Ransomware Report

Team 1: Jrew Simpson, Anthony Striepe, Jackson Hallahan, TJ Quinn

University of Louisville

CIS 481: Introduction to Information Security

Dr. Andrew Wright

8/6/2024

**Contents**

Title Page………………………………………………………………………………. 1

Table of Contents……………………………………………………………………... 2

Executive Summary……………………………………………………………………3

Introduction (Why is Ransomware an Important Issue?)…………………………..4

Motives Behind Past Ransomware Attacks………………………………………….5

Different Types of Ransomware............................................................................6

Analysis of Ransomware Deployment……………………………………………… 8

Countermeasures against Ransomware Deployments......................................10

Proven Solutions to Live Ransomware attacks..................................................14

Future Evolution of Ransomware & Possible Protections Against Them...........15

Executive Summary

Ransomware is a form of malware that involves an execution of malicious code that results in a user’s files being encrypted and/or the user being locked out of their computer. In the grand scheme of things and the general timeline of the internet, ransomware is a relatively new issue and is growing at an alarming rate. Many sectors including finance, healthcare, transportation, oil, and natural gas have been affected by ransomware.

Malicious actors have deployed ransomware against targets for many reasons, the most popular reason being financial gain. Other reasons these actors have deployed ransomware includes a sense of power, political beliefs, and ideological beliefs. There have been a large variety of malicious actors who have deployed ransomware, these actors have been individuals motivated by financial gain and have even been organizations backed by governments. When these malicious actors gain access into a target’s system, they run the malicious code usually in the form of an executable (.exe) file to encrypt a user’s files or lock a user out of their machine. Afterwards, the ransomware will demand a payment from the user to regain access to their data and/or system.

Thankfully, there are solutions that exist to resolve some ransomware deployments. There are downloadable decryptions, some of which are created by popular antivirus companies such as Bitdefender. You may also run frequent data backups whether that be to an external drive you own, a server you run, or even data backups to the cloud. But as of today, there is still ransomware that exists which does not have an easy solution to a live attack when data backups aren’t available.

In the future ransomware will unfortunately become a larger and large issue because of its strengths. Ransomware is one of the strongest forms of malware when deployed to unsuspected users, users must act quick against ransomware otherwise other machines on a network may get infected and files will be deleted the longer ransomware runs for without getting the ransom paid. With the development of Ai, malicious actors could even use machine learning to further automate deployments

# Introduction: Why is Ransomware an Important Issue?

Ever since 2013 when ransomware first became popular, ransomware has targeted both normal pc users and businesses alike. In 2023, reported ransomware payments hit a record $1.1 billion (KnowBe4, 2023) with the median ransomware payout being $10 million in 2022 (O’Donnell-Welch, 2024). Since ransomware has only been popular for a little over a decade, most normal pc users aren’t very informed on the issue. This combined with ransomware’s nature is a recipe for disaster. Ransomware encrypts a user’s files and/or locks them out of their system and demands a ransom payment to regain access, if the payment is not received in a timely manner as determined by the malicious actor. Then files will start being deleted, this will obviously cause users and businesses alike to start to panic they were not prepared for the attack.  
   
 In 2022, a report by Statista stated that roughly 68% of reported cyberattacks involved ransomware while 155 million ransomware attacks were reported in quarter 4 of year 2022 (Petrosyan, 2024). As Americans we need to be more aware of these attacks since we were ranked first with the number of targeted attacks followed by second and third place, Singapore and Austria (Petrosyan, 2024). Between 2018 and 2023, US government organizations experienced roughly 423 different ransomware attacks which Impacted over 250 million people and resulted in around $860 million in damages (Bischoff, 2024). That is around $172 million per year in damages just to US government organizations alone. Unfortunately, it was reported that $6.8 million was paid out to ransomware deployers which will only further incentivize them and others to continue conducting attacks due to the large payday for their attacks (Bischoff, 2024).   
  
 Many users may not be worried about ransomware statistics that are related to businesses, but the reality is that these affect both businesses and users. In early 2024, UnitedHealth was hit with a ransomware attack that resulted in hundreds of millions of dollars lost by UnitedHealth in damages, but this is because the ransomware attack was not your typical attack. The attackers deployed ransomware that encrypted important files for UnitedHealth’s operations, but the attackers also collected data from UnitedHealth which includes patient records. These records of course are tied to typical consumers who are not working for UnitedHealth but unfortunately get affected by these ransomware attacks. The hackers who carried out the attack are known as AlphV or BlackCat and demanded a $22 million ransom for the encrypted data which is stated to have been “likely paid” by UnitedHealth (Greig, 2024). When law enforcement managed to disrupt BlackCat’s operations and steal back the $22 million ransom payment the gang threatened to leak a reported 4+ terabytes of data which was also connected to other organizations such as CVS & Medicare along with personal records of thousands of patients (Greig, 2024).

## Motives Behind Past Ransomware Attacks

The BlackCat gang’s motivation during the UnitedHealth attacks was a mix of financial gain and a gain in popularity and power. They of course demanded a $22 million ransom which was again stated as “likely paid out”, the success of this attack and their gain in popularity will encourage themselves and other malicious individuals and gangs to carry out future attacks. After law enforcement reportedly stole their ransom payment their motivation shifted more towards popularity and power which worked in their favor. They were mentioned in reports by major news reporters such as CBS and CNN.

Interestingly, a Stanford University report showed that attempted ransomware attacks were increased during election times for multiple countries. A sizable portion of these attempted attacks were carried out by organizations with ties to Russia. The figures in the report demonstrate that ransomware attacks from Russia based groups increased by around 30% when a Canada, USA, UK, or German election was 1-2 months away (Nershi & Grossman, 2023). Along with this, the Russia and Ukraine war has benefited cybercriminals. There’s evidence that Russia recruited cybercriminals to their cyber warfare teams with the most notable example being them recruiting members from a malicious group known as Conti (Nershi & Grossman, 2023). Conti were known to carry out political attacks before the invasion though, but there’s no concrete theory as of now. The most popular inference is that Conti has many Russian patriots in their ranks which led them to carry out attacks against companies that condemned or withdrew operations in Russia. During Conti’s highest activity period, 2021, they were estimated by researchers to have stolen around $180 million dollars in ransom payouts and the US Department of State even offered a $15 million reward for information to assist with convicting and identifying Conti members (Meegan-Vickers, 2023)  
  
 In 2017, there was a ransomware variant named “RanRan” that was discovered by malware researchers at Palo Alto Networks Unit 42 (Paganini, 2017). This ransomware was known to target organizations in the Middle East, some of which were government organizations. When the ransomware was deployed and executed, instead of the demand being for finances, the ransomware would demand a political statement to be posted by the organization. The political statement that the ransomware would extort victims to share would be an advocacy to incite violence against a political leader from the Middle East. The political statement would also force the victim to announce that they would be hacked by the RanRan ransomware. So, there was a mixed motivation for the threat actors split between spreading political beliefs and gaining popularity.

### Different Types of Ransomware

The most common and popular form of ransomware is file encryptors, with the most notable example of a file encryptor being WannaCry. As can be inferred from the name, file encryptors are an executable file that encrypts and user’s files and demands a ransom payment most frequently in the form of cryptocurrency. The most famous incident in relation to WannaCry is the attack on the NHS in 2017, which resulted in thousands of delays and cancellations of healthcare appointments in the United Kingdom. During this specific attack, the WannaCry application would demand a payment of $300 in Bitcoin from each affected computer. If the payment wasn’t delivered in 7 days, the application would delete all of the user’s encrypted files (Collier, 2017).

Another commonly deployed type of ransomware is locker ransomware. Other names include desktop or screen lockers due to its simple approach, locking the desktop on a victim system and preventing any ways of bypassing the ransom screen. In this case, the malware mimics a lockscreen but differs from file encryptors as there is no data encryption taking place on the victim’s machine. While this form of locker ransomware targets desktops, a more dangerous approach targets mobile devices with the goal of changing user login credentials such as passwords or pins. These attacks have a higher potential to affect a targeted system and its functions after system compromise, and even result in a higher chance of locking a device or causing permanent data loss (Checkpoint, 2023). As attacks and the ransom notes have become more creative, not only will file encryptors just prevent victims from accessing their files, but in the case of lockers they will even go as far as impersonating law enforcement in an attempt to legitimize the threat. This scare tactic, along with a countdown clock for added stress, makes locker ransomware an effective and more commonly used type when attacking different types of machines.

Leakware, is a modified approach to an older type known as Doxware. The name comes from the term “doxing” which is the act of publishing someone’s personal information online. Leakware is a hybrid type of malware that goes a step further than traditional file encryption. Its goal is to leverage the possession of confidential formation of not only an individual, but the clients, customers or the employees of larger organizations that is found on an infected system. With the nature of this attack, common targets include healthcare organizations like hospitals or insurance companies, law firms, court systems and a variety of financial services as they all collect and store substantial amounts of confidential data. These larger enterprises and the potential value for accessing their information makes this malware more dangerous than file encryption because not only is data encrypted, while a decryption key is in the attacker's possession, the data possession is exploited and then used to threaten its disclosure to the public without the ransom payment. As these types of hybrid ransomware attacks have become more commonly deployed, those bad actors trying to make a name for themselves in the hacker communities have followed suit. Groups like Maze have led the way in forming extortion gangs, creating platforms to share stolen data of successful attacks, intelligence and tactics used to educate and encourage other ransomware operators (Abrams, 2020). Just as with the other mentioned types of ransomware, this type targets email compromise through phishing attempts as a way into new systems. For the average mobile and desktop users, the threat of exposing personally identifiable information, photos, and other private data can not only risk embarrassment, but can potentially lead to identity theft if enough information is collected. For corporations, the risks are significant. The biggest threat to information security is personnel, due to a lack of training and awareness of the potential vulnerabilities that can be exploited. Without proper training and testing of phishing attacks inside the office and when accessing servers remotely, email compromise remains an easy way in. Once an attacker has found a way in, other network resources and systems can be targeted adding to the strength of an attack. Once a bad actor has stolen confidential data of customers, or even the intellectual property of an organization, the price of the ransom can significantly increase as will the cooperation of the corporation under attack.

Analysis of Ransomware Deployment

One of the big reasons that cybersecurity experts do not recommend victims to pay ransoms to malicious actors is due to the unreliability of the word from the deployers. Similar to traditional malware, ransomware gets executed and can install additional processes that can harm the user later or when deployed. For example, Jigsaw installs an additional service when deployed and will restart if the computer is turned off and on. A popular example of malware that also does this is “YouAreAnIdiot.exe”, which will automatically start if a user restarts their computer. This process is also known in the information security space as a backdoor. Which is an established process of a malicious actor attacking a system then implementing a process that allows them to re-access a system in a way that’s easier than the way they got in initially. A way to remove backdoors is to perform a system scan with an antivirus tool such as Malwarebytes to detect any traces of malware or ransomware processes after you stop the malicious program. Antivirus scans won’t detect backdoors such as a malicious actor adding or changing forms of authentication for a user. It’s good to stay informed though on new backdoors and exploits since there’s new bugs in systems and software alike every single day.

ZScaler, a company that creates software related to information and network security, recently posted an article on the technical analysis of CryptNet, a form of ransomware. They informed readers that CryptNet is known as a ransomware-as-a-service and is a ransomware group which is known to be founded around April 2023. CryptNet’s ransomware is written in a .NET programming language with notable .NET programming languages being C, C#, and C++. This is standard since C and C++ are known to be the most common programming languages used to write malware and ransomware alike. Besides C and C++, Python and Windows Powershell are both commonly known languages used to write ransomware or assist with deployment because of the automation that the scripts provide. When CryptNet’s ransomware is deployed, they first generate a decryption ID and encrypt the user’s files using two different functions for both tasks. So that the system can still be in running condition, some files are excluded from the decryption such as bootmgr, desktop.ini, and ntuser.dat. To encrypt the files CryptNet uses AES symmetric encryption in CBC mode and the AES key will be encrypted with a 2048-bit RSA key (Vicente & Stone-Gross, 2023).   
  
 After the encryption, a ransom note will appear explaining to the victim what has happened and how to recover their files. The ransom note will instruct the victim to install Tor browser and to enter a .onion link into Tor to decrypt their files. The victim will need to enter their given decryption ID and will need to complete a captcha to confirm they aren’t a bot. The next page will notify the victim that they have 3 days to recover their files and can even upload one file to test the decryption algorithm from the malicious actors. Surprisingly, there’s even a “live chat” option available to the victim to contact the CryptNet organization which is likely used to negotiate ransom payments. Again, paying ransoms is highly not recommended because of the untrustworthiness of cyber criminals and the underlying ethical reasons such as giving them more of an incentive to carry out more attacks. Unfortunately, CryptNet not only extorts the victim stating that files will be deleted but also explains that important files will be uploaded to the internet if the ransom is not paid by the end of the three days.

Countermeasures against Ransomware Deployments

With the ever-changing environment of the digital age, more and more deployment methods are found or created over time. However, there are several common deployment methods that people can be aware of in order to better secure their machines and information. Remote Desktop Protocol is a large offender of allowing ransomware to make it onto machines. Those without a properly secured Remote Desktop Protocol can create an easy way for bad actors looking to take control of your machine and install ransomware onto it. Without already having access to a victim’s network, an attacker would have to use network port 3389 to use RDP to connect to a victim’s machine. Thankfully, this port is normally closed, and you would have to go into your router’s settings to open this network port.  
  
 Another very common deployment method is the use of phishing via email, social media, or suspicious websites. These phishing attempts usually include directions to a link of some sort that, when clicked on, installs ransomware and gains control. The emailers usually imitate household name companies such as Amazon, Chase Bank, Coinbase, and eBay for example. Phishing emails will commonly have a document attached that if opened will deploy a malware payload such as ransomware. More specifically a common spoofing tactic will have the attacker send an executable that looks like a .pdf file. The icon will be a pdf icon, and the visible name will have a .pdf extension but if you look in the properties of the file, the extension will be a .exe or .msi extension. In real time, this process would have a cybercriminal imitate Chase Bank and send blanket email out to thousands of possible victims, in the email the cybercriminal will tell the possible victim that they have received a large deposit or a withdrawal and will instruct the victim to click the attached “receipt”. When the victim clicks the fake receipt file that is an executable, their computer will be infected with ransomware.  
  
 To combat phishing, you of course want to use extra caution when receiving emails, especially from companies with which you usually don’t interact. If you get an email from “Amazon” that claims you have ordered an expensive item that you know you haven’t there are ways to confirm if this is true without opening the email. The first thing you can do is of course log into your Amazon account by searching Amazon’s website on your own browser instead of using any links given in the email. Then check your past orders and if there is a false order, then you can contact Amazon on their official support page through their website instead of any contact information listed on the email. Secondly, you should verify the email and make sure it’s the official Amazon domain. Most phishers do not have the resources to spoof an email address to have it appear as Amazon’s official domain without a misspell in the domain, or the use of a special character such as À instead of “A” in the Amazon domain. Lastly, never respond to phishing emails because all that does is confirm to the attacker that your email is active. The attackers will then use other emails to try to scam you and/or deploy malware.  
  
 This can also be the case when attempting to pirate a product or information, as places that offer free access to things that you do not own are less than ethical in nature. These pages will very commonly have fake download buttons that when clicked can install malicious files such as ransomware. Also, even clicking the “correct” download button can result in the user installing ransomware on the machine. When installing pirated software whether that be games, music, videos, or utility software such as Adobe Premiere Pro, you are putting your faith in an unknown internet user to upload the correct file without any changes to it. Downloading pirated software is also illegal so the action should not be done anyways, sharing pirated software can lead to 5 years in prison and $250,000 in fines. The owner of the material may also file a lawsuit(s) against you for sharing pirated software. As stated earlier, it’s quite simple for attackers to spoof files by hiding the extension and changing the file icon(s) in the folder(s). This and phishing methods are both social engineering examples which is one of the most common deployment methods and can take place both online and in person. Social Engineering can result in access to a machine through tricks, trust, coercion, or other methods.

The habits and practices are the easiest to understand and implement at any level of organizational or technological understanding. These habits include things such as understanding how to spot phishing attempts, knowing not to visit suspicious links, and not to download or run unknown files. Additionally, being in the habit of creating backups for critical information keeps it from being compromised. These very simple tasks significantly help protect machines from ransomware and other malicious attacks. Another great way to counter ransomware deployment is by configuring a machine’s settings to be more secure. Remote desktop protocol is a critical component of this. The information that allows the protocol to be used on a machine should never be shared anywhere online that is unsecure, and if it doesn’t need to be used, the protocol should be disabled within the system settings. One more countermeasure is using programs to help act as a second line of defense to the best practices. Defense programs offer protection for several stages of a ransomware attack. If real time protection is in place, it can prevent the initial installation of the ransomware in the first place. Not all of these programs have free real time protection but will allow for users to run a scan on their system, and quarantine possibly dangerous items or applications. Many other methods can be used to countermeasure ransomware attacks, but these are some of the most important and simplest to implement to increase a machine’s safety.

It is important for users to be aware of these common deployment methods, not just for ransomware, but for anything possibly malicious. Being knowledgeable of the countermeasures is also extremely important, as a few relatively easy habits, computer settings, and programs can make your machine much safer. However, not all users are fully aware of the countermeasures, and when in an organization, not fully responsible for them. The CISO needs to ensure these countermeasures are known and followed in the form of policies and procedures to ensure safe machine usage. Additionally, the chain of command needs to ensure that machines are compliant with the level of security they desire as well as have the appropriate supporting software installed.   
  
 Another great countermeasure against ransomware is the use of data backups. In our opinion, all technology users should have some form of a data backup process whether that be a cloud solution such as Google (Drive, Photos), Microsoft OneDrive, or Apple iCloud. Or you can use an on prem solution such as the use of an external hard drive, storing on another device, or storing backup data on a server. You could even print out documents or photos physically and store them in a secure physical location if you’d like. You can use one of these, two of these, or a mix of three of these options, it’s up to users to determine which data backup configuration is best for them. The weakness of cloud solutions is the fact that you are trusting a third-party company to handle your data and depending on the size of your data stored in the cloud, it could be expensive to move your data away from the cloud. The weakness of on prem solutions is that you must do your own maintenance and build automated backup processes yourself. Also, if your site is damaged such as from a flood or other natural disaster, you either must work with your insurance company to replace the equipment or you must pay out of pocket to replace the equipment. Either way the data will be lost unless you have additional backups stored in a different location such as the cloud. This is why the mixed configuration is popular and used by many individuals and organizations alike. One form of ransomware that data backups are weak against is leakware since leakware will leak your important files if the ransomware is not paid in a timely manner. The best solution against leakware is the use of real time protection with examples of companies that offer these services being Malwarebytes and Bitdefender. But you will at least still have your data after the attack and will not have to pay the ransom to recover your data.

# Proven Solutions to Live Ransomware Attacks

After ransomware is deployed onto a machine, the first step of the response is to isolate the attack. This means the machine needs to be disconnected from the main network, privileged accounts need to be restricted and afterwards it will be time to investigate what type of ransomware was deployed. There is a website known as ID Ransom that offers users a free service that gives information on what type of ransomware has affected them and if there are any known solutions. ID Ransom offers users the option to either upload a ransom note or a sample encrypted file, afterwards ID Ransom will notify you what type of ransomware you’re dealing with, some key attributes, and whether the ransomware is currently decryptable. Next, the ransomware process needs to be disabled which you could do from the task manager in Windows. The name of the process will be different depending on which ransomware type is running. We will use Jigsaw for our example, when Jigsaw runs it imitates Firefox in the background, so ending the firefox.exe processes will stop the ransomware from running but the files will already have been encrypted.   
  
 If the ransomware is decryptable, you can download the decryption which will be offered by ID Ransom, and you can run the decryption to decrypt your files and recover them. Another website that offers a large variety of decryptions against ransomware is a website named nomoreransom.org. Similarly to ID Ransom, they write a description of the ransomware and how it works then afterwards they offer one or sometimes multiple different decryption options especially if a ransomware has multiple forks such as jigsaw.exe. If the deployed ransomware is not decryptable, then ID Ransom will offer you the option to enter your email address and you will be notified when a decryption becomes available. In the meantime, it’s best to grab an empty external drive to save the encrypted files on until a decryption is released.   
  
 The last solution is the simplest but requires the victim to have followed the countermeasure of using data backups. If you have up to date data backups and have been successfully attacked with ransomware, then your first step is the same as the beginning of this chapter which is to isolate the machine. After isolating the machine, you will wipe the machine and either restore it from an image backup or do a fresh image. If you do a fresh image after setup, you can reconnect the machine to the network then restore your needed data from a backup whether that be from a cloud service or self-managed on prem backup.

# Future Evolution of Ransomware & Possible Protections against Them

There are multiple ways that ransomware will evolve in the future, one way is ransomware as a service (RaaS). RaaS allows people who wouldn’t normally know how to use ransomware the ability to purchase it. These platforms that offer this have a user-friendly interface, user manuals, and 24-hour support which could cause a lot of companies to lose valuable information. Another way ransomware will evolve deals is with double extortion methods. By doing this, those sending these attacks are not only making them pay to get back in control of the system but also threatening to release negative information to the company or public (Kahriman, 2024).

Targeted ransomware attacks and supply chain attacks are two other ways that ransomware will evolve in the future. With targeted attacks instead of being generalized it will be more precise to go for high-end targets, such as healthcare providers and financial institutions to max out their extortion efforts. Supply chain attacks are not just affecting one company, they are affecting everyone associated with that supply chain. This means it could affect multiple countries because of how global some supply chains are (Ho, 2024).

There are many protections against ransomware. One protection is having regular employee training. This would help prevent an organization dealing with ransomware attacks by teaching about suspicious links, websites, and unusual activity. Another protection is network segmentation. This means that the networks are divided to restrict access to sensitive information and do not give access privilege to that many people to avoid as much as of a chance of being an issue. AI can be used in ransomware detection and response to prevent attacks. AI can be used to analyze endpoint behavior to find indicators of ransomware infection and can also be used to detect patterns or deviations from the normal network behavior to show if an attack is occurring (Ho, 2024).

**Final Thoughts and Recommended Solution**

Ransomware is a constantly evolving and prevalent tool in today’s cyberspace. With the amount of information constantly flowing into and around the internet, there will always be someone with the intention of taking it and using it in malicious ways. Because of the longevity of this crime and its fluctuation in nature, individuals and organizations will always have to be alert and informed in order to stay as protected as they can from it. No company or individual is exempt from the scope of ransomware, and so our recommendation is to stay informed and diligent to ways that ransomware can infect your system. This goes for both individuals and organizations, with the difference being the extent to which it should be followed. We recommend that individuals pay attention to their devices and network habits by making sure they have the latest updates as well as a protective software such as Malwarebytes installed, while also being diligent of suspicious links or downloads online. For organizations, we recommend that they have a compliance program to ensure the security of their devices as well as having a secure environment for employees. Having a well configured firewall, consistent backups of data, and the same protection we outlined for individuals can help strengthen an organization by a lot. There are many different cybercrimes, but with these steps and pieces of information, hopefully your encounter with ransomware will be slim to none.

References

Abrams, L. (2020, June 3). *Ransomware gangs team up to form extortion cartel*. BleepingComputer; BleepingComputer. <https://www.bleepingcomputer.com/news/security/ransomware-gangs-team-up-to-form-extortion-cartel/>

Bischoff, Paul (2024, January 15). Ransomware attacks on US government organizations have cost over $860m. Comparitech. https://www.comparitech.com/blog/information-security/government-ransomware-attacks/#:~:text=Between%202018%20and%20December%202023,estimated%20%24860.3%20million%20in%20downtime.

Collier, R. (2017). NHS ransomware attack spreads worldwide. Canadian Medical Association Journal, 189(22), E786–E787. <https://doi.org/10.1503/cmaj.1095434>

Ho, A. (2024, May 21). *Emerging trends in ransomware: What to expect in 2024?* Retrieved from Acronis: https://www.acronis.com/en-us/blog/posts/ransomware-trends-2024/

Kahriman, J. (2024, May 30). *The Future of Ransomware.* Retrieved from HornetSecurity: https://www.hornetsecurity.com/us/security-awareness/the-future-of-ransomware/

Nershi, K., Grossman, S., (2023, July 14) *Accessing the Political Motivations Behind Ransomware Attacks*. Standford University. [New Paper: Assessing Political Motivations Behind Ransomware Attacks | FSI (stanford.edu)](https://fsi.stanford.edu/news/new-paper-assessing-political-motivations-behind-ransomware-attacks)

O’Donnell-Welch, Lindsay (2024, February 7) *Ransomware Payments Hit $1.1B Record In 2023.* Duo. <https://duo.com/decipher/ransomware-payments-hit-usd1-1b-record-in-2023>

Paganini, Pierluigi (2017, March 21) *RanRan and PetrWrap Threats: Political and Criminal Abuses in the Ransomware Landscape.* Infosec. <https://www.infosecinstitute.com/resources/malware-analysis/ranran-petrwrap-threats-political-criminal-abuses-ransomware-landscape/>

Petrosyan, Ani (2024, Janurary 10). *Ransomware – Statistics & Facts*. Statista. <https://www.statista.com/topics/4136/ransomware/#topicOverview>

Vicente, S., & Stone-Gross, B. (2023, May 16). CryptNet Ransomware | ThreatLabz. Zscaler.com; Zscaler. https://www.zscaler.com/blogs/security-research/technical-analysis-cryptnet-ransomware

‌ *What is Locker Ransomware*. (2023). Check Point Software. <https://www.checkpoint.com/cyber-hub/ransomware/what-is-locker-ransomware/>

*What is ransomware?.* (2023)KnowBe4. <https://www.knowbe4.com/ransomware>​

Meegan-Vickers, Jack (2023, June 27). *The rise and fall of the Conti ransomware group.*  Global Initiative. https://globalinitiative.net/analysis/conti-ransomware-group-cybercrime/

‌