nexagate

2023

CYBER THREAT INTELLIGENCE

Document Reference:
NEXA-MS-CTI-Q1-2023-v1.0

Published Date:
22nd May 2023

nexagate

TABLE OF CONTENTS

FOREWORD

At Nexagate, we understand that the threat landscape in the realm of cybersecurity is constantly evolving. As we enter Quarter 1 of 2023, we find ourselves facing new and complex challenges that demand our unwavering attention and proactive response. It is with great pleasure that we present this Threat Report, which provides a comprehensive overview of the emerging threats and trends that have defined the cybersecurity landscape in recent months.

In an era where technology permeates every aspect of our lives, the risk of cyberattacks has never been greater. Malicious actors continue to exploit vulnerabilities, targeting organizations of all sizes and sectors. It is within this context that we witness the rise of ransomware attacks, insider threats, and the ever-present vulnerabilities in popular software platforms.

This report aims to shed light on the evolving tactics employed by threat actors and the impact they have on businesses and individuals alike. We delve into the tactics, techniques, and procedures utilized by these adversaries, emphasizing the importance of proactive defense strategies and effective incident response protocols.

Nexagate has had the privilege of collaborating with industry experts and conducting in-depth research to compile this report. We have analyzed real-world incidents, observed emerging patterns, and identified best practices that can empower organizations to enhance their cybersecurity posture.

We are proud to share the valuable insights contained within this report, as we believe that knowledge is the key to effective cybersecurity. By understanding the evolving threat landscape and adopting proactive measures, organizations can mitigate risks, protect their sensitive data, and ensure business continuity.

As we navigate the ever-changing cyber landscape together, we are reminded of the importance of collaboration, knowledge sharing, and continuous improvement. It is our collective responsibility to remain vigilant, resilient, and adaptive to the challenges that lie ahead.

We extend our sincere gratitude to all the cybersecurity professionals, researchers, and organizations dedicated to combating cyber threats. Your relentless efforts contribute to a safer digital ecosystem, inspiring us to continue our mission of providing innovative cybersecurity solutions.

We hope that this Threat Report serves as a valuable resource, empowering you to make informed decisions, fortify your defenses, and stay ahead of cyber adversaries. Together, we can create a safer and more secure digital future.

EXECUTIVE SUMMARY

This report provides an overview of the Quarter 1 Threat Report for the year 2023, with a specific focus on evolving malware and ransomware. The report analyzes the emerging cybersecurity threats, vulnerabilities, and trends observed during the first three months of the year. The insights aim to assist organizations in understanding the evolving threat landscape and taking proactive measures to mitigate risks, particularly with regards to the latest malware trends.

Sophisticated Malware Strains

In Quarter 1 of 2023, Nexagate witnessed a surge in the development and deployment of sophisticated malware strains. Adversaries continue to evolve their tactics, techniques, and procedures (TTPs) to bypass traditional security defenses and evade detection. Advanced malware strains leverage complex obfuscation techniques, polymorphic code, and zero-day exploits to infect systems and compromise sensitive data. Organizations need to deploy advanced threat detection and response mechanisms to effectively counter these evolving malware strains.

Fileless Malware

Fileless malware attacks have become increasingly prevalent during Quarter 1 of 2023. This type of malware operates in memory, leveraging legitimate system tools and processes to carry out malicious activities. Fileless malware poses significant challenges for traditional signature-based antivirus solutions, as it leaves little to no trace on the file system. Implementing behavior-based detection techniques, application whitelisting, and regular patching of vulnerable applications are crucial in mitigating the risks associated with fileless malware attacks.

Emotet Malware Resurfaces

Emotet, one of the most notorious malware strains, has re-emerged in the first quarter of 2023. Emotet is banking trojan that steals sensitive financial information and spreads through phishing emails. The new version of Emotet has improved evasion techniques and is now harder to detect and remove. Organizations should implement advanced email filtering and endpoint protection solutions to detect and block Emotet malware and its associated threats.

EXECUTIVE SUMMARY

Mobile Malware Is Becoming More Advanced

Mobile devices remain a prime target for cybercriminals, and Quarter 1 saw a rise in mobile malware attacks. Malicious applications, infected app stores, and social engineering techniques are used to distribute mobile malware, compromising user privacy, harvesting sensitive data, and delivering additional payloads. To combat mobile malware threats, organizations should promote mobile security best practices among employees, including regular updates, installing apps from trusted sources, and utilizing mobile security solutions.

Ransomware-as-a-Service (RaaS)

The first quarter of 2023 witnessed an increase in the availability and utilization of Ransomware-as-a-Service (RaaS) platforms. RaaS allows less technically skilled individuals to initiate ransomware attacks by providing them with pre-built malware, payment infrastructure, and support. This development expands the proof of potential threat actors, leading to a surge in ransomware attacks. Organizations should focus on strengthening their overall security posture, including regular data backups, network segmentation, and incident response planning, to mitigate the risks associated with RaaS.

Malware Targeting Industrial Control System (ICS)

During Quarter 1, there was a notable increase in malware targeting Industrial Control System (ICS). These systems, used in critical infrastructure sectors such as energy, water, and manufacturing, are vulnerable to malware attacks that can disrupt operations, cause physical damage, and endanger public safety. Securing ICS requires a combination of network segmentation, access controls, regular patching, and continuous monitoring to identify and mitigate potential threats.

AI-Driven Malware

The utilization of artificial intelligence (AI) in developing and deploying malware is an emerging trend observed in Quarter 1. Adversaries are leveraging AI techniques to automate tasks, evade detection, and launch highly targeted attacks. AI-driven malware can adapt and learn from the environment, making it challenging to detect using traditional security solutions. Organizations need to enhance their security capabilities with AI-driven threat detection and response technologies to effectively combat this evolving threat.

Q1 2023 THREAT TIMELINE

January 10, 2023 – The Evolving Tactic of Vidar Stealer
Researchers discover a new tactic being used by the Vidar Stealer malware, which is capable of bypassing security measures by using legitimate Windows processes to execute its malicious code. The new tactic increases the malware's chances of avoiding detection by security software.

January 20, 2023 – Emotet Returns with New Methods of Evasion
The Emotet malware returns with new evasion techniques, including the use of encrypted macro-enabled documents and polymorphic code. The new methods make it more difficult for security software to detect and block the malware.

February 5, 2023 – New Medusa Botnet Emerging via Mirai Botnet
A new botnet named Medusa is discovered, which is using the Mirai botnet as a delivery mechanism. The Medusa botnet is capable of launching DDoS attacks and spreading malware and is actively recruiting new bots.

February 18, 2023 – New Frebniis Malware
A new malware strain called Frebniis is discovered, which is capable of stealing sensitive data from infected systems. The malware is spread through phishing emails and uses a range of evasion techniques to avoid detection.

March 2, 2023 – PlugX Malware Being Distributed via Vulnerability Exploitation
The PlugX malware is being distributed via the exploitation of a vulnerability in widely-used software. The malware is capable of giving attackers full control of infected systems and is being used in targeted attacks against high-value targets.

March 18, 2023 – Uncovering HinataBot
A new botnet named HinataBot is uncovered, which is capable of launching DDoS attacks and spreading malware. The botnet is unique in that it uses a combination of peer-to-peer (P2P) and centralize command and control (C&C) mechanism to coordinate its activities.

March 18, 2023 – Uncovering HinataBot
A new botnet named HinataBot is uncovered, which is capable of launching DDoS attacks and spreading malware. The botnet is unique in that it uses a combination of peer-to-peer (P2P) and centralize command and control (C&C) mechanism to coordinate its activities.

These incidents demonstrate the ongoing evolution and sophistication of cyber threats during Quarter 1 of 2023. Organizations need to stay vigilant and implement robust security measures to protect against these threats and mitigate the risks they pose.

THE CYBER THREAT LANDSCAPE

The threat landscape of cyberattacks is an ever-present and evolving challenge that can have severe consequences for both businesses and individuals. Among the most pressing concerns are ransomware attacks, which have grown in prevalence and intensity, posing significant threats to cybersecurity professionals. Despite concerted efforts to bolster cybersecurity measures, attacks continue unabated, necessitating proactive steps by organizations to safeguard their assets.

When a business falls victim to a cyberattack, the financial toll can be staggering. The impact extends beyond monetary losses, as operations are disrupted, resulting in delays, decreased productivity, and potential revenue loss. Moreover, the aftermath of an attack can be even more detrimental, with potential reputational damage, erosion of customer trust, and even legal ramifications.

However, the ramifications of cyberattacks extend beyond monetary consequences. The relentless pressure and burden placed on cybersecurity professionals to safeguard against, detect, and respond to attacks can exact a toll on their well-being. The escalating frequency and intensity of attacks compound these challenges, leading to heightened stress levels, burnout, and compromised mental health. This underscores the urgent need to address the well-being and resilience of cybersecurity professionals who face an unrelenting barrage of threats, disruptions, and pressure.

With the rise of ransomware and insider threats incidents, organizations are starkly reminded of the significant risks that cyberattacks pose to their operations and the individuals involved. The far-reaching and devastating impacts of these attacks necessitate investments in the necessary resources, support systems, and technologies to effectively manage and mitigate these risks. Such proactive measures are critical for businesses to remain resilient, adaptable, and successful in the face of the persistent and ever-evolving challenges presented by the cybersecurity landscape. By prioritizing comprehensive cybersecurity strategies, organizations can better protect themselves, their stakeholders, and their future success.

RANSOMWARE REVOLUTION:
EVOLVING TACTICS AND TARGETS

Potential Impact: High

Action: Awareness

The threat of ransomware has entered a new era, with cybercriminals continuously adapting their tactics to exploit vulnerabilities in the digital realm. As organizations across sectors face this global menace, ransomware groups are deploying sophisticated schemes and disguising breaches, challenging cybersecurity professionals to keep pace with the evolving cyber threats.

One notable example is the rebranding and restructuring of LockBit, a prominent Ransomware as a Service (RaaS) group, seeking to shed its negative reputation. To incentivize hacking attempts, LockBit has introduced a groundbreaking bug bounty program, offering rewards of up to $1 million for exploitable vulnerabilities. Additionally, they have implemented an affiliation program, granting affiliates 20% of the ransom proceeds. Notably, LockBit's affiliates predominantly operate in Southeast Asia, with a particular focus on countries like Malaysia. This strategic targeting aligns with the fact that most LockBit developers were born and raised in the Soviet Union, leading to a self-imposed prohibition on attacking post-Soviet nations.

Furthermore, other ransomware groups, such as ALPVH/BlackCat and Hive, are adapting their techniques by leveraging Rust, a powerful cross-platform programming language. Rust's flexibility and customization options make it an effective tool for targeting Linux systems, presenting an emerging threat to organizations relying on this operating system. By leveraging programming languages like Rust and Go, these groups exploit features such as code security and concurrent programming, expanding their range of potential targets. The growing adoption of Rust is already evident, with Trend Micro Research reporting that Linux was the second most targeted operating system for malware detections last year, following Windows.

Recommendation

The ransomware revolution marks a significant shift in the cyber threat, as cybercriminals continually evolve their tactics and target new vulnerabilities. Organizations must remain vigilant, updating their cybersecurity measures to address these emerging threats. Effective defenses require robust strategies, proactive threat intelligence, and enhanced collaboration between cybersecurity professionals to counter the ever-growing sophistication of ransomware attacks. By staying ahead of the curve, organizations can bolster their resilience and protect against the devastating consequences of this evolving cyber threat.

INSIDER THREATS: UNVEILING THE HIDDEN DANGER

Potential Impact: High

Action: Awareness and apply remote control access

Insider threats pose a significant security risk to companies and organizations, yet they often remain overlooked despite their potential for substantial damages. These threats involve individuals with authorized access exploiting their knowledge or position to harm the organization, either for personal gain or other motivations. Recent cases at Nexagate highlight the real-world impact of insider threats, emphasizing the need for heightened awareness and preventive measures.

Shocking statistics reveal the magnitude of the insider threat problem. Over 70% of such incidents go unreported, resulting in millions of dollars in damages per occurrence. This alarming trend necessitates immediate action to address the vulnerabilities and risks posed by insiders.

GURUCUL's 2023 Insider Threat Report provides valuable insights into the evolving insider threat landscape. The survey, which included responses from 326 cybersecurity professionals, uncovers the latest trends and challenges faced by organizations in combating this growing menace:

- Increased Frequency: A staggering 74% of organizations reported a rise in the frequency of insider attacks.
- Vulnerability Assessment: An alarming 74% of organizations rated themselves as at least moderately vulnerable or worse to insider threats.
- Occurrence Rates: More than half of the organizations surveyed experienced at least one insider threat incident in the past year, with striking 8% encountering over 20 incidents.
- Cloud challenges: The report also reveals that 53% of organizations find detecting insider

Real-World Cases

One recent incident at Nexagate involved an employee who misused their authorized access to the company's Google Drive. Coordinated with unauthorized access from an unknown user, the employee created a new Google account to gain access to sensitive data, leading to potential data theft and subsequent negative impacts on the company's processes and reputation.

Recommendation

The prevalence and potential consequences of insider threats demand immediate attention and proactive measures. Organizations must acknowledge the gravity of this risk and invest in comprehensive security strategies to detect, prevent, and mitigate insider threats effectively. Strengthening cybersecurity awareness, implementing robust access controls, and fostering a culture of reporting suspicions are essential steps in combating this hidden menace. By addressing insider threats head-on, organizations can safeguard their assets, reputation, and overall business continuity in today's complex threat landscape.

MICROSOFT VULNERABILITIES: A PRIME TARGET FOR THREAT ACTORS

Potential Impact: High

Action: Update latest windows patch

Microsoft has faced significant challenges in recent years due to vulnerabilities and cyberattacks on their products, making them an attractive target for threat actors. The exploitation of these vulnerabilities has had a significant impact on the cybersecurity landscape, prompting Microsoft to take measures to address them. Understanding the evolving threat landscape surrounding Microsoft vulnerabilities is crucial to mitigating potential risks.

Microsoft has made significant strides in bolstering security by blocking the use of macros, a widely exploited initial access vector for cyberattacks. Malicious macros embedded within emails posed a significant risk, as unsuspecting recipients could inadvertently trigger them, leading to potential security breaches.

In January 2023, EclecticIQ analysts investigated the use of QakBot malware, which exploited unpatched vulnerabilities in Microsoft's Windows OS security features. QakBot, primarily known as a banking Trojan, was utilized by threat actors to steal credit card information from victim devices. Notable vulnerabilities, including CVE-2021-34473 and CVE-2021-34523, allowed threat actors to deploy cryptocurrency miners using the Microsoft Exchange ProxyShell, enabling them to profit from Windows domains.

Microsoft's March 2023 Patch update aimed to address 80 security flaws, with eight rated as critical, 71 as important, and one as moderate. Two of these vulnerabilities, CVE-2023-23397 and CVE-2023-24880, were actively exploited in the wild. The former was a privilege escalation flaw in Microsoft Outlook, while the latter was a security bypass flaw in Windows SmartScreen. Exploiting the latter flaw enabled the distribution of the Magniber ransomware, with over 100,000 downloads associated with European users. Additionally, the patch addressed other vulnerabilities, such as remote code execution flaws and information disclosure vulnerabilities.

Recommendation

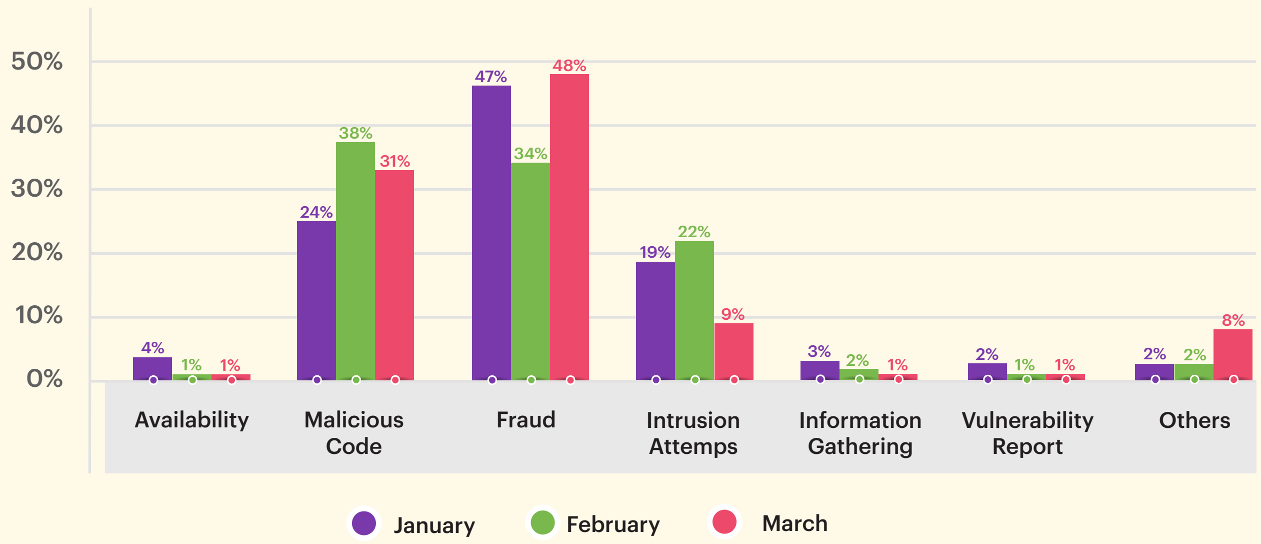
The ransomware revolution marks a significant shift in the cyber threat, as cybercriminals continually evolve their tactics and target new vulnerabilities. Organizations must remain vigilant, updating their cybersecurity measures to address these emerging threats. Effective defenses require robust strategies, proactive threat intelligence, and enhanced collaboration between cybersecurity professionals to counter the ever-growing sophistication of ransomware attacks. By staying ahead of the curve, organizations can bolster their resilience and protect against the devastating consequences of this evolving cyber threat.

TREND ANALYSIS & TOP THREATS

Reported Incidents based on General Incidents Classification Statistics for Quarter 1 of 2023

Nexagate Cybersecurity enabled clients to defend their network from threats of high severity (e.g., Denial of Service, intrusive activity, spam, vulnerabilities, malicious code, fraud) encountered in Quarter 1 of 2023. Data for these incidents were sourced through our pro-active monitoring, including referencing data from MyCert(3) as well as our client base within the country and abroad ranging from home users, private sectors, government sectors, industries, cyber security organizations from abroad, cyber threat intelligence, and special interest groups.

Reported Incidents Statistics for Q1 2023



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2023
and MyCERT Incident Statistics - Reported Incidents based on General Incident Classification Statistics for Quarter 1 of 2023.

The reported incidents in Q1 2023 were identified and harvested from various security appliances, intelligence and general incidents. These data are then associated across industry verticals to observed an overview in Malaysia. Fraud continues to be the most frequently reported incident, indicating its high prevalence in the country. This could be due to factors such as insufficient cybersecurity measures, limited awareness and education on cybersecurity, and increased reliance on digital technologies. Malicious code and Intrusion attempts remain as prevalent threat, indicating a huge market for spammers and hacktivist to capitalize on weak organizational defenses. Other threat captured includes, availability, information gathering, vulnerabilities report and other.

[3] https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&amp;id=96c526d0-67e6-4f8e-91c8-006230405ece

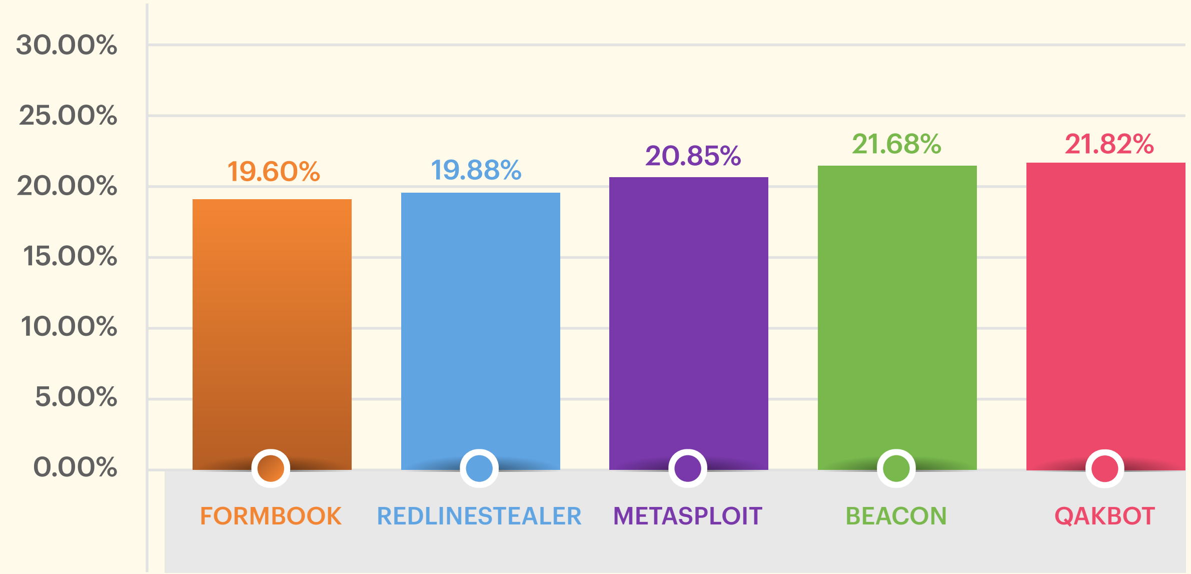
TREND ANALYSIS & TOP THREATS

Top 5 Active Malwares

Malware campaign remains a prevalent threat throughout the year. We observed leading pack for active malware for Q1 2023 was QakBot, a backdoor written in C/C++ that implements a plug-in framework to extend its capabilities via embedded and downloaded plugins. QakBot communicates using HTTP, HTTPS, or a custom binary protocol over TCP. QakBot's capabilities also include keylogging, file transfer, file execution, and process termination. QakBot also targets credentials by intercepting browser activity, injecting malicious code into browser sessions, and extracting credentials stored by browsers, email clients, and FTP clients.

As we witnessed in majority of high-profile breaches, threat actors leverage third parties to reach their desired victims. As the list of cases continue to grows, organizations are encouraged to invest in comprehensive cybersecurity suite – in people, process and technology.

Most Active Malwares Q1 2023



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2023.

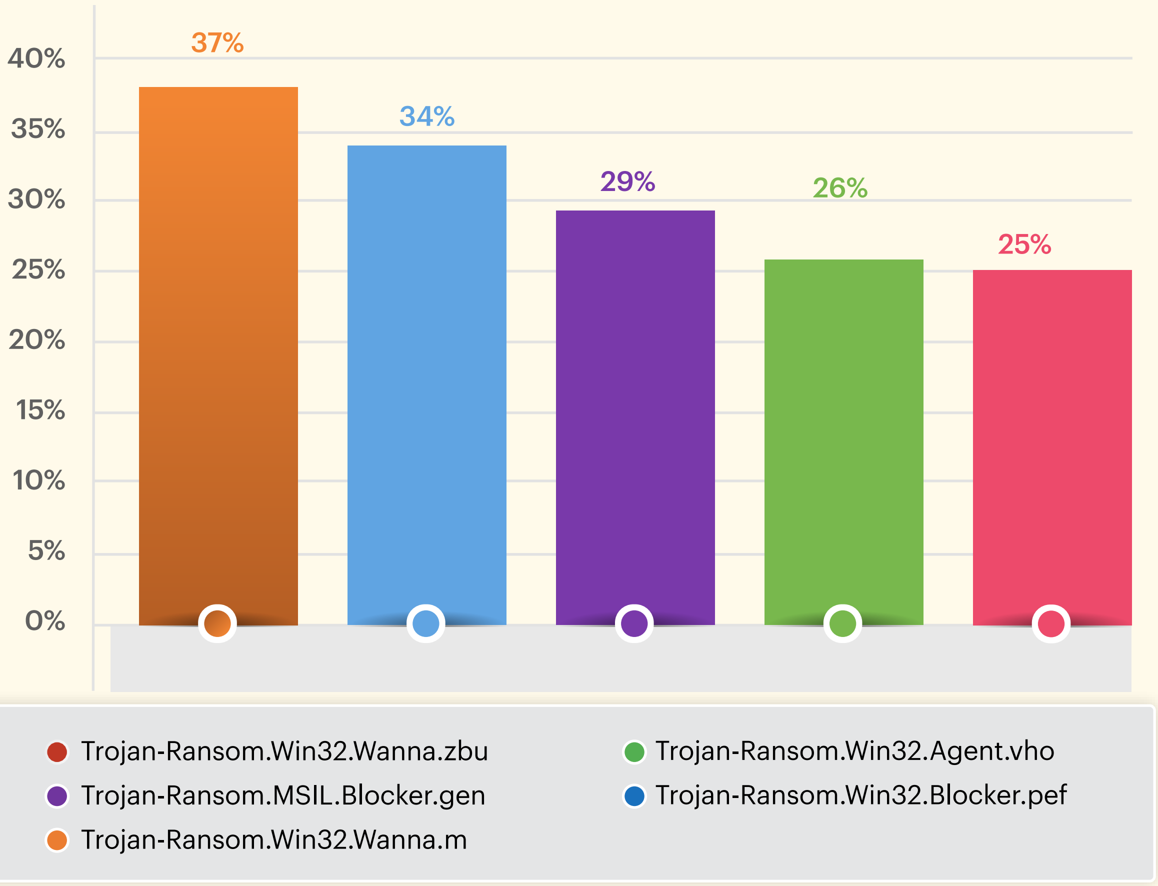
TREND ANALYSIS & TOP THREATS

Top 5 Active Ransomware

Ransomware campaign remains a prevalent threat throughout the year. As we can see, most of it was Trojan-Ransom and this type of Trojan modifies data on the victim computer so that the victim can no longer use the data, or it prevents the computer from running correctly. Once the data has been "taken hostage" (blocked or encrypted), the user will receive a ransom demand. The ransom demand tells the victim to send the malicious money; on receipt of this, the cyber criminal will send a program to the victim to restore the data or restore the computer's performance.

We observed leading pack for active ransomware for February 2023 was Trojan-Ransom.Win32.Wanna.m; this family consist of malware of the WannaCry type. This malware encrypts user files. It is distributed by exploiting a vulnerability of the SMB protocol.

Most Active Ransomware Q1 2023



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2023.

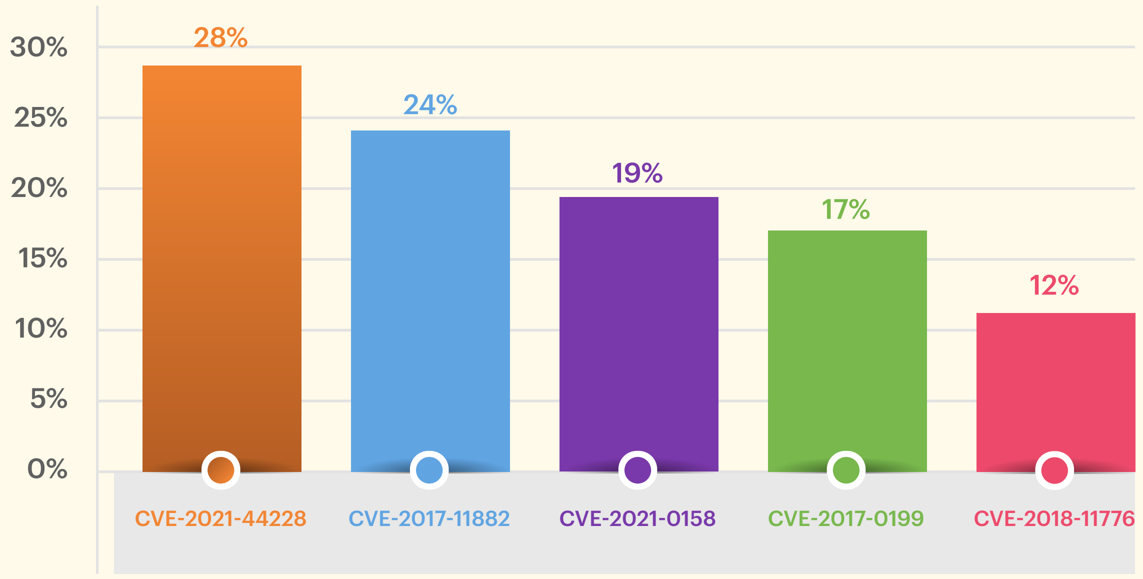
TREND ANALYSIS & TOP THREATS

Top 5 Active Vulnerabilities

In particular, the top 5 most active vulnerabilities for Q1 2023. Leading the pack for exploitation attempts for Quarter 1 2023 was CVE-2021-44228, a Log4j2 Remote Code Execution vulnerability, an input validation vulnerability exists within the Java Naming and Directory Interface (JNDI) features in Apache Log4j 2.14.1 and earlier that, when exploited, allow attacker to remotely execute arbitrary code. From log4j 2.15.0, this behavior has been disabled by default.

In order to protect from such threats, organization should proactively identify relevant threat. This can be done with threat hunting or setting up a team of threat intelligence analyst to monitor and keep malicious threats at bay.

Most Active Vulnerabilities Q1 2023



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2023.

BEST PRACTICES FOR DEFENDING AGAINST RANSOMWARE AND INSIDER THREATS

Ransomware

To protect against and detects ransomware attacks, our experts recommend user to:

1. **Regularly Backup Data:** Implement a robust data backup strategy that includes regular backups of critical data. Ensure backups are stored securely and are not accessible from the main network to prevent them from being compromised during an attack. Test the restoration process periodically to ensure backups are functional.
2. **Keep Systems and Software Updated:** Promptly apply security patches and updates for operating systems, software, and applications. Vulnerabilities in outdated software can be exploited by ransomware. Enable automatic updates whenever possible to ensure timely patching.
3. **Use Strong Passwords and Multi-Factor Authentication (MFA):** Enforce strong password policies that require complex, unique passwords for all accounts. Enable MFA wherever possible to add an extra layer of security. This makes it harder for attackers to gain unauthorized access to systems and accounts.
4. **Implement Security Awareness Training:** Educate employees about the risks of ransomware and the importance of cybersecurity hygiene. Train them to identify phishing emails, suspicious attachments, and malicious links. Encourage reporting of any suspicious activity or potential security incidents.
5. **Employ Email and Web Filtering:** Utilize email and web filtering solutions to block malicious attachments, links, and websites known for distributing malware. These filters can help prevent ransomware from entering the network through email or malicious websites.
6. **Use Endpoint Protection:** Deploy reputable antivirus and anti-malware software on all endpoints, including computers, laptops, and mobile devices. Configure regular scans and real-time protection to detect and block ransomware threats.
7. **Restrict User Privileges:** Limit user access privileges to the minimum required for their roles. Users should only have access to the data and systems necessary for their job functions. Implement the principle of least privilege to minimize the impact of a potential ransomware attack.

8. **Segment Network and Implement Firewalls:** Divide the network into segments and implement firewalls to restrict lateral movement of ransomware within the network. This helps contain the impact of an attack and prevents the rapid spread of ransomware.

9. **Monitor and Detect Anomalies:** Implement a robust security monitoring system q that can detect suspicious activities, such as unauthorized access attempts, unusual file modifications, or network traffic patterns. Establish alerts and auto mated responses to potential threats.

10. **Develop an Incident Response Plan:** Create an incident response plan that out lines the steps to be taken in the event of a ransomware attack. This plan should include actions such as isolating affected systems, notifying relevant stakehold ers, engaging with law enforcement, and restoring data from backups.

Remember that no single defense measure is foolproof against ransomware. A layered approach that combines multiple security measures is essential to effectively defend against these threats. Regularly reassess and update your security practices to stay ahead of evolving ransomware tactics and techniques.

Insider Threats

Here are some best practices to help organizations defend against insider threats:

1. **Implement Strong Access Controls:** Maintain strict control over user access privileges by following the principle of least privilege. Grant employees access only to the resources and information they need to perform their job responsibilities. Regularly review and revoke access rights for employees who change roles or leave the organization.

2. **Conduct Thorough Background Checks:** Perform comprehensive background checks and vetting processes for new hires, particularly for positions that involve handling sensitive data or have elevated privileges. This can help identify any red flags or potential risks early on.

3. **Establish Clear Security Policies and Procedures:** Develop and enforce robust security policies that clearly outline acceptable use of company resources, data handling guidelines, and expectations of employee behavior. Regularly communicate and educate employees on these policies to ensure understanding and compliance.

4. **Implement Employee Training and Awareness Programs:** Conduct regular training sessions and awareness programs to educate employees about the importance of data security, confidentiality, and the potential risks associated with insider threats. This includes identifying suspicious activities, reporting procedures, and maintaining a strong security culture.

5. **Monitor and Analyze User Behavior:** Implement monitoring solutions that can detect and analyze user behavior to identify anomalous or potentially malicious activities. This can involve monitoring access logs, network traffic, and behavior analytics to detect any unauthorized or unusual activities.

6. **Encourage Reporting and Whistleblowing:** Create a culture that encourages employees to report any suspicious behavior or potential insider threats without fear of retaliation. Establish clear reporting channels and provide assurances of anonymity and protection for whistleblowers.

7. **Regularly Review and Audit User Activity:** Conduct regular audits of user activity logs, system access, and data transfers to identify any unusual or unauthorized actions. This can help detect insider threats in real-time or during post-incident investigations.

8. **Implement Data Loss Prevention (DLP) Solutions:** Deploy DLP solutions that can monitor and control the movement of sensitive data within the organization. These solutions can help prevent unauthorized data exfiltration and detect potential insider threats attempting to access or leak sensitive information.

9. **Foster a Positive Work Environment:** Promote a positive work environment that encourages open communication, fairness, and transparency. Address employee grievances and concerns promptly to minimize the risk of disgruntled employees becoming insider threats.

10. **Regularly Evaluate and Improve Security Measures:** Continuously assess and enhance security measures to adapt to evolving threats and technologies. Stay updated on industry best practices, emerging insider threat trends, and leverage advanced technologies to strengthen your defense against insider threats.

Remember that insider threats can come from both intentional and unintentional actions. By implementing these best practices, organizations can better protect themselves against insider threats and minimize the potential damage caused by malicious insiders or inadvertent security breaches.

USE THREAT INTELLIGENCE TO PRIORITIZE YOUR SECURITY PROGRAMS

With organized cybercrime becoming more innovative and sophisticated, threat intelligence has become increasingly important to prioritize activities in cybersecurity programs. Threat intelligence is key to understanding what threats you must protect your organization from and how to mitigate them.

In the current threat landscape, it's no longer a question of if, but when you'll be the victim of a cyber breach. However, when you use threat intelligence as a strategic tool, you make your security investments smarter and force threat actors to renew their game.
To know how to prioritize which security countermeasures to implement, threat intelligence should be an element in all decisions relating to cybersecurity, from strategic planning to individual technical projects.

How We Help

Nexagate can provide the expertise and services needed to stop the attackers and minimize the impact of a cyber breach by identifying vulnerabilities and implementing solutions that close the doors on cybercriminals. We combine the knowledge and insight gained from managing the largest cyber incidents, tracking vulnerabilities and leaks on the dark web and continuously analyzing how attacks are evolving.

Covering the [entire cybersecurity spectrum]() gives us an in-depth understanding of current threats and how threat actors operate, as well as the unique skills necessary to identify the greatest threats to your organization.

NEXA SECURITY INTEL
UNIFIED CYBERSECURITY MANAGEMENT

CONTACT INFORMATION

☎ +603 2935 9363
✉ sales@nexagate.com
🌐 www.nexagate.com
📍 BO2-D-13A-1, Boutique Office 2, Menara 3
KL Eco City, Jalan Bangsar
59200 Kuala Lumpur, Malaysia

Follow Us: @nexagate