nexagate

2022

CYBER THREAT INTELLIGENCE

Document Reference:
NEXA-MS-CTI-2022-v1.0

Published Date:
12nd April 2023

nexagate

TABLE OF CONTENTS

Foreword 03-04

Executive Summary 05

Recommendations and Priorities for 2023 06

The Cyber Threat Landscape Overview 07-11

- Different Types of Attacks
- The Ransomware Ecosystems
- Who Are The Ransomware Victims?
- Cyber Espionage - The Silent Threat

Trend Analysis & Top Threats 12-14

- Reported Incidents based on General Incident Classification Statistics
- Top Active Malwares
- Top Active Vulnerabilities

Cyber Threats and How To Tackle Them 15-22

- Threat Actors Are Faster
- It's Too Easy to Get Full Control of a Network
- Increased Use of Vulnerability Exploit
- Securing Your Digital Accounts: Beyond Passwords
- Denial of Service Attacks Are Increasing

Outlook For 2023 23-24

How Do We Really Stop Cybercrime 25

Use Threat Intelligence to Prioritize Your Security Programs 26

FOREWORD

A Message From Our Founder

As the founder and managing director of Nexagate, it is my pleasure to present to you our latest Cyber Threat Intelligence report. In this report, we provide an in-depth analysis of the current state of global cybersecurity, including emerging threats, new attack vectors, and shifting trends.

At Nexagate, we understand the importance of staying ahead of potential cyber threats. That's why we have invested in a team of cybersecurity experts who are dedicated to researching and analyzing the latest threats and trends. In this report, we not only present our findings on global threats but also on customer threat trends that we have identified.

We believe that it is essential to share our knowledge with our clients and the broader community to empower organizations to protect their digital assets. With this report, we aim to provide valuable insights into the evolving threat landscape and the steps that organizations can take to mitigate their risks.

Our research has revealed some alarming trends, such as the increasing sophistication of cyber attacks and the growing use of social engineering tactics. However, it has also highlighted the importance of implementing effective cybersecurity measures and training programs to protect against these threats.

I would like to extend my gratitude to our team of cybersecurity experts who have worked tirelessly to produce this report. I am also grateful to our customers who have provided us with valuable insights into their specific cybersecurity challenges.

At Nexagate, we remain committed to providing innovative solutions and world-class support to our clients. We believe that this report will help us achieve that goal by providing valuable intelligence to help our clients stay ahead of the ever-evolving cyber threat landscape.

Thank you for choosing Nexagate as your cybersecurity partner. We hope that you find this Cyber Threat Intelligence report informative and useful.

Khairil Effendy
Managing Director
Nexagate Sdn Bhd

FOREWORD

Threat Intelligence can be considered "The Art of Taking The Adversary by Surprise". Anticipating, mitigating and preventing surprises in the form of cyberattacks is the primary mission of practical threat intelligence program.

Achieving that goal requires a proactive approach that answers critical questions like the following: Which threat actors are most likely to cause an impact in my organization? What are their motivations, goals and capabilities? How do they behave, and what cyber-weapon do they use to achieve those goals? And most importantly, what actionable countermeasures can I deploy to improve my organization's cyber defense capabilities?

Our team is proud to release our first Nexagate Threat Intelligence Report. The mission of this report is to provide our clients with actionable intelligence on targeted attacks, cybercrime-motivated threat actors, and campaigns targeting organizations like yours so that you can make well-informed decisions and take prompt effective actions.

In this first edition, you'll find reports from threat researcher and intelligence analyst on Nexagate Threat Intelligence team, an experts who understand not only technical threats but also local and global geopolitical developments and their impact on organizational threat models in each region. To produce this report, the team leveraged data and telemetry obtained from our Security Operations Center and analytical capabilities, complemented by other public and private intelligence sources.

I want to thank our Nexa Threat Intelligence team who made this report possible and continue to produce numerous "first-to-market" research report while continuously improving Nexagate Cybersecurity-as-a-Service.

Suziyanti Shahrudin
Chief of Managed Security
Nexagate Sdn Bhd

EXECUTIVE SUMMARY

This report is based on the premise that it should help you meet today's cybersecurity challenges, regardless of whether you are a business leader, an incident responder, an analyst in a security operation center, or a cybersecurity engineer trying to protect your customers.

Our suggested recommendations and priorities are based primarily on knowledge and insights acquired while responding to actual incidents, conducting forensic investigations post-attack with our Incident Response Team, and preventing and mitigating cyber breaches in our Security Operation Center. We have delved into each incident to fully understand the root causes, how the impact could have been minimized, and how the breaches could have been prevented.

The Ransomware Industry

Ransomware remains the top threat to medium and large corporations. Ransomware gangs only interest is to maximize profits. They continue to expand their operations and improve their business model. To increase their revenue, many ransomware gangs have become faster and increased their number of attacks. By using heavily scripted attacks reminiscent of assembly line operations, the major ransomware gangs can increase the number of victims by spending less time on each attack and recruiting less tech-savvy affiliates that need only follow instructions in ready-to-use frameworks.

The pervasiveness of ransomware and other cybercrime means that organizations should shift their mental models from just preventing breach to assuming breach. It has become a question of attrition; attackers will eventually find a vulnerable victim or system to exploit to achieve initial access. This has not by any means reduced the need for prevention; instead, it has made it necessary to adopt a holistic view of cybersecurity where prevention, detection, and response are all integral parts.

From Phishing to Vulnerability Exploitation

In 2022, exploitation of vulnerabilities in public-facing systems has, for the first time, overtaken phishing as the primary attack vector in ransomware attacks. This was likely due to the speed and ease with which cybercriminals can now leverage vulnerabilities.

There are also many tools that can quickly locate vulnerable systems on the internet. The exploits can then quickly be leveraged in mass attacks against the vulnerable systems before the affected organizations have had time to apply the patch. You should benchmark your vulnerability and patch management programs against the two-day rule. The rule states that once a patch is available for a publicly available system, it should be applied within two days for internet-facing applications and systems.

RECOMMENDATIONS AND PRIORITIES FOR 2023

Assume Breach Mentality

Begin by assuming breach to make the necessary transition from a prevention-only mindset to a more holistic one. While attackers need only find one vulnerability to enter your digital garden, conversely, with proper detection, it will also only require one misstep for them to be discovered. Early detection is key to minimizing the consequences of a breach.

Detection and Response Capability

Ensure you have a detection capability worth its name. This roughly translates into having capability that consists of functionality for detecting suspicious behavior, responding to threats, for example, by isolating clients and servers from the network, and a central console for administration and investigation. No matter what you read or hear, there are no products on the market that will function efficiently without supervision by human operators. Alarms and potential threats must be evaluated by someone who understands the context of the alert and can determine if a deeper investigation is necessary.

Public Attack Surface Hardening

While detection capabilities are essential, preventive measures are still very much needed. Many of the incidents during 2021 began with attackers exploiting known vulnerabilities in publicly facing systems and applications. Another prevalent vector is using valid credentials for remote services not requiring a second factor when authenticating users.

Towards a Zero-Trust Architecture

Given the assumption of breach, we need to make the crown jewels of our networks harder to reach and exploit. Don't use accounts with administrative privileges, except when necessary. Access to data and systems should leverage a tiered access and identity model that grants access based on roles, use cases, resources, and a combination thereof. Threat actors shouldn't be able to move swiftly across the infrastructure without roadblocks to stop them.

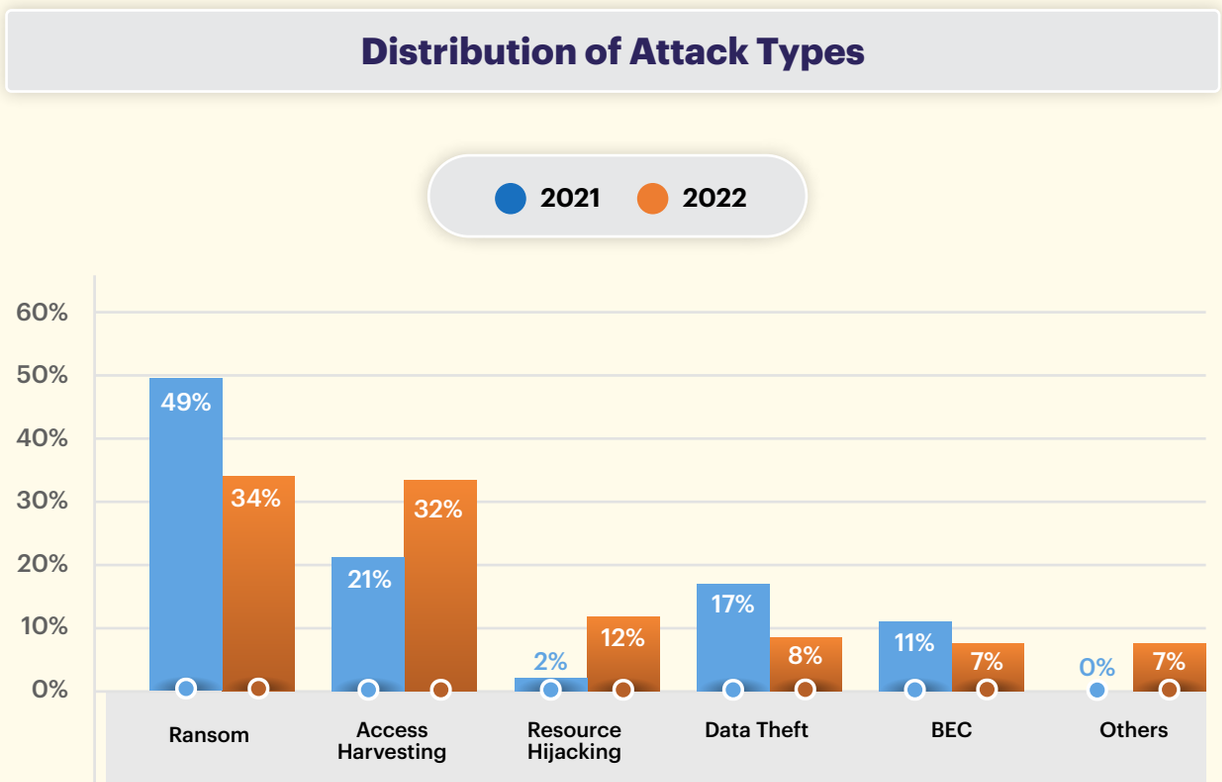
DIFFERENT TYPES OF ATTACKS

The total number of cyber incidents events that Nexagate handled during 2022 increased by 100% compared to 2021. This increase may partly be because we have continued strengthening our position in the Malaysian cybersecurity market as the top Cybersecurity-as-a-Service. However, it also represents a continued rise in overall cyber incidents in Malaysia.

The percentages of serious cyber incidents shown below should be viewed in the context of overall increase of attacks. Therefore, even if the observed percentage of ransom attacks has decreased, the actual number of attacks has increased significantly.

DIFFERENT TYPES OF ATTACKS

Ransom attacks consist mainly of ransomware attacks, but other forms of cyber extortion also fall under this category. Though not common, some cybercriminals only steal sensitive corporate data and use it as ransom without encrypting the environment. Another type of ransom attack that has increased in 2022 is distributed denial of service (DDoS) extortion. Threat actors direct DDoS attacks against corporations with significant internet presence and demand ransom in cryptocurrency to stop the attacks.



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2021 & 2022.

Access harvesting occurs when a threat actor obtains access to a network with the intent to sell the access to other cybercriminals for profit. There appears to be an overall increase in access harvesting that is matched by a decrease in full ransomware attacks. Most of these access harvesting attacks would likely have led to full ransomware encryption. The numbers consequently suggest that more ransomware attacks are stopped now than before. This aligns with other data that indicates that ransomware actors now appear to prioritize quantity over quality in their attacks.

Resource hijacking is malware that steals computing power, primarily to mine cryptocurrency. The increase in resource hijacking is likely due to the ban on cryptomining farms in countries like China, which has forced some, mainly Chinese, crypto mining actors to move into resource hijacking botnets (cryptojacking) to continue their business. There are, however, also Russian cryptomining botnets.

Business email compromise (BEC) is a form of cyber attack that relies exclusively on weaponizing access to corporate mailboxes to steal money. The attack usually begins with a phishing mail to steal credentials, followed by a login to the victim mailbox from the outside to add forwarding rules. The attacker then monitors the mail traffic, and once a promising exchange has been identified, the attacker hijacks the conversation and modifies the banking details to redirect the payments.

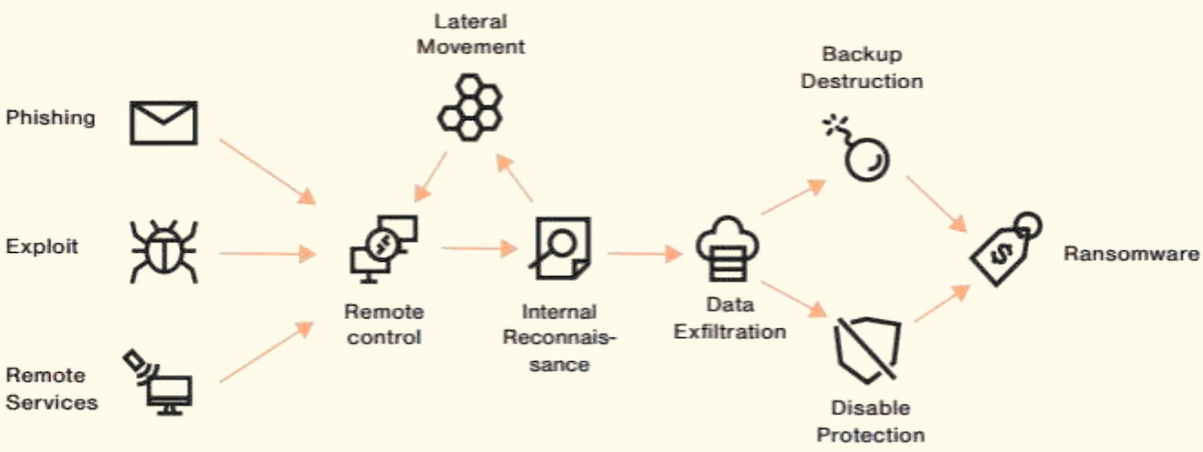
The Ransomware Ecosystem

Ransomware remains the top threat to medium and large corporations. In 2022, Nexagate found 26% more ransomware incidents than the previous year. We believe that this represents a continued rise in ransomware attacks in Malaysia. We also believe that currently, the gangs' inability to recruit enough talented hackers, rather than better defenses, is limiting their ability to expand their criminal enterprises further.

Ransomware gangs' only interest is to maximize profits. The major criminal groups prefer to hit large organizations that will quickly lose income if the IT environment cannot be rapidly restored. The ransom demanded by attackers is typically based on a percentage of the company turnover, and a large organization means a better payoff. At the same time, they are opportunistic and strike at smaller organizations when they find an easy target.

The cybercrime gangs also continue to expand their operations and improve their business model. In 2022, Nexagate observed how many groups experimented with new tactics to extort even more money from their victims. In addition to encrypting their victim's data, many groups now steal sensitive data and threaten to sell it or leak it publicly. Some groups also added DDoS attacks and threatening phone calls to their arsenal of threats to force victims to pay the ransom.

The figure below illustrates a general overview of all steps in a ransomware attack, from initial access to full encryption:

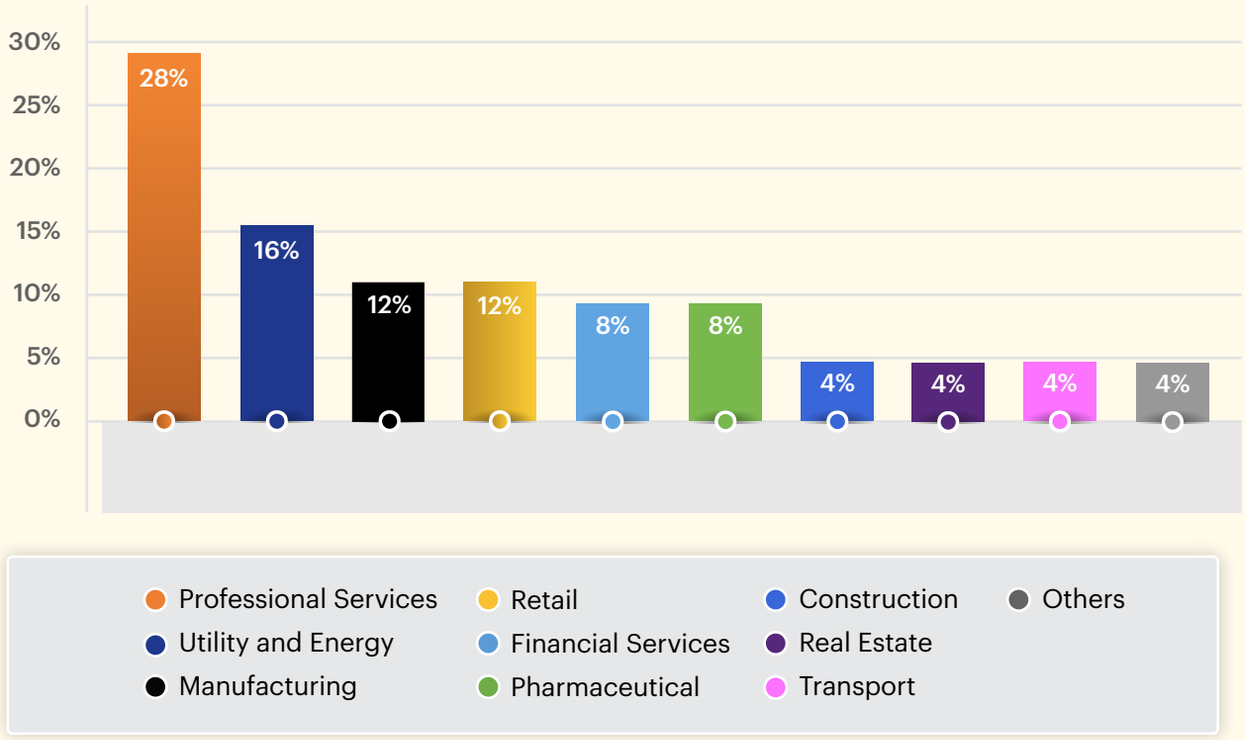


WHO ARE THE RANSOMWARE VICTIMS?

Looking at the statistics, there appears to be no discernible difference between sectors as to who will be affected by a ransomware attack. The slightly higher representation of professional services could just be a reflection of the strong service sector, including IT, in Malaysia. The only conclusion we can reasonably make is that all sectors are affected, and none will be spared. Instead, we'll have a look at the broader picture and attempt to understand why these companies were targeted in the first place.

Perhaps one thing that can be gleaned from the data is a slight preference towards larger organizations where the payout is higher. This likely comes as no surprise considering that ransomware operations are very much a business where higher profits are sought.

Percentage of Ransomware Victims by Industry



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2022.

It's important to note that this should not be construed as an indication that smaller businesses are never affected by ransomware attacks. Smaller firms simply consider paying for the services of professional incident response team too costly.

CYBER ESPIONAGE – THE SILENT THREAT

Most large, industrialized nations support their national security objectives with some form of cyber espionage-enabled intelligence gathering. As we have seen this year, less developed nations that don't have the capability to build their own cyber espionage programs can now hire mercenary organizations like the Israeli NSO group or criminal groups like RocketHack to perform cyber espionage on their behalf.[1]

Despite the ethical questions surrounding some of these operations, especially when non-democratic nations include dissidents, journalists, and human rights activists in the category of national security objectives, overall regular cyber espionage is an accepted part of international relations.

Some nations, notably China, also use cyber operations for industrial espionage. This is outside the norms of traditional cyber espionage.[2] Chinese industrial espionage is known for being large-scale and persistent. Unlike ransomware attacks, cyber espionage can cause silent yet significant damage. State-sponsored hacking operations in China are the biggest threat to intellectual property today, supporting domestic research in various sectors. Although not limited to one country, Chinese espionage is particularly notorious and poses a threat to national security and fair market competition.

The theft of intellectual property is the main objective of industrial espionage, which has become easier with the digitization of blueprints and widespread availability of CNC machinery. Cyber espionage enables the theft of designs, putting companies and their innovations at risk.

Cyber espionage can also be used to gain an advantage in trade negotiations and bidding. It is far from uncommon that negotiations involving Chinese corporations or the Chinese government, either as part of the negotiations or as a competitor, result in cyber attacks aimed at gaining inside information that can be used as leverage in negotiations.

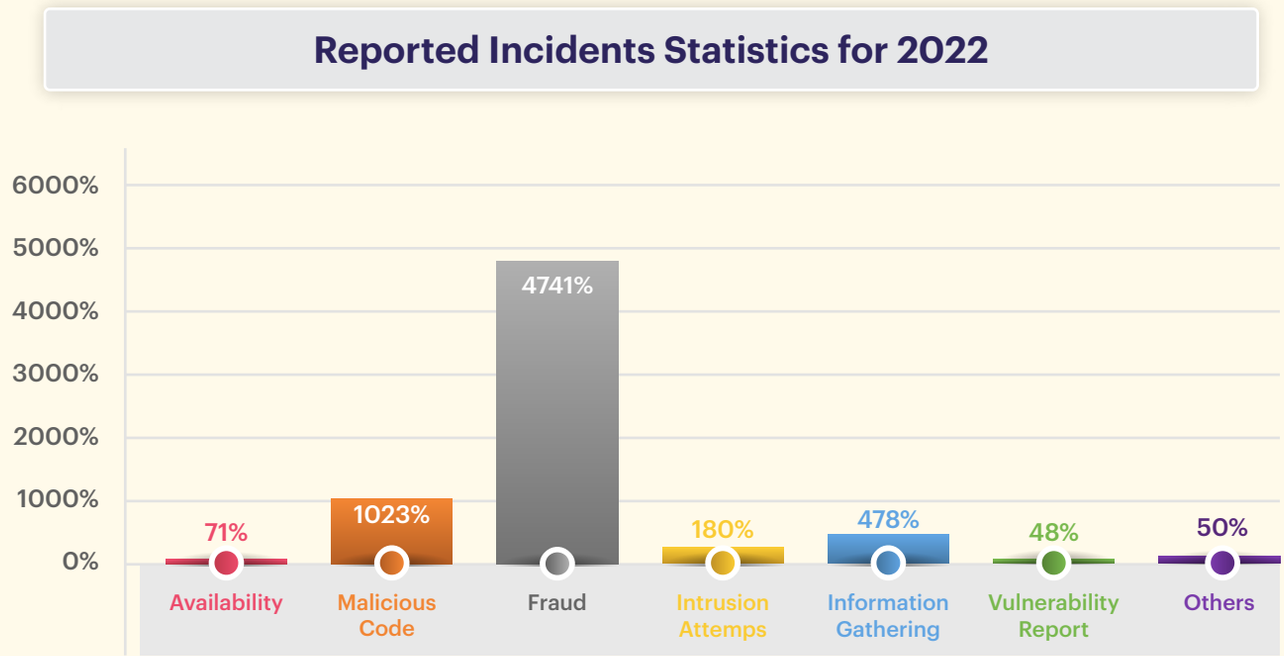
The growing geopolitical tensions between the U.S. and China and the resulting economic decoupling will limit China's ability to steal intellectual property by copying Western-owned production sites in China. As a result, China may resort to even more aggressive cyber espionage abroad to make up for the loss of access to foreign technology and maintain its position as a global leader.

1. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group
2. https://edition.cnn.com/2022/05/04/politics/china-hackers-economic-espionage-manufacturing/index.html

TREND ANALYSIS & TOP THREATS

Reported Incidents based on General Incidents Classification Statistics for 2022

Nexagate Cybersecurity Services 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 2022. 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.



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2022
and MyCERT Incident Statistics - Reported Incidents based on General Incident Classification Statistics 2022.

The reported incidents in 2022 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. The most reported incidents is **online fraud** with total of 4,741 incidents coming from, home users, private sectors, industries as well as from foreign entities. Malicious code and information gathering remain as prevalent threat, indicating a huge market for spammers and hacktivist to capitalize on weak organizational defences. Other threat captured includes, availability, information gathering, vulnerabilities report and other.

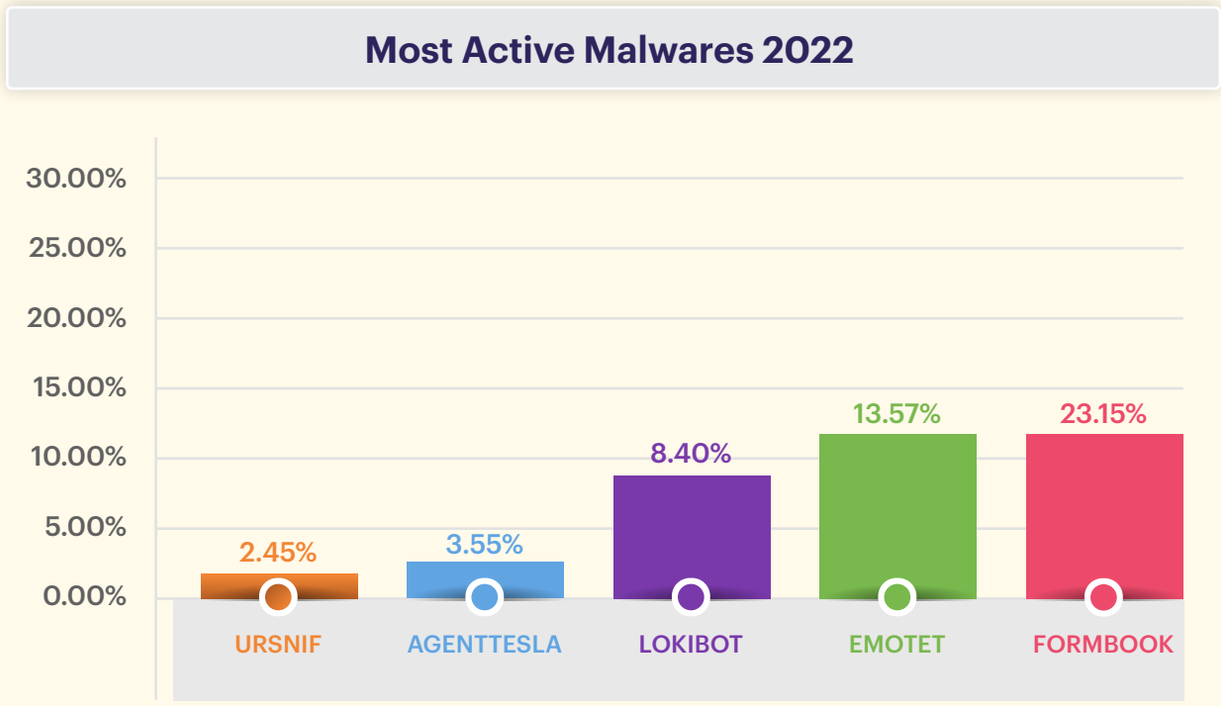
3. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=96c526d0-67e6-4f8e-91c8-006230405ece

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 2022 was Formbook, a backdoor written in C that communicates via HTTP. Supported commands include screenshot capture, shell command execution, file download and file execution. Formbook is also capable of capturing keystrokes, monitoring the clipboard, stealing web browser cookies, and extracting credentials stored by web browsers. Formbook also uses hook to intercept credentials and account information associated with web browsers and email 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.



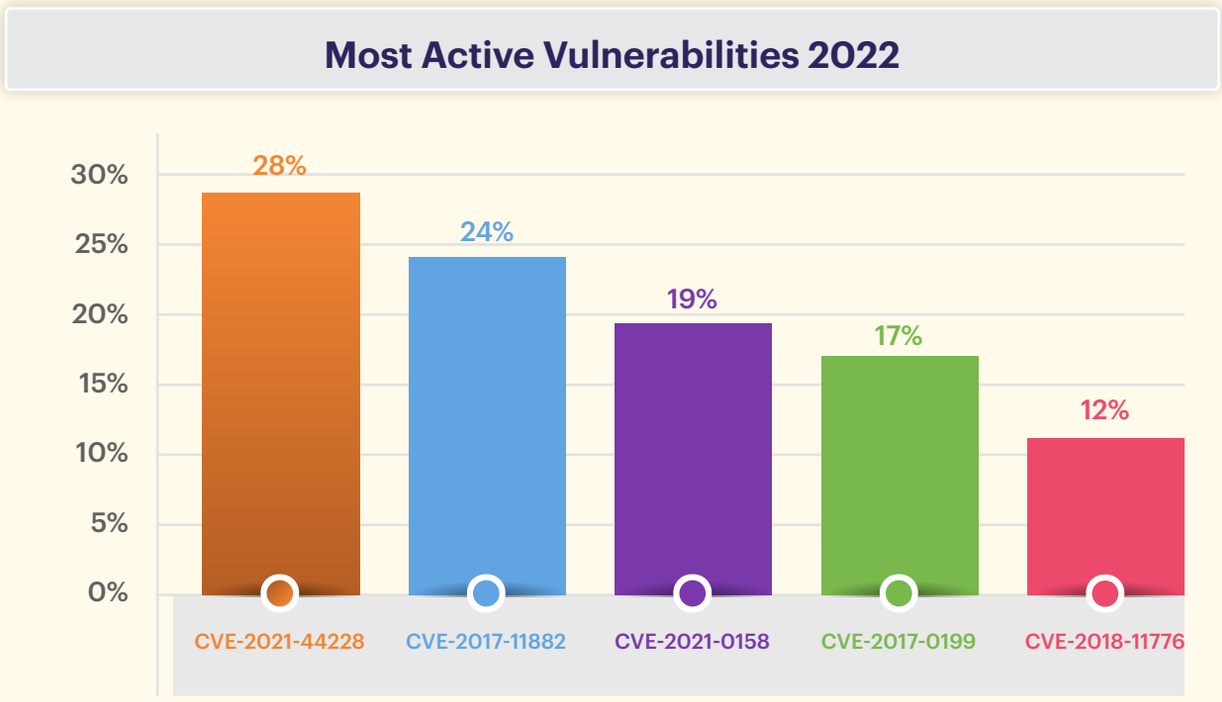
Source from Nexagate Cyber Fusion Centre (CFC) Data, 2022.

TREND ANALYSIS & TOP THREATS

Top 5 Active Vulnerabilities

In particular, the top 5 most active vulnerabilities for 2022. Leading the pack for exploitation attempts for 2022 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.



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2022.

CYBER THREATS AND HOW TO TACKLE THEM

This section is based on Nexagate's many years of experience investigating and preventing cyber attacks in Malaysia and Southeast Asian. We hope it will clearly show the importance of investing in cybersecurity and using threat intelligence to guide your priorities.

In the following five chapters, we will demonstrate identified key weaknesses that threat actors often use to compromise systems. Each chapter details a particular challenge and provides advice on solutions.

- Threat Actors Are Faster
- It's Too Easy To Get Full Control Of A Network
- Increased Use of Vulnerability Exploits
- Securing Your Digital Accounts: Beyond Passwords
- Denial Of Service Attacks Are Increasing

Our suggested recommendations and priorities are based almost entirely on responding to real-world incidents during 2022. We have delved into each case to fully understand the root causes and what could have prevented the breach or minimized the impact.

Whether you are a cybersecurity specialist responsible for protecting your organization, or a decision-maker in charge of overall financial priorities, the advice here will help you getting started immediately to strengthen your defensive capabilities.

CYBER THREATS & HOW TO TACKLE THEM

Threat Actors Are Faster

Challenge

Highly Scripted And Automated Attacks

Major ransomware gangs are becoming faster. By using heavily scripted attacks and something that could be likened to assembly line operations, these cybercriminals can increase the number of victims by spending less time on each attack and recruiting less technically savvy affiliates who only have to follow instructions in ready-to-use frameworks.

The increase in the speed of the attackers means that cybersecurity has less time to react. It is imperative that organizations can respond to intrusions promptly. Too often, Nexagate is called to assist victims of cyber attacks, where the signals that could have alerted a security operations team to the attack were buried in logs that had not been inspected.

Solution

Constant Monitoring Is Vital

Constant monitoring of your environment is key to proper cybersecurity. No matter how well hardened your network is, protection will never be 100% effective. With proper monitoring, you can still evict threat actors before they can cause too much harm. Of all measures that improve cybersecurity, proper monitoring is one of the least time consuming to implement.

Proper monitoring requires a mixture of host-based, network-based, and cloud-based sensors, depending on the network's structure. The chosen solution must allow custom detection rules to minimize false positives. It is also crucial that 24/7 monitoring is done by trained personnel. The time between an initial breach and full internal compromise can be as short as one hour; therefore, quick reaction time is essential.

The importance of having personnel to monitor the solution really cannot be overstated. While products certainly are improving, they are not yet ready to eliminate the need for humans to weed out false positives or otherwise trim detection rules.

CYBER THREATS & HOW TO TACKLE THEM

It's Too Easy To Get Full Control Of A Network

Challenge

From Breach To Full Compromise in Hours

As soon as cybercriminals gain a foothold in a network, their next objective is to take control of an account that has administrative privileges, typically a domain administrator account. After that, it is often "game over" as the threat actor will have the ability to take over the entire network and deactivate defenses.

If high-privilege accounts are routinely used to perform interactive logons such as Remote Desktop Protocol (RDP) to arbitrary systems, the domain admin credentials will be stored in the server's memory until logoff. Several tools are available, like Mimikatz, that make it easy for cybercriminals to extract such credentials from their foothold and use them to move further in the network, taking control of more accounts until they gain administrative privileges. All it takes is an hour or so, and the threat actor can have full compromise of a network.

It's Too Easy To Get Full Control Of A Network

Solution

Identity Tiering

When a high-privilege account is logged on to a system in a lower security tier, any attacker with control of this system could obtain the high-privilege credentials and therefore escalate their privileges. The fact that administrators use high-privilege accounts such as domain admins to access arbitrary systems highly increases the spreading of these credentials, and therefore, the likelihood of an intruder obtaining them.

Identity tiering should be used to tackle this issue. Tiering defines a domain model to avoid the exposure of credentials to systems in a lower-security zone. For example, domain admins should only be able to access domain controllers and other systems in the same tier. More details are available as part of Microsoft's Privileged Access Strategy and Security Rapid Modernization Plan. It is also important that service accounts are included in tiering and privileged access strategy.

The Primary Reason Credentials Are Exposed To Systems

The primary reason credentials are exposed to systems is that the account performed an interactive logon, such as console access or classic RDP logons. These interactive sessions allow the single sign-on (SSO) experience – which means the logged-on user has SSO to other resources from that session without having to re-enter their credentials every time. For this to be possible, Windows maintains the credentials in memory (usually in their hashed form) for the duration of the session.

Non-interactive logons such as Remote PowerShell, remote WMI, MMC snap-ins connecting to remote systems, etc., do not present the same issue. They do not have SSO from the remote system, and the credentials are not stored in the memory of the remote system. These ways of managing systems should be preferred to regular RDP.

Additionally, administrators should use dedicated machines, i.e., Privileged Access Workstations (PAW), when using high-privilege accounts to limit the exposure. At the same time, they should ensure PAW machines are under the correct control and built using tooling that prevents access to unauthorized users. These can be tools like PowerShell Deployment Toolkit, Microsoft Deployment Toolkit, or other tools that do not leave an agent behind.

Local accounts such as the built-in local administrator account should not share passwords. Threat actors often leverage this dependency to gain access to additional systems after initial access. For Windows systems managed by Active Directory, Local Administrator Password Solution (LAPS) can be used to ensure passwords are unique and centrally managed.

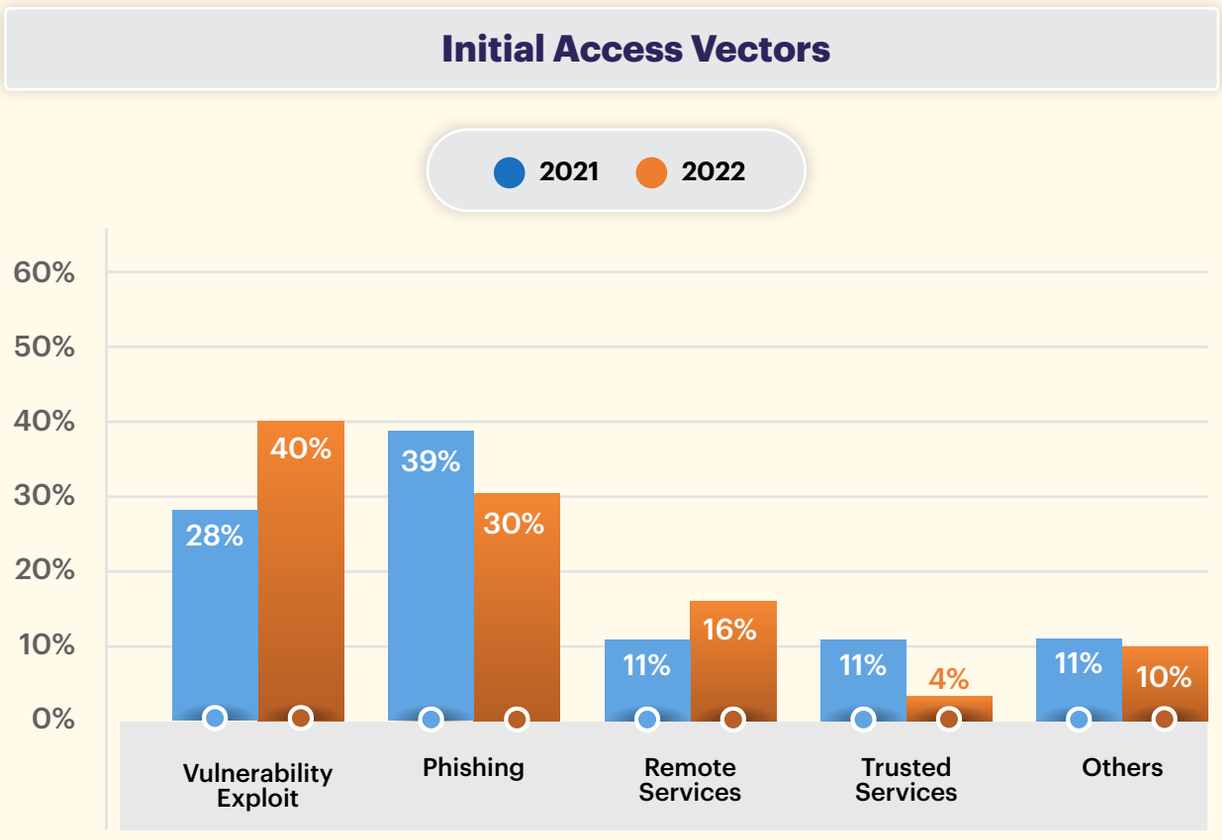
CYBER THREATS & HOW TO TACKLE THEM

Increased Use of Vulnerability Exploits

Challenge

Cybercriminals Are Efficient At Exploiting New Vulnerabilities

Cybercriminals are constantly evolving their business model. They are also becoming more and more efficient at exploiting vulnerabilities to gain a foothold in environments. Zero-day exploits represent the pinnacle of vulnerability exploits, but these are difficult and expensive to obtain. It is much more effective to exploit vulnerabilities that are already published before the intended victims have time to patch their systems.



Source from Nexagate Cyber Fusion Centre (CFC) Data, 2021 & 2022.

As soon as a promising patch is released, cybercriminals begin to reverse engineer the patch to discover the vulnerability it is intended to fix and develop an exploit. Within two to three days, these criminals can have a working exploit.

Increased Use of Vulnerability Exploits

Once an exploit is developed, there are many tools available today that can scan the entire internet for vulnerable systems in a relatively short time, or that already have indexed most internet resources. The exploits can then quickly be leveraged in mass attacks against the vulnerable systems before the affected organizations have had time to apply the patch.

These attacks are highly effective at catching organizations that have not yet managed to patch or update their systems. Some of the exploits most widely used by cybercriminals are still effective in attacks against large organizations several months after a patch was available. This also means that vulnerability exploits have now overtaken phishing as the main attack vector in serious ransomware attacks.

Solution

Effective Patch Management

One of key trends Nexagate has observed in 2022, is that more than 40% of all attacks originated from publicly accessible and vulnerable systems. Once a vulnerability in a popular software has been disclosed, it may be only a matter of hours until worldwide scanning is initiated to search for vulnerable systems.

You should benchmark your vulnerability and patch management program against the two-day rule. The rule simply states that once a patch is available for a public available system, it should be applied within two days for internet-facing applications and systems.

CYBER THREATS & HOW TO TACKLE THEM

Securing Your Digital Accounts: Beyond Passwords

Challenge

Single Factor Authentication Is Not Enough

The rise in remote working after the COVID-19 pandemic has led to more attack vectors for cybercriminals. Exploiting insecure RDP or VPN connections, as well as external access to mail-boxes, are common attack vectors.[4]

There are frameworks available to cybercriminals that allow for automated password-guessing attacks that originate from multiple IP addresses, that can bypass protections against pass-word-spraying blocks. It is also a simple fact that a sizeable group of users in most organizations are using simple and easily guessable passwords, something cybercriminals are aware of.

As with exploiting vulnerabilities, there are tools available to cybercriminals that can be used to scan large parts of the internet for available remote-access services. Even if many connections are protected with multi-factor authentication (MFA), a single unprotected system can be enough to allow cybercriminals entry to a network. It is now often easier for cybercriminals to find weak spots to attack, using the aforementioned tools, than it is for the IT administration to perform proper asset inventory.

An unprotected mailbox can represent a much larger threat than the loss of corporate email. If cybercriminals gain access to a corporate mailbox, they can impersonate a legitimate user to send phishing emails to other users in the organization and other organizations. Phishing attacks, in large part, rely on social engineering, and the chance of success rises dramatically if the attacker can use a legitimate mailbox to send the lure.

Solution

Always Enforce MFA

Solutions should be implemented to ensure that all internet-facing authentication services require MFA, with a high priority on systems that authenticate using internal credentials. If legacy systems do not support MFA, the service should be moved behind a VPN service with MFA, or migrated to a more modern product that supports MFA.

It is also important to understand that there should be no exemptions to this rule. A single unpro-tected login can be enough for cybercriminals to exploit and gain entry. There are many tool cybercriminals can use to find such weak spots.

4. https://www.drizgroup.com/driz_group_blog/why-single-factor-authentication-isnt-enough-to-protect-your-organizations-network

CYBER THREATS & HOW TO TACKLE THEM

Denial Of Service Attacks Are Increasing

Challenge

The Growth Of DDoS Ransom Attacks

Over the last year, there has been a rise in the impact of DDoS attacks, following an already established trend. During 2022, we saw attackers targeting different types of victims with one common goal, extorting their victims for a large ransom. Typical ransom amounts today are 1-5 Bitcoins.

There have been many new things observed during the last year, and two attack vector categories stood out. The UDP reflection attacks, also known as volumetric attacks, became more varied with frequent occurrences of floods from CoAP[5], ARMS3[6], and WS-DD[7] amplification sources. From the look of it, these reflection sources are now well known to many of the malicious actors, and therefore seen in more attacks. Given the rise in more connected devices, the potential for new and growing numbers of amplification sources is a threat that cannot be ignored. Flooding the infrastructural parts of a service with traffic from amplification sources affects the overall accessibility, limiting potential customers from reaching a website, or employees from accessing their resources.

A notably more popular attack vector is the HTTP-based DDoS attack, that has both come in greater numbers, and with much more traffic due to larger botnets. Simulating normal web traffic behavior from thousands of bots towards a site, usually affects the overall user experience since the process of identifying bots is likely to affect the experience for normal users as well. If identification fails, the botnet might drain a service of its resources, making it unavailable to friendly users.

Stopping HTTP-based attacks is much more difficult than stopping volumetric attacks. Of particular concern are services that use SSL for incoming traffic. Unless certificates are stored in the cloud, incoming traffic must be decrypted on-prem, before it is even possible to determine if the incoming traffic is legitimate or not, which can be enough to flood a service and make it unavailable.

Common for both attack vector categories is that the involved hosts are used in different setups targeting different customers, which to some extent reveals that there is more than one command and control instance that is orchestrating the attacks. Finding these C&C instances and their operators is key to closing the circle and removing the threat.

Solution

Implement Proper DDoS Protection

Being available on the internet will always make you a potential victim for these kinds of attacks. Reducing the potential damage that comes from them is achieved by scaling your infrastructure to a degree that makes it possible to perform analysis and mitigation on a sophisticated enough level that false positives become minimal. Having a single mitigation pipeline is not enough to cope with large volumetric attacks; the solution lies in a distributed infrastructure which can handle the load.

For further reading on this subject: 5 Ways to Prepare Your Website for High Traffic

5. hCoAP = Constrained Application Protocol. A protocol typically used in internet of things (IOT) devices, that can be abused for DDoS reflection attacks.
6. ARMS = Apple Remote Management Service, is a part of ARD function that can be abused to conduct DDoS reflection attacks.
7. WS-DD = Web Service Dynamic discovery, A discovery multicasting protocol inside LAN that can be abused for DDoS reflection attacks.

OUTLOOK FOR 2023

Nexagate predicts that in 2023, most cybercriminals will continue to operate with relative impunity in Russia. Their main efforts in 2023 will likely be to improve their operational security to meet increased pressure from outside on their infrastructure. They will probably also mix different cryptocurrencies, using even more anonymous forms of cryptocurrency, such as Monero, to make transactions even more difficult to trace.

Fierce Competition

Ransomware attacks will continue to increase in number and efficiency, but the rate of growth will likely decrease somewhat. The primary bottleneck for the ransomware criminals to further expand their operations appears to be their difficulty in recruiting new hackers. This forces the gangs to recruit less experienced hackers to expand their ranks. This, in turn, means that many attacks will become more stereotypical and consequently predictable, increasing the value of utilizing threat intelligence to stay ahead of the attackers.

The competition for talent between different ransomware gangs may tempt some groups with stronger ties to the Russian government to leverage their contacts and convince the Russian security service (FSB) to tip the scales in their favor. This can even be disguised as a crackdown on cybercrime to appease the West. Such a development would likely lead to a consolidation of the ransomware gangs into fewer but more powerful groups with even stronger ties to the Russian government.

The Same Old Tactics Still Works

Part of the decline in phishing as an initial attack vector in 2022 is perhaps due to the takedown of the Emotet botnet early that year. In 2023, Nexagate expects that there might be a resurgence of phishing attacks as an initial attack vector in ransomware attacks as cybercriminals develop alternatives to the old Emotet, like Datoploader. In the Q4 of 2021, FIN12/Wizard Spider, the main ransomware gang buying access from the Emotet botnet, even appears to have tried to rebuild the Emotet botnet, this time under their own control.

As more enterprises begin to strengthen their cyber defenses, the risks incurred by those organizations that maintain large, flat, and decentralized networks without proper segmentation will rise as they will be part of a shrinking pool of ”low-hanging fruits” for the cybercriminals.

OUTLOOK FOR 2023

What To Watch Out For

It is possible that in 2023, some of the larger ransomware gangs will attempt to normalize their business by selling various forms of "insurance" to potential victims, basically in the same way other organized crime sells "protection." This, of course, is still nothing more than thinly disguised extortion. Such a development would not be possible until there was some form of consolidation among the major ransomware gangs into one or more cartels. It is hard to see how such "insurance" would have any value in the current competitive climate as it would only apply to one of the many ransomware gangs active today.

Some Russian cybercriminals have even begun outreaching to Chinese criminals to recruit them into partnership on ransomware operations. These attempts are not expected to lead to a significant change in the cybercrime ecosystem, at least not in the short term. The cultures of the Chinese and Russian cybercrime ecosystems are quite different, and it seems unlikely that Chinese hackers will accept working under Russian leadership. However, if Chinese cybercriminals were to broadly adopt ransomware as a tactic, that could potentially be a game changer and a radical escalation of the ransomware threat.

HOW DO WE REALLY STOP CYBERCRIME?

This report contains many helpful recommendations on how to increase your organization's cyber resilience. However, to truly protect our society against cybercrime we need more than just technical measures. Cybercrime is a challenge for our entire society, and one that requires a coordinated response from all of those affected.

Stop the Flow of Money

There is an insidious danger in accepting ransomware and other forms of cybercrime as normal. Instead of joining forces to combat crime, some organizations now prefer to acquire cyber insurance that covers the cost of the ransom, hire a professional negotiator, and pay the criminals. This is precisely what the criminals want us to do. They want us to pretend it is "only business." Every time a victim pays the ransom, the criminals grow stronger and bolder, and we all lose.

It is also important to understand the crucial role cryptocurrency plays in the explosion of ransomware attacks. Without easily tradeable cryptocurrency, there would be no way for the criminals to obtain the vast untraceable ransom amounts they extort every year. Regulating cryptocurrencies would go a long way to making ransomware crimes more difficult.

Stop Blaming the Victims

At the same time, we must also stop blaming the victims and remove the stigma of being a victim of cybercrime. We are caught in a vicious circle where victims of crime do not want to report cybercrime to law enforcement for fear of being ostracized. This means that law enforcement lacks data regarding the extent of the criminal activities, so they receive insufficient funding to combat cybercrime. This leaves the field virtually wide open for the criminals to continue to attack more victims.

While data protection laws like GDPR are necessary to safeguard the privacy of personal data, it is important to realize that they have been weaponized by cybercriminals as it makes it even harder for their victims to report cybercrime. If a victim reports a cybercrime to law enforcement, the result can be a GDPR fine if they are found to have been careless with their customers' personal data. This makes victims even more reluctant to report a crime. Creating an environment where victims feel safe to report cybercrime should be one of our top priorities.

Hold Government Responsible

One reason ransomware has reached such epidemic levels is that cybercriminals operate safely from countries like Russia. In Russia, the government tolerates and protects them, and they can perform criminal extortion all over the world without fear of arrest. Holding these countries that either passively or actively enable cybercrime accountable for the attacks is also important. Ultimately, we need to recognize that all stakeholders must work together to combat the scourge of organized cybercrime. Cybersecurity professionals, politicians, law enforcement, and private corporations need to cooperate with a holistic strategy to stop the flow of money that feeds criminal enterprises.

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.

nsi | 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