Sri Lanka Institute of Information Technology

Ransomware is rising to a crisis level

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT19187488	Y.K.Lumindu Dilumka

Date of submission

2020/04/30

Abstract:

Ransomware has rapidly become one among the most dangerous threats on the web, with new variations being deployed periodically. It is a growing threat to the information of companies and as a result of the large amounts of money to be made, new variants appear frequently. Ransomware outbreak became a worldwide prevalence, with the main objective of making monetary gains through outlawed means.It may end up in loss of sensitive information regular operations' disruption and harm to an organization's reputation. It encrypts target files and displays notifications requesting for a payment before the information is also unlocked. This malware is liable for several dollars of losses annually. The ransom demands typically within the sort of virtual currency, Bitcoin as it's hard to trace. This report gives an overview of the history of ransomware, types of ransomware, how widespread it is.Best practices of preventive measures & Future ransomware challenges.

Table of Content

1.Introduction…… 03

2. Types of Ransomware……..05

3. Evolution of Ransomware……..09

4. How widespread is the problem of ransomware……..15

5. How much will a Ransomware attack cost you…….19

6. Preventing strategies of Ransomware……..20

7. Future hold for ransomware……22

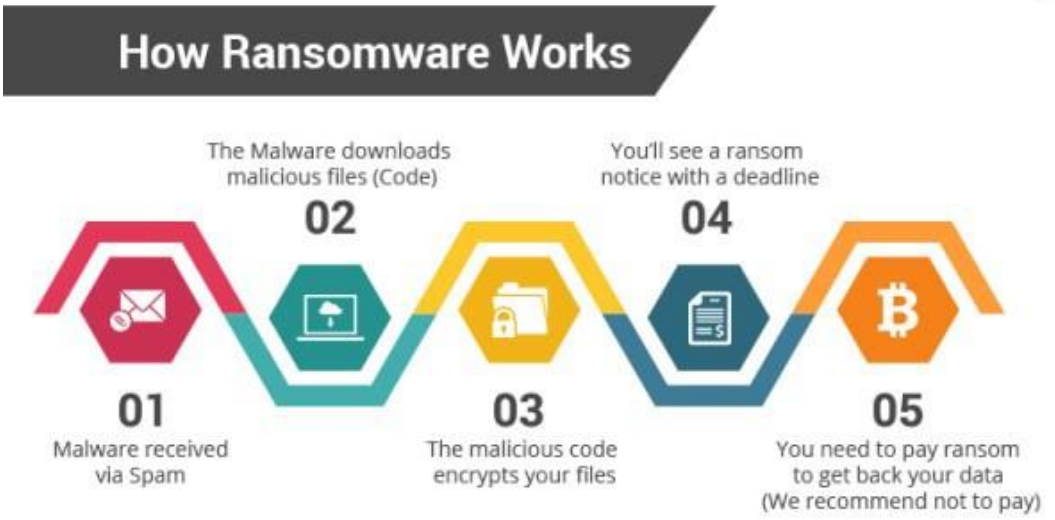
8.Conclusion……..27

9.References……28

1.Introduction

If you have gotten a mail notifying you of a receipt, you're working away on your Laptop and it forces you to access the receipt with the connection provided. You access and open the file, without worrying too much. For a while, you'll notice you can't access your files which are generated several copies of a file named "DECRYPT YOUR DATA.txt".

Your machine's vital records, and probably the network on which you are connected, were encrypted. In one of the fastest-growing types of cyber threats, they were effectively held hostage: ransomware threats.



Ransomware, as the name implies, is a ransomware produced to make data of a victim unavailable or to block access to a Computer before a ransom is usually paid in hard to track virtual currency. The scene mentioned above is a typical incident involving ransomware, a pit every machine consumer falls into. Ransomware is becoming increasingly sophisticated: the current models will bind without the least bit linking to the network, rendering it nearly untraceable to their source. The lucrative and fast pay-off, coupled with the transaction's secrecy and relative anonymity, has rendered this form of ransomware assault highly attractive to attackers.

Cyber attackers make all malware millions of dollars. As forecasts and projections by analysts, the danger of ransomware will begin to increase over the coming years.

Recently, other groups have been struck hard by ransomware along with a police hospital in Massachusetts, a church in Oregon, colleges in South Carolina and a variety of other medical centers in California and Kentucky, one in all that ended up charging 40 bitcoins (about $17,000) to the attackers.

Threats on people seldom attract news, but the Federal Bureau of Investigation (FBI) received around 2,500 accounts of ransomware threats in 2015 alone, amounting to about $24 million in harm to victims.

Advanced cryptography, tor network and Bitcoin technology are enabling the ransomware to grow and develop, allowing hackers to stage more capable assault while covering their trace.

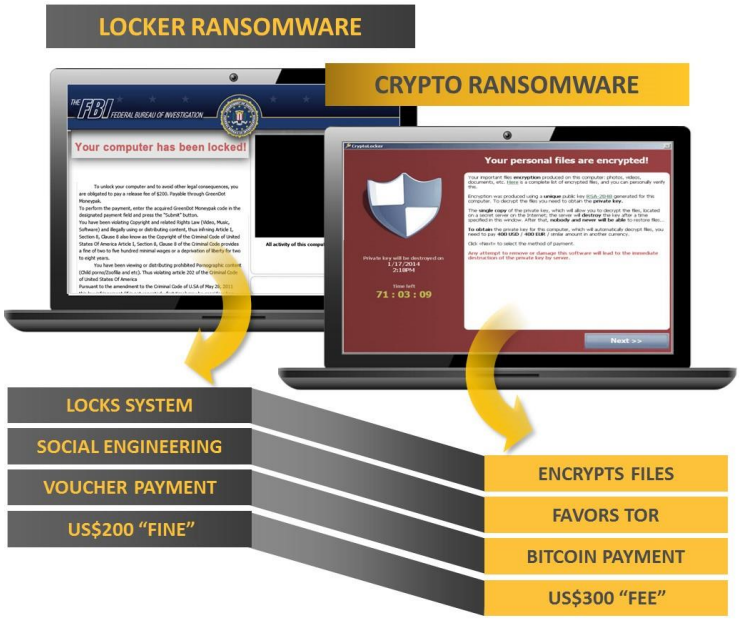
In certain instances, victims are faced with little alternative but to compensate the perpetrators, and even the FBI routinely urges victims to pay the ransom as the only solution is that. Old techniques and methods are not enough now to pander to the rapidly changing landscape of ransomware viruses and new ways of identifying and countering its terrible consequences are required.

2.Types of Ransomware

There are two main categories of ransomware today:

- Locker ransomware (computer locker):prevent access to the computer.
- Crypto ransomware (data locker): Denies access to files or data.

  Crypto ransomware does not need to use encryption to avoid users from entering their files, but the overwhelming majority of it does.



(locker ransomware and crypto ransomware)

Both sorts of ransomware are towards firmly at our digital style. They are built to refuse us approach to everything we want or need and payment of a ransom they promise to return what is rightfully ours. Although they have similar goals, the strategies followed by each sort of ransom are very dissimilar.

4.1.Locker ransomware (Computer locker)

Locker ransomware is perform to prevent entering to computer files. This Normally comes in the consists of blocking the machine or platform programme and after requesting the consumer to compensate a charge to re-energize entry to the PC. Locker ransomware machines are also have minimal features, like letting the victim to communicate only with the ransomware and paying the bounty. It implies that entry to the mouse may well be deactivated, and the keyboard features might be restricted to numeric keys, enabling the user to point the transaction code only by form numbers.

(A number of law enforcement-themed request alerts display in computer locker)

Computer locker is usually construct solely to block approach to the user UI, left the fundamental computer and data fairly intact. Which assumes the malicious code might theoretically be delete in order to rebuild a device to something similar to its previous form. This helps computer locker fewer beneficial in collecting bounty payments than it is more harmful data locker. Tech-savvy causalities are also recover entry which use numerous methods and tactics delivered by safety manufactures including Symantec.

Because Computer Locker could generally be lifted cleanly, it appears to be the kind of ransomware that went a long a way to use social engineering strategies to trick victims having to allowance. This malware also dresses up as regulatory officials and claims to send users fees for alleged indiscretions or illegal activity online.

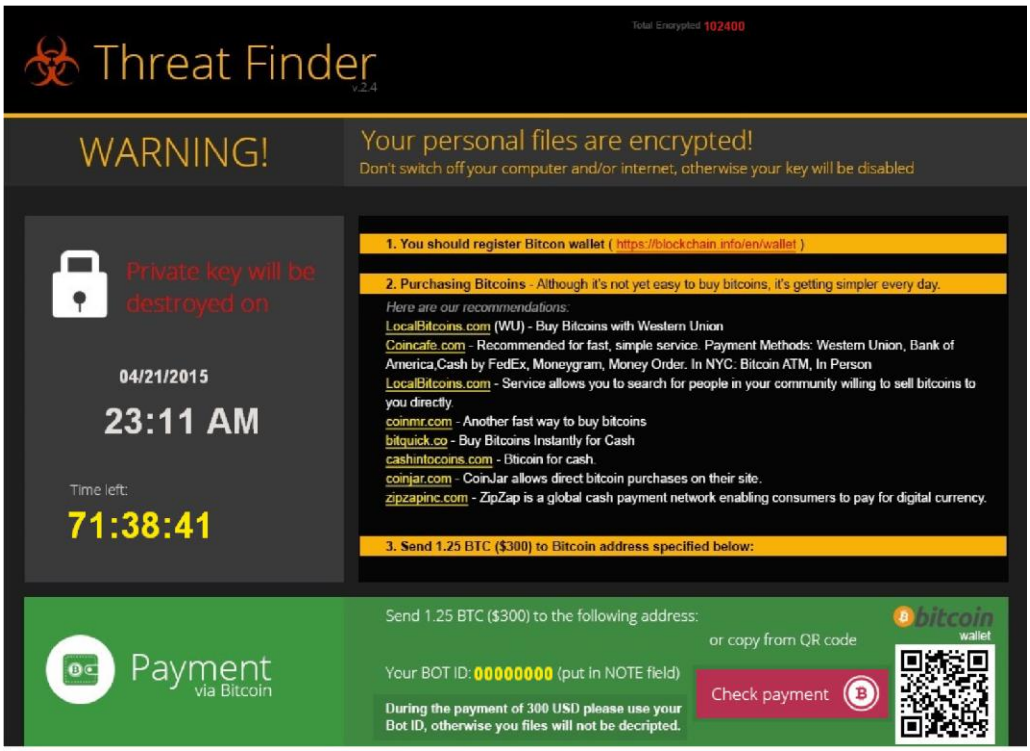
Computer Locker can be notably successful on computers which have restricted features for user interaction. It's a huge weak point given the modern development in portable technologies and even the IOT, where this kind of ransomware might potentially endanger countless connected devices.

4.2.Crypto ransomware (Data locker)

This kind of ransomware is aims to search and encrypt useful files contained on the machine, creating the files and data useless unless the person obtain the decryption key. As community existences are more digital, their computers and phones store more important personal data.

Most end users do not seem to be sensitive to make backups systems to secure toward hard drive faults or device loss or theft, as well as a potential data locker strike. This may be because victims haven't any idea or know the expense of documents before it's destroyed. To make a good backup mechanism involves a certain amount of effort and self-control, so this isn't a pleasant proposal for the common victim.

Data Locker exploits those vulnerabilities for extortion purposes within the traditional user's protection posture. The founder of data locker understand that documents saved on Machines is probably going to be crucial to users. As an instance, the information might consist things stuffs like memories, essential student's data, or financial documents. The ransomware victims is also needing to take their files again, prefer to pay the ransom to revive approach instead of clearly do forever and endure the implications.



(A common data locker ransomware demand screen)

A common vulnerability to crypto-ransomware is secretly checking after installation for cryptographic documents. The purpose would be remain under the target list until it can locate and coded every data which may useful to victim. The harm is already done by the time the user is faced with the message from the malware which tells them that their information is encrypted.

The infected device continues to work normally like most crypto-ransomware infections, because the malicious will not attack sensitive documents or refuse entry to PC functions. It indicates victim can control the machine to conduct an operation array, apart from entering the encrypted data.

3.Evolution of Ransomware

The evolution of ransomware has been strongly affected by the spread of technological, financial, safety and cultural improvements since 1989.

Modern day ransomware could be a huge challenge to worldwide especially for high tech countries. Threats which can modify and develop to their environment will endure ,although people who can't or will not adapt will eventually vanish. The environment of ransomware may be a blueprint for where Darwinian-style evolution functions.

5.1.Ransomware Origins

With the appearance of AIDS Trojan, modern ransomware has grown significantly from 26 years earlier. The AIDS Trojan was sent to the world by mail using a 5 1⁄4 "floppy disks" in 1989. Despite the general public being unready for this new variety of attacks all so many years earlier, the AIDS Trojan was largely futile because of variety of things. After that, several individuals used PC, the World Wide Web was just a concept, so the Web was only used by scientific and technological expatiators. At the time, the availability and strength of encryption methods had also been quite reduced. Along with this, global transactions have become more difficult to process than they are today.

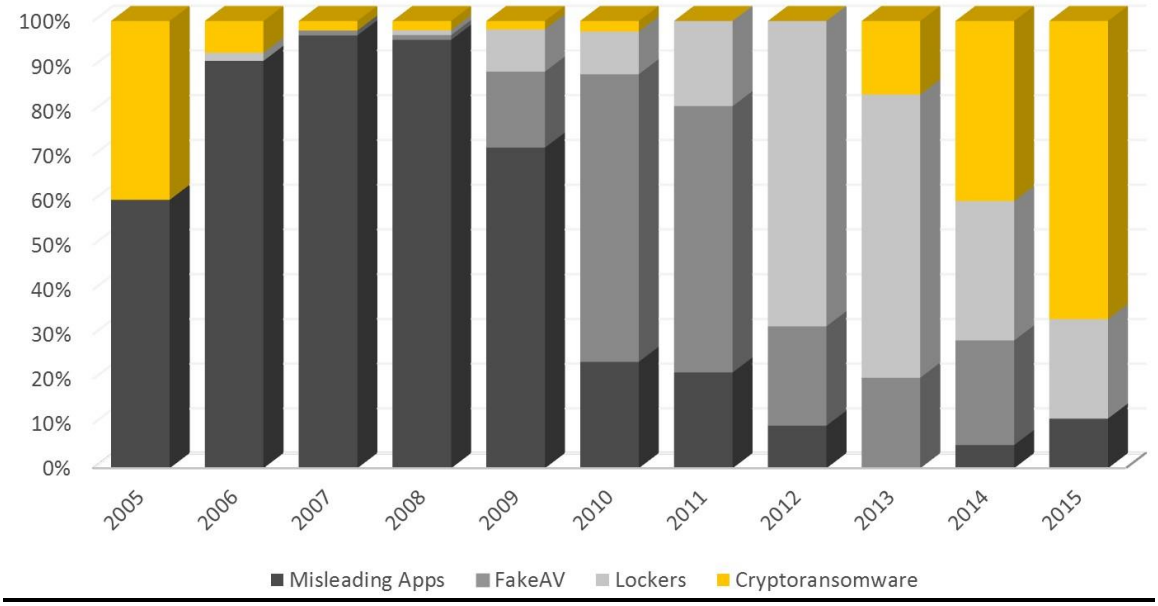
While the ransomware threat was identified with the advent of AIDS Trojan, this form of malware was not commonly used in cybercrime until a few years later. Back in the 1990s and early 1990s, the threat environment was significantly different. That was period where malware was used to realize popularity in jokes and criminal damage; today, malicious software is typically implement for benefit.

The development of malware, especially data locker, has increased in previous periods since many copycat criminal organizations have leaped into the sector to forge achievement on everyone else.

5.2.Vital times in ransomware history

When we look at the recent ransomware past, it's important to think about the image of ransomware attacks in the last 10 years to encourage the development of present ransomware.

The chart below illustrates how every year since 2005 the marketplace for ransom malware has been spread out. Although each threat has never completely vanished, it is easy to see how expectations changed.



(deceptive software, bogus AV, locker rand crypto malicious software discovered from 2005 to 2015)

5.2.1Misleading applications and early ransomware

In 2005 the first misleading application appeared. The application presented as fake malware detection application, like Spy Sherriff, Performance Optimization and RegistryCare.Those scam methods mostly spread to windows computer but also infected to mac computers. Typically they distorted the effect of problems in PC's, including pristine registry access and missing data, and claimed they could fix those problems if the user did so Payed US$ 40 to US$ 100 for a certificate. In fact,there was nothing many of them repairing.

The primary wave of contemporary crypto-ransomware threats emerged even at this early point. The Trojan. Gpcoder family was created in March 2006, originally use poor and easily resolve custom encryption methods.It also used symmetric encryption techniques, which meant that both encryption and decryption used the same key. against basic breakdowns, the developers of malicious coders didn't hand over and proceeded to build new copies of the hazard, make improvements at all stage as they studied from previous mistakes.

In 2006, the data locker theory eventually to boost popularity as the hackers began playing with the theory. A revival of data locker brings to the emergence in March 2006 of attacks such as Trojan. Cryzip. Cryzip duplicate personal documents to single password-protected files so the previous ones were deleted. The passcode has already been inserted in the Trojan code it's own, however, allowing you to get the passcode back.

In 2006, Trojan. Archiveus appeared too. Like Cryzip, Archiveus used encryption-protected archive files but this malware did not enkindle cash payment in an extremely strange twist.Instead, the victim was told to shop medicine online using other online seller links. The causality then had to request an ID to trigger the passcode to get files in the folder. In this path ,hackers received revenue from the sale, that is called a ransom allowance, although this language may not have been accepted by Archiveus manufacturers.

5.2.2.Fake AV

Between 2008 and 2009, the next pivotal moment occurred when computer criminals shifted to scam antivirus apps, a more violent subcgroup of deceptive software. The programs mimiced the looks and features of real security software, and conducted mock scans, pretending to search the device for vast amount of attacks and safety problems. After that users should pay around US$ 50 to fix these issues.They will be asked to buy fraudulent, multi-year support services too. Although several scam AV users,tend to disregard the messages or uninstall the application, leading to a reduce on financial return by the cybercriminals. To fix the inherent shortcomings of fake antivirus scams, hackers finding new paths to improve the call-to-action.

("Nortel Antivirus")

5.2.3.The move to locker ransomware

From 2011 to 2012, hackers have switched from fake antivirus software to a more destructive sort of extortion. This time, the cybercriminals restrict machine access and power, essentially locking the device out of use. Locker ransomware moved up the benchmark as opposed to bogus antivirus and deceptive software in terms of ransom numbers. A regular ransomware threat locker costs approximately US$ 100 to US$ 180 pay via bitcoin.

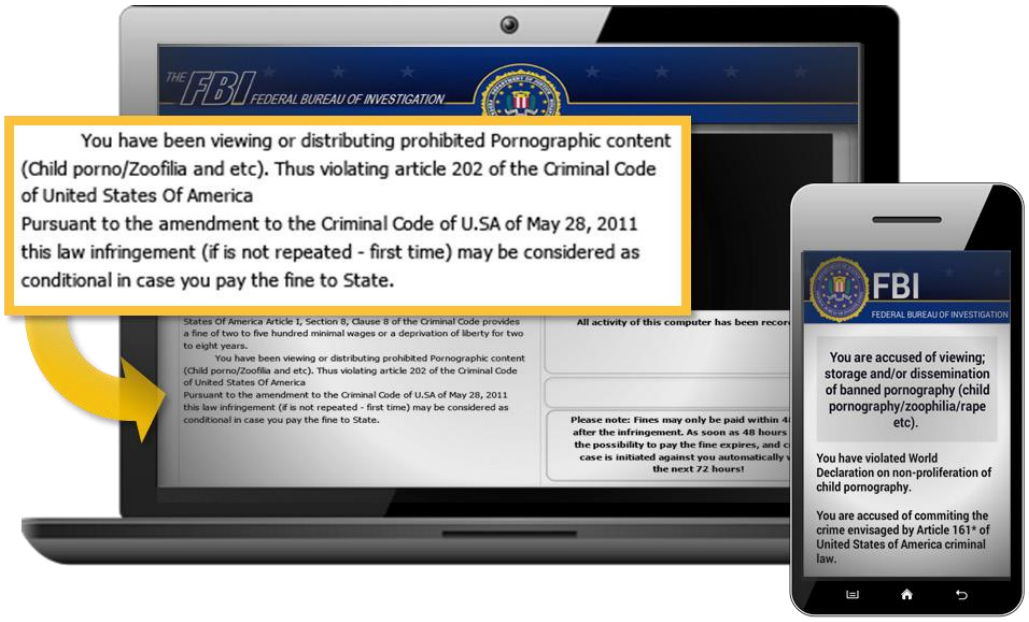
This ransomware arrived a couple of years back it exploded in 2010 to 2011. The main mere computer-locking ransomware reached users in the form of Trojan. Randsom. C.This founder spooofed a Protection Center notification at beginning of 2008 and told the consumer to dial a prime-rate number to reactivate a security program license. The PC was inaccessible at in this situation , and the victim cannot use the machine for the other reasons.

(Fake message from Windows Security Center asking victims to pay the ransom)

When computer locker improved, it goes from presenting pure non-existent issues to being very down to add failures. Finally, it abandoned any notion that merely displaying a transparent appeal for payment to recover access to the PC was a valuable method. It could be because, in time, the perpetrators fooled users into using bogus software to fix machine issues. Today, ransomware can be enabled by attacks such as drive-by installs, without any user input.

Considering this, the locker ransomware developers have been using techniques of social exploitation to persuade victm to pay the ransom. Rather than antivirus applications

and system management devices, the attacks started to surface as compliance alerts. They usually alleged the victim violate by downloading copyrights like songs, videos or applications or by accessing any illicit digital items such as indecent images of minors or animals.



(displaying alleging to illegal content)

Such serious allegations, along with the enforcement authorities' real-looking (but fake) attacks, allowed cyber criminals to develop their demands for ransom from just a few prices for a service to a perfect transaction.

Judging by the amount of ransomware-themed law enforcement that has proliferated since 2012 and 2014, that was obviously a successful method to make people compensate. The tactic may be very persuasive, but they can often contribute to unintended consequences. An person in Virginia, for example,turned him to cops after seeing child porn dealing fees display his computer since he thought that false compliance alert is genuine.

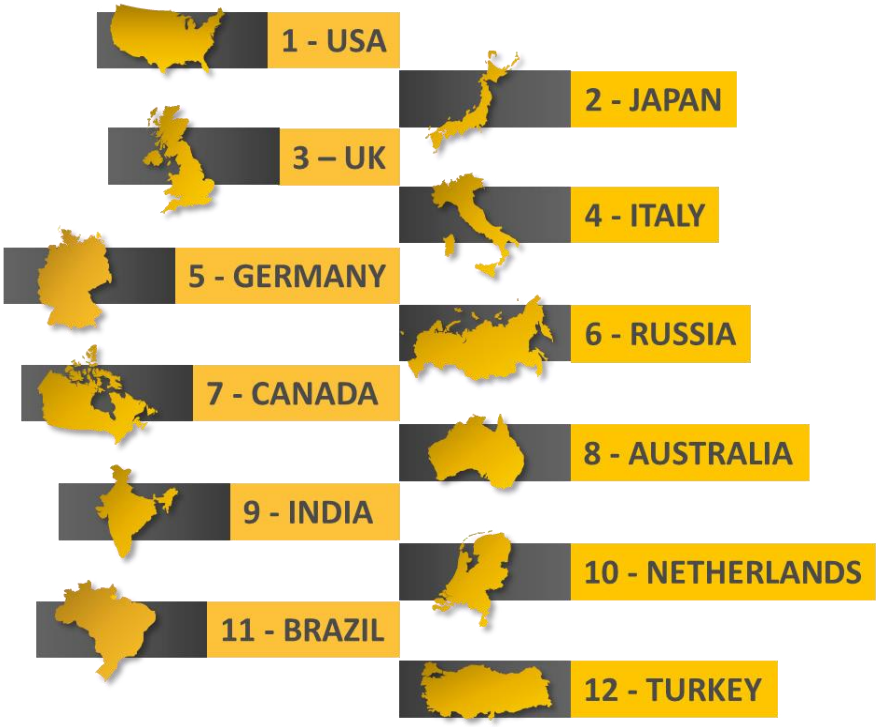
Although computer locker became successful, it's also entirely achievable for victims to get rid of those threats using Symantec and other manufactures security software and restore access to the Device. The rise in the sum of documents on such schemes managed to boost consciousness of scams, which contributed to a reduction in the earnings of the hackers.

5.2.4.The move to crypto ransomware

Weaknesses with all the other hacking methods finally took hackers back to their initial ransomware shape.There is a critical return to crypto ransomware from 2013 to the current day. Crypto ransomware does not seem to use social manipulation, but instead is up front with its motives and demands. The attacks usually show an extort warning that offers data to be returned when large ransoms are paid. Crypto ransomware has extend their ransom to a huge level. A typical vulnerability to crypto ransomware involves compensation of about US$ 350 for one device. Today's challenges to data lockers are more competitive than their predecessors, with stronger operating processes and cryptography.

4.How widespread is the problem of ransomware?

Many common ransomware uses the file encryption intensively as a form of extortion. Basically, they encrypt various data onto the hard drives of a target before calling for a ransom to trigger the decrypted information. Ransomware has been a problem globally, leading individuals and companies to risk an outsize amount of money. While this is a worldwide tragedy, it appears like certain countries are more impacted than others. According to research surveyed by Symantec's telemetry, it has been found that certain countries are more ransomware-driven, it has been discovered that certain types of binary-based ransomware are most frequently aimed at countries such as the USA, the UK, Japan, Canada, Germany, etc.. The advent of ransomware as a cybersecurity problem takes little exceptional, from its latent implementation almost three decades ago to the current, where ransomware is prevalent and has become a serious danger. This telemetry shows that the hackers are attacking richer or more populous countries under ransomware in the expectation of discovering rich pickings in the foreground. As a consequence, 11 of the top 12 countries hit by ransomware are G20 nations of established and emerging economies that make up around 85 percent of the domestic product (GDP) worldwide.



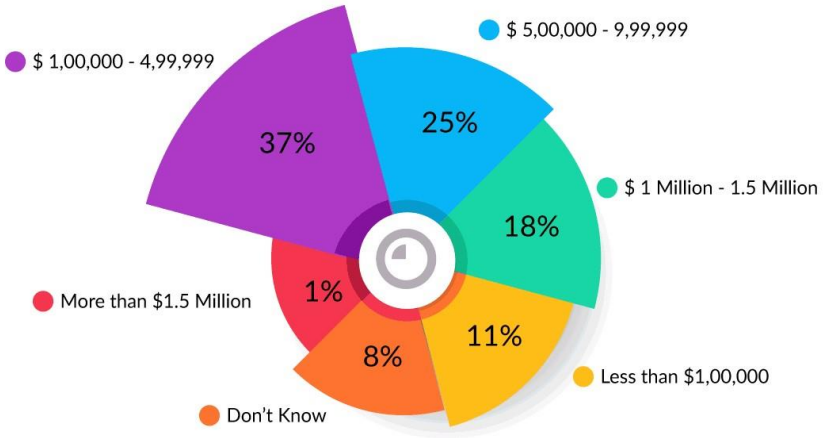
(Top countries impacted by binary-based ransomware)

Ransomware includes a huge break-potential and it's fast growing malware mainly because it's designed to make money from victims. Year 2017 witnessed the highest amount of ransomware family findings although a minor decline occurred in 2018. Ransomware is anticipated to make a return albeit with minor ransom requests. The truth is that financial benefits and large sums of demand retreat customers shell out the money was carried out for Ransomware attacks. Thus, cyber criminals can make it possible to own further transactions by reducing the sum of money to $60-70. Secondly, ransom notes will be detailing step by step process on the path to buy cryptocurrency and how precisely payment should be produced. This could make it simpler for new consumers to claim intervention. Here is the chart on Ransomware statistics on attack consequences like, though not limited to, destruction, dissemination worldwide and reasons of successful assault.

RANSOM PAYMENT STATISTICS

- **46%** didn't pay Ransome. They decrypted on their own or replaced encrypted data with backup.
- **19%** Paid ransom everytime to get back data.
- **13%** Paid ransom amount sometime.
- **15%** Insurer paid the ransom amount.
- **7%** Didn't pay the ransom and lost the data.

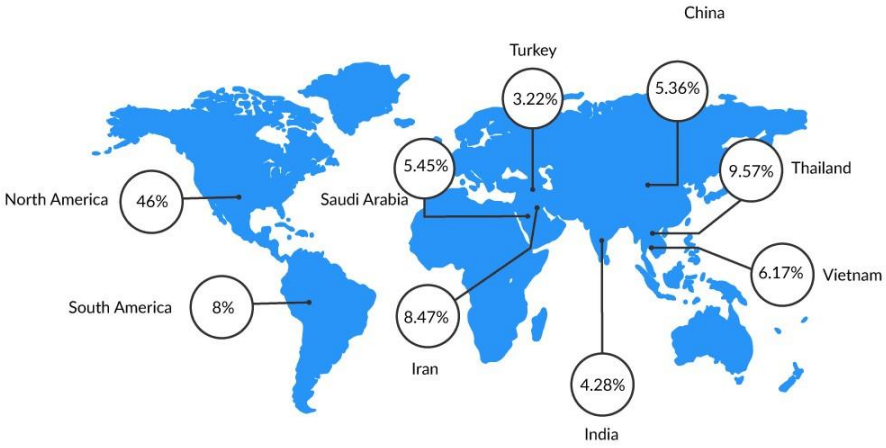
ESTIMATED TOTAL COST OF ATTACK



NUMBER OF NEWLY DISCOVERED RANSOMWARE FAMILIES

WannaCry remains the most commonly encountered type of encryption with a share of 7.71% worldwide followed by Locky (6.7%), Cerber (5.89%), Jaff (2.58%) & Spora (2.2%)

DISTRIBUTION OF RANSOMWARE ATTACK



5.How much will a Ransomware attack cost you.

Definitely, the most serious risk linked to being compromised by ransomware before it is charged is that the demand for payment, which may depend on the type of ransomware or the scale of the enterprise.

Latest analysis showed that 1/4 of companies offering a ransom spent more than £5,000 to recover their encrypted records, whilst another quarter charged hackers between £3,000 and £5,000.

The most expensive ransom charged by small and medium-sized companies was between £500 and £1500 which demonstrates that targeted organizations of this scale often find money easy.

In order to restore access to their encrypted networks and databases, examples of high-profile targets that pay five-figure payments are often given, particularly in situations where offenders are threatened to erase data if not charged.

Ultimately, whatever the scale of the enterprise, time is capital, and so the longer the network is down due to ransomware, the more it costs the company to return.

Extra charges will happen if you re-enter the protected records by charging a ransom. In order to avoid cyberattacks, specially if you are marked as a simple target, be ready to speculate on extra cybersecurity software and pay for additional training for staff.

There is also the possibility of customers losing trust in the company because of weak cybersecurity and moving their practice elsewhere.

6.Preventing strategies of Ransomware

- Educate and inform

  To order to remain healthy and protected digitally, the electronic, financial and retail sectors need to establish and introduce a big effort to inform existing and future clients. The trick is to encourage the communication and awareness of company staff, managers as well as private consumers and small business owners. Education is essential to defending your company against ransomware. It is important that your employees recognize what ransomware is, and indeed the risks it presents. Provide the team with detailed examples of suspect emails and explicit guidance for what to do should they find a potential ransomware lure.

- Make backups plan

  There is no need to offer a ransom to force the data back if the data is safe. Instead, it should, of example, be retrieved from the archives, the archives must be up to date. It is important to preserve backups of sensitive data which are kept separate from the internal computer network of the company and to check the backups periodically to ensure that they operate properly. A survey performed by Osterman's research on individuals who choose not to pay the ransom requested from them found that the existence of recent backups was commonly listed as the explanation the company could opt not to pay the ransom. This could be popular for backups to restore data and systems to a known good state before infection with ransomware.

- Keep upgrading your apps and security package

  Keeping updated your apps and security package will help defend you from malware. That after installing an update, you're making sure you actually have the advantage of the new security updates, making it more impossible for cyber attackers to exploit bugs in your apps.

- Should not access untrusted email attachments

  Another way you can connect ransomware to your device is via an email attachment

  Do not open senders' email attachments which you don't like. Observe who the email originates from to make sure the email address is right. Until launch, take caution to determine if an attachment is genuine. If you are unsure, please contact the person you think has submitted it and test it against.

  Never open attachments that ask you to be able to view macros. When the attachment becomes corrupted, the malicious macro will run opening, granting power of the malware over your device.

7.Future hold for ransomware?

We cannot guess how future ransomware attitude transform .We should analyze past trends and reach out to learn in what could arise in upcoming years. We hope ransomware concept has now progressed to a significant scale.Another potential indication is the advent of RaaS implementations that the concept of crypto ransomware is approaching maturity and market saturation.

For now, we are attentive to a number of developments emerging within the threat environment of ransomware which can form the near-term direction for ransomware.

- Concentrate on operational security

  As software manufacturers and regulators dedicate more resources to attacking operations, hackers behind ransomware may be compelled to build and develop constantly the way they operate. The Federal Bureau of Investigation contributes a bounty worth of US$ 300 millions for sensitive details culminating in the arrested and/or convicted of Evgeniy Mikhailovich Bogachev, the perpetrator behind the disgraceful Cryptolocker.

  Most organizations introduced policies for security including the use of Tor and thus the I2P (Invisible Internet Project).Such technologies offer better anonymity in system interaction and conceal the position of their online sites, that in effect resists any attempts made by law enforcement or protection vendors.

WANTED
BY THE FBI

Conspiracy to Participate in Racketeering Activity; Bank Fraud; Conspiracy to Violate the Computer Fraud and Abuse Act; Conspiracy to Violate the Identity Theft and Assumption Deterrence Act; Aggravated Identity Theft; Conspiracy; Computer Fraud; Wire Fraud; Money Laundering; Conspiracy to Commit Bank Fraud

EVGENIY MIKHAILOVICH BOGACHEV

Aliases: Yevgeniy Bogachev, Evgeniy Mikhaylovich Bogachev, "lucky12345", "slavik", "Pollingsoon"

DESCRIPTION

Date(s) of Birth Used: October 28, 1983
Height: Approximately 5'9"
Weight: Approximately 180 pounds
NCIC: W890989955
Occupation: Bogachev works in the Information Technology field.
Hair: Brown (usually shaves his head)
Eyes: Brown
Sex: Male
Race: White

Remarks: Bogachev was last known to reside in Anapa, Russia. He is known to enjoy boating and may travel to locations along the Black Sea in his boat. He also owns property in Krasnodar, Russia.

(Most wanted poster for creator of Cryptolocker ransomware)

Hackers use blockchain technology such as Cryptocurrency for extortion transfers, more complicated for regulations to monitor concealment or expenditure of ungotten gains.

They use bullet resistant host, a service offered by some unethical domainhosting or internet-hosting companies that gives their consumers great leniency in legal matters. A number of these malicious hackers use name DGA algorithms with numerous forwarding stages to raise misdirection and reduce the chances of knockdown.

- Expansion of localization

As we mentioned in this document earlier, ransomware affects most of the G20 countries, but is especially prevalent in the wealthy Member States. The challenge of pandering to a global audience is to find material for mother tongues and societal conventions to optimize prospects for return. For many years now, Ransomware has been targeted to European countries. Any types of ransomware utilize regionalized terminology and symbols in law enforcement, along with the payment methods accessible local.

(Localized crypto ransomware targeted at Japanese users)

In September 2014, Symantec released a variant of TorLocker that centered specifically on Japanese attackers. Not only was the user Interface language translated into Japanese, but the picture used was also translated into a cartoon character that has cultural meaning for the native population.. It assume that, in the context of this scenario, cyber criminals are conscious of Japan's modern culture and probable to be Japanese citizens or an international community of Japanese associates (maybe affiliates) offering localisation services.

- Ransomware approaches IOT

  One unmistakable shift we see in world culture is that computing is growing with its interactive, linked, and pervasive existence. IoT and wearable computing are technologies that will create growth for the IT industry, and this extension also provides new possibilities for ransomware manufacturers. We now have smart TVs, smart watches, smart clothes, smart refrigerators, smart locks and internet-enabled vehicles, and the list is rising day by day. All of these machines are actually computers that potentially may be exploited and ransomed by cybercriminals. Many forms of systems are also more susceptible to their use or architecture character than others. We saw crypto ransomware as an illustration for specified information-rich devices such as the Network Attached Storage (NAS) devices. Trojan. Synolocker is only one such hazard that Synology NAS goods are based.

Think of a instance in which your IOT room lock forbids access into your room or where your car is drawn over by ransomware and forbids to kickoff, access, acceleration, or curtailment until payment of a bounty is made.

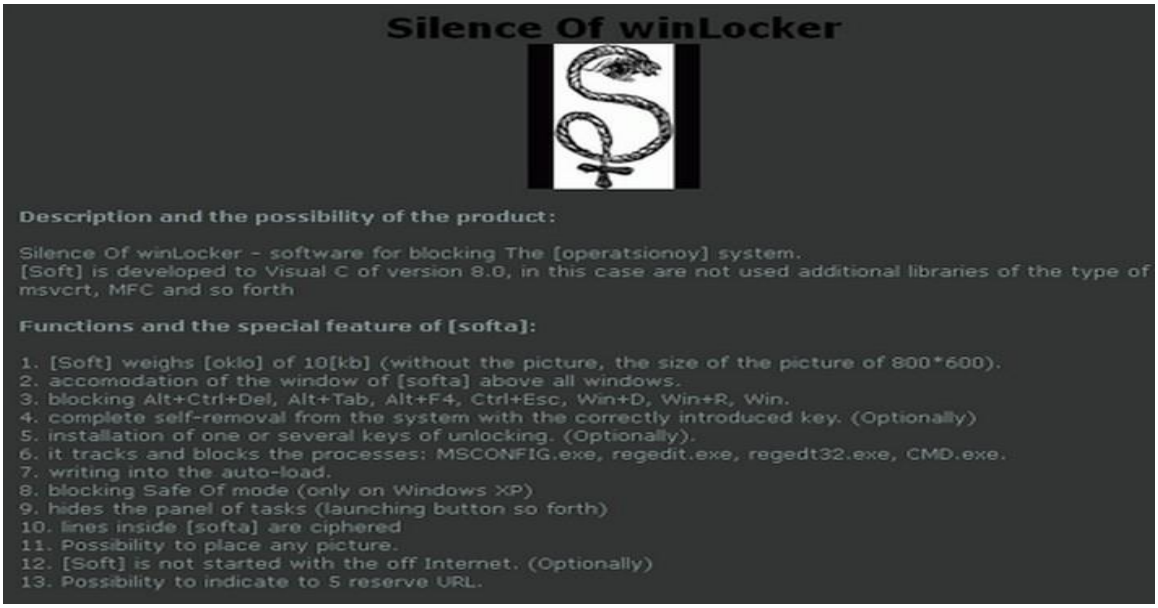
This scenario may not be as plausible as it would seem. We've noticed that experts can take charge of a traveling Jeep Cherokee vehicle remotely and take care of the driving power. The researchers have been able to track almost every aspect of the car's functionality including illumination, air circulation, wipers, entertainment system, steering, transmission and braking. As more cars become exposed to embedded digital technologies, further malicious attacks can inevitably be seen on them unless they are properly designed and enforced.

Previous few years, ransomware outbreak failed to necessarily endanger lives. Within the coming years, this fearsome possibility can only become a slightly closer to the truth.

- Increased franchising and co-operations

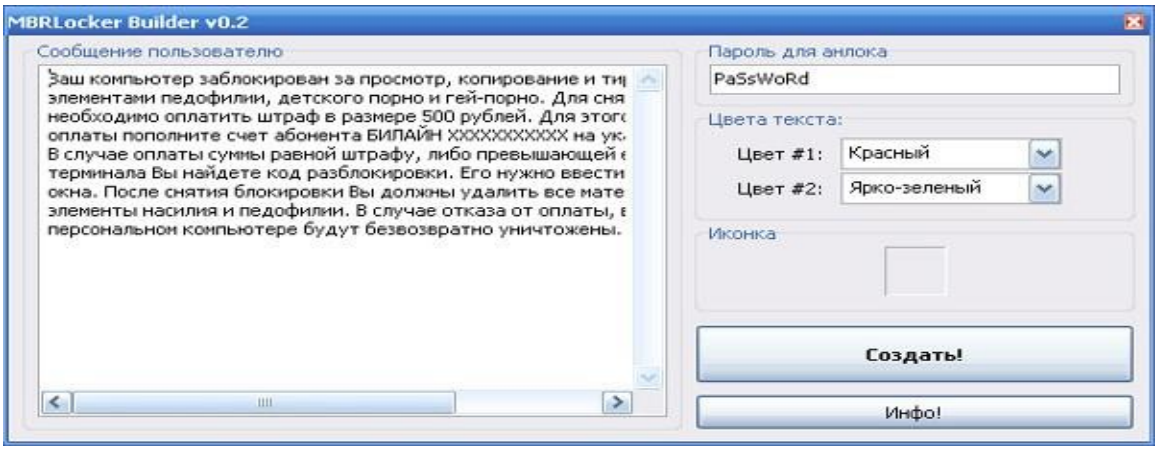
There's a vibrant underground economy for the inexperienced cybercriminal with minimal awareness and expertise selling crimeware toolkits. This toolkits allow the uninitiated to quickly into the world of ransomware extortion. A variety of Ransomware toolkits have appeared over the last few years. While originally sold in underground websites, many of these resources are now available for free.

Tools like WinLocker's Silence (Trojan. Ransomlock. K) have granted entry to whatever they need to execute ransomware threats at a cost of 2500 WMZ for non-technical cybercriminals. That involves the constructor to produce the malicious binary that holds the infected device hostage, and the backend C&C server control panel software that helps cybercriminals to construct and choose any picture they need to help their victims.



(Forum that show the availability of the "Silence Of winLocker" ransomware toolkit for sale)

Other publicly accessible tools, like MBRLocker (Trojan. Bootlock. B), affect the master boot record (MBR) of a compromised computer. This prevents booting up of the operating system before the bounty is payed and entry of the unlock code.



(MBRLocker available for free on dark websites)

8.Conclusion

Throughout this report, I have broadly researched on areas of ransomware in terms of its origin, evolution, malicious effects and prevention practices. Ransomware has become one of the most challenging problems in the Cyber world nowadays. It has become an emerging threat to its home users, companies, healthcare systems, and data security professionals. Ransomware has become one of the main targets of the many cyber-criminals resulting in its rise due to its huge feasible monetary gains. Moreover, studied how they spread and how they being expert at leveraging human psychological terms to emphasize their demands. Hitting the bulk of the nations that compose G20 group has showed how widespread ransomware is, within the globe. Increasing localization of ransomware shows that the matter is both global and native at the identical time. Also looked into how technological trends like IoT can allow cybercriminals to target new dimensions with ransomware.

Regardless of anything, this research spotlights the security is the paramount for all by reducing and minimizing vulnerabilities at its best. Dealing with ransomware is definitely a huge and challengeable task which each individual has to play a role in it. Just considering the conventional benign use cases is not enough anymore for the product designers who are creating and inventing new technological aspects. If there are any vulnerabilities, which enables product to be subverted or denied functionality to its user, then its pave the way for cyber criminals to find such products very easily. The challenge to designers of products is to enhance security and take malicious usage and scenarios into consideration. Potential victims of ransomware must thoroughly aware and practice basic security procedures to shield their data, such as avoiding clicking malicious links or attachments and patching exploitable software vulnerabilities and study the various possible threats of ransomware and take necessary steps to minimize the appropriate risk from these ransomware attacks.

9.References

[1].U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal and A. Kumar, "Ransomware Threat and its Impact on SCADA," *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, London, United Kingdom, 2019, pp. 205-212. .[Online].Available:https://ieeexplore.ieee.org/document/8688327/references#references

[2].D. Garg, A. Thakral, T. Nalwa and T. Choudhury, "A Past Examination and Future Expectation: Ransomware," *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Paris, 2018, pp. 243-247.[Online].Available:https://ieeexplore.ieee.org/document/8441743/references#references

[3].Asibi O. Imaji,"Ransomware Attacks: Critical Analysis, Threats, and Prevention methods",Fort Hays State Universit,March 5, 2019. [Online]. Available: https://www.researchgate.net/publication/332551447_Ransomware_Attacks_Critical_Analysis_Threats_and_Prevention_methods#pf18

[4].B. Dickson, "How to deal with the rising threat of ransomware". 2016 [Online]. Available: https://techcrunch.com/2016/04/16/how-to-deal-with-the-rising-threat-of-ransomware/

[5].K. Savage, P. Coogan and H. Lau, "The evolution of ransomware", 2015 [Online]. Available: https://docs.broadcom.com/doc/the-evolution-of-ransomware-15-en

[6].J.Clement,]"Ransomware - Statistics & Facts", 2019 [Online]. Available: https://www.statista.com/topics/4136/ransomware/

[7].Osterman Research,"Second Annual State of Ransomware Report: US Survey Results", July 2017[Online]. Available:

https://www.malwarebytes.com/pdf/white-papers/SecondAnnualStateofRansomwareReport-USA.pdf

[8]"How to prevent ransomware attacks: All you need to know | Kaspersky", *Kaspersky.com*, 2020. [Online]. Available: https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

[9]D. Palmer, "What is ransomware? Everything you need to know about one of the biggest menaces on the web | ZDNet", *ZDNet*, 2018. [Online]. Available: https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/