Journal of Danubian Studies and Research

Malicious Cyber Attacks

Luca Iamandi[1], Ionel Vladimir Vîrgolici[2], Alina Melania Ioniță[3], Alexandru Drăgănescu[4]

Abstract: Information plays a vital role in the development of human society, an element that cannot be neglected in interpersonal relationships. The use of information technologies in all fields has proven its effectiveness through the speed and efficiency with which activities are carried out. This makes cybercrime play an increasingly important role in organized crime. To counter this phenomenon, states must improve their IT systems and technologies, while at the same time creating a legal framework that criminalizes all antisocial acts generated through information technologies. Also, more attention should be paid to the training of those who are involved in combating this phenomenon and the appropriate information of the people who use the computer systems, thus creating a stronger security barrier against this type of crime.

Keywords: Ransomware; Security; Cyber-attacks; Information; Cybercrime

1. Introductory Aspects of Cyber Attacks

Cyberattacks caused by cybercrime are expanding rapidly thanks to the interconnectedness and transcendence of physical and virtual boundaries. Criminals exploit people's vulnerabilities in search of easy income and social and economic

[1] Professor, PhD, Danubius University of Galati, Romania, Address: 3 Galati Blvd, Galati 800654, Romania, E-mail: luca_iamandi@yahoo.com.
[2] Ministry of Finance, Romania, Address: 16 Libertății Blvd, District 5, Bucharest, Romania, Corresponding author: vladimir.virgolici@gmail.com.
[3] Ministry of Finance, Romania, Address: 16 Libertății Blvd, District 5, Bucharest, Romania, E-mail: alina.ionita@mfinante.gov.ro.
[4] Regional Transport Police Department, Romania, Address: 1 Strada Gării, Galati 800222, Romania, E-mail: draganescu_alexandru@yahoo.com.

disparities. Computer security is becoming more and more important for prevention and for preventing hackers of any level of knowledge.

Ransomware is an advanced variant of malware that blocks and simultaneously encrypts data, requiring a ransom to unlock the compromised device. Some malware variants exploit simple algorithms to lock devices. This way even if computer literate people can eliminate cyber-attacks, the data can only be recovered with the key provided by the attackers, which is usually demanded in exchange for some winnings. Since this type of attack can be paid for by anonymization, it is almost impossible to trace their trail. In addition, tracing the trail of redemption money can be difficult due to its payment in Bitcoin.

2. REvil Cyber Attack

The REvil ransomware, also known as Sodinokibi, became notorious due to the scope of its attacks as early as 2019. The group attacked critical infrastructures that led to delays and even supply shortages.

REvil was among the most active ransomware variants in 2021, but in early 2022 it was officially shut down after Russia's Federal Security Service announced that it had dismantled the REvil hacker group and indicted two of its members its . However, IT security companies believe that their guard should not be let down, even if the REvil group has a damaged image and the recruitment of new affiliates, at least for the time being, would be unlikely.

As a modus operandi, the group stole and encrypted victims' data and later demanded a reward to hand over the decryption key. If the information could harm the victim's image, they would not only notify the victim that their data was encrypted, but also blackmail the victim that they will publish the obtained data on their Happy Blog page if the reward is not paid.

Among the cyber-attacks launched by the REvil group are listed:

- The theft of approximately one terabyte of personal computer data from the Grubman Shire Meiselas & Sacks law firm;
- In May 2020, US President Donald Trump was the victim of a cyber-attack, after which a reward of 42 million dollars was requested.

The group said it managed to breach the security of the servers of a company used by the US president to protect his data;

- On May 16, 2020, the group sent online information about the singer Lady Gaga, and the next day they sent 169 emails informing the recipients that they had compromising information about Donald Trump.
- On March 18, 2021, an affiliate of the REvil group mentioned that it downloaded computer data from the multinational hardware and electronics corporation Acer and allegedly infected their systems with ransomware, and the reward requested in this case was 50 million dollars, and if it is not paid within 24 days, then the value will be doubled;

On March 27, 2021, the Harris Federation was the victim of the attacks, after which several financial documents were published and which led to the blocking of the educational activity of 37,000 students.

- The group's most high-profile attack took place in April 2021, when plans for future Apple products were stolen from Quanta Computer. The hackers threatened to make this data public if they did not receive $50 million.
- The months of May and June 2021 represented difficult periods of time for the Brazilian company JBS SA (field of activity - meat processing) and the American company Invenergy SA (energy field). The company JBS SA was asked for a reward of 11 million dollars, an amount that was also paid to the hackers.
- The attack of July 2, 2021 led to the blocking of the activity of a significant number of providers. Their number was estimated to be between 800 and 1500. The attack targeted an IT company that managed the Kaseya application, used for supplier management, and the requested reward was 70 million dollars.
- On July 7, 2021, REvil's latest resounding attack was launched, hackers breached the servers of Florida HX5, a weapons launch and space Technology Company that had contractual relationships with the United States military and NASA, and later publish part of the stolen documents on their website. Following this attack on July 9, there was a telephone conversation between the President of the United States Joe Biden and the President of Russia Vladimir Putin about the attacks of this group.

REvil is a virus that starts by locking files. At the same time, after infecting files, it encrypts their contents, and when the encryption process is completed, it leaves a message requesting a ransom. The content of the message states that the victim must pay a ransom in virtual currency and if the ransom is not paid by the mentioned deadline, then the ransom amount is doubled.

After analyzing the program, it was identified in its hash code (ccfde149220e87e97198c23fb8115d5a) the name Sodinokibi where

"Sodinokibi.exe" was the internal file name. As I mentioned before, it is also known as REvil.

REvil is a Ransomware-as-a-Service (RaaS) program. Early in its informational development, REvil ransomware was observed to propagate by exploiting WebLogic vulnerabilities of Oracle servers.

REvil was later discovered to be part of the Ransomware-as-a-Service family. Ransomware-as-a-Service requires some members of the hacker group to know the code of the program, and other members, known as affiliates, are responsible for spreading the ransomware.

This type of ransomware allows the affiliated hacker group to spread the REvil ransomware in all possible ways, such as mass propagation attacks using exploit kits or phishing campaigns, and then other affiliate groups that have a targeted approach intervene loading tools and scripts. This way they get more rights to execute the ransomware on the victim's network or access the device by brute force. Looking at how the REvil attacks were carried out, most had different modus operandi, but several started by exploiting vulnerabilities in remote access protocols.

We can say that the REvil group was recruiting affiliates to distribute the ransomware for them. As a result of the deal, affiliates and ransomware developers would receive percentages, based on contribution, of revenue generated from ransom payments.

Considering how Ransomware-as-a-Service is done, from a practical point of view it is difficult to pinpoint the exact location of the hackers.

In September 2021, Romanian cybersecurity firm Bitdefender published a free decryption guide to help victims recover data encrypted by the REvil ransomware. As a result, from September to early November 2021, more than 1,400 companies were able to decrypt data and in doing so, avoided paying approximately $550 million in ransom.

On October 21, 2021, REvil's servers were "hacked" in an operation that took place with specialized authorities from several countries.

The action was called GoldDust and involved 17 countries, Europol, Eurojust and INTERPOL. Authorities have detained five people linked to the REvil hack and two suspects allegedly involved in the spread of the GandCrab ransomware. The aforementioned hackers are believed to be responsible for infecting more than 5,000 devices and causing approximately half a million euros in ransom payments.

As we mentioned at the beginning of the presentation of this cyber-attack, in early 2022, the REvil group was destroyed by the Federal Security Service of Russia.

3. Ryuk Cyber Attack

Ryuk is a ransomware version that is produced by hackers from the WIZARD SPIDER group, who through their criminal activity have managed to compromise government institutions, academic institutions, healthcare, manufacturing and technology organizations. In 2019, Ryuk had the largest ransom demand for a single cyber-attack, worth $12.5 million, and by the end of 2020 it is estimated that it would have capitalized a total of $150 million.

Ryuk ranks among the most dangerous ransomware cyberattacks. According to a report by a cyber security company, Ryuk holds the top 3 out of 10 ransom demands of 2020, at $5.3 million, $9.9 million, and $12.5 million. Considering the amount of ransoms demanded they are considered to be "big game hunters".

Regarding the mode of operation, when the ransomware infects a system, it first stops 180 services and 40 processes to facilitate the attack, and from this point the encryption can be done. It essentially encrypts all data that might be of interest.

Ryuk has the ability to encrypt remotely, having the Wake-On-Lan feature, which allows the device to be turned on remotely and start encryption, thus streamlining the encryption process. Hackers leave a .txt note on the desktop with the titles "RyukReadMe.txt" or "UNIQUE_ID_DO_NOT_ REMOVE."

Ryuk can use download-as-a-service (DaaS), which involves downloading malicious programs in order to infect the target devices.

Victims unknowingly fall prey to phishing attacks that are intended to initiate the infection process. An IT security company estimates that 91% of ransomware attacks start with phishing emails.

As with REvil, Ryuk is part of the Ransomware-as-a-service (RaaS) family and is considered one of the most well-known programs of its kind.

Once the victim clicks on the infected attachment or link from the phishing email, Ryuk downloads additional malicious elements called droppers, Trojans such as BazarBackdoor, Trickbot, Zloader, BazarBackdoor, which are designed to run and install Ryuk ransomware.

Although there may be signs of compromise and identification of precursors to a Ryuk infection, the job of a network administrator is a difficult one, as infection can occur with many different attack vectors.

The Ryuk ransomware has been used by hackers to attack government institutions, the education system, and even technology companies.

Among the Ryuk attacks is the attack against an IT security firm. But ransomware is recognized for its attacks against the medical field, thanks to the fears instilled by the COVID-19 pandemic.

On September 27, 2020, Universal Health Services, a medical company that owns hospitals in the US and UK, suffered a Ryuk ransomware attack, after which it recorded an estimated $67 million in damage.

Following the analysis of the attack by a company in the field, it turned out that the infection has a high chance of having a phishing e-mail as its starting point. A code fragment of a Trojan horse called Emotet was discovered in that email. Running Emotet led to the installation of another Trickbot trojan, and later allowed the hacker group, WIZARD SPIDER, to manually install the Ryuk ransomware.

Although hospitals were working at full capacity and the medical field was operating at high levels of stress, in October 2020 hackers infected two more medical institutions, Lawrence Health System in New York and Sky Lakes Medical Center in Oregon. The attacks made it impossible to use the computers, making it impossible to record medical records, and it would have taken several weeks to restore the functionality of the devices.

5. Recommendations and Law Proposals

Given how indispensable computer technologies are to the conduct of human activities, cybercrime developed today poses a real risk and harms society. To limit these threats, states must step up their modernization efforts, create an adequate legal framework, and train people in the fight against cybercrime. The eminence of caution must apply to all users of computer systems, so as to ensure an adequate level of security. Antivirus and operating system performance must be up to date, and equipment or devices affected by attacks must be unlocked as quickly as possible. In addition, it is recommended not to make payments to hackers, but to use specialized services in the field of computer security. These measures can help limit the contribution to the spread of cybercrime.

It is clear that educating people who use computer systems about computer security must be a priority. This can help limit the risks caused by Ransomware malware. Thus, several measures can be taken to protect the computer system from cyber harm, such as making backup copies of databases, installing a working antivirus program, updating software and operating systems, isolating infected devices, carefully checking links and files attached in emails, enabling the display of file extensions and monitoring processes. Payment of the amounts demanded by hackers is not encouraged because, by making these transactions, one is acting in favor of cybercrime.

References

Acronis (2021). *Acronis Cyberthreats Report 2022 unveils cyberthreat predictions.* https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/.

CISA (2021). *AA21-265A-Conti Ransomware TLP White.* https://www.scribd.com/document/529330620/AA21-265A-Conti-Ransomware-TLP-WHITE.

ENISA (2021). *Enisa Threat Landscape 2021*. https://www.enisa.europa.eu/publications/enisa-threatlandscape-2021.

UNODC (2021). *Digest of Cyber Organized* Crime. https://www.unodc.org/documents/organizedcrime/tools_and_publications/21-05344_eBook.pdf

Surdu, Ileana-Cinziana (2018). Cybersecurity. Risks, Threats, and Trends of Manifestation in Romania. *International Conference RCIC'18,* pp. 365-372. https://www.afahc.ro/ro/rcic/2018/rcic'18/volum_2018/365-372%20Surdu.pdf.

Hive Ransomware Attackers Extorted $100 Million from over 1,300 Companies Worldwide. https://thehackernews.com/2022/11/hive-ransomware-attackers-extorted-100.html.