TLP: GREEN

2022 Cybersecurity Threat Outlook: What to Watch Out for

AhnLab Contents Planning Team

2022. 01. 04

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	2022-01-04	2022 Cybersecurity Threat Outlook: What to Watch Out for

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 2021 was quite an eventful year for cybersecurity threats. Major cybersecurity issues, including 'DarkSide Ransomware' that attacked the U.S. Colonial Pipeline and 'Log4j vulnerability' that continues to threaten enterprise users till this very moment, left many cautious of cybersecurity threats.

What security issues should users watch out for in the new year? Let's take a closer look at the top 5 cybersecurity threats in 2022.

2022 Cybersecurity Threat Outlook: What to Watch Out for

AhnLab announced the 'Top 5 Cybersecurity Threats in 2022.' The major security threats for 2022 predicted by AhnLab are the following: ▲Exploit attacks using political and social events ▲ Increase of targeted attacks against IoT environments ▲ Nation-state threat groups targeting advanced technologies ▲ Ransomware group using advanced attack methods ▲Discovery of new attack points.

Figure 1. Top 5 Cybersecurity Threats in 2022

Chyang-kyu Han, Head of AhnLab Security Emergency response Center (ASEC) said, "As various fields are undergoing digital transformation, attackers will focus on exploiting the rapidly changing IT environment and the issues that follow." He also added that as "IT technologies are becoming part of our life, attack targets will expand and the attack methods will become more advanced, meaning both individuals and organizations must adhere to security advisories in everyday life to protect important assets."

Let's dive deep into each cybersecurity threat mentioned in Figure 1.

1) Exploit Attacks Using Political and Social Events

The Year 2022 has a number of global sport (Beijing Winter Olympics in February and Qatar World Cup in November) and political events, including the presidential election in Korea. Such major social events have been traditionally exploited for cyber-attacks. This year will be no exception; attackers will deploy social engineering attacks using attack methods, such as spear phishing* email and smishing.

As there is also a possibility of a cyber-attack group attacking to cause confusion in the society while people are being drawn to huge events, users should always take caution not to open suspicious attached files of emails and not run texts.
*Spear phishing: A type of targeted phishing attack that sends malicious emails to a specific person (or organizations) instead of mass distribution.

2) Increase of Targeted Attacks Against IoT Environments

As remote working has become more common over the last two years, attacks targeting people working from home have increased. In 2022, there will also be attacks that target IoT environments. With the availability of fast and stable 5G-based network, there will be an increase in the network connection points, such as wall pads, smart speakers, and home cameras, thus the increase of attack surface.

Like the recent wall pad video leak incident, attackers in 2022 might target new IoT products or services used in daily life and perform attacks, such as stealing information or remote control. Individual users should keep basic security rules, such as changing the default password assigned to IoT devices, while institutions and companies should establish security policies and come up with response methods that take into consideration of the shifting network environment.

3) Nation-State Threat Groups Targeting Advanced Technologies

Year 2021 saw continued hacking attempts targeting major national research institutions, and the trend of nationally supported organizations aimed at cutting-edge technologies is expected to continue in 2022 as well. Besides the defense industry that works for national security, cyber-attacks may also target social infrastructures, OT (Operation Technology) environments, such as smart factories, and technology-intensive industries. Technology-intensive industries include machinery, automobile, and bio industry.

The bio industry that is gaining importance in the pandemic era and the aerospace industry might become another target for threat groups. Relevant institutions and companies should be on the lookout for security trends and heighten the overall security level by introducing security solutions and carry out relevant security trainings.

4) Ransomware Group Using Advanced Attack Methods

Many nations in 2021 cooperated in global investigations to prevent ransomware damage to achieve the desired result. Yet the ransomware attack groups are becoming even more advanced to avoid getting caught. First of all, attackers will continue with their exclusive operations, such as strengthening the requirement to join their groups. At the same time, they will be more likely to transition into small-scale groups at an accelerated level to avoid getting tracked by judicial agencies.

The aspects of ransomware attacks are becoming more diversified as well. Attack groups are now going beyond the traditional strategy of mass ransomware distribution to obtain ransoms and began to target companies that have valuable information. The change of strategy was to threating to release the stolen data in return for higher ransom. As the trend is becoing increasingly popular, companies and organizations should review their ransomware defense strategy based on the latest ransomware attack methods and consider adopting threat intelligence services and advanced threat defense solutions.

5) Discovery of New Attack Points

Like the recently discovered 'Log4j' vulnerability, attack groups will attempt to exploirt vulnerabilities that are not well known but exist in most online solutions. Also, as

cryptocurrency and NFT (Non-Fungible Token) are gaining popularity, they will be targeted for attacks.

There might be attacks that collect or leak cryptocurrency wallet addresses saved in PCs, and even attempts to inflict monetary damage in NFT transactions by exploiting the existing malware feature of sending cryptocurrency to a wallet address set by the attacker. To prevent such cases, it is essential to adhere to basic security advisories, such as not opening suspicious URLs or attached files from emails, and keeping the security patches of softwares/programs up-to-date.

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