# RANSOMWARE ATTACKS IN DISTRIBUTED SYSTEMS

Abhishek Kesiraju, Saurab Gour, Mohammed Arshil Riaz Syed, Sreeja Atluri

## ABSTRACT

Ransomware is a form of malicious software which uses cryptography to encrypt all of the information stored on the system, rendering it inaccessible to legitimate users. The attacker software asks the users to pay a ransom amount for providing a decryption key for regaining access to the system and its files. In general, they target large organizations, such as government agencies, hospitals, and businesses. They choose targets who are likely to have a combination of two important characteristics, vulnerable IT systems, and the financial resources to pay a ransom which could amount to millions or more [1]. According to IBM's cybersecurity researchers' team 'X-Force', Ransomware was the number one attack type observed by X-Force last year, decreasing to 21% of attacks from 23% in the previous year. Ransomware attacks have been evolving over the decade with increasing footprint and with it the ransom amount number has increased to seven, eight-figure numbers. Its evolution reached the stage where it is now recognized as one of cybercrime's strongest business models. The paper aims to present a survey of recent advances in ransomware attacks, how they effect the distributed system model, present effective countermeasures and security approaches that could be helpful in reducing the vulnerability towards these attacks.

## INTRODUCTION

There have been quite a lot of advancements in the field of cybersecurity and so did the evolution of dangerous attacks upon institutions and enterprises. According to ISC Cyber workforce report, there exists 2.72 million people skill gaps in the field and the amount of talent is not meeting required demand surge. Organisations have begun increasing education in the security field for the future generations to meet our challenging needs. Evolution of Web2 to Web3 and the advent of blockchain which are still going through improvements have increased possibilities for malicious attacks to take place and Ransomware attacks among them are a major predicament. This is because, attackers can hide themselves without them being traced due to blockchain's very concept of anonymity during transactions. A report by Kaspersky suggests that 34 percent of businesses hit with ransomware took a week or more to regain access to their data. The paper describes various surveys which highlight the types of ransomware attacks in the next section, their process and provide recent advances in the solutions produced that are considerably authentic.

## CONCEPTUAL FRAMEWORK

### Attack Anatomy

The anatomy allows us to look at how a ransomware attack in general occurs.

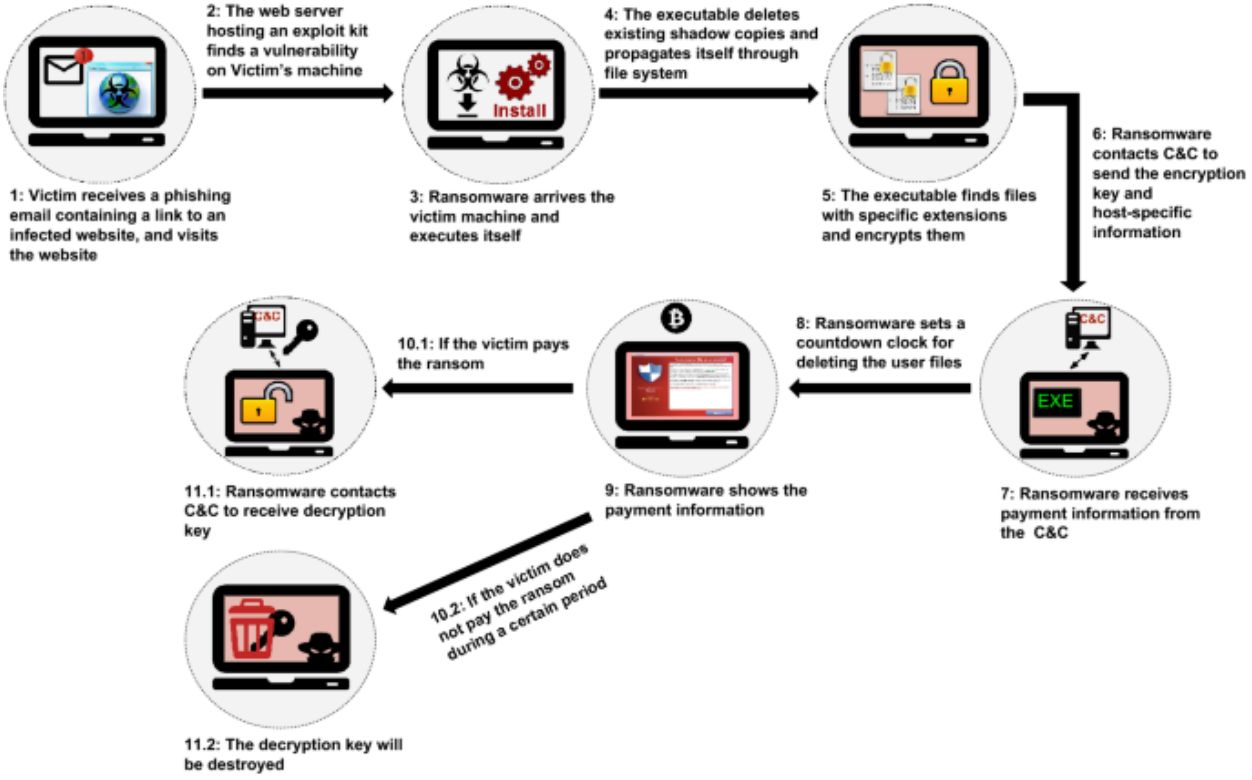
Stage 1: The most common and the foremost initial way to gain access into an organisation's node or bubble continues to be phishing, exploiting any vulnerability and remote services in a distributed system such as remote desktop control.

Stage 2: Gaining access over one node here can be termed as exploiting the initial vector, the next step may involve intermediary remote access tool (RAT) or malware prior to establishing interactive access with an offensive security tools like Cobalt Strike, Metasploit etc.

Stage 3: The attackers then understand and infiltrate the network during third stage, they are consistently focused on about understanding local system the domain they currently have access to and try to keep acquiring sensitive data like passwords, credentials to increase lateral movement

Stage 4: Data collection and exfiltration Almost every ransomware incident X-Force IR has responded to since 2019 has involved the “double extortion” tactic of data theft and ransomware[].. The next stage of the ransomware operators is to find, identify valuable information and exfiltrate it.

Stage 5: Ransomware deployment in almost every single ransomware incident X-Force IR has responded to, the ransomware operators targeted a domain controller as the distribution point for the ransomware payload. In many cases of ransomware deployment, the attackers or operators targeted domain controller as distribution point for the ransom payload.[3]




## SURVEY OF COMMON VARIANTS

GpCode [8] likewise utilized the custom symmetric encryption yet the malware has been improved over time. The malware was spread as job advert through spam emails. In its initial assault in May 2005, a static key was created to encode all the non-system files. The original data was erased when the encryption is finished [9]. Nonetheless, the key was discovered by comparing the original data with the encoded information. Another variation of GpCode, called GpCode.AG was found in June 2016, encryption depended on 660-piece RSA public key. In June 2008, another variation, GpCode. AK, was recognized yet it was truly hard to crack owing to the computational demand.

Reveton, which is otherwise called Police Ransomware, is generally spread through obscene sites [10]. It changes the extensions in the windows inside system32 folder and presents a notification webpage to its victims [11].

Locker Ransomware was identified in 2007 [8] and it doesn't alter its victim’s information yet just locks their devices and applications. Data on this device can then be transferred to another location. Additionally,

ColdBrother Ransomware locks casualties' mobile phones, takes photos with cell phone cameras, answers and drops incoming calls, and looks to cheat victims through banking applications. Crypto Ransomware encrypts basic documents on victims' computer as a payload for blackmail. Critical files are identified and encrypted with 'hard-to-guess' keys. The type of encryption keys and coordination of assaults are performed by an order and-control server [12]. Crypto Wall, Tesla Crypt, CTB Locker, and Lock are variations of Crypto Ransomware.

CryptoWall was introduced in November 2013, and it is circulated by email as an attachment, and it consists of script file and an exploit kit. In this attack, malware is injected into explorer.exe and codes are copied into %APPDATA%, this will create a registry value run key in the local registry. This keeps the malware in the victim's computer even after reboot and ensure that the system cannot be restored to an prior point by running processes like vssadmin and dcbedit. In CryptoWall 2.0, walmare was update with multiple propagation such as e-mail attachments, drive-by download, and exploit kits. A few randomized information was brought into CryptoWall 3.0 and 4.0 to make malware detection more difficult by using exploit kits for privilege escalation and the Invisible Internet Project (I2 P) network for achieve anonymous peer-to-peer network.

CryptoLocker makes a set of extensions in the admins account which enables it to change internet files and create creates executable files in localAppData folder and important files are detected for encryption. The malware utilizes the RSA + AES algorithm for its encryption and its endeavor pack is known as Angler [16].

Curve Tor Bitcoin (CTB) Locker is also circulated through exploit units and email, command and control server is hidden on the Tor network. Difference with CTB Locker is its capacity to encrypt target files with no association with the Internet and it utilizes a mix of AES, SHA256, and Curve25519 for its encryption. This malware basically targets WordPress-based sites through a PHP scripts [13].

TeslaCrypt, a new variation of ransomware, takes advantage of weak sites utilizing AnglerINuclear exploit kits and has a similar distribution as CryptoWall.

Locky had its initial attack in February 2016 and the malware program was spread by connecting a Microsoft Office document to spam email. Attached document to the email would contain a macro that would download a malicious program. Locky extends it encryption to external storage devices as well , along with all network resources and databases. These documents are attacked to put the victim under a lot of pressure for him or her to pay. There are additional efforts made to prevent shut down of command-and-control server. This sort of malware utilizes hardcoded order and control server Internet Protocol (IP) addresses [15]. Locky is one illustration of a forceful ransomware variation. For example, In 2016, it was compromising as many as 90k victims per day. Around then, the normal payoff for a Locky assault was ordinarily somewhere in the range of 0.5 and 1 Bitcoin. Overall, 2.9 percent of compromised casualties in a ransomware assault would pay the payment. All things considered, Locky would possibly taint upwards of 33 million casualties more than a year time frame, coming in the middle between $287 million and $574 million in recover installments [2]

Cerber use the Dridex spam network to circulate the malware by means of huge spam campaigns. The notification of attack is voiced through a text-to-discourse module [15]. Devices on Windows 10 Enterprise have been attacked with more than 200 cases around December 2016.

PowerWare was launches through a phishing campaign and malware process is like that of Locky however its encryption and hard-coded keys are somewhat feeble. A decryption tool has been developed to evade ransom.

ScareMeNot Ransomware is for the most part focused on at Android based devices and it has gone after more than 30,000 gadgets [19]. TROJ_CRYZIP.A was found in 2005 [7]. Documents on targets computer are normally zipped and locked.On Contrary, KeRanger is focused on at Apple based devices and is spread as a trojan on the Transmission Bit Torrent client. Victim installs the application, a binary file that is placed in the computer is renamed and stored in the library directory as 'Kernel_process' for execution. All the files with a particular file extension are encrypted after 3 days in the victim's computer.

Seftad launches its attack on Master Boot Record (MBR), which contains the executable boot code and partition table [9].In this attack, it replaces the boot code in the active partition with a robust MBR and then that displays the attack notification, further it prevents the target computer from loading its boot code. Since the key is not hard coded generally, payment of ransom can be evaded through reverse engineering.

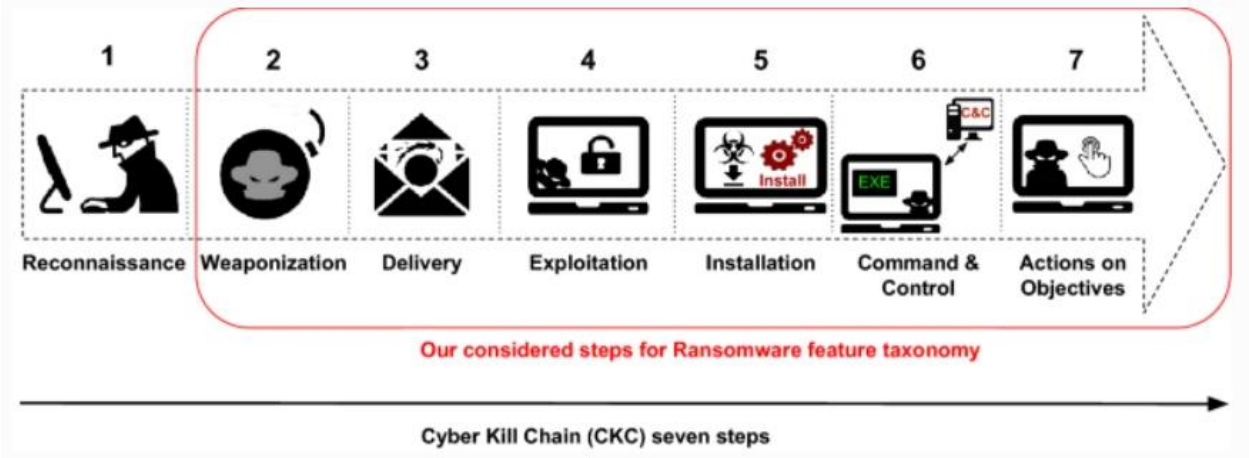
LowLevel04, otherwise called Onion Trojan-Ransom, was spread through the Remote Desktop or Terminal Services through brute force attack. Files will be encrypted using AES encryption using the RSA algorithm. SilentCrypt pays special attention to explicit confidential files to know whether the code if running in an analysis environment or not. DirCrypt utilizes a hybrid approach to deal with encrypt victim files. The initial 1024 bytes are encrypted utilizing RSA while the rest are done using RC4.

Petya Ransomware when first gets installed will replace boot drive's existing Master Boot Record, with a malicious loader. This boot record contains information which is placed at beginning on hard drives which tell PC how OS should be booted. This will then reboot the windows in order to execute the new malicious software, when starting it will pretend to be the CHKDSK instead of the fake one whilst it corrupts the Master File Table and encrypts it. When this happens, the computer will not remember what files existed in the computer or if they are present anymore. Once the malicious CHKDSK is finished, it will present a locked screen with instructions that are connected to a TOR site where we must pay the ransom using a unique ID.

**EXISTING SOLUTIONS AND STRATEGIES**

According to IBM's X-force, attackers are taking an average of 17 months before they rebrand themselves and attack with a new name and Europe of all countries is the second most attacked. The section presents the methods followed by the cybersecurity expert organisations.

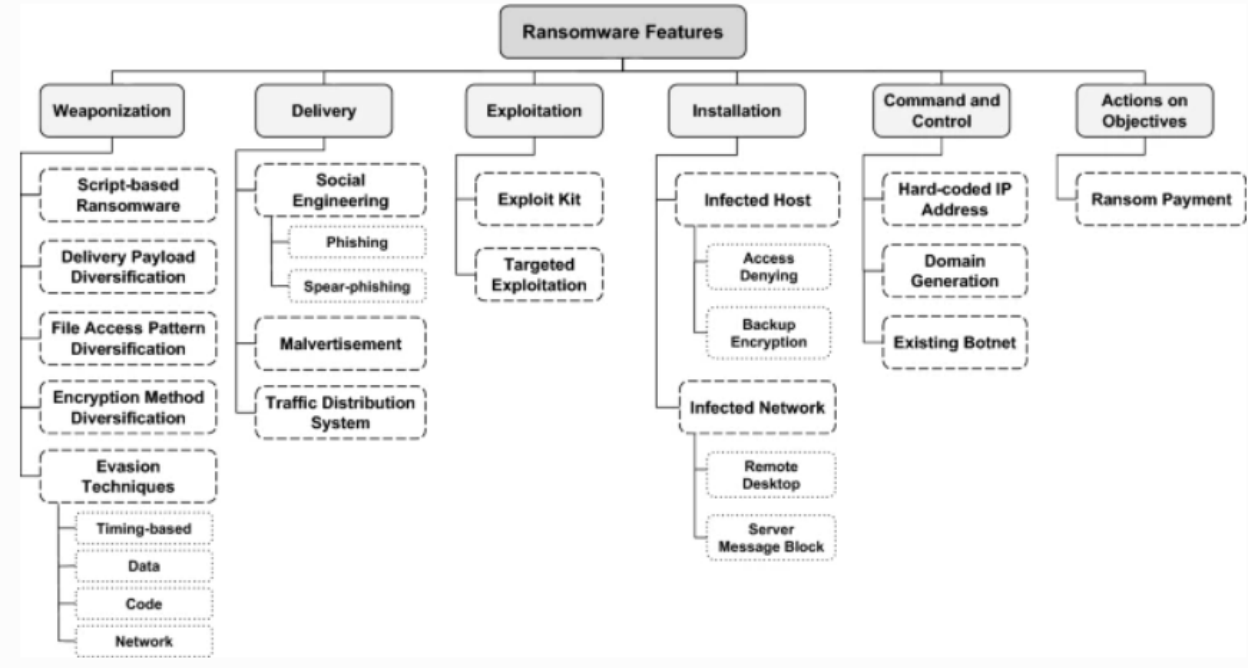
1. Lockheed Martin proposed the Infiltration Kill Chain (IKC), commonly known as Cyber Kill Chain (CKC), in 2011 and it was quickly adopted by the market for simulating network attacks from the hackers' point of view [22]. To produce (threat) intelligence regarding the TTPs (Tactics, Techniques, and Procedures) of attackers and attack attribution, the CKC model is utilised [20]. In order to recognise, guard against, and moderate against attacks and ransomware variants like [22], many investigators have embraced the original CKC model [20]. Nevertheless, other researchers [23] modified the CKC model's initial description to suit their own needs and offered other phases for the cyber attack chain model.




2. Requirements are as follows of the Lockheed Martin Cyber Kill Chain (CKC) [22]. The subsection highlighted mostly by red rectangle identified six processes that we took into account when creating our malware feature classification.

CKC outlines seven processes for hackers to follow in order to accomplish their goals (see Fig. 2): reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on goals.

| Phase | Detect | Deny | Disrupt | Degrade | Deceive | Destroy |
|---|---|---|---|---|---|---|
| Reconnaissance | | | | | | |
| Weaponization | | | | | | |
| Delivery | | | | | | |
| Exploitation | | | | | | |
| Installation | | | | | | |
| C&C | | | | | | |
| Actions on Objectives | | | | | | |




1. **Zero Trust assists:**
   A paradigm shift, or unique strategy to security concerns, zero trust assumes a violation has indeed occurred and seeks to make it more difficult for a hacker to operate around a network. Determining where sensitive information is located, who has the accessibility to it, and implementing reliable measures throughout a system to make sure only the appropriate people are using it in the appropriate direction are at the core of the process. Since many malware attackers try to spread their malware to a system using a breached network adapter, implementing the access controls rule on datacenters and administrator rights credentials in especially can raise hurdles for these attackers. Using MFA further makes it increasingly challenging for hackers to gain access to internal systems by enabling them to use other multifactor authentication in addition to their account hijacking.
2. **Security automation –**
   Enhancing incident management capabilities is vital, whether those entails locating and eliminating, types of threats before they would infect a system with malware or swiftly and effectively addressing problems to free bandwidth hogging during the next occurrence. Security automation is essential in this incredibly quickly climate, delegating to computers duties that may take a human researcher or staff hours, and figuring new ways to streamline operations.
3. **Extended detection and response:**

   Recognition and feedback techniques give organisations a strong benefit in locating and eliminating intruders from a system before they could even complete their strike, such as malware implementation or data breaches. This is especially true while several possible methods are merged into a prolonged prevention and detection (XDR) solution.

**Develop a response plan for ransomware.**

Each organization and region is susceptible to a malware assault, and how your team reacts in the crucial moment will determine how much effort and cost are invested in the recovery. — Incorporate initial control

measures, who must be notified, how your organisation will securely store and recover from archives, and a secondary site where vital business operations may be carried out while cleanup is being carried out in your response plan. — Include a possibility of data breaches and leakage as part of the malware assault in your plan; this is a highly popular strategy utilised today and is seen in a sizable portion of the cybercrimes that X-Force resolves. Use malware simulations to consider how your company would pay a hostage and what reasons might change your choice. — Make sure your malware action plan has a particular backup for internet incidents, as they can call for more equipment and expertise. — Flash storage technologies that assist in preventing loss of information, promoting organizational consistency, and reducing operational expenses can prevent you from getting memory leaks related to virus or extortion assaults.


Figure 1: Incident response lifecycle (based on the NIST)

Role-based, end-user education

Although end users frequently experience security problems initially, proactive end-user education and training are essential in assisting in the prevention of breaches of all forms. Hacking, corporate email breach (BEC) theft, hazardous spam (malspam), and consequently ransomware and malware events, should be highlighted in training. It is advised that end users receive frequent training in the following subjects because users are the first line of defence against even the most secure environments: What actions they should take and avoid taking in response to threats; What risks they are likely to experience; How and where to report problems In the end, a workforce that is security-aware is a culture asset that is doable and may effectively increase the company's cybersecurity posture.

**PREPARATION**

1. Role Based User Education:
   Preparing employees on basic cybersecurity education helps many organisations to find out the attack and avoid them. This is because about 41% of the time, the mode of attackers is by phishing business email boxes.
   Hence it is important that the employees are trained upon:
   - Kind of threats that they can possibly encounter
   - What are the actions or tasks that they should perform at that moment?
   - Where and how they can report these issues from being spread or can be looked into?

   Some of the other recommended strategies include disabling macros, misconfigurations at various entry points, not using default passwords and deploying MFA wherever possible, stripping emails with attachments or executables wherever possible, disabling flash etc

**DETECTION**

The first and foremost step is to contain the infection without spreading and isolating the systems which were infected. Teams inside organisations should be trained upon being alert regarding such scenarios.

Few of the common scenarios include:

Network users getting to files on network share that are encrypted, users attempting to open files that are locally presented and are encrypted, finding random messages on computer, users identifying massive file manipulation etc. Some commonly practiced and recommended strategies are:

Isolating the user computers from network that were identified, they should be disabled from contact to the network, location, organisation's VPN and should be washed out.

Not rebooting the system while the network is still connected and notifying the IT staff immediately.

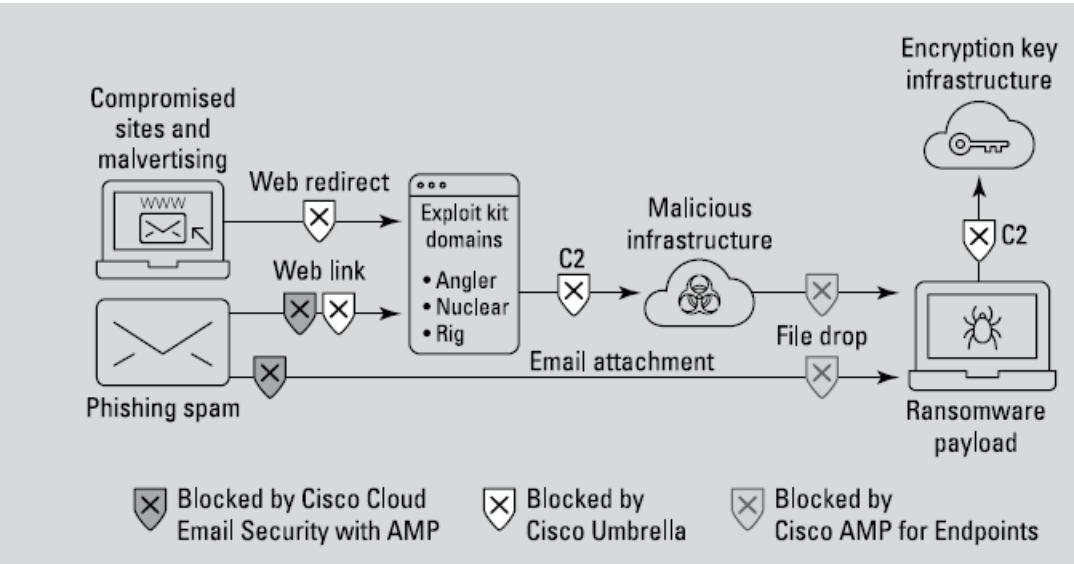
**ANALYSIS**

Analysis can be classified into two steps:

- First is finding out what is the specific variant of the software.
- Second, performing root cause analysis where it arrived from.

Here we can use different kinds of methods like using the features chart provided above to classify what kind of malicious variant has infected the network. Next is to do the RCA (root cause analysis), so the point from where attack happened. Some of the common scenarios include email entry, browser exploitation, drive by download entry, manual methods etc.

Cisco provided a closer look at provisioning advanced email security as shown in the figure below:



## CONTAINMENT

The containment phase of a ransomware attack is critical, and we have to make sure that the systems effected are isolated with no possibility of connection to other systems or networks. This method removes the possibility of the ransomware to be continuing the encryption process.

Having an antivirus protection that provides an Endpoint Detection and Response solution as a part of the security automation helps in detecting these infections at early stages.

## ERADICATION

This phase involves removing the ransomware from infected systems. “Rely on trusted templates and settings that are kept safely for cases like these infections.” [3]

If malware was identified to be arrived from email, considering scrapping all the email boxes and isolating those systems and do not connect them back till all the systems are checked and eradicated. It is highly recommended to use MFA to devices and not use default passwords. If the attacked happened through browser, block all the infectious websites and should be actively monitored. Any weaknesses or vulnerabilities in the browser should be found out and fixed.

Decryption of the algorithms although not possible in many situations, once the specific variant is identified from the templates, can be applied but data recovery is never guaranteed.

## POST-INCIDENT ACTIVITIES

This includes patching all vulnerabilities that are present in the system due which the attack occurred. Data is to be restored from the backups maintained using secure streamlines. The X-force recommends the strategy of maintaining redundant backups segregated in different locations and some of them present offline in cold storage. In situations where data loss occurs due to these attacks, then can be brought to life once the incident is completely solved.

## CONCLUSION

The paper presented an abstract survey of various kinds of ransomware attacks that occurred for the last two decades and then provides the common view of how such cybersecurity incidents are tackled that were provided corporate leagues such as IBM, Microsoft etc. Investigating various such threats and vulnerabilities is an in-demand research area where businesses are thriving towards ethical practices of carbon footprint and to avoid data loss or businesses exploited of their work. Paying the ransom is never a solution to this problem since it only strengthens the business model of attackers. As the time evolves, variants of ransomware have been increasing due to the profitability of such acts. Automation in this field is an iterator approach and it is said that it almost takes one week on an average to recover from a ransomware attack. Hence it is highly needed that organisations continue research and create solutions for recovering and defending systems better and faster.

**REFERENCES**


[1] Mike Chapple, *CISSP: Cert Prep (2021): 3 Security Architecture and Engineering*. (Feb. 2022), Ransomware. Accessed: Jul. 7, 2022. [Streaming video]. Available: LinkedIn Learning database.

[2] Ransomware Defense For Dummies®, Cisco 2nd Special Edition

[3] IBM Security X-Force Threat Intelligence Index 2022 Full Report

[4] Dargahi, T., Dehghantanha, A., Bahrami, P.N. et al. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. J Comput Virol Hack Tech 15, 277–305 (2019). https://doi.org/10.1007/s11416-019-00338-7

[5] https://boingboing.net/2016/03/28/ransomware-gets-a-lot-faster-b.html

[6] https://www.globenewswire.com/en/news-release/2022/04/27/2430299/0/en/Cybersecurity-Skills-Gap-Contributed-to-80-Percent-of-Breaches-According-to-New-Fortinet-Report.html

[7] https://www.ibm.com/security/threat-intelligence

[8] R. Richardson and M. North, "Ransomware: Evolution, Mitigation and Prevention," International Management Review, vol. 13, p. 10, 2017.

[9] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the gordian knot: A look under the hood of ransomware attacks," in International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, 2015, pp. 3-24.

[10] D. P. Pathak and Y. M. Nanded, "A dangerous trend of cybercrime: ransomware growing challenge," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume, vol. 5, 2016.

[11] P. Zavarsky and D. Lindskog, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," Procedia Computer Science, vol. 94, pp. 465-472, 2016.

[12] M. Weckstén, J. Frick, A. Sjöström, and E. Järpe, "A novel method for recovery from Crypto Ransomware infections," in Computer and Communications (ICCC), 2016 2nd IEEE International Conference on, 2016, pp. 1354-1358. [13] H. Haughey, G. Epiphaniou, and H. M. Al-Khateeb, "Anonymity networks and the fragile cyber ecosystem," Network Security, vol. 2016, pp. 10-18, 2016.

[13] H. Haughey, G. Epiphaniou, and H. M. Al-Khateeb, "Anonymity networks and the fragile cyber ecosystem," *Network Security*, vol. 2016, pp. 10-18, 2016.
[14] K. Cabaj and W. Mazurczyk, "Using software-defined networking for ransomware mitigation: the case of cryptowall," *IEEE Network*, vol. 30, pp. 14-20, 2016.
[15] E. Kalaimannan, S. K. John, T. DuBose, and A. Pinto, "Influences on ransomware's evolution and predictions for the future challenges," *Journal of Cyber Security Technology*, vol. 1, pp. 23-31, 2017.
[16] K. K. Gagneja, "Knowing the ransomware and building defense against it-specific to healthcare institutes," in *Mobile and Secure Services (MobiSecServ), 2017 Third International Conference on*, 2017, pp. 1-5.
[17] B. Herzog and Y. Balmas, "Great Crypto Failures," 2016.

[18] A. Green, "Ransomware and the GDPR," Network Security, vol. 2017, pp. 18-19, 2017.

[19] T. C. Back, "Intel's Core M Chip could let manufacturers build ultraslim laptops."

[20] B. Kim, "AN ANALYSIS OF VULNERABILITY EXPLOITATION TECHNIQUES USED BY OSX MALWARE AND THEIR DEFENSES."

[21] M. H. U. Salvi and M. R. V. Kerkar, "Ransomware: A cyber extortion," Asian Journal of Convergence in Technology, 2016.

[22] A. Kharraz, S. Arshad, C. Mulliner, W. K. Robertson, and E. Kirda, "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware," in USENIX Security Symposium, 2016, pp. 757-772.

[23] M. Wecksten, J. Frick, A. Sjostrom, and E. Jarpe, "A novel method for recovery from Crypto Ransomware infections," in 2nd IEEE International Conference on Computer and Communications, ICCC 2016, 2017, pp. 1354-1358.

[24] L. Usman, Y. Prayudi, and I. Riadi, "Ransomware analysis based on the surface, runtime and static code method," Journal of Theoretical and Applied Information Technology, vol. 95, pp. 2426-2433, 2017.

[25] M. Simmonds, "How businesses can navigate the growing tide of ransomware attacks," Computer Fraud and Security, vol. 2017, pp. 9-12, 2017.