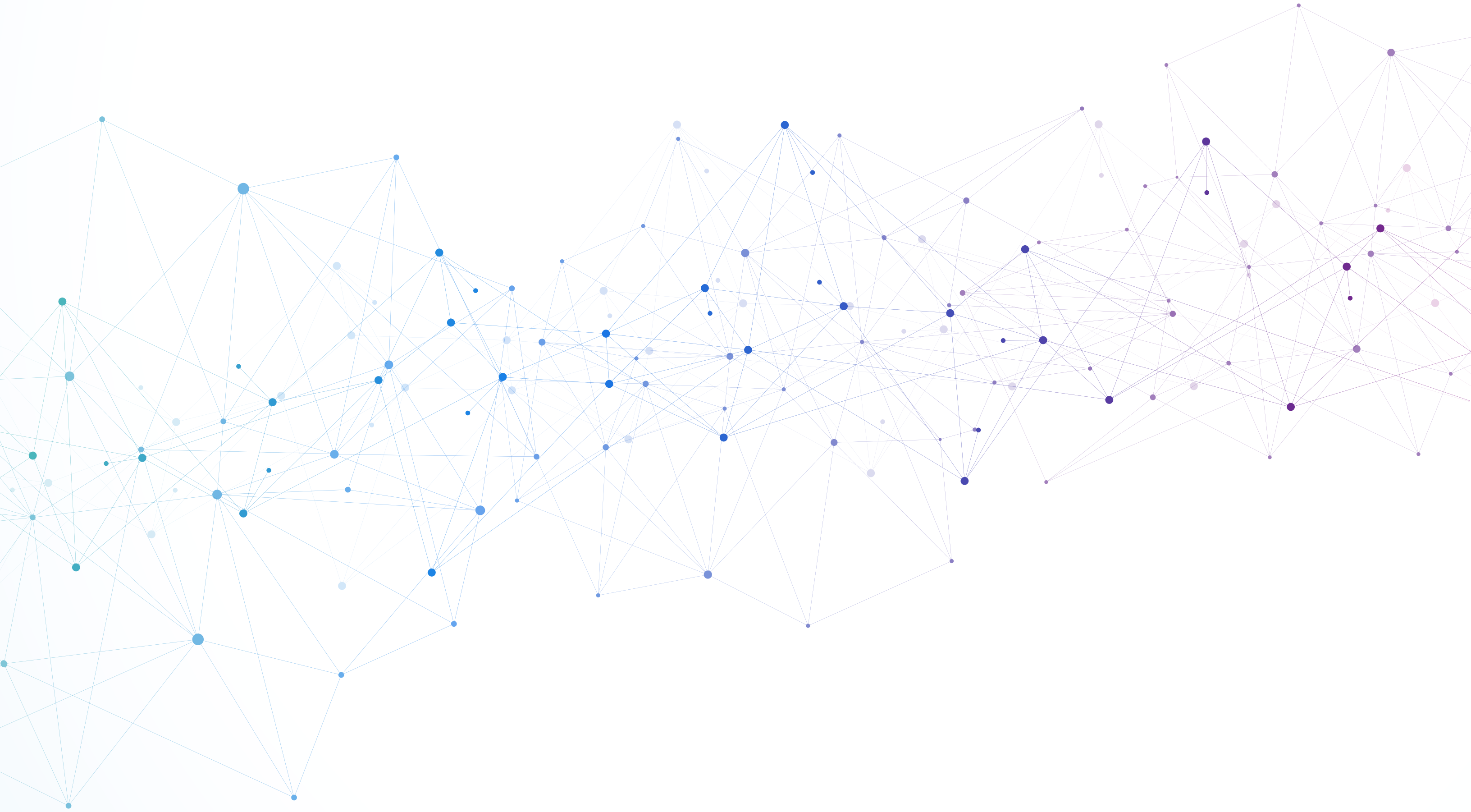
NOVEMBER | 2023

Arete

Crimeware Report

Trends and Highlights from Q3 2023



This report covers trends observed during Arete's response to ransomware and extortion attacks from July 1 through September 30, 2023. The volume of attacks in Q3 was consistent with that observed in the first half of 2023. However, the ransomware ecosystem showed noticeable changes as criminal affiliations shifted. The data examined includes ransomware variants, ransom demands, and sectors impacted by ransomware. The report concludes with a view into how geopolitics impact the cyber landscape and an outlook for the quarter ahead.

Overview

ALPHV/BlackCat dethroned LockBit as the most prevalent ransomware variant Arete observed in Q3, as LockBit encountered internal instability (see page 4), and ALPHV/BlackCat increased the volume and speed of its attacks. The number of identified threat groups increased slightly compared to Q2, but Q3 saw a greater variety in unnamed variants.

Q3 was marked by instability and an increase in unnamed ransomware variants, potentially due to affiliates shifting between names to find the highest profits while reducing exposure to law enforcement. Well-known Ransomware-as-a-Service (RaaS) operators like ALPHV/BlackCat, LockBit, and Akira are competing for high-quality affiliates.

Across the ransomware incident response cases Arete responded to in Q3, several notable trends emerged:

- Multiple ransomware groups demonstrated increased aggression and use of pressure tactics in negotiations, including one group making unsubstantiated threats of physical violence.
- Cl0p continued impacting victims from the MoveIt exploit campaign, using torrents for faster data exfiltration.
- Luna Moth returned in high volumes, using call-back phishing with Peloton lures to gain initial access. The group primarily targets law firms in exfiltration-only extortion events.

Meanwhile, global geopolitical instability continues to reverberate through the cyber domain. More than 100 threat actor groups are conducting malicious cyber activity in relation to the Israel/Hamas conflict. Collateral cyber damage is minimal at this time but may escalate to impact non-participating organizations as the conflict continues.

Overview

NUMBER OF THREAT ACTORS

Q3 2023	Q2 2023 Comparison	Q3 2022 Comparison
32	31	30

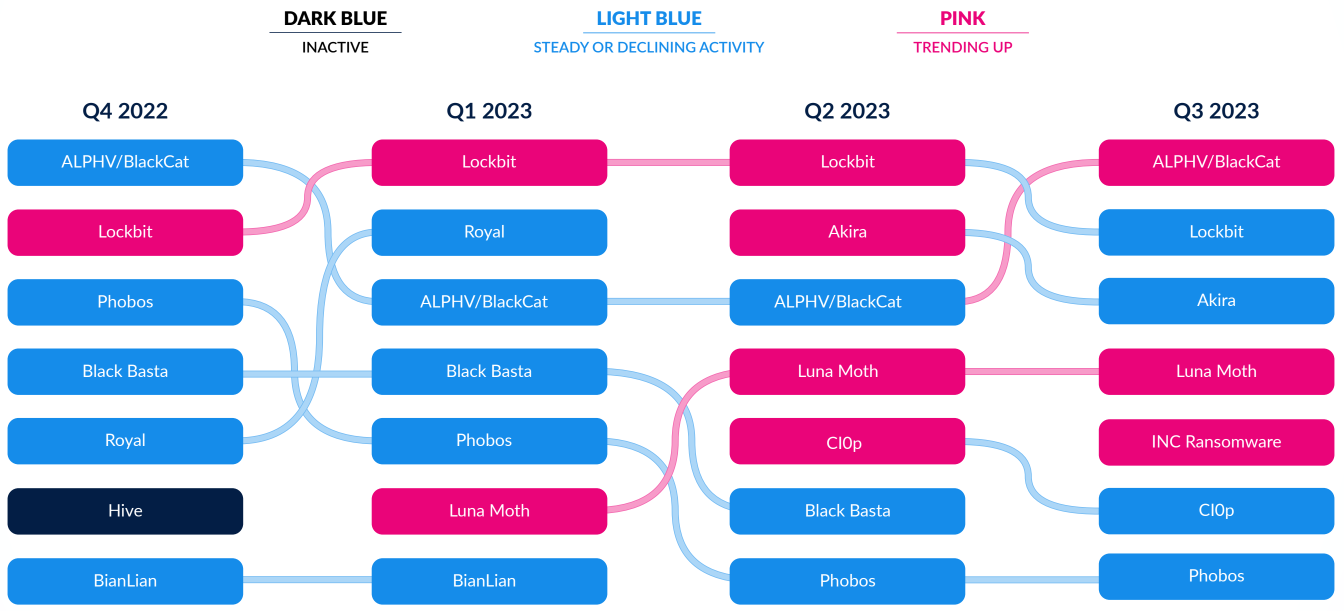


Figure 1: Top Ransomware Variants Observed from Q4 2022 to Q3 2023

Arete responded to nearly 50% more ALPHV/BlackCat engagements in Q3 compared with Q2, as the group expanded operations and began working with more affiliates. Meanwhile, Lockbit ransomware activity remained stable despite the group's internal conflicts. Akira's operations took the biggest hit, potentially indicating that its affiliates are moving to work with different ransomware operators. INC ransomware surged onto the scene in Q3 as a previously unseen operation. Luna Moth rounded out the top 5 in Q3, with most of their activity centered in September after appearing to take the summer months off. Cl0p failed to make the top 5 in Q3 due to a slight decline in activity.

Trends in Q3 Ransom Demands

17%

% of Time a Ransom is Paid

$158K

Median Ransom Payment

73.6%

Average Discount % Across all Ransomware Variants

$20M

Highest Initial Ransom Demand

Figure 2: Reflects Projects Started between July 1 and September 30, 2023.

Figure 3 shows the prevalence of variety in ransomware variants observed in Q3 alongside the median ransom demanded by each variant. Initial ransom demands were consistent across all major RaaS operators (ALPHV/BlackCat, Lockbit, Akira, and INC), coming in at less than $1 million per engagement. Cl0p ransomware was a significant outlier, demanding outsized ransoms reminiscent of older "big game hunting" ransomware operations, specifically targeting high revenue businesses to demand larger ransoms.

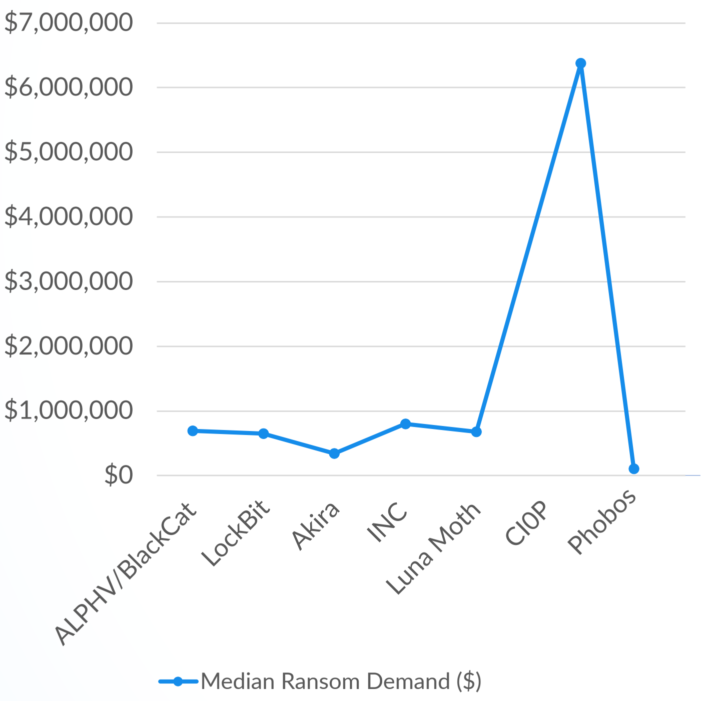


Figure 3: Top Ransomware Variants and Median Ransom Demands Observed in Q3 2023

Trends in Q3 Ransom Demands

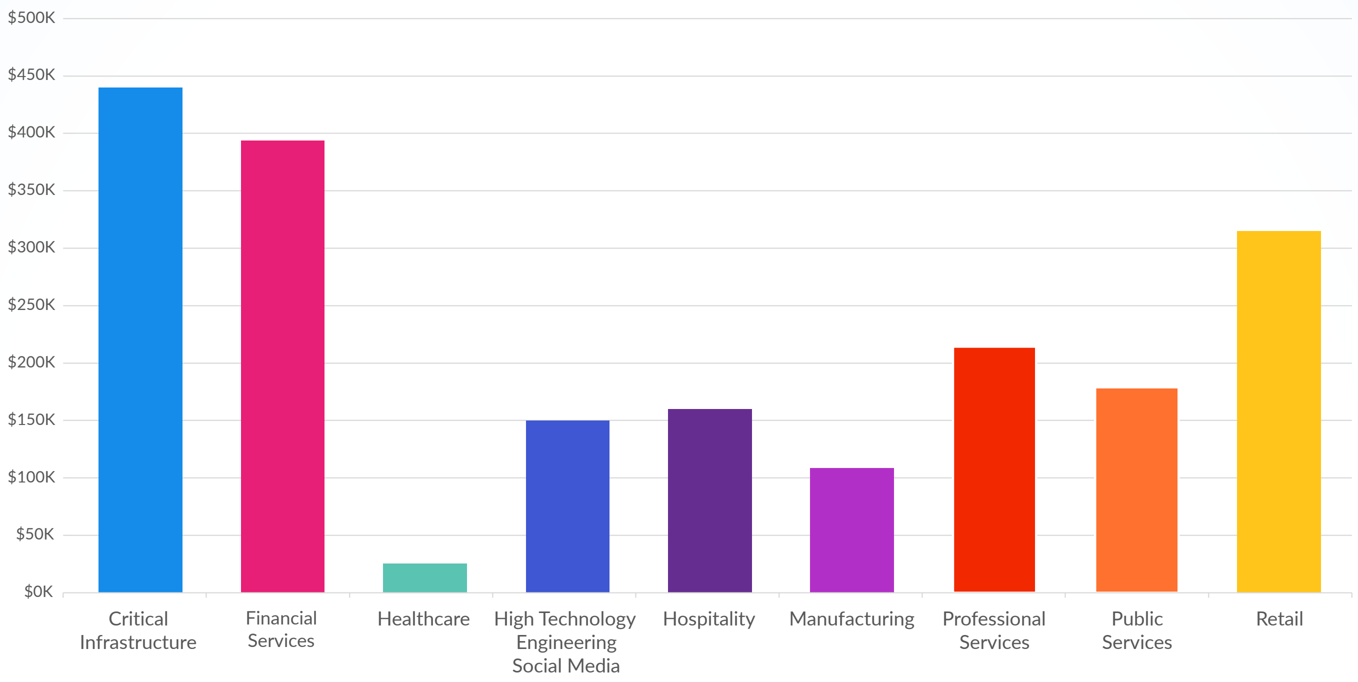


Figure 4: Average Ransom Demand by Industry

Ransomware groups demand the highest average ransoms from Critical Infrastructure ($440K) and Financial Services Companies ($394K), likely due to the pressure for uptime in those industries combined with the associated revenue of those companies. Retail ($315K) and Professional Services Firms ($214K) come in third and fourth among industries as threat actors take advantage of perceived reputational harm that comes from a publicized ransomware attack. Because most ransomware engagements Arete responds to involve double extortion, in which threat actors both encrypt and exfiltrate an organization's data, these numbers primarily reflect ransoms demanded to decrypt and prevent the publication of stolen data.

Threat Actor Spotlight – LockBit

Throughout Q3, LockBit showed indications of internal disorganization and conflict with its affiliates. Arete observed an increasing number of engagements across Q2 and Q3 in which LockBit encrypted systems twice or used multiple LockBit variants in the same victim environment. In at least three engagements where LockBit 2.0 ransomware was identified, LockBit 3.0 or LockBit Black ransomware variants were also present. This dual infection pattern causes restoration delays after payment but, as of October 2023, has yet to result in multiple payments.

On September 16, 2023, LockBit polled its affiliates to determine a new policy on how they conduct themselves during negotiations with victims. The primary operators expressed that some affiliates who are desperate for money essentially waste the profit opportunity when attacking large companies. Overall, the primary LockBit operators lamented the “lack of discipline and regulation of the amount of payments in the partner program.” The group further expressed frustration that this disorganization impacts the discounts being given to victims by the various affiliates. LockBit offered the following options to its affiliates:

a. No changes in payment policy; payment options will remain "unregulated" and remain up to the affiliates.

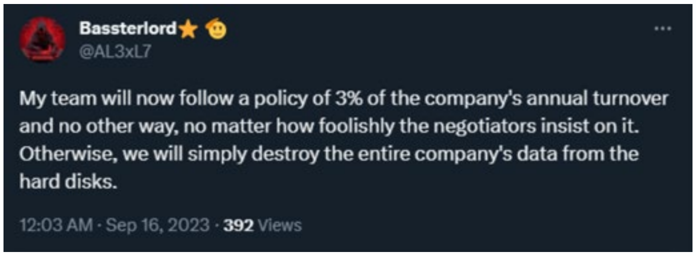
b. Establish new rules that set the minimum payment allowed to be 3% of the victim company's annual revenue with the option of a 50% discount, bringing it down to 1.5% of annual revenue.

c. Establish a new rule that affiliates can only grant a 50% discount on the original ransom price.

d. Establish a new rule that affiliates will not accept a payment below the victim’s maximum ransomware insurance policy.

e. Establish a new rule that affiliates will accept a minimum payment of 50% of the victim’s ransomware insurance policy.

None of these changes have influenced Arete ransom negotiations with LockBit to date, but one identified LockBit affiliate signaled their intent to implement a policy for determining ransom demands, as shown in Figure 5.



Bassterlord⭐
@AL3xL7

My team will now follow a policy of 3% of the company's annual turnover and no other way, no matter how foolishly the negotiators insist on it. Otherwise, we will simply destroy the entire company's data from the hard disks.

12:03 AM · Sep 16, 2023 · **392** Views

Figure 5: National Hazard Agency Tweet (Source: VX-underground)

While LockBit attacks slowed down in Q3, its constant development efforts and continued iterations of its ransomware encryptor means it is unlikely to go away. LockBit’s use of affiliates enabled it to be responsible for an estimated quarter of all ransomware activity globally between June 2022 and June 2023. LockBit originally recruited affiliates through its cost-effectiveness, offering exceptional service and an effective encryptor at a reasonable profit-sharing model. The group further incentivized affiliates by continuing to iterate on its malware, producing encryptors capable of encrypting Windows, Linux, and VMWare ESXi. Increased law enforcement and security industry scrutiny, however, has made the operating environment more challenging for LockBit and its affiliates, driving some affiliates to work with other RaaS operations.

Meanwhile, more and more RaaS operations are offering many of the same benefits as LockBit, but without the scrutiny. LockBit’s recent frustrations with lost profit opportunities and its challenges with multiple payloads in an environment reflect an organization more broadly suffering from its own criminal success. Despite these struggles, LockBit is likely to continue to victimize companies by offering ransomware payloads that meet the needs of affiliates until law enforcement can effectively disrupt the group’s operations and infrastructure.

CRITICAL INFRASTRUCTURE IMPACTS

Across Arete's ransomware engagements in Q3, 46% of impacted organizations fell within the 16 critical infrastructure sectors designated by the Cybersecurity and Infrastructure Security Agency (CISA). Community and Government-based Operations and Essential Functions encompass the government facilities sector and government-adjacent community functions. That sector was most impacted by ransomware and extortion incidents, followed by Transportation and Logistics, Housing-related Services, and Financial Services. In Transportation and Logistics, no industrial control system (ICS) impacts were reported.

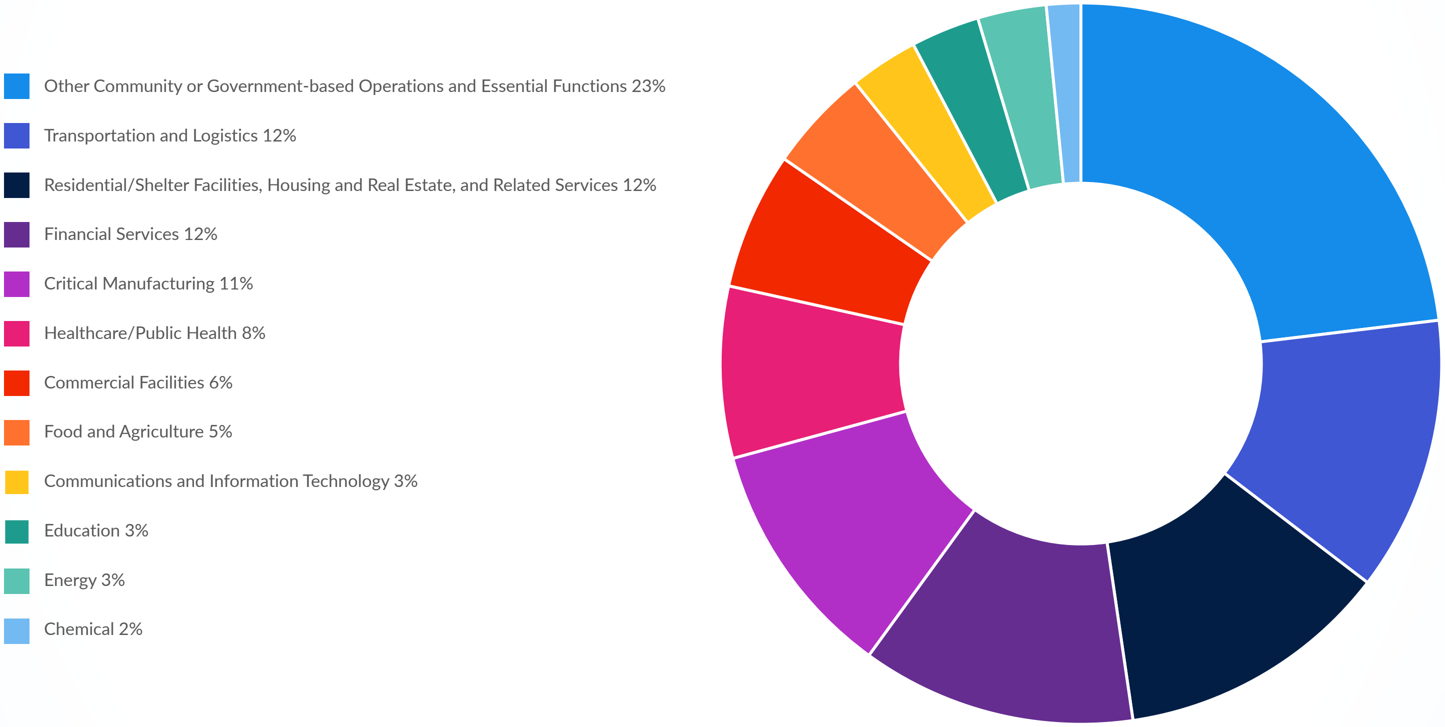


Figure 6: Critical Infrastructure by Sector

Conclusion

GEOPOLITICAL CORNER

The end of Q3 saw deadly attacks in Israel, reigniting the conflict between Israel and Hamas in the Middle East. Over 100 cyber threat groups are engaging in malicious cyber activity surrounding the conflict. Most of the activity consists of low-skill website defacements and distributed denial-of-service (DDoS) attacks that, while disruptive, have little long-term impact on organizations. However, some malicious activity posed a significant threat to Israeli critical infrastructure. In at least one instance, threat actors accessed an alert app used by the Israeli government to communicate with citizens. Threat actors are also distributing a fake version of the app preloaded with spyware.

At least three historically Russian-aligned cyber threat actors are engaged in pro-Palestine activity, and multiple pro-Palestine organizations are launching low-skilled attacks against NATO countries in support of Russian objectives. The overlap between these groups is expected, as both seek to introduce chaos into already chaotic situations.

At least three historically Russian-aligned cyber threat actors are engaged in pro-Palestine activity, and multiple pro-Palestine organizations are launching low-skilled attacks against NATO countries in support of Russian objectives.

Meanwhile, the Ukrainian Computer Emergency Response Team (CERT) reported additional wiper malware deployed by Russian-sponsored threat actors. The wiper malware has thus far been contained in Ukraine, but a more widespread impact is possible. The Russia-Ukraine conflict also continues to drive threat actors to base their operations out of new geographic areas, including Turkey and France. These movements appeared to initially disrupt groups in 2022 at the start of the conflict, but shifting geographies seems to have settled and likely did not significantly impact ransomware operations in Q3.

CONCLUSION

Q3 reflected ongoing instability in the ransomware ecosystem and the world. In Q4, the ransomware ecosystem is likely to continue to shift, with affiliates likely to move between big-name groups. Some affiliates will likely conduct strictly exfiltration-based extortion to avoid sharing profits with RaaS operations like LockBit, ALPHV/BlackCat, Akira, and Phobos. Other groups may rebrand to avoid law enforcement scrutiny and reputational harm created by affiliates making headlines. Meanwhile, ransomware groups that moved their operations in response to geopolitical events will likely face heightened law enforcement actions as new geographies expose them to different enforcement practices and extradition risk.

Resources

Arete Internal Data

Arete Dark Web Services

https://cybernews.com/security/clop-publish-all-moveit-victim-ransom-data-clearweb/

https://www.securityweek.com/nearly-1000-organizations-60-million-individuals-impacted-by-moveit-hack/

https://unit42.paloaltonetworks.com/cl0p-group-distributes-ransomware-data-with-torrents/

https://flashpoint.io/blog/israel-hamas-war-intelligence/

https://falconfeeds.io/blog/post/the-evolving-landscape-of-cyber-warfare-in-the-israelpalestine-conflict-a-comprehensive-analysis--356011

https://twitter.com/vxunderground/status/1702925435443585286

https://socradar.io/lockbits-new-regulations-sets-minimum-for-ransom-demands/

https://flashpoint.io/blog/lockbit/

https://www.wired.com/story/israel-hamas-war-hacktivism/

https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/

https://www.hackread.com/hackers-fake-rocket-alerts-red-alert-app-israel/

https://www.bleepingcomputer.com/news/security/fake-redalert-rocket-alert-app-for-israel-installs-android-spyware/

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

https://cert.gov.ua/article/6123309

https://www.ft.com/content/d5ba3c90-c2f2-4d4e-9cf0-b929930ad8f7

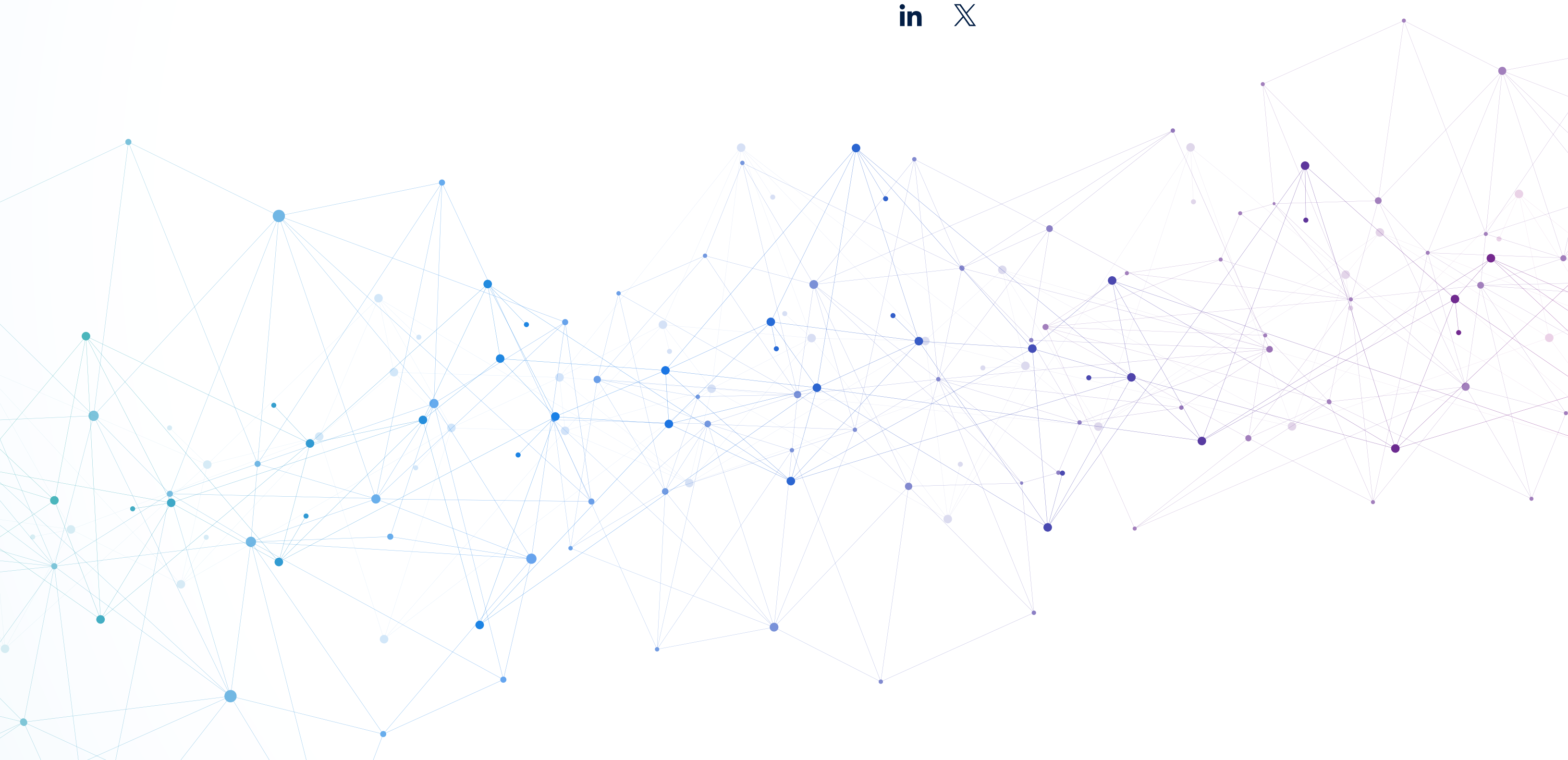
Arete

Cyber Emergency Helpline 866 210 0955
Phone 646 907 9767

New Engagements
arete911@areteir.com

General Inquiries
marketing@areteir.com

www.areteir.com



Arete Advisors, LLC makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the contents of this report and expressly disclaims liability for errors and omissions in the content. Neither Arete Advisors, LLC, nor its employees and contractors make any warranty, express or implied or statutory, including but not limited to the warranties of non-infringement of third-party rights, title, and the warranties of merchantability and fitness for a particular purpose, with respect to content available from this report. Arete Advisors, LLC assumes no liability for any direct, indirect, or any other loss or damage of any kind for the accuracy, completely, or usefulness of any information, product, or process disclosed herein, and does not represent that the use of such information, product, or process would not infringe on privately owned rights. Information contained in this report is provided for educational purposes only and should not be considered as legal advice.