ADMM Cybersecurity and Information Centre of Excellence

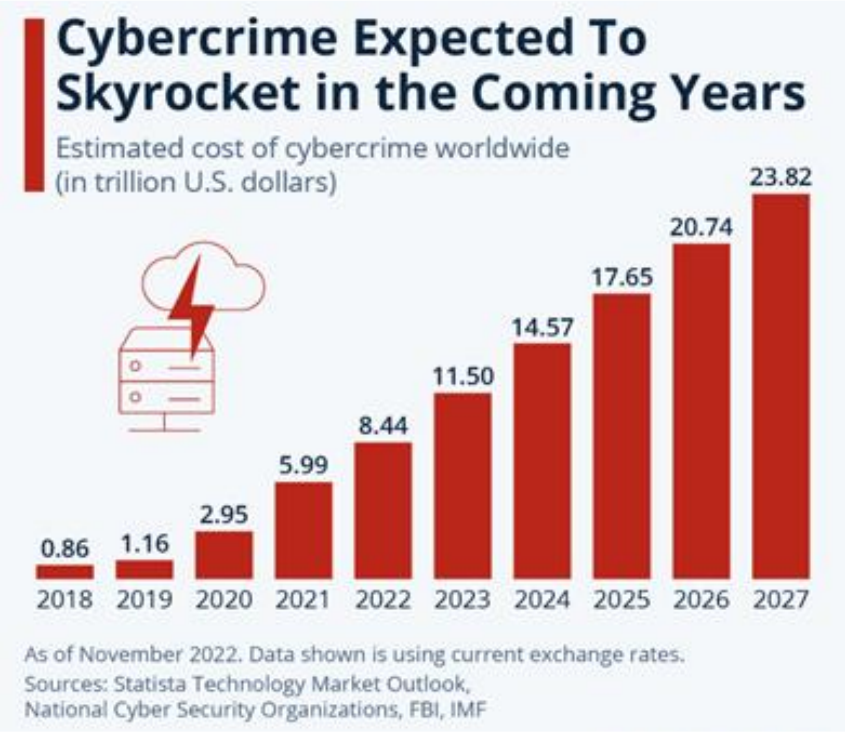
UPDATE ON THE CYBER DOMAIN

Issue 1/24 (January)

In Review: Cybersecurity Trends and Challenges in 2023

INTRODUCTION

1. 2023 has been a challenging and dynamic year for the cybersecurity industry, as new threats emerged following the increasing proliferation and normalisation of cloud technologies and Artificial Intelligence (AI). Experts estimate that global cyberattacks spiked by 40-45% from 2022 to 2023. The threat landscape is expected to expand further with the growing connectivity of devices and systems in this era of 5G and the Internet of Things (IoT).

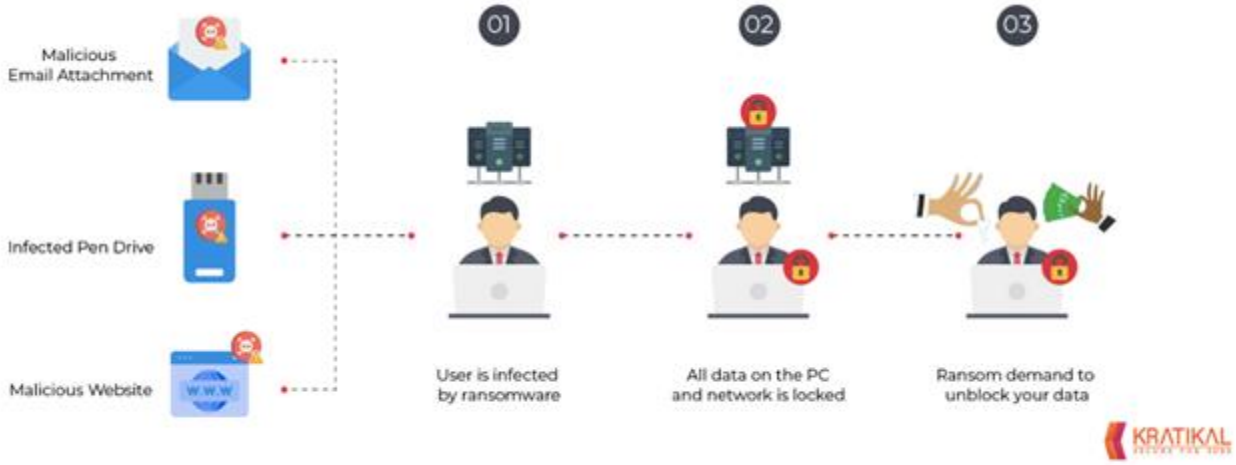


Trends in Global Cybercrime Costs (Source: Statista)

2. There are five key trends and challenges that shaped the cybersecurity landscape in 2023. These trends underscore the adaptability and resilience of threat actors in exploiting vulnerabilities for disruption and financial gain – serving as a reminder to all that a culture of perpetual vigilance and cyber resilience is necessary in a world of ever-evolving cyber threats.

ONE: INCREASED INTENSITY AND SCALE OF RANSOMWARE ATTACKS

3. **Increased Intensity of Ransomware Attacks**: Ransomware is a type of malware designed to lock and encrypt a victim's data, rendering them inaccessible and unusable by legitimate users. In doing so, attackers would demand a ransom for the recovery of access to users' data and systems. In 2023, there was an alarming increase in both the frequency and severity of ransomware attacks, with Corvus Insurance reporting a 95% year-on-year increase in ransomware attacks.

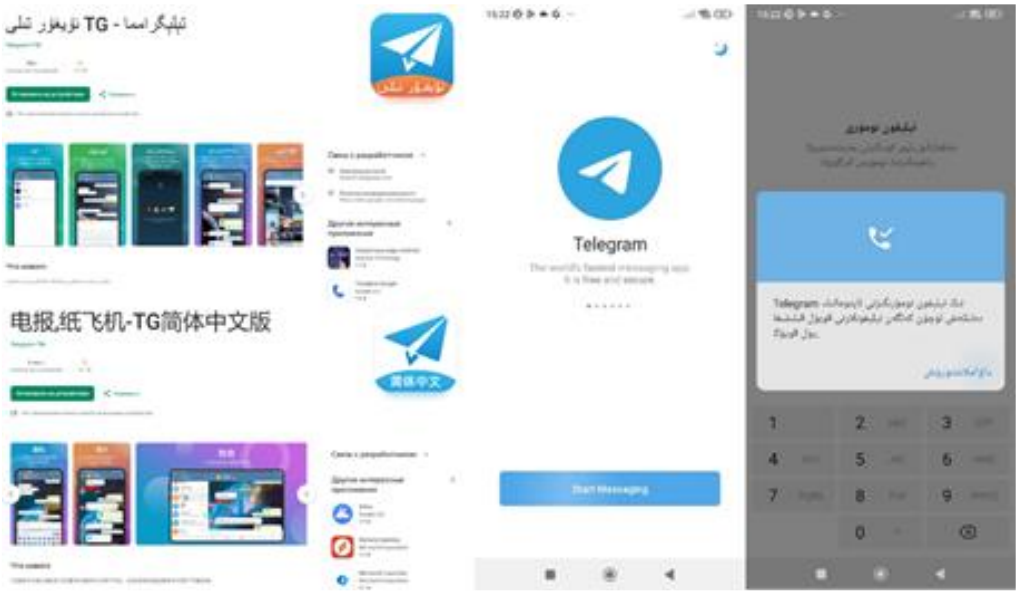


How Ransomware Works (Source: Kratikal)

4. **Adaptive Tactics**: Malicious actors have adapted their modus operandi to make ransom attacks more effective. First, attackers now increasingly target victims' backups, to prevent organisations from restoring their data and negating the need to pay a ransom. Veeam's 2023 *Ransomware Trends Report* found that 93% of ransomware attacks in 2023 specifically targeted backup data. Second, many ransomware attacks incorporate data theft alongside data encryption. Such attacks – also known as double extortion attacks – cannot be fixed using backups. This makes them a greater threat to businesses, as they exert more pressure on organisations to pay ransoms, rather than risk a data-leak. Proactive ransomware defence is therefore even more necessary, with regular security patching and enhanced user training necessary to guard against ransomware attacks.

TWO: MOBILE MALWARE DISGUISED AS INNOCUOUS APPLICATIONS

5. **Malware Disguised as Innocuous Applications**: Mobile malware which disguises itself as innocuous applications, such as QR code readers, flashlights, and games, have become common. However, the tactics employed to compromise users' mobile devices and gain access to private data has evolved beyond the creation of fake applications. Attackers now increase the distribution of cracked and customised versions of legitimate applications by exploiting the familiarity of well-known app names. Unsuspecting victims may be tricked into downloading a customised version of an official application that is designed to look legitimate from direct downloads or a third-party app store, resulting in malicious code being installed unknowingly. For example, trojanised Telegram mods were discovered on the Google Play Store in 2023, which looked and worked the same as the ordinary app, but contained code which gave backend unauthorised access to the user's contacts and messages.

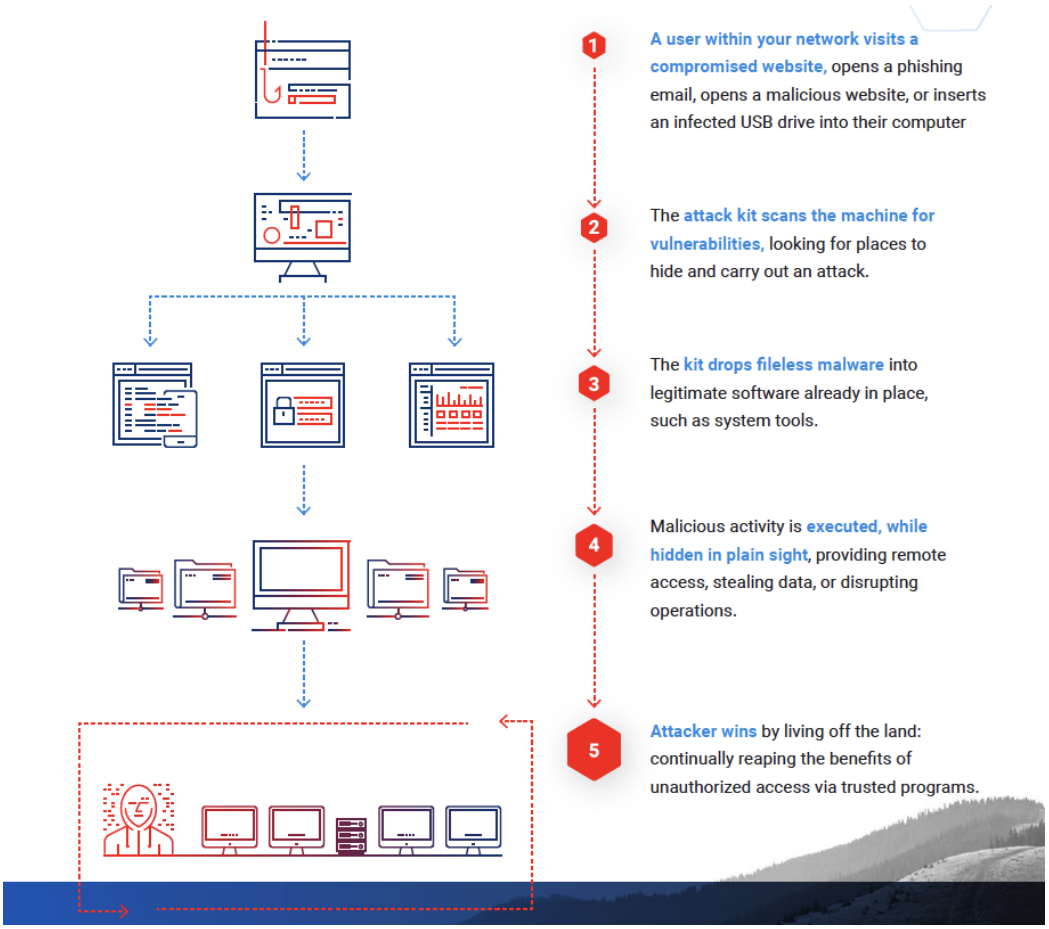


Google Play Store listings and user interfaces of trojanised Telegram apps (Source: SecureList)

6. **Danger of Mobile Malware**: Despite the growing threat of mobile malware, individuals remain less conscientious in protecting their mobile devices as compared to their computers. Surveys by McAfee and security.org show that only 50% of individuals have installed anti-virus solutions on their mobile devices, as compared to 80% doing so on their computers. As more businesses and organisations allow employees to access corporate networks with their personal mobile devices, the increased prevalence of mobile malware has the potential to lead to large-scale data loss through this less-protected access point. Hence, it is imperative that good cyber hygiene practices such as downloading applications from trusted sources and regular software and mobile updates are adhered to.

THREE: EXPLOITATION OF LEGITIMATE TOOLS

7. **Living Off The Land (LOTL) Attacks**: In LOTL attacks, attackers use legitimate and widely-available tools already in the victim's environment to gain unauthorised access to systems and networks. The use of such tools, like remote access software, system patching infrastructure, and system administration tools, allow attackers to operate discreetly as such software is already included in default whitelists and no malicious artefacts are written to hard drives. Such fileless attacks leave fewer traces and are able to bypass signature-based antivirus programmes, thereby increasing the chance of penetration and success. An example of such a fileless attack is the Stuxnet computer worm, which exploited legitimate software from Microsoft Windows and Siemens to carry out its malicious activities. The complex nature of LOTL attacks meant that they were once a technique employed exclusively by sophisticated actors. However, this has now evolved into a widely-used technique in the modern day, with Crowdstrike's *Global Threat Report* noting that 62% of threat actors leveraged legitimate built-in tools to conduct their cyberattacks.

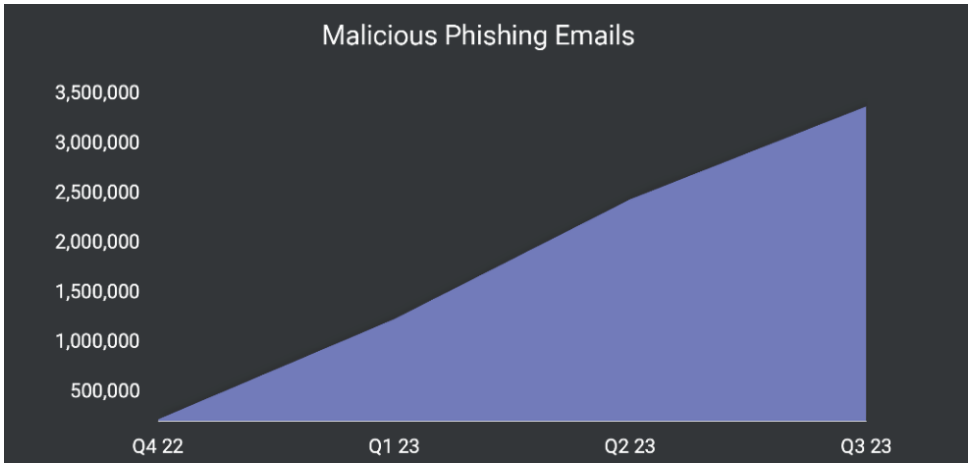


How a 'Living Off The Land' attack works. (Source: IronNet)

8. **Comprehensive Cybersecurity Approach Needed**: The increasing prevalence and sophistication of LOTL attacks means that more comprehensive cybersecurity solutions need to be put in place to prevent such attacks. Hence, organisations should implement more advanced endpoint protection programmes that leverage upon machine learning and behavioural analysis, in place of traditional signature-based detection mechanisms to detect and prevent such attacks.

FOUR: SURGE IN PHISHING ATTACKS DUE TO AI TOOLS

9. **Escalation of Social Engineering Attacks**: Social engineering attacks like phishing have undergone a significant evolution in 2023. Cybercriminals have increasingly embraced AI and spoofing methodologies to create persuasive and personalised phishing endeavours. Cybersecurity firm SlashNext reported that since the launch of ChatGPT in Q4 2022, there has been a 1,265% increase in malicious phishing emails, with a 967% rise in credential phishing in particular. ChatGPT's ability to draft highly authentic texts with adaptable writing styles and language patterns makes it possible for cybercriminals to impersonate an individual in a highly realistic manner, allowing for instances of phishing to be created faster, more authentically, and at a significantly increased scale.



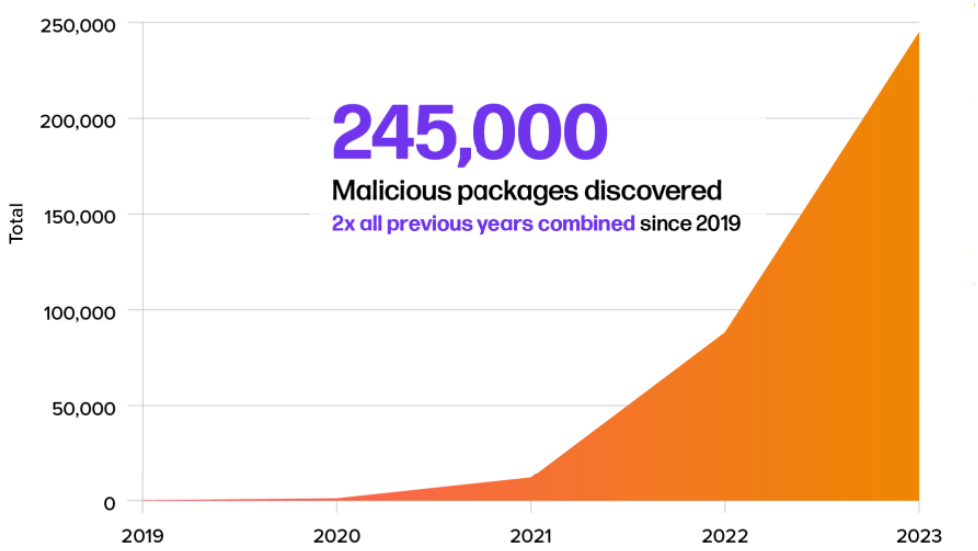
Spike in malicious phishing emails (Source: SlashNext)

10. **Phishing-as-a-Service (PhaaS)**: The increased ease of scaling and executing phishing attacks has led to the emergence of PhaaS. PhaaS allows individuals to hire cybercriminals to launch a phishing campaign for as low as USD$15 per day. This amplifies the intricacy and reach of potential social engineering attacks, presenting a significant hurdle for organisations fortifying the security of their digital resources and data. With the capabilities of generative AI models used in phishing expected to improve over time, it is expected that the phishing modus operandi and the scale of PhaaS campaigns will continue to evolve and surpass existing safeguards.

FIVE: SURGE IN SOFTWARE SUPPLY CHAIN ATTACKS

11. **Software Supply Chains**: The software applications used by organisations are not built from code that is entirely proprietary and custom. Instead, external components such as open-source code from third-party sources are often used, with up to 90% of code used in proprietary software from open-source origins. The software supply chain hence refers to the chain of code, tools, people, and processes involved in the development of software. Organisations inherit the software supply chain of all parts of their software, with the large, complex, and interconnected system of infrastructure, people and technology presenting multiple attack points.

12. **Surge in Software Supply Chain Attacks**: 2023 witnessed an unprecedented surge in software supply chain attacks, with Sonatype's annual *State of the Software Supply Chain* report recording twice as many attacks in 2023 as the cumulative total from 2019 to 2022. This increase can be attributed to a decline in the standards of open-source maintenance – with 18.6% of open-source projects failing to be maintained in the last year. This reduces the chances of software vulnerabilities being discovered and patched, creating security gaps for attackers to exploit and gain unauthorised access to systems and supply chains.



Exponential rise in number of malicious packages in 2023 (Source: SonaType)

13. **MOVEit Compromised**: In 2023, MOVEit, a software company used by thousands of organisations worldwide to transfer sensitive data over the internet, was compromised. While Zellis (the original user of the MOVEit software) confirmed the data breach in June 2023, the size of its software supply chain resulted in downstream delays between the vulnerability being exploited and their customers finding out. The breach was therefore able to spread, and affect companies such as the BBC, British Airways, and Boots. This exposed the personal information of more than 60 million individuals, with the estimated cost to businesses totalling over USD$9 billion to date, resulting in the largest supply chain attack in recent history.

WAY AHEAD

14. As we review the tumultuous cyber terrain of 2023, organisations must converge on a unified strategy for resilience. Organisations should cultivate a culture of perpetual vigilance, recognising that cyber threats are multifaceted and ever-evolving. This entails continuous monitoring, threat intelligence integration, and taking a proactive stance against emerging risks. As organisations fortify their cyber resilience, they not only safeguard their digital assets, but also contribute to the collective defence against the evolving landscape of cyber threats.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

References

1. Reflecting on the Evolution of Cybersecurity in 2023 - Forbes [Link: https://www.forbes.com/sites/emilsayegh/2023/12/12/reflecting-on-the-evolution-of-cybersecurity-in-2023/]

2. Cybersecurity Trends & Statistics: More Sophisticated and Persistent Threats So Far in 2023 - Forbes [Link: https://www.forbes.com/sites/chuckbrooks/2023/05/05/cybersecurity-trends--statistics-more-sophisticated-and-persistent-threats-so-far-in-2023/]

3. Ransomware Trends Report 2023 - Veeam [Link: https://www.veeam.com/ransomware-trends-report-2023]

4. Q3 Ransomware Report - Corvus Insurance [Link: https://www.corvusinsurance.com/blog/q3-ransomware-report]

5. BianLian Ransomware Pivots Encryption, Pure Data Theft, Extortion - Dark Reading [Link: https://www.darkreading.com/cyber-risk/bianlian-ransomware-pivots-encryption-pure-data-theft-extortion]

6. IT Threat Evolution Q3 2023: Mobile Statistics - Securelist [Link: https://securelist.com/it-threat-evolution-q3-2023-mobile-statistics/]

7. Trojanized Telegram Mod Attacking Chinese Users - Securelist [Link: https://securelist.com/trojanized-telegram-mod-attacking-chinese-users/]

8. The Rise of Mobile Malware - CSA Singapore [Link: https://www.csa.gov.sg/Tips-Resource/publications/cybersense/2023/the-rise-of-mobile-malware]

9. What are Living Off the Land Attacks - IronNet [Link: https://www.ironnet.com/blog/what-are-living-off-the-land-attacks]

10. Cybersecurity Advisories - CISA [Link: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a]

11. 5 Facts About Vice Society: The Ransomware Group Wreaking Havoc on K-12 Schools - Malwarebytes [Link: https://www.malwarebytes.com/blog/business/2023/01/5-facts-about-vice-society-the-ransomware-group-wreaking-havoc-on-k-12-schools]

12. State of Phishing 2023 - SlashNext [Link: https://slashnext.com/state-of-phishing-2023/]

13. Threat Landscape 2023 - ENISA [Link: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023]

14. State of the Software Supply Chain - Sonatype [Link: https://www.sonatype.com/state-of-the-software-supply-chain/]

15. Why Open Source Software Supply Chain Attacks Have Tripled in a Year - CSO Online [Link: https://www.csoonline.com/article/654560/why-open-source-software-supply-chain-attacks-have-tripled-in-a-year.html]