International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Elucidating Ransomware Attacks In Cyber-Security

Cyrus Mehra, Arvind K. Sharma, Avinash Sharma

Abstract* — *Attack Detection and Prevention services or activities has distinct significance in the subdomains like 'Computer-Security' and 'Internet-Security' of Networking as compare to other activities of the same area. Major issues arise when resources get compromised with the unauthorized user(s) having adverse effects afterward. Even though much standard security mechanism like IDS, Cryptographic Techniques available to provide security & authenticity still some attacks are un-detectable like Ransomware which force security providing agencies to take initiative in this direction with proper conceptions.

Keywords: Adversary, Anti-Piracy, Antivirus, Bit-Coins, Cyber-Security, Dark-Web, Encryption-Decryption, Internet-Security-Suite, Intrusion-Detection-Systems (IDS), Malware, Software;

I. INTRODUCTION

In Computer-Networking particularly i.e., in an inter-connected environment over the past few decades, Technology has become an intrinsic aspect of the workplace. Security threats have also withal transmuted from physical to cyber, as the world has made a move from the physical to the Digital scene. Digital wrongdoings have represented trillions of dollars in misfortunes, according to 'Juniper' research inquire about the sum in 2019 was $2 trillion. As a result, firms and Organizations/Corporates everywhere the planet, as well as governments and industries of varied countries, are giving 'Cyber-Security' a prime priority and setting standards for the 'cyber-security' protocol for the coming years. 'Cyber-Criminal(s)' stole money from bank accounts, industrial espionage and in some cases also took over the company system and demanded money as a ransom to unlock them. Ransomware has maintained a reputation as one of the major threats since 2005, with the first attack occurring much earlier. The primarily known ransomware assault happened in 1989 and the health-care industry was focused on [13]. At that point, 28 years after the fact, the health-care industry stays a top goal for "ransomware attacks". It was started by an AIDS researcher "Dr. Joseph Popp", 'Ph.D.', who distributed 20,000 'floppy disks' to other AIDS researchers spread across more than 90 countries, claiming that the disk delimited a program that analyzed the peril of acquiring 'AIDS' through the utilization of questionnaire.

However, with this program, the disk withal contained the **'Malware program that initially remained dormant in systems and triggers when the system was powered on 90 times".** After reaching the 90th start threshold, the malware exhibited a message importunating a payment of $189 and another $378 for a software lease. This "Ransomware-Assault" wound up known as the "AIDS Trojan" or the "PC Cyborg". In December 1989, a large number of floppy disks holding what professed to be an intuitive database on 'AIDS' and a computer-based questionnaire that professed to determine patient's peril of contracting 'AIDS' were sent to participants at a "World Health Organization" (WHO) and endorsers of a computing-publication. Relative to "PC-Cyborg Corporation", the software had a licensing agreement that should of deep interest to the Anti-piracy Entertainment industry legal-enforcers". "**If you install [this] on a Microcomputer, then under terms of this license you agree to pay 'PC-Cyborg Corporation' in full for the cost of leasing these programs, it read. The cost, $378 U.S., was to be sent to a post office in Panama"**. Proceeding noxiously, it expressed: "On account of the breakdown of this legal-agreement, "PC-Cyborg" maintains all authority to start a lawsuit important to recuperate any outstanding-debts payable to "PC-Cyborg Company" and to utilize programming mechanisms to guarantee the end of your utilization. These program systems will unfavorably influence other program applications. You are thus informed with respect to the sternest consequences of your inability to comply with the terms of this legal-agreement; your integrity may haunt you for the rest of your life and, your 'PC' will quit working conventionally. You have sternly precluded from distribution of this product with others".

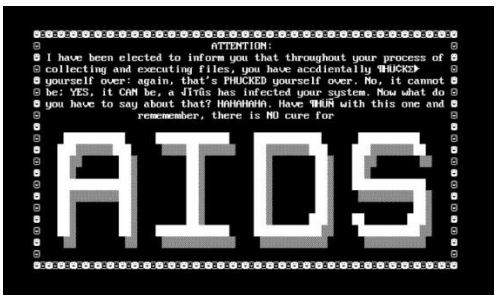

Fig 1.1: AIDS

The rest of the paper organized as Section-II describe thoroughly about 'Ransomware' and its well-known Types, Section-III about Infection Vector i.e. how this attack going to infect resources, then in Section-IV, V we're covering various famous application area where this attack gain interest unlawfully with that particular attack cost. After all these sections suitable conclusion provided.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Cyrus Mehra*, Scholar, MM Institute of Computer Technology & Business Management (MCA), Research Scholar, University School of Engineering & Technology Rayat Bahra University, Sahibzada Ajit Singh Nagar, Punjab, India.
Arvind K. Sharma, Assistant Professor, MM Institute of Computer Technology & Business Management (MCA) Rayat Bahra University, Sahibzada Ajit Singh Nagar, Punjab, India.
Avinash Sharma, Professor, MM Engineering College (MMEC) MM(DU), Mullana, Ambala, Haryana, India.

II. RANSOMWARE

Variants and Attacks [23] have increased over the year(s) and targeted sectors ranging from Public/Private 'Healthcare' to 'Banking-Bodies' suggest that ransomware has gradually increased as a result of progression made in this field, by its creator(s). **Ransomeware** [1][5] **Developers are not only making 'Encrypted' files harder to recover but also making sure that ransomware is hard to detect** – by changing the predictable nature of the same, make it more difficult for the 'Security Software(s)' (i.e. IDS, Antiviruses, Internet Security Suits, etc.) to find and eliminate it. **Ransomware creators are going to slow down the speed of the Encryption and Randomizing it to avoid detection**. For instance, if the threshold of the security software is looking for 'X' number of files being accessed in 5 seconds, they are spreading the time frame over 1000 seconds so that they will not be detected. This process of spreading the time of encryption over a large amount of time not only encrypts files but also attacks 'Backup-Files' and encrypt them. With regards to randomizing this process, while '**Anti-Ransomware Tools**' look for linear patterns in encrypting data, ransomware developers overwrite files rather than going through them in a linear manner, just to avoid any type of detection. They are also using 'Polymorphic –Codes' in order to complicate the ransomware detection process. The polymorphic code changes every 10-20 seconds which makes statistical detection of ransomware files extremely difficult. Statistics and data on ransomware express that cybercriminals or adversaries are concentrating more progressively on industries that will often be equipped to pay thousands of dollars to get their data back. [14]. Have a look:

- Ransomware produces over $25 million as income for Cybercriminals each year. (Source: "**Business-Insider"**)
- An average ransom demand augmented to $1077 in 2018.
- Ten percent of all payoff requests are over $5000. (Source: "**Datto"**)
- Fewer than 33% of organizations that pay the payment get the majority of their data back. (Source: "**Courant"**)
- It took a week or more for 34% of businesses organizations affected by malware to recover access to their data.. (Source: "**Kaspersky Labs"**)
- 1.5 million new phishing sites are built every month. (Source: "**PhishMe"**)
- A new organization will be a victim of ransomware every 14 seconds in 2019 and every 11 seconds by 2021. (Source: "**Cyber-Security Ventures"**)
- Ransomware attacks have amplified by more than 97 percent in the previous two years. (Source: "**PhishMe"**)

Now let's have a look in some more detail about this particular type of attack starting from vary basics onwards.

What is Ransomware?

"Ransomware" or "Ransom-Malware" is a sort of malware that prevents or victims from retrieving access to their systems or personal files by encrypting them and demands payment of a ransom from the victim to re-establish access to the information or data upon payment. To Users instructions provided on how to pay money to get the 'Decryption-Key' (i.e. About Encryption-Decryption/Authentication process various renowned standard algorithms available, about this information is fully provided in our another article, so we're not focussing on this task here [11][12][23]). The cost can range from a few hundred dollars to thousands, payable to cybercriminals in Bitcoin.

Digital Gold – Bitcoin

With ransomware and other Cyber Attacks becoming a cumulative risk around the world, there's a growing interest in 'Bitcoin' as it appears to be the preferred currency of hackers to receive ransom money. It is a completely 'Digital-Currency' that is independent of any bank account or governments, the currency is worth more than gold. **Bitcoin is the preferred method of payment among libertarian crowds and tech enthusiasts and it's also preferred throughout the 'Dark Web' and with hackers. This is because transactions can be anonymized. Though every transaction bitcoin had a traceable history, due to the lack of data on user there's no way to recognize the recipient, hence anonymity**. Using Bitcoin is as modest as creating a 'Virtual-Wallet', and united with how easy it is for cybercriminals to create and distribute ransomware, hackers can easily make a profit through this service. Once they have the bitcoins, it's very simple to wash them via Dark Web. '**Washing of Bitcoins**' generally refers to the process of removing all traces of previous ownership and transactions. So, that they can convert the coins into cash.

Types of Ransomware

Ransomware is categorized into the following three categories: -

Ransom Scareware

Scareware incorporates maverick security programs or software and technical` support tricks. A pop-up up message will be appeared, guaranteeing that malware was found and the best way to dispose of this is to pay up. In scareware, the files are essentially safe but the pop-ups appear frequently until the payment has been made. This sort of ransomware can be effectively evacuated by "Anti Malware" or by moving the contaminated drive to another non-infected system and getting access to the data from another "Operating-System" as a non-bootable drive.

Screen Locking Ransomware

This type of ransomware embraces the whole operating system interface hostage, making it apparently difficult to influence the operating system in any way. Screen lockers freeze your system completely, after firing up the system, a full-sized window will show up which won't permit you to do anything else associated with the original purpose of the computer system. Usually accompanied by an "FBI" or the "United States Department of Justice" stamp saying that criminal behavior or illegal activity has been identified on your computer system and you need to pay a fine.

Encrypting Ransomware

Encoding Ransomware is the most feared sort of ransomware on the grounds that it keeps its capacity to scramble your documents making them unusable until the "Encryption Key" is given. In this sort of ransomware, the hackers grab up your data and encrypt it, demanding ransom so as to decrypt and redeliver. Once cybercriminals get a grip on your records, no security program or software can return them to you. There's no assurance that cybercriminals will give your data back on the off chance that you do pay up.

III. INFECTION VECTOR

Ransomware attackers aim to inject their malicious code and program onto potential victims' systems or other devices, and there are various strategies that they utilize to accomplish this.

Malicious E-mail attachments and Links

With malevolent email attachments and links, the assailant creates an email so that it looks likely from a real or authentic source, for example, 'Human–Asset' or 'IT' and appends a vindictive file, for example, "Portable Executable" (PE) document, a "Portable Document Format" (PDF) document, a ".JS" file or a "Word Document". The victim downloads the attachment discerning the Email has been directed from trusted sources. When the file is opened, the payload is unwittingly downloaded which contaminates the computer system and encrypts the data.

Exploit Kits

"Exploit Kits" are executed when an individual visits a compromised website. Malignant code is hidden on the site, even in an advertisement (i.e. "**Malvertising**"), inadvertently redirecting the victim to the landing page where the exploit-kit is installed. And if a victim is vulnerable, at that point a "drive-by-download" of a vindictive payload will be executed which really taints the computer system and the data will be held for ransom.

Downloaders and Trojan Botnets

Downloaders are released from software hosting websites, whose official goal, apart from providing software to its users, is to permit users to download legitimate files, and as a hidden functionality malware without the user noticing it.

Social-Engineering Strategies

Social engineering can be explained by the statement ─ "There's no patch to human stupidity". Victims are tricked into downloading an email attachment or clicking on some infectious link or sometimes deceiving users into installing a fake 'Antivirus', by showing results of scans allegedly showing malware on the user's computer system or device.

Malvertising

In the case of 'Malvertising', an individual visits a legitimate website that showcases advertisements provided by an outsider promoting system. And these ads contain vindictive code, it will endeavor to exploit the unpatched vulnerability in the victim's web- browser so that the ransomware can be downloaded.

Social Media or Messaging Applications

Sometimes cybercriminals put forth an admirable attempt to contaminate the victims with ransomware or some exploit, and one of the initiatives uses messaging apps like 'Facebook-Messanger' as an attack vector. The cybercriminals send messages over the messaging amenity to a wide scope of users or victims (i.e. in groups) and these messages comprise a picture or image in 'Scalable Graphics File' (SVG) format that includes an implanted piece of malicious 'Java-Script'. Opening the image redirects the victims to a video on a spoofed 'You-Tube' site that actually asks users to download and install a browser extension or plugin – in order to view the video. Installing an extension reasons the "malware-downloader" to run and infects the system with various variants of malware including the Locky ransomware.

Traffic Distribution Systems (TDS)

TDS [15] is just like malvertising, cybercriminals buy redirected web traffic to the site hosting the exploit kit as to enable the "drive-by-download" of the malicious program, and act as a service for mass-marketing malware. TDS vendors sell the traffic from when a victim clicks on a link.

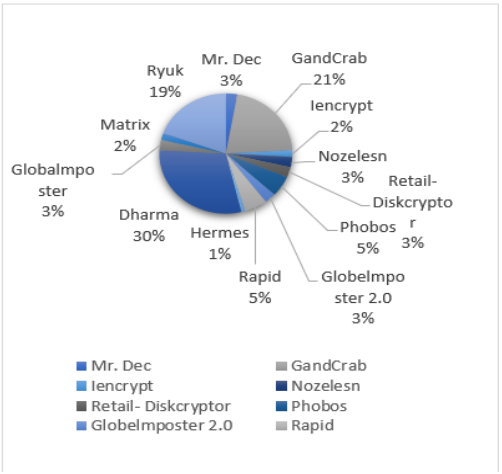

Fig 3.1: Ransomware Market Share

The above pie-chart demonstrates the ransomware market share by type in Q1 of 2019 [16]. Here, the Dharma/Crysis ransomware continued to be the most predominant type of ransomware in Q1 2019 Kaspersky Labs, nevertheless Ryuk also grew substantial market share. The 3 most common types (Dharma, Ryuk, and GandCrab) are unique in their spreading methods, targets, and costs. Crysis/Dharma is delivered manually in the targeted attacks by exploiting leaked or weak Remote Desktop Protocol (RDP) credentials. This implies a hacker is accessing the victim's machine prior to the infection by 'Brute-Force' the RDP protocol in Windows on port 3389 [17]. Ryuk is used exclusively for tailored attacks and its encryption scheme is intentionally designed for small-scale operations, such that only important resources and data in each target network will be infected with its infection and distribution carried out manually by the cyber criminals [18]. Gand-Crab follows an affiliate marketing business model, which is 'Ransomware-as-a-Service' (RaaS), which actually allows cybercriminals to create ransomware without technical knowledge of how to create them. An individual can discover different RaaS bundles in the market that diminish the necessity to code the malware. [19]. A comparison between the top three types of ransomware by attack vector is shown in the below-given figure.

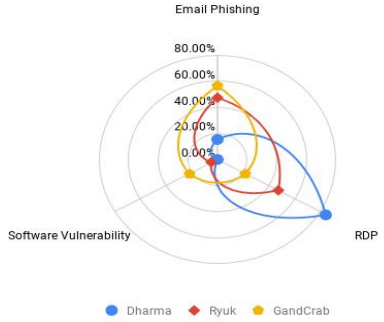

Fig 3.2: Ransomware Attack Comparison

Variations in the attack vector mimicked the intricacy and prophecies of threat actors dispensing ransomware. “Dharma” kept on exploiting the RDP ports, typically found in small businesses. Whereas, Ryuk relies heavily on targeted email phishing, indicating the preference of threat actors to go after large organizations.”Gandcrab” is one of the main ransomware-type to use software-vulnerabilities.

IV. VULNERABLE APPLICATION/AREA

According to the report by ‘Kaspersky-Lab’, the most popular vulnerabilities in the ‘Microsoft –Office’ suite was “CVE-2017-11882” and “CVE-2018-0802”. They are related to the "Equation-Editor Component" and cause buffer overflow with subsequent remote code execution. The share of vulnerabilities discovered in browsers is nearly five times lower than Microsoft-Office by 14%. Exposing browser vulnerabilities is often a problem because browser developers always come up with new options to protect against certain types of vulnerabilities, while techniques to circumvent them often require the use of entire vulnerability chains to achieve the objective. Which increases the cost of such attacks. [16]. Specialist administrations, for example, law offices and CPA firms, are concentrated by ransomware at all times. Minor ‘Healthcare-organizations’, for example, local ‘specialist-offices’ are frequently focused too. These organizations tend to under-put resources into IT security and reinforcement approaches and have a low resilience for information misfortune, which makes them defenseless ransomware targets.

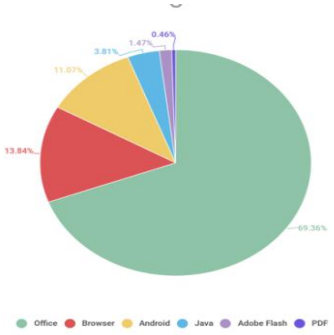

Fig 4.1: Ransomware Ratio on Different Application Softwares

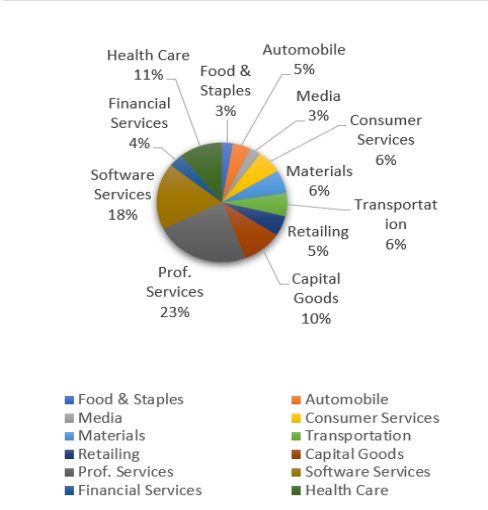

Fig 4.2: Target Industry Percentage of Ransomware Attack

RANSOMWARE-AS-A-SERVICE (RaaS)

Ransomware-as-a-Service (RaaS) obtains from the Software-as-a-Service (SaaS) model. This is a membership-based vindictive model that empowers tenderfoot cybercriminals to execute ransomware attacks without much effort and without specialized learning of how to make ransomware. This malevolent model enables anybody to turn into an “affiliate” of a built-up RaaS bundle or Service [22].

HOW RaaS WORKS?

As per this noxious deployment model, cybercriminals compose ransomware code and sell or lease it under a member program to different cybercriminals who have the intent to dispatch the assault. They also provide step by step procedure to dispatch a ransomware assault by utilizing the service, a platform that can also display attack status using a "real-time" dashboard. “**Once the attack is successful, the ransom amount is divided among the service provider, coder, and an attacker”** [22]. Raas Service providers also advertise their services on the “Deep web”. There are several reasons for cybercriminals to be drawn towards this "Franchise-like distribution". It empowers the ransomware creators to gain some brisk cash. With respect to the members, it diminishes the requirement for them to compose malicious code. Individuals without technical knowledge can essentially lease simple to-utilize bundles along with step by step instructions to use it.

V. ATTACK-COST

The all-out cost of a ransomware attack can be isolated into two principle costs:

Recovery-Cost:

These expenses provide support for forensic reviews and reconstruction servers and work-stations. In the event that a payment is paid, at that point that is likewise a recuperation cost.

Downtime-Cost:

The most expensive cost of a ransomware-attack is the overall cost of downtime. The cost of downtime is typically 5–10x the actual ransom amount and is measured in lost productivity (sluggish labor, lost revenue opportunities, and loss of goodwill).

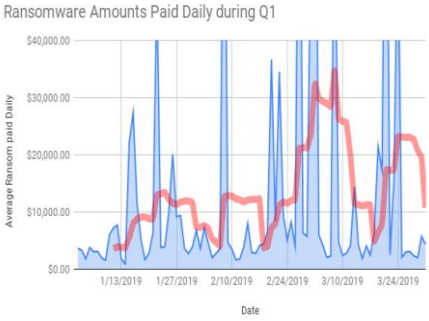

Fig 5.1: Average Amount Paid Everyday

“In Q1 of 2019, the average ransom rose 89% to $ 12,762 compared to $ 6,733 in Q4 of 2018”. The ransom increment reflects increased infections of more exclusive types of ransomware like “Ryuk”, “Bitpaymer”, and “lencrypt”. These sorts of ransomware are prevalently utilized in bespoke targeted attacks on larger undertaking targets.

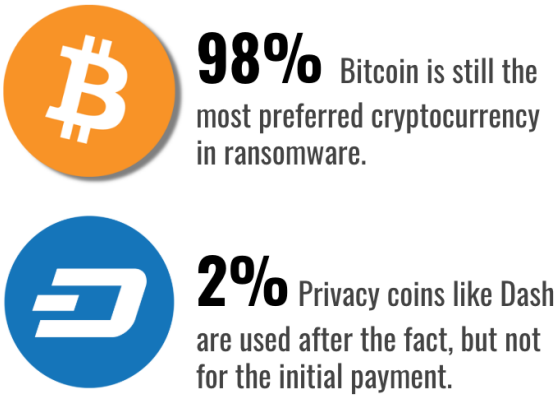

Fig 5.2: Famous Payment type as Ransome

"Bitcoin" keeps on being the most widely recognized 'Crypto-Currency' for ransomware payment and dealing with 'Crypto-currency' kept on being a significant source of friction for threat actors as well as for the victims of ransomware. Bitcoin has become an inextricable part of the ransomware model. Bitcoin transactions are publicly documented in the' Block-Chain', which allows cybercriminals to verify that a payment has been made. Bitcoin isn't the most private 'Crypto-Currency', but mixer and tumbler services allow criminals to essentially launder ransom payments and keep their identities hidden. "Gandcrab" is the main basic kind of ransomware that acknowledges payments in either "Dash" or "Bitcoin". The victims of "Gandcrab" who pay with Bitcoin are charged 10% further because of the blending expenses acquired by the threat actors to anonymize the bitcoin after payment of ransom.

VI. CONCLUSION

In this particular article, we discussed the exponential increase of 'Ransomware-Attack(s)' around the globe. Every single 'Ransomware–Attack' has a distinct nature but the goal is the same almost i.e. ransom money. Since from last decade onward millions of systems influenced by the ransomware due to the lack of awareness among society (also among IT Experts). Various types of ransomware are discussed in the article along with the different techniques which it uses for altering/corrupting the data/resources. Encryption-Algorithms (i.e. whether Public-Key/Single-Key) are used by different ransomware for encrypting the confidential information. Awareness about 'Ransomware' is also required & some of the mitigation techniques are also gone through.

REFERENCES

1. Stephen Cobb, 'Ransomware: An Enterprise Perspective', November 2018.
2. Nolen Scaife, 'Cryptolock (And Drop It): Stopping Ransomware Attacks On User Data', '2016 Ieee 36th International Conference On Distributed Computing Systems', 2016.
3. Azad Ali, 'Ransomware: A Research And A Personal Case Study Of Dealing With This Nasty Malware', 'Issues In Information System', Vol.14, 2017.
4. Abdulrahman Alzahrani, 'An Overview Of Ransomware In The windows Platform', '2017 International Conference On Computational Science And Computational Intelligence', December 2017.
5. Jagmeet Singh Aidan, 'Comprehensive Survey On Petya Ransomware Attack', '2017 International Conference On Next Generation Computing And Information Systems (Icngcis)', December 2018.
6. Amin Kharraz, 'Protecting Against Ransomware: A New Line Of Research Or Restating Classic Ideas?', 'Ieee Security & Privacy', 2018.
7. Sharma Divya Mukesh, 'An Analysis Technique To Detect Ransomware Threat', '2018 International Conference On Computer Communication And Informatics (Iccci -2018)', Jan. 04 – 06, 2018, Coimbatore, India.
8. Bathiya Lokuketagoda, 'R - Killer: An Email Based Ransomware Protection Tool', 'The 13th International Conference On Computer Science & Education (Iccse 2018)', August 8-11, 2018, Colombo, Sri Lanka.
9. Ana Ferreira, 'Why Ransomware Needs A Human Touch', '2018 International Carnahan Conference On Security Technology (Iccst).
10. Nurfadilah Ariffin, 'A Conceptual Scheme For Ransomware Background Knowledge Construction', '2018 Cyber Resilience Conference (Crc)', 2018.
11. Arvind, 'A Comprehensive Study On Digital- Signatures With Hash Functions', 'International Journal Of Computer Sciences And Engineering', Vol. 07, Issue-4, April 2019.
12. Arvind, 'Cryptography & Network Security Hash Function Applications, Attacks And Advances: A Review', Ieee, '3rd International Conference On Inventive Systems And Control (Icisc 2019), 10-11 January, 2019, Pg. 177-188.
13. Https://Www.Beckershospitalreview.Com/Healthcare-Information-Technology/First-Known-Ransomware-Attack-In-1989-Also-Targeted-Healthcare.Html
14. Https://Phoenixnap.Com/Blog/Ransomware-Statistics-Facts
15. Https://Www.Trendmicro.Com/Vinfo/Us/Security/News/Cybercrime-And-Digital-Threats/Blacktds-Traffic-Distribution-System-For-Malware-Offered-As-A-Service-In-The-Dark-Web
16. Https://Www.Coveware.Com/Blog/2019/4/15/Ransom-Amounts-Rise-90-In-Q1-As-Ryuk-Ransomware-Increases
17. Https://Blog.Malwarebytes.Com/Threat-Analysis/2019/05/Threat-Spotlight-Crysis-Aka-Dharma-Ransomware-Causing-A-Crisis-For-Businesses/
18. Https://Research.Checkpoint.Com/Ryuk-Ransomware-Targeted-Campaign-Break/
19. Https://Www.Malwarebytes.Com/Gandcrab/
20. Https://Securelist.Com/It-Threat-Evolution-Q1-2019-Statistics/90916/
21. https://www.securityfocus.com/columnists/102
22. Https://Www.Tripwire.Com/State-Of-Security/Security-Data-Protection/Ransomware-Service-Raas-Works/
23. Https://Healthitsecurity.Com/News/Ransomware-Costs-On-The-Rise-Causes-Nearly-10-Days-Of-Downtime/
24. William Stallings "Cryptography And Network Security Principles", 5th Edition.
25. Forouzan, "Data Communication And Networking", 4th Edition, Mcgraw Hill.

AUTHOR PROFILE

Cyrus Mehra presently pursuing a Bachelor of Computer Application Degree from Maharishi Markandeshwar (Deemed to be University), His area of interest is Cyber-Security, Penetration Testing and Networking.

Arvind K. Sharma working as Assistant Professor in Department of "MMICT&BM (MCA)" M.M. University, Mullana, Ambala (Haryana). Previously he worked for Chandigarh University (CU) in the Department of CSE, Mohali (Punjab). He is pursuing his Ph.D. from Rayat Bahra University, Mohali in the field of CSE in the Networking and Security branch. He has received his M.Tech. CSE Degree from Lovely Professional University, Phagwara in 2015 and, MSc. Computer Science Degree from Guru Nanak Dev University, Amritsar in 2011. His Area of Interest is "Networking and Security", "Routing & Switching", "Programming", "R-DBMS".

Dr. Avinash Sharma Presently Professor, in Maharishi Markandeshwar Engineering College, Mullana, Ambala (Haryana) Constituent institution of Maharishi Markandeshwar University, Mullana is NAAC accredited 'A' grade deemed university.
Also Dean Faculty of Engineering and Technology & Member of Board of Studies & DRC Committee for Researched-Principal & Professor, Rajasthan College of Engineering for Women. Publications: International Journals: Published: 45 (Accepted: 61);International Conferences: Published: 90 (Accepted: 102) National Conferences & Workshops:75 (Accepted: 110 & more)Text Books/EDITED: 06. Total Experience: 20 years (10 years PG) + 03 years Research International Conferences Organized:10. Approximate 20 years of rich experience in Teaching, research, and industry managing technical institution. Played leading role in accreditation of the institution and ISO 9001:2000 certification. (including05 years of industrial/research experience).