Threats in Cyberspace in 2022

Cyberspace is transforming into a public space with important socio-economic activities where all citizens participate regardless of their living space or age. The arrival of a society in which real space and cyberspace are fused together is becoming a reality in every aspect, from the infrastructures that support people's lives and socio-economic activities such as finance, aviation, railroads, and medical care, to national functions related to public safety and security such as police and defense.

On the other hand, uncertainty surrounding cyberspace is constantly changing and increasing due to changes in the international society, including the emergence of competition among nations over political, economic, military, and technological issues, the advances in information and communication technologies, and the deepening interdependence of complex socio-economic activities.

Under these circumstances in Japan, as the domestic damage caused by ransomware have been expanding, the cases affecting business activities throughout the supply chain and local healthcare systems have also been confirmed and the cyberattacks targeting crypto asset businesses, academics and researchers at think tanks have been revealed.

In addition, the number of phishing reports has increased and the number of victims of online banking fraud has temporarily surged. The threats in cyberspace continue to be extremely serious.

In 2022, the number of ransomware cases reported to the National Police Agency (NPA) through prefectural police organizations was 230 (+57.5% vs. 2021), indicating a continuous increase since the second half of 2020. The damage was widespread, regardless of the sizes of companies and organizations, or types of industry. The domestic automobile company was forced to suspend production and sales activities, and the medical institutions experienced disruptions in their electronic medical record systems, resulting in the postponement of surgeries, the temporary suspension of outpatient treatment and emergency outpatient services. As a result, the suspension or degradation of social infrastructure caused by these incidents made a significant impact on people's lives and socio-economic activities. Moreover, looking at the infection routes, many cases of intrusion through vulnerabilities of VPN devices that were disclosed in the past were reported. Once infected, the damage is not limited to the organization itself, cases of infection spreading to supply chain businesses were also confirmed.

There have been cases where it took more than 2 months to restore infected systems, and cases where more than 50 million yen was required for investigation and restoration.

In response to this situation, the NPA, in cooperation with related ministries, has issued a series of alerts to ensure that appropriate cybersecurity measures are taken not only by government agencies and critical infrastructure providers, but also by industry in general. The prefectural police also promoted cooperation with economic organizations such as the Chamber of Commerce to share information regarding crime methods and issue alerts.

Cyberattacks targeting specific businesses and academics have occurred in Japan. There have been cyberattacks against Japanese crypto asset exchange service providers by the methods similar to those used by the cyberattack group called ‘Lazarus’, which is believed to be a subordinate organization of the North Korean authority. The situation strongly suggests that the group has been targeting those Japanese businesses for several years. Also, a number of cyberattacks have been confirmed in recent years, in which cyber actors have attempted to steal information by executing malware programs against academics and think tank researchers using certain common methods. The NPA, in cooperation with related ministries, has announced an alert to the public about these cyberattacks with specific method and information.

Furthermore, amid the tense international situation, including the situation in Ukraine, cyberattacks against overseas government agencies and companies or facilities related to critical infrastructures have continued to occur one after another, and some of these attacks are suspected to be due to state-sponsored cyberattack groups. In Japan, several websites operated by government agencies such as ‘e-Gov’ were temporarily unavailable, and it was confirmed that a pro-Russian hacker group such as ‘Killnet’ had released a statement implying that they had committed the crime.

The number of online banking fraud incidents had been on a downward trend in terms of both the number of incidents and the amount of damage since 2020, but in the second half of the year 2022, there was a sharp increase, with 1,136 incidents and approximately 1.5 billion yen in total damage, the first year-on-year increase in 3 years (+94.5% and 85.2%, respectively, vs. 2021). Most of the damage is believed to be caused by phishing, and a large number of emails are being confirmed in which directing users to phishing sites disguising as financial institutions. According to the Council of Anti-Phishing Japan, there were 968,832 phishing reports in 2022 (+84.0% vs. 2021), and the number is increasing steadily.

The number of accesses detected by the NPA as vulnerability scanning activities remained at a high level of 7,707.9 per IP address per day. Most of these accesses originated from overseas, and it is recognized that the threat related to cyberattacks from overseas continues to increase. In terms of the destination ports of the accesses detected, accesses to ports with port numbers 1024 or higher accounted for the majority, and many of these accesses are believed to be for the purpose of searching for IoT devices with vulnerabilities or cyberattacks against IoT devices.

Since the threats in cyberspace continue to be extremely serious, the NPA's Cyber Affairs Bureau and the National Cyber Unit were newly established in April 2022. These are playing a key role in the investigation and clarification of the actual situation through collaboration between the NPA and the prefectural police organizations, as well as cooperation with various entities in Japan and overseas. At the same time, the NPA is promoting effective damage prevention measures in cooperation with related ministries and agencies, private companies, to ensure the safety and security of cyberspace as well as real space.

1 Threat trend in 2022

(1) Ransomware situation and countermeasures

A) Overview

Ransomware is malware which infects devices to encrypt stored data to be unusable, then demands ransom in exchange for decrypting the data.

In many recent cases, the double extortion method has made up the majority, in which the perpetrators not only encrypt the victims' data, but also steal them and demand ransom, extorting "If you refuse to pay, we will expose your data".

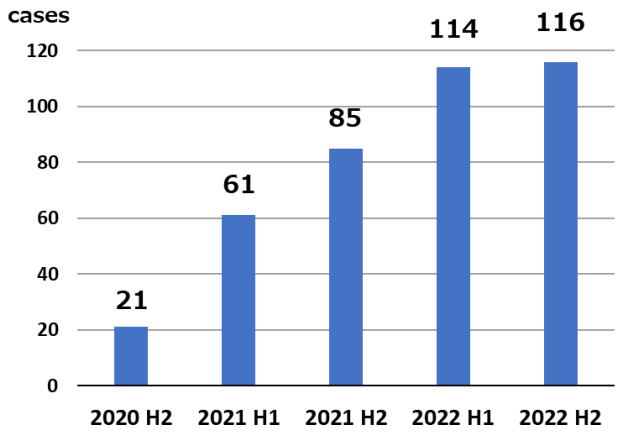
Dominant infection method in 2022 was exploitation of vulnerabilities in VPN devices disclosed on the web or weak credentials to infiltrate into the organizations' networks and infect them with ransomware, as in 2021.

B) Ransomware damages

a. Number of cases

In 2022, the number of ransomware cases reported to the NPA through the prefectural police organizations was 230, indicating a continuous increase since the second half of 2020.

【Fig1: No. of Reported Ransomware Cases】



b. Major Observation

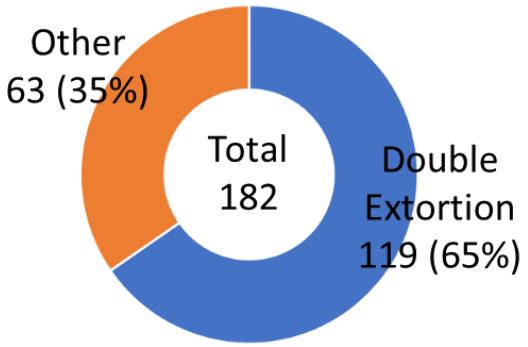
○ Double extortion is the most common cause of damage

Among the 230 cases of ransomware damage, the police could identify types of ransomware in 182 cases, and the double extortion methods were used in 119 cases (65%).

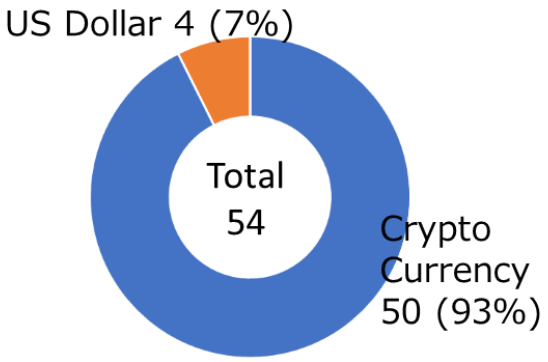
○ Crypto assets account for a large portion of money demands

Among the 230 cases, 54 cases directly demanded money, of which 50 cases (93%) demanded crypto assets.

【Fig. 2: No. of Reported Cases by Modus Operandi】



【Fig. 3: No. of Reported Cases by Demanded Payment Method】

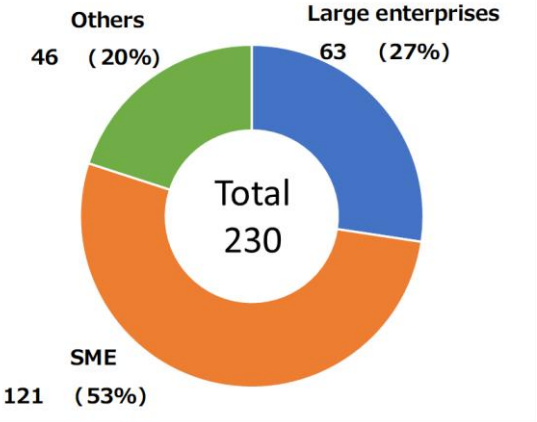


c. Sizes of Victim Corporations

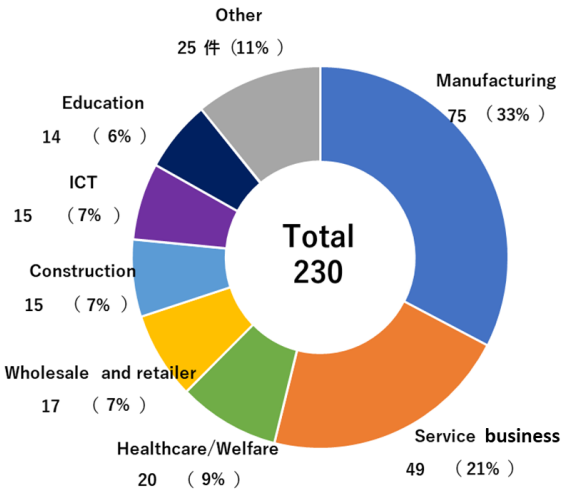
Figure 4 shows a breakdown of the 230 ransomware cases by the size of the affected businesses[*1], in which large enterprises accounted for 63 cases, while small and medium enterprises accounted for 121 cases.

Focusing by types of industry[*2] shown in Figure 5, manufacturing accounted for 75 cases, service business for 49 cases and healthcare/welfare for 20 cases, indicating the occurrence of damage regardless of their sizes or types of industry.

【Fig. 4: No. of Reported Cases by the Sizes of Victims】



【Fig. 5: No. of Reported Cases by the Types of Industry 】



*1 Classified in accordance with Article 2, Paragraph 1 of the Small and Medium-sized Enterprise Basic Act

*2 Classified in accordance with Japan Standard Industrial Classification

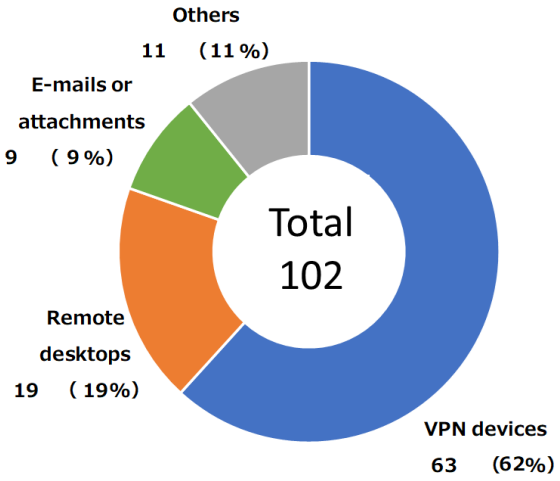
C) The state of ransomware damage

In order to grasp the actual damage by ransomware, the police sent a survey to 230 victim entities and received 140 responses which they analyzed.

a. Infection Routes

Regarding the infection routes of ransomware, 102 valid responses were received, of which 63 (62%) were through VPN devices and 19 (19%) were through Remote Desktop, indicating the majority (81%) of infections appeared to have exploited vulnerabilities in the devices often used for remote work or weak credentials.

【Fig. 6: Infection Routes】

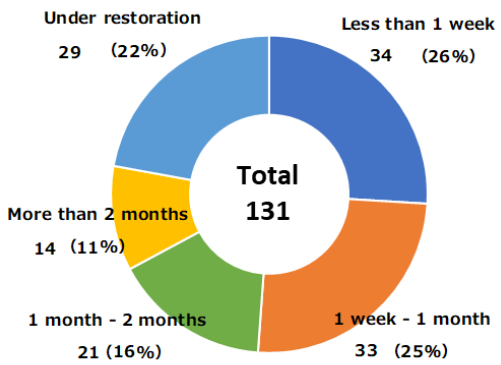


b. Time and costs required for restoration

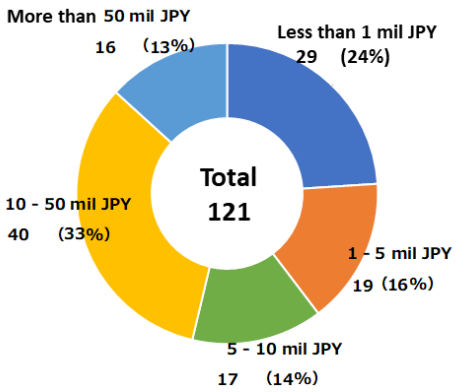
Regarding the time required for restoration, 131 valid responses were received, of which 35 respondents took 1 month or more.

Regarding the total research and restoration costs incurred due to ransomware, 121 valid responses were received, of which 56 (46%) respondents paid 10 million yen or more.

【 Fig. 7: Time Required for Restoration 】



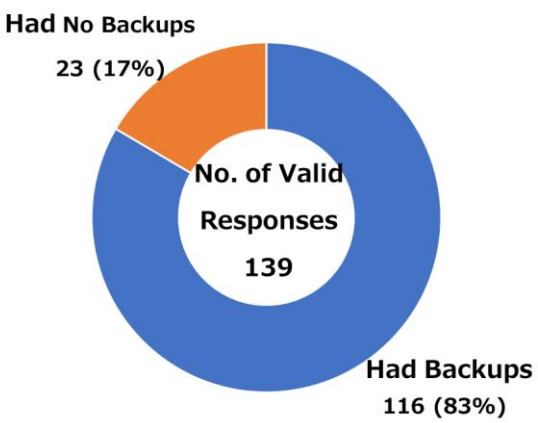
【 Fig. 8: Costs Required for Restoration 】



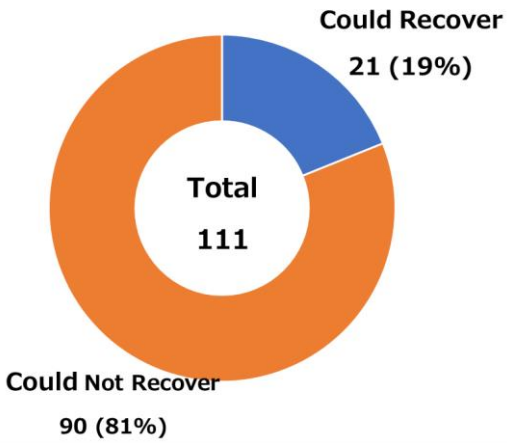
c. Data Backups

Among 139 valid responses about data backups of the victimized systems or devices, 116 (83%) stated they had been backed up. Among 111 responses about recovery attempts from backups, 90 (81%) stated their systems or devices could not be recovered to the pre-incident extents.

【Fig. 9: Availability of Backups】



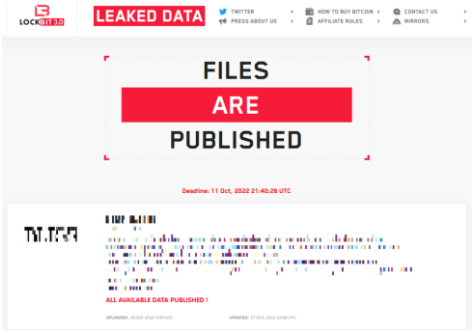
【Fig. 10：Recovery from Backups】

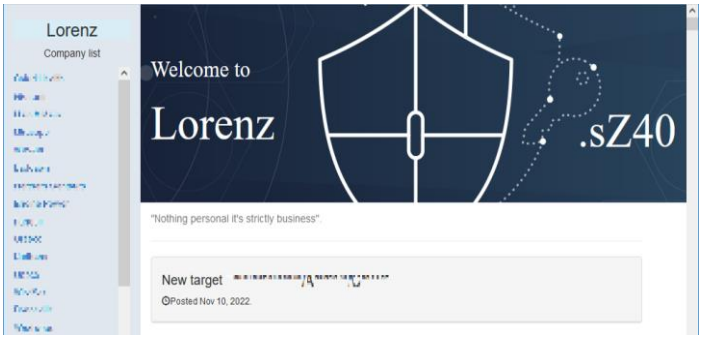


D) Status of ransomware leak sites

The police have been observing websites on the Dark Web and confirmed in 2022 that the data of Japanese businesses leaked by ransomware was posted on their leak sites. The exposed data included the victims' product information, user IDs and passwords.

【Fig. 11: Examples of leak sites on the Dark Web】





E) Police Efforts

- Anti-ransomware campaign for SMEs and medical institutions

In Japan in 2022, ransomware incidents stopped production, sale and services of SMEs, and suspended medical institutions' reception of new patients caused by inaccessibility to electronic health record systems.

Accordingly, the police enhanced cooperation with the Chamber of Commerce and the Hospital Associations as well as their members to raise awareness of ransomware and shared information of their crime methods.

The police also utilized diverse media and opportunities including TV, radio, websites and security seminars, as well as through councils of prefectural police and pertinent organizations, to actively implement anti-ransomware campaigns.

- Joint cybersecurity awareness campaigns with pertinent government agencies

In response to occurrence of ransomware incidents and heightened risks of cyberattack cases, the NPA, the National center of Incident readiness and Strategy for Cybersecurity (NISC) and pertinent government agencies repeatedly implemented joint alerts for businesses and organizations including critical infrastructure operators to encourage enhancement of cybersecurity by suggesting specific cybersecurity measures to be implemented.

【Fig.12: Joint Alert Issued by the NPA, the NISC & Pertinent Agencies】

令和４年 12 月 20 日
経済産業省
総務省
警察庁
内閣官房内閣サイバーセキュリティセンター

年末年始休暇において実施いただきたい対策について（注意喚起）

サイバー攻撃被害のリスクの高まりを踏まえ、本年８月には、関係府省庁の連名にて「夏季の長期休暇において実施いただきたい対策について（注意喚起）」を発出しましたが、その後も、ランサムウェアによるサイバー攻撃被害が国内外の様々な企業・団体等で続き、国民生活に影響が出る事例も発生しました。また、エモテットと呼ばれるマルウェアへの感染を狙う攻撃メールについては、本年１１月に活動再開とその新たな手口（【参考】内※１，２，３を参照）を確認しており、感染や被害の拡大が懸念される状況にあります。

さらに、本年９月には、日本の政府機関や企業のホームページ等を標的とした DDoS 攻撃と思われるサービス不能攻撃により、業務継続に影響のある事案も発生したほか、国家等が背景にあると考えられる攻撃者による暗号資産取引事業者等を狙ったサイバー攻撃や、一定の集団によるものとみられる学術関係者等を標的としたサイバー攻撃も明らかとなり、国民の誰もがサイバー攻撃の懸念に直面することとなっています。

このように依然として厳しい情勢の下での長期休暇においては、休暇中の隙を突いたセキュリティインシデント発生の懸念が高まるとともに、長期休暇後に電子メールの確認の量が増えることで偽装のチェックなどがおろそかになるといった感染リスクの高まりが予想されます。さらに、長期休暇中は、通常と異なる体制等により、対応に遅延が生じたり、予期しない事象が生じたりすることが懸念されます。

こうした長期休暇がサイバーセキュリティに与えるリスクを考慮し、別紙の対策を参考に、適切な管理策によるサイバーセキュリティの確保について、サプライチェーンも含めてご検討をお願いいたします。

あわせて、不審な動き等を検知した場合は、早期対処のために速やかに所管省庁、セキュリティ関係機関に対してご連絡いただくとともに、警察にもご相談ください。

(2) Cyberattack Incidents and Police Efforts

A) Major Cyberattack Incidents

- Malware infection at multiple chemical enterprises

In January 2022, a chemical engineering corporation announced the occurrence of unauthorized accesses to their in-house servers and potential leaks of partial data stored therein. In relation to these incidents, the corporation also announced that unauthorized accesses were made to their affiliate companies' in-house servers as well, causing potential leaks of their stored data.

- Unauthorized accesses to a major system integrator

In May 2022, a major system integrator and their affiliate companies announced that they had confirmed that unauthorized accesses were made to some of their communication control equipment (CCE) by exploiting vulnerabilities, and that communication packets which were passing through the targeted CCE were potentially stolen.

- Inaccessibility to multiple websites

In September 2022, multiple websites including "e-Gov" run by Japanese government agencies and those of private companies temporally became inaccessible. Coincidently, suggestive claims of responsibility issued by the pro-Russia hacker groups including "Killnet" were confirmed.

"Killnet" announced opposition to Japan's stance against Russian invasion of Ukraine but denied their relations with the Russian government.

B) Police Efforts

- Awareness-raising for critical infrastructure operators

Police continuously implement awareness-raising campaigns for critical infrastructure operators against cyberattacks. In 2022, police alerted about vulnerabilities of particular telecommunications equipment, and issued individual alerts when receiving cyberattack information from cooperating foreign government agencies and organizations to prevent and minimize expansion of damage from cyberattacks against critical infrastructure operators.

- Takedown of C2 servers

Police made continuous efforts including identifying servers in Japan functioning as C2 servers through analysis of malware used in cyberattack incidents, and requesting their operators to take down their illicit functions.

- Joint response drills

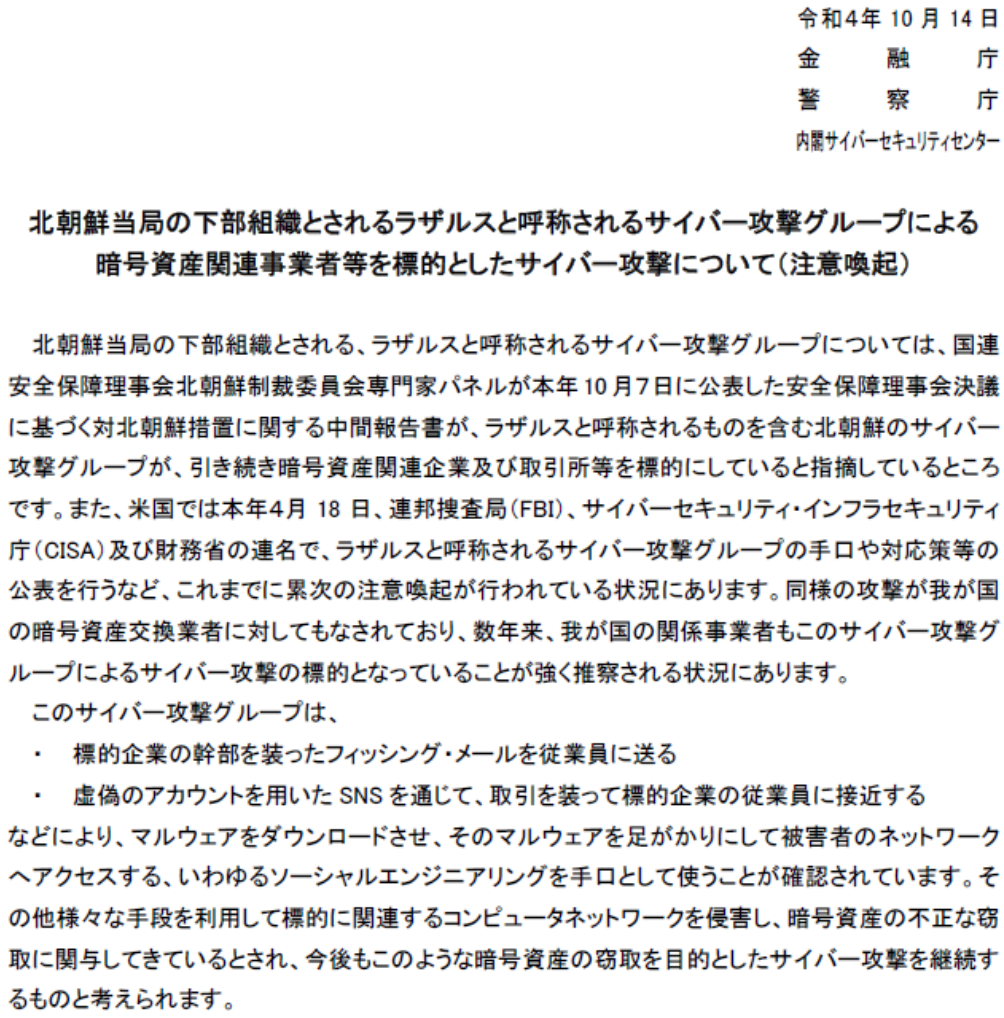
  Police continuously implement joint response drills with critical infrastructure operators in anticipation of cyberattack incidents. In 2022, police implemented 596 joint response drills for wide-ranging entities from local governments, electric power providers to financial institutions to consolidate collaboration with police and enhance cyberattack response capability of each entity, in which the trainings against spear-phishing emails and onsite practical trainings were conducted to confirm cooperation with police.

- Awareness-raising against “Lazarus” cyberattack group

  Commitment of “Lazarus” cyberattack group, an alleged subordinate of North Korean authority, in cyberattacks targeting crypt asset management firms in Japan turned out to be strongly presumable through investigations and researches by prefectural police departments concerned and the National Cyber Unit.

  While cyberattacks aimed to steal crypto assets presumably committed by “Lazarus Group” are expected to continue, crypto assets transactions expand not only among businesses but also among individuals, increasing potential risk of victimization of the latter. Hence, the NPA issued an alert jointly with the Financial Services Agency (FSA) and the NISC on October 14, 2022, to raise awareness among the individuals and businesses engaged in crypto assets transactions that they need to enhance their cybersecurity under the circumstances where organized cyberattacks are committed.

【Fig. 13: Excerpt from the Alert】



令和4年 10 月 14 日
金　　融　　庁
警　　察　　庁
内閣サイバーセキュリティセンター

北朝鮮当局の下部組織とされるラザルスと呼称されるサイバー攻撃グループによる暗号資産関連事業者等を標的としたサイバー攻撃について（注意喚起）

北朝鮮当局の下部組織とされる、ラザルスと呼称されるサイバー攻撃グループについては、国連安全保障理事会北朝鮮制裁委員会専門家パネルが本年 10 月7日に公表した安全保障理事会決議に基づく対北朝鮮措置に関する中間報告書が、ラザルスと呼称されるものを含む北朝鮮のサイバー攻撃グループが、引き続き暗号資産関連企業及び取引所等を標的にしていると指摘しているところです。また、米国では本年4月 18 日、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）及び財務省の連名で、ラザルスと呼称されるサイバー攻撃グループの手口や対応策等の公表を行うなど、これまでに累次の注意喚起が行われている状況にあります。同様の攻撃が我が国の暗号資産交換業者に対してもなされており、数年来、我が国の関係事業者もこのサイバー攻撃グループによるサイバー攻撃の標的となっていることが強く推察される状況にあります。

このサイバー攻撃グループは、

・　標的企業の幹部を装ったフィッシング・メールを従業員に送る
・　虚偽のアカウントを用いた SNS を通じて、取引を装って標的企業の従業員に接近する

などにより、マルウェアをダウンロードさせ、そのマルウェアを足がかりにして被害者のネットワークへアクセスする、いわゆるソーシャルエンジニアリングを手口として使うことが確認されています。その他様々な手段を利用して標的に関連するコンピュータネットワークを侵害し、暗号資産の不正な窃取に関与してきているとされ、今後もこのような暗号資産の窃取を目的としたサイバー攻撃を継続するものと考えられます。

○ Awareness-raising against cyberattacks targeting academics and think tank researchers

In recent years, cyberattacks targeting academics and think tank researchers which uses emails disguised as requests for speeches or interviews to deceive the recipients into executing malware that allows the attackers to illicitly view the content of the victims' computer files have been detected frequently.

The NPA analyzed these cyberattack incidents to find out cases with a certain degree of affinity and issued an alert jointly with the NISC on November 30, 2022, to widely inform the crime methods out of concern for the expansive occurrence of data thefts.

【Fig. 14：Excerpt from the Alert】

令和4年 11 月 30 日
警察庁サイバー警察局
内閣サイバーセキュリティセンター

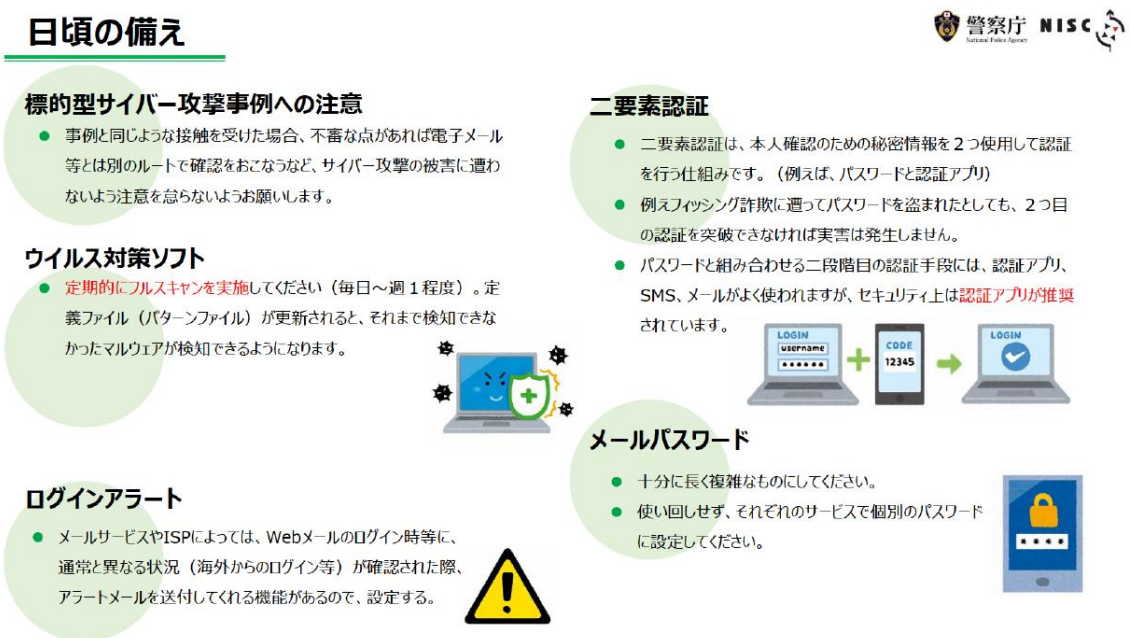
学術関係者・シンクタンク研究員等を標的としたサイバー攻撃について（注意喚起）

近年、日本国内の学術関係者、シンクタンク研究員、報道関係者等に対し、講演依頼や取材依頼等を装ったメールをやりとりする中で不正なプログラム(マルウェア)を実行させ、当該人物のやりとりするメールやコンピュータ内のファイルの内容の窃取を試みるサイバー攻撃が多数確認されています。

このサイバー攻撃に共通する特徴は以下のとおりです。

（1） 手口

- 実在する組織の社員・職員をかたり、イベントの講師、講演、取材等の依頼メールや資料・原稿等の紹介メールが送られてくる。
- 日程や内容の調整に関するやりとりのメールの中で、資料や依頼内容と称したURLリンクが本文に記載されたり、資料・原稿等という名目のファイルが添付されたりする。当該URLをクリックしたり添付ファイルを開いたりすると、マルウェアに感染する。



○ Awareness-raising against Emotet

Activities of Emotet malware which spreads mainly through email attachments had once subsided since mid-July 2022. However, the NPA detected events suggesting reprise of Emotet activities in Japan as it internally detected multiple emails in November 2022 which commanded copying attachments to the designated folder and made macros executable to infect with Emotet, and published an alert on the NPA's website.

【Fig. 15：Alert against Reprise of Emotet Activities】

令和４年11月４日
警　　察　　庁

マルウェアEmotetの活動再開に関する注意喚起について

マルウェアEmotetは、令和４年７月中旬頃から活動を停止していましたが、今般、警察庁では、Emotetメールを複数確認するなど、国内において活動が再開したとみられる事象を確認しております。

Emotetは、主にメールを感染経路としたマルウェア（不正プログラム）です。メールソフトに登録されている連絡先から知り合いのメールアドレスを盗んで使うなどして、本人作成のメールであると信じ込ませ、不審に思わず開封してしまいそうなメールの返信を装うなど巧妙化が進んでいます。感染すると、情報を盗まれる、ランサムウェア等の他のマルウェアにも感染するといった被害に遭うおそれがあります。

今回の手口では、添付ファイルを指定されたフォルダにコピーするよう指示を行い、マクロを実行可能とさせEmotetに感染させるといった特徴があります。

なお、これまで、添付ファイルのマクロを有効化した場合に、Emotetに感染させる手口や、ショートカットファイル（LNKファイル）を添付し、これをダブルクリックなどで開いた場合にEmotetに感染させる手口が確認されています。

不用意にメールの添付ファイルを開かないようにするなど、マルウェアに感染しないように注意してください。

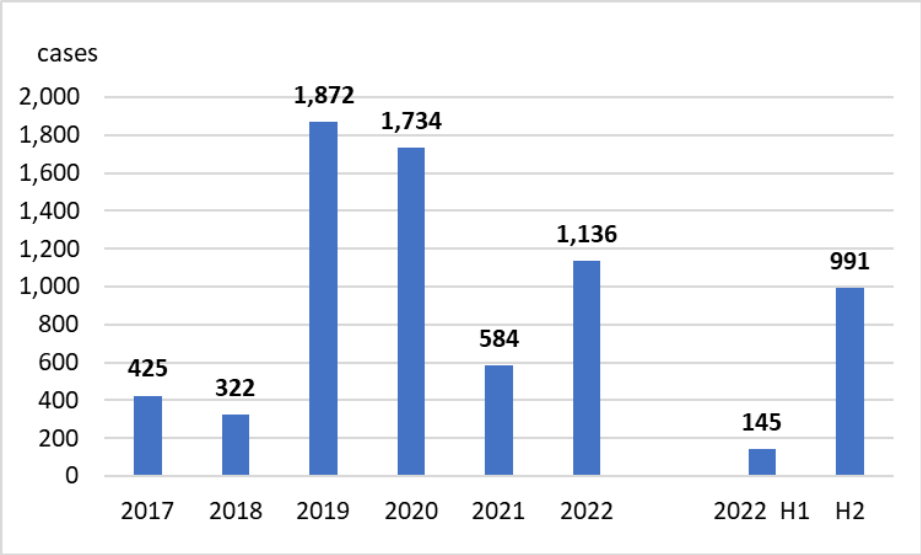
(3) Phishing-based Online Banking Fraud and Police Countermeasures

A) Online Banking Fraud

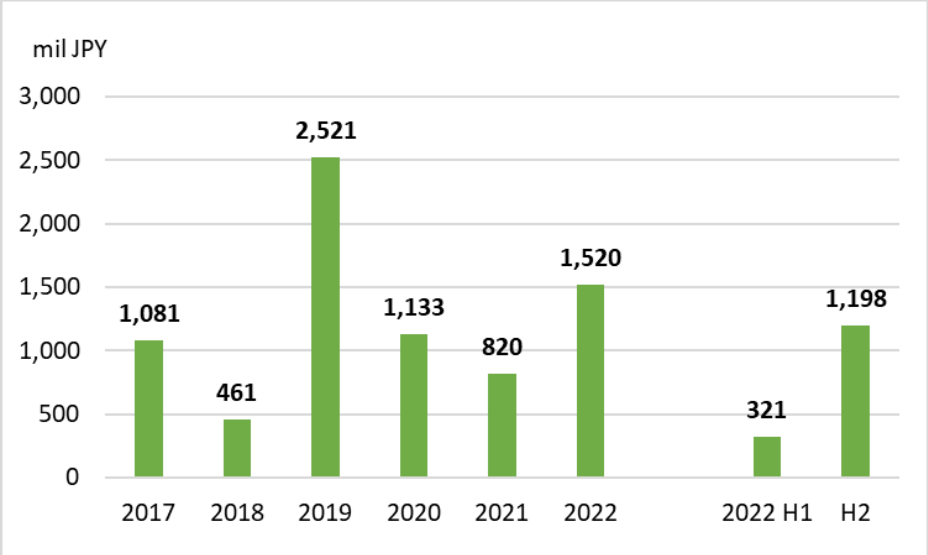
The number of online banking fraud cases increased sharply from late August to September in 2022.

In 2022, the total number of cases was 1,136 and the total amount of damages was 1,519.5 million yen, an increase in both the number of cases and the amount of damages compared to the previous year.

【Fig. 16: No. of Online Banking Fraud】



【Fig. 17: Total Loss from Online Banking Fraud】



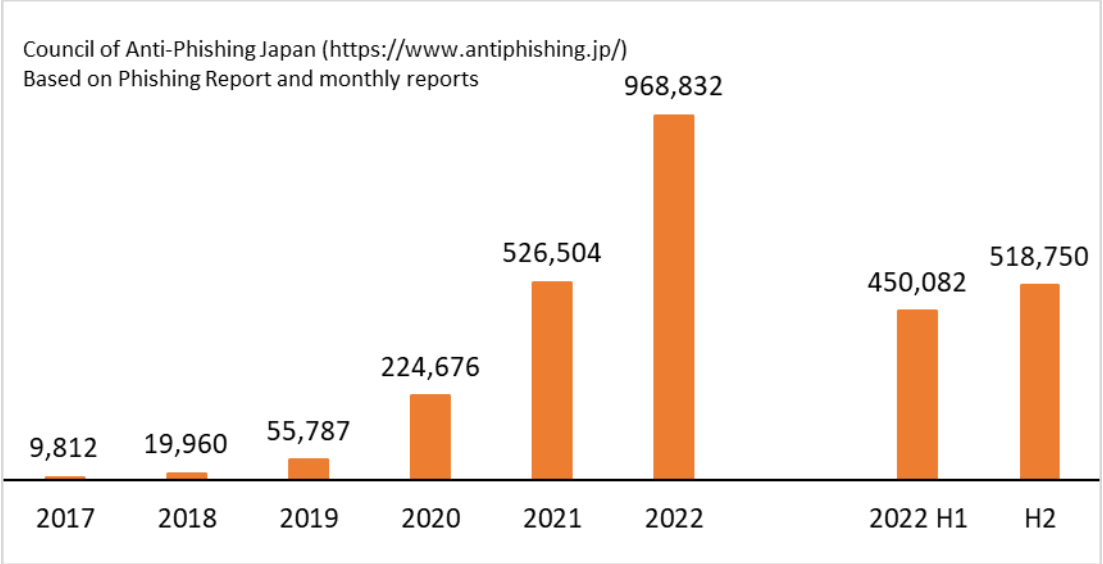
B) Damage from Phishing

Much of the cybercrime damages which surged from end-August to September 2022 was presumed to be phishing-driven and the police detected many emails designed to mislead the recipients to the fake login

websites spoofed as those of financial institutions.

According to the Council of Anti-Phishing Japan, the reported number of phishing incidents has been on the rise with 968,832 in 2022 (+442,328 vs. 2021), and the major industries spoofed in phishing were credit card and e-commerce companies.

【Fig. 18：Trend in No. of Phishing Reports】



C) Police Efforts

○ Enhancing cooperation with financial institutions

The NPA provides information on the damages caused by online banking fraud to pertinent organizations including the FSA and the Japanese Bankers Association to curb further damages.

○ Request for enhanced security against phishing

In response to the surge in damages from the apparently phishing-driven online banking fraud observed from end-August through September 2022, the NPA jointly issued alerts with the JC3 for the public not to enter personal information including IDs and passwords on the websites accessed from the links embedded in emails and short messages (SMS). In September 2022, in cooperation with the FSA, the NPA jointly requested that pertinent organizations including the Japanese Bankers Association enhance security against phishing by adopting countermeasures such as Domain-based Message Authentication, Reporting and Conformance technology (DMARC).

○ Protection against SMS phishing

The NPA participated in the cooperative effort among the major telecommunications companies to develope a system to block the

delivery of fraudulent short messages designed to mislead the recipients to phishing websites. As a result, in March, June 2022 and February 2023, three major telecom companies started providing automatic delivery blocking of the phishing short messages respectively.

- Access prevention to phishing websites

  The NPA gathers phishing websites' URLs and other relevant information detected by prefectural police organizations and shares them with the pertinent parties including the antivirus software vendors in order to prevent access to phishing websites through measures such as antivirus software alerts.

- Awareness-raising against SMS phishing

  Since August 2022, the surge in scam SMS messages and emails demanding national tax payment or warning of seizure enforcement was detected. The NPA and prefectural police organizations implemented awareness-raising campaign to prevent access phishing websites in cooperation with the National Tax Agency in September 2022.

  The NPA and the FSA also issued warning about the phishing website abusing their logos, on respective websites in October 2022.

- Partnered investigation with the JC3

  In May 2022, the police arrested a company employee (49 year-old male) for computer fraud based on information reported by JC3. He used illegally obtained credit card information of other people to reserve an accommodation through a booking website, and stayed there without paying the in December 2021.

2 Threats in Cyberspace

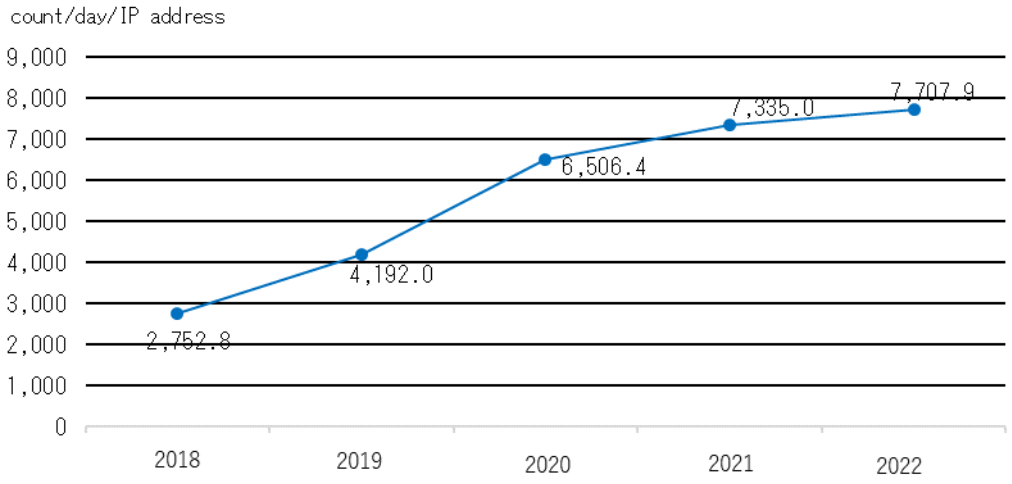
(1) Monitoring vulnerability scanning in the cyberspace

A) Unexpected connection attempts

The NPA sets up sensors on the internet to gather communication packets sent to the sensors. As these sensors do not provide any services, they usually do not receive external communication packets except for the observable ones sent indiscriminately to the unspecified number of IP addresses by cyberattackers to search for potential targets. Analysis of these communication packets facilitates understanding of the phenomena taking place on the internet e.g., vulnerability scanning of the connected devices, consequent attacks, and behaviors of the malware-infected computers.

The number of unexpected connection attempts detected at the sensors has risen to 7,707.9 per IP address per day in 2022, showing a continuous upward trend. Reasons for surge in extraordinary access attempts may include the increase of potential targets resulting from the diffusion of IoT devices, and continual evolvement of attackers' methods enabled by the advancement of technology.

【Fig. 19: No. of Unexpected Connection Attempts Detected at the Sensors】

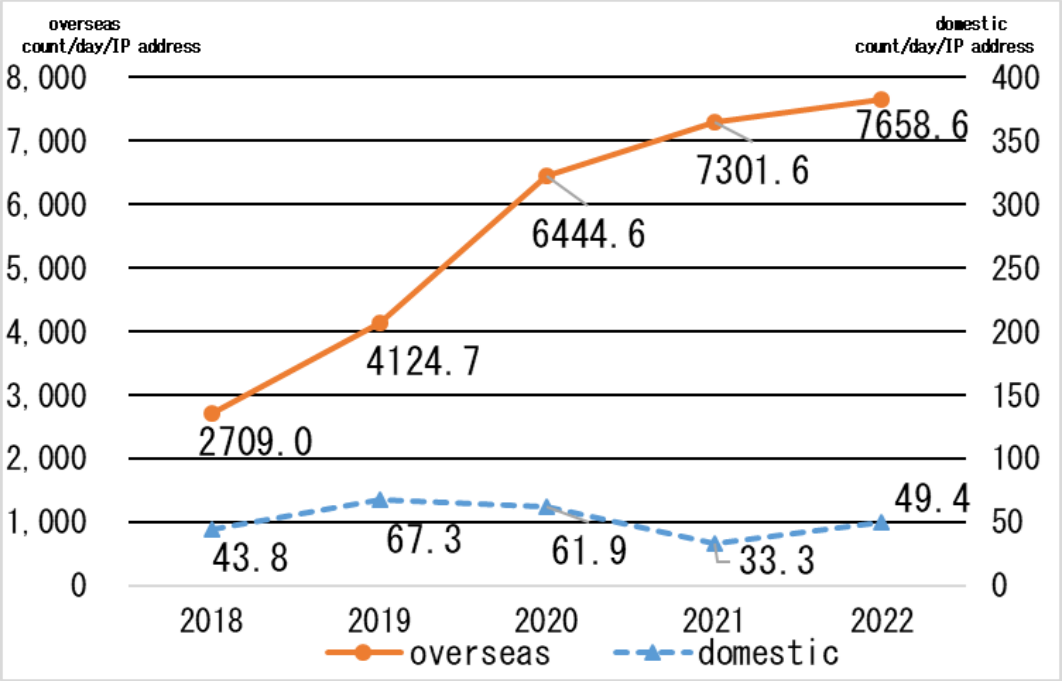


B) Major Observation

- Surge in Access from offshore

Focusing on the country/region of origin of the detected accesses shows that a high percentage of the accesses originated from overseas.

【Fig. 20: No. of Unexpected Connection Attempts by Originating IP Addresses】

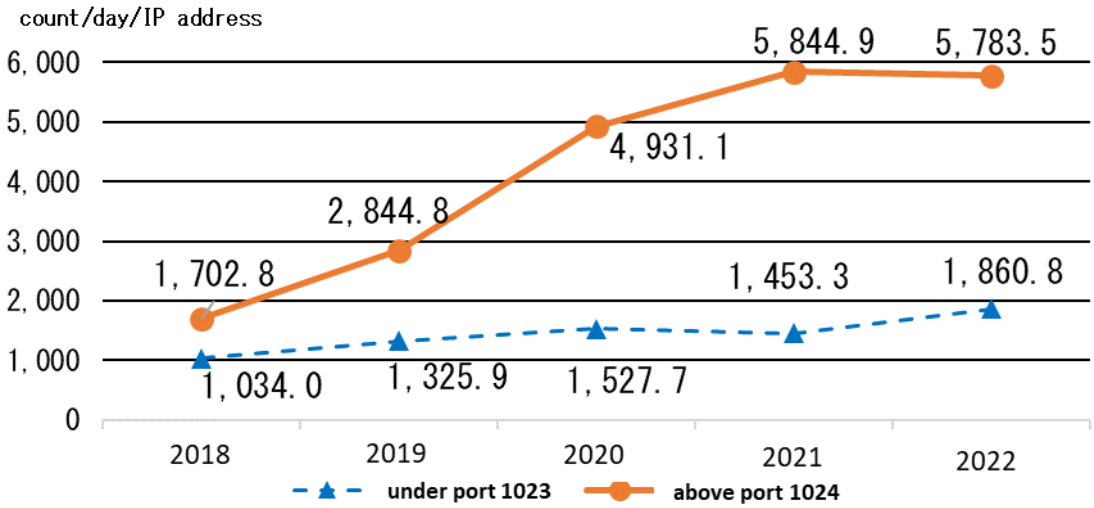


In 2022 as well, origins of the detected accesses were mostly overseas with 7,658.6 accesses per day/IP vs. 49.4 accesses per day/IP from within Japan, suggesting a continuous need for measures against the transnational threats.

○ Vulnerability search targeting IoT devices

Among the detected destination ports, a majority of the unexpected accesses were made to ports 1024 or higher, causing the high level of number of the unexpected accesses.

【Fig. 21：Trend in No. of Access Per Day/IP by Detected Destination Port】

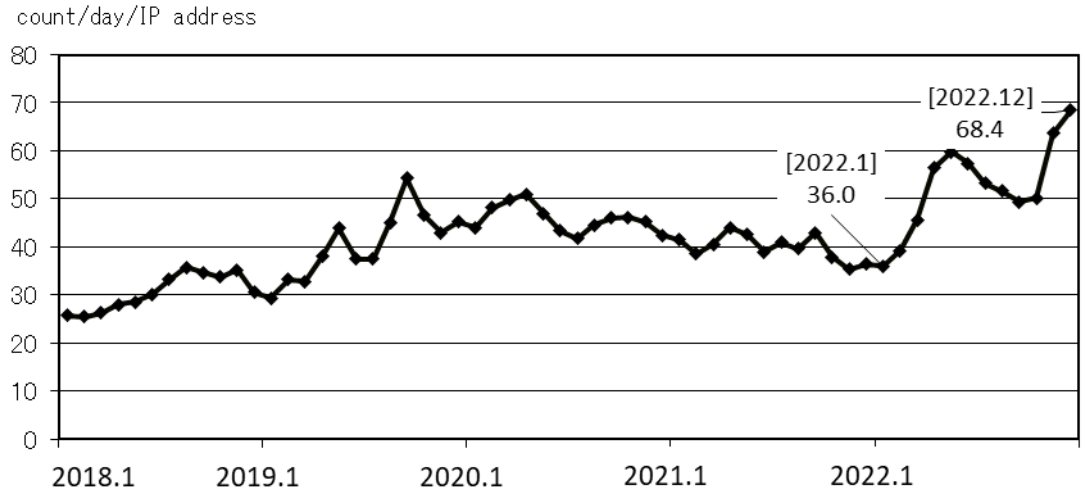


The unexpected accesses to 1024 or higher ports usually, which are used as standard ports of IoT devices, suggests that a majority of these accesses are presumably intended to explore the IoT devices with vulnerabilities or to launch cyberattacks targeting IoT devices.

○ Unexpected accesses targeting Remote Desktop services*3

From 2018 through 2022, unexpected accesses to port 3389/TCP, which is used as the standard Remote Desktop port, has been on a gradual rise. Notably in December 2022, the observed number of unexpected accesses to port 3389/TCP almost doubled vs. that in January 2022.

【Fig. 22：Trend in No. of Access to Port 3389/TCP Used by Remote Desktop】



In-depth observation of the unexpected accesses reveals a surge in number of accesses aimed to probe the operational status of Remote Desktop services, reaching the record high in 2022. Besides, unexpected accesses to explore weak credential settings were also detected, suggesting the expanding risk of being cyberattacked.

As remote work has become socially accepted, the opportunities to use Remote Desktop services are increasing. To ensure secure use of Remote Desktop services, it is important to implement appropriate security measures, such as limiting the number of access attempts to a specified time, changing IDs and passwords to strong credentials, and implementing multifactor authentication.

*3 The function to operate the desktop environment of other networked computers.

(2) Spear Phishing Attack

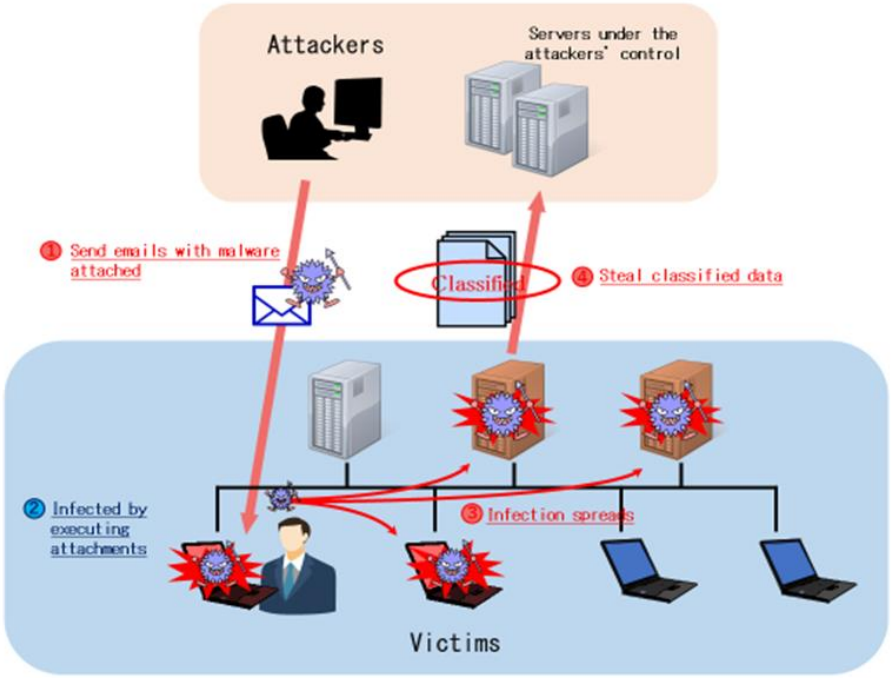
A) Observed Trends

Among the spear-phishing email attack incidents observed by the nationwide police in 2022, attachment of various types of malwares attached to the spear phishing emails were detected. The identified crime methods include sending and exchanging emails impersonating real people in order to deceive the recipients into executing malware files named with keywords of interest to the recipients.

B) Counter Cyber-intelligence Information-Sharing Network

The police and approximately 8,500 organizations nationwide (as of December 31st, 2022) with cutting-edge technologies have established the Counter Cyber-intelligence Information-Sharing Network (CCI Network) to integrate and analyze information on cyberattacks including the spear phishing attacks to provide warnings to businesses. The CCI Network also shares analyses on spear phishing attacks against government agencies provided from the NISC with businesses.

【Fig. 23: Sample Scheme of Data Theft by Spear Phishing Attack】



C) Major/Typical Incidents

The following are the spear-phishing incidents reported by businesses through the CCI Network.

In 2022, as in the previous years, sophisticated business-spoofing spear phishing emails and suspicious emails, including phishing emails

apparently intended for password theft, were continuously detected.

○ Spear phishing email attacks targeting a think tank

Spear-phishing emails directing the recipients to open the malware-embedded attachments were sent to the think tank.

○ Spear phishing email attacks targeting a pharmaceutical manufacture

Spear phishing emails were sent to the pharmaceutical manufacturer that urged the recipients to open the attachment leading to the fake login webpage and to enter the work account passwords, .

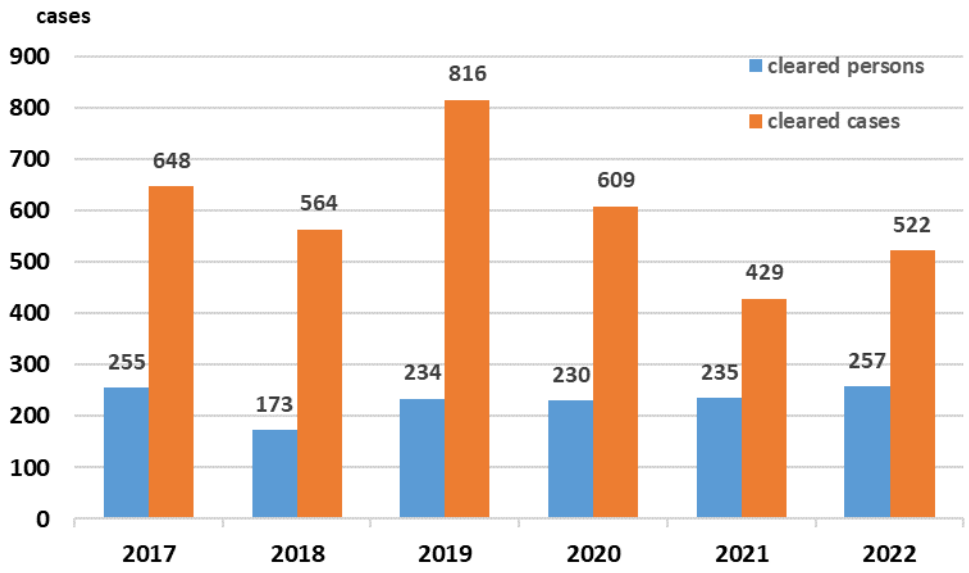
(3) Cybercrime Status

A) Violations of the Act on Prohibition of Unauthorized Computer Access*4

a. The number of cleared cases

The number of cleared cases of violations of the Act on Prohibition of Unauthorized Computer Access reached 522 in 2022, 93 cases increased from 2021.

【Fig. 24: No. of Cleared Cybercrime Cases】



*4 The following 5 acts are defined as violations of the Act on Prohibition of Unauthorized Computer Access: 1) Acts of Unauthorized Computer Access, 2) Acts of Obtaining Someone Else's Identification Code, 3) Acts of Facilitating Unauthorized Computer Access, 4) Acts of Wrongfully Storing Someone Else's Identification Code, and 5) Acts of Illicitly Requesting the Input of Identification Codes.

b. Major Observation

482 cases of all the cleared cases were classified as the identification-code-abuse type[*5] and accounted for approx. 92.3% of the total.

- ‘Exploited the authorized users’ lax password management’ was the most

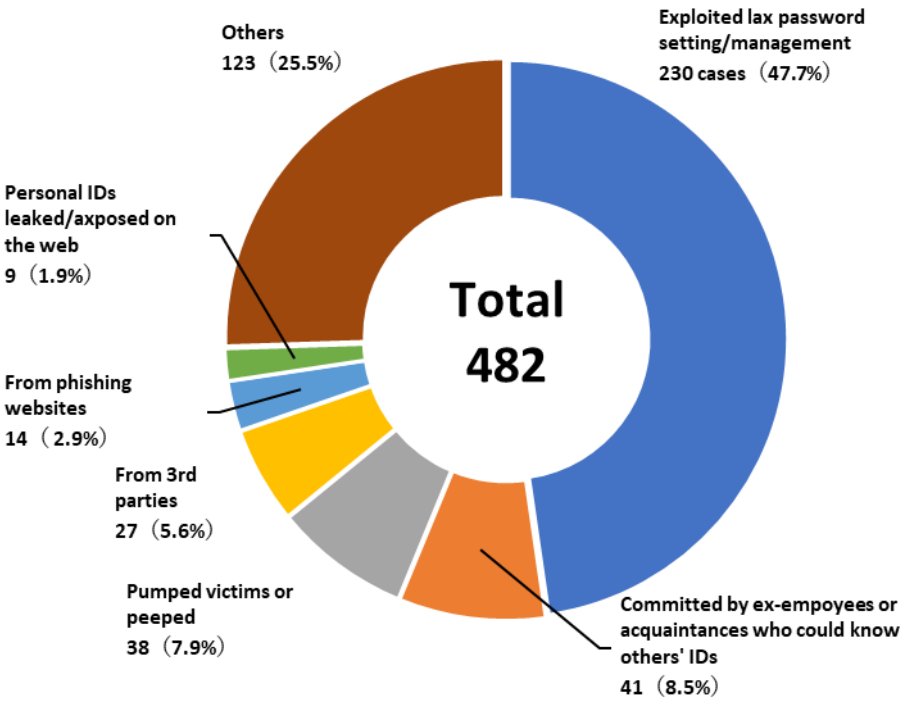
  Among the crime methods used in identity theft types of unauthorized accesses, ‘exploited the authorized users’ lax password management’ was the most prevalent with 230 cases (47.7%), followed by ‘Committed by ex-employees or acquaintances who could know others’ IDs’ with 41 cases (8.5%).

- Online game community websites were most abused

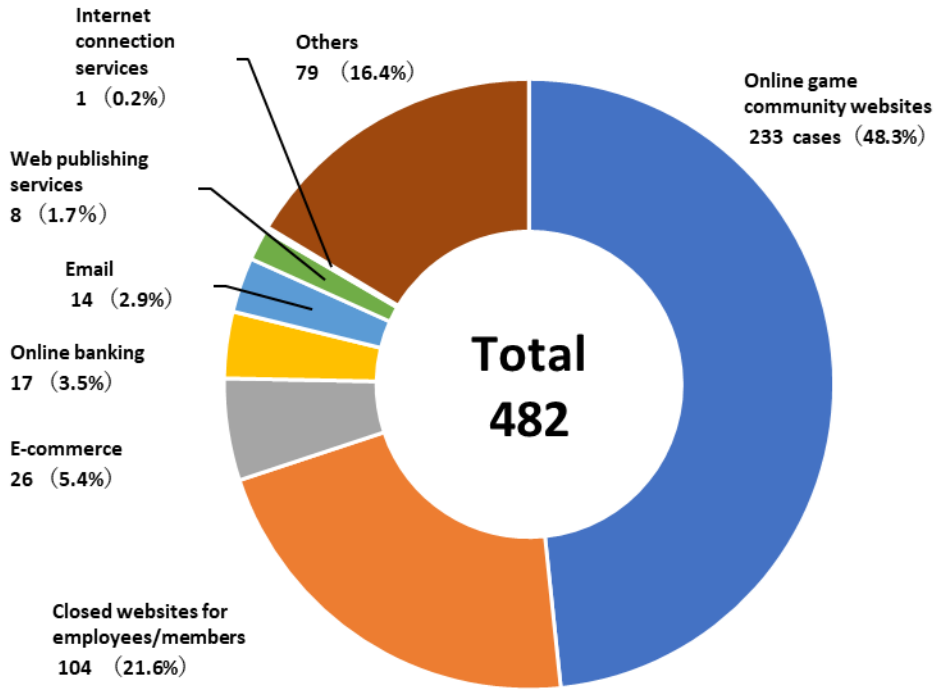
  The services most abused by suspects of the password theft-based unauthorized accesses were online game community websites with 233 incidents (48.3%), followed by ‘Closed websites for employees/members’ with 104 incidents (21.6%).

*5 Unauthorized access can be categorized as the ’identity theft’ which abuse the identifiers of others, and the ‘security hole attack’ which abuse the non-identifier data or commands to evade specific access restrictions.

【Fig. 25：No. of Cleared Cases in Unauthorized Access by Modus Operandi】



【Fig.: No. of Cleared Cases in Unauthorized Access by Service】



B) Crimes targeting computers or electromagnetic records[*6]

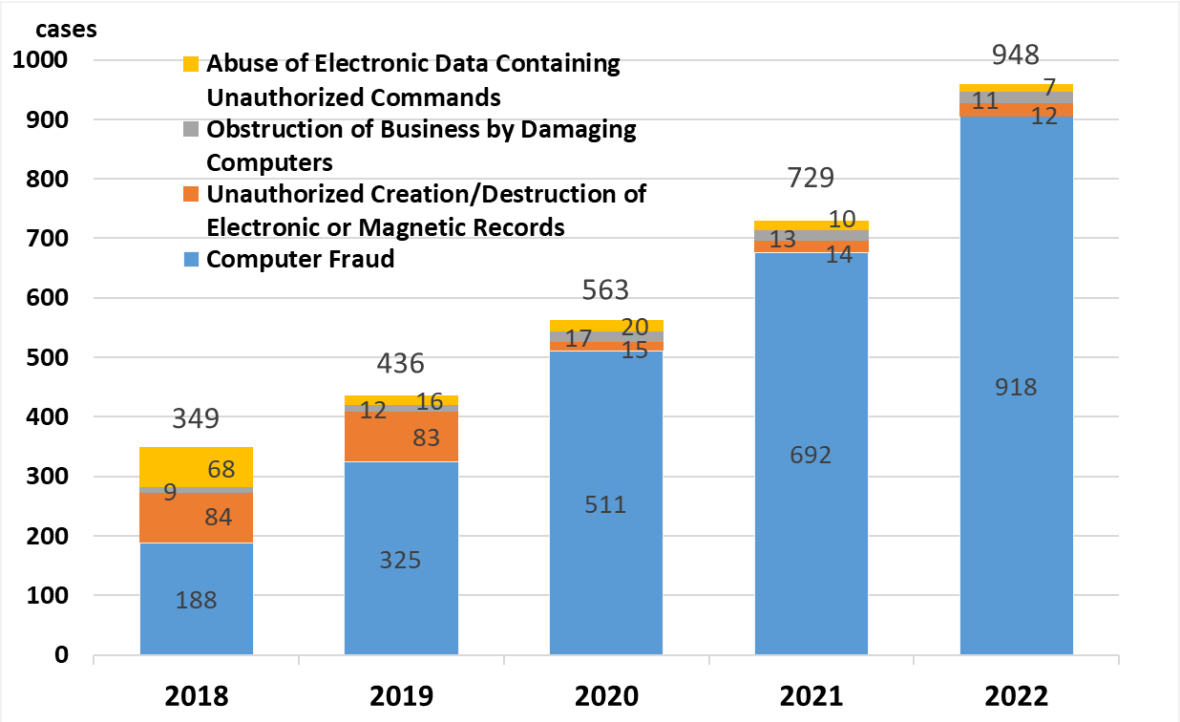
a. The number of cleared cases

The number of cleared cases regarding crimes targeting computers or electromagnetic records in 2022 was 948, increasing from 2021.

b. Major Observations

The most dominant crime type among the cleared cases in this category was computer frauds, reaching 918 cases and 96.8% of the total.

【Fig. 27: No. of Cleared Cases Targeting Computers or Electromagnetic Records】



*6 Crimes defined by the Penal Code as targeting computers or electronic records.