TLP: GREEN

2022 Threat Recap and 2023 Predictions

AhnLab Contents Planning Team

2022. 12. 15

AhnLab

Guide on Document Classification

Publications or provided content can only be used within the scope allowed for each classification as shown below.

Classification	Distribution Targets	Notices
TLP: RED	Reports only provided for certain clients and tenants	**Documents that can be only accessed by the recipient or the recipient department** Cannot be copied or distributed except by the recipient
TLP: AMBER	Reports only provided for limited clients and tenants	**Can be copied and distributed within the recipient organization (company) of reports** Must seek permission from AhnLab to use the report outside the organization, such as for educational purposes
TLP: GREEN	Reports that can be used by anyone within the service	**Can be freely used within the industry and utilized as educational materials for internal training, occupational training, and security manager training** Strictly limited from being used as presentation materials for the public
TLP: WHITE	Reports that can be freely used	Cite source Available for commercial and non-commercial uses Can produce derivative works by changing the content

Remarks

If the report includes statistics and indices, some data may be rounded, meaning that the sum of each item may not match the total.

The version information of this report is as follows:

Version	Date	Details
1.0	2022-12-15	2022 Threat Recap and 2023 Predictions

CAUTION

This report contains a number of opinions given by the analysts based on the information that has been confirmed so far. Each analyst may have a different opinion and the content of this report may change without notice if new evidence is confirmed.

Overview

The year 2022 had started with the aftermath of the Log4j vulnerability—which had occurred in December 2021—still present. It was a year with many political and cultural events scheduled, so it was predicted that cyber threats would be especially prevalent this year. Held earlier than any global event every year, CES attracts global attention as several companies demonstrate their technology and strategic direction throughout the year. At CES 2022, cybersecurity appeared as one of the five topics, and this was a good incentive to help people focus deeply on cybersecurity activities. Furthermore, we were faced with new and unexpected situations like the Russia-Ukraine war and the intense activities of cyber threat actors.

This report aims to look back at the turbulent year of 2022 to recall the major cybersecurity threats that emerged across the globe, examine our current security status, and think about ways to solve or alleviate problems.

Afterwards, the report will cover the top 5 threat predictions in 2023.

Looking Back at the Top 10 Cyber Threat Trends of 2022

1) The emergence of Log4j vulnerability, aftermath, and its remnants...

Due to Log4j's popularity as an open-source utility, its different versions have appeared over time. After the Log4j vulnerability was discovered, even getting a grasp on the situation was not easy for manufacturers and companies that used the utility, as many applications required Log4j as an essential utility. Additionally, security vulnerabilities that could be exploited continued to appear, making companies work continuously in order to respond to the problem.

In some cases, though not many, cryptocurrency miners and other related malware were installed in vulnerable servers due to the Log4j vulnerability. The most notable case was where Night Sky—a target ransomware gang—had exploited the Log4j vulnerability.

Night Sky is infamous for using a double extortion technique; After exfiltrating and encrypting the internal data of companies, they demand monetary compensation to decrypt the files. Then, they threaten their victims by informing them of the breach and that internal data will be disclosed on the dark web. These cyber attacks are on a much larger scale compared to malware that installs a cryptocurrency miner or an Infostealer that collects and leaks the PC user's data.

Night Sky has not been as exuberant as other target ransomware groups, but the fact that they exploited the Log4j security vulnerability and communicated with their victims through Rocket.Chat instead of Tor makes them noteworthy. This ransomware was not enough influence the path of other target ransomware, but this exploitation of Log4j was still a relatively significant case.

Returning to the Log4j vulnerability, most cases never reached the final malware installation stage and only went as far as to communicate with malicious servers after processing strings. This, however, increased the burden on security managers. Not only did this make it difficult to identify the attacker's motive, but there was a constant concern that another security incident might occur before a security patch could be completed.

At this point in time where guidelines have been made for individual security patches and relevant monitoring is currently being carried out thoroughly on a national and corporate level, we must look back and see if there are any problems on the individual application level. Now that companies are also applying policies that decisively block communication with servers that continuously send vulnerable strings, analyzing the state and changing trend of cybersecurity threats together will surely assist the companies in making decisions if similar cybersecurity threats occur in the future.

Moreover, we would like to thank and give a round of applause to all security managers and related departments that devoted themselves to handle the Log4j vulnerability and are carrying out their duties to this day.

2) Disclosure of target ransomware master keys and creation of a decryption tool

First, here is a table of the major target ransomware groups whose master keys were disclosed, along with their active periods.

Ransomware group	Active period
Maze	May 2019 - October 2020
Egregor	September 2020 - February 2021
Sekhmet	March 2020 and ongoing

Table. Ransomware groups that had their master keys disclosed, and their active periods

The Maze ransomware group—considered a first-generation target ransomware group—performed targeted attacks on various global and Korean companies. They were infamous for using the double extortion method where they disclosed internal information of companies on the group's public website. Despite the monetary gain and the name they obtained from active attacks, the ransomware group abruptly disappeared after announcing their retirement on October 2020. Just before their disappearance, the Egregor ransomware group had emerged, and some analysts speculate that certain members of the Maze group had joined Egregor.

The Egregor ransomware group jumped on the target ransomware bandwagon by attacking

a large bookstore franchise, 'Barnes & Noble,' as well as software development companies such as 'Crytek' and 'Ubisoft.' On February 2021, their operation was forced to cease along with Netwalker ransomware group as they were arrested by the coordinated efforts of European authorities. It is speculated that Sekhmet is the same ransomware group as Egregor because they use the same ransom note.

The master keys of ransomware previously mentioned and a decryption tool using them was created and disclosed. It was presumably a member of one of these ransomware-creating groups that had disclosed these items, who are claiming that they are unrelated to the arrest of ransomware-creating groups taking place throughout Europe and the eastern region.

Our current technology does not yet allow us to mathematically decrypt ransomware. It may be possible with quantum computing which has recently become a hot topic, but that is only if it becomes available in our daily lives without any restrictions, which unfortunately is impossible at the current moment. Regardless, waiting for the source groups or investigative agencies to disclose the master keys, as what happened in this case, would be thinking too wishfully. The master key disclosure in this case was due to someone's good intentions after a fair amount of time had passed since the retirement or the arrest of ransomware groups. The number of times master keys have ever been disclosed can be counted on one hand.

The disclosure of the master key and decryption tool for Maze ransomware group is enough to make it a meaningful incident since Maze was the first-generation target ransomware group that caused massive damage throughout the world. If there are companies or institutes that have been harmed by the ransomware of these groups and need their files to be decrypted, then we recommend using this decryption tool. It should be noted that a ransom note is required for decryption.

3) Polarization of Ransomware

There are ransomware that are so rampant that we can recognize them by their names; LockBit is one of them. After going through several evolutions, LockBit 3.0 has become a targeted ransomware that is capable of triple threats: file encryption, disclosing stolen information, and DDoS attacks.

As the name 'targeted' ransomware suggests, now there are rarely any cases of ransomware attacks without intentions. People must not forget that malware attacks are always carried

out with carefully calculated intentions and thorough preparation.

The LockBit 3.0 attack case article posted on AhnLab ASEC blog indicates that the threat actor distributed malicious DOC files disguised as job applications. The files were cleverly disguised using people's names like 'Lim Gyu Min.docx' and 'Jeon Chae Rin.docx'.

This attack pattern alone makes it clear that this attack of theirs was not accidental. These types of attacks mostly adhere to the following procedure: breach either the company's internal network or a victim's computer > install malware > distribute additional malware or attack tools according to the intent > steal admin account > delete recovery image and terminate and service to interfere with system recovery > achieve goal. It can easily be inferred that these attackers approach their targets with clear intent, considering the actions they take after successfully accessing the internal networks of companies or organizations.

One thing that should be noted is that the proportion of creating new ransomware has been decreasing by the year. A type of polarization is happening in the ransomware market as the average creation and distribution of malware do not bring large profits now. On one hand, infamous and large-scale targeted ransomware make profit by actively attacking government agencies and major companies. On the other hand, numerous other ransomware disappear after only one or two attacks. The total number of ransomware are in a decreasing trend, but we must remember that the number of attacks carried out by top-ranking targeted ransomware, which are the actual threats, are not lowering the attack level.

4) Attackers determined to disable security systems

Disabling the security systems of PCs and servers is similar to intruders removing the guards in movies. Guards are tasked to stop unknown and suspicious people, so in this regard, their dynamics are similar.

The battle between attackers and defenders continues to this very day in the realm of cybersecurity and continuous development of technology. Anti-virus (AV) products remove files that are recognized as malware from the OS, while attackers attempt various methods to prevent AV products from functioning properly.

Until now, attackers were prevented from uninstalling AV products as that would prompt the input of a CAPTCHA code. However, various attempts to disable security systems have been

identified recently such as the direct involvement of attackers. Here are two examples.

First, by looking at the Analysis Report on Lazarus Group's Rootkit Attack Using BYOVD published last September, it can be noted that the attacker exploited an older version of INITECH process to initially breach a company before downloading and executing Rootkit malware from the attacker's server. Rootkit malware exploited vulnerable driver kernel modules to directly read and write from the kernel memory area. It then disabled all monitoring systems inside the OS including AV software.

Another instance is the ransomware making a name for itself as a 'Korean type' ransomware, Gwisin ransomware. This malware avoids AV products by encrypting files after rebooting the PC in safe mode. Only the bare minimum services such as default Windows drivers become active in safe mode, so the ransomware is able to bypass the detection of AV products as well.

Therefore, in this situation where attackers are doing their utmost to disable security systems, the most optimal action that defenders can take is to monitor their security systems constantly and not provide attackers an opportunity to attack. Not only is it crucial to be aware of the attack trends, but it is also important to actively assess one's current situation and respond accordingly. We must stand against attackers who are determined to disable our security systems with our own persistence.

5) International investigation to arrest cyber threat actors

It would not be an exaggeration to say that the news of cyber threat actors being arrested started a year ago with the arrest of an accomplice of the CLOP ransomware in Korea. With this arrest as the trigger, another arrest followed in Ukraine from an international investigation. In October 2021 threat actors related to LockerGoga ransomware and other various cyber-attacks were also arrested.

Recent news reported that cybercriminals from an unidentified ransomware group were arrested, who had caused around one million dollars' worth of damage in 50 countries. Through the active efforts of Korea and other main countries in the West, cybercriminals are continuously being investigated and arrested.

Last January, it became known that the REvil ransomware group, which was once known as

BlueCrab in Russia and Sodinokibi in other countries, was arrested. Cybercriminals being arrested in Russia is considerably unprecedented news. This could have been a strategic decision by Russia where they deemed cooperation with an international investigation would be more beneficial than protecting their own people. Hence, there is a possibility that this is a 'cover' to make it seem like the DarkSide and REvil ransomware group are unrelated to Russia.

Given the precedents between USA and Russia where neither had acknowledged nor cooperated for cyber threats, Russia's decision has given us a look into what their future strategic decisions may be.

6) Activities of cyber-attack groups with national support

Korea held its 20th presidential election last March. At the time, various countries watched closely from their own areas to see how cyber-attacks would unfold in Korea with its 'big event'. Currently, countries in political or military opposition with Korea have little to gain by performing a cyber attack at such special times. However, it appears that indirect methods were devised to acquire information from various areas in order to prepare for various situations.

As part, attacks continue to occur where document files with malicious scripts inserted are sent to a limited number of recipients. The malicious scripts used in these attacks are obfuscated to prevent normal users from being able to read them. This type of attack works by prompting the user to open the document file, which activates the malicious scripts. Then sensitive information from the user's PC is collected and leaked along with the information about the PC itself. This could be interpreted as the attackers' way of clearly distinguishing their targets.

AhnLab discussed an example of this method in a recent ASEC blog post, Malicious Word Document Being Distributed in Disguise of a News Survey. The malicious Word document disguised itself as a CNA Singaporean TV program interview under the filename, 'CNA[Q].doc' and targeted individuals related to North Korea. The moment the user starts typing, a message box appears, requiring the user to enable macro to continue typing. Users would then click the 'Enable Content' button to fill in the answers in the document, which executes the VBA macro embedded in the file.

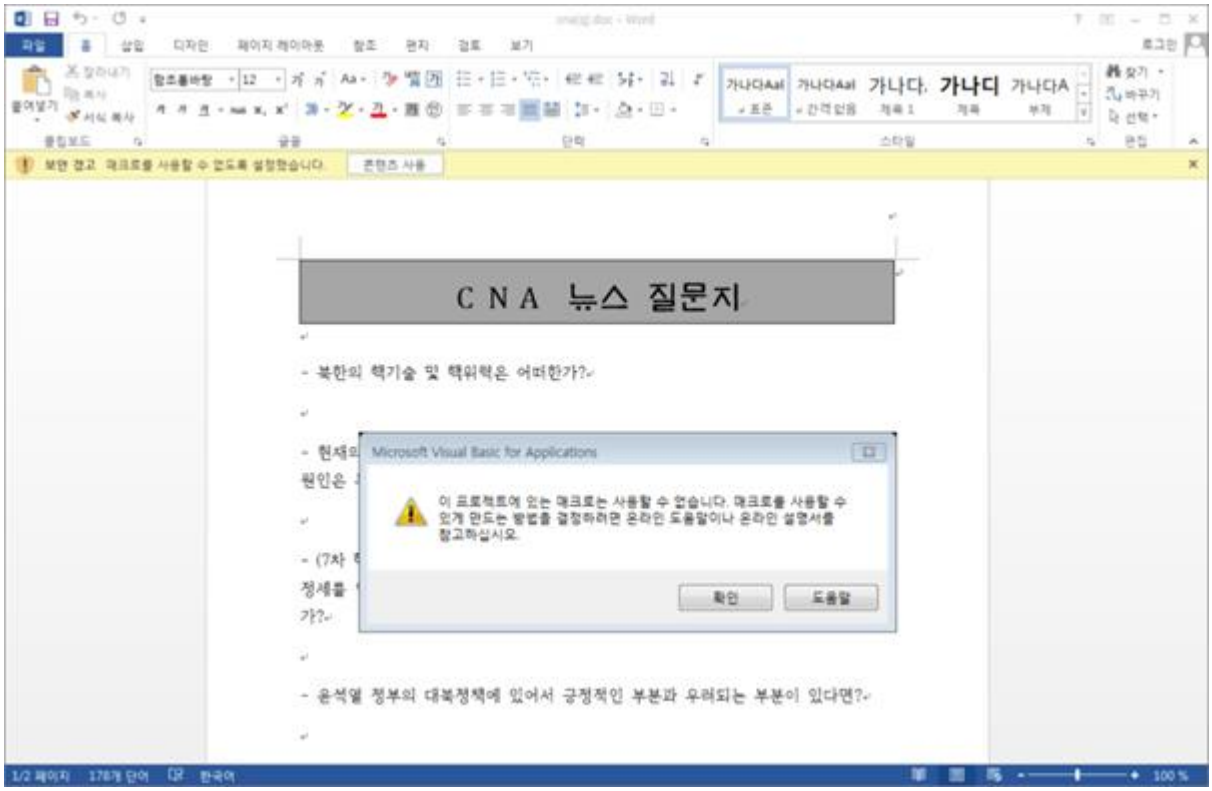

Figure. Word document content and message box generated upon typing

This type of attack is similar to that of Infostealer, which collects and leaks user information. However, there is an important difference that nationally supported cyber-attack groups have clear goals as seen in this example. The industrial groups that are currently the main targets of these attacks include political, unification, diplomacy, aerospace, defense, energy, and renewable energy sectors. Therefore, organizations handling key national technology or main company technology and materials must be especially vigilant.

7) Multi-factor authentication under spotlight; what is left for us to think about?

In May 2021, there was an incident where although the targeted non-governmental organization (NGO) had set multi-factor authentication (MFA) as their default protocol, a Russian cybercriminal abused a misconfigured account to register a new device for MFA to access the victim's network. During this process, the operator exploited the Windows print spooler vulnerability, 'Print Nightmare (CVE-2021-34527),' to execute codes with system privileges.

Since MFA verifies users through two or more authorized devices, it is undeniably a type of defense that attackers find difficult to handle. However, many concerns have arisen as incidents have occurred where MFA was circumvented. Naturally, MFA cannot be said to be a 100% perfect security system that blocks all attacks, but if used correctly, it can make attacker actions inconvenient and prevent them from easily achieving their intended goals.
Therefore, rather than suspecting and not utilizing MFA because of such security breaches, the appropriate approach would be to properly review the configuration policy to prevent chances of exploitation. Additionally, risk factors can be minimized by periodically checking and removing user accounts that no longer exist, and quickly applying patches for known security vulnerabilities. If these measures are carried out continuously, the effectiveness of MFA can be maximized, allowing users to focus on their business in safer environments.

8) Info is for stealing

Infostealer is an information-stealing malware that aims to seize user credentials such as cryptocurrency wallet addresses and files that are saved in programs like web browsers and email clients. According to the Q3 2022 ASEC Report, Infostealer makes up 55.1% of all malware that had been distributed during that time.

Recent Infostealer trends show that they are continuously changing and working in connection with each other. A typical example of this would be Emotet, an online banking malware. Quickly distributed through its connection with Trickbot, Emotet had appeared and disappeared frequently. However, after its infrastructure was seized by authorities in early 2021, it subsided.

Then nine months later at the end of 2021, Emotet halted its previous connection with bot-type malware and returned with its own spam-sending feature and the ability to propagate itself. In addition, Emotet's original information collecting and leaking features were also improved. It would be reasonable to categorize Emotet as an Infostealer, which has now emerged as a major malware group since last year. AhnLab will also continue to closely monitor its future activities.

9) Vulnerability attacks on IoT devices

Along with endless vulnerability attacks against various IoT devices connected to the network, rampant cyber-attacks are being observed exploiting vulnerabilities of routers used by many customers around the world. Considering that a single router can control all devices that have wired or wireless Internet connection, the impact may be significant.

Then here comes the question: What can attackers gain by taking control of routers? They can intercept various personal information entered by users and create a phishing website disguised as a normal webpage to induce user access. In addition, stolen routers can be used to carry out DDoS attacks on random targets that are connected to the network. Mirai and Tsunami are some of the main examples of malware that attack IoT devices.

To gain security against these sorts of attacks, security vulnerabilities of primary attack targets (wired and wireless routers) must be patched, and users must be wary of DDoS attacks from compromised routers and Brute Force attacks on login accounts. Furthermore, damage caused by threats can be minimized through continuous management of login accounts. Unused accounts should be removed whenever possible, and a security policy that only allows specific users to access devices should be established.

10) Miners and their own economy

Miner is a common name given to applications developed for the purpose of mining cryptocurrency. Its official name is CoinMiner but is called Miner for short.

When interest in cryptocurrency was high in early 2018, cryptojacking malware caused immense damage through web browsers. Although interest in crypto miners has declined this year due to the accelerated economic downturn, related malware are still being produced and distributed.

Rather, miners have recently been expanding their reach as cases has appeared of them working with InfoStealer to collect and leak user credentials. As explained previously, data stolen by Infostealer includes user account credentials saved to web browsers or applications along with cryptocurrency wallet addresses. To add on, malware with Clipper functions have also appeared, which replace the cryptocurrency wallet address with the attacker's address.

For reference, CryptoShuffler malware back in 2017 had the feature to switch cryptocurrency wallet addresses, and this function was remade and upgraded in the form of Clipper. Unlike CryptoShuffler which had a file size of tens of megabytes due to the wallet address inside the malware, Clipper reduced its size considerably by identifying the related cryptocurrency through the internal calculation structure and replacing it with the attacker's address. From the attackers' perspective, this is a malware that combines the advantages of various other malware with its reduced file size, ability to target multiple cryptocurrency wallets, Infostealer features of stealing and leaking information, and even the ability to mine like a CoinMiner.

Until now, people have believed that Miners could only go as far as to deplete the resources of companies and groups. However, they are active and continuously being produced in their own economic structure. They have evolved from past versions where they could only perform simple features, and are now capable of collecting and leaking important information and stealing cryptocurrency wallet addresses. Companies and organizations must be aware of these changes and actively monitor their internal infrastructure for mining activities.

Prediction of Top 5 Cyber Threat Trends of 2023 by AhnLab

Last year was a year in which cybersecurity became more important than ever before. There had been a significant increase in new and variant ransomware attacks and nationally supported hacking group activities where corporations and government institutions were targeted. This trend will most likely continue in 2023.
Concerning such matters, Keon-woo Kim, Head of AhnLab Security Emergency Response Center (ASEC), stated, “rather than searching for a single universal key that solves all security issues, a multi-dimensional approach is required from companies and users as hackers will continue to maximize the effectiveness of their attacks by making use of every vulnerability at their disposal.”

This report examines the outlook on the top five cybersecurity threats of 2023 that those in the IT field and security industries must know.

AhnLab’s outlook on the top five cybersecurity threats of 2023 is as follows.

1) Ransomware Groups' Strategy: "Quality Over Quantity"

The emergence of new ransomware has been recently declining, and it is expected that ransomware groups will pursue a "Quality Over Quantity" approach where they will aim to gain maximum profit and impact through minimized attacks. To achieve this goal, attack groups will first take control of a company’s core infrastructure and impose "multiple threats" by persistently attacking a single target with information leakage, ransomware infection, and DDoS (Distributed Denial of Service) attacks. Furthermore, it is also possible to speculate that the pressure of global-scale investigations and arrests of ransomware groups will instigate cybercriminals to retire after initiating mass attacks. Companies must therefore utilize their TI (Threat Intelligence) as well as establish basic security systems to identify recent attack trends and vulnerabilities.

2) 'Parasitic' Attack, Resulting in Long-term Leakage of Key

Company Information, Becomes the Dominant Trend

2022 was rampant with attacks on virtual asset exchanges, major companies, and public institutions that had key assets such as technology and personal information. Some attack groups even publicized their accomplishments. Since attackers value their return on investments, attempts to steal key technology and assets of major institutions and companies will continue. It is expected that their methods will become even more secretive and advanced. In particular, unlike in the past when attackers destroyed or publicized systems for pretentious purposes, it is expected that "parasitic" attacks, which take control of infrastructures and carry out long-term leakage of key technology or sensitive information, will rise as the majority. Attack methods may also become diversified with methods such as screen capturing, audio and video recording, and also the collection of account credentials. Therefore, companies should establish an integrated security framework that can respond to all system areas.

3) Discovery and Constant Exploitation of Highly Impactful "Jackpot" Vulnerabilities

Last year, the BYOVD (Bring Your Own Vulnerable Driver) attack technique which exploited vulnerable drivers that were still able to access key system privileges was discovered. This year, attackers will continue to utilize highly impactful 'jackpot' vulnerabilities for their attacks regardless of whether they're on PC, mobile, cloud, or OT (Operational Technology). They may exploit software that are no longer supported by security patches for information leakage and ransomware attacks. Unpatched vulnerabilities that attackers purchase from the dark web or discover by themselves may also be abused for the same purposes. Those in charge of company security must therefore apply security patches regularly and delete unused programs.

4) Attacks on Supply Chains Spread to Mobile Environment

Until now, attackers had focused their attacks on supply chains centralized within PC software; however, these attacks may also spread due to the increase in money transactions and the use of personal information within mobile environments. Instead of using the conventional method of generating and distributing malware, attackers are likely to lean toward infiltration at the initial stage of app creation through hacking development tools and developers that

can register apps to normal app markets. Furthermore, they may attempt to inject malware during either the app distribution or update stage. Attackers may also use stolen mobile app certificates to create and distribute applications. Thus, mobile service providers must take the matter of security into account during their development and distribution stages while also implementing threat detection and response systems for key assets.

5) Intensifying Attacks Against Virtual Asset Wallets of Individuals

With massive cryptocurrency exchanges and major blockchain services being hacked, more users are transferring their virtual assets, such as coins and NFTs (Non-fungible Tokens), to their personal wallets. As such, attacks aiming to target virtual asset wallets of individuals are also expected to increase this year. Most users record and save seed syntaxes or mnemonic keys, which are used for account ownership authentication and wallet recovery, as images, emails, or memos on their mobile phones because they are too difficult to memorize as the former is a combination of random words and the latter is a configuration of 12 or 24 words. Attackers are likely to expand their distribution of information leakage malware, phishing websites, and apps that disguise themselves as famous virtual asset wallets to steal credentials of mnemonic keys and wallet accounts. Personal wallet users must therefore store their seed syntaxes and mnemonic keys in safe places and use wallets that are free from the risk of key loss. Also, users must thoroughly check whether the wallet they are trying to make a wire transfer to has been involved in criminal activities.

To prevent such security threats, companies must implement the following preventative measures: △regularly inspecting security and applying patches for internal PCs, OS, software, and websites, △utilizing security solutions and services and educating executives and staff members about security, △monitoring verification for admin accounts, and △implementing multi-factor authentication (MFA).

There are several security regulations that individuals need to strictly follow to prevent such security threats: △Refraining from opening attachments and URLs from suspicious emails, △Downloading content and software from official paths, △Applying the latest security patches to software, OS, and Internet browsers, △Using two-factor authentication for logins, and △Updating anti-malware to the latest version and executing the real-time scan feature.

More security, More freedom

AhnLab, Inc.

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea
Tel : +82 31 722 8000 | Fax : +82 31 722 8901
www.ahnlab.com
www.asec.ahnlab.com/en

About ASEC

AhnLab Security Emergency Response Center(ASEC), through our team of highly skilled cyber threat analysts and incident responders, delivers timely and accurate threat intelligence and state-of-the-art response on a global scale. The ASEC provides the most contextual and relevant threat intelligence backed by our groundbreaking research on malware, vulnerabilities, and threat actors to help the global community stay ahead of evolving cyber-attacks.

About AhnLab

AhnLab is a leading cybersecurity company with a reliable reputation for delivering advanced cyber threat intelligence and threat detection and response (TDR) capabilities with cutting-edge technology. We offer a cybersecurity platform comprised of purpose-built products securing endpoint, network, and cloud, which ensures extended threat visibility, actionable insight, and optimal response. Our best-in-class researchers and development professionals are always fully committed to bringing our security offerings to the next level and future-proofing our customers' business innovation against cyber risks.

AhnLab