Security Trends

2020 Reviews

2021 Predictions

AhnLab

Security Trends

2020 Threat Review

Top 5 Security Threat Trends for 2020

AhnLab

01
Ransomware:
Familiar Attacks, Substantial Damage

Ransomware has always been included in threat reports and threat predictions in the recent years. Due to the widespread of ransomware, it has now become very well-known. Yet, ransomware manages to continue its high-stake operation. In 2020, there was a significant increase in the number of targeted ransomware attacks that stole sensitive, internal information while threatening to release the information to other sources before encrypting the data.
The two notable cases of worldwide ransomware attacks from last year are as follows:

A. Worldwide Ransomware Attacks by Maze Ransomware

Maze Ransomware launched targeted attacks on various companies worldwide. The threat group stole the company's internal data and threatened for money. If the victim did not pay the requested ransom, the attackers would release the stolen data on their website. The attack ended in early November 2020 when the threat group announced their retirement. In return, they demanded that those who want their data deleted from their website should contact them within the stated period.

B. DoppelPaymer Ransomware that Took a Patient's Life

In September 2020, ransomware attacks toward the Dusseldorf University Hospital in Germany stopped medical systems, causing the death of an emergency patient. A total of 30 servers within the hospital were impacted by the ransomware, restricting most medical services. This incident has led to delayed treatment and death of an emergency patient. After the investigation, the German investigating agency announced the ransomware responsible for the attack was DoppelPaymer. The attacker may not have intended to kill a patient, but this incident suggested that lives could also be in danger if a critical infrastructure could be infected by malware, such as ransomware.

© 2021 AhnLab, Inc. All rights reserved.

02
Nation-State Attacks

In 2020 several Nation-State hacking groups have attempted to hack into global corporations, government agencies, universities, and individuals for their country's interests. For some corporations, their employees' account information and internal data were leaked, and for individuals cryptocurrencies were stolen.

COVID-19 is closely related to the trend of these Nation-State attacks. With a sudden increase in the number of confirmed COVID-19 cases and multinational pharmaceutical companies competing with one another to develop the vaccine, Nation-State groups were not hesitant in attempting to attack relevant organizations, such as government agencies and pharmaceutical companies.

The EMA (European Medicines Agency) has been the main target of many Nation-State hackers due to the fact that they have COVID-19 vaccine-related documents. Also, cases of illegal access to COVID-19 vaccine technology, research results, and cold chain (low-temperature distribution system) by Nation-State groups have been continuously reported.

HWP documents, which have consistently been targeted by global hacking organizations, became less vulnerable than the previous year. This is because the ghost script vulnerabilities, which attackers exploited, were patched. This must've led the hackers to assume that the attacks exploiting this specific vulnerability was no longer effective. Despite the decrease in the exploitation of HWP documents, script malware, such as Macro, PowerShell, WSF, and VBS, has increased as an alternative attack method.

© 2021 AhnLab, Inc. All rights reserved.

03
Advanced **Phishing Attacks**

Phishing attacks distributing malware have advanced to the point where it is hard to recognize what is real and fake. Malicious websites would disguise as normal portal sites with login screens that look almost like the original websites to steal account credentials from the victims. The screen in the past looked quite awkward, but now they have designed it close enough to make it difficult to distinguish, even for experts. These phishing websites send information to the server once the user enters their account information and then redirects them to the normal websites to avoid any suspicion.

The same concept also applies to emails. They mainly consist of task-related information, such as ‘system maintenance info,’ ‘account access restriction,’ and ‘order forms,’ to trick users into downloading or executing malicious links and attachments without any suspicion. In the past, spam emails were sent to random individuals but recently reported cases show that the mails are now customized for each user, such as being written in Korean or containing contents related to the user. This shows that the malware developers are conducting more sophisticated phishing attacks to increase the success rate of their attacks.

© 2021 AhnLab, Inc. All rights reserved.

04
Mass Distribution of **Botnet Malware**

Botnet malware, which is a type of malware like Emotet, was distributed in large numbers worldwide. Botnet malware infects many users and conducts malicious behaviors, such as leaking user information and downloading additional malicious files, upon the attacker's command.

Although Emotet malware started as an info stealer malware for financial information, it gradually developed into a downloader for additional info stealer malware, such as TrickBot and QBot.

Most of the reported botnet malware in 2020 was distributed through malicious email. When a macro inserted into an email attachment file is executed, malicious files are downloaded.

Botnet malware is mostly developed through the Builder, allowing quick alterations of attached files and executable files in a matter of hours. However, since the malware performs malicious behaviors by receiving commands from the attacker, it is difficult to figure out the malware's ultimate goal quickly. Also, the damage caused by the malware differs for every user with respect to the period.

© 2021 AhnLab, Inc. All rights reserved.

05
Increased Distribution of **Malicious Apps**

In 2020, the type and number of malicious apps distributed through Google Play has increased significantly. The distributed apps usually steal financial information, subscribe to subscription services without the user's consent, and distribute malicious advertisements.

In countries that use Wireless Application Protocol (WAP) billing services, 'Trojan/Android.Joker,' which was first discovered in 2020, has been continuously distributed through Google Play by disguising as document scanners and photo editing apps. Malicious app Cerberus, which source code has been published by the malware operator, has continuously been distributed through Google Play.

Malicious apps that expose malicious advertisements disguised itself by providing useful features to users via games or other apps. After they have enough users, they expose aggressive advertisements according to the commands received from the attacker's server (C2). Since malicious apps that spread through Google Play wait and hide for a certain period of time before executing malicious features, it create a substantial number of victims.

© 2021 AhnLab, Inc. All rights reserved.

Security Trends

2021 Threat Predictions

2021 Threat Predictions

AhnLab

01
Emergence of New Ransomware to Replace Maze Ransomware

Last November, Maze ransomware, which has been actively distributed, announced its retirement. As Maze ransomware is merely one of many ransomware, its disappearance will be soon be replaced by another ransomware. Thus, damages caused by ransomware will continue. Significantly, targeted ransomware groups will most likely expand their impact by improving their attack techniques to increase their source of financial profit.

Businesses today use various software to increase productivity and work efficiency. However, if a vulnerability exists within the software, attackers will exploit it to take control of the system or business and perform malicious activities. Thus, attackers will continue to advance their methods to effectively execute successful stage-by-stage attacks, such as infiltration, control, and theft.

In Korea, there are actual cases of hackers exploiting vulnerabilities within the corporate software. In 2021, ransomware attacks are expected to continue, but in a more impactful way.

There is no guarantee that the aforementioned death of a patient due to a seized medical system caused by a ransomware attack won't happen again in other parts of the world. Enhanced security systems, improvement in security awareness, and security regulations are necessary to prevent such incidents.

© 2021 AhnLab, Inc. All rights reserved.

02
New Work Environments due to COVID-19

It's been a year since coronavirus first emerged. In 2020, we experienced drastic changes in our daily lives due to COVID-19. For instance, there was a steep increase in online purchases and delivery services, and many businesses transitioned online.

In a remote, contactless work environment, individuals need to be aware of their security. It is because the corporate security policies do not protect remote work environments. However, it is difficult to maintain a certain security level due to cost and resource issues, which has created challenges for businesses while creating opportunities for attackers. Hacking attempts, such as phishing and targeted attacks, towards remote work environments, are expected to continue in 2021.

Therefore, security should become mandatory for remote work environments. When using the VPN (Virtual Private Network), correct policy settings, and enhanced user verification is also essential. In environments that lack security administrators, SaaS (Software as a Service) security solutions can create a secure work environment.

© 2021 AhnLab, Inc. All rights reserved.

03
Diversification in Malware Development Languages

In 2021, developing executable malware, such as EXE and DLL, will become more diversified. Until recently, many PE (Portable Executable) files have been developed in programming languages, such as C, C++, Visual Basic, Delphi, and C#. But lately, malware has been developed in Python or GoLang.

It seems that the attackers are taking full advantage of easy compilation and binary generation and the fairly easy addition of libraries or modules. Furthermore, attackers will most likely use the fact that these files have a completely different form and structure from the signature patterns of existing anti-malware products and use it to their advantage.

© 2021 AhnLab, Inc. All rights reserved.

04
Modularization of Malware Operation Methods

Malware operation methods are already being modularized. Instead of one file communicating with the attacker's C2 server, downloading, leaking information, and generating files, the mentioned activities are performed by different files conducting separate, malicious behaviors. This is to bypass anti-malware programs and maintain malicious behaviors while being under the radar as long as possible. For instance, if an encoded file is downloaded from the attacker server and there is a separate file that decodes the encoded file, it is not easy to identify the exact function and the flow of malicious behaviors just by the file information of a single file.

Hence, it is expected that malware will become more modularized in 2021. It is also expected that the malware will cause damage to the target system by prompting users to access malicious servers, download malicious files, and continuously replace the planted files.

© 2021 AhnLab, Inc. All rights reserved.

05
Expansion of Countries being Targeted by Malicious Apps

Attacks usings malicious apps to target mobile devices tend to be effective only in a single country, mainly due to language, culture, and payment system differences. The phishing app (Dropper/Android.PhishingApp), which targets smartphone users, was spread through phishing messages related to social issues, including delivery status, wedding invitations, and COVID-19 related information. The malicious app was used to steal money by leaking information within the user's smartphone and using that information for voice phishing.

In 2020, cases of malicious app distribution carried out by the same developer have been identified in various countries. The attacker disguised as a well-known delivery company in each country. Furthermore, we have identified malware distributed by disguising itself as popular content providers, such as Netflix and Disney. Then, the malware would persuade the users to subscribe to browser notification advertisements.

This type of malware can be easily distributed to users in various countries because advertisement providers offer advertisements in the operating language of the target device. Malicious apps that used to work locally due to limited profitability have now begun to target smartphone users in various countries, and this trend is expected to continue in 2021.

© 2021 AhnLab, Inc. All rights reserved.

Security Trends

2020 Reviews

2021 Predictions

Publisher AhnLab, Inc.

Contributors ASEC Researchers

Editor Content Creatives Team

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, Korea

Tel. +82 31 722 8000 | Fax. +82 31 722 8901

© 2021 AhnLab, Inc. All rights reserved.

Reproduction and/or distribution of a whole or part of this document in any form without prior written permission from AhnLab are strictly prohibited.

AhnLab.com ASEC Blog LinkedIn

AhnLab