ebook

Ransomware Landscape H1/2024

Table of Contents

Executive Summary

There are emerging signals that the ransomware industry peaked in scale in the second half of 2023 (H2) and ransomware productivity is starting to level off.

Ransomware numbers and payments were still higher in the first half (H1) of 2024 than H1 2022, and H1 2023.

It is still not clear what the long term impact of Law Enforcement action will be on the ransomware ecosystem. In the short term it has ALMOST CERTAINLY contributed to the decrease of ransomware productivity.

Since 2022, Small / Medium sized businesses are increasingly posted to Ransomware data leak sites as a proportion of all victims.

Events surrounding Lockbit and ALPHV have LIKELY driven ‘nomadic’ ransomware affiliates towards more established RaaS brands. There is competition between ransomware franchises for affiliates.

Lockbit is ALMOST CERTAINLY in a rebuild phase intending on returning to the industry with a more robust operation.

Ransomware actors TTPs remain broadly consistent from 2023 into 2024. There has been an increased adoption of initial access through edge service exploitation since 2022, and a consistent and frequent use of legitimate remote management tooling.

Architecture of a Ransomware-as-a-Service Collective

Some ransomware brands will operate as a ‘private’ defined group where operations spanning initial access to extortion are kept internal. For this reason, we must specify where RaaS (Ransomware as a Service) models are employed – this is the case for most successful ransomware flavours.

In the WithSecure report ‘The Professionalization of Cyber Crime’, we detail the impact that ransomware has had on the cybercrime landscape. What is most important to note from this research is that ransomware groupings can, in the most part, no longer be entirely considered as a defined group of individuals working under a single brand umbrella. Despite the fact we track ransomware on a ‘per variant’ basis, this makes attribution of pre-ransom activity and TTP tracking very difficult for blue teams.

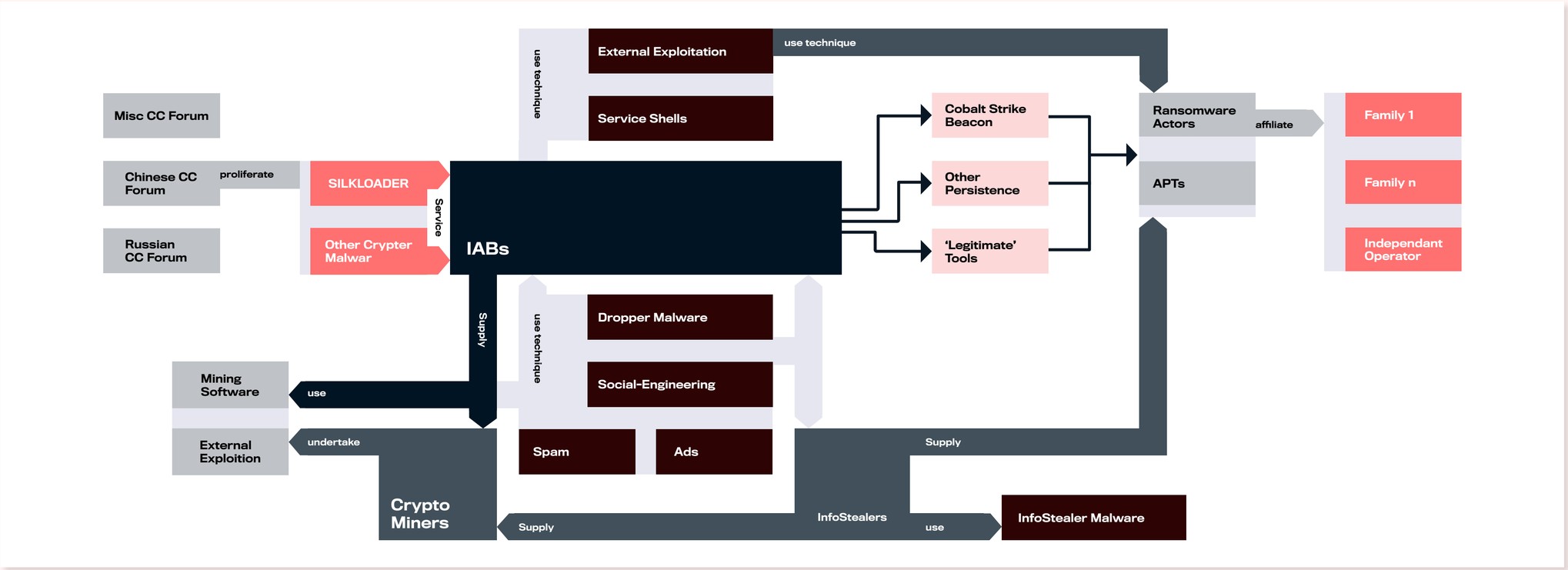


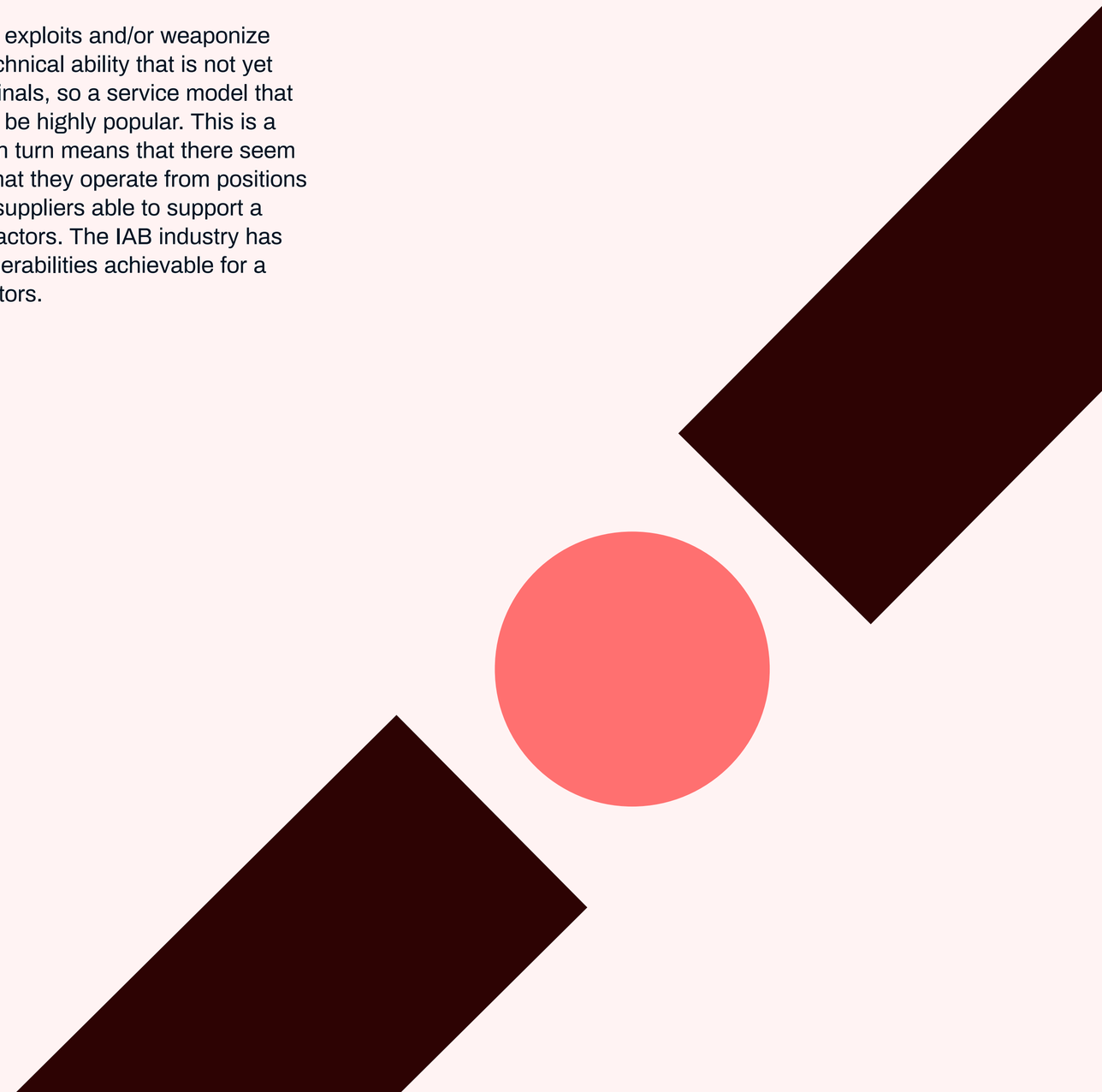
Figure 1 - Everything-as-a-Service ecosystem

The cyber security industry has had a stark reminder of this when excellent action by a Law Enforcement Agency (LEA) coalition infiltrated and disrupted Lockbit, by far the most prolific, organized and successful ransomware brand we have seen. As a result of the disruption, many of Lockbit's affiliates simply found a new ransomware brand to deploy and monetize their intrusions through.

Actors, particularly Initial Access Brokers (IABs), have industrialized Internet wide exploitation. One of the barriers to entry for malicious actors is the complexity involved with successfully orchestrating an internet wide exploitation attempt. Actors must:

- Understand how a vulnerability can be exploited
- Weaponize the exploit
- Bypass traffic filters in order to scan/exploit en-masse
- Record, maintain, and organise accesses/equities gained
- Develop and/or sell those accesses

The ability to reverse engineer exploits and/or weaponize them still requires a level of technical ability that is not yet accessible to many cyber criminals, so a service model that removes this barrier is likely to be highly popular. This is a scalable business model and in turn means that there seem to be relatively few IABs, but that they operate from positions of being well funded, capable suppliers able to support a wide range of other malicious actors. The IAB industry has made rapid exploitation of vulnerabilities achievable for a wider range of ransomware actors.



Exiting the industry

Lockbit takedown

On the 20th of February, an International Law Enforcement Agency (LEA) action codenamed Operation Cronos posted a seizure notice in place of the Lockbit leak site. In a deeply enjoyable display of irony and humor, the format of the Lockbit leak site was itself used to taunt Lockbit and to present information about the successes of the LEA operation, and information gained about Lockbit operations. LEA also gained access to the affiliate communications/control panel and were able to leave messages threatening Lockbit affiliates.

While the full extent of LEA's access to Lockbit is not presently public knowledge, what is known is that the operation seized several hundred cryptocurrency wallets holding ~$120 million, took control of 34 Lockbit servers, retrieved 1,000 decryption keys for Lockbit victims, and at the same time coordinated the arrest of two Lockbit associated hackers in Ukraine and Poland, respectively. In the week following the operation the Lockbit leak site was brought back online, along with a long message that attempted to downplay the effects of the take down. LEA also offered a $15 million reward for information leading to the arrest of senior Lockbit members, which does at least imply that they do not currently have such information.

The initial action taken against Lockbit was extremely successful for a few reasons, including (but not limited to) the amount of organisations it helped protect, and the psychological damage inflicted upon Lockbit's affiliates. With the ransomware ecosystem as well established as it is, degradation of a single ransomware brand does not always convince an individual actor to exit the industry when they can move to another RaaS project. This is discussed further in: 5.1.4 Lockbit and ALPHV Impact.

Particularly in June of 2024, Lockbit is showing signs of being in a rebuild phase. Researchers have noted that their extortion infrastructure is in a state of flux, with domains moving, different technologies being used to build the services and test-victims being added. While there has been Lockbit activity since the LEA action, It is almost certain Lockbit is working to harden its operations and return to operations.

At the time of writing this report, law enforcement work continues to attribute real world identities to Lockbit affiliates. This is significant work because it will really test the operational security of ransomware actors and the ability of western authorities to break through their veil of secrecy. If successful then the demonstration of this, particularly through offensive techniques, will likely be a strong deterrent for ransomware affiliates, especially those operating in a region with law enforcement who are willing to cooperate with the EU/US.

The Head of the Hydra

As noted, there are seemingly few factors motivating enough to compel a ransomware affiliate to exit an industry as lucrative as cybercrime. This concept is demonstrated when we look at the number of ransomware brands. Looking quarter by quarter since Q1 2023, we can see that the number of unique ransomware brands that posted at least one victim has gradually increased until Quarter 1 of 2024, where it peaked.

If we look at this data on a month-by-month basis, of course the general trend of victims is holding relatively level, however there is not a net increase of 'new' brands following LEA intervention into Lockbit or the ALPHV's exit scam (this is detailed further in subsequent sections). It is almost certain that as uncertainty rises in the ransomware landscape, affiliates have turned to more established brands. This is true as of June 2024.

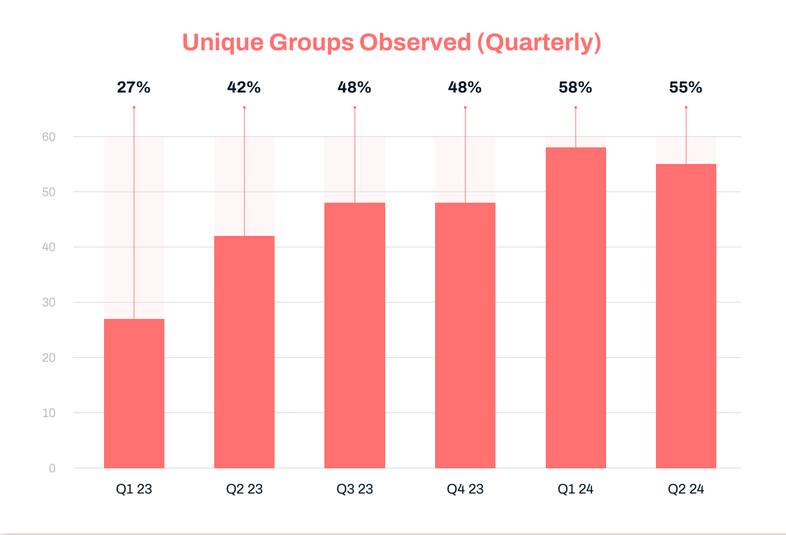


Figure 2 – Unique ransomware groups per quarter

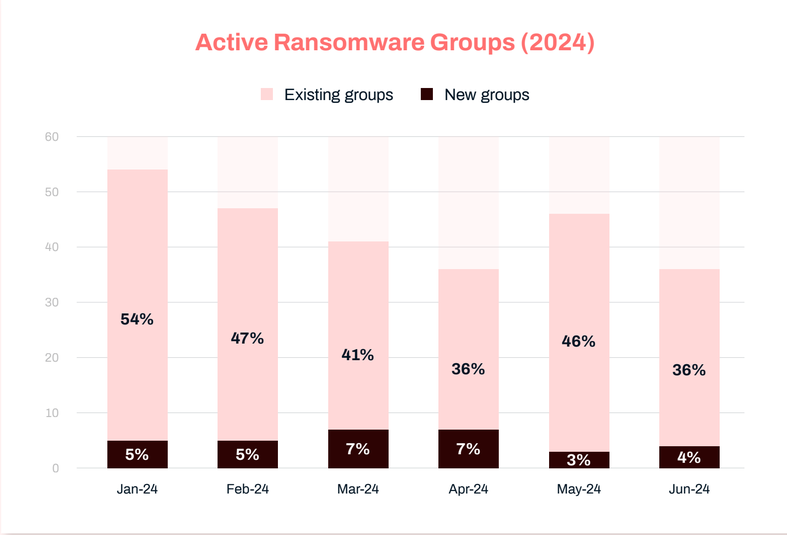


Figure 3 - Active ransomware groups by month (2024)

Throughout 2023, WithSecure observed and tracked **35 new** Ransomware groups. Of the total number of operational ransomware groups tracked in 2023 (67), **31** have not been operational in Q2 2024.

31 new ransomware groups have been seen in 2024, of which **nine** of these have not been observed at all in Q2. **13** new groups in 2024 have posted 5 victims or less, and it is unlikely many, if any of these projects will survive.

The role of trust

While on one hand the ‘everything as a service’ ecosystem lowers the bar for budding, lower skilled actors to enter the ransomware field, it does introduce a new weakness that can, and has been exploited – the role of trust between criminal actors. External measures such as the Lockbit LEA action, and LEA actions against AlphV/Blackcat will almost certainly have eroded inter-actor trust, there have been internal events that also will impact upon criminal relationships.

ALPHV ‘bow out’ with exit scam

In Q1, the US healthcare/pharmacy organization Change Healthcare suffered an ALPHV ransomware attack which resulted significant real-world impact for healthcare across the country and for the ransomware landscape. Several weeks after the attack, a person claiming to be the ALPHV affiliate who performed the Change Healthcare cyberattack posted on a Russian language cybercrime forum. They stated that while Change Healthcare had paid the $22 million ransom to ALPHV to prevent stolen data being leaked, ALPHV had not passed on the share that was owed to the affiliate. Instead, they suspended the affiliate’s account and kept the money. Change Healthcare has not confirmed that they paid such a ransom, however a cryptocurrency address which researchers have previously linked to ALPHV did receive a single, $22 million payment.

An apparent member of the core ALPHV brand posted to the same cybercrime forum stating that they were shutting down the group and had already found a buyer for their ransomware source code. They also stated that they “got screwed by the feds”, and ALPHV’s website was replaced with a law enforcement takedown notice. However, researchers rapidly noted that the takedown notice was just a screenshot of the previous takedown notice from when ALPHV were last taken down by law enforcement in 2023.

Looking at the sequence of events that have been reported, the most plausible explanation is that ALPHV have performed an exit scam, claiming to have been taken down by law enforcement and forced to shutter by forces beyond their control. It is almost certain they simply exited with the stolen money that they in turn had stolen from one of their fellow criminals. Despite Change Healthcare almost certainly paying a large ransom to prevent stolen data being leaked, the cybercrime forum member who claimed to be the affiliate who performed the attack has stated that they still have the stolen data. As such, it is very likely that they re-extorted Change Healthcare.

This is extremely significant as it is widely being cited as a reason not to pay a ransom. As mentioned earlier in the report, ransomware actors rely on organizations being confident that they can recover from the incident if demands are met, and this erodes this confidence. This has also impacted inter-actor relationships and trust, and this case has probably been the key driver behind some emerging RaaS brands the affiliation payment model of RaaS brands.

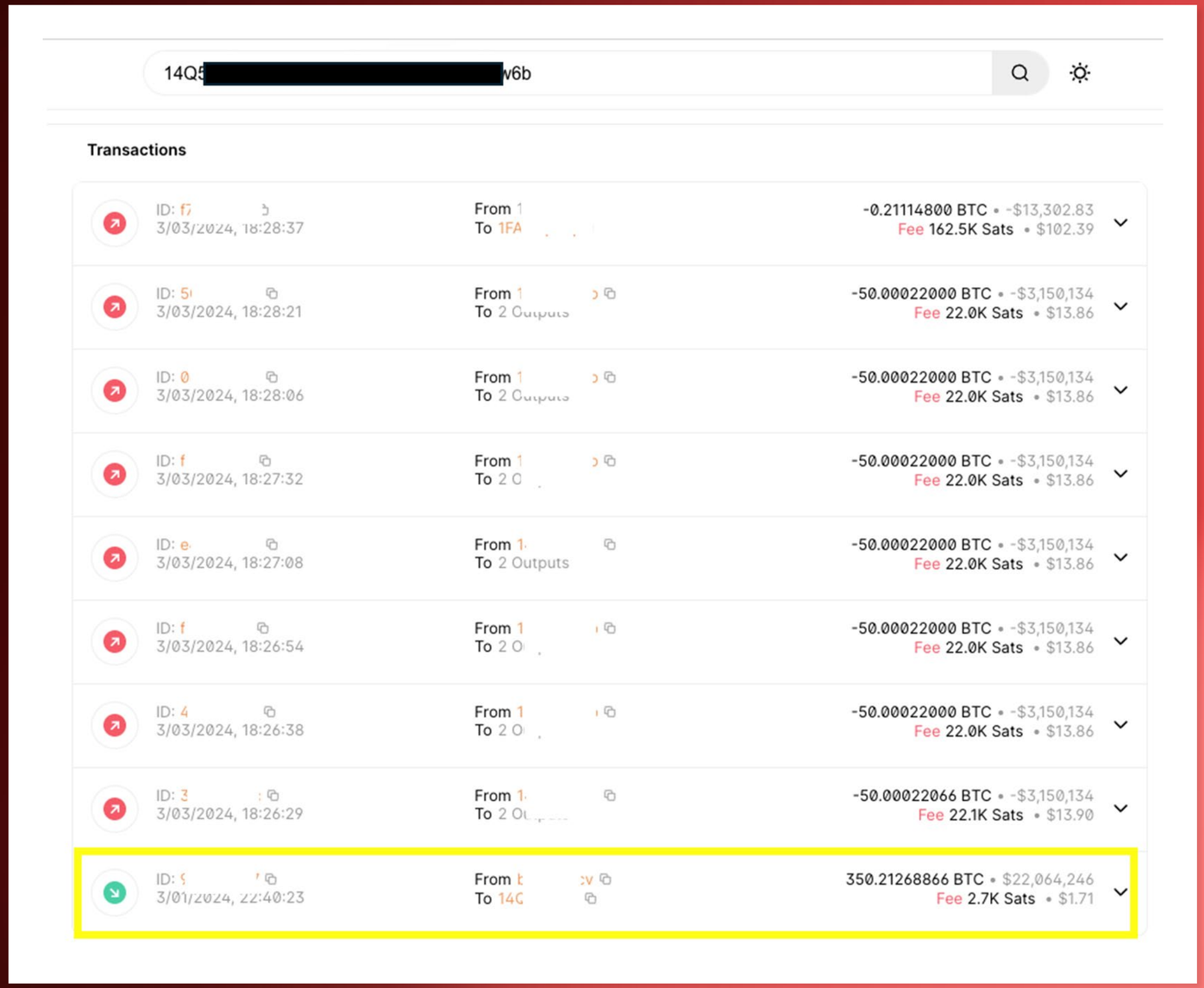


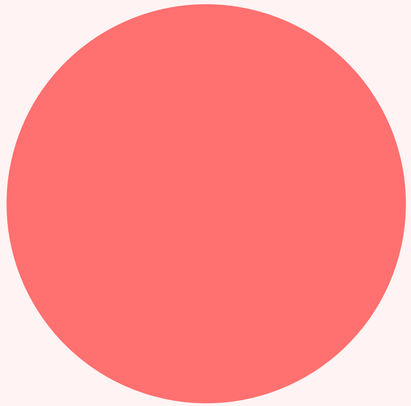
Figure 4 - $22million BTC deposit. Source: Blockchain.com

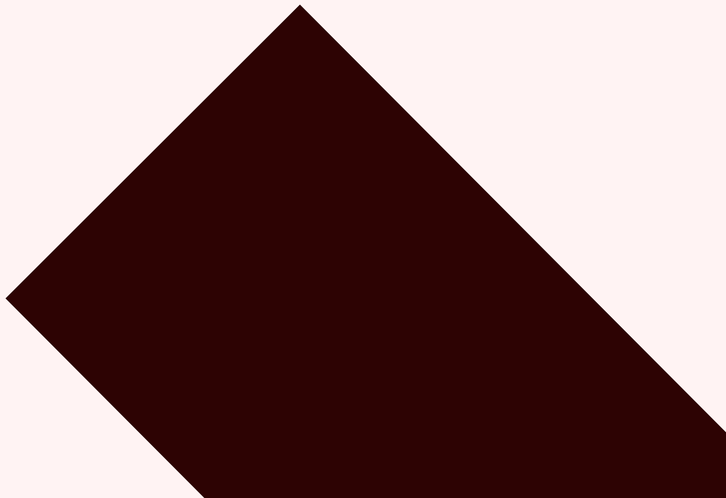
Rivalries

A report from researchers at GuidePoint Security investigates the ransomware ecosystem and gives insight into how it has responded to the recent shockwaves of the Lockbit and ALPHV (LE took control of ALPHV's breach site in December 2023) action, and the recent ALPHV exit scam. Interestingly, several smaller/newer ransomware brands such as Medusa, RansomHub, and Cloak appear to be trying to attract affiliate operators who have been directly affected or discouraged by the Lockbit takedown and ALPHV exit scam.

Medusa are offering generous profit-sharing percentages, with up to 90% going to the affiliates, stating that they would accept non-Russian speakers. Cloak's offering is not as radical as the other two groups, they still offer an 85% profit share to affiliates, with no initial payment needed to become an affiliate. This appears to have worked for Medusa, as victim numbers on the DLS surged following LEA action against Lockbit.

RansomHub on the other hand, are disrupting the RaaS orthodoxy by letting affiliates accept payment from the victims directly, before then sending their share to the RansomHub. This appears to be a clear attempt to reassure those who may have been spooked by ALPHV's exit scam, which was only able to occur because the payment from victims first went to crypto-wallets controlled by ALPHV, before ALPHV then sent the affiliate's share on to their own crypto-wallet. This appears to have worked as Change healthcare's second ranosom did go to RansomHub. Increases of victim numbers on RansomHub's leak site is also a signal that they have successfully lured some affiliates from rival brands.





These relatively dramatic offerings could be taken as an indication that while the law enforcement takedown of Lockbit and ALPHV may not have been immediately and directly able to eradicate the brands, they have applied great pressure to the ransomware industry, and it would appear that trust in Ransomware as a Service brands by their affiliates is at a very low ebb. From the perspective of a defender this is ideal, because if cybercriminals do not trust each other, and do not collaborate with each other, it is a very reasonable assumption that they will be less effective, less efficient, and easier to defend against.

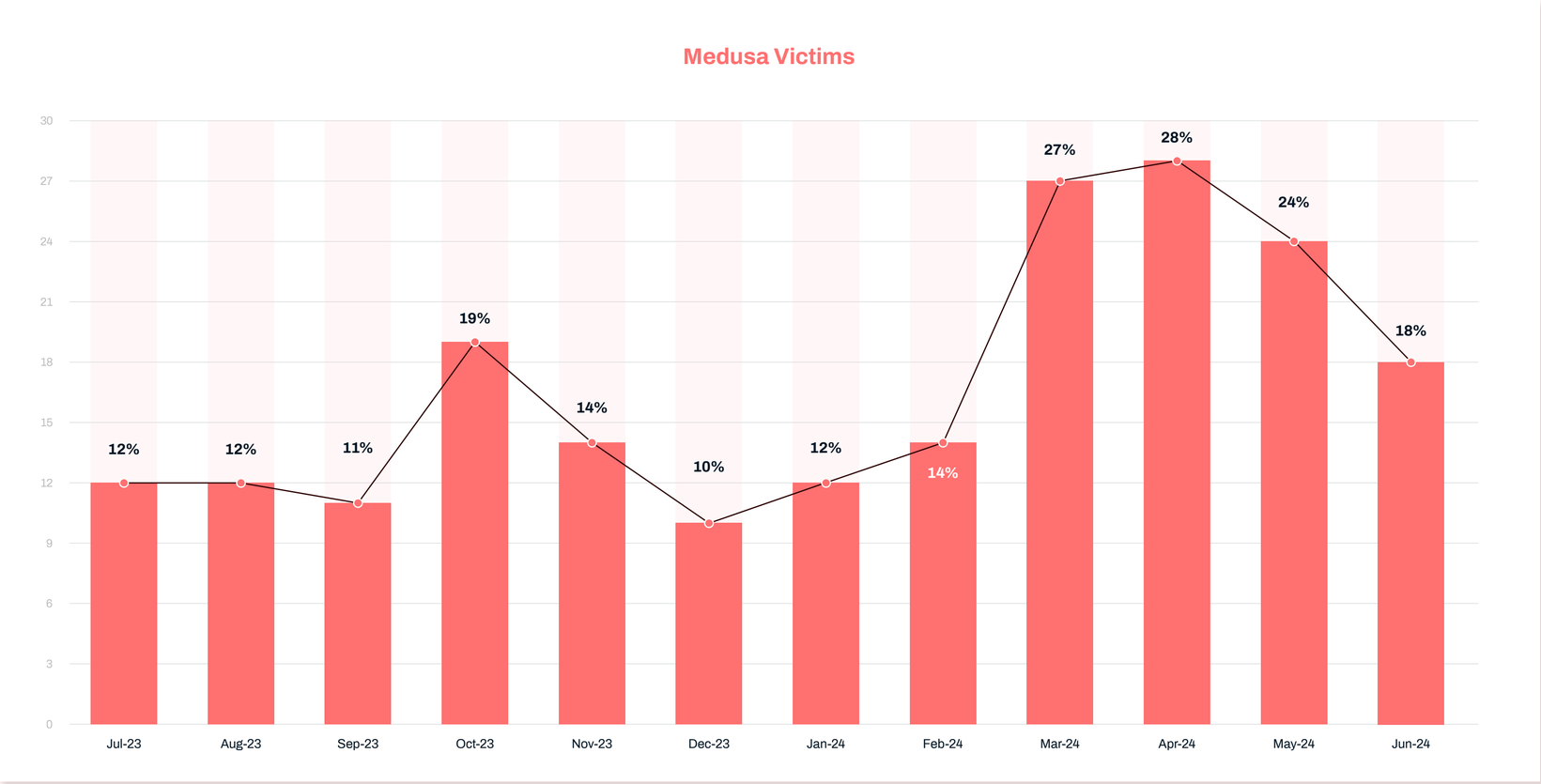


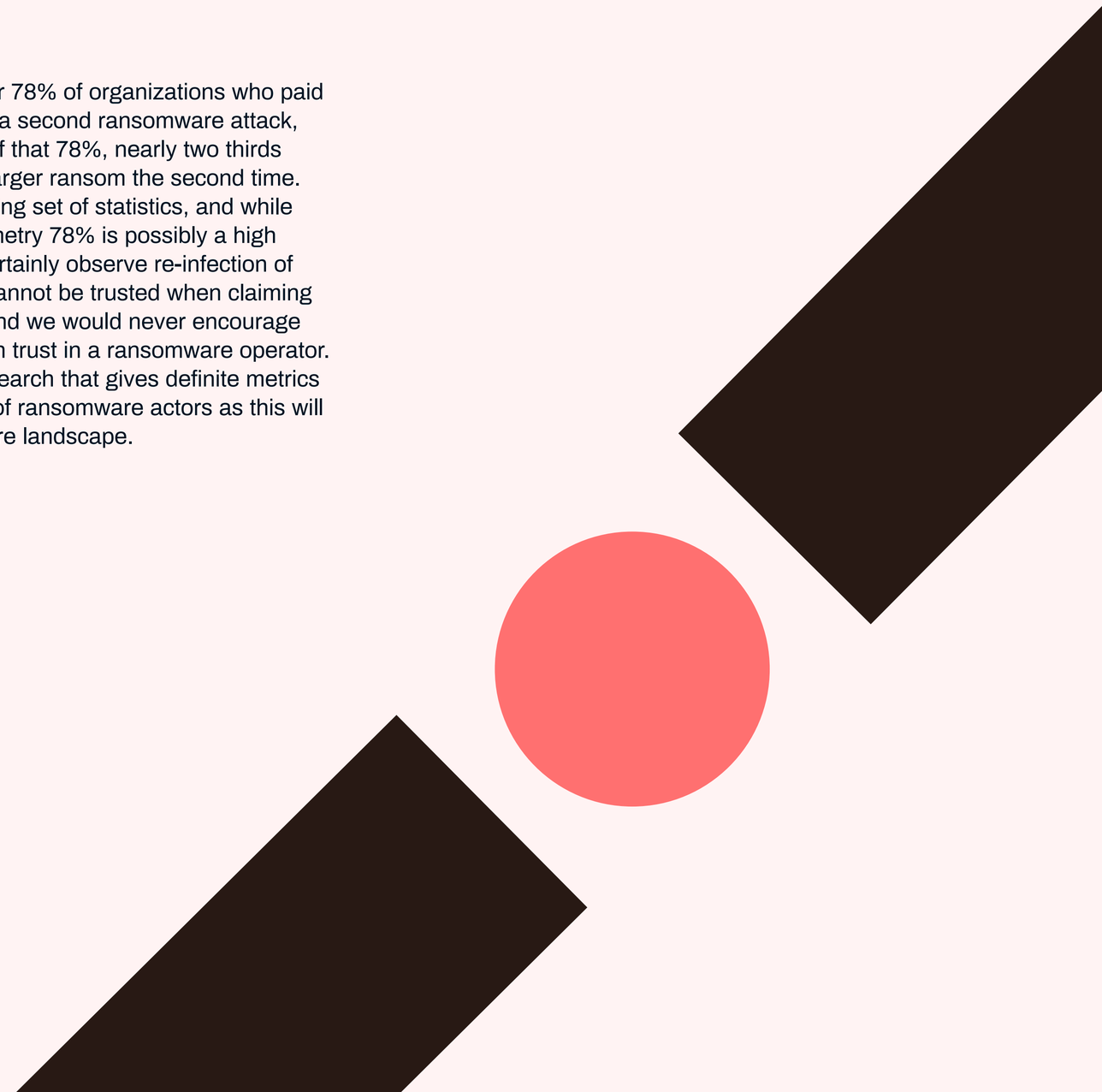
Figure 5 - Medusa victim count

Reinfection

Ransomware brands traditionally put a lot of effort into instilling a level of confidence in victims that they can recover if the ransom is paid. Successful extortion is based on the victim's belief that payment will ensure that normal business operations can resume as smoothly as possible. The argument for banning ransomware payments in legislature relies on this concept – it will undermine the core principle of ransomware operations; the willingness of victims to pay.

To better 'convert' victims into paying, many ransomware gangs attempt to project an air of competence, marketing themselves as 'pentesters' [penetration testers – legitimate offensive cyber security consultants] who offer a service to customers, namely offering details as to how the breach occurred, offering assurance that data will be deleted, and files will be decrypted.

According to Cybereason, over 78% of organizations who paid a ransom demand were hit by a second ransomware attack, often by the same actor, and of that 78%, nearly two thirds of them were asked to pay a larger ransom the second time. It's an interesting and concerning set of statistics, and while compared to WithSecure telemetry 78% is possibly a high percentage; WithSecure do certainly observe re-infection of victims. Ransomware actors cannot be trusted when claiming they will not re-infect victims and we would never encourage payment of a ransom based on trust in a ransomware operator. It is important to recognize research that gives definite metrics around the untrustworthiness of ransomware actors as this will directly impact the Ransomware landscape.



Ransomware Statistics

Victim Leak Sites

Data biases

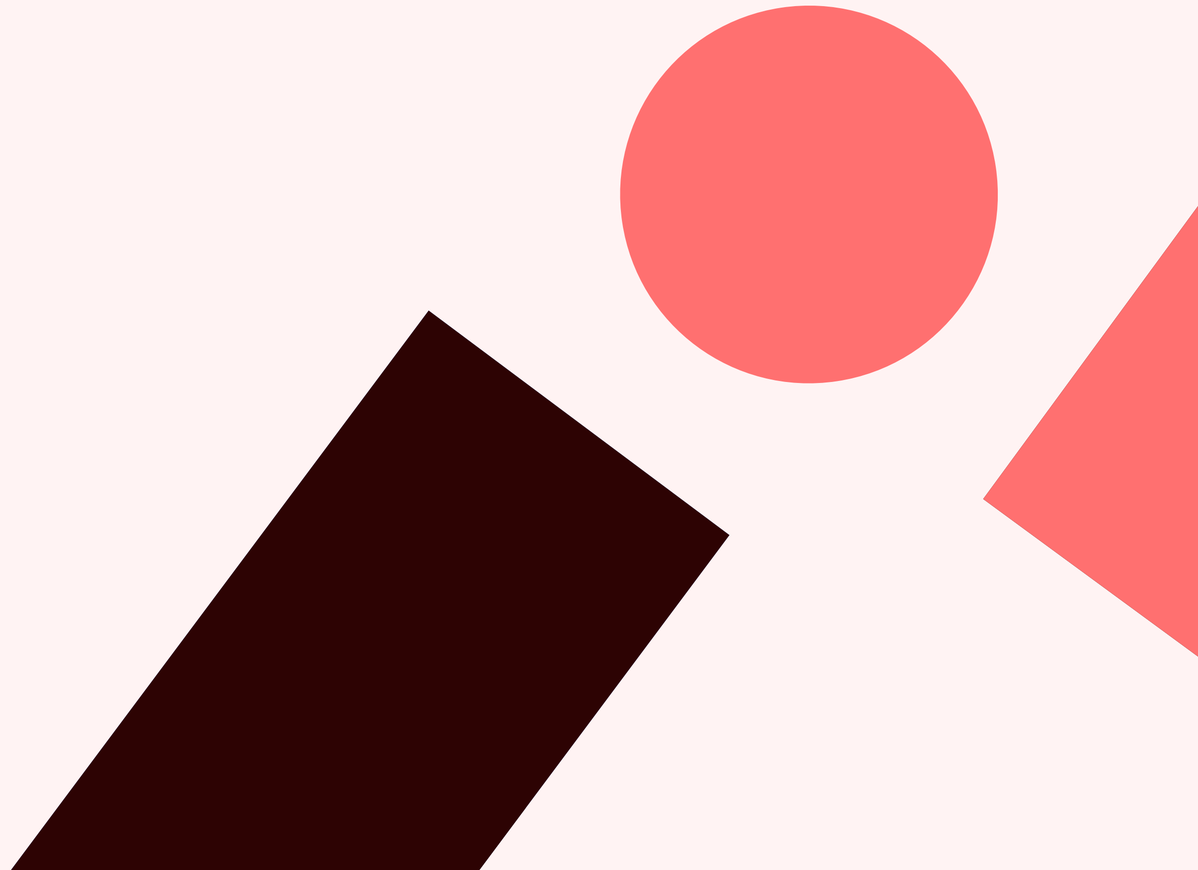
When looking at ransomware statistics, we often use the analogy that analysis of the ecosystem is like looking through a telescope backwards, where every dataset has a different view and perspective.

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 are still able to draw some insight from this data if we can make and state sensible assumptions – and recognizing the data isn’t perfect, it does provide us with a decent gauge. 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



Victim Numbers

Unique victims counted on ransomware data leak sites remain broadly consistent on a month-by-month basis through the first half of 2024, with a very slight declining trend over a 12-month period.

Instead, the numbers are skewed by the anomalous months of July and August 2023 which saw increased numbers based on Cl0p's MoveIT mass exploitation campaign.

Despite all the LEA action and changes in the criminal ecosystem, numbers for 2024 so far are significantly higher than those across the same time periods of 2022 and 2023.

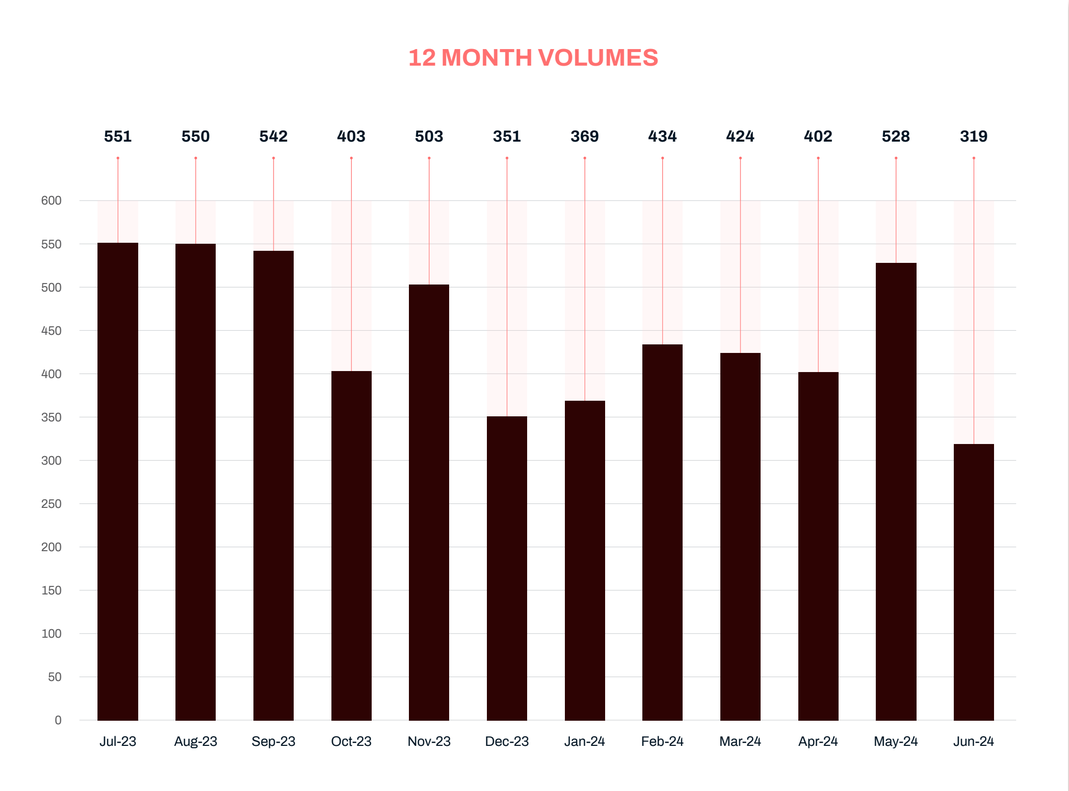


Figure 6 - Ransomware victims posted to DLS (12 months)

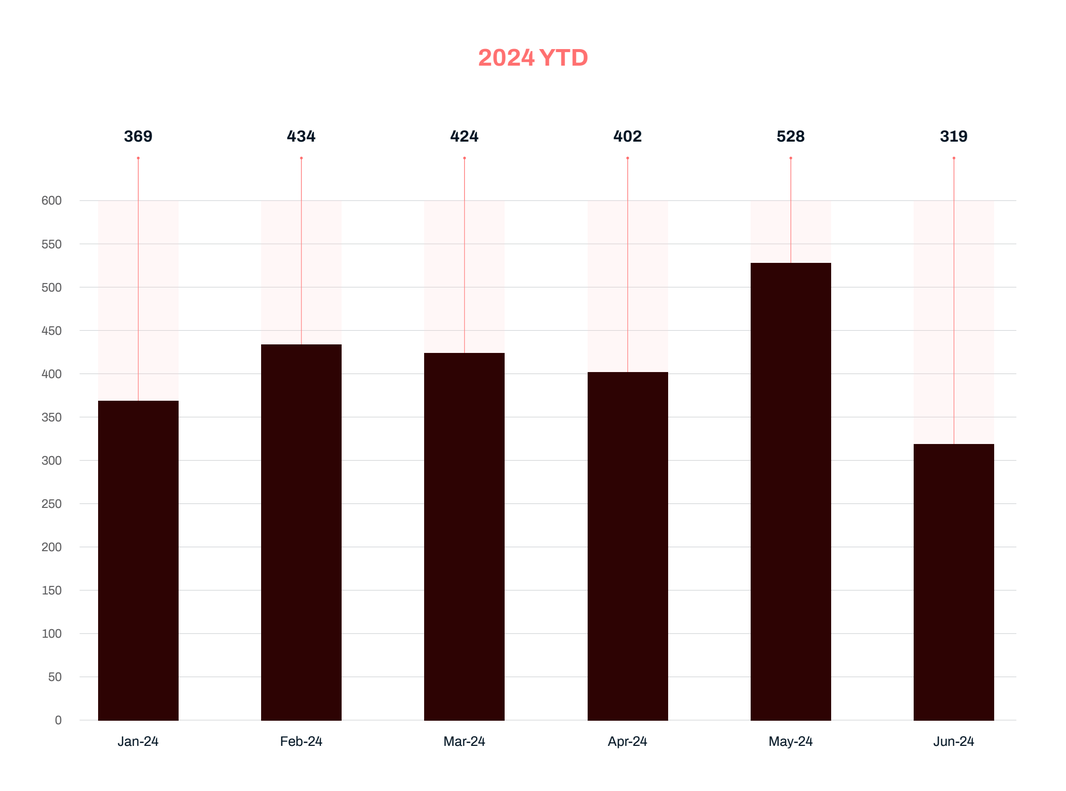


Figure 7 - Ransomware victims posted to DLS (2024 year to date)

Considering numbers through a lens of a particular month across different years helps us understand the impact of seasonal variance, but it does appear that victim postings to ransomware leak sites peaked in Q3 2023, and numbers posted since have remained relatively consistent since.

Figure 8 - Year on Year victims - H1 of each year

Victim Sizes

Ransomware tracker ecrime.ch collects and enriches detailed ransomware leak data and has provided WithSecure statistics on organizational sizes by employee count with a view to track whether there was any themes or patterns over time that suggested a change in the size demographic of victims. Adjusting for inflation of total numbers, there has been a relative consistency in the demographics, which we have relatively arbitrarily broken down by headcount as small (0-200), medium (200-1000), large (1000-5000) and extra-large (5000+).

The bias that this data has upon has been noted earlier in the report, but it is still clear where real-world events impact the data. For example, we see a dip in small and medium sized organizations posted (as a proportion of the total) in August 2023. This is where mass exploitation occurred because of a vulnerability in an enterprise file transfer appliance Move-It and a disproportionate number of larger, enterprise sized businesses were impacted.

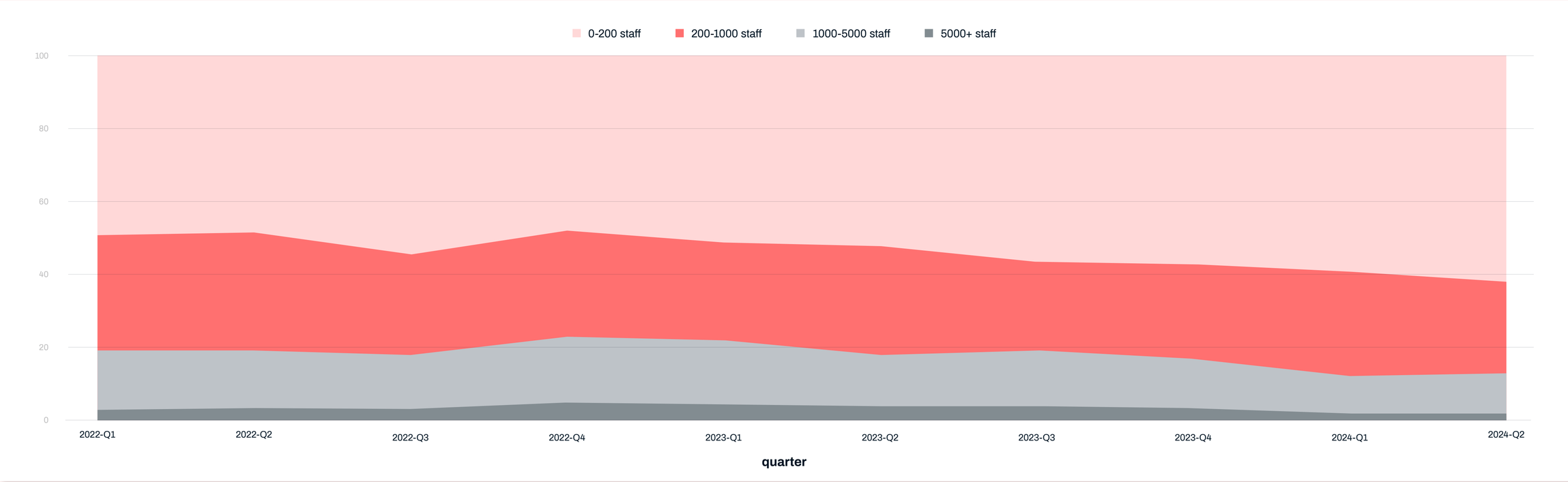


Figure 9 - Ransomware victim sizes by proportion of total numbers. Source: ecrime.ch

In Figure 10 below, we depict percentages on a year-on-year basis. We can see that in 2024, small victims make up almost 61% of all leak site victims, ~5.5 percentage point increase year-on-year since 2022 where 50% of victims were in this category. This concept is explored further in subsequent sections of this report in commentary on payment research by Coveware that correlates with this conclusion.

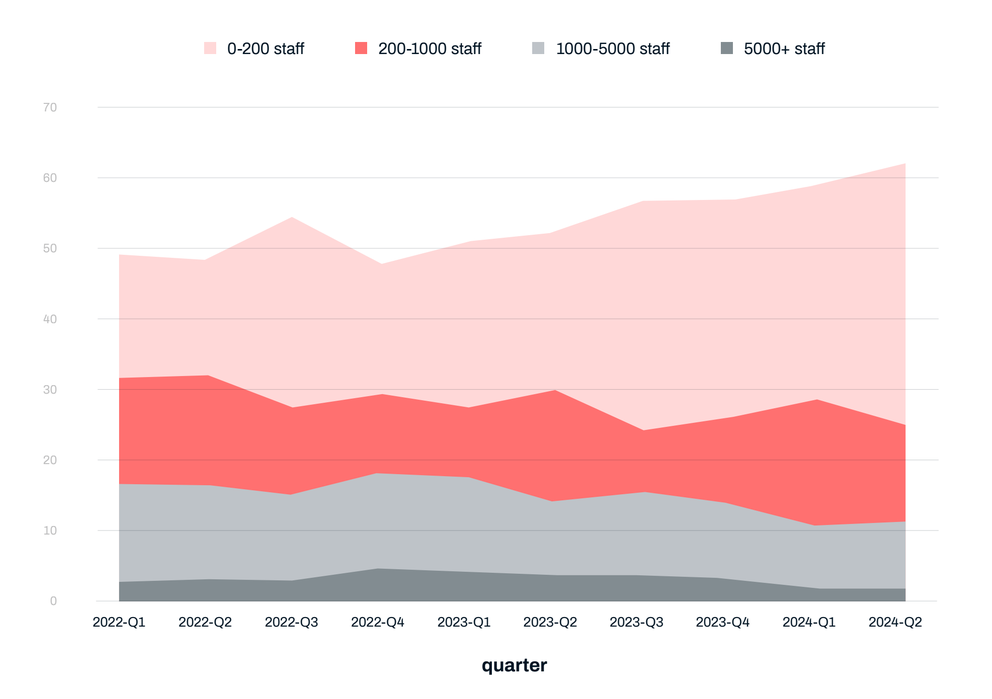


Figure 10 - Ransomware victim sizes - stacked. Source: ecrime.ch

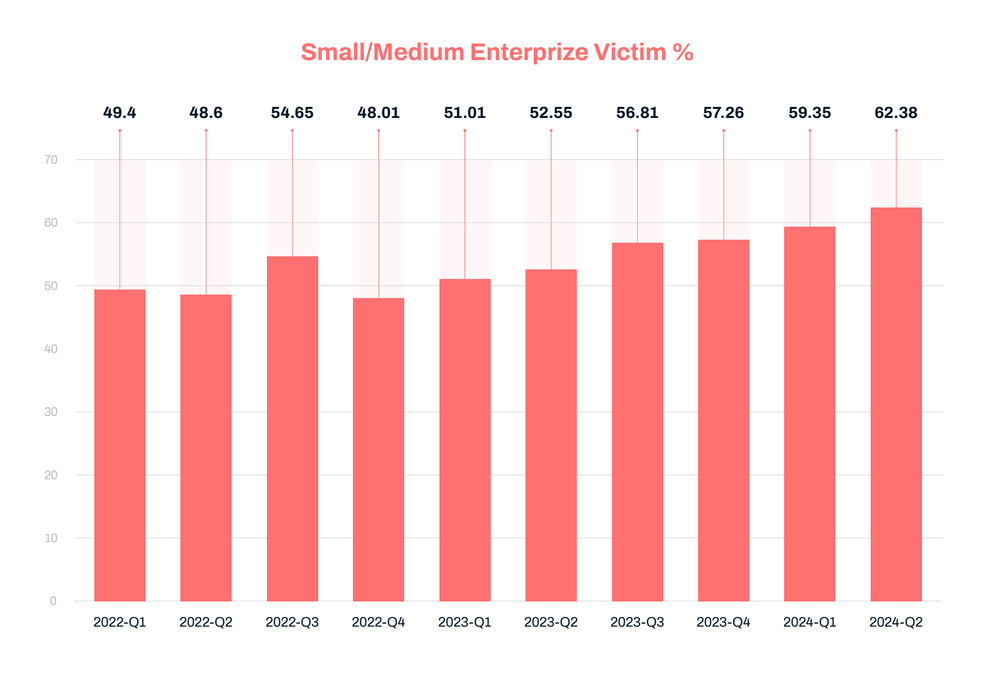


Figure 11 - Percentage of Small/Medium sized victims. Source: ecrime.ch

Medium sized businesses represent a relatively consistent proportion of victims – 30% in 2022, 27% in 2023 and 29% in 2024. Large and Extra-Large victims being posted to leak sites have fallen:

- **Large:** 16.5% (2022) -> 10.9% (2024)
- **Extra Large:** 3.25% (2022) -> 3.5% (2023 – increase likely due to MoveIT) ->1.5% (2024)

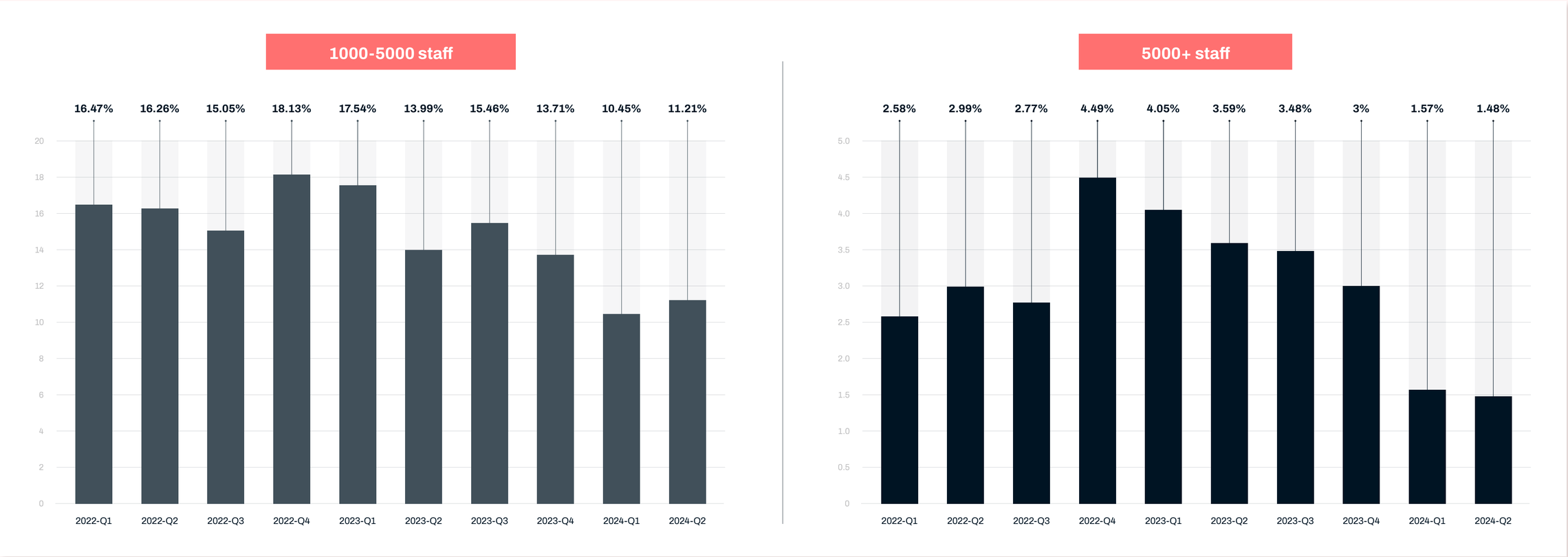


Figure 12 – The % decline of larger victim organisations. Source: ecrime.ch

The conclusion we draw from this data may not be as straightforward as the data suggests. It might be tempting to arrive at the conclusion that there is a decreasing risk of ransomware facing organizations with over 1,000 staff, but here we must revisit one of our key principles: payment rates have remained relatively consistent. On a month-by-month basis this is a defendable assumption, but on a year over year basis we need to note that the landscape in 2022 was very different from that in 2024. Total numbers were far lower, there were less ransom groups operating and the cyber insurance market has rapidly changed.

Cyber insurance is a realistic risk mitigation strategy to large enterprise and therefore we do need to be aware that there is a realistic possibility these numbers are skewed by an increase in payment rates for this demographic, particularly as the cyber insurance market size is increasing by billions of dollars each year.

Geography

Europe and the Middle East seem to have been positively impacted by disruptions to Lockbit and ALPHV, with clear reductions in impact in the months following the events as a proportion of geographic spread. As proportion of total victims, Figure 13 clearly depicts this drop:

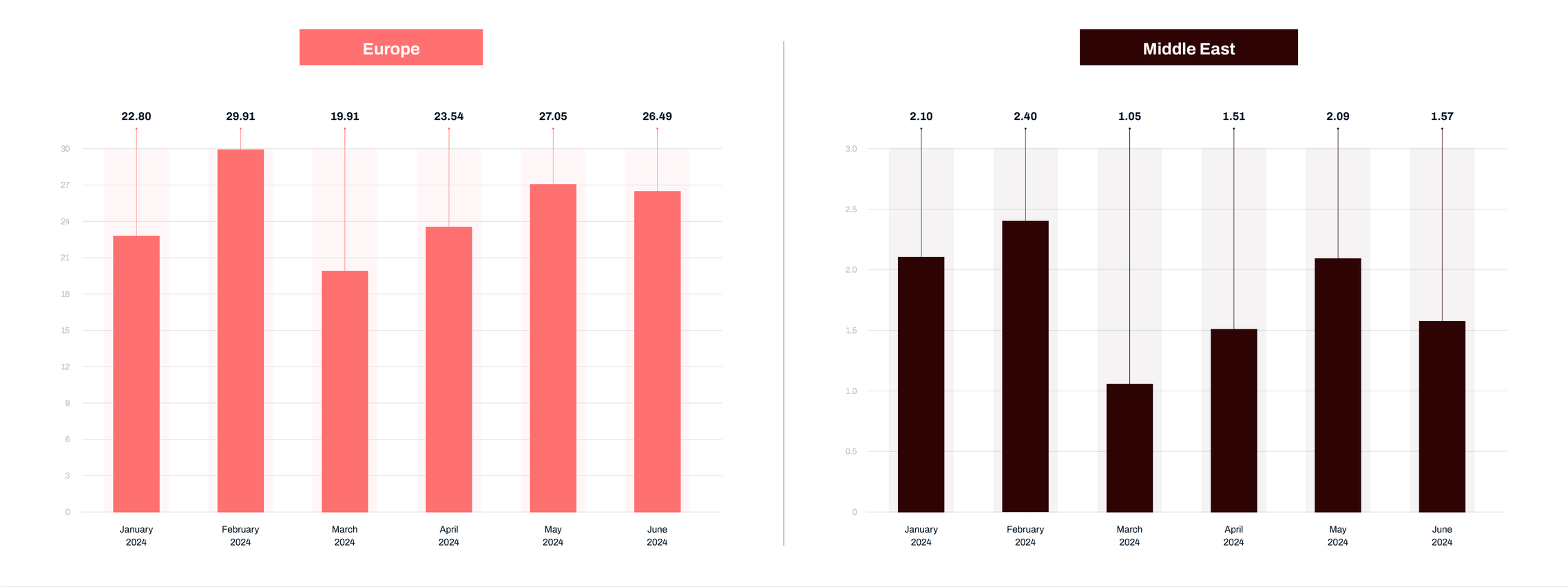


Figure 13 - Europe and Middle East victim proportions

The United States is the most impacted geography with **52%** of all victims posted to leak sites. Europe represents **25%** of victims.

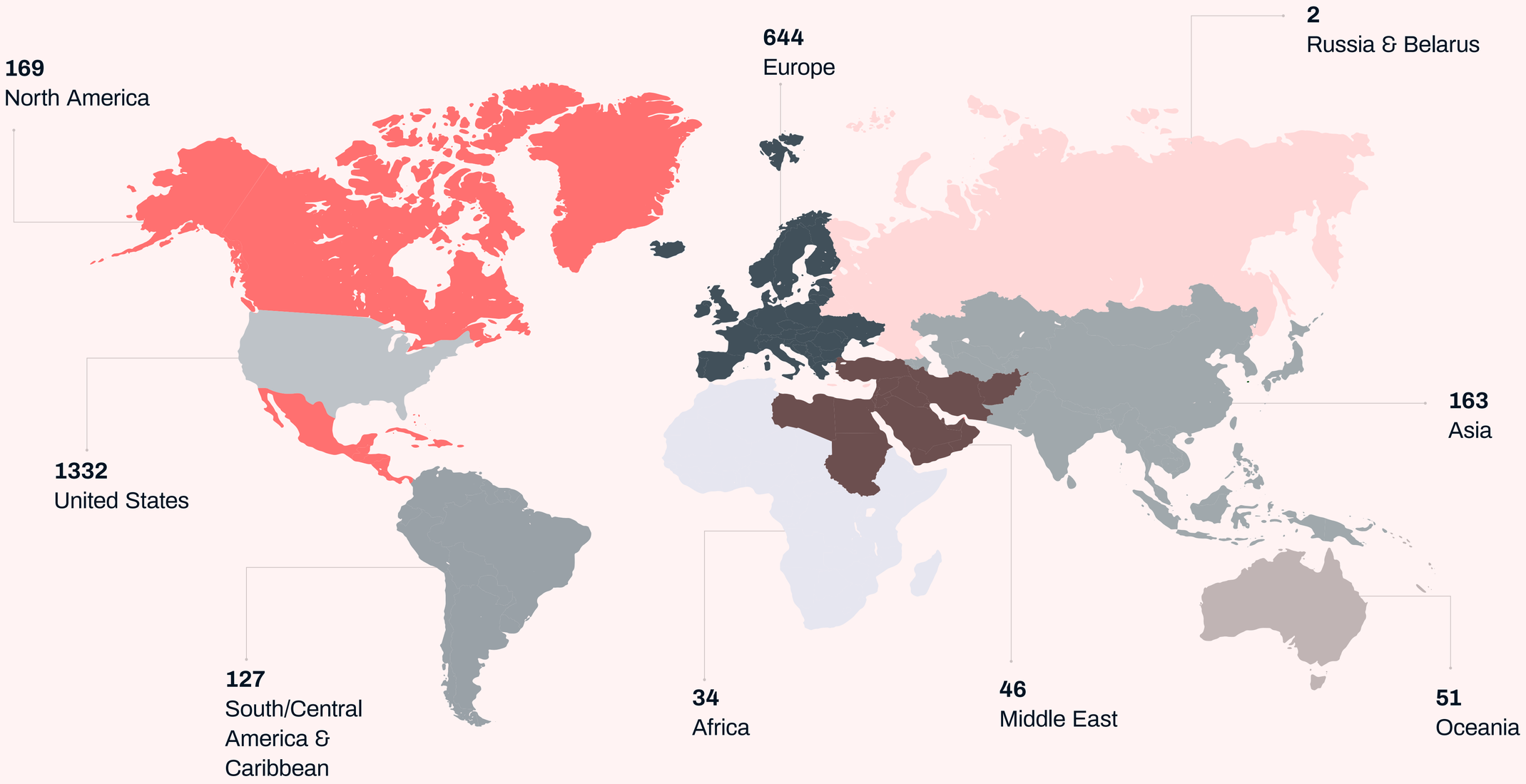


Figure 14 - Ransomware victim geography proportions

Figure 15 - All ransomware geographies by proportion of victims

Figure 15 - All ransomware geographies by proportion of victims

Lockbit and ALPHV Impact

Law enforcement action has splintered larger ransomware affiliates, almost certainly bolstering existing groups or adding new ones. While we cannot track many individuals' affiliations and can only extract observations based on the data. **BlackSuit**, first seen in July 2023, sharply increased victims posted to their leak site following LEA action on Lockbit, and ALPHV's exit scam. This was not the only group whose numbers increased; **Medusa**, who had never posted victims in the twenties, posted 27. **INC Group** posted increased numbers, starting in March and **Quilin** and **Hunters International** have continued posting increased numbers, an increase first observed in early 2024. The success that **RansomHub** and **Medusa** are experiencing as a result of changes to the affiliate payment model has already been noted earlier in this report.

Figure 16 below depicts the aforementioned RaaS groups throughout H1 2024, and the marked increase in victim numbers since the events surrounding Lockbit and ALPHV.

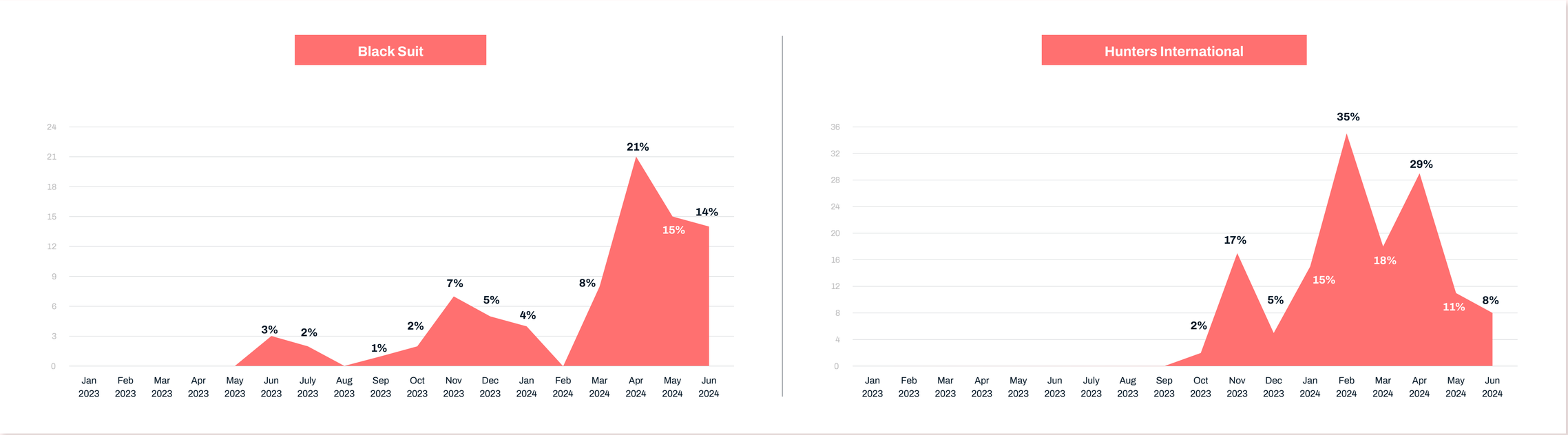


Figure 16 - RaaS group productivity increases following Lockbit/ALPHV events

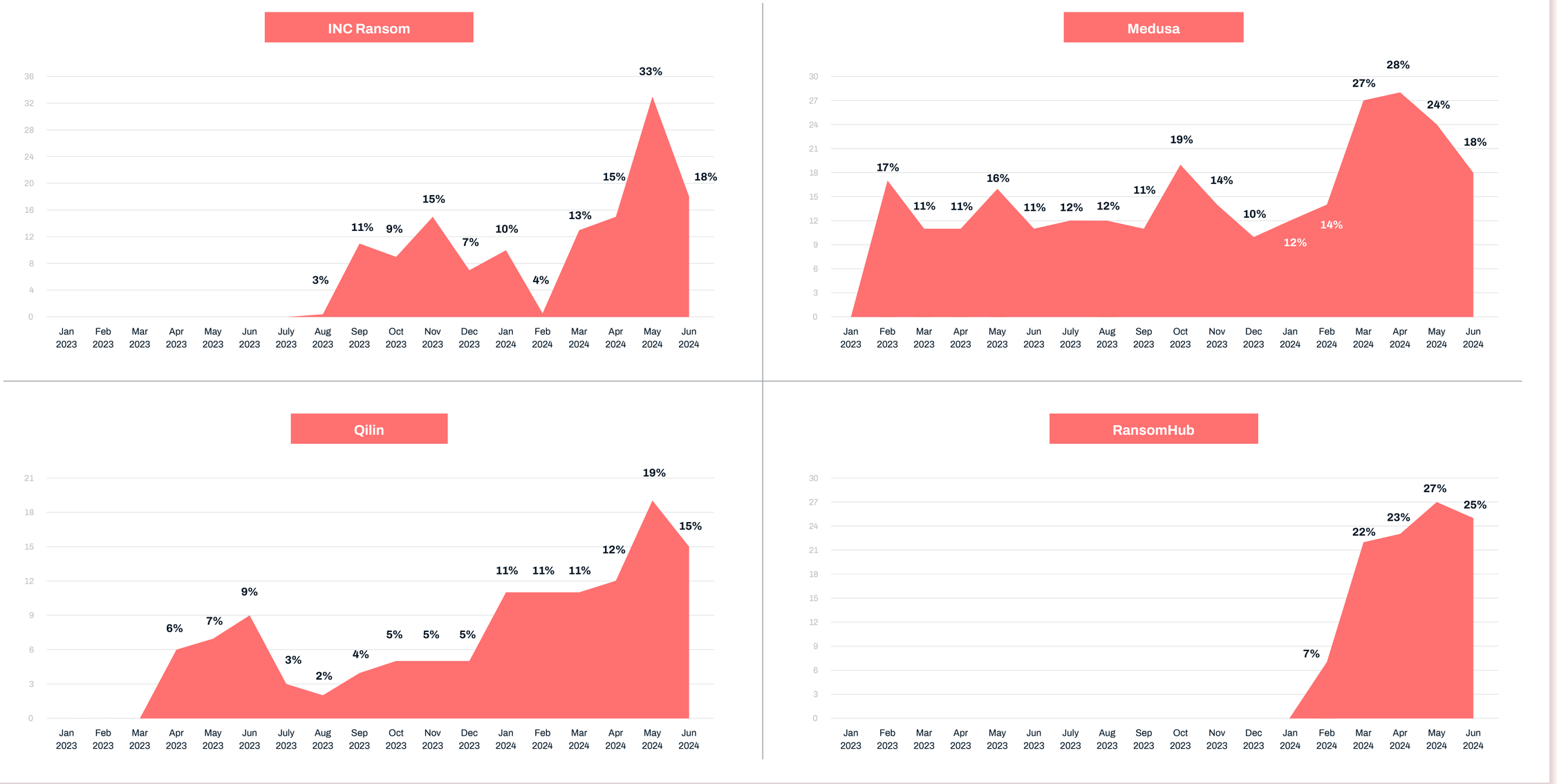


Figure 16 - RaaS group productivity increases following Lockbit/ALPHV events

Payment Statistics

Statistics published by Coveware state that in Q4 2023 ransomware payment rates dropped to 29%, and the average ransom payment dropped by 33% compared to Q3, to $568,705 dollars. Coveware suggest that this is due to a decline in the size of victim organizations, which they report saw a 32% drop compared to Q3 2023. Coveware state this may be linked to an increase in the number of “small game” actors who specifically target smaller organizations. While Coveware’s data covers Q4 2023 specifically, recently released statistics by Chainalysis for the whole of 2023 show that total ransom payments in 2023 doubled compared to 2022, and increased by 10-15% compared to 2021, rising to $1.1 billion.

These statistics, when combined could paint a picture of a ransomware environment where payment rates are lower, and total cost is higher – therefore more organizations are being impacted. However, to balance this we note the time periods are different in the two research pieces and wish to reiterate the complexity of the landscape and gaps in the information we have.

Ransomware Targets

For the most part, ransomware actors do not appear to target specific sectors or industries. As with any generalization, it is likely that there are exceptions, however if a particular affiliate has a preference towards a particular sector, this insight will be obfuscated by other affiliates working to the same ransomware brand.

Targeted Sectors

Engineering and Manufacturing was the most impacted sector in the first half of 2024 with 20.59% of all victims observed.

Sector Group	Proportion
Engineering and Manufacturing	20.59%
Real Estate and Construction	9.02%
Health Services	7.17%
Financial Services	7.02%
IT and Software	6.82%
Business Services	6.09%
Retail	5.63%
Transportation and Logistics	5.05%
Legal Services	3.97%
Education	3.89%
Other	24.75%

Table 1 - Sector group victim proportions

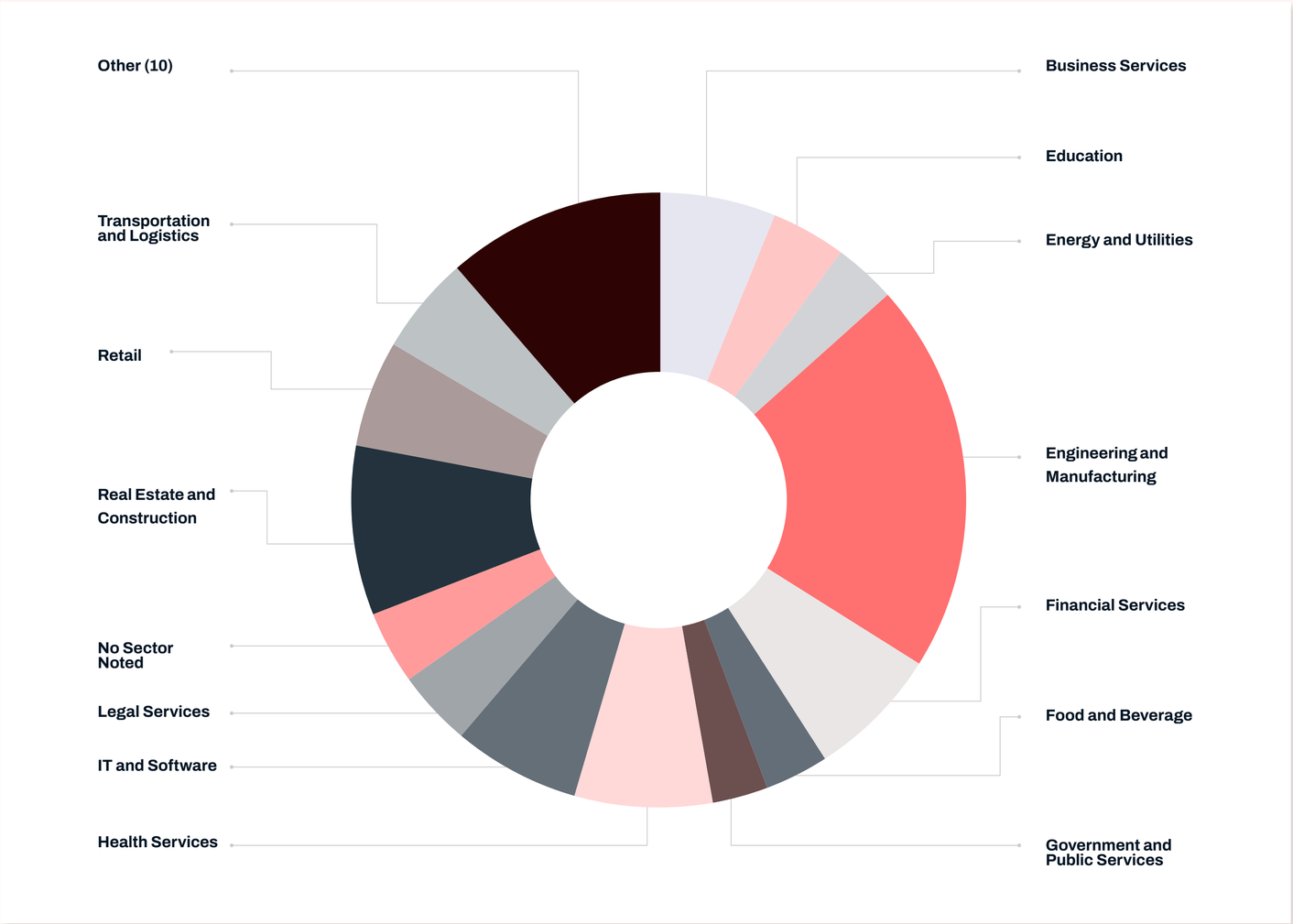


Figure 17 - Sectors impacted by ransomware

Releasing the shackles

Following the LEA action taken against Darkside due to their ransomware attack on Colonial Pipeline, there appeared to be a concerted effort by ransomware collectives to avoid sanction. Ransomware collectives would try to fall below a perceived line that they believed would incur action by a competent authority, with many groups publicly stating they would not attack hospitals. In 2023, it appeared many ransomware variants have abandoned these positions and have no reservations about targeting any western organisation. It was hypothesised that successful extortion (twice) of Change Healthcare will have encouraged criminals to more prioritise targeting of healthcare. However, the data does not suggest that this has happened. Numbers of victims in healthcare have slightly increased from January – May, but as a proportion of overall victims, healthcare has remained relatively consistent over 2024.

It is really important to note that Healthcare is one of the more interconnected industries, and as we have seen with attacks on a British labatory and the aforementioned Phobos attack impacting ~100 Romanian hospitals, a singe victim can impact a broad set of healthcare institutions and therefore systemic impact to the healthcare sector can far exceed what is counted on data leak sites.

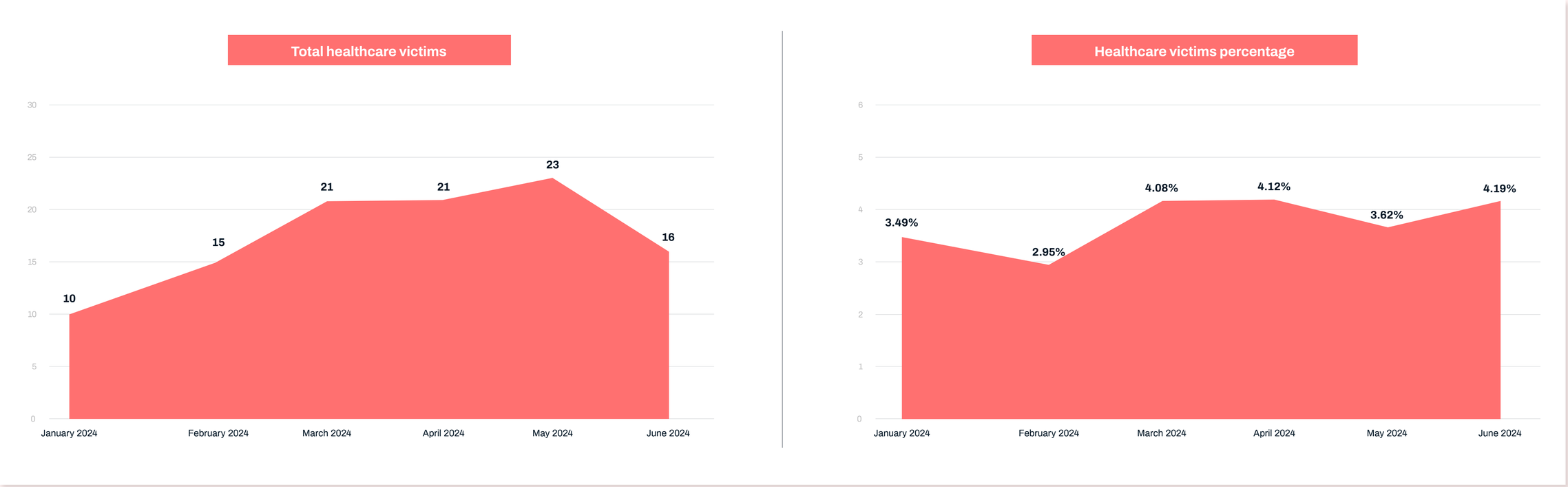


Figure 18 - Healthcare victims as a percentage of total and actuals

WithSecure have also noted a large trend of local governmental organisations across UK, US, France and Australia over late 2023 and early 2024. There is a realistic possibility that such self-imposed targeting restrictions are being eroded. Particularly if these are only in place as a technique to prevent LEA action that may be perceived by criminals as inevitable. Ability for Western LEA to act against individuals in Russia may also be curtailed due to sanctions against Russia and the Russian financial system mean actors are now less likely to have assets within reach of Western authorities.

Despite its prominence in media, 'Government victims and Public Services' sector was not a common target of ransomware with only 3.05% of victims belonging to this sector group. This being said, relevant victims do appear to follow a pattern that coincides with events surrounding BlackCat/ ALPHV and Lockbit, and the subsequent periods of relative inactivity by these brands.

Figure 19 show victimology in this sector broken down as a percentage of all sectors, and a simple count of victims, both diagrams showing a marked drop immediately after Lockbit/ALPHV events.

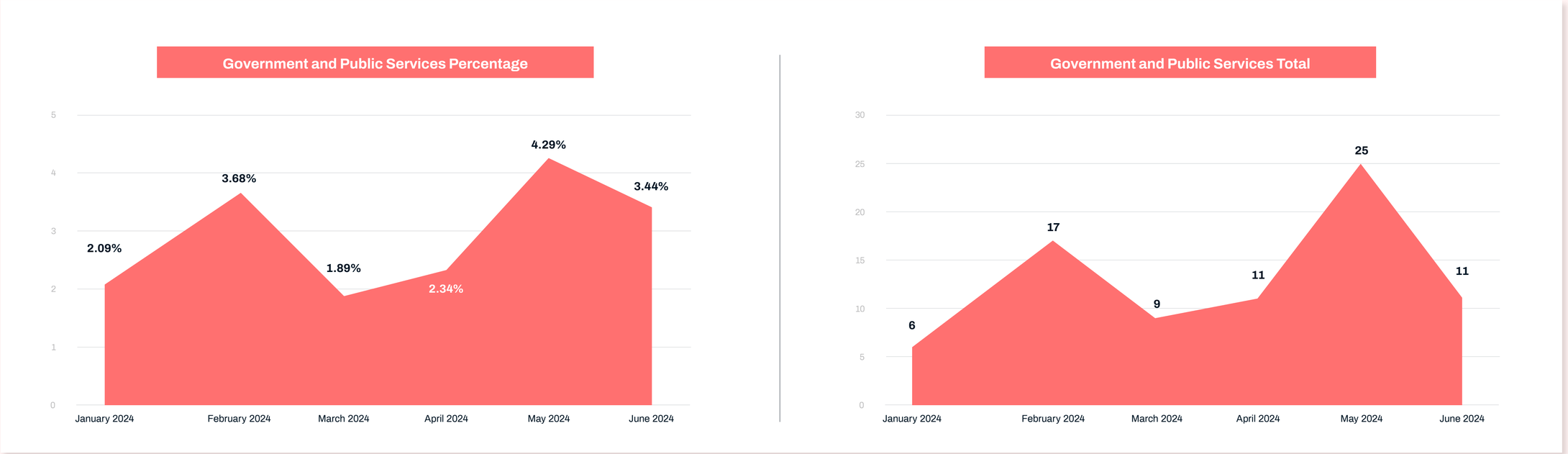


Figure 19 - Government and Public Services victims as a percentage of total and actuals

There is little by the way of clear insight pertaining to other sectors throughout 2024, except for a slight but consistent decrease in the ‘Engineering and Manufacturing’ sector, and a rise in victims in the ‘IT and Software’ industry. These are shown in Figure 20:

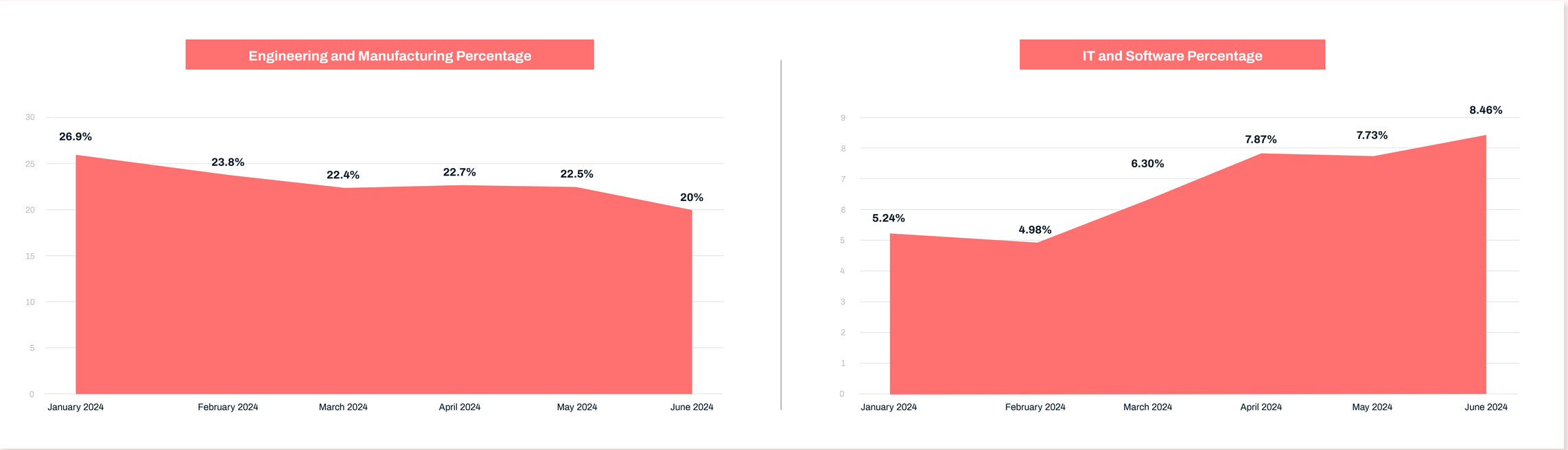


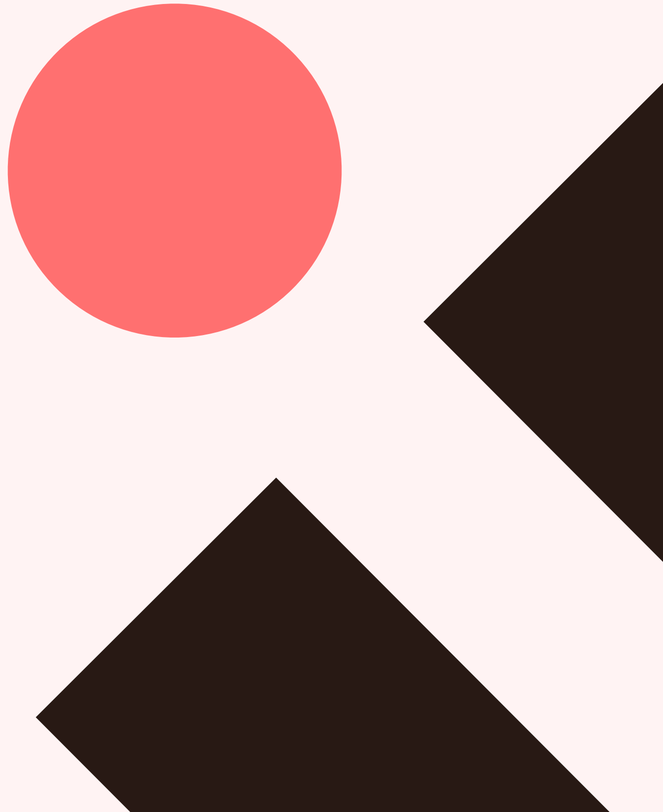
Figure 20 - Engineering and Manufacturing % decline and IT and Software sector % increase

FBI Reporting

The FBI issued their 2023 report on cybercrime which included statistics on various types of cybercrime, including ransomware. Their numbers (based on incidents reported to them by victims) show that compared to 2022 there was an 18% increase in reported ransomware attacks to 2,825, and a 74% increase in losses due to ransomware attacks, NB: do note that is losses incurred, not ransoms paid.

An even more concerning statistic is that of the 2,825 reported attacks, 1,193 were against critical infrastructure organizations, an increase of 37% on the previous year. The reported losses to ransomware rose 74% from $34.3 million to $59.6 million, which is a relatively small amount when compared to the $4.57 billion lost to investment fraud in 2023. Most investment fraud referenced cryptocurrency, which made up $3.96 billion of the reported losses. This is a 38% increase in investment fraud losses on 2022, and a 53% increase in cryptocurrency investment fraud.

We should note that the FBI will collect data on a specific subset of victims, namely those in the US who are mandated, or volunteer to report events. From these numbers one could draw the conclusion that ransomware profits are growing faster than investment fraud profits; however, it should be noted that this is a complex space and there are caveats that should be placed upon these statistics.



Ransomware Tactics

Initial Access

It is not always easy to identify an intrusion vector when collecting statistics. We do not believe 2024 has or will show a significant change in the type of vectors deployed by actors, however there is a continual shift in trends of how frequently the tactics are employed. Table 2 shows, in no order, initial access tactics observed by W/Incident Response teams:

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

Table 2 - Initial access vectors observed

Mass Exploitation

With ~45% of all cases, exploitation of a public facing application (MITRE ATT&CK ID T1190) was the most common infection vector across WithSecure Incident Response engagements in H1 2024. This observation is shared by others in the industry, research by Symantec published towards the end of quarter 1 (Q1) 2024 also stated that the primary infection vector for Ransomware has changed from botnets to vulnerability exploitation.

Exploits

According to CISA KEV (Known Exploited Vulnerabilities), four vulnerabilities have been added to the list in 2024, of which three have been assessed by an authority to be a perfect 10.0 CVSS – this the highest score possible for a vulnerabilities' severity score. This is also only newly exploited vulnerabilities that have not been expressly observed only in cases referred to CISA. The technologies in this list are enterprise scale

- mobile Device Management services,
- data servers,
- VPN servers
- remote management tooling

This is more demonstrative of the increasing availability of 1-day exploits to ransomware actors and the lowering barrier to compromising vulnerabilities a.) en-masse and b.) in tooling specifically designed for network security.

Supply Chain Attacks

In 2023, WithSecure's Threat Intelligence team released a whitepaper detailing the supply chain threat. The whitepaper still conveys an accurate representation of the threat posed by lateral movement through the supply chain, however there is one area in which an element of supply chain threat has developed past the limit to which it was referred to in the report, and that is where Log4j was referred to as a 'special case'. The concerning reality is that there have been a number of CVSS CRITICAL vulnerabilities either directly in enterprise services, or unknown/undocumented software libraries contained within enterprise services. Here we consider exploitation of an externally exposed element of the software supply chain as 'T1190 Exploit Public-Facing Application', and not a 'supply chain attack' which we would cite when lateral movement of tooling or access occurs through a trusted relationship – such as the events we observed with February 2024's ScreenConnect (CVSS 10.0) vulnerabilities.

In Q1 2024 around 100 hospitals in Romania were affected by a wave of Phobos ransomware attacks. The volume of attacks in a short timeframe, and the close logical association of the victims (all being hospitals, and all in Romania) strongly implied that the cause was a supply chain attack. This has now been confirmed by the Romanian Cyber defense agency. The campaign began with the compromise of Romanian Soft Company's Hipocrate Information System, an integrated healthcare management system platform. Fortunately, most hospitals have backups in the past 1-3 days, however they will still lose some data, which in a healthcare environment could be critical. Targeting of healthcare institutions internationally has been on the rise in recent months, most likely due to the life-or-death consequences of operational disruption. Indeed, US cyber authorities have recently issued a warning to the healthcare sector regarding targeted ransomware attacks by the ALPHV ransomware brand.

Identity Attacks

Identity targeting is also very common. Infostealer malware is cheap on darkweb marketplaces, and brute-force, password spraying, and credential stuffing techniques are very common methods of initial access, particularly into cloud services where extra layers of security are not enabled.

Insider Threat

WithSecure recognise the risk posed by an insider is still extant, and these are still actively recruited and advertised on underground forums.

Dual use tooling

Increased use of dual-purpose tooling provides an issue for network defenders as malicious applications or installations of legitimate tooling may bypass anti-malware controls, and blend into legitimate usage telemetry. The tools for remote access, persistence and exfiltration that have been observed by W/Incident Response are contained in Table 3:

Remote Access Tool	Exfiltration
PDQ Connect	rclone
Action1	rsync
AnyDesk	winSCP
TeamViewer	SFTP
Atera	Megaupload
Syncro RMM	FileZilla
SplashTop	cURL
NetSupport	
NinjaRMM	
ScreenConnect	
RustDesk	
SimpleHelp	
QuickAssist	

Table 3 - Dual-use tooling employed by RaaS actors

Environments

There are now numerous examples of where ransomware actors do not have variants that are only Windows specific. Numerous families have variants that target Linux and ESXi services. This is not new for 2024.

While also not new for 2024, cloud services are also increasingly targeted by ransomware actors. As network migrate to cloud (perimeter-less) architectures, attacks on identity are the new battlegrounds. Okta, an identity, and access management company released a report warning of “unprecedented” credential stuffing attacks, stating the following in the April 2024 report:

From March 18, 2024, through to April 16, 2024, Duo Security and Cisco Talos observed large-scale brute force attacks on multiple models of VPN devices.

From April 19, 2024, through to April 26, 2024, Okta’s Identity Threat Research team observed a spike in credential stuffing activity against user accounts from what appears to be similar infrastructure.”

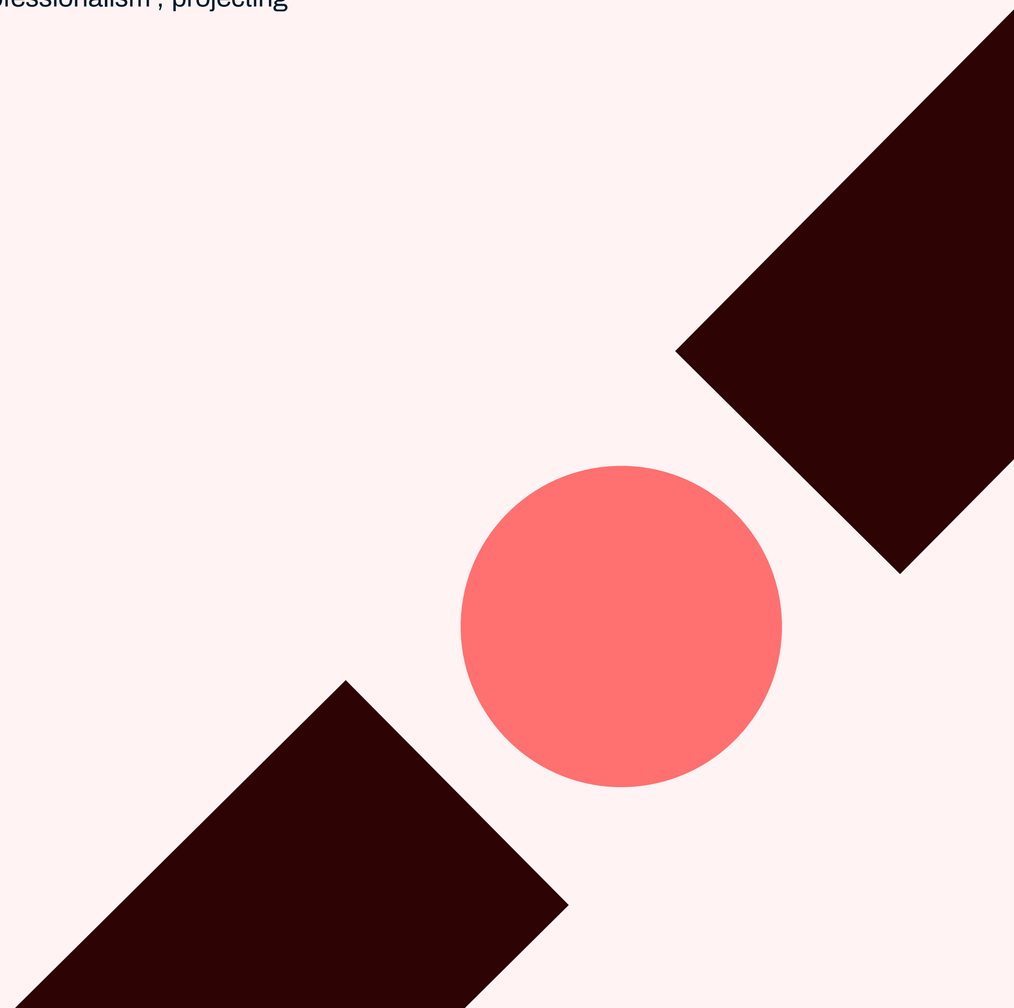
As actors often demonstrate a preference to data theft (perhaps with deletion) over encryption, cloud services are an extremely attractive target for ransomware actors.

Extortion

As of the end of Q1 2024, there have been no significant changes to trends from 2023 when considering extortion methods. Many actors will prefer data theft and ransom only, whereas some will continue to deploy a ‘traditional’ encryptor without even attempting to exfiltrate data. Dual-factor extortion is probably still the most desirable outcome for ransomware actors, however there are numerous examples of where affiliates have prioritized data theft – whether that is by targeting vulnerable file transfer systems, or cloud environments. This is likely due in part to increasingly competent anti-encryption capabilities and network segmentation, but also to the efficiency with which actors can operate.

Carefully penetrating a network avoiding detection is time consuming and still reserved for more capable ransomware actors (at least where sufficient enterprise security tooling is employed). When there is still a fair chance that organizations will pay for sensitive data retrieval stolen following a more rudimental ‘smash and grab’ attack, it is probably seen as an inefficient use of time to perform a whole system compromise to drop encryptors.

There have been examples of where actors attempt to add more pressure to their extortion demands – threatening DDoS attacks, notifying media / shareholders etc. WithSecure do not have data on the efficacy of these tactics, but these are almost certainly tertiary concerns to a victim. Many ransomware actors still attempt to retain an air of ‘competence’ and ‘professionalism’, projecting their victims as clients and not victims.



Not just a ‘Russia’ problem

Eastern Europe and Russia is heavily cited as the source of most ransomware attacks probably due to execution guardrails that was often put into ransomware binaries that prevented detonation if the computer it was deployed on used Cyrillic characters, and the abundance of Russian language cybercrime forums. This is less and less the default, and it is quite important to note that ransomware operations are being launched from all over the world.

There have been numerous examples of affiliates being arrested in the US and Europe, but there are also ransomware groups primarily operating out of other 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. It is also important to note that the cyber security industry is primarily focused on larger ransomware affiliate models that typically prefer affiliates operating out of CIS (Commonwealth of Independent States) counties. There is almost certainty a significant number of unreported independent ‘small game hunters’ who are able to capitalize on leaked ransomware source code and burner email addresses operating outside of the sphere of Russia and CIS,

State-operated ‘ransomware’

Ransomware has become so prolific that its usefulness cannot simply be limited to financial gain. The industry has 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 of the sphere of conflict in Eastern Europe, however this threat model will change with increasing geopolitical tensions. Private organizations not in countries fighting in Russia’s illegal war 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.

With Geopolitical tensions rising across Europe, between Iran/Israel and if China/Taiwan escalates there will be a need to revisit this threat model.

North Korea (DPRK) is always 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 likely utilizing established ransomware-as-a-service models to undertake their attacks. WithSecure have detected overlap between intrusions orchestrated by DPRK and those of ransomware affiliates.

Conclusion

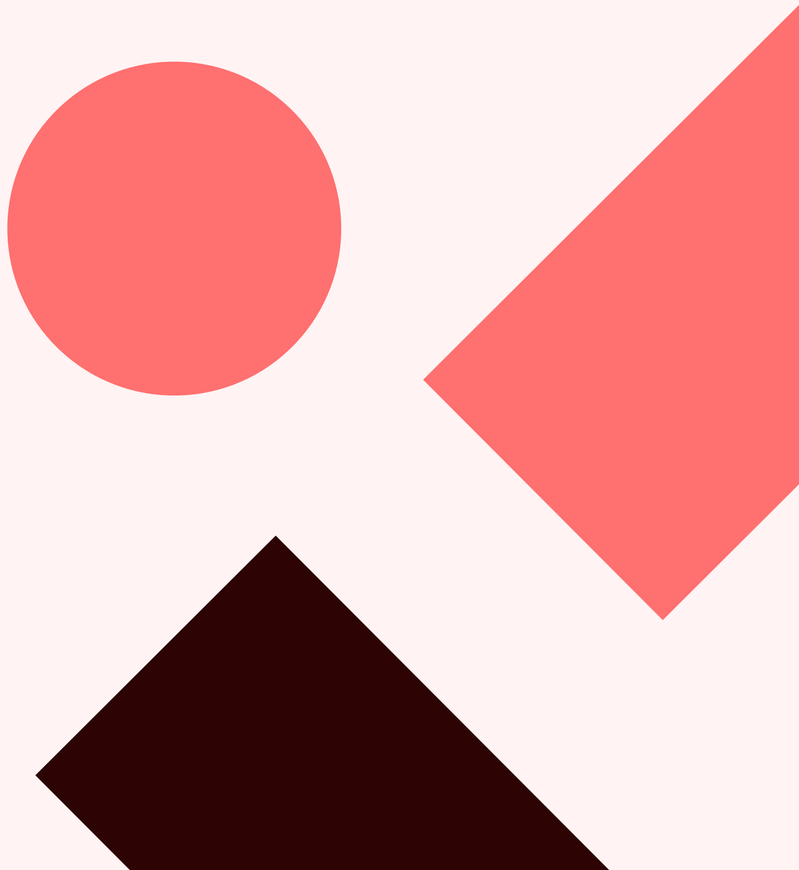
Ransomware is a major global issue, impacting hundreds of organizations and resulting in billions of dollars of damages. Ransomware probably represents the most significant risk to most organizations' networks, particularly those that are small/medium sized.

A mature, developed ransomware ecosystem exists, however recent events have likely eroded the trust between entities that operate within it. The more successful ransomware brands were those that operated in a way that closely emulated organized and well-structured legitimate businesses. Following disruption into these, it is unlikely that significant volumes of ransomware actors have left the cybercrime industry, instead have moved towards existing, but less established ransomware brands. This is possibly a key reason for a relatively stagnant number of victims being posted to leak sites throughout 2024. It is almost certain that law enforcement action has significantly impacted the ransomware ecosystem. While it is currently too soon to draw conclusions on the long-term effectiveness of this, in the short term there has been a marked, positive impact. Lockbit is showing signs of being in a consolidation phase, and is almost certainly seeking to regroup, rebuild and harden its operations.

Ransomware actors appear to be shifting away from the concept of 'big-game-hunting'. Small to medium sized organizations are increasingly being posted to ransomware leak sites. This may be in part due to the ability for larger enterprises to meet attackers demands through risk mitigation strategies that are not particularly available to small organizations – i.e. Insurance. Smaller, but more frequent extortion attempts likely also reflects a more efficient return on investment for ransomware actors.

As attackers are increasingly exploiting edge service vulnerabilities for initial access, organizations with robust exposure management processes and mature security tooling are far better equipped to successfully mitigate ransomware attacks.

In H1 of 2024, there are positive signals that ransomware productivity is waning, however the industry and western authorities must keep applying pressure and imposing cost on ransomware actors wherever possible.



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 outcomebased 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.

www.withsecure.com

W / T H secure