FERRIS STATE UNIVERSITY

IMAGINE MORE

Information Security & Intelligence

Ransomware: Current Trends, Challenges, Target Areas, And Its Prevention

Mehul Suresh Modi

Spring 2020

Presented to the Information Security & Intelligence Program

Ferris State University

In partial fulfillment of the requirement for the degree of Master of Science

CAPSTONE REPORT

Approved by

_____

Dr. Greg Gogolin, Professor at Ferris State University

Mehul Suresh Modi

Ransomware: Current Trends, Challenges, Target Areas, And Its Prevention

MISI 799 – Integrated Capstone Project

Instructor: Professor Greg Gogolin

Ferris State University

Date: 04/22/2020

Abstract

In this digitized world, the accessibility of information and data has become very easy and is available at the fingertips anytime and anywhere. It has improved the lives of everyone and the efficiency and productivity within organizations. However, security concerns and integrity of data remains a big challenge. Cyberattacks such as ransomware, malware, trojans, phishing, spam, and viruses cause a lot of productivity loss and millions of dollars damages to organizations worldwide. This literature research will address the target areas of ransomware attacks and the current trends in ransomware attacks and its prevention measures.

Table of Contents

Introduction

Ransomware attacks have become a global epidemic. It continues to accumulate victims worldwide, forcing the victims to pay significant sums of a ransom in return for their hacked data. Ransomware has taken thousands of individuals and entire corporations as hostage, destroyed valuable data and collected hundreds of millions of dollars as ransom.

The idea of ransomware already appeared in 1989 when one was created by Joseph Popp and was used to hide files on the hard disk of the victim and encrypt their names. Then in 1996 Adam L. Young and Moti Yung conceived the notion of using cryptography for offensive purposes, as opposed to defensive which was the norm. The increased value and ease of development, due to ubiquitous network access that provides easy access to many possible targets and malware markets that allows attackers to simply buy or rent malware, makes it an interesting proposition for these attackers and the main concern for home users as well as network administrators.

Ransomware has attracted great attention from cyber-security experts in recent years because of the fast growth of its attacks and the creation of new variants capable of bypassing antiviruses and anti-malware. One area where ransomware is predicted to experience rapid growth is in connected devices collectively known as the Internet of Things (IoT). With the years passing by we are witnessing new variants of ransomware attacks. They have shifted their focus from individuals to organizations.

For the past decade, hackers have been motivated by financial gains. In recent time, the ransomware attacks have been seen in businesses and government organizations at an alarming rate. Thus, our literature research will address the target areas of ransomware attacks whether they are government organizations, non-profit organizations or the business sector. Our research will also address the current trends in ransomware attacks and its prevention measures.

Background of the Study

In the last five years, digital extortion has significantly increased as the number of online applications and services, and smart mobile devices continue to grow exponentially. Ransomware is now rated as the biggest cyber scam to hit businesses because the impact of ransomware was very tremendous. Destructive ransomware can spread by itself and hold entire networks hostage.

According to the Federal Bureau of Investigation (FBI), estimated losses of about one billion US dollars ($1 billion) were incurred to ransomware attacks in the year 2016. This shows that to have their data unlocked a good number of victims eventually pay the ransom. Nearly 40 percent of ransomware victims paid the ransom. On an average of three out of four ransomware criminals were willing to negotiate prices for decryption. Unfortunately, traditional preventive and reactive security measures are not adequate to handle the effect of ransomware attacks.

This data shows that it is important to conduct research to find preventive measures and address the current trends in ransomware attacks, the target areas of ransomware attacks, the damage caused by ransomware attacks, and best practices in avoiding and preventing these ransomware attacks.

Purpose

The purpose of this research project is to present literature that addresses the current trends in ransomware attacks, the target areas of ransomware attacks, the damage caused by ransomware attacks, and best practices in avoiding and preventing these ransomware attacks. Another purpose is to share the research findings about ransomware that currently challenges the computer and network security, and data privacy.

Problem Statement

This research project aims to present literature that addresses the current trends in ransomware attacks, the target areas of ransomware attacks, the damage caused by ransomware attacks, and best practices in avoiding and preventing these ransomware attacks.

This paper will address the following research questions:

1) What are the various types of ransomware and what they do? What are the mechanisms used to encrypt and how it propagates?

2) What are the best practices in avoiding and preventing ransomware attacks?

2 A) What are the methods for recovering from a ransomware attack?

3) In recent five years (2015-2020), what are the trends in the ransomware attacks?

3 A) In recent five years (2015-2020), what are the target areas of ransomware attacks (geographically and type of exploit wise)?

Secondary Research

Limitation of Current Defense Mechanisms

Ransomware attacks share undebatable similarities with other types of malware attacks particularly in making use of evasion techniques and distributing malicious payloads. Perhaps the main reasons for this level of similarity are that adversaries' main goals before launching an attack on victims' machines are:

1) To bypass common anti-malware solutions.

2) To utilize every possible distribution channel to expose as many victims as possible to such attacks (Kharraz, Robertson, & Kirda, 2018).

Therefore, it is worthwhile to investigate which specific problems in detecting ransomware attacks are similar to other malware attacks, and which problems are different in nature and require more investigation. For example, similar to other types of malware attacks such as Trojans, opening email attachments or clicking on malicious advertisements may increase the risk of being infected by malware including ransomware. Therefore, some of the current techniques that are used to identify suspicious payloads are still useful in detecting the malicious binaries that deliver ransomware (Kharraz et al., 2018).

Similarly, some of the general static analysis techniques such as Portable Executable (PE) analysis tools or packer detection techniques can still provide helpful information about a given malicious binary. However, these tools and techniques can barely provide very useful insights about the specific behavior of a given ransomware sample. More specifically, unlike most of the modern malware attacks, ransomware attacks are not usually designed to be stealthy after the infection phase as the whole point of the attack is to notify victims that their machines are infected (Kharraz et al., 2018). Furthermore, the core functionality of a ransomware sample, the

cryptosystem module, usually works similar to the favorable applications that are often used for privacy-preserving purposes. The similarity of the behavior of ransomware compared to a subset of benign applications as well as the differences with other types of malware attacks in the attack strategy have made the current automated analysis techniques less effective in detecting and analyzing the attacks or protecting end-users. Therefore, it is quite useful to develop tools that can accurately extract the ransomware behavior and improve the current automated analysis systems, or end-point solutions given these similarities and differences (Kharraz et al., 2018).

Similarities and Differences with Other Classes of Malware

Ransomware payloads are usually armed with techniques that make the detection or analysis of the payload more difficult which is similar to other malware attacks. The thing that differentiates the malicious payload from other types of malware attacks is that the malicious binary has an additional set of core functionalities. This function determines how the encryption keys should be generated and maintained, how the malicious process should attack user data and request a ransomware fee (Kharraz et al., 2018).

Enhancing Detection Techniques

Malware research is an arms race. Therefore, there is always the possibility that malware developers find heuristics to bypass the detection mechanisms used in the analysis systems, or on end-user machines. Therefore, developing techniques that can increase the cost of evasion, enhance the malware detection systems, and assist malware analysts to unmask the inner workings and functions of the malicious code is quite useful in detecting all types of malware including ransomware (Kharraz et al., 2018).

1) Automating Payload Analysis:

Malware authors usually use several anti-analysis techniques to increase the level of the attack sophistication. This makes the payload analysis largely a manual process. Therefore, developing techniques that facilitate the automatic examination of malicious binaries is highly desirable. Dynamic analysis is a promising technique to analyze the malicious binary and reveal the main functionalities of the malware sample (Kharraz et al., 2018). Running a malware sample in an analysis environment and extracting its behavior is a non-trivial task as most of the current malware families, including ransomware, perform several different environmental checks to ensure that they are being executed in real-user machines and not in an analysis environment.

Recently, Kirat et al. proposed a bare-metal automated analysis environment, called BareCloud, which does not introduce any in-guest component which makes the proposed solution more transparent to sophisticated evasion techniques. Similarly, Kharraz et al. proposed UNVEIL, a sandbox that is specifically designed for detecting ransomware. UNVEIL creates a fake but enticing user environment for the malicious binary to run by manipulating the return values of some of the system functions that are frequently used by a malicious process (Kharraz et al., 2018).

2) Improving Monitoring Techniques:

Work by Kirat et al. discussed the necessity of developing reliable monitoring mechanisms in malware sandboxes to reveal the inner workings of ransomware samples. It is very important and useful to understand how the encryption key is generated by analyzing the execution traces, how a ransomware sample makes user data inaccessible and how malware authors employ cryptosystems (Kharraz et al., 2018). For example, UNVEIL uses a kernel-level module that

monitors the system-wide monitoring by intervening in the interaction of user-mode processes with the filesystem. The filesystem monitor in UNVEIL has direct access to data buffers involved in I/O requests, giving the system full visibility nearly all filesystem modifications. The generation of I/O requests happens at the lowest possible layer to the filesystem. Whenever a user thread invokes an I/O API, an I/O request is generated and is passed to the filesystem driver (Kharraz et al., 2018). In each malware execution, UNVEIL generates a set of I/O access sequences for the sample. The detection criterion used by the system to detect ransomware samples are to identify privileged operations in I/O sequences in each malware run.

More recently, Xu et al. proposed a novel technique, called CryptoHunt, which complements current malware forensics techniques by identifying cryptographic functions in an obfuscated binary (Kharraz et al., 2018). CryptoHunt captures the semantic of possible cryptographic algorithms using bit-precise symbolic execution in a loop. While CryptoHunt can facilitate the identification of ransomware samples in an obfuscated binary, and potentially expedite the malware analysis process, it is also desirable to find cryptographic functions in attacks where the malware samples incorporate customized cryptosystems rather than well-known, standard cryptosystems to bypass detection techniques. Recent studies have shown that malware authors utilize home-brewed cryptosystems to evade techniques that infer the functionality of a suspicious binary by looking at API calls imported by the program (Kharraz et al., 2018).

Methodology

Study design

This research adopted a descriptive methodology. A descriptive method was chosen because it is real-world issue and a lot of research has been going on for the solution of this issue. Explicitly, a descriptive approach is warranted when the nature of research questions require exploration (Stake, 1995). Descriptive research questions often begin with how or what, so that the researcher can gain an in-depth understanding of what is going on relative to the topic (Patton, 2002). This research aims to present literature that addresses the current trends in ransomware attacks within last five years, the target areas of ransomware attacks, the damage caused by ransomware attacks, and best practices in avoiding and preventing these ransomware attacks.

Audience

The primary audience members for this research are leaders in information security departments such as Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), and Information Technology (IT) program managers. Information security department leaders will be interested in this information because they will be able to stay informed of any high-security and high-risk situations related to ransomware and will be able to delegate the work to prevent ransomware attacks.

As the ransomware attacks the integrity and the structure of the organizations, this information will be of interest to the CIOs because they do not want to oversee their responsibilities. CIOs will be able to make informed and often crucial decisions regarding the

security of their IT infrastructure in a timely manner. IT program managers can be benefitted from this information as they can devise and implement plans to address the ransomware threats. In many cases, Chief Executive Officers (CEOs) will also find the information on ransomware and how to prevent attacks useful due to the risk posed by ransomware to organizations.

Data Collection Method

The search strategy I employed involves the use of Google Scholar and the FLITE library - Ferris State University, which provided access to research databases related to Information Technology subjects. I started the search by using keywords such as ransomware, bitcoins, and cryptocurrency; I then narrowed the search to ransomware amongst organizations. The most reliable and trusted databases that provided significant information regarding ransomware were ScienceDirect, ResearchGate and ProQuest. I found several relevant journal articles and other scholarly sources by searching within these two research databases. Because ransomware is a fairly recent phenomenon occurring amongst various industries and organizations, I narrowed the date range of the searches to the last few years, ranging from 2015-2020. The search also resulted in articles about ransomware that is present in various industries including healthcare and both the private and government sector. Even though ransomware has only become a widely discussed subject in the last few years, the search resulted in a surplus of informative articles and real-life examples.

Libraries and search engines. I used the following library and search engines in searching for research materials required for this Capstone:

• FLITE Library - Ferris State University.

• Google Scholar.

Databases. I used the following databases for the research:

• ScienceDirect.

• FLITE Library - Ferris State University database.

• ProQuest.

• ResearchGate.

Key words and phrases. I used the following keywords to search for appropriate reference sources:

• Ransomware.

• Cybersecurity.

• Bitcoins.

• Malware.

• Cyberattack.

• Corporate cyber-attacks.

• Business cybercrime.

• Trojan attacks.

• Enterprise cybercrime.

• Cyber worm.

• Computer virus.

• Backup encryption.

• Ransomware amongst organizations.

Literature Review

Introduction

Ransomware is a type of malware that cybercriminals use to hold people to ransom. Ransomware has now become a global epidemic. In a ransomware attack, the target can be an individual or an organization (Lawler, 2000). There are various ways through which it can spread some of which are given below:

- Attachments or links in phishing emails.
- Downloads from infected web sites.
- Infected USB sticks.

Ransomware attacks a computer or network and once that is done it blocks access to the system or it encrypts the data on that system. To regain access to the data and computer cybercriminals demand a ransom from the victims (Lawler, 2000).

Types of Ransomware

Ransomware can be mainly categorized into two types:

1) Crypto Ransomware
2) Locker Ransomware

- Crypto Ransomware encrypts important files on the computer due to which the user cannot access them. To get back the files, victim has to pay the demanded ransom to the cybercriminals that conducted crypto ransomware attack (Lawler, 2000).
- Locker Ransomware is a bit different than crypto ransomware. It does not encrypt files but locks the victim out of their device. The victim has to pay the ransom in order to unlock the device (Lawler, 2000).

Common Ransomware Variants

PC Cyborg. The first reported ransomware variant was known as PC Cyborg and it was launched in December 1989. In this attack, the victim received messages that read the user's license has expired. This attack used a symmetric cryptography encryption algorithm which was not difficult to decrypt (Lawler, 2000).

GpCode. In May 2005, a new variant of ransomware known as GpCode was reported which employed custom symmetric encryption. This malware propagated as a job advert through spam e-mail attachment. All non-system files were encrypted using a static key. As soon as the encryption was completed, the original data was deleted. However, this key was discovered simply by comparing the original data to the encrypted data. In June 2016, a new variant of GpCode called GpCode.AG was discovered which was based on 660-bit RSA public key (Lawler, 2000).

Reveton. It is a ransomware that is commonly spread through pornographic websites. It is also known as Police Ransomware. It displays a notification page to its victim by changing the extensions in the windows/system 32 folder (Lawler, 2000).

Locker Ransomware. In 2007, the Locker Ransomware was identified. The data can be transferred to another location as the victims' data are not locked but only their devices are locked. A similar ransomware for mobile devices was also identified. It locks the victims' mobile devices. It takes photos with mobile phone cameras, answers and drop incoming calls and

defrauds victims through mobile banking applications. This ransomware is known as ColdBrother Ransomware (Lawler, 2000).

Crypto Ransomware. This ransomware encrypts important files on the computer due to which the user cannot access them. To get back the files, the victim must pay the demanded ransom to the cybercriminals that conducted the Crypto Ransomware attack. Command and control server control the choice of encryption keys and coordination of attacks. CTB Locker, Lock, Tesla Crypt, and Crypto Wall are all variants of Crypto Ransomware (Lawler, 2000).

CryptoWall. In November 2013, CryptoWall was introduced. This malware is distributed by e-mail as an attached zip file and contains a script file and an exploit kit. The codes are copied into %APPDATA% and the malware is injected into explorer.exe which creates a registry value run key in the local user registry root path. Due to this, even after a reboot, the malware remains in the victims' computer. Processes like 'vssadmin' and 'dcbedit' are run by the malware to ensure that the system cannot be restored to an earlier point. Thereafter, to encrypt files and communicate with the command and control server, a svchost.exe is initiated. About 31% of ransomware attacks were traced to CryptoWall which makes it one of the popular ransomware variants (Lawler, 2000).

CryptoLocker. It can manipulate the Internet files by creating a set of extensions in the administrator's account. Critical files are detected for subsequent encryption and executable files are created in 'localAppData'. The malware performs the encryption process by using the RSA +

AES algorithm. Its exploit kit is known as Angler. On the other hand, CryptoDefense uses a low-level cryptographic API that is available in Windows operating systems (Lawler, 2000).

TeslaCrypt. It is another variant of ransomware that uses AnglerINuclear exploit kits to exploit vulnerable websites. All shadow copies are deleted using the 'vssadmin' command and it has a distribution scheme similar to CryptoWall (Lawler, 2000).

Locky. In February 2016, a ransomware known as Locky had its first attack. The malware program was spread by attaching a Microsoft Office document to spam e-mail. The target's computer is filled with a malicious program from a macro that is attached to the document (Lawler, 2000). Locky also has the ability to extend its encryption to all network resources, external storage devices, database files and wallet.dat which makes it even more harmful in comparison to other ransomware variants (Lawler, 2000). Hardcoded command and control server Internet Protocol (IP) addresses are used by this kind of malware. A text-to-speech module is used to voice the notification of attack. Between December 2016 and January 2017, more than 200 cases were reported to have been attacked by this ransomware and most of these devices ran on Windows 10 Enterprise (Lawler, 2000). Locky mainly spreads by tricking victims to install it via fake emails with infected attachments and has the ability to encrypt over 160 file types. This method of transmission is called phishing which is a form of social engineering (Lawler, 2000).

WannaCry. I personally have observed this variant of ransomware three years ago in 2017 when I used to work as a Programmer Analyst in India. In 2017, it spread across 150 countries. It

affected 230,000 computers globally. It was designated to exploit a vulnerability in Windows (Lawler, 2000). The NHS suffered a loss of an estimated £92 million, as the attack hit a third of hospital trusts in the UK. This attack locked the users out of their system and demanded the ransom in the form of Bitcoins (Lawler, 2000). Leaving the vital health service vulnerable to attack, the attack highlighted the problematic use of outdated systems. WannaCry created a global financial impact by causing worldwide financial losses worth $4 billion (Lawler, 2000).

Figure 1. WannaCry Ransomware Extortion Dialog. Retrieved from https://www.avast.com/c-wannacry

Best Practices in Avoiding and Preventing Ransomware Attacks

Ransomware is insidious. We know that it travels through phishing emails, but it also takes advantage of vulnerabilities (Zetter, 2016). According to experts some of the recommendations for individuals and businesses trying to prevent ransomware infection are as follows:

1) Take a Backup of the Systems Locally and in the Cloud. The first and most essential step is to take a backup of the systems both locally and in the cloud. There is no need to pay a ransom to get the data back if the data is backed up (Zetter, 2016). It has the following advantages:

- The data will be backed up at a safe place where hackers cannot access the data (Zetter, 2016).
- In case of an attack, it will be easier for us to wipe our old system and repair it with backup files (Zetter, 2016).

Failure to back up our system can cause irreparable damage (Zetter, 2016).

Cloud backups are another solution. Cloud backups introduce redundancy and add an extra layer of protection to the data, thus keeping it safe from infection by ransomware (Zetter, 2016).

Apart from this, it is safer to have multiple backups. There are chances that our last back might get overwritten with encrypted ransomware files. Thus, having multiple backup files mitigates this problem (Zetter, 2016).

2) Avoiding Email Links and Attachments. The most common way to spread ransomware is the phishing attacks. The best way to avoid ransomware is to avoid clicking on links or opening attachments in spam email. However, cybercriminals have started targeting trusted websites using compromised advertising known as ‘malvertising’ to spread ransomware (Zetter, 2016). Turning off Java and JavaScript can also be helpful in avoiding ransomware.

Ad blockers can protect against malvertising (Zetter, 2016). Standardizing ad blocking software should be considered by corporate IT and employees should be trained to avoid suspicious email. According to a report by PhishMe, in March 2016, 93 percent of all phishing emails contained crypto ransomware which is said to be a drastic rise as compared to 56 percent in 2015. PhishMe also estimates that 6.3 million phishing emails were sent in the first quarter of 2016 (Korolov, 2016). According to PhishMe, there is an increase in targeted phishing emails in addition to standard phishing. For example, a resume might be included in a phishing email. Most recipients would either ignore it or forward it to HR, while an HR recipient might open it without thinking about it. Most malicious email attachments can be avoided by individual users by forwarding their emails through Gmail because it blocks suspected attachments. Corporate users can use application whitelisting, but that is not currently available for individual users (Bradley, 2015).

3) Patch and Block. Always keep the operating systems, security software and browsers up-to-date and patched. If third-party plug-ins are used, then they also need to be kept patched. Limiting user rights and whitelisting can be used by business systems which reduces the chance of a ransomware infection (Zetter, 2016). Another advantage is that these steps reduce other types of malware infections as well. The systems cannot only depend on antivirus software to block the ransomware attack as ransomware is constantly evolving to stay ahead of antivirus software (Rosenberg, 2015).

4) Drop-and-Roll. As soon as there is a sign of infection the first essential thing to be done is to turn off or unplug the infected machine immediately to minimize the damage to files. Administrators should immediately shut down the network if the infected machine is connected

to a network. This should be done to minimize the propagation of ransomware infection (Zetter, 2016).

5) Segment Network Access. When the machines are connected in a network there is a risk of the whole network getting infected as ransomware propagates through the network. We can prevent that by limiting the data an attacker can access. To ensure that the entire network security is not compromised in a single attack we can use dynamic control access. To do this, we need to segregate the network into distinct zones with each zone requiring different credentials (Dobran, 2020).

6) Install Anti-Malware or Ransomware Software. To prevent ransomware, we need to have our systems installed with the latest antivirus software that consists of antivirus, anti-malware, and anti-ransomware protection. We cannot assume that our antivirus software has the latest definition of viruses, so we need to update our virus definitions regularly (Dobran, 2020).

7) Early Threat Detection Systems. To prevent intrusions early unified threat management programs can be used. Along with antivirus software, it is beneficial to have these programs as they often offer gateway antivirus software (Dobran, 2020).

To block unauthorized access to our computer or network we can use a traditional firewall. We can add programs that filter malicious web content with these programs. To keep unwanted attachments from spam emails we should use email security best practices and spam filtering (Dobran, 2020).

To define how a group of users can use our system, we can use Group Policy offered by Windows which blocks the execution of files from our local folders. Normally such folders include downloads folder and temporary folders. Attackers place malware in a local folder which when opened infects the system (Dobran, 2020). Group Policy prevents such kind of attacks.

Software updates and patches should be downloaded and installed regularly as they improve the functionality of our systems and repair vulnerable spots in security thereby preventing attackers to exploit software vulnerabilities (Dobran, 2020).

8) Run Frequent Scheduled Security Scans. We need to scan our computers and mobile devices regularly. The second layer of defense in the security software is provided by these scans. They detect threats that the real-time checker may not be able to find (Dobran, 2020).

9) Create Recovery and Restore Points. Windows offer good functionality of System Restore (Dobran, 2020). To do this, we should go to the control panel and enter System Restore in the search function. Once we are in the System Restore, we can turn on system protection and create regular restore points. In the event we are locked out, we may be able to use a restore point to recover our system (Dobran, 2020).

10) Enforce Strong Password Security. We should encourage best practices for password security. We can do this by utilizing a password management strategy that incorporates an enterprise password manager (Dobran, 2020). Most users use the same password for multiple sites and significantly weak passwords. Multiple strong passwords should be encouraged for sensitive information (Dobran, 2020).

11) Think Before Clicking. We should not open an email with attachments that have .exe, .vbs, or .scr files unless it is from a trusted source. These files are executable files and there are chances that it may not be from a trusted source. It may be a virus or ransomware (Dobran, 2020). We should be careful with the links supposedly sent by friends who may have their addresses spoofed. We should be careful and not click on any link sent to us from an unknown. It might be a link to a webpage that may download ransomware into our system (Dobran, 2020).

12) Set Up Viewable File Extensions. The file extension shows us the type of file in our system. It is a dot followed by three or four letters. Windows has the feature to show file extensions. It can be turned on or off. It is recommended to keep this feature on so that we can see the type of file we are attempting to open. This will reduce the chances of accidentally opening a malicious file and executing ransomware (Dobran, 2020).

13) Block Unknown Email Addresses and Attachments on Our Mail Server. We can set up our mail server according to our usage. It is recommended to reject addresses of known spammers and malware. We can start filtering and rejecting incoming mails with executable files and attachments (Dobran, 2020).

14) Add Virus Control at the Email Server Level. We should install antivirus and malware software on our mail server. It can act as a safeguard for malicious email. Most of the time, a user is fooled into opening a malicious email. The virus propagates after opening or clicking on the malicious email (Dobran, 2020).

15) Block Vulnerable Plug-Ins. It is recommended to stop using third-party plug-ins. But if it is important for us to use these third-party plug-ins, it is essential to update them regularly to ensure they don't get infected by viruses (Dobran, 2020). The most common plug-ins are Java and Flash. These programs are standard on most sites. So, they are easy to attack. Hackers can use them to infect our systems (Dobran, 2020).

16) Limit Internet Connectivity. One of the best ways to protect critical data on our private network is to keep away from the Internet entirely (Dobran, 2020). Logically, if we don't bring anything into our network, our systems won't be infected with ransomware or any other malicious programs (Dobran, 2020). Most of the companies rely on the Internet and email to do

their business so this option might seem impractical but keeping Internet access away from critical servers may be a way to combat ransomware and viruses (Dobran, 2020).

17) Train the Employees and Spread Awareness. The lack of training and education often makes companies or individuals victim to ransomware. Poor cybersecurity practices and inattentiveness makes the system and network more vulnerable to cybercriminals (Dobran, 2020).

Employees should be kept up to date on the latest cyber-attacks and ransomware. They should recognize the signs of a phishing attack. They should be aware not to click on any executable files or unknown links. In order to prevent ransomware attacks from getting through to the systems, regular employee security awareness training should be provided to them which will remind them of their roles (Dobran, 2020).

Employees should be taught about the importance of examining links and attachments to make sure they are from a reliable source. They should be aware of the dangers of giving out the company or personal information in response to an email, letter or phone. For employees who work remotely, they should be aware not to use public Wi-Fi as hackers can easily break in this type of network (Dobran, 2020).

Recovery from a Ransomware Attack

Ransomware Incident Response Plan

Research by VinRansomware (2020) shows that, the following incident response plan should be followed in case of ransomware infection:

- Turn off all wireless functionalities and disconnect the system from the network.
- Determine the type of ransomware and the scope of infection: shared drives/folders, external hard drives, storage devices.
- Check for a decryptor tool.
- Restore files from backups.
- Negotiate or pay the ransom
- Protect future attacks by determining infection vectors.

Ransomware Disaster Recovery Plan

Research by Dobran (2020) shows that, in the case of ransomware infection, we should follow the following disaster recovery plan:

- A communication plan detailing who should contact whom should be set up.
- A list of equipment to be bought or rented to keep the operations going should be ready.
- Explicit instructions on where the data is stored and how to retrieve it should be written.
- To prevent ransomware from causing loss of data, a policy should be implemented of backing up data regularly.
- Vendors who may be able to restore the systems should be contacted and a list of their phone numbers should be ready.
- A disaster recovery service should be implemented.

Responding to a Ransomware Attack

Research by Malecki (2019) shows that, in an event of a ransomware attack in the network of an organization, they should follow the following steps:

- Shut down the system immediately and before doing that take a snapshot of the system. This might help to save system memory, decryption, and providing further details about the attack.
- It is recommended to shut down all the systems and the network to prevent the propagation of the ransomware infection in the network.
- At the network level, the Remote Desktop Protocol (RDP) should be blocked.
- Until the origin of the attack is fully understood, all email attachments should be blocked.
- Determine the point of entry and assess the damage.
- To get the business up and running quickly with minimal reverberations, a reliable and well-tested backup is necessary. It might take more planning to pull an entire server offline, so the organization should assess which systems were infected and depending on that take a decision to restore the infected systems from a backup.
- Restore the system's data from reliable and well-tested backup files.
- In the case of a situation where the organization does not have a backup system, it will have to depend on an alternative approach. The assessment of the value of the data that has been encrypted should be done by the IT team of the organization. Then they should decide whether it is worth hiring a ransomware expert to try and recover the data.
- The last option which is not a good idea is to pay ransom to the cybercriminals to receive the decryption keys. This is a bad idea as there is no guarantee of receiving the decryption keys even after paying the ransom. Cybercriminals often increase the ransom the longer they wait.
- Reassess the overall data protection policies of the organization.

Ransomware Data Recovery Methods

Research by Stellar Data Recovery (2020) shows that, the below given three ransomware data recovery methods can be used to recover the encrypted or deleted ransomware data:

1) Backup. This is the best option for recovering data from a ransomware attack. Data can be recovered if a backup is taken regularly. Backup can be taken on any external storage device or in the cloud. If a backup is taken in an external hard drive, SSD, SD card, Pen drive, cloud storage or any other storage device, the encrypted ransomware files can be easily recovered by restoring original files from the external backup device (Stellar Data Recovery, 2020).

2. Data Recovery Software. Data recovery software can be used to recover encrypted ransomware files from external hard drive, SSD, SD card, Pen drive, cloud storage or any other storage device. This option is used when there is no backup available (Stellar Data Recovery, 2020).

3. Ransomware Data Recovery Services

Steps to Reduce the Impact of Ransomware Incident

Research by The British Computer Society (2020) shows that in the case of ransomware infection, we should follow the following steps to reduce its impact:

Before the incident

- Start with an assumption that you will have a ransomware incident.
- Preplan parameters of response in the worst condition that can occur and what options to choose from: pay the ransom, recover locally or accept the loss?
- Circulate a template to each team of the organization for review and feedback and capture what each team has to do in the process with a supporting per-incident checklist.

- To prepare the team to achieve the right outcome and to react quickly, the organization needs to work with the teams who will be responsible for remediation.

During an incident

- The ransomware response checklist should be actively managed around the relevant teams.
- An identified contact in each team responsible for reporting is essential.
- Double-check everything.
- Users and senior management should be kept informed regular updates from various teams should be coordinated.
- To cover any slippage of activities extra time is to be built at the end of the day. This can be done by setting the end-of-day deadlines early than usual.

After the incident

- The completed ransomware response checklist after the incident should be preserved and used for lessons learned activities.
- Preserve the incident response plan ready.
- Preserve the disaster recovery plan.

Current Trends and Target Areas in Ransomware Attacks (2015 to 2020)

In the 2010s, a new ransomware trend emerged. Cybercriminals started the use of cryptocurrencies and the ransom payment method. Cryptocurrencies are specifically designed to provide an anonymous and untraceable payment method so the appeal to the extortionists is obvious (Fruhlinger, 2020). Bitcoin is considered as the most high-profile cryptocurrency which is why most ransomware gangs demanded payment in bitcoins. Later, as the popularity of the bitcoin made its value more volatile, they began shifting their demands to other currencies (Fruhlinger, 2020).

By the mid-2010s attacks shot up to crisis levels. In 2018, ransomware gangs came up with another illicit way that did not require victims to figure out what a bitcoin wallet was, and it was known as cryptojacking (Fruhlinger, 2020). The cryptojacking script is used by spammers and DDoS attackers. In cryptojacking, the script quietly generates cryptocurrency in the background and eats up idle computing cycles thus converting the compromised machines into bitcoin mining rigs. As a result, in 2018, cryptojacking attacks increased by 450 percent whereas the ransomware attacks declined gradually (Fruhlinger, 2020).

Some of the trends, facts and statistics surrounding the ransomware attacks are given below:

- After 2015, cybercriminals started targeting small to mid-sized businesses and they were at the largest risk (Comparitech Limited, 2020).
- In 2018, the Beazley Group paid the highest ransom for its client which was about $930,000 (Comparitech Limited, 2020).
- According to Insider Higher Ed, cyber-attacks and ransomware marred the 2019-2020 academic school year for two American colleges. In late August, the Regis University in Denver, Colorado, faced a cyber-attack which had its entire phone and internet services shut down. Due

to the ransomware attack, all the files were locked down in the Monroe College in New York City (Comparitech Limited, 2020).

- According to SC Magazine, in early 2020, the New Orleans City Government was infected by a ransomware attack which cost the city over $7 million. The city had cybersecurity insurance due to which they received $3 million back (Comparitech Limited, 2020).
- According to Baltimore Sun, in 2019, massive ransomware hit the Baltimore City Government which cost the city a loss of $18 million (Comparitech Limited, 2020).
- According to CNET, in 2019, a ransomware attack hit New York City's capital that took several of its key services offline (Comparitech Limited, 2020).
- According to Coveware, the large rise in ransomware payments costs started with the Ryuk ransomware. In comparison to other ransomware whose, ransom payment costs are around $10,000, Ryuk demands $288,000 per incident. It also started the trend of targeting large companies and organizations with an average of more than 250 employees (Comparitech Limited, 2020).
- According to CBS News, in June 2019, a ransomware attack hit the City of Riviera Beach in Florida which cost them around $600,000 to recover their files (Comparitech Limited, 2020).
- According to Health IT Security, in early 2019, multiple healthcare providers were hit by ransomware attacks which cost them around $75,000 individually (Comparitech Limited, 2020).
- According to Symantec, in 2018, enterprise ransomware infections increased by 12 percent and that they accounted for 81 percent of all ransomware attacks (Comparitech Limited, 2020).
- According to Times Union, in late 2019, Albany County in New York was hit by three cyberattacks in three weeks. There was also a Christmas day attack on the Albany County

Airport Authority (ACAA). The ransom amount was undisclosed by the ACAA (Comparitech Limited, 2020).

- According to BBC, the biggest ransomware attack against a commercial business in history was faced by Danish company Demant which cost them around $85 million. The company had to reduce its workforce to using pen and paper until the ransomware infection was resolved as they lost access to 22,000 computers in 40 countries (Comparitech Limited, 2020).
- According to Datto, businesses incurred a loss of $75 billion per year due to ransomware attacks. The FBI suggests ransom payments are totaling around $1 billion (Comparitech Limited, 2020).

- Ransomware is now included in the top 5 threat worldwide. Verizon has named it as a top-five threat as it continues to grow in popularity (Eric, 2020).

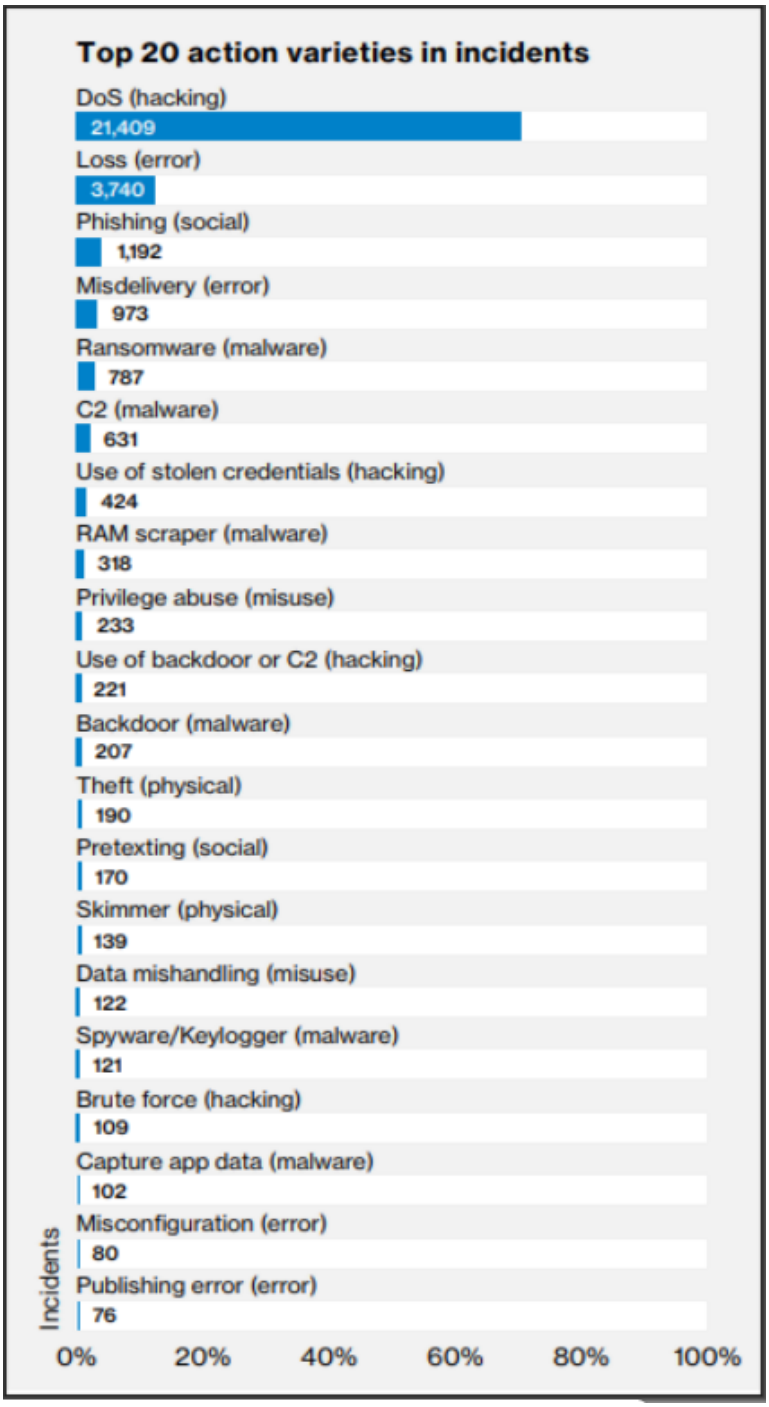

Figure 2. Ransomware included in top 5 threat by Verizon. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- As the biggest ransomware targets are still small and medium-sized businesses, consumer ransom rates are on a decline (Eric, 2020).

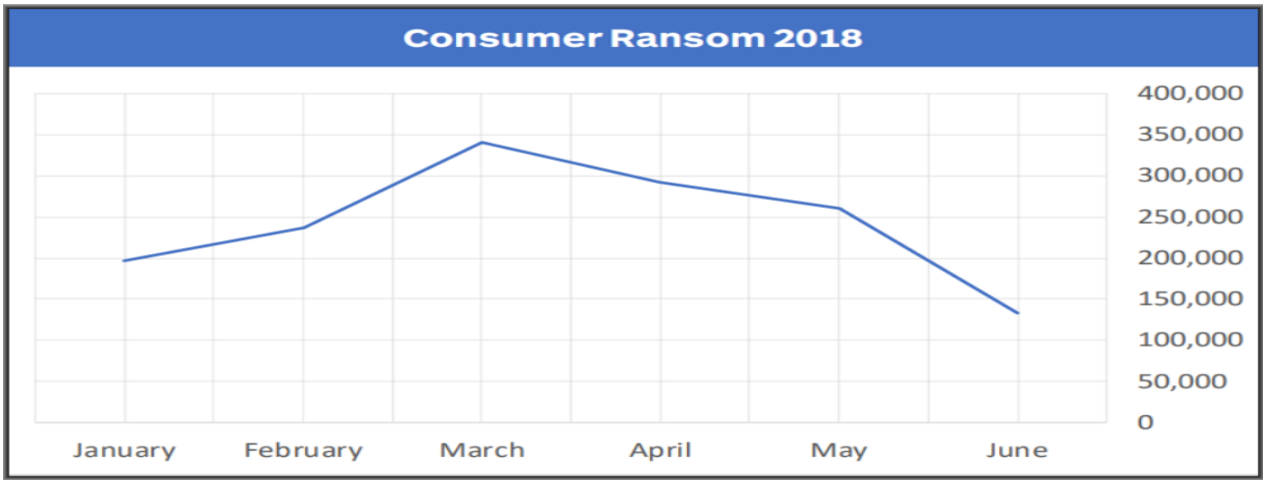

Figure 3. Declining Consumer Infection Rates. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- A common method to deploy ransomware to a target's machine is via Malware. Ransomware accounts for around 56 percent out of 1,379 incidents involving Malware (Eric, 2020).

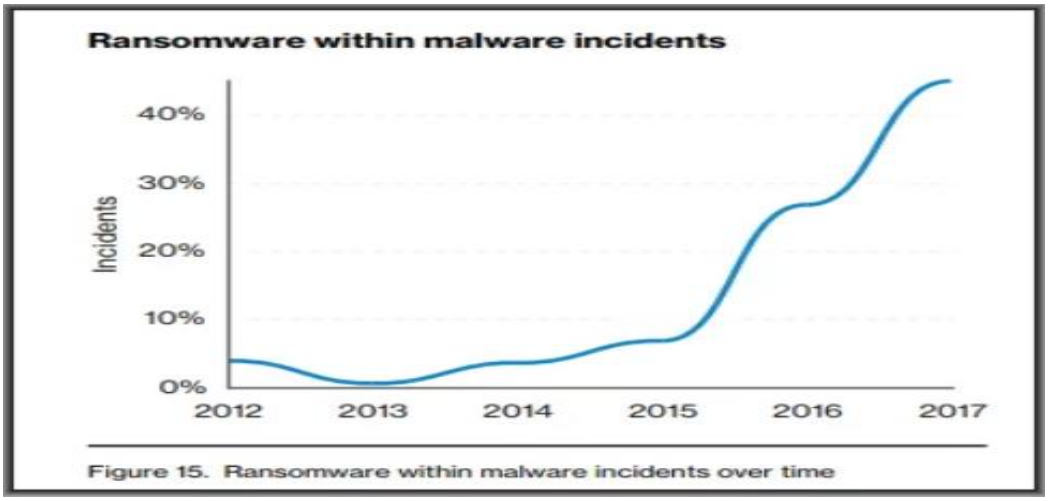

Figure 4. Ransomware and Malware are highly Correlated. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- Ransomware is the second largest cybersecurity threat for retail businesses because they often house large databases of their customers' information (Eric, 2020).

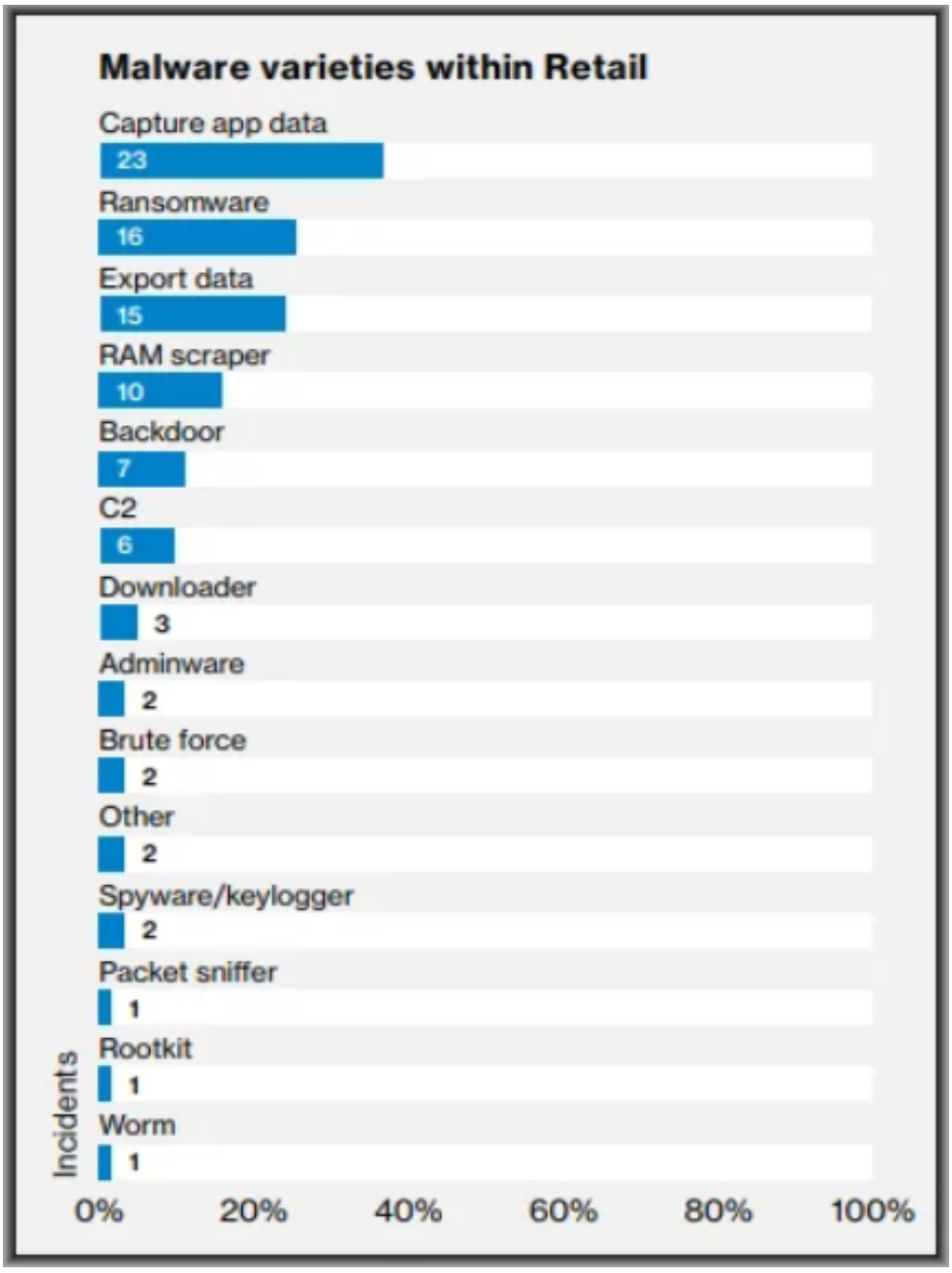

Figure 5. Ransomware – 2nd biggest cybersecurity threat in retail. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- The overall ransomware infection rates are growing steadily. Larger businesses are becoming targets while consumer ransomware is declining (Eric, 2020).

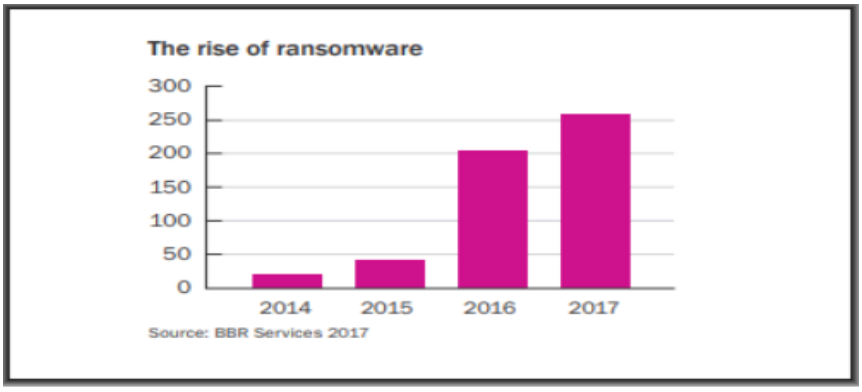

Figure 6. Ransomware continues to grow annually. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- According to Barracuda, 47% of businesses have been affected by ransomware. Of these businesses, the healthcare industry is the most attacked at 46%, while the financial and professional services industries follow at 12% each respectively (Eric, 2020).

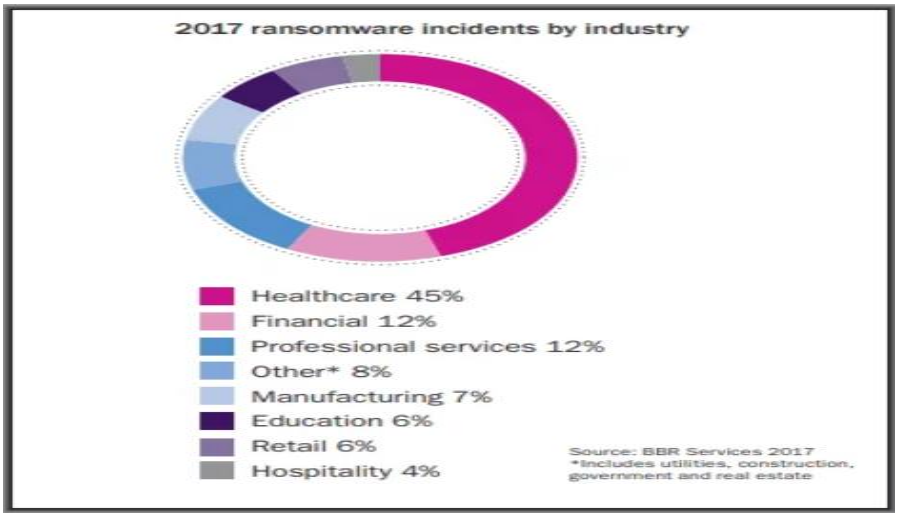

Figure 7. Healthcare industry is the most targeted industry by ransomware. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- Ransomware is constantly evolving, and the number of variants is increasing every year (Eric, 2020).

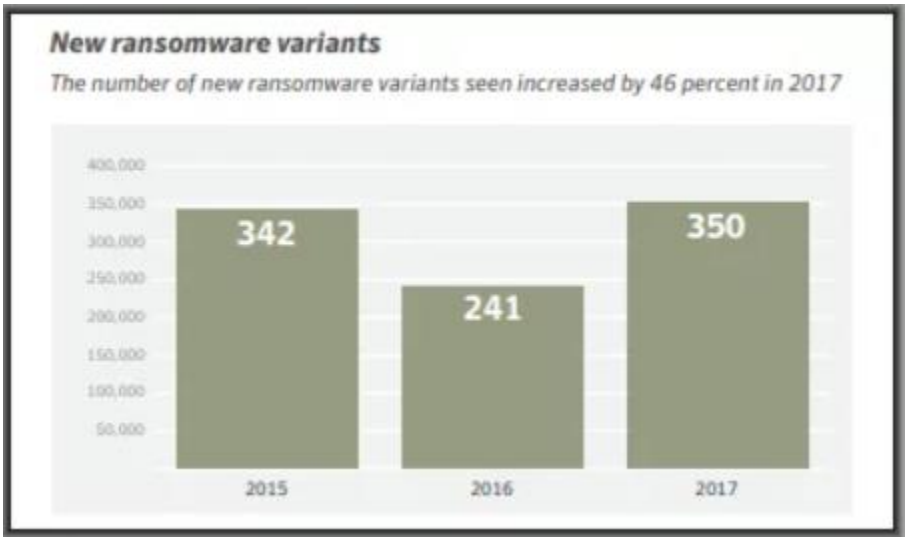

Figure 8. New ransomware variants growing annually. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- Companies in the United States are the second most affected by the well-known Petya ransomware with businesses in Ukraine being the first (Eric, 2020).

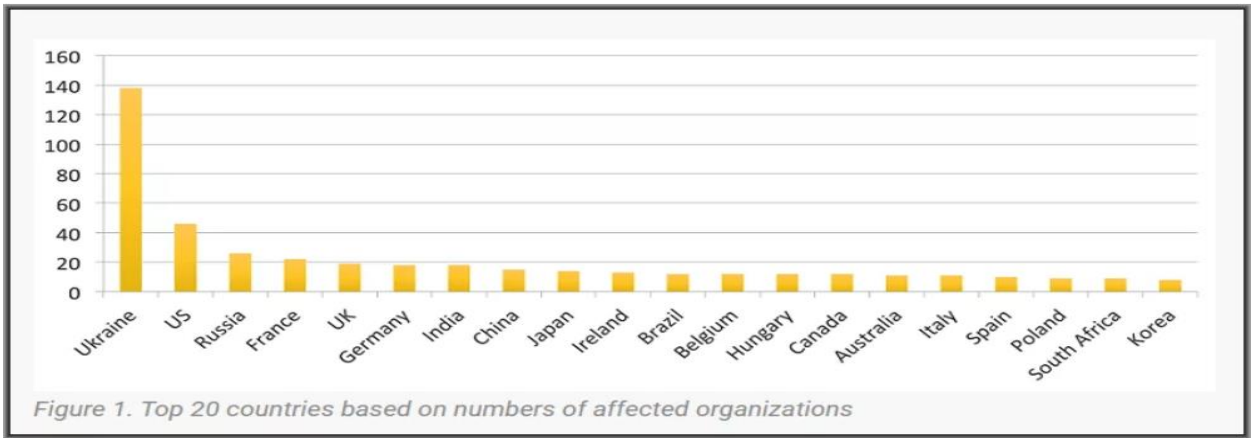

Figure 9. U.S. companies are 2nd most affected by Petya ransomware. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- Due to the swift rise in crypto prices, ransomware has become a major player in the crypto industry (Eric, 2020).

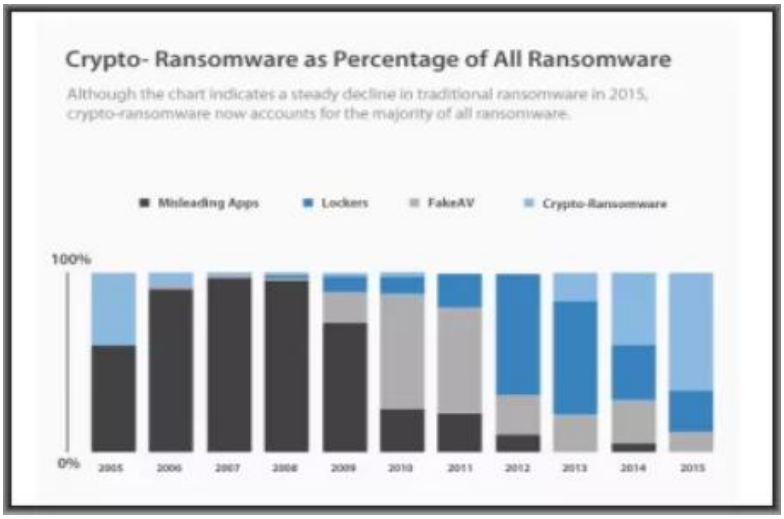

Figure 10. Ransomware is a major player in crypto industry. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- Ransomware is rarely paid by the organizations in the United States. However, 22 percent of German businesses, 58 percent of United Kingdom companies, and 75 percent of Canadian companies did pay the ransom in ransomware attacks (Eric, 2020).

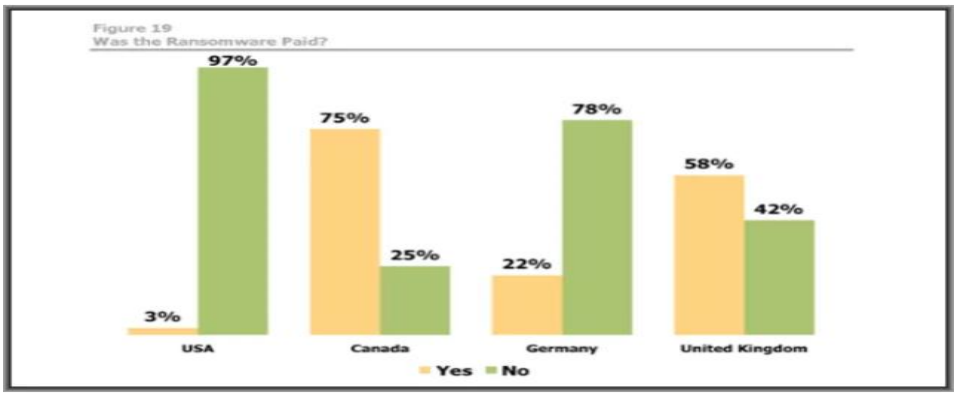

Figure 11. Ransomware is rarely paid by organizations in the U.S. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- According to 99 percent of multiple service providers, the most frequent target of a ransomware attack is the Windows operating system. However, any operating system can fall victim to a ransomware attack (Eric, 2020).

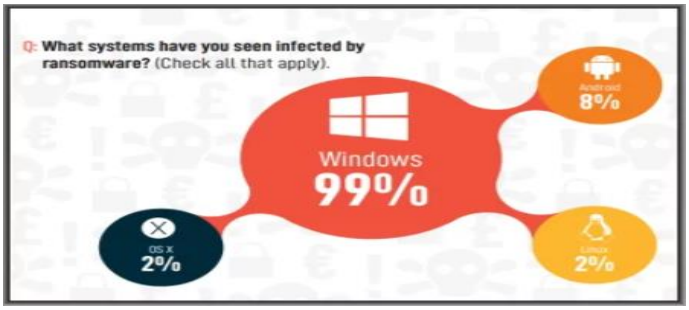

Figure 12. Windows is still the most targeted system of ransomware. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

- Ransomware attacks are worldwide. Many countries and its sectors have been infected by ransomware attacks and its variants (Eric, 2020).

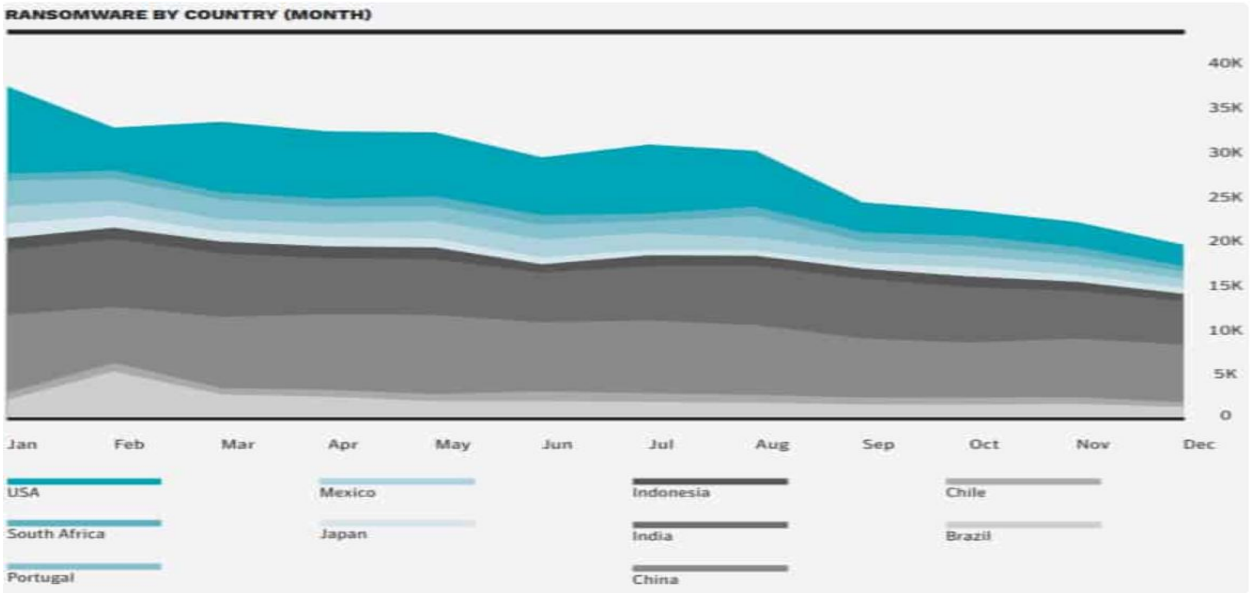

Figure 13. Ransomware by country. Retrieved from https://www.comparitech.com/antivirus/ransomware-statistics/

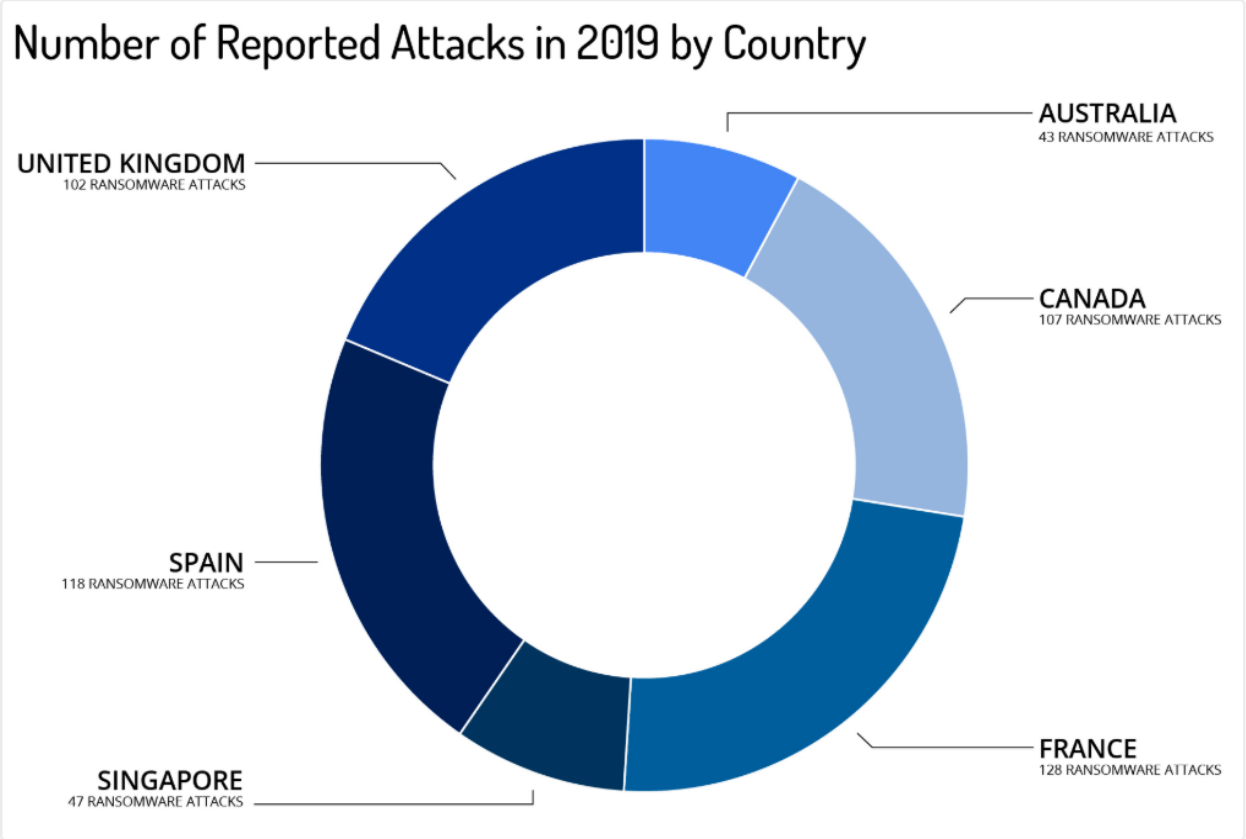

Figure 14. Number of reported ransomware attacks in 2019 by country. Retrieved from https://www.recordedfuture.com/ransomware-trends-2020/

Australia	Canada	France	Singapore	Spain	United Kingdom
Utilities	Publishing	Publishing	Hospitality	Telecom	Finance
Publishing	Construction	Service	Banking	Service	Healthcare
Finance	Banking	Pharmaceuticals	Publishing	Petroleum	Pharmaceuticals
Automotive	Education	Metals/Mining	Education	Finance	Transportation

The top four sectors hit by ransomware attacks for each country.

Figure 15. Top 4 sectors hit by ransomware attacks for each country. Retrieved from https://www.recordedfuture.com/ransomware-trends-2020/

- Some of the ransomware variants and their attacks geography wise are given below:

Ryuk

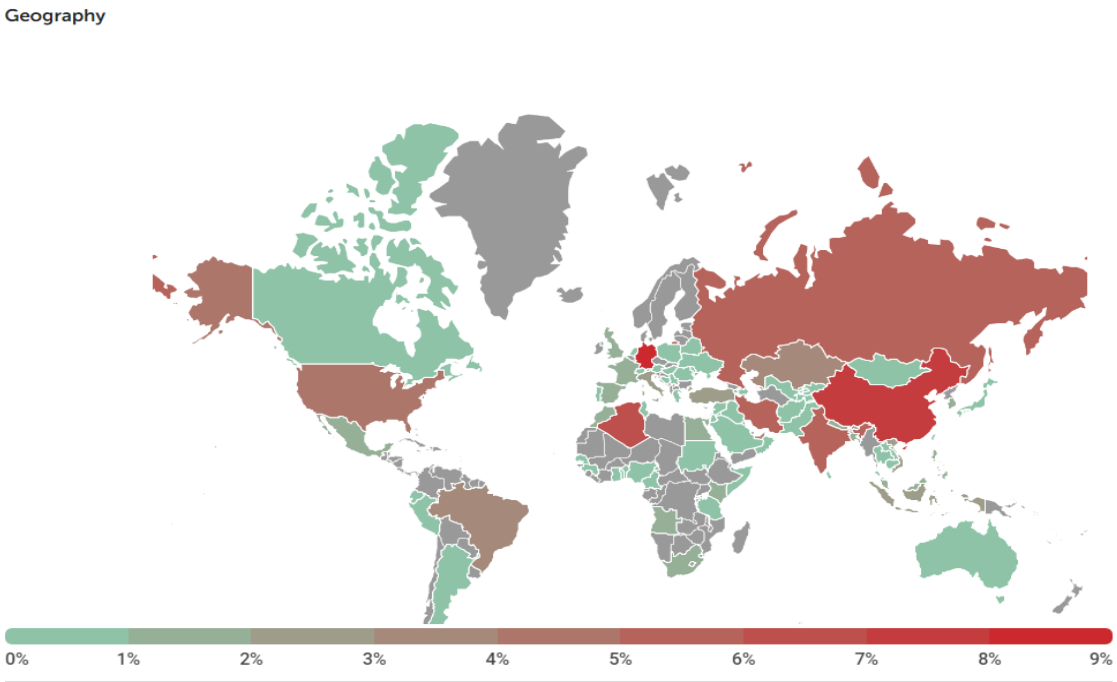

Figure 16. Ryuk ransomware infected areas geography wise. Retrieved from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

TOP 10 countries

	Countries	%*
1	Germany	8.60
2	China	7.99
3	Algeria	6.76
4	India	5.84
5	Russian Federation	5.22
6	Iran	5.07
7	United States	4.15
8	Kazakhstan	3.38
9	United Arab Emirates	3.23
10	Brazil	3.07

**Percentage of users attacked in each country by Ryuk, relative to all users attacked worldwide by this malware*

Figure 17. Percentage of users attacked by Ryuk ransomware in each country. Retrieved from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

Purga

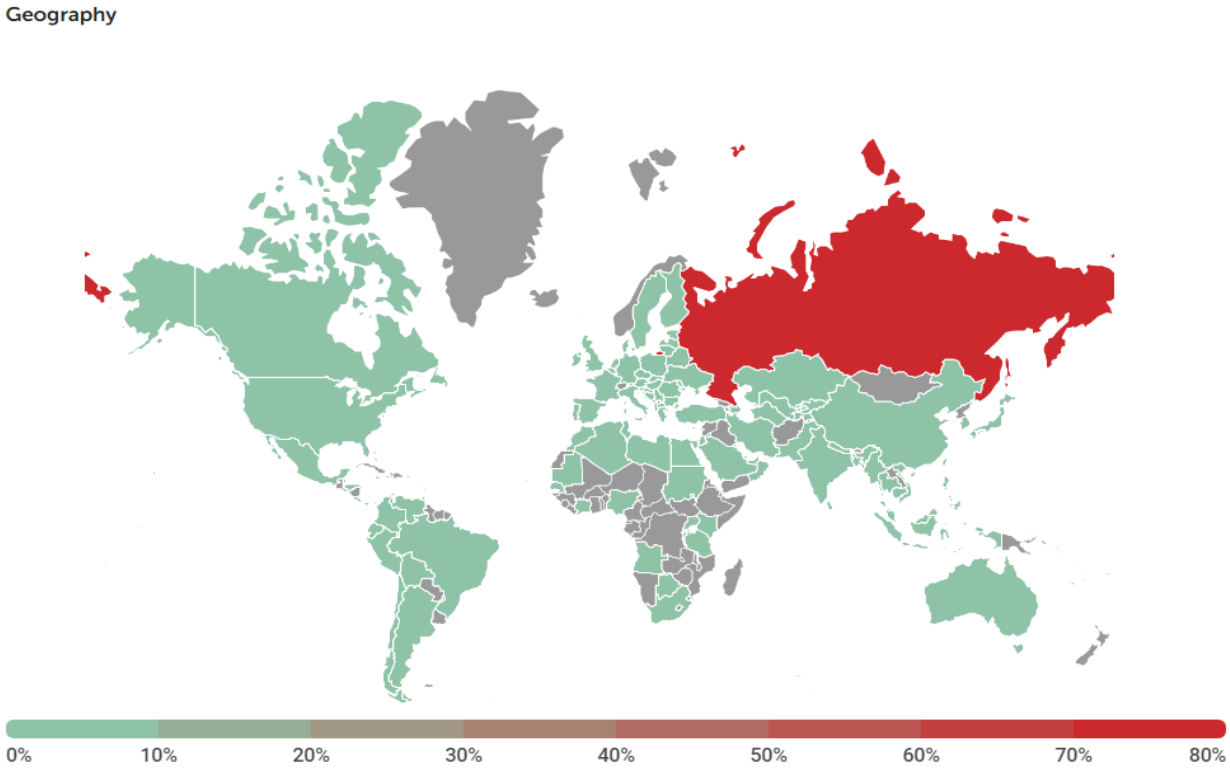

Figure 18. Purga ransomware infected areas geography wise. Retrieved from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

TOP 10 countries

	Countries	%*
1	Russian Federation	85.59
2	Belarus	1.37
3	Turkey	0.85
4	India	0.80
5	Kazakhstan	0.74
6	Germany	0.62
7	Ukraine	0.54
8	China	0.46
9	Algeria	0.40
10	United Arab Emirates	0.40

**Percentage of users attacked in each country by Purga, relative to all users attacked worldwide by this malware*

Figure 19. Percentage of users attacked by Purga ransomware in each country. Retrieved from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

Stop

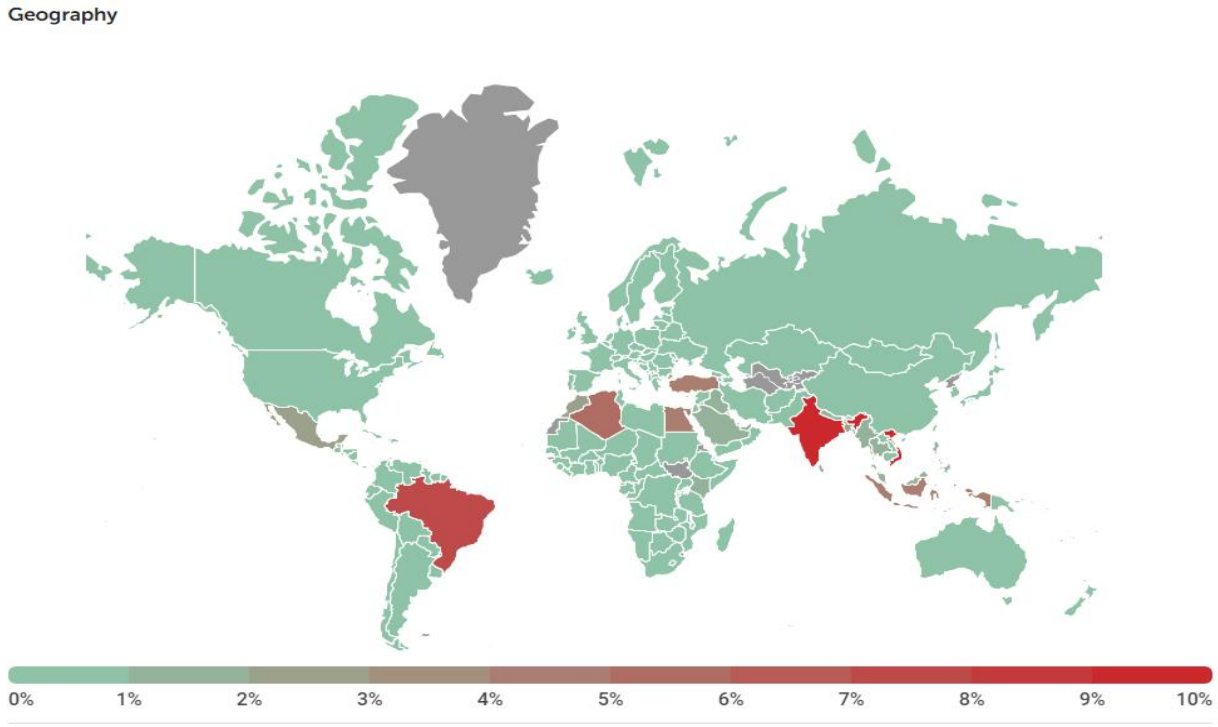

Figure 20. Stop ransomware infected areas geography wise. Retrieved from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

TOP 10 countries

	Countries	%*
1	Vietnam	10.28
2	India	10.10
3	Brazil	7.90
4	Algeria	5.31
5	Egypt	4.89
6	Indonesia	4.59
7	Turkey	4.30
8	Morocco	2.42
9	Bangladesh	2.25
10	Mexico	2.09

**Percentage of unique users attacked in each country by Stop, relative to all users attacked worldwide by this malware*

Figure 21. Percentage of users attacked by Stop ransomware in each country. Retrieved from https://securelist.com/story-of-the-year-2019-cities-under-ransomware-siege/95456/

Conclusion

Ransomware attacks have become a global incidence. The primary aim of ransomware attacks is to make monetary gains through illicit means. Although the attack started through emails, it has continued to evolve and expand through spamming and phishing. Ransomware encrypts the files of its target and displays notifications thereby requesting payment before the data can be unlocked. The demand for the ransom is usually in the form of bitcoins or any other virtual currency as it is difficult to track. Due to the profitability of the illegal act, the variants of ransomware have continued to increase. However, there is a burgeoning effort to control the spread of these ransomware attacks. A good understanding of the behavior of ransomware will help individuals and enterprises to clear up their vulnerabilities to this kind of attack. With the recent spread of ransomware attacks on Windows, Linux, and Mac operating systems, the analysis of ransomware on these platforms is needful. To avoid data theft and illegal extortion of ransomware, individuals and organization need a robust network security platform. This topic is an emerging field of study in academic research. Therefore, to stop the growing trend of ransomware attacks more research effort is needed.

References

Kharraz, A., Robertson, W., & Kirda, E. (2018). Protecting against Ransomware: A New Line of Research or Restating Classic Ideas? IEEE Security and Privacy, 16(3), 103–107. https://doi.org/10.1109/MSP.2018.2701165

Lawler, E. E. (2000). Research Directions. Human Resource Management Review, 10(3), 307–311. https://doi.org/10.1016/S1053-4822(00)00031-0

Zetter, K. (2016, May 13). 4 ways to protect against the very real threat of Ransomware. Retrieved from Security, http://www.wired.com/2016/05/4-ways-protect-ransomware-youre-targe

Korolov, M. (2016, June 1). 93% of phishing emails are now ransomware. Retrieved from http://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-nowransomware.html

Bradley, S. (2015, April 23). How to defend yourself from ransomware. Retrieved from Windows Secrets, http://windowssecrets.com/top-story/how-to-defend-yourself-from-ransomware/

Rosenberg, J. M. (2015, April 8). A Q&A about the malicious software known as ransomware. Retrieved April 8, 2015, from http://www.salon.com/2015/04/08/a_qa_about_the_malicious_software_known_as_ransomware/

Dobran, B. (2020, January 10). 15 Critical Security Tactics For Preventing and Detecting Ransomware. Retrieved from https://phoenixnap.com/blog/preventing-detecting-ransomware-attacks

VinRansomware. (2020). 30 Best Practices for Ransomware Prevention and Incident Response Checklist. Retrieved from http://www.vinransomware.com/best-practices-for-ransomware-prevention

Malecki, F. (2019, June 28). Best practices for preventing and recovering from a ransomware attack. Retrieved from https://www.itproportal.com/features/best-practices-for-preventing-and-recovering-from-a-ransomware-attack/

Stellar Data Recovery. (2020, April 17). [Solutions]: How to Recover Data Deleted or Encrypted by Ransomware? Retrieved from https://www.stellarinfo.co.in/blog/ransomware-virus-removal/

The British Computer Society. (2020). Ransomware recovery. Retrieved from https://www.bcs.org/content-hub/ransomware-recovery/

Fruhlinger, J. (2020, February 20). Recent ransomware attacks define the malware's new age. Retrieved from https://www.csoonline.com/article/3212260/recent-ransomware-attacks-define-the-malwares-new-age.html

Comparitech Limited. (2020). Ransomware Statistics 2018-2020: 50 Ransomware Stats & Facts. Retrieved from https://www.comparitech.com/antivirus/ransomware-statistics/

Eric, C. (2020, April 22). Ransomware Facts, Trends & Statistics for 2020. Retrieved from https://www.safetydetectives.com/blog/ransomware-statistics/

Stake, R. (1995). *The art of case study research*. Thousand Oaks: Sage Publications.

Patton. M. Q. (2002). Qualitative research and evaluation methods (3rd ed.). Thousand Oaks, CA: Sage Publications.