

Cybercrime is the world's third largest economy, ransomware victims are likely increasing, and geopolitical relationships are strained. Society is becoming more and more digitised and connected. It is little wonder that the CEO of the UK NCSC publicly stated that the risk facing the UK is "widely underestimated". This will also apply to other European countries.

Organisations in the European mid-market are faced with a broad spectrum of threats, pursuing many different objectives, with different techniques, tactics, and procedures, and varying degrees of sophistication. In order to keep ahead of these threats, security teams must ensure they can operate as proactively as possible to ensure that the mitigations they have in place against ever-evolving threats do not become more and more obsolete.



# About WithSecure™

WithSecure™, formerly F-Secure Business, is Europe's cyber security partner of choice. Trusted by IT service providers, MSSPs, and businesses worldwide, we deliver outcome-based cyber security solutions that protect mid-market companies. Committed to the European Way of data protection, WithSecure™ prioritizes privacy, data sovereignty, and regulatory compliance.

Boasting more than 35 years of industry experience, WithSecure™ has designed its portfolio to navigate the paradigm shift from reactive to proactive cyber security. In alignment with its commitment to collaborative growth, WithSecure™ offers partners flexible commercial models, ensuring mutual success across the dynamic cyber security landscape.

Central to WithSecure's™ cutting-edge offerings is Elements Cloud, which seamlessly integrates AI-powered technologies, human expertise, and co-security services. Further, it empowers mid-market customers with modular capabilities spanning endpoint and cloud protection, threat detection and response, and exposure management.

WithSecure™ Corporation was founded in 1988, and is listed on the NASDAQ OMX Helsinki Ltd.

<sup>1</sup> Agentic AI is a type of artificial intelligence (AI) that can make decisions and take actions independently, with little to no human intervention. Agentic AI systems can learn from their environment, adapt to changing conditions, and pursue complex goals

<sup>2</sup> <https://rhinosecuritylabs.com/aws/s3-ransomware-part-1-attack-vector/>

<sup>3</sup> [https://www.trendmicro.com/en\\_us/research/24/fj/fake-lockbit-real-damage-ransomware-samples-abuse-aws-s3-to-steal.html](https://www.trendmicro.com/en_us/research/24/fj/fake-lockbit-real-damage-ransomware-samples-abuse-aws-s3-to-steal.html)

<sup>4</sup> <https://www.sentinelone.com/blog/the-state-of-cloud-ransomware-in-2024/>

<sup>5</sup> <https://www.greynoise.io/blog/ivanti-connect-secure-exploited-to-install-cryptominers>

<sup>6</sup> <https://viz.greynoise.io/trends/active>

<sup>7</sup> <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china>

<sup>8</sup> A visual representation of China's territorial claims in the South China sea, encompassing Taiwan.

<sup>9</sup> <https://www.bbc.co.uk/news/articles/cm2796pdm1lo>

<sup>10</sup> <https://www.bbc.co.uk/news/articles/ce8vedz4yk7o#:~:text=The%20US%20and%20South%20Korea,have%20accidentally%20hired%20North%20Koreans.>

<sup>11</sup> <https://www.bbc.co.uk/news/articles/cly2jyvx55do>

<sup>12</sup> <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/#:~:text=Published%20by,and%20consumer%20connected%20car%20markets.>

<sup>12</sup> <https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/#:~:text=Published%20by,and%20consumer%20connected%20car%20markets.>

<sup>13</sup> <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>

<sup>14</sup> <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/>

<sup>15</sup> <https://www.mittrade.com/insights/news/live-news/article-3-527770-20241217>

<sup>16</sup> <https://labs.withsecure.com/home>

<sup>17</sup> <https://www.statista.com/statistics/255080/number-of-e-mail-users-worldwide/>

<sup>18</sup> <https://www.ofcom.org.uk/internet-based-services/technology/whatsappening-in-the-world-of-online-communications/>

<sup>19</sup> <https://www.theverge.com/2024/7/30/24209395/dashlane-passkey-report-adoption-passwordless-sign-on>

<sup>20</sup> <https://www.darkreading.com/cloud-security/passkey-redaction-attacks-subvert-github-microsoft-authentication>

<sup>21</sup> <https://www.cnet.com/home/internet/possible-tp-link-ban-in-2025-what-it-means-for-your-internet-connection/>

<sup>22</sup> [https://www.jlaundry.nz/2024/creating\\_a\\_c2\\_using\\_blob\\_core\\_windows\\_net/](https://www.jlaundry.nz/2024/creating_a_c2_using_blob_core_windows_net/)

<sup>23</sup> <https://www.bleepingcomputer.com/news/microsoft/phishing-uses-azure-static-web-pages-to-impersonate-microsoft/>

<sup>24</sup> <https://www.zscaler.com/blogs/security-research/abusing-microsofts-azure-domains-host-phishing-attacks>

<sup>25</sup> [https://www.theregister.com/2023/06/19/npm\\_s3\\_buckets\\_malware/](https://www.theregister.com/2023/06/19/npm_s3_buckets_malware/)

<sup>26</sup> <https://www.sentinelone.com/blog/the-state-of-cloud-ransomware-in-2024/>

<sup>27</sup> <https://www.mitiga.io/blog/microsoft-breach-by-midnight-blizzard-apt29-what-happened-and-what-now>

<sup>13</sup> <https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/>