



**K7 THREAT
PREDICTION
REPORT 2024**

Back to the Future.....3

Rising Cyber Threats.....4

Unmasking the Ransomware Onslaught.....5

Zero-day Vulnerabilities and IABs.....7

The Upsurge of Stealer Malware and RAT Attacks.....8

Phishing Threats and Advanced Technology.....9

 Making it even easier- Scama.....10

 The Global Impact10

 Spear Phishing and BEC11

 Smishing12

 The Significance of Generative AI13

Perpetual Attack Trends on Individuals.....13

 Adware13

 Banking Trojans14

 Malware Dropper14

 Spyware.....14

 Investment Scams.....14

 Romance Scams.....15

 QR phishing and the relevance of OTP.....15

 SIM Swapping.....16

Hacktivism will spread its wings further.....16

Proactive Defense for the Enterprise.....18

 Key Takeaways.....18





Back to the Future

Identifying and thwarting oncoming threats primarily focuses on crafting a framework that supports informed decision-making and shapes robust cybersecurity strategies to repel potential cyber onslaughts. However, it's not a simple or linear process but a complex, multi-level, ongoing effort. Thanks to our years of combating digital malice at K7 Computing, we've accumulated a wealth of knowledge, allowing us to anticipate what cybercriminals are plotting.

Our K7 Cyber Threat Prediction Report 2024 incorporates input from our extensive industry experience, our gathered threat intelligence, and the evolution of diverse threats to provide a comprehensive view of the 2024 threat landscape.

Though promising, new applications and technologies may have security flaws, as they are usually developed with customers demanding a sense of urgency and a lax attitude towards cybersecurity.

Adding to this complexity is the prevalence of cyberattacks backed by nation-states. Cyber warfare involves high-level techniques to penetrate enemies' digital networks, steal sensitive data, or disrupt critical services, instigating a digital power play. It calls for a global understanding of the repercussions and regulations of this digital battlefield.

To stand against these threats, businesses and MSMEs need a multi-pronged strategy that includes examining established threats, predicting shifts in tactics, and acknowledging how emerging technologies like generative AI play a crucial role. As our digital universe expands, our understanding and protection against the fluid landscape of cyber threats need to keep pace.

We hope you have a secure and enjoyable 2024, safe from cybercriminal acts. Lastly, we wish you an enriching read and a wonderful new year!

Rising Cyber Threats

New cutting-edge technologies and existing ones are unprecedentedly shaping our world, driving progress alongside, unfortunately, boosting the scope for harmful cyber activities. Cyber threats, a continuous spectre over digital connectivity, are growing exponentially.

The clandestine threat actor communities and flourishing dark markets act as hotbeds for exchanging cybercrime methodologies, data, and tools. These, coupled with emerging technologies like generative AI, increasingly sophisticated deepfake tools, and initial access brokers, (IAB) provide threat actors with an extensive, easily accessible repertoire of subversive techniques. For the uninitiated, Initial access brokers are individuals or groups specialising in gaining unauthorised access to corporate networks and systems. They often sell this access to other threat actors, such as ransomware operators or data thieves, who exploit compromised networks for financial gain or espionage. Yet, these factors alone do not explain the escalation in cyber threats.

What fuels this growing tide is the widespread ignorance about these cyber threats, combined with a lackadaisical approach to cyber hygiene. Enterprises and individuals frequently overlook basic cybersecurity measures, leaving digital doorways open for threat actors. Moreover, the need for adequate investment in cybersecurity further compounds the problem. Cybersecurity, often seen as an expensive, non-essential burden, tends to be disregarded in budget allocations.

The barrage of cyber threats is unlikely to wane if this indifference continues. There is an urgent call for comprehensive cyber education, stringent cyber hygiene practices, and a prioritised focus on cybersecurity budgets to counter the growing menace. Technologies are mere tools, and their use for disruption is a human issue that deserves serious attention.

In the accompanying infographic, you will find a deeper focus on these significant concerns, as we aim to highlight the gravity of the situation and channel awareness towards rectification.

UNMASKING CYBERSECURITY THE RISE OF CYBERCRIMES



Increasing Digitisation

As enterprises embrace the digital revolution, they create exploitable digital footprints, attracting cybercriminals.

Insufficient Cybersecurity Training

Employees are often uninformed about safe digital practices, making them vulnerable to phishing attacks or malware.



Evolving Cyber Attacks

Cybercriminals consistently enhance their methods, deploying sophisticated tools to exploit unprepared businesses.

Inadequate Incident Response Plans

As enterprises embrace the digital revolution, they create exploitable digital footprints, attracting cybercriminals.



The Growing Internet of Things (IoT)

As the IoT ecosystem grows, end users risk being targeted through unprotected smart devices at home.

Lax Personal Cybersecurity Practices

Ignorance about secure online practices or using outdated security protocols expose individual users to cyber threats



Unmasking the Ransomware Onslaught

The ransomware threat landscape continues to evolve, with transnational organised actors enhancing their capabilities to carry out impactful attacks. These attacks extort funds, disrupt critical services, and expose sensitive data. While essential services and critical infrastructure have been frequent targets, there has been a notable increase in ransomware attacks targeting governments worldwide. Major cybercrime groups have diversified their ransomware business models, incorporating newer forms of extortion and enhancing the capabilities of their malware to target a broader range of technical assets. Although some ransomware groups may cease operations due to various factors, they often find ways to rebrand, reconstitute, or renew their activities. This evolving threat landscape requires heightened vigilance and proactive measures to safeguard against ransomware attacks.

The threat landscape for ransomware is evolving rapidly, with a 13% increase in ransomware breaches year-over-year, according to data from Verizon (1). As the FBI (2) reported, these attacks have become more targeted, impacting the healthcare, food, and agriculture sectors. The 2023 Allianz Risk Barometer (3) highlights those cyber incidents that rank among the top perils facing 19 countries, including the UK, France, Austria, Spain, India, and Japan. Small companies in these countries are particularly concerned about business interruptions due to cyberattacks.

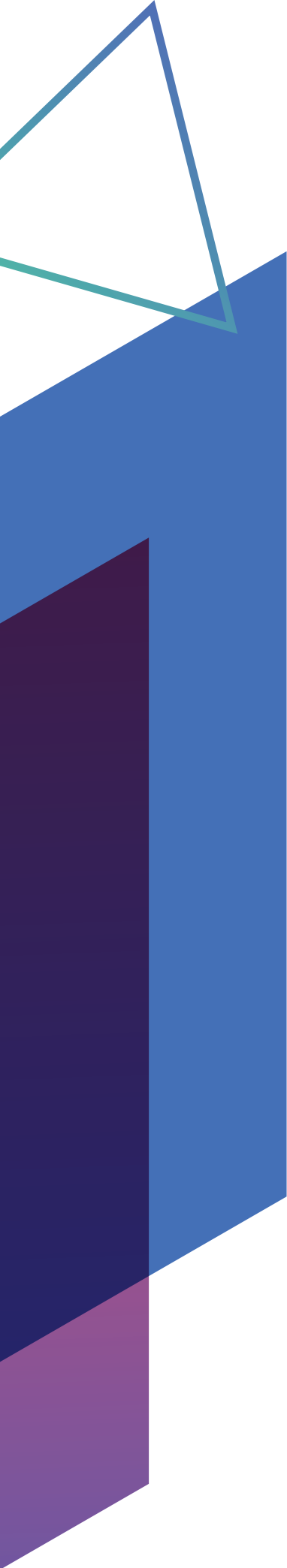
The K7 Telemetry data (TI and escalations) asserts that in 2023, 1.3 out of every ten attacks were ransomware. The numbers could be smaller because ransomware actors and affiliates have single-eyed businesses and yanked individual users from their lists in the past few years.

13%

RANSOMWARE



out of the total number of threats in 2023



The recent White House National Cybersecurity Strategy of the US has reclassified ransomware as a top security threat, emphasising the need for a comprehensive federal approach in collaboration with international partners to combat it. Research (4) predicts global ransomware damage costs will double from \$21 billion in 2021 to \$42 billion annually in 2024 and escalate to \$265 billion by 2031 due to more frequent attacks on governments and critical infrastructures.

Notably, ransomware gangs such as Lockbit, CLOP, Medusa Locker, Royal, AlphaVM (BlackCat), 8BASE, Royal, PLAY, and Black Basta are expected to intensify their malicious activities by refining their payloads and employing sophisticated extortion techniques. Ransomware attacks are on the rise, with a 13% increase (1) in ransomware breaches year-over-year, and they are becoming more targeted. Threat actors now have easier access to powerful ransomware tools, enabling them to launch costly attacks with modest technical skills. The availability of ransomware and other malware for purchase and the global average cost of a data breach at \$4.35 million (1) further exacerbate the situation. The emergence of Ransomware-as-a-Service (RaaS) kits has made it even easier for threat actors to deploy attacks quickly and affordably, posing a significant challenge for cybersecurity leaders.

Besides focusing on the larger enterprises to make massive money, attackers will lean more towards small and mid-market businesses as they know that with the increased digitisation in the MSMEs, lack of cybersecurity professionals, often inundated with outdated or misconfigured solutions managed by inadequately trained IT teams, offers great scope for cyber attacks.

In 2024, cybercriminals are anticipated to use a wide range of extortion methods to increase their chances of receiving payments from their victims'. Along with encrypting networks, stealing data, and holding the stolen sensitive data to ransom, ransomware operators may threaten the victims' partners or clients and execute DDoS attacks or wiper malware to wipe out the entire enterprise data after taking a backup of it in their systems.

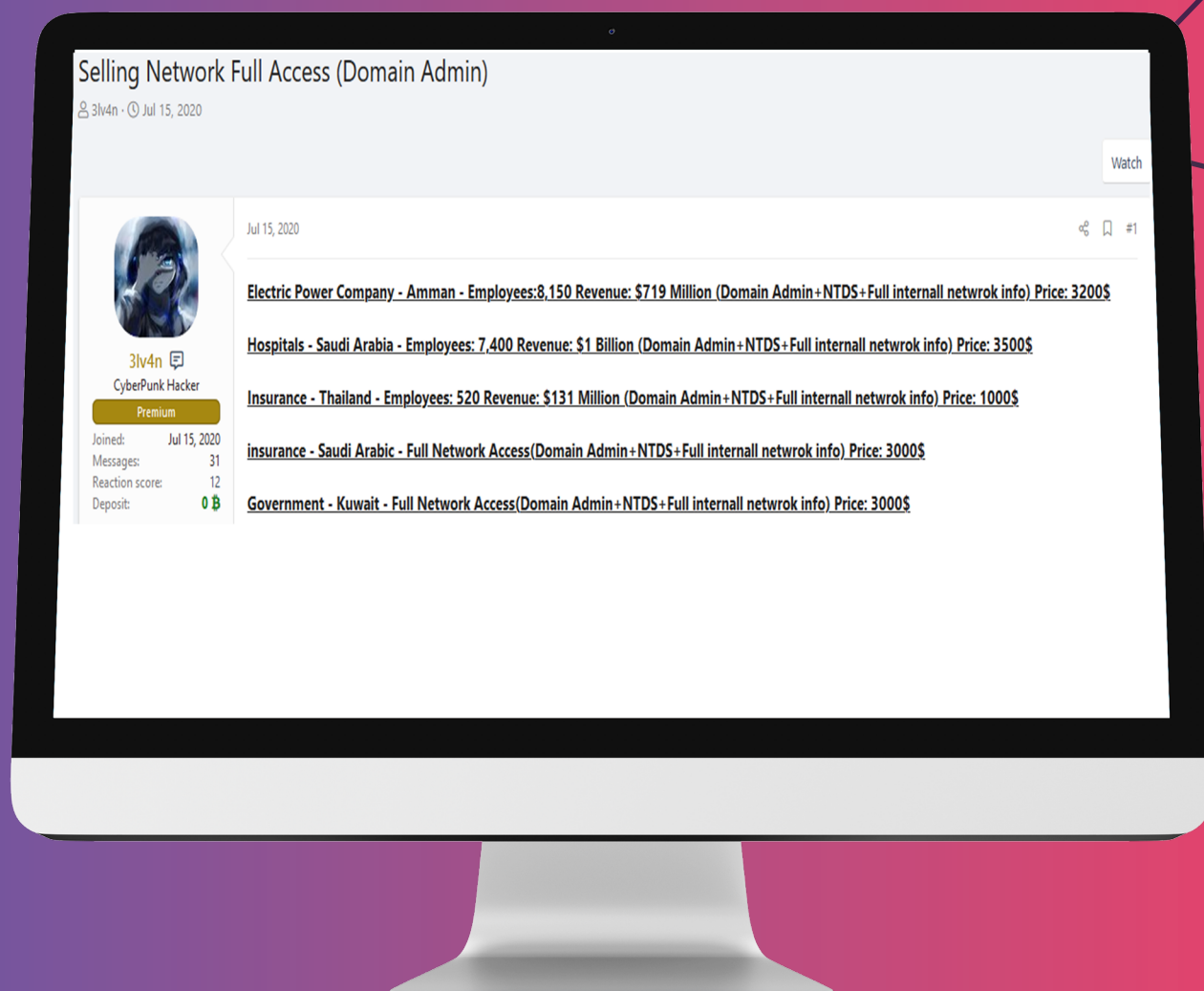
In light of the alarming accessibility of ransomware kits for as little as \$66 in underground forums and the prevalence of free phishing kits, the imminent surge in ransomware attacks is undeniable. This surge fuels the escalating number of software vulnerabilities, internet-exposed unsafe services, applications, emails, web security issues, and compromised system reputations. Furthermore, using cryptocurrency for ransom payments, which are immutable and challenging to trace, adds another layer of complexity to combating ransomware attacks. In response, we strongly advise organisations of all sizes to maintain high vigilance and proactively safeguard themselves against the escalating ransomware threat.

Zero-day Vulnerabilities and IABs

Initial access brokers play a critical role in the operations of ransomware actors, nation-state threat actors, and advanced persistent threats (APTs) by providing them with a means to gain initial access to target networks. These brokers leverage their expertise and resources to identify and exploit vulnerabilities in corporate and MSME networks, enabling threat actors to establish a foothold and carry out their malicious activities. They also sometimes deal with zero-day vulnerabilities in exchange for hefty sums from several high-profile threat actors.

Initial Access Brokers (IABs) escalate in influence through their sales of network access to various threat actors, including ransomware operators and affiliates. Access deals usually occur off-forum, a trend noted by innumerable researchers interacting with IABs through covert channels.

These off-forum transactions often cost less than purchases made directly through open forums. This cost-effectiveness increases the appeal of these deals for frequent buyers. It incentivises an ongoing relationship between the IABs and the buyers, ensuring a steady stream of profits for the IABs while giving buyers consistent access to systems and networks.



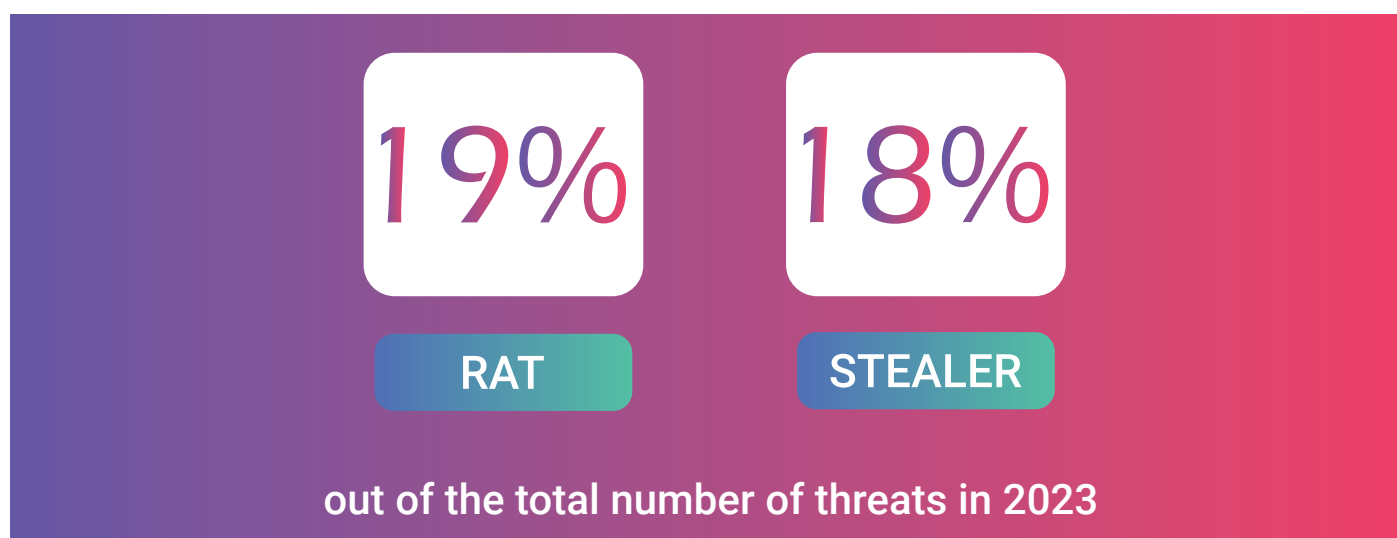
Furthermore, the established rapport between IABs and buyers on these off-forum channels often guarantees discounts, especially for access to high-value networks. Proactive notifications on upcoming access sales are also typical, allowing buyers to stay ahead in the constantly evolving cyberthreat landscape.

These brokers often offer compromised credentials of users, root, enterprise, local or domain admins, or service access such as VPN, RDP, cPanel, SSH, SQL, FTP, CMS, Webshell, database, etc., and charge between a few dollars to thousands.

The Upsurge of Stealer Malware and RAT Attacks

Understanding the Escalating Cyber Threat Landscape While the attack frequencies of remote access Trojans (RATs) and information stealers may be higher than ransomware or phishing, these threats are less publicised because they often remain hidden and silent when infiltrating a network or device. RATs and information stealers typically operate in the background, secretly gathering information without noticing their presence, unlike ransomware, notorious for its overt disruptiveness, locking users and organisations from their systems until a ransom is paid. The impact is immediate, often crippling enterprise operations, which creates high-profile news stories. Similarly, because of their direct effect on individuals through email scams, phishing attacks gain a lot of attention. Such attacks can lead to immediate financial loss, identity theft, and other personal damage, leading to their widespread discussion.

Notably, the K7 Telemetry report reveals that in 2023, RAT and stealer malware were responsible for 19% and 18% of the total number of thwarted attacks in the country, respectively. Surprisingly, these figures are much higher than the statistics for ransomware during the same period. It is worth mentioning that these two malware types are preferred by various threat actors, including nation-state ones, due to their effectiveness in achieving their objectives.



It is important to note that stealers are readily available for little or no cost on various online platforms and are commonly used to extract sensitive information such as credentials, session cookies, and internet history from the victim's browser. This information is often used for triggering ransomware attacks. Furthermore, initial access brokers usually employ these two malware types to gather information about potential victims, such as networks, and then sell it at a higher price.

In sync with the current cybersecurity trend witnessed in 2023, RATs will continue to be prominent and arguably one of the most observable forms of malware in the forthcoming years.

These malware types are deployed with an array of nefarious intentions, ranging from establishing enduring persistence within a network or a system to gaining remote control of a victim's device. Once triggered, RATs grant the invader the ability to extract text and files, acquire screenshots, record audio or video, and perform copious other undertakings. What makes them particularly insidious is their capacity to install additional malevolent software programs, amplifying the attack's scope. To add insult to injury, RATs also play a crucial role in facilitating other damaging campaigns like ransomware, augmenting the threat landscape.

In 2024, a marked increase in the attack statistics for Novel stealer families besides the prevalent ones such as Raccoon, Metastealer, Atomic Stealer, Shadow Vault, Sapphire, Redline Stealer, and others, is expected across various platforms.

Phishing Threats and Advanced Technology

Phishing attacks have reached unprecedented levels, posing a significant risk to organisations of all sizes. The availability of generative AI has empowered threat actors to craft flawless phishing emails, eliminating the telltale signs of spelling mistakes, grammar errors, and broken English that once made such scams easier to spot. These sophisticated emails can now be tailored to the recipient's language and even include personal details, making it increasingly challenging to distinguish between genuine and fraudulent communications. As a result, phishing has emerged as the most prevalent cyber threat in recent years, with a staggering 74,213 internet users encountering thwarted phishing scams between July and September 2023 alone, according to K7 Telemetry. It equates to an alarming average of 24,738 attacks per month, 825 attacks per day, 34 attacks per minute, and one attack every two seconds.

In the second quarter of 2023, the Anti-Phishing Working Group (APWG) observed (5) a significant prevalence of phishing attacks, with 1,286,208 attacks recorded globally. While this figure represented a decrease from the record high of 1,624,144 attacks in the first quarter of 2023, it still marked the third-highest quarterly tally in APWG's historical observations. Notably, this total was substantially higher than the 888,585 attacks in the fourth quarter of 2022 and on par with the 1,270,883 phishing attacks in the third quarter of 2022. This trend indicates a persistent threat of phishing attacks despite a slight decrease from the previous quarter.

74,213

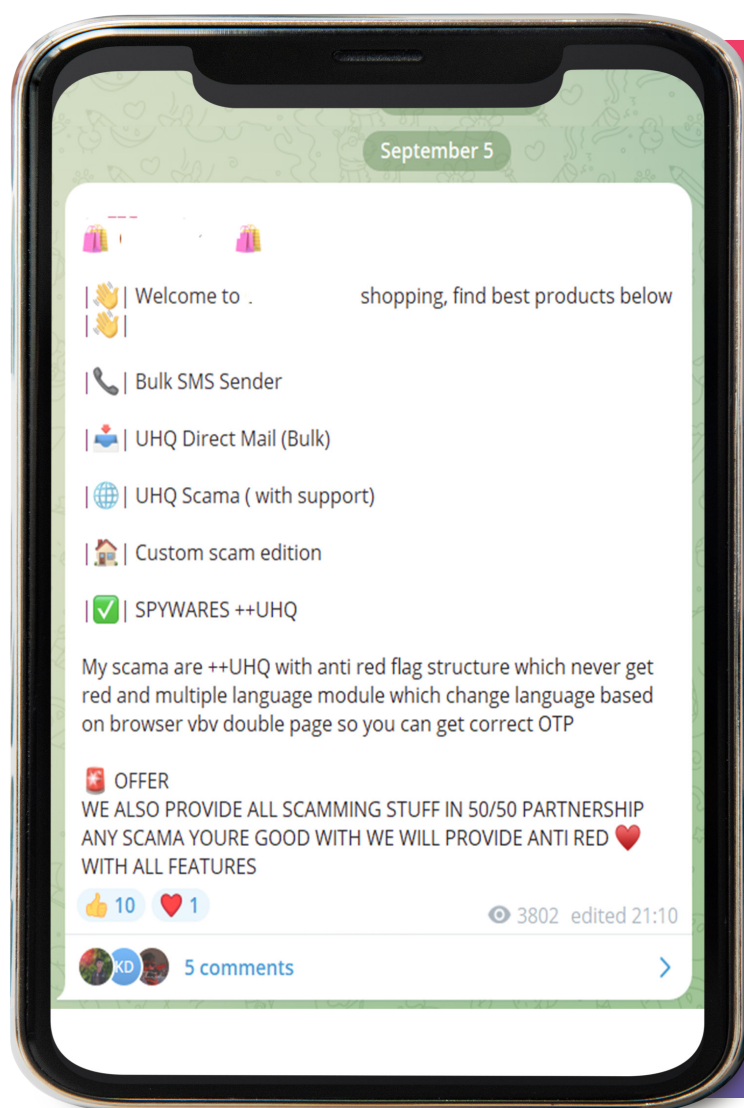
Phishing Incidents IN

Q2 2023-24



Making it even easier- Scama

Both findings indicate a concerning prevalence of phishing attacks, with no signs of abating in the foreseeable future. These incidents are projected to escalate with each passing month. Of particular note is the proliferation of Phishing-as-a-service (PhaaS), an infamous business model that peddles sophisticated phishing kits, also known as scama, to individuals willing to pay. Scama, a term denoting a collection of malicious assets packaged and sold to threat actors, is readily available on social platforms like Telegram, primarily hosted on well-known web hosting platforms in the Asia-Pacific (APAC) region. These kits equip cybercriminals with all the necessary tools to orchestrate a successful phishing campaign, including deceptive email templates and counterfeit web pages that mimic legitimate brands and services. Many of these malicious toolkits showcase sophisticated capabilities, including anti-bot protection, responsive design, and verifiable effectiveness, intensifying the threat landscape.



The Global Impact

Phishing's continued evolution is primarily due to assaults using spear phishing or the delivery of malware, such as RATs, wipers, ransomware, etc., onto the victims' devices. Advanced Persistent Threats (APTs), often associated with nation-state actors, organised crime groups, or other advanced adversaries, leverage sophisticated phishing campaigns to infiltrate and create persistence majorly in government agencies, critical infrastructure, and private sector organisations to pursue political, economic, or military objectives. Such phishing assaults have increased across Europe and the US since Russia invaded Ukraine, showing how APTs prioritise phishing attacks to accomplish their goals.

Spear Phishing and BEC

Spear phishing email threats and Business Email Compromise (BEC) pose a growing risk to individuals and businesses. Cybercriminals are becoming increasingly sophisticated in using social engineering tactics to create convincing emails that trick recipients into revealing sensitive information or transferring funds to fraudulent accounts. With generative AI, spear phishing emails utilised in these BEC scams can convincingly emulate the writing style and tone of a colleague, boss, or trusted third party. This ability raises the danger level significantly since it can create deceptive emails that bypass standard rule-based security systems and deceive even discerning human eyes. According to the Anti-Phishing Working Group (5) (APWG), the average wire transfer amount requested in BEC attacks in Q2 2023 was \$293,359, up 57 percent from Q1's average of \$187,053.

According to the FBI (2), threat actors earned almost \$43 billion between 2016 and 2021. We anticipate a significant increase in cyber threats in the upcoming year as threat actors exploit various sources and technologies to intensify and obfuscate their attacks.

In 2024, major global events such as the US, India, Indonesia, Mexico, Taiwan, and UK general elections and the European Parliament elections are crucial and will reshape the cyber threat landscape.

Different actors, from nation-states to individual cybercriminals, find these events opportune to launch their attacks. High-worth individuals - politicians, business leaders, or influential figures - may be targeted due to their financial worth and the potential leverage their information might provide.

This trend is expected to pose a more significant challenge for organisations in detecting and mitigating these threats. CXOs and employees of corporations and MSMEs must remain vigilant and proactive in enhancing their cybersecurity measures to combat these evolving threats effectively.

EXPLOITING EVENTS AND EMOTIONS

THE INTRICATE WEB OF PHISHING

The LURE OF HIGH TRAFFIC EVENTS

Pretending to be popular business, cybercriminals use crowd-pulling events like Cyber Monday or Black Friday to target more significant demographics with too-good-to-be-true deals.



INFORMATION OVERFLOW

In the frenzy of big news or events, people are prone to overlook malicious links exposing their private data.



FEAR AND URGENCY

Masquerading as health or government bodies, scammers drive victims to make immediate decisions to avoid purported threats.



SOCIAL ENGINEERING

Cybercriminals adapt their approaches based on current events or trend, using commanding or alarming language to extract sensitive information.



IMPERSONATION AS A TRICKERY TOOLS

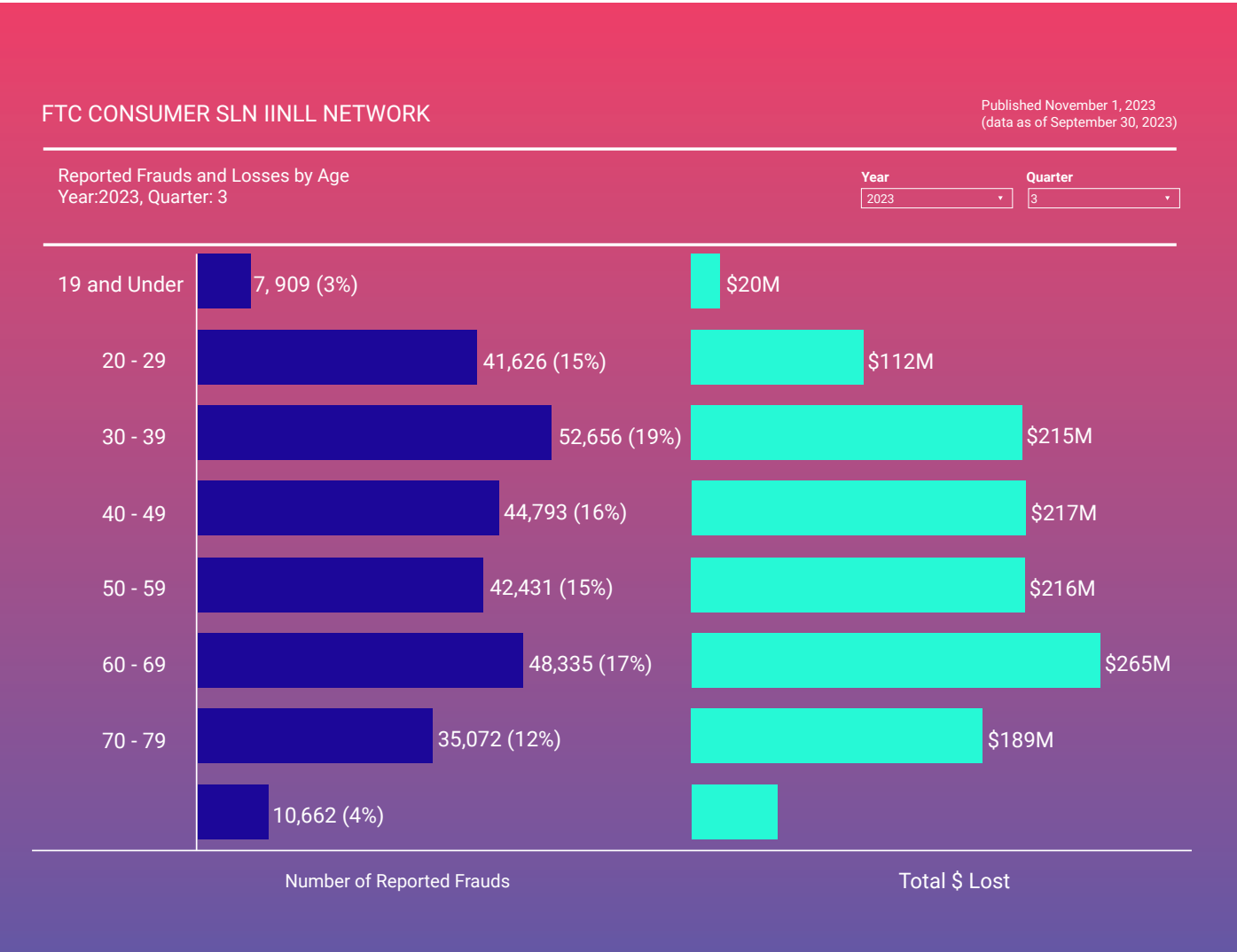
Fraudsters mimic reputable institutions associated with the event to gain the victim's trust.



Smishing

The prevalence of smishing attacks continues to pose a significant threat to mobile phone users, particularly the older generation, as they struggle to discern the authenticity of SMS messages. This lack of awareness (6) has contributed to the high success rate of smishing, with only 23% of mobile phone users over 55 accurately defining the term. Alarmingly, even millennials have shown limited awareness, with only 35% of individuals aged 23-38 familiar with smishing. The insidious nature of smishing, which leverages social engineering tactics, makes it challenging to detect, leading to less than 35% of mobile phone users recognising when this form of fraud targets them.

In the first half of 2023, the United States witnessed a staggering surge in smishing attacks, with an estimated 78 billion malicious messages circulating and resulting in a substantial financial loss of \$13 billion, as reported by Robokiller (7). The report identified delivery, bank scams, travel, and COVID-19-related messages as the most prevalent types of smishing attacks. Furthermore, the Federal Trade Commission's Q3, 2023 findings (7) revealed a concerning trend in the financial impact of smishing attacks across different age groups. Individuals under 20 suffered losses amounting to \$20 million, while those in the 20-29 age bracket experienced a significant increase in losses up to \$112 million. The severity of the financial impact continued to escalate with age, reaching an alarming estimated loss of \$1157 million for individuals aged 30 and above.



These findings underscore the pervasive and detrimental nature of smishing attacks and how the landscape could transform into a more gruesome one in 2024 and the time ahead. Still, on a happier note, various governments, including India, are putting enormous effort into educating mobile phone users concerning the onslaught through different social media platforms.

The Significance of Generative AI

Spear phishing and smishing will become more prevalent as technology advances, becoming more convincing than ever using complex tools powered by artificial intelligence (AI). However, although AI is employed in many threat detection processes, bad actors are already developing more sophisticated assaults utilising the technology. For instance, Deepfake AI technologies, significantly help threat actors pass for real people when launching social engineering assaults.

Threat actors can significantly benefit from using the Generative Pre-Trained Transformer (GPT4) and the sensational AI-driven chatbot, ChatGPT, to spoof

employees' writing styles and send automated emails that are difficult to distinguish. Many recent AI-driven software solutions can also produce speech and video from a few seconds of audio or video input. The cloned outcome would be next to the original and could pass a biometric test.

We advise MSMEs and businesses to set up cybersecurity education and awareness programmes to teach staff members how to spot social engineering, phishing, phone scams, and spoof calls. The enterprises should also practise phishing or social engineering simulation exercises to combat the onslaught.

Perpetual Attack Trends on Individuals

Bad actors will retain their furious momentum until all the businesses and governments adopt the essential precautions to confront and stop the onslaught. Here are a few key threat patterns we saw throughout 2023; we predict they will intensify further in the next year.

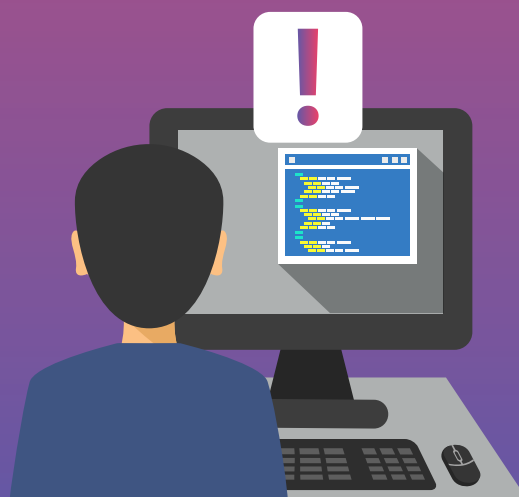
Adware

Initially perceived as an annoyance, adware now poses a severe cyber threat. The most troubling aspect is that adware attacks are relatively straightforward, yet their consequences can be significantly damaging.

Adware's mode of operation is relatively less invasive than counterpart threats such as ransomware or crypto-jacking. It works under the guise of legitimate software, making it difficult for typical anti-virus tools to detect. Cybercriminals are increasingly adopting this method for delivering malicious payloads to victims' systems without raising the alarm. Adware is also highly manipulative, capitalising on users unknowingly consenting to complex terms and conditions. This ambiguity provides a legal shield to adware, making it difficult for judicial bodies to hold threat actors accountable.

The K7 Telemetry data 2023 plots adware as the most prevalent threat, with a 20% share of the total number of attacks, hinting that its trend would continue to rise. It predicts a possible evolution of adware, with threats likely to become more deceptive, sophisticated, and destructive. Threat actors may develop more robust versions of adware that can evade advanced security measures, making detection and removal more difficult.

20%
Adware found
IN
2023



Banking Trojans

Banking Trojans frequently target mobile banking users to steal their credentials and replicate themselves to expand their victim base. Appearing on the official app stores of Google, Apple, and third parties, these Trojans often masquerade as utility apps such as book readers, media players, photo editors, etc. and intercept SMS messages. Besides regular malicious activities, we overlooked a few Trojans, such as Rusty Droid, which tracks user activities and creates a backdoor for other nefarious purposes. In 2024, we anticipate many new families of banking Trojans to surface in the wild. Hence, we recommend updating your smartphone's operating system to the latest version. Additionally, install K7 Mobile Security for Android and iOS to block cyberattacks.

Malware Dropper

The Android app store was inundated with a wide range of dropper apps in 2023 that passed off as genuine programs, offering various productivity and utility. Dropper apps are preferred among other malware distribution techniques for their ability to handle the infection remotely, deliver a payload, and evade different malware detection technologies. As a result, they will thrive in their spectrum in 2024 across platforms.

Spyware

Spyware is one of the most prevalent malware, primarily targeting high-worth individuals' smartphones and employees of large enterprises. The key reason behind the skyrocketing numbers of spyware infections is the increasing espionage activities by several governments for political interests and by malware actors as part of initial intrusion methods. Pegasus and Predator are two of the most well-known malware families associated with this group.

Investment Scams

Despite their startlingly low success rate, the effect and concern surrounding investment-related frauds will increase over time. According to reports, investment-related thefts are the most expensive cyber danger, surging to \$3.31 billion in 2022 from \$1.47 billion in 2021 (3). Federal Trade Commission claimed that in Q3 2023, investment-related scams topped the list of all online crimes with a total reported (8) loss of over \$931.2m in the US.

Investment fraudsters frequently swarm social media platforms and instant messenger chat rooms, such as LinkedIn, Twitter, Telegram, Reddit, YouTube, etc., with an effective hourly rate of over 100 victims. These con artists often pose as investment gurus, startup owners, or claim to have made large sums of money through a cryptocurrency trading or mining platform or similar to persuade their victims to invest alongside them or learn how to trade effectively.

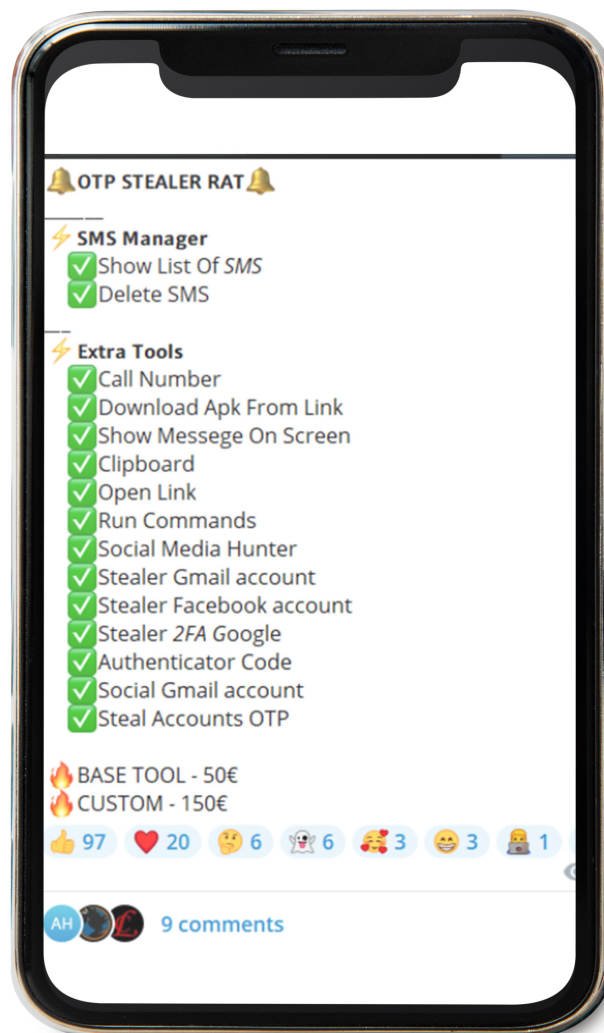
Riding on the rage of the burgeoning cryptocurrency markets, investment-related scams, including pig butchering, will escalate their victim list to a new height in 2024. Therefore, we recommend that potential investors be more sceptical about social media advice and research before investing anywhere.

Romance Scams

Scams related to duping victims in the name of falling in love and making money are notoriously known as “romance scams.” They can be found on every dating platform and popular social media site, such as Facebook. The romance scam ranks third after investment fraud, with an estimated reported (8) loss of over \$137.5mn Q3 2023 and is expected to surge further. Therefore, users should be cautious before forming a rapid online relationship, restrict their data, and never pay an unacquainted person.

QR phishing and the relevance of OTP

Scammers use various tricks to obtain OTPs from their victims. Once the OTP is received, the scammers call their victims and ask them to reveal it immediately to take over the victim’s wallet or bank account and gain access to their money. Unfortunately, many consumers do not pay enough attention to the importance of keeping OTP messages secret. It is crucial to be vigilant and never share OTPs with anyone, as this is often the first step in a scammer’s scheme to defraud unsuspecting victims.



QR code phishing is much more sophisticated and has a higher success rate, but con artists seldom use the technique in extensive campaigns. However, the sophistication of this method and the increasing acceptance of QR codes among the masses indicate such activities will become more prevalent.

SIM Swapping

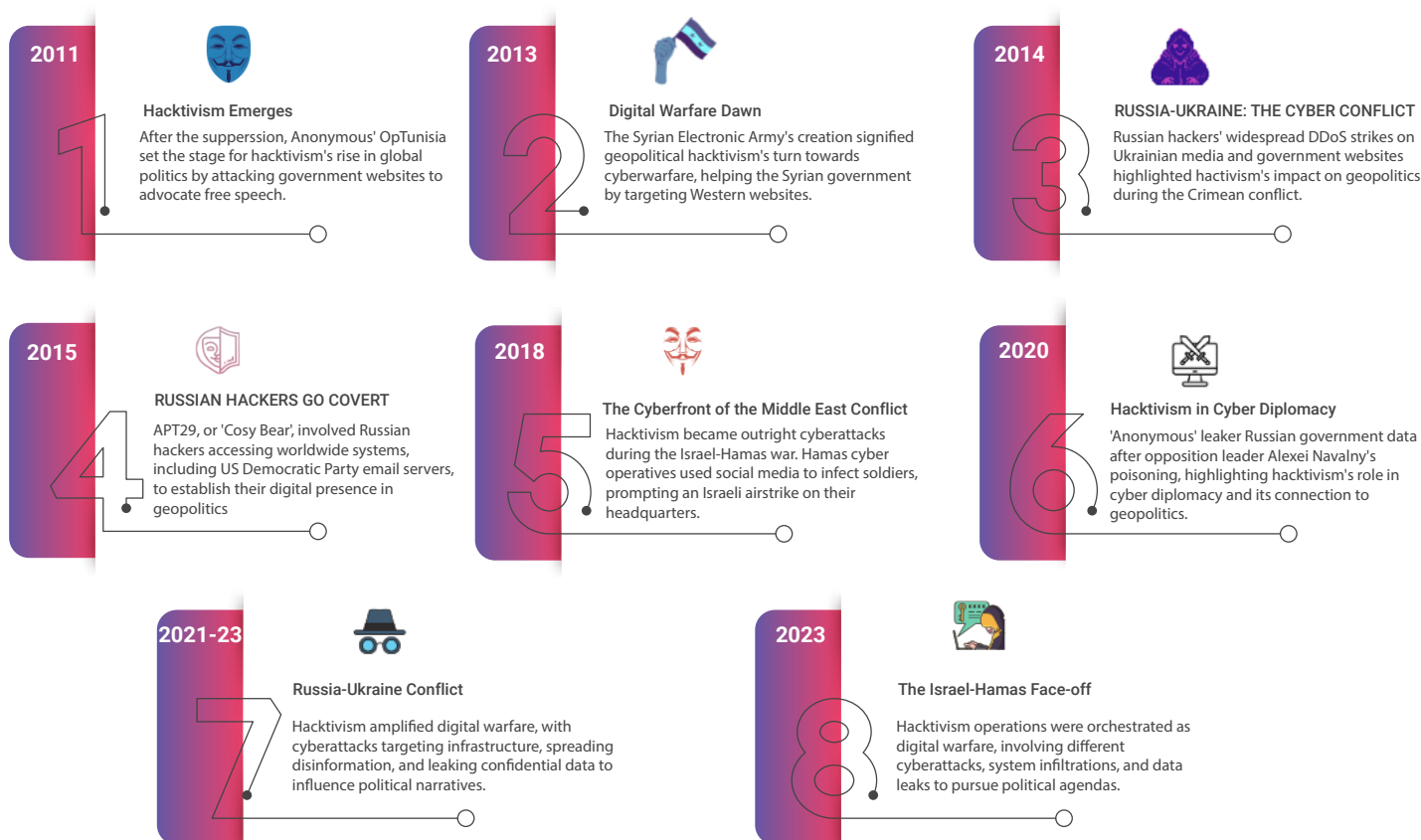
In May 2023, a con man deactivated a businessman's SIM card and had a new one issued. He then withdrew INR 79.70 lakh from the businessman's account. However, the Cybercrime Police in India intervened, recovered INR 50 lakh from the fraudulent activities, and returned that sum to the victim.

Swapping a SIM card or issuing a duplicate becomes easy if you have shared too much personal information online. Sharing OTPs is another trap fraudsters use to swap a victim's SIM card and empty their bank accounts (9).

Hactivism will spread its wings further

During the Russia-Ukraine war, we oversaw how the internet became a playground for hacktivists from both countries—roughly disciplined digital soldiers using the internet's tools to wage information warfare to sway public opinion and pressure the authorities. Both sides have been employing DDoS attacks, data leaks, and misinformation campaigns, increasing the worldwide conflict's visibility and dramatising their stakes.

Next, thrashing through the tumultuous waves of the Middle East, we arrive at the Israel-Hamas clash. The conflict became a digital battlefield, with hacktivist groups on both sides leveraging their skills to disrupt each other's digital infrastructure, online communication, and even military drone systems. Hacktivists also played a role in influencing international opinion through strategic leaks, doxing, and propaganda dissemination.



Hactivism has influenced geopolitical hotspots globally despite its volatility. Whether it's the intensifying territorial disputes in the South China Sea involving multiple nations or the ongoing civil war in Yemen, hactivism has found a way to interject itself, whether through disseminating secret documents, crippling government websites, or spreading propaganda to influence the local and international narrative.

As we look ahead, we see an accelerating rise of hactivism in line with the increasingly digital world. The rise of hactivism is fueled by increasing government and corporate surveillance and concerns over data privacy and information manipulation.

Simultaneously, the ethical implications emerge more prominently. When does hactivism pass from becoming a tool of resistance to a form of online terrorism? How do we demarcate what's in the public interest versus what's pushing a particular agenda? Can hactivism be controlled without intruding on online freedoms?

Bearing these questions in mind, let's move forward, guided by a foresight of an increasingly complex digital world where hactivism plays an ever-influential role. Let's continue to unravel the intricacies of this trend, which might be crucial in navigating the future landscape of global conflicts. It's high time to comprehend this digital phenomenon shaping our geopolitical realities today and, likely, tomorrow.



Proactive Defense for the Enterprise

Key Takeaways

- 1. Get Basics Right:** Data breaches often occur due to overlooked basics, such as open API without authentication, weak passwords, and unattended phishing attempts. Organisations should prioritise routine cyber hygiene to improve their overall security posture.
- 2. Inclusive Security Culture:** Creating a cyber-resilient infrastructure demands collaborative efforts by all departments, not just the IT department. Each department should be accountable for its specific applications, decisions, and processes. Outlining clear line of responsibilities infuses security thinking across the enterprise.
- 3. Shared Accountability and Responsibility:** In cybersecurity, leadership must establish clear accountability and responsibility lines. Exempting personnel based on rank sends mixed signals about security protocols and opens up vulnerabilities. Promoting shared accountability will augment resilience against potential threats.
- 4. Analyse and Understand Risks:** The risk attractiveness of an organisation to attackers often depends on its societal importance and vulnerability due to legacy technology. Businesses with a potentially more significant impact from a breach, such as hospitals, are more desirable targets. Understanding these risks allows for a better security response.
- 5. Balanced Security Strategy:** A sustainable cybersecurity strategy requires the IT department to align with business goals. Security is not an isolated aspect but one among several business risks that demand an enterprise-wide robust approach.
- 6. Smart Resource Allocation:** Diligent resources should be focused on proactively avoiding breaches via practices such as robust patching programs rather than only dealing with the aftermath of instances that could have been avoided.

References

1. <https://www.verizon.com/business/resources/reports/dbir/>
2. https://www.jic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
3. <https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/Allianz-Risk-Barometer-2023.pdf>
4. <https://reprints2.forrester.com/#/assets/2/1795/RES176325/report>
5. https://docs.apwg.org/reports/apwg_trends_report_q2_2023.pdf?_ga=2.6160442.844673322.1701919341-1106216060.1701351066&_gl=1*agmlbj*_ga*MTewNjlxNjA2MC4xNzAxMzUxMDY2*_ga_55RF0RHXSr*MTcwMTkxOTM0MS4yLjAuMTcwMTkxOTM0MS4wLjAuMA..
6. <https://earthweb.com/smishing-statistics/>
7. <https://www.robokiller.com/robokiller-2023-mid-year-phone-scam-report>
8. <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>
9. <https://timesofindia.indiatimes.com/city/ahmedabad/bca-degree-holder-arrested-for-80l-sim-swap-fraud/articleshow/105429913.cms>



www.k7computing.com

Copyright © 2023 K7 Computing Private Limited, All Rights Reserved. This material has been compiled by K7 Security. This work may not be sold, transferred, adapted, abridged, copied or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Computing Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.