Revista Argentina de Clínica Psicológica
2021, Vol. XXX, N°1, 13-27
DOI: 10.24205/03276716.2020.2001

Advanced Persistent Threats in COVID-19 Pandemic Process

Hamza Fatih Sapanca[a], Sezer Kanbul[b], Omer Sami Kaya[c], Ata Taspolat[d]

Abstract

Information is important in every period and obtained in different ways and easily accessible. Today, with the development of technology, it has become easier to reach information, and almost any information could be obtained at the desired location and time using technology. It is important that people choose the right information and protect it online. In this context, this importance has increased further with the COVID-19 process, where human vulnerabilities have surfaced. In the process in question, people have to spend more time on the internet, and in addition, they experience negative emotions such as anxiety, stress and fear caused by the pandemics. Attackers took this as an advantage to obtain data using various methods. The importance of awareness in terms of ensuring the data security of individuals or institutions and not getting into the hands of the attackers have once again emerged in the pandemic process experienced. In this study, advanced persistent threats (APT), which have higher risk levels than the risk level of the attackers, were tried to be expressed in detail and explained through a case study. In line with the data obtained, it is important to raise awareness of users. Solutions should be produced by the state and scientific studies should be included in this regard. Systems should be created for training individuals who are experts in their field.

Keywords: digital citizenship, covid-19, apt, deep and silent threat, network security

1. Introduction

Information comes from the Greek concept of epistemology meaning "absolute truth"(Sveiby, 1997). In the 21st century, companies, states, institutions, individuals and societies all live in the common age of knowledge and have to keep up with the requirements of the information age (Bhatt, 2000). In this context, knowledge has continued to be an indispensable source of power from the past to the present, so it is wanted to be obtained continuously (Stewart, 1997; Engin, 2005). Protecting valuable information is increasingly difficult from those who want to obtain them by using all kinds of resources (people, time, money, etc.) and constantly develop themselves.

In our age, the development of Information and Communication Technologies (ICT) tools began to be among the must-haves in our daily lives and in parallel, its use began to increase. This development offers time and space independence for the individual at the point of access to information. This independence has led to the emergence of the concept of digital citizens (Isman & Gungoren, 2014). The correct use of technological tools corresponds to citizens who pay attention to human rights and ethical rules in a virtual environment, respect, and have security and responsibility awareness (Mossberger, Tolbert, & McNeal, 2007). According to a report released by Data reportorial in January (2020), 4.54 billion internet and 3.80 billion social media users in the world, 62.07 million internet and 54 million social media users in Turkey have been announced (Kemp, 2020). These results reveal that the vast majority of the population is internet users. It can be said that this situation reveals the increase in individuals with digital citizen characteristics. However, in addition to the benefits of evolving technology, online environments have been abused by some people and moved the concept of security into a virtual environment (Kim, Jeong, Kim, & So, (2011). Due to the severity of this situation in the countries, some legal regulations have been introduced. The most comprehensive regulation on the subject in Turkey was issued in 2004 in Articles 5237 TCK 243, 244 and 245 and a penalty return was provided (what punishment?). In addition, the Personal Data Protection Act is issued with the

[a] Near East University, Mersin 10 Turkey, fatih.sapanca@neu.edu.tr
[b] Near East University, Mersin 10 Turkey, Assoct. Prof. Dr, Distance Learning and Information Technology Center Manager, sezer.kanbul@neu.edu.tr
[c] Near East University, Mersin 10 Turkey, omersami.kaya@neu.edu.tr
[d] Near East University, Mersin 10 Turkey, ata.taspolat@neu.edu.tr

approval of the 2016, intended to ensure that unwanted collection, use and sharing of personal data on demand do not occur (Kişisel Verileri Koruma Kurumu, 2018).

In December 2019, the COVID-19 virus began in China and gradually began to appear in many countries. It was declared pandemic on March 11, 2020 with the increase in spread (Aslan, 2020). Many measures such as closing borders, canceling flights and stopping businesses, keeping people in their homes, and closure of schools, have been put in place by states to reduce the spread rate in the countries seen (Telli & Altun, 2020). As a result of these measures, many companies, schools and universities have started to work remotely (Techinside, 2020). Zoom app, one of the apps that allows people to meet online, can be considered as an indication that people are turning to virtual environments (Iqbal, 2020). People were able to move on with the help of tools like Zoom without leaving their homes. Parallel to increasing number of online users, cyber-attacks have also increased (Security World Market, 2020; Gözel, 2020; WHO, 2020). This increase during the time the COVID-19 process has been shown in the Figure 1 (Radoini, 2020). Increased purchases of domain names like corona virus and COVID-19 are mentioned in (*Siber COVID-19'a Dikkat!*, 2020).

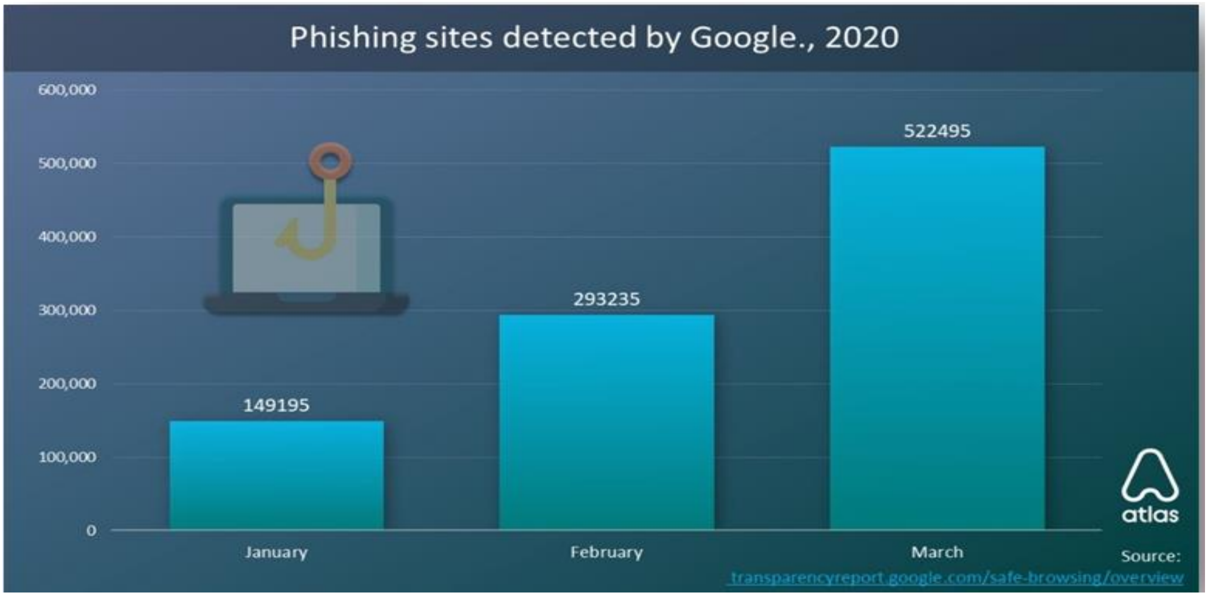


Figure 1. **Active Phishing Websites Detection Chart [17]**

2. Related Research

Given the number of individuals who have access to the internet in the age we live in, it seems that digitalization has been adopted in society. With this adoption, people make transactions in a virtual environment using their personal data, such as shopping, social life, business, and public services (Chen, 2012). In parallel with this increase, there has also been an increase in virtual environment crimes and criminals (Vozikis, Darra, Kuusk, Kavallieros, Reintam, & Bellekens, 2020) resulting in large-scale damage as a result of cyber-attacks. In this context, it is announced that losses as a result of cyber-attacks could reach $ 6 trillion in 2021 (Roth, 2020). The methods that the attackers had used; malware (malicious software) viruses, trojans, worms, rootkits, phishing, spyware, social engineering and advanced persistent threats (Naidoo, 2020).

Naidoo (2020) has studied how attackers use this condition during the COVID-19 pandemic. Through his work, he performed thematic and content analysis on 185 different documents used by attackers. According to the data he obtained, he identified the methods of various cybercriminals using the pandemic process to exploit people.

In addition, it has been determined that people use negative emotions such as uncertainty, anxiety, and anxiety like emotions. The researcher believes that the study will contribute to a safer digital world (Naidoo, 2020).

Another study in the process, Buil-Gil, Miró-Llinares, Moneva, Kemp and Díaz-Castaño (2020), covered the review of cybercrime in the UK between May 2019 and 2020. They have assessed this process in terms of cyber attackers. According to the results, they found that the rate of cybercrime has increased significantly. In particular, cyber-crimes such as shopping, auction fraud, hacking of social media tools and mail addresses have come to the fore. Another point they also point out is that individuals, not institutions, are more victims in this process.

A study by Hakak, Khan, Imran, Choo and Shoaib (2020) also found that cybercriminals are forced to work at home during the COVID-19 process, and the result is that they try to take over video conferencing environments such as zoom, exploiting the pandemic process using information theft and other known methods. He pointed out that IT managers should take the necessary measures for environments that have to work in their homes. It has been stated that establishing a VPN connection and providing remote access is more reliable than other environments. Another result obtained is awareness of the human factor. He mentioned the importance of increasing awareness that the most important element in this process is human.

Xia, Wang, Luo, Wu, Zhou, Bai and Liu (2020) studied cryptocurrencies during the pandemic process in their study. The increased interest of cryptocurrencies during the pandemic has also attracted the attention of attackers. But it has been noted that people are not very aware of this situation. They identified 195 cases spread through social engineering using pandemic-related content. 200 different fraud addresses were identified and 6 329 victim addresses were identified. The money from the victims is 330 thousand US dollars. As a result of the data obtained, it was noted that it is important to reduce the impact of early detection in the use of social media tools in such attacks. In addition, it was noted that studies should be included in ways that increase people's awareness.

Gvili (2020) said that Apple and Google collaborated against possible attacks due to the covid-19 epidemic, and this collaboration aimed to reduce and prevent the spread of possible attacks by governments and health institutions. In this study, this situation is considered and presented as a report. The report found that people would be more likely to adopt, due to the fact that the technology world has a widespread network of uses in partnership with two major giants. In this way, it was thought that the risks of possible attacks would be reduced in this way. The resulting data focused more on system security, while also accessing data on information security.

In their study, Okereafor and Adelaide (2020) also noted that the use of online technologies is widespread because of the social distance rule that occurs to reduce spread in the COVID-19 process, because of the situation in which people conduct their work remotely. With this spread, a noticeable increase in Computer Crimes, privacy violations and service disruptions has been identified. Attacks by attackers took advantage of people's vulnerability to the negative situation due to COVID-19. The researcher developed the random cyber-attack simulation model (RCSM) in this study. By detecting cyber-attacks through the Model, it will prevent, reduce the impact of an attack and ensure that individuals or institutions are already present against these situations.

Lallie, Shepherd, Nurse, Erola, Epiphaniou, Maple and Bellekens (2020) in their study, COVID-19 process is an unprecedented event, so it is stated as a new norm state. The attackers, who knew the growing concern from people because of the outbreak, said they were injured. Their work was based on the perspective of cyber attackers. As a result of the results, they determined that the attackers carried out 3 or 4 attacks per day. With carefully prepared data to achieve success in attacks, they also revealed that they carried out attacks using government announcements. According to another result, jobs closed due to the pandemic led to an increase in the unemployment rate. This has led to people spending more time online, as well as an interest in cyber attackers/attacks.

As December March 2019, the World Health Organization declared COVID-19 disease as a pandemic in China as a result of the data obtained from the literature. Countries have taken some measures against the disease. People are confined to their homes to reduce the risk of infection. As a result, people were forced to continue their educational lives, work and social lives in their homes. Because of this, the number of online users and the time spent has increased greatly. However, the disease has caused an increase in negative emotions such as fear, anxiety and anxiety on human psychology. Cyber attackers who know this situation have also begun to take more action. In light of the resulting data, it was determined that attackers went on the path of increasing the success rate in an attack by using images with “COVID-19” content, mimicking organizations. According to the results, it was noted that safer environments were provided in this process, where they had to work at home. Another aspect, human awareness, has been noted. It is important that people have a high level of readiness for such attacks.

Cyber defense has lost its importance because people's focus shifts to the health crisis. It has been determined that since posts on social media related to Corona increase feelings of anxiety, stress and fear on people, it is tried to obtain information through the related posts (Aksakallı, 2020). In this process, Zoom application has been considered with an increase in the number of users. However, it was found that the information of a particular user using the Zoom app was stolen and put up for sale through the website used by cyber criminals (Dailymail, 2020; O'Flaherty, 2020). In addition, many methods were implemented such as the establishing of fake charities to raise funds and online selling of materials that are important for the process such as masks and disinfectants without approval by the relevant organization, and trying to obtain people's information without permission using fake e-mails and news content (COVID-19 Cyber Security, 2020). Given these, the importance of the concept of digital citizenship is emerging. The internet risks that are among the characteristics of being a digital citizen and the importance of safe internet use have been understood once again in this period. In this context, considering digital citizenship from a cyber security point of view provides a guide to safe internet use, viruses and prevention. Attackers are trying to obtain data using a wide variety of attack methods. One of them is APT which refers to a long-term, hidden and advanced cyber-attack process that targets one or more individuals or organizations to accomplish a specific purpose (Chandra, Challa, & Pasupuleti, 2016; Huang & Zhu, 2020). While the number of such attacks has increased recently, it is not possible to say the same for the increase in awareness about the threat Sood & Enbody, 2012).

Another goal of this study is to identify the behavior patterns and general characteristics of APT attacks that have been carried out in the past and are still increasing. In this study, data was based on literature for the purpose of collecting data by qualitative method, and data was obtained by case study in the light of the results obtained by consulting field experts. Concepts were expressed by summarizing the information obtained by scanning the literature. In addition, research conducted in the pandemic process is summarized. Experts have been consulted and officials who can get first-hand information about the issue have been accessed. Finally, the case is mentioned on the subject (Lin, 1976).

The topics in the study are edited as follows: The definition and common characteristics of APT are examined in Chapter 3. In Chapter 4, the life cycle of an APT is discussed with its stages. Chapter 5 describes the methods and environments that APTs use to spread. In Chapter 6, a review of the APT, Calypso, is presented as a case study and the results reached in Chapter 7 are presented to the evaluation.

3. APT Features

3.1 Definition

The term APT was first used by the United States Air Force in 2006 (Xia et al.,2020). While the concept of APT has not a clear definition agreed upon, it refers to an advanced and long-term cyber-attack carried out for a specific purpose (Miller, 2012). Supported by states or large groups, developed to carry out the desired attacks in cyber wars, it is also defined as a set of malware which are supported by states or large groups, developed to carry out the desired attacks in cyber wars and headed towards clearly identified targets (bircan, 2012; Chen, Desmet, & Huygens, 2014). Attacker or attackers are often state-sponsored and aim to obtain critical intelligence about other states [41], (Nicho &McDErmott, 2019). However, private organizations may also be the target of attacks. The word APT word can be summarized as follows (Radack, 2011; Brewer, 2014; Chen, Su, Yeh, & Yung, 2018; Lv, Chen, & Hu, 2019).

Advanced: Attackers take advantage of all computerized attack techniques and technologies. The sub components of the attack may not be classified as "advanced," but these components are assembled to achieve more advanced tools and multiple attack methods and tools are combined to reach the goal.

Permanent: Attackers prioritize a specific task rather than a financial gain they can get right away. This distinction shows that attackers are driven by external organizations. The attack is carried out continuously through monitoring and interaction to achieve the specified task. This means there is no limit to continuous attacks and updating malware. In fact, a quiet and deep (low-and-slow) approach is often more successful.

Threat: Means that the attack is associated with people working collaboratively rather than a code that exhibits automated behaviors. The attackers have a specific purpose and are motivated for this purpose. They are also talented and generally well-funded.

Attackers don't necessarily need to violate perimeter security checks. They can use and often use insider threats and trusted connections for their interests to access targeted systems (Feng, Zheng, Hu, Cansever, & Mohapatra, 2015; Liu, De Vel, Han, Zhang, & Xiang, 2018).

Misuse of trusted connections is a key component for most APTs. While companies use complex technologies to prevent targeted organizational infection and the seizure of digital systems, attackers often enter the organization by stealing the username and password information of the company's partners, remote offices or workers (Ussath, Jaeger, Cheng, & Meinel, 2016). Almost any organization or remote campus can be a victim of an APT and can be used as an entry or information harvest point.

3.4 Silent and Deep Attacks

One of the most important requirements for APT is to be invisible for as long as possible. Attackers focus on silent and deep attacks and secretly move from one host to another without creating regular or predictable network traffic in order to get what they want (Fossi, Egan, Haley, Johnson, Mack, Adams, & Wood, 2011). So much effort is made to prevent harmful behaviors from being observed by system operators Alshamrani, Myneni, Chowdhary, & Huang, 2019).

Malware is a key component in successful APT operations. Modern commercial malware; with all the features and functions required to infect digital systems while hiding from intrusion detection systems, navigate across networks, capture critical data, and provide remotely controlled video surveillance via silent and confidential channels, is readily available on the Internet.

3.2 Remote Control

Remote control lies at the core of each APT. Attackers depend on this feature to advance to a specific machine within the target organization, exploit local systems, and gain constant access to critical information. If an APT cannot contact the attackers behind it, it cannot transmit the information it collects. This characteristic causes APT to look like a subcategory of botnets. While it is possible for APT to remain hidden at host level, remote controlled network activity can be more easily detected. APTs are most actively located, detected, and blocked in the network layer (L2) Chen, Desmet, & Huygens, 2014).

3.3 Difference from Other Threats

The most important difference between APTs and regular threats is that APTs target a particular organization. Ensuring environmental safety and the use of standard security checks can protect an organization from an ordinary attack, but these measures may not be sufficient against APTs. Attackers can patiently wait for new flaws that will create a vulnerability, or combine seemingly small flaws to carry out large-scale attacks [53]. The superiority of APTs can be clearly seen compared to regular threats (Figure 1). When faced with such a threat, normal rules no longer apply. In the past, many organizations have felt the need to have better security than other internet-connected organizations. Therefore, the attackers used to give up and move on to easier targets. But with APTs, organizations must defeat their enemies who are focused on them and looking for a weakness to attack instead of moving to another target.

The operating time of APT can also make it difficult to detect it. In a standard security breach, a large amount of data can be stolen in a short period of time. In this case, it is possible to detect the violation with firewalls and intrusion detection systems. For an attacker behind an APT, it could take months or even years to steal targeted data by circumventing fully-featured and well-configured systems (Huang & Zhu, 2020).

4. APT Lifecycle

Although each APT is specially designed for the target and purpose of the attack, there are some common phases involved in the preparation and implementation of the attack. A typical APT will spend most of its shift slated to collect critical information after long research, successfully entering critical systems and gaining influence. Looking at the model in Figure 2, it is estimated that it has been built upon penetration into the net as far as it can go until it reaches its goal (Mandiant, 2013). APT attacks, like a specialist agent, start work within a plan, always ready to improvise in the face of potential security barriers and opportunities. During the entire life cycle, they perform all their activities for their purposes (Geers, Kindlund, Moran & Rachwald, 2014; Tubitak Bilgem Siber Güvenlik Enstitüsü).

4.1 Research Phase

The most important difference that distinguishes APTs from traditional mass attacks is conducting longitudinal research before and during the attack. Well-funded organizations behind APTs will spend a lot of time and resources exploring their very clearly determined goals. They will try to learn and understand network architecture, systems used in the past, potentially threatened systems, applications, version numbers, and everything else they can use. They can investigate specific details about company culture or target individuals and use this information to send fake emails about company activities. They can also mimic the target with highly detailed emails or phone calls and trick users into sharing critical information.

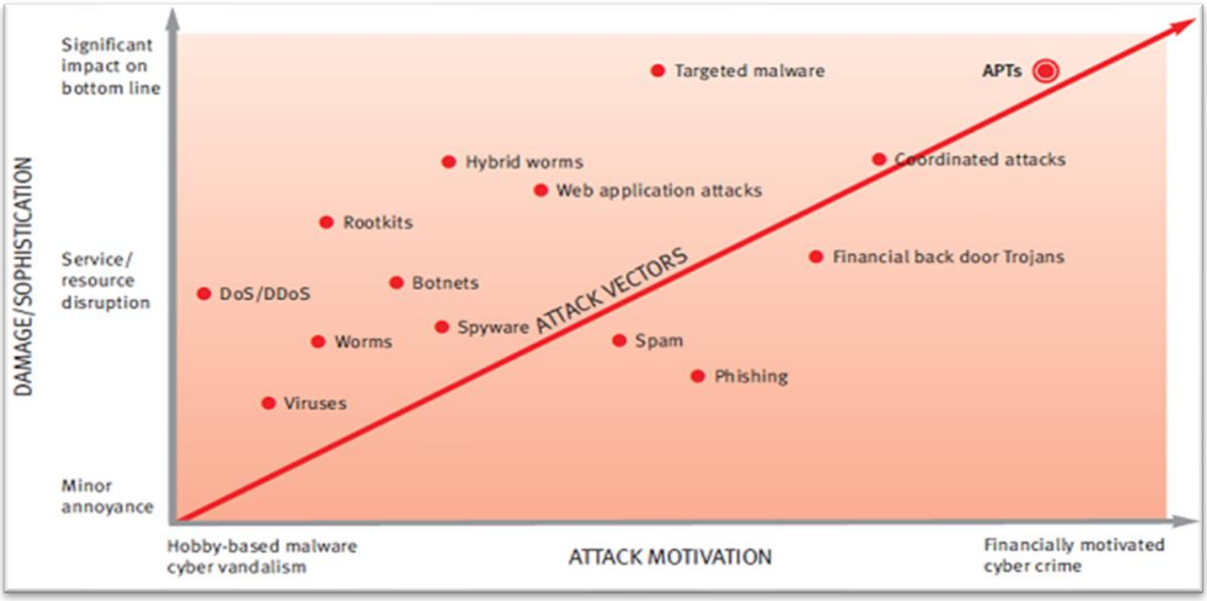


Figure 2. **Comparing ATMs with Other Threats (Cury, Hartman, Hunter, Martin, Morean, & Wolf, 2011)**

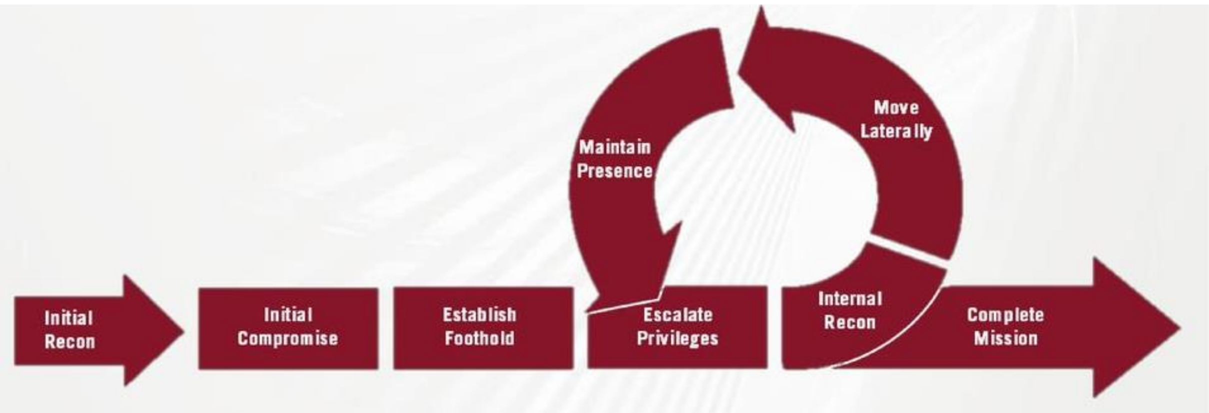


Figure 3. **APT Life cycle (Mandiat, 2013)**

Today, the vast majority of information can be obtained by making a creative Google search on Facebook pages, tweets, etc. Easy-to-reach penetration testing tools allow attackers to greatly explore an organization's network and systems. In time-spanning phone calls with several different departments of the company, harmless questions that are asked by pretending to be a distant employee of the company provide critical information. Of course, the ongoing attack continues to be confidential (Mainka, Somorovsky & Schwenk, 2018).

Preliminary research has shown that APT attackers often begin to make some advanced plans for other stages of the attack. They identify people and systems closest to their goals. Then they draw a map where they can identify different ways to succeed themselves. They can explore social engineering options, explore existing tools that can help them log in and systematically penetrate the network for purpose. The research phase also requires the development of the main tools to be used in the attack and to be customized according to the requirements.

An APT attack can use common malware codes, penetration test modules, and other tools by making minor changes to or on their original form. Examples of the Stuxnet attacks in 2010 were later redesigned and used to attack companies in the service and energy industries (V3.co.uk, 2011). Some tools are used to expose vulnerabilities that can be exploited, while others are used for specific facades of a multi-stage attack.

As a result of the data obtained, attackers create a profile that covers the target and its surroundings. They can even sometimes establish a one-to-one copy of the target system. In this way, they can test the different entry scenarios they plan to implement in the attack without the risk of being noticed in the actual system. They can also analyze potential risks and threats. This stage is critical to the success of the attack to be carried out (Sood & Enbody, 2012).

4.2 Entry Phase

Perhaps the first proof of the permanence of an APT is that it gains a solid place in the network where the attack can be kept at the entry phase. The attackers will try successive methods until they make a successful entry. They can even try a few different methods simultaneously to focus on others that work if one of the methods is detected.

Experts believe that harpooning (spear phishing) is among the most commonly used techniques in the entry phase of an attack (Krombholz, Hobel, Huber, & Weippl, 2015). Harpoon ingenue typically use a file that is added to the sent e-mail. The file in question has an extension, such as a PDF, and contains malicious code. However, neither the email itself nor the attachment is required. A message containing malware can also be sent via a web mail, a social networking account, instant messaging, etc. to circumvent e-mail antivirus mechanisms. This can also be accomplished with a simple link instead of an e-mail attachment. The link in question shows the malicious file stored in one of the public file sharing services.

The popularity of social networks is important in the spread of APTs. Because of the trust environment in these networks, people's awareness about the dangers of certain activities is decreasing.

All other methods, along with the aforementioned ones, are used for one thing: to obtain a place on the network that has minimal remote access and control authority and can hold on.

Remote Access Tools, known as RAT, are pre-made and relatively common tools. Attackers use these tools for their own benefit. Once the RAT is settled, attackers can use the settled platform in accordance with the later stages of the attack.

Regardless of the technical aspect of the attack, social engineering plays a key role. The information collected during the research phase is indispensable to obtain the credentials needed to trick users into accessing the critical network. However, the tactic should be expertly prepared after a while so that people will not be allowed to suspect. An APT avoids leaving traces that will give clues about higher-level targets even in the early stages of the attack. Those who detected an APT developing in their organization were able to see the first signs of the attack as if they were considering it as an ordinary malware or a simple spam email, but when they looked back.

4.3 Penetration Phase

Success is rarely achieved in the early stages of influence, but attackers can obtain important information from the systems that were first penetrated.

Because the first penetrated systems are constantly gathering information about networks, traffic patterns, potential vulnerabilities, connected servers, and others, attackers can discover that they need to do more research. In addition, remote control of each permeated system can capture valuable information such as users' IDs and access authority levels.

When attackers get enough information from the systems they first penetrate, they will start to proceed patiently towards their target system or systems.

4.4 Harvest Stage

The attackers are closer to their goals during the harvest. This stage is specifically called "harvest" as APTs simply collect information and leave the system. After collecting everything they can collect, they patiently wait for new and changing data to become useful. This is where APTs are differ from other malicious software. The effort of other malware to extract as much data as fast as possible often causes security systems to sound alarm. However, APTs will do the same with great patience in the long run and are designed to be caught by maintaining their privacy (Blue Coat, 2012).

5. Methods of Spreading

The purpose of the spread is to generally install malicious software on the target machine and use this platform to collect information. There are some common patterns, although they vary widely in practice.

5.1 Haphazard (Drive-by) Downloads and Phishing

The attacker aims to download malicious software from the internet with indiscriminate download attacks (Cova, Kruegel & Vigna, 2012). To do this, the user is forced to visit a previously influential website. This site directs the user-driven browser to another field name running the Browser Exploitation Pack (Browser Exploit Pack). This package is designed to find and exploit the openings contained in the user's browser or browser plug-ins. These openings are used to install malicious software directly into the system (Sood & Enbody, 2011).

Phishing means redirecting the targeted user to a haphazard download site. It can be thought of as a specialized form of an angling attack to focus on a goal. Simply, by email with personal and corporate information, the user is tricked and intended to visit a pre-captured site. This is usually accomplished through a link in the message.

Botnets provide a useful mechanism for anonymity, especially in phantom attacks targeting a group of users. However, the current anonymity of botnets is useful in cases where individuals are targeted. Figure 3 shows in detail the common strategy of attacks that combine harpoon and indiscriminate downloads.

The process works as follows: Attackers begin collecting email addresses to start phishing. They do this by researching resources and websites on the Internet. Initiates a process in which emails with offensive lye attachments that obtain the needed email addresses are automatically sent.

The technique of sending emails with harmful attachments is an effective attack vector. High-value organizations use software to verify e-mail attachments, but file types such as PDF, XLS, or DOC can circumvent these soft-wares with malicious code they host.

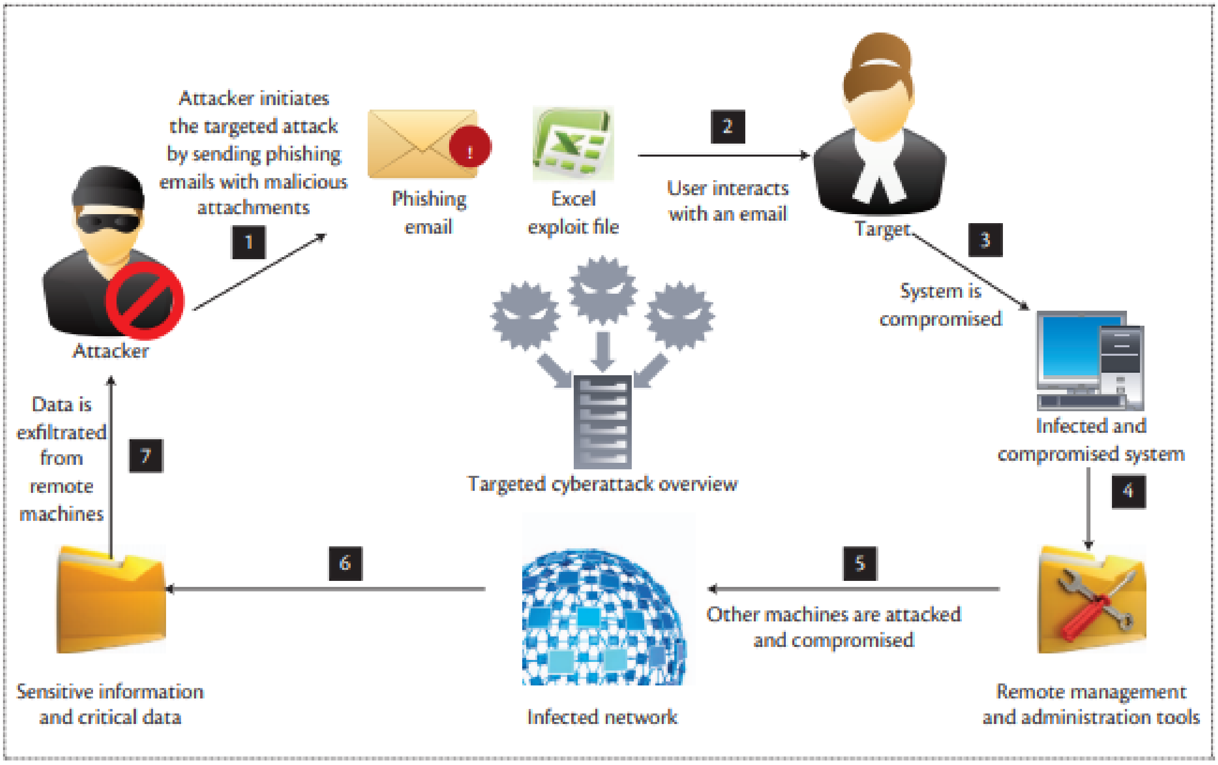
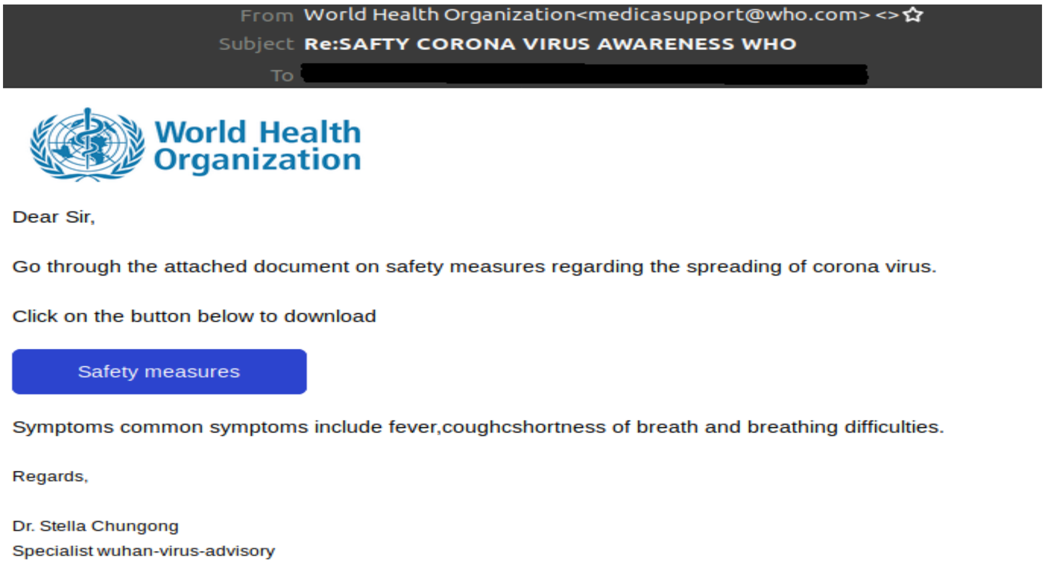

Attacker initiates the targeted attack by sending phishing emails with malicious attachments
1
Phishing email
Excel exploit file
2
User interacts with an email
Target
3
System is compromised
Attacker
Data is exfiltrated from remote machines
7
Targeted cyberattack overview
Infected and compromised system
4
6
5
Other machines are attacked and compromised
Sensitive information and critical data
Infected network
Remote management and administration tools

Figure 4. **Demonstration of a Typical Phishing APT Attack (Sood & Enbody, 2012)**

One advantage of the use of e-mail in the attack is that sent emails often circumvent security-based device such as Intrusion Detection Systems and firewalls. Security is left to check the e-mail attachment. When a user inside the organization opens the email, many levels of security will already be circumvented. From this point on, malware attacks software in the system, which has vulnerabilities to expand its exploitation. It can even download more harmful content by connecting to remote servers. The main idea here is to smuggle something that looks small and harmless from the eyes of the defense mechanisms in the system, and then inject more harmful software.

COVID-19-related content, which causes pandemic singing around the world as an example of harmful e-mail attachments, is used to lure people into traps. For this reason, they try to attract more attention and attention by using the name WHO, an enterprise organization that is important worldwide (Beyersdorf, 2020).



From World Health Organization<medicasupport@who.com> <>☆
Subject Re:SAFTY CORONA VIRUS AWARENESS WHO
To [redacted]

World Health Organization

Dear Sir,

Go through the attached document on safety measures regarding the spreading of corona virus.

Click on the button below to download

Symptoms common symptoms include fever,coughcshortness of breath and breathing difficulties.

Regards,

Dr. Stella Chungong
Specialist wuhan-virus-advisory

Figure 5. **Malicious Mail Attachment Sample Image (Beyersdorf, 2020)**

The malicious code used in the attack is usually designed to download a RAT. RAT allows the attacker to remotely control the exploited system. RAT consists of advanced software embedded in a variety of tools that allow you to manage systems over a network. Because the internal security mechanisms are weaker than the external security mechanisms, the malware can spread from one machine penetrated to other machines in the network. Now the assailant is inside the castle.

One of the best examples of this is the attack on the RSA. Attackers had placed malicious software that used a vulnerability to Adobe Flash software in an XLS file (Branco, 2011).

5.2 Exploiting Web Infrastructure

Security errors for web applications play an important role in APT attacks. The two techniques, called XSS (Cross-Site Scripting) and SQLI (SQL Injection), are used to manage mass attacks where attackers exploit a certain vulnerability available on many servers on the Internet. Attackers exploit SQLI vulnerability in particular, taking database details and using the information obtained to manage additional attacks. Some attackers combine XSS and SQLI techniques to use a hybrid technique called SQLXSSI. In this technique, the database of an unprotected website is updated with malicious I frame using SQLI. When a user visits this unprotected site, it withdraws the contents of the site from the database. There are also I frames that source a server that hosts malware in the captured content. In another scenario, a domain name can be compromised by an SQLI attack. It is now possible to install malicious software directly (Tang, Qiu, Huang, Lian, & Liu, 2020).

5.3 Exploiting Communication Protocols

Attackers tend to exploit several communication protocols used online to prevent the normal flow of operations. By seizing SMTP servers, they can set them as "open relays" that emit emails for harpoon attacks. In addition, unsecured FTP and HTTP servers can be used as storage resources that host malware. Attackers can exploit the DNS protocol to manipulate DNS records so that they can route traffic to malicious sites. Of course, some of these activities can affect many more people from the targeted individual or group and increase the likelihood of detection Karadoğan & Daş, 2015).

5.4 Exploiting Online Social Networks

The growth of online social networks provides a generous source of personal information, while increasing opportunities for social engineering. On social networks, users connect and share information. From an aggressive point of view, these networks allow you to exploit inter-friend trust. After all, there is a better chance of clicking on a link from a friend that is recommended. Large-scale attacks on social networks demonstrate the potential of a focused attack.

5.5 Exploiting Common Area (Co-location) Services

There are several services in a location. With the increase in numbers, they are more often exploited and useful for attacks.

Virtual hosting is useful for business, but with an attacker taking over only one website, the likelihood of taking control of the entire hosting server is more likely. Having such a server allows you to host malicious software in many places. Attackers use virtual hosting to access target servers and thus use two approaches to exploit them. The first approach captures an unprotected website and the client (host) is seized by establishing a remote management shell such as the C-99. In the second approach, the attacker writes a script that injects harmful I frame to capture all clients on the server.

Cloud services provide another platform for hosting malware. Targeted users can cause thousands of users to take over cloud services if they are infected. The IsecLab report on Amazon's cloud service AWS has shown this in full (Balduzzi, Zaddach, Balzarotti, Kirda & Loureiro, 2012).

Open or low-security wireless networks and malicious WI-FI services pose another attack front. Vulnerabilities here indiscriminately lead to the shelter of malware or information collection to be downloaded. For example, the software access point (soft AP) feature in Windows 7 can convert it to a malicious access point. This ensures an unauthorized network that can contact machines on the network without the administrator's permission. As a result, secret spreads can be performed using peer-to-peer (P2P) protocols.

Bluetooth services can also be exploited in a way that leads to the shelter or collection of information from malware. In 2004, Cabir was the first evidence to show the applicability of malware using Bluetooth (Welivesecurity, 2016).

Finally, other environments that spread malware are instant messaging and online chats. Like social networks, this approach exploits trust between friends and colleagues to increase the likelihood of a link being clicked.

5.6 Physical Attacks

Another attack front is hardware. USB sticks are widely used and are often shared among individuals. Thus, the trust limit is easily exceeded. The malware can copy itself to USB memory, which can spread to another machine with the same memory attached. This technique is especially useful for machines that do not have internet connection (E.g. Stuxnet). Shared memory hardware, such as CDs, DVDs, and memory cards, can also become carriers. In the recent past, small human-interface equipment was used to manage physical attacks. In these attacks, user-backed attackers were using USB memory to run the programs they wanted on target devices. These small devices can gain the ability to make themselves look like a keyboard or mouse with the design. Once they contact the CPU, they can obtain the information of the keys printed and process the actual data (Rutkowska, Tereshkin & Wojtczuk, 2009; Sood & Enbody, 2012).

Recent research has focused on equipment with pre-installed back doors (Ussath, Jaeger, Cheng & Meinel, 2016). A backdoor means the possibility provided to install malware. The most obvious feature of these equipment is that it survives all internet security. Because the backdoor is placed in the hardware and transported to any environment as a natural component of the machine. Hardware-based back doors have the capabilities to access (malware) cores and use a direct memory access engine (Kemp, 2020).

6. Example Case: VICIOUS PANDA APT

According to a 2019 report by Positive Technology (2019), an attack group thought to be based in China has attacked public institutions of 6 different countries, including Turkey. They infiltrated systems by taking advantage of the openness in Windows-based operating systems in public institutions. It was determined based on the available data that the group began carrying out their attacks in 2016. They had success in attacks of 34% in India, 18% in Brazil and Kazakhstan, 12% in Russia and Thailand, and finally 6% in Turkey. Other interesting information from the report is that the codes used in the software contain

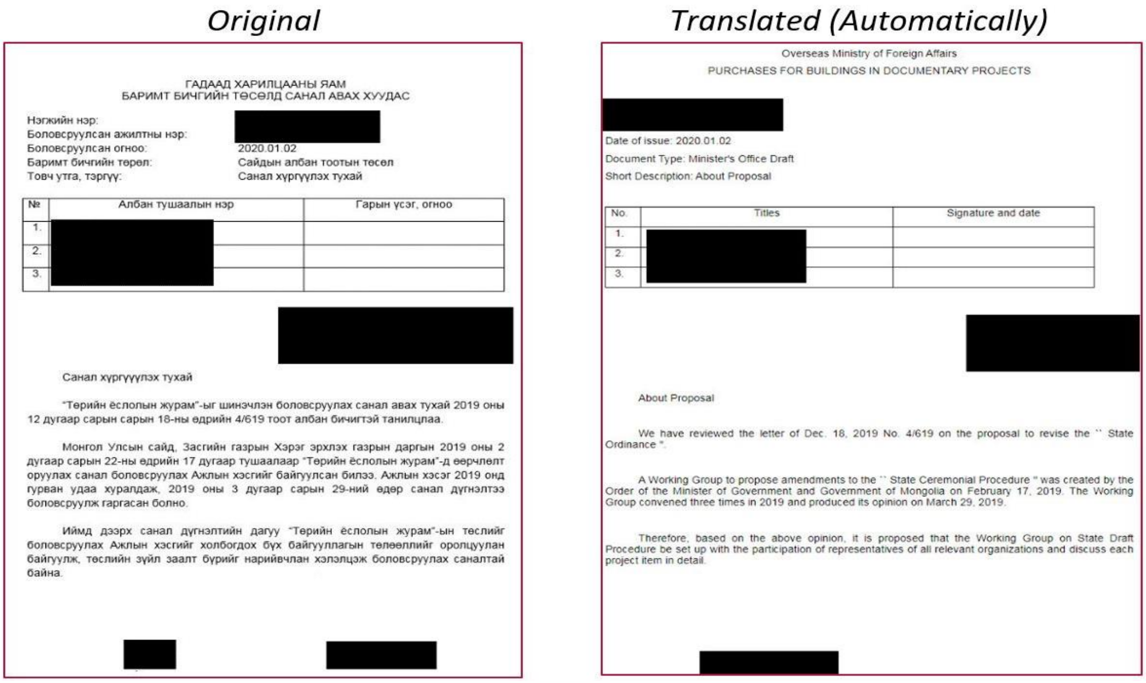
Chinese content. It is understood that the group's infiltration was to steal sensitive data and place malware for espionage purposes rather than a ransom demand.

They have carried out attacks using utilities used by experts such as SysInternals, Nbtscan, Mimikatz, ZXPortMap, TCP Port Scanner, Net cat, QuarksPwDump, WmiExec, Earth Worm, OS_Check_445, Double Pulsar, Eternal Blue and Eternal Romance, which are widely used in network management, using openings of these programs.

The Chinese group is the weakness of MS17-010, which is the most important factor in using Windows-based computers. Attackers have been able to infiltrate the systems and have access to the systems by taking advantage of this vulnerability. The vulnerability of MS17-010 applies to Windows Server 2016 Datacenter, Windows Server 2016 Essentials, and Windows Server 2016 Standard operating systems, and this vulnerability was fixed by the patch issued by Windows on March 14, 2017 (Cyber Security review, 2019).

Attackers exploited the MS17-010 vulnerability or stored their own malware and utilities in "C:\RECYCLER" or "C:\Program Data" directories on computers seized using stolen credentials.

According to Check Point and Malware bytes reports, the Calypso group COVID 19 was released in public institutions in Mongolia with the attack "Vicious Panda". The investigation began with the detection of two suspected RTF (Rich Text Format) documents sent to the Mongolian public sector. The documents are in Mongolian language and a document has been documented as if it were published by the Ministry of Foreign Affairs in Mongolia. Malicious codes for RTF files in Figure 6 and Figure 7 were recorded in the background and an attack was carried out (Ibliography Check Point Research, 2020; Threat Intelligence Team, 2020).



Original

ГАДААД ХАРИЛЦААНЫ ЯАМ
БАРИМТ БИЧГИЙН ТӨСӨЛД САНАЛ АВАХ ХУУДАС

Нэгжийн нэр:	[redacted]
Боловсруулсан ажилтны нэр:	
Боловсруулсан огноо:	2020.01.02
Баримт бичгийн төрөл:	Сайдын албан тоотын төсөл
Товч утга, тэргүү:	Санал хүргүүлэх тухай

№	Албан тушаалын нэр	Гарын үсэг, огноо
1.	[redacted]	
2.	[redacted]	
3.	[redacted]	

[redacted]

Санал хүргүүлэх тухай

"Төрийн ёслолын журам"-ыг шинэчлэн боловсруулах санал авах тухай 2019 оны 12 дугаар сарын сарын 18-ны өдрийн 4/619 тоот албан бичигтэй танилцлаа.

Монгол Улсын сайд, Засгийн газрын Хэрэг эрхлэх газрын даргын 2019 оны 2 дугаар сарын 22-ны өдрийн 17 дугаар тушаалаар "Төрийн ёслолын журам"-д өөрчлөлт оруулах санал боловсруулах Ажлын хэсгийг байгуулсан билээ. Ажлын хэсэг 2019 онд гурван удаа хуралдаж, 2019 оны 3 дугаар сарын 29-ний өдөр санал дүгнэлтээ боловсруулж гаргасан болно.

Иймд дээрх санал дүгнэлтийн дагуу "Төрийн ёслолын журам"-ын төслийг боловсруулах Ажлын хэсгийг холбогдох бүх байгууллагын төлөөллийг оролцуулан байгуулж, төслийн зүйл заалт бүрийг нарийвчлан хэлэлцэж боловсруулах саналтай байна.

[redacted] [redacted]

Translated (Automatically)

Overseas Ministry of Foreign Affairs
PURCHASES FOR BUILDINGS IN DOCUMENTARY PROJECTS

[redacted]

Date of issue: 2020.01.02
Document Type: Minister's Office Draft
Short Description: About Proposal

No.	Titles	Signature and date
1.	[redacted]	
2.	[redacted]	
3.	[redacted]	

[redacted]

About Proposal

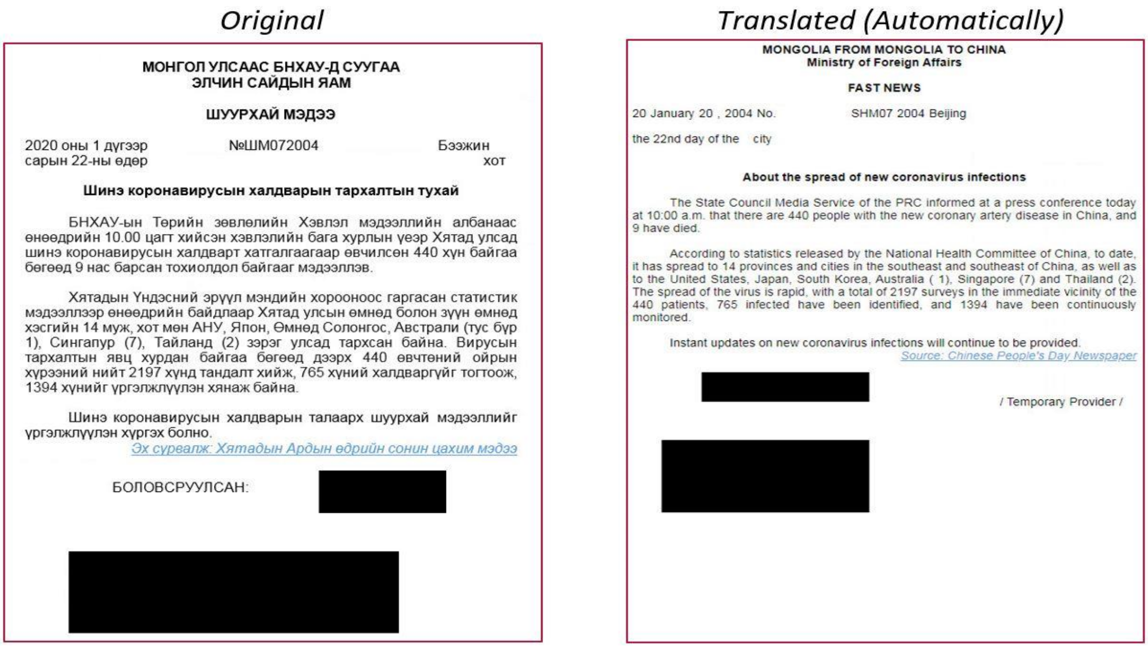
We have reviewed the letter of Dec. 18, 2019 No. 4/619 on the proposal to revise the `` State Ordinance ".

A Working Group to propose amendments to the `` State Ceremonial Procedure " was created by the Order of the Minister of Government and Government of Mongolia on February 17, 2019. The Working Group convened three times in 2019 and produced its opinion on March 29, 2019.

Therefore, based on the above opinion, it is proposed that the Working Group on State Draft Procedure be set up with the participation of representatives of all relevant organizations and discuss each project item in detail.

[redacted]

Figure 6. **Information on Corona virus Allegedly published by the State Department**



Original

МОНГОЛ УЛСААС БНХАУ-Д СУУГАА
ЭЛЧИН САЙДЫН ЯАМ

ШУУРХАЙ МЭДЭЭ

2020 оны 1 дүгээр сарын 22-ны өдөр №ШМ072004 Бээжин хот

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн зөвлөлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10.00 цагт хийсэн хэвлэлийн бага хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хатгалгаагаар өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгааг мэдээллэв.

Хятадын Үндэсний эрүүл мэндийн хорооноос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өмнөд болон зүүн өмнөд хэсгийн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (тус бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын явц хурдан байгаа бөгөөд дээрх 440 өвчтөний ойрын хүрээний нийт 2197 хүнд тандалт хийж, 765 хүний халдваргүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэх болно.

Эх сурвалж: Хятадын Ардын өдрийн сонин цахим мэдээ

БОЛОВСРУУЛСАН: [redacted]

[redacted]

Translated (Automatically)

MONGOLIA FROM MONGOLIA TO CHINA
Ministry of Foreign Affairs

FAST NEWS

20 January 20 , 2004 No. SHM07 2004 Beijing

the 22nd day of the city

About the spread of new coronavirus infections

The State Council Media Service of the PRC informed at a press conference today at 10:00 a.m. that there are 440 people with the new coronary artery disease in China, and 9 have died.

According to statistics released by the National Health Committee of China, to date, it has spread to 14 provinces and cities in the southeast and southeast of China, as well as to the United States, Japan, South Korea, Australia (1), Singapore (7) and Thailand (2). The spread of the virus is rapid, with a total of 2197 surveys in the immediate vicinity of the 440 patients, 765 infected have been identified, and 1394 have been continuously monitored.

Instant updates on new coronavirus infections will continue to be provided.

Source: Chinese People's Day Newspaper

[redacted]

/ Temporary Provider /

[redacted]

Figure 7. **Purchases for Buildings in Documentary Projects**

7. Discussion and Conclusions

After COVID-19 was declared pandemic on March 11, many people have undergone radical changes in their work and education life, had to take a break from their social lives and has faced many extraordinary situations, such as staying away from other people. Because of these situations, cyber attackers who had the opportunity to create negative emotions such as fear and anxiety in humans have increased their activities. By taking advantage of the effects of the COVID-19 process, they have tried to increase their likelihood of success with attractive social engineering tactics such as spam and harpoon campaigns. Given that man is the weakest link in data security, it is important to raise people's awareness of the elimination of the threat. Digital citizenship education will increase the number of conscious internet users and strengthen this weak link. Since the COVID-19 process is an unusual situation, the importance of information security awareness has been understood once again in this process.

APTs are well-prepared and highly coordinated attacks designed to circumvent any defensive mechanisms. They are customized to target specific groups or organizations and are used in cyber operations to achieve a specific purpose. In this context, the structures that are in the target group/are likely to be budget allocation for this issue and work must be taken to take the necessary measures.

APTs are not a new type of threat. But their increasing activity in recent years requires companies to put APs at the top of the security agenda. Although government agencies have been targeted by ATMs in the past, private organizations have also been targeted. Organizations may need comprehensive and well-coordinated warning systems to prevent ongoing attacks. But most of the time, when an organization began to suspect an APT attack, the attack had already reached its target.

APTs are more complex than known attack scenarios, but a type of attack that occurs after its effect. In this context, financial losses after the attack may be much greater. This condition can be likened to cancer disease that occurs in the human body. Antivirus used in the detection of APTs and network attack detection and prevention systems need to be restructured due to the lack of strategies they use.

Due to the great danger, the work done in this field in the world and in Turkey is increasing day by day. In this study, it was aimed to raise people's awareness by examining some common behaviors and characteristics exhibited by these high-level threats. Because people's awareness enables the empowerment of the weakest rings in their security systems and to prevent security breaches. People should not open emails from individuals they do not know, not click on random links and have knowledge of the situation by following such topics at date.

In summary, APT is a huge threat that can cause serious harm to countries and institutions. These threats are well organized. Detection of such attacks can be provided by expert teams. In order to prevent this situation, users should be informed first. Awareness should be created by stating the methods used by attackers. Institutions should organize their systems very well and take security measures. Plans should be made for possible threat institutions. Incentives should be made to increase scientific studies on these issues. Conferences, seminars or activity should be held towards advanced persistent threats. In a world where such cyber-attacks are increasing instead of physical wars, solutions must be produced within the state.

References

[1] Aksakallı, G. (2020, April 7). *Koronavirüs (Covid-19) Salgını ve Koronafobi Etkisi*. Güvenli Web: https://www.guvenliweb.org.tr/blog-detay/koronavirus-covid-19-salgini-ve-koronafobi-etkisi accessed.

[2] Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D., (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys Tutorials,* vol. 21, no. 2, pp. 1851–1877.

[3] Aslan, R. (2020). Endemic Diseases in history and Today and Covid-19. *Ayrıntı Dergisi*, *8*(85).

[4] Balduzzi, M., Zaddach, J., Balzarotti, D., Kirda, E., & Loureiro, S. (2012, March). A security analysis of amazon's elastic compute cloud service. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing* (pp. 1427-1434).

[5] Beyersdorf, M. (2020, February 12). *Coronavirus is also dangerous by email*. Hornet Security: (accessed on 25 April 2020).

[6] Bhatt, G. D. (2000). Information Dynamics, Learning and Knowledge Creation in Organizations. *The Learning Organisation*, 7 (2),89-98.

[7] Bircan, B. (2012). Gelişmiş Siber Silahlar ve Tespit Yöntemleri. *TÜBİTAK BİLGEM, http://docplayer. biz. tr/1142152-Gelismis-siber-silahlar-ve-tespit-yontemleri-bahtiyar-*

bircan-uzman-arastirmaci-siber-guvenlik-enstitusu. html (22.01. 2016).

[8] Blue Coat, (2012). Blue Coat Labs Report: Advanced Persistent Threats. https://view.publitas.com/blue-coat/advanced-persistent-threats/page/1 (accessed on 13 May 2020).

[9] Branco, R. (2011). Into the Darkness: Dissecting Targeted Attacks. *Qualys Blog, Nov*.

[10] Brewer, R. (2014). Advanced persistent threats: minimising the damage. *Network security*, *2014*(4), 5-9.

[11] Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2020). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, 1-13.

[12] Chandra, J. V., Challa, N., & Pasupuleti, S. K. (2016, March). Advanced persistent threat defense system using self-destructive mechanism for cloud security. In *2016 IEEE International Conference on Engineering and Technology (ICETECH)* (pp. 7-11). IEEE.

[13] Chen, J., Su, C., Yeh, K. H., & Yung, M. (2018). Special Issue on Advanced Persistent Threat. *Future Generation Computer System*, vol. 79, pp. 243–246.

[14] Chen, P., Desmet, L. & Huygens, C., (2014). A Study on Advanced Persistent Threats," in Communications and Multimedia Security, ser. Lecture Notes in Computer Science. *Springer Berlin Heidelberg*, 2014, vol. 8735, pp. 63–72

[15] Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In *IFIP International Conference on Communications and Multimedia Security* (pp. 63-72). Springer, Berlin, Heidelberg.

[16] Chen, Y. K. (2012). Challenges and opportunities of internet of things. In 17th Asia and South Pacific design automation conference (pp. 383-388). IEEE.

[17] Cova, M., Kruegel, C., & Vigna, G., (2012). Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code. *Proc. 19th Int'l Conf. World Wide Web*, ACM, 2012.

[18] *COVID-19 Cyber Security*. (2020). Digitpot: https://digitpol.com/covid-19-cyber-security/ accessed.

[19] Cury, S., Hartman, B., Hunter, D. P., Martin, D., Morean, D. R., Oprea, A., ... & Wolf, D. E. (2011). Mobilizing Intelligent Security Operations for Advanced Persistent Threat. *RSA security brief, RSA*.

[20] *Cyber Security review*. (2019, October 31). Calypso APT Emerges from the Shadows to Target Governments: https://www.cybersecurity-review.com/news-october-2019/calypso-apt-emerges-from-the-shadows-to-target-governments/ (accessed on 05 May 2020).

[21] Dailymail, (2020, April 14). *More than 500,000 Zoom user credentials have been stolen and sold on the dark web for less than a PENNY each* DAilymail: https://www.dailymail.co.uk/sciencetech/article-8218723/More-500-000-Zoom-user-credentials-sold-dark-web-PENNY-each.html (accessed on 25 April 2020).

[22] Engin, A. O. (2005). The Importance and Position of Knowledge in Human Life. *Atatürk Üniversitesi Kazım Karabekir Eğitim Fakültesi Dergisi*, (11), 427-453.

[23] Feng, X., Zheng, Z., Hu, P., Cansever, D., & Mohapatra, P. (2015, October). Stealthy attacks meets insider threats: a three-player game model. In *MILCOM 2015-2015 IEEE Military Communications Conference* (pp. 25-30). IEEE.

[24] Fossi, M., Egan, G., Haley, K., Johnson, E., Mack, T., Adams, T., ... & Wood, P. (2011). Symantec internet security threat report trends for 2010. *Volume XVI*.

[25] Geers, K., Kindlund, D., Moran, N., & Rachwald, R. (2014). World War C: Understanding nation-state motives behind today's advanced cyber attacks. *FireEye, Milpitas, CA, USA, Tech. Rep., Sep*.

[26] Gelişmiş Siber Tehdidler (APT): Genel Bakış Zararlı Yazılım Analiz ve Mücadele Merkezi TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü. https://docplayer.biz.tr/4161254-Gelismis-siber-tehdidler-apt-genel-bakis.html (accessed on 25 May 2020).

[27] Gözel, S. (2020, April). *COVID-19 Döneminde Teknoloji ve Siber Güvenlik*. kpmg: https://home.kpmg/tr/tr/home/gorusler/2020/03/covid-19-temali-siber-tehditlere-dikkat.html accessed.

[28] Gvili, Y. (2020). Security analysis of the covid-19 contact tracing specifications by apple inc. and google inc. *IACR Cryptol. ePrint Arch.*, *2020*, 428.

[29] Hakak, S., Khan, W. Z., Imran, M., Choo, K. K. R., & Shoaib, M. (2020). Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *IEEE Access*, *8*, 124134-124144.

[30] Huang, L., & Zhu, Q. (2020). A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. *Computers & Security*, *89*,

101660.

[31] Ibliography *Check Point Research*. (2020, March 12). Vicious Panda: The COVID Campaign: https://research.checkpoint.com/2020/vicious-panda-the-covid-campaign/ (accessed on 05 May 2020).

[32] Iqbal, M. (2020, Mayıs 13). Business of Apps. https://www.businessofapps.com/data/zoom-statistics/ accessed.

[33] Isman, A., & Gungoren, C. O. (2014). Digital citizenship. *Turkish Online Journal of Educational Technology-TOJET*, *13*(1), 73-77.)

[34] Karadoğan, İ., & Daş, R. (2015, May). Analysis of attack types on TCP/IP based networks via exploiting protocols. In *2015 23nd Signal Processing and Communications Applications Conference (SIU)* (pp. 1785-1788). IEEE.

[35] Kemp, S. (2020, January 30). *Digital 2020: Global Digital Yearbook*. Datareportal: https://datareportal.com/reports/digital-2020-global-digital-yearbook?utm_source=Reports&utm_medium=PDF&utm_campaign=Digital_2020&utm_content=Yearbook_Promo_Slide (accessed on 25 April 2020).

[36] Kim, W., Jeong, O.-R., Kim, C., & So, J. (2011, 5). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, 675-705.

[37] Kişisel Verileri Koruma Kurumu. (2018, April). 100 Soruda Kişisel Verilerin Korunması Kanunu. Mayıs, 2020 tarihinde www.kvkk.gov.tr: https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/7d5b0a2f-e0ea-41e0-bf0b-bc9e43dfb57a.pdf (accessed on 25 April 2020).

[38] Krombholz, K., Hobel, H., Huber, M., & E. Weippl (2015). Advanced social engineering attacks. *Journal of Information Security and Applications,* vol. 22, pp. 113 – 122, 2015, special Issue on Security of Information and Networks.

[39] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*.

[40] Lin, N. (1976). *Foundations of Social Research*, McGraw-Hill, USA.

[41] Liu, L., De Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. *IEEE Communications Surveys & Tutorials*, *20*(2), 1397-1417.

[42] Lv, K., Chen, Y., & Hu, C. (2019). Dynamic defense strategy against advanced persistent threat under heterogeneous networks. *Information Fusion*, *49*, 216-226.

[43] Mainka, C., Somorovsky, J., & Schwenk, J. (2012, June). Penetration testing tool for web services security. In *2012 IEEE Eighth World Congress on Services* (pp. 163-170). IEEE.

[44] Mandiant, APT1: Exposing One of China's Cyber Espionage Units (Feb. 2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (accessed on 25 April 2020).

[45] Miller, R. (2012). Advanced persistent threats: Defending from the inside out. *CATechnologies, Jul*.

[46] Moon D, Im H, Lee JD, Park JH. MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats. *Symmetry*. 2014; 6(4):997-1010.

[47] Mossberger, K., Tolbert, C., & S. McNeal, R. (2007). *Digital Citizenship: The Internet, Society, and Participation*. London, England: The MIT Press.

[48] Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, 1-16.

[49] Naidoo, R., (2020). A multi-level influence model of COVID-19 themed cybercrime, European Journal of Information Systems, 29:3, 306-321, DOI: 10.1080/0960085X.2020.1771222.

[50] Nicho, M., & McDermott, C. D. (2019, September). Dimensions of 'Socio'Vulnerabilities of Advanced Persistent Threats. In *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)* (pp. 1-5). IEEE.

[51] O'Flaherty, K. (2020, April 1). *Zoom User Warning: This Is How Attackers Could Steal Windows Passwords*. Forbes: https://www.forbes.com/sites/kateoflahertyuk /2020/04/01/zoom-user-warning-this-issue-could-allow-attackers-to-steal-windows-users-passwords/#50f74f6661fd (accessed on 25 April 2020).

[52] Okereafor, K., & Adelaiye, O. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. *International Journal of Recent Engineering Research and Development (IJRERD*). Volume 05 – Issue 07, PP. 61-72.

[53] *Positive Technology*. (2019, October 31). Calypso APT: new group attacking state institutions: https://www.ptsecurity.com/ww-en/analytics/calypso-apt-2019/#id1 (accessed

on 05 May 2020).

[54] Radack, S. (2011). *Managing information security risk: organization, mission and information system view* (No. ITL Bulletin March 2011). National Institute of Standards and Technology]

[55] Radoini, A. (2020, May 11). *Cyber-crime during the COVID-19 Pandemic*. Unicri: http://www.unicri.it/news/article/covid19_cyber_crime (accessed on 5 June 2020).

[56] Rakes, T. R., Deane, J. K., & Rees, L. P. (2012). IT security planning under uncertainty for high-impact events. *Omega*, *40*(1), 79-88.

[57] Roth, J. (2020, february 13). *$6 Trillion is Expected to Be Spent Globally on Cybersecurity by 2021*. International Institute of Business Analysis: https://www.iiba.org/iiba-analyst-catalyst-blogs/$6-trillion-is-expected-to-be-spent-globally-on-cybersecurity-by-2021/ (accessed on 25 April 2020).

[58] Rutkowska, J., Tereshkin, A., & Wojtczuk, R. (2009). Thoughts about trusted computing. *Invisible Things Lab, EuSecWest May*, 27-28.

[59] Security World Market. (2020, March 31). Global cyber attacks on the increase during COVID-19 crisis: https://www.securityworldmarket.com/int/News/Business-News/during-covid-19-no-one-is-immune-to-cyber-attacks (accessed on 25 April 2020).

[60] *Siber COVID-19'a Dikkat!* (2020, March 29). Cyber Mag: https://www.cybermagonline.com/siber-covid-19a-dikkat (accessed on 25 April 2020).

[61] Sood, A. K., & Enbody, R. J. (2011). Browser Exploit packs-death by bundled exploits. In *Proc. 21st Virus Bulletin Conf*.

[62] Sood, A. K., & Enbody, R. J. (2012). Targeted cyberattacks: a superset of advanced persistent threats. *IEEE security & privacy*, *11*(1), 54-61.

[63] Stewart, T. A. (1997). *Entelektüel Sermaye: Kuruluşların Yeni Zenginliği.,* Çev. Elhüseyni, N., Z., MESS Yayınları, Yayın No:258, İstanbul.

[64] Sveiby, K. E. (1997). *The new organizational wealth: Managing & measuring knowledge-based assets*. Berrett-Koehler Publishers.

[65] Tang, P., Qiu, W., Huang, Z., Lian, H., & Liu, G. (2020). Detection of SQL injection based on artificial neural network. *Knowledge-Based Systems*, 105528.

[66] Techinside, (2020, April). https://www.techinside.com/:https://www.techinside.com/ zoom-kullanici-sayisi-300-milyonu-gecti/ (accessed on 25 April 2020).

[67] Telli, S. G., & Altun, D. (2020). The Coronavirus and the Rising of Online Education. *Üniversite Araştırmaları Dergisi*, *3*(1), 25-34.

[68] Threat Intelligence Team. (2020, April 9). *Malwarebytes Lab*. APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure: https://blog.malwarebytes.com/threat-analysis/2020/04/apts-and-covid-19-how-advanced-persistent-threats-use-the-coronavirus-as-a-lure/ (accessed on 05 May 2020).

[69] Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016, March). Advanced persistent threats: Behind the scenes. In *2016 Annual Conference on Information Science and Systems (CISS)* (pp. 181-186). IEEE.

[70] Ussath, M., Jaeger, D., Cheng, F., & Meinel, C. (2016, March). Advanced persistent threats: Behind the scenes. In *2016 Annual Conference on Information Science and Systems (CISS)* (pp. 181-186). IEEE.].

[71] V3.co.uk, April 7, 2011, "Two-thirds of energy firms at risk from Stuxnet-like Scada attack" http://www.v3.co.uk/v3-uk/news/2041556/-thirds-energy-firms-risk-stuxnetscada-attack (accessed on 25 April 2020).

[72] Vozikis, D., Darra, E., Kuusk, T., Kavallieros, D., Reintam, A., & Bellekens, X. (2020). On the importance of cyber-security training for multi-vector energy distribution system operators. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-6.

[73] Welivesecurity (2016, November 1). *A history of mobile malware from Cabir to SMS Thief.* https://www.welivesecurity.com/2016/11/01/history-mobile-malware-cabir-sms-thief/ (accessed on 25 April 2020).

[74] *WHO reports fivefold increase in cyber attacks, urges vigilance*. (2020, April 23). WHO: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (accessed on 25 April 2020).

[75] Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., & Liu, X. (2020). Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams. *arXiv preprint arXiv:2007.13639*.