Ransomware threat and its impact on SCADA

Usman Javed Butt
Electonic and Computer Engineering
Brunel University
London, UK
usman.butt@brunel.ac.uk

Maysam Abbod
Electronic and Computer Engineering
Brunel University
London, UK
maysam.abbod@brunel.ac.uk

Anzor Lors
Engineering & Environment
Northumbria University
London, UK
anzor.lors@northumbria.ac.uk

Hamid Jahankhani
Engineering & Environment
Northumbria University
London, UK
hamid.jahankhani@brunel.ac.uk

Arshad Jamal
Engineering & Environment
Northumbria University
London, UK
arshad.jamal@northumbria.ac.uk

Arvind Kumar
Engineering & Environment
Northumbria University
London, UK
arvind.kumar@northumbria.ac.uk

Abstract Modern cybercrimes have exponentially grown over the last one decade. Ransomware is one of the types of malware which is the result of sophisticated attempt to compromise the modern computer systems. The governments and large corporations are investing heavily to combat this cyber threat against their critical infrastructure. It has been observed that over the last few years that Industrial Control Systems (ICS) have become the main target of Ransomware due to the sensitive operations involved in the day to day processes of these industries. As the technology is evolving, more and more traditional industrial systems are replaced with advanced industry methods involving advanced technologies such as Internet of Things (IoT). These technology shift help improve business productivity and keep the company's global competitive in an overflowing competitive market. However, the systems involved need secure measures to protect integrity and availability which will help avoid any malfunctioning to their operations due to the cyber-attacks. There have been several cyber-attack incidents on healthcare, pharmaceutical, water cleaning and energy sector. These ICS's are operated by remote control facilities and variety of other devices such as programmable logic controllers (PLC) and sensors to make a network. Cyber criminals are exploring vulnerabilities in the design of these ICS's to take the command and control of these systems and disrupt daily operations until ransomware is paid. This paper will provide critical analysis of the impact of Ransomware threat on SCADA systems.

.

Keywords *Ransomware, Ransomware Attack, Industrial Control Systems, Supervisory Control and Data Acquisition, Cybersecurity, Information Security, Cyber Attack, Operation Technology, Malware, Malicious Software, Cryptor, Locker, Encrypting, Network, Ransom, WannaCry, Petya, Cyber Actor, Data Extortion, Device Compromising, Infected System, Data Backup, Downtime, Data Mitigation, Ransomware Threating, Cryptojacking, Cryptocurrency, Coin Miner, Threat Report, Industrial Control, Data and System Access, Cyber threat, Cybercriminals, Ransomware Prevention, Human Machine Interface, Programmable Logic Controllers, Remote Terminal Units, Industrial Processes, Ransomware Deadline, Ransomware Strategies, Ransomware Taxonomy, Ransomware Incidents, Industrial Networks.*

I. Introduction

Since information technology integration and networking became more affordable and available around the world, industrial companies found means of cost savings by connecting facilities together and controlling distributed systems from a single control center. There are numbers of increasingly diverse and extensively connected set of technologies controlling significant parts of the global process within different sectors such as; pharmaceutical, electrical grid, oil refineries and pipelines, food manufacturing and modern rail systems used for logistics and public transportation every day. All these divisions of the advanced control technologies are represented by Industrial Control Systems (ICS). This includes components, which allow them to increase their efficiency, accountability, and safety (SCADA, distributed control systems and programmable logic controllers). But at the same time, due to vulnerabilities in their security design, these systems are also prone to breaches. [1] While the components of the ICS's are heterogeneously connected, it means more efforts are required to ensure that there is an efficient and secure communication between these components. Unfortunately, due to the complexity of its design and lack for security framework, these critical systems are prone to cyber-attacks [2].

Nowadays, due to the ease of knowing the vulnerabilities of the security module in any ICS whether connected via internet or local control units, it is getting easier for the potential attackers to intrude and take down the operations of an entire system [3].

The cyber threats that industrial control system's operators face today are more challenging than ever before since the volume, types, and severity of cyber-attacks against ICS are rapidly increasing [4]. Operators across a range of industries disclosed that cyber intrusions in their networks had physically disrupted, and in some cases destroyed their systems. Cybercriminals expanded tactics and developed novel techniques for profiting off operational technology (OT) breaches, including selling access to supervisory control and data acquisition (SCADA) networks and targeting ICS operators with malicious software (e.g. Ransomware) [5].

This paper provides an overview of the recent Ransomware Attacks towards the diverse uses of SCADA (ICS) systems in different industries. Observing incidents, variations of methods and its impacts complement the overview of events. Assessments on trends in targeting, threating or hacking tactics of the infamous types of ransomware attacks is covered in methodology part. To support methodologies there is data analysis part which includes recent reports and tables/charts. It will allow to analyze what in common malicious software has and what would be reasonable steps to avoid (prevent) the cyber threat.

II. The Nature of Ransomware

Today cyber security specialists determine the definition of Ransomware as a type of malware which is used to deny access to entire systems or database. A former hacker and now a cybersecurity consultant, Pierluigi Paganini [6] reports:

"..it is a type of malware that infects computers and encrypts their content with strong encryption algorithms..",

Afterwards it requires the victim to pay a ransom in order to decrypt the data (also called "demand a ransom"). The victims are threatened to pay the ransom, otherwise the hacker or cyber actor owning the access, will intend to corrupt or delete the encrypted files. Usually, the infected system shared storage drives with data. As noted by FBI government cybersecurity resource [7], in most cases if the ransom is not sent, the system or encrypted files remain with no access or get lost as the worst-case scenario.

Experts from Kaspersky Lab define Ransomware in two forms [5]. The most likely to witness is the crypto ransomware. The purpose of a crypto ransomware is to encrypt data on the victim's device and hold it until the ransom is received. Another form of ransomware attack is locker ransomware which infects the system and blocks access of user to the data with no impact on the stored files. The demand is usually displayed across the whole screen predominantly mimicking the government style with report of illegal web content detection and spot-fine requirements [8]. As the payment method cyber criminals demand a certain sum in cryptocurrency for privacy and lose the trace once the ransom attack completed [9].

The reports [10], [5] state that in the last year during the first and the third quarter attacks on individuals increased from 20 to 10 seconds while on business the threat rate changed from 2 minutes to 40 seconds. Most of the business attacks were aimed on ICS. In addition, 20% of the business organization who paid the ransom never got the encrypted files back [5]. Kaspersky Lab states that according to the collected data, 0.5% of computers involved into ICS were attacked by encryption at least once in the first quarter of 2017 (Fig. 1)

Rank	**Country**	**% of systems attacked**
1	Ukraine	1.33
2	Malaysia	1.31
3	Denmark	1.12
4	Korea	1.06
5	Turkey	0.88
6	Brazil	0.85
7	Russia	0.8
8	Romania	0.67
9	Iran	0.65
10	Austria	0.65

Figure 1 Countries based on the percentage of ICS computers attacked by encryption malware

Another report from Symantec states that the total amount infected and protected devices increased from 340,000 in 2015 to 463,000 in 2016 [11]. The energy sector, specifically, is increasing its vulnerability to cyber threats such as Ransomware which is a growing method of attack amongst hackers and cyber criminals due to the inventions of different approaches to encryption [12]. According to Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) 2015, there are more incidents in critical manufacturing than in the energy sector in United States [13].

Out of 295 total incidents reported as primary target incidents in USA, the report suggests that 98 incidents included industries such as communication sector, commercial facilities, chemical and healthcare (Fig 2).

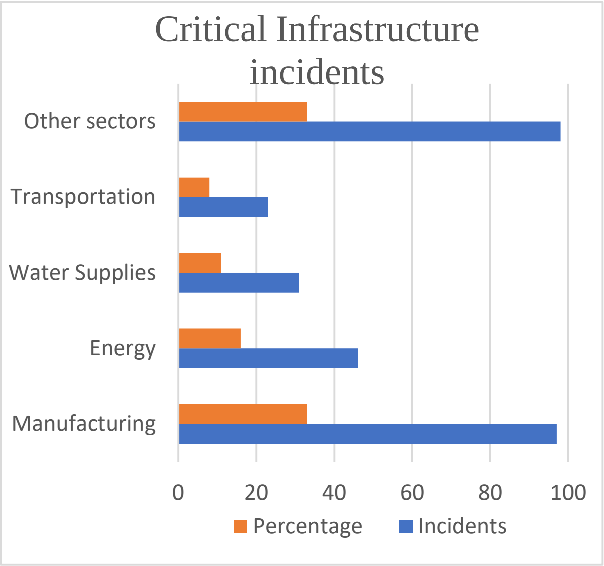

Figure 2 Reported incidents in US

Symantec 2018 [14] and Trend Labs 2016 [15] reported continuous in Ransomware threats to industrial control systems. Around 350 new ransomware families have been discovered and the its vector of spreading has increased phenomenally (Fig 3). On the other hand, the depth of damage on industries that could be done by those malware families is also sufficient because the victims had the quickest way to retrieve critical files. For example, FBI revealed the Hollywood Presbyterian Medical Centre, the University of Calgary and the Horry Country School had been threatened to delete several valuable files and database [15].

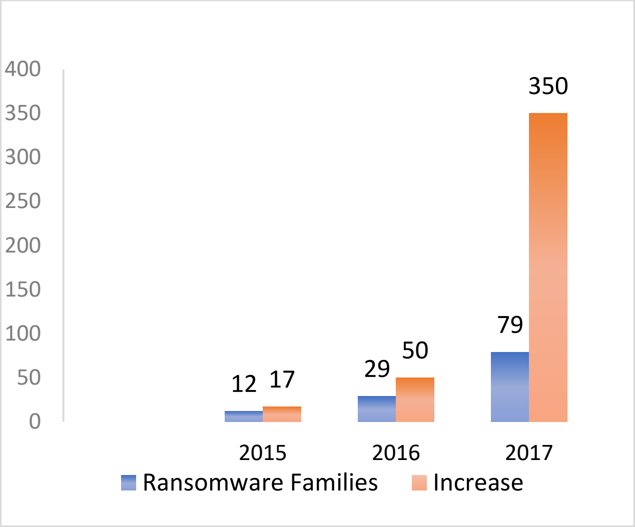

Figure 3 Number of newly added ransomware families

III. Recent Ransomware attacks

The malicious software demanding some ransom had a long-standing origin but to introduce the ransomware form of threat it is sufficient to start with the most recent incidents. There were numbers of Ransomware cyber threats that were revealed in the last two-three years. Those include the ICS targeted attacks as well. All of the following incidents are taken from recent reports of information security organizations such as Kaspersky Lab, Symantec, Dragos etc.

Back in 2015, a backdoor Trojan software named “Duuzer” was detected in South Korean manufacturing organizations. The malware was used to steal valuable data and demand a ransom from the most ***electronic manufacturing companies*** which apparently were headquartered in the same country [15]. In May 2016, the victim of multiple ransomware threats was a hospital located in Kansas. A software has been identified as the Samsam malware. Although the ransom was sent by the hospital, the cyber actors did not return full access to the data. The attackers demand another sum to pay, which made the hospital to refuse for the new payment. The report has not clearly identified whether the hospital sorted out the attack with mitigation or was given the decryption key [16].

Another attack on healthcare sector was on March 29, 2016. The Washington Post reported there were over 250 outpatient centers across 10 hospitals which were forced to shut down their computer systems. There were important data such as patient history prescription, etc. which went missing after the attack. As a result, patients were diverted to other medical centers and rescheduled their appointments [17]. Similarly, there was another threat in 2016, when attackers encrypted the email and patient logs at a hospital based in California. There was an initial ransom of $3 million, but after negotiations with the actors it was changed to $17,000 [18].

There was a smaller incident in November 2016 that happened at Municipal transit system in San Francisco overtaken by malware with a ransom demand amounting to $70,000. It took a few days to repair the system [19].

Cybercriminals add new techniques and tricks to convince users to pay the ransom. As it is reported a ransomware called JIGSAW applied threatening trick to get ransom by deleting data for every hour [20]. On the other hand, in the same year another malicious software - SURPRISE - threatened by increasing the ransom if it is not sent by the deadline [21]. If the target is enterprise machines and endpoints, for example, servers; cybercriminals would rather build more sophisticated ransomware than sending malicious URLs or spam emails. Thus, it was designed and used, for instance CRYPSAM/SAMSAM and ZCRYPT ransomware. The first one was used to get access to unpatched servers due to vulnerability of Java built-in applications [22]. For the case of ZCRYPT, the attack was simply through USB dongles and flash drives/accessories that could be used in any business [23]. The ransomware encrypts the user’s files and change the extension of the malicious software to its marker. It can encrypt almost any format such as .zip, .mp4, .txt, .pdf, etc. The ransom is set around 1.2 BTC that can be increasing once the victim approaches or surpasses the deadline of ransom.

In June 2017 a food production company named Cadbury’s was attacked in Hobart, Australia. As it reports in the Guardian, the ransomware threat OT systems in the factory and it demanded a ransom of $300 in bitcoin. The detected malware was identified as **“Petya”** ransomware. Although it was not a “huge” loss for the company, it has conveyed players in the food industry to manage their security issues [24].

There are incidents towards the ICS that was reported by many Information Security Agencies. For example, the victim of ransomware in 2016 in Michigan became the Landing Board of Water & Light. The network of the company was infected after an employee opened an email with the threat malware. It encrypted the data, forced the computer systems of the BWL to shut down and had a crucial impact on accounting, email and phone communication for the customer support. However, the corporate network was not affected by this incident which means the light and water service was not attacked [25].

The most infamous ransomware incidents that happened across the world in last years were **WannaCry** and **Petya (“notPetya”)** ransomware. On the 27th of June 2017 cyber threat Petya malware that hit computers across the world, causing systems to be infected by encrypting data and demand a ransom. When vast amount of investigations was carried out, it appeared to be comparably similar to the ransomware attack “WannaCry” that the world became aware earlier. The Petya ransomware exploited Windows OS vulnerabilities in the certain protocol (SMB, Server Message Block) alongside with other exploits like harvesting credentials and running utilities remotely. That spread the attack in the networks overwriting the Master Boot Record (MBR). Focusing on the recent WannaCry spread that happened in May 2017, it was noticeable that many victim’s OS were not patched for the SMB vulnerability. Expanding the Petya ransomware attack, it can be noticed that despite the recent incident by WannaCry attack, there were still numbers of systems had the same vulnerabilities not patched [26].

Observing the reports, there are few things that the ransomware attacks have in common:

- The easiest way to infect was email, USB, URL-share by unawareness of employee (social engineering).
- The most widely spread attacks were related to use of operational system vulnerabilities.
- The purpose of the attacks was to get money through means of massive data extortion.

The above-mentioned incidents of ransomware attack have been recorded over the last 2 years which makes researchers to predict that the ransomware type of cyberattack gains momentum and will be one of the main problems in cyber security area.

IV. ICS Ransomware Methodology

Research papers [27], [28], [29] have different approach to describe the ransomware attacking behavior. Focusing on ICS the common steps are the following; initial infection, optional step of movement, locking and encrypting, demanding/negotiation ransom. The basic scenario would be PLC infection on corporate network level which will later on spread onto more PLCs, then harvest the credentials and access control lists/resources. Then comes the encryption step with emailing or sending a ransom note from PLCs.

As shown in figure 4, hybrid encryption technique is used to effectively infect the system and these are the following; RSA 2048bit for the public key and AES 256bit for the user file encryption. After data encryption, the ransomware is expected to encrypt the files by assigning a public-private key for the randomly generated symmetric key.

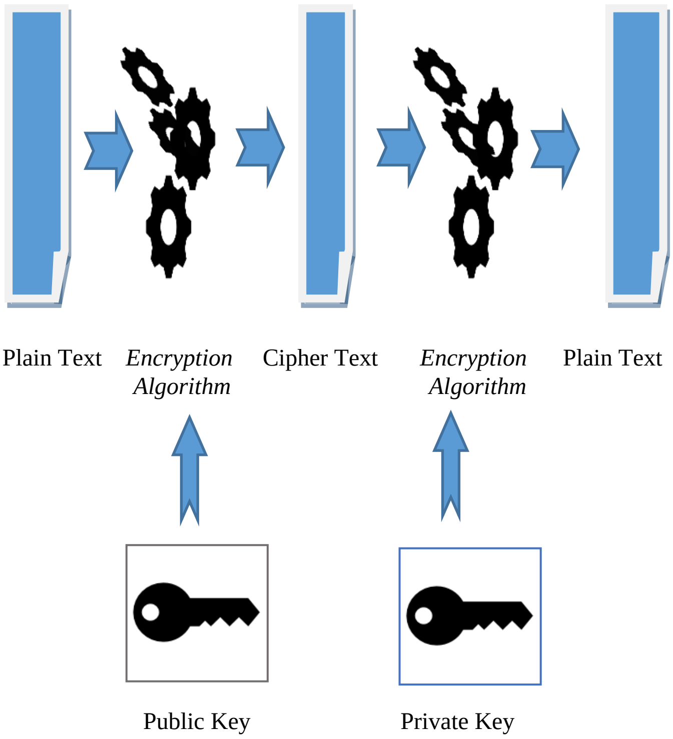

Figure 4: Process of Encryption Used by Ransomware.

Due to the fact that with this encryption method, the attacker manages to keep only a single encryption key, the attack of the ransomware becomes more effective and the user would have difficulty unlocking the ciphered code [30]. An initial infection can be either a direct Internet-facing attack on aimed PLC or a corporate network attack in general ICS flow. The infection by itself is not different from the standard attack method in IT networks with an idea to feasibly compromise a device using its weakness and vulnerabilities and to pivot inside the network for the further steps. The first one covers few devices as maximum and easy to implement using malware directly, while the attack on corporate networks demands more effort and complex strategies because it is targeting a chain of devices and workstation [27].

To make the attack profitable, once an actor get access to the network the actor could infect another PLCs next to the targeted one. Moving throughout the infected network, stepping through levels of an enterprise architecture (the Purdue reference model [31]) is called horizontal and vertical movement. Those can be implemented simultaneously as well as separately.

The horizontal movement implies the infecting devices on Level 1, using PLC as backdoor into internal network. The more devices it compromised the more ransom could be demanded. One of the limitation of the horizontal movement is the fact that it has a low reconnaissance of weakness on the targeted network. If the victim has backup of the compromised device, getting hold of the control over the network becomes more difficult. However, it is known that ICS companies use multiple PLCs of the same model or from the same vendor, which makes it easy for an attacker to hack due to having similar vulnerabilities amongst the devices. In fact, due to the high probability of the similar PLCs the horizontal movement is much more profitable. On the other hand, the vertical movement allows an attacker to survey the valuable data which makes easy to implement the intrusion using a standard malware. Stepping down form the corporate level (level 4) through the control level 3 by aiming HMIs or workstations, it is possible to own the backup copy of device programs and strengthen the control over it. The only setback of this is the length of time for acquisition making it unsuitable for quick-hack scenario.

Once ransomware like WannaCryptor hits an organization with a SCADA network that runs unpatched Windows on its HMI (Human Machine Interface) stations [32], there are three ways the ransomware can damage ICS networks:

- Freeze SCADA configuration and management abilities – HMIs would go into passive mode losing the ability to implement configuration changes.
- Damage HMIs ability to monitor and send commands to the controllers – This wouldn’t actively cause malfunction, but you would lose the ability to detect machinery or controller malfunction and therefore be forced to shut down operations until fixed.
- Paralyze Historian-dependent operations – Historian database servers are used to store all historical controller data from the SCADA network and this data is essential to run processes such as oil refineries. If a ransomware infection locks logs/historian database up with encryption, you may be forced offline until the ransom is paid [33].

Considering above mentioned ransomware attacks, the success of those attacks can be defined through the value of the encrypted data for the company, particularly in case with healthcare, where it contains sensitive information such as patient’s data and history. Regarding to ICS it could be the same reason – some of the encrypted elements are extremely crucial. To be certain, there are number of different elements in network of the ICS and those are the valuable elements in terms of operation continuity and production of manufacture goods [34].

The typical ICS network consists of sensors, PLC (Programmable Logic Controllers), actuators, Remote Terminal Units (RTU) and Wi-Fi networks. Depending on the network design patterns, those elements are connected to the Internet which is also an entry point for malicious software into the system. Despite the case, there are a few supervisory capabilities in some network models which maintains the SCADA system to connect to the Internet. If a cyber-actor can go through the supervision network and find out some vulnerabilities, the actor can easily take the network down once proven that there are no preventive measures. Some network types include both corporate and supervisory networks which makes it difficult to infiltrate vulnerabilities and attack the system [27].

In terms of traditional ransomware, a balancing equation of how the ransom is calculated has been formulated [35], [28]. The demanding payment depends on two factors; how valuable the stolen data is and the scope of victims which relates to how easily the ransomware spread through the targeted area. The profit for the attacker according to [28] in overall will be:

$$\text{Profit} = \text{Population} * \text{Value} – \text{Cost}$$

In fact, there are two types of victims on the end of the cyberattack – a typical Internet user; whose valuable data are photos, personal documents which are encrypted after the attack or companies whose data is crucially significant to continue daily operations. The ICS states that cybercriminals usually carry out attacks on “small pool” targets. Every encrypted file will be important which make it easy to attacker to hold a ransom playing with the trade-off equation in his favor [28].

Downtime is the highest value for the regular ICS Company. It can affect catastrophically on profits even more than just loss of local data. For instances, there was an incident with a car manufacturing company making the company lose millions of dollars every hour of downtime. Locking the PLC or any other main elements in ICS could call this downtime affect that in large scale may turn out into huge amount of costs. Furthermore, the more PLCs are attacked, the longer the recovery process is which, in turn, causes more downtime [28].

Another important thing that make ICS ransomware different is the vulnerability on equipment health and human safety. It seems to be the unique characteristics of ICS networks, since the interaction with the physical world (actions on valves, centrifuges, hazardous chemicals, etc). The threatened ICS network can jeopardize not only the operation or the equipment, but also human being’s safety and health. This attack is also called as the “logic bomb” due to its high profitable type of threat that moves the ICS into a vulnerable state, operates the outputs to cause the most damage.

Although ransomware attacks on ICS has just started and has the general principles of running it, it can evolve and go over the standard ransomware attack. It is reported by Raj Samani, chief scientist at McAfee, that cyber actors demonstrate very sophisticated approaches to gain a ransom using innovative tools and tactics [36]. Considering cryptocurrency growth in value, ransomware attacks can be adopted with mining schemes. Hackers take control of victim's systems by popular infecting methods and instead of prompting victims to pay ransom they simply set the infected system to monetize their criminal activity by mining Bitcoin without any third party. This ramification of ransomware is called cryptojacking. Compared to simple ransomware attack it is simpler and more straightforward. It does not demand any middleman or prompting to make payment. The more infected systems are controlled the more "coins" can be obtained. The complex method is difficult to detect which makes it very effective and less risky. Due to unsecured vulnerabilities within ICS devices and the high probability of being infected by an advanced malware, the anatomy of ransomware and its behaviour is developing the approaches and strategies to take control over the ICS flow [37], [36].

V. The defensive strategies for SCADA systems

There is no unique approach and mitigation for ICS/SCADA area, but it may decrease the risks of the fallacy of air-gap security and additional equipment that involved into ICS flow. Defense for the in-depth strategy works for all sectors and the important point for the ICS would be at the endpoint level: periodic password change, particularly default ones; remote control check should be disabled; updating device's firmware; making a reserved store for data. In addition, including new equipment, security features must be ensured. With regards to the network level, segmenting the network (control and IT) and frequently monitoring for suspicious anomalies alongside with active IP control and firewalls would increase the resistance and successful intrusion's probability [29]. Furthermore, if users would be trained and be able to identify suspicious emails with URLs and attachments it may completely reduce the numbers of ransomware attacks. Alternatively, there should be a responsive plan that must be completed if some compromised data or device program is detected – these include backups and the facility/service check.

VI. Ransomware prevention

To protect potential victims against ransomware there are several measures for prevention of the damage from being inflicted in the first place. There are multiple proposed procedures to avoid blackmail and threat from ransomware [38] and these are the following: **Proactive** and **reactive prevention**. The goal of **proactive prevention** is simply to stop the execution coming from the malware. Several preventive procedures to reduce ransomware infection have been proposed by Yung and Young [39]. It includes constraining and monitoring "access to cryptographic tools". These preventive methods did not fit an advanced ransomware. The final countermeasures were to apply a new strategy – NIZK proof employing, involving "the coexistence of both private and public keys" before the encryption stage starts [40].

Another approach was put forward by Luo and Lia [41] and [42]. Proposing a **proactive framework** compounded policy and procedures, control and management, exposure analysis and report, awareness and education. They established the generic way of prevention that can be applied to any sector. The **reactive method of prevention**, aims to mitigate the effect of the attack by restoring the extorted files from backup. To overtake the attack, the victim needs to revert to the previous (or older) version of the files [43]. Although this type can save the data, if the targeted victim is naive and unsophisticated, the user usually does not follow the necessary preventive precautions [44].

VII. Recommendations

A commitment to cyber hygiene and best practices is critical to protecting vulnerable networks. Here are some basic steps to protect a network from ransomware attack:

1. **Backups:** Copy and store on different device the most valuable or critical information. Better if it is stored offline since the main vector of a ransomware attack is through the internet. Checking the ability to revert those backups is also required to ensure the data is not lost.
2. **Risk Estimation:** It is recommended to conduct cybersecurity risk analysis of the organization.
3. **Training staff:** Develop the knowledge and best practices of cyber security elements.
4. Check the vulnerabilities on **patch** updates
5. Check the application "whitelisting". The software that ran on the organization's network must be credited.
6. Plan and exercise the incident response strategy. Depending in what sector of the industry the organization belongs to, it should have the response plan to take procedures if "worst-case" scenarios seem to be witnessed.

7. Business Continuity implies about sustaining the business operations without access to certain systems. It is the main issue when ransomware take down the system and due to downtime effects, the loss triples and lead to inevitable collapse of the business profit.

8. Penetration Testing would be as an additional measure to be ready for ransomware attack

VIII. Conclusion

Cybersecurity nowadays, faces various type of risk coming mostly from deliberately performed malware and attacks. There are numerous incidents of cyber threat so far and it has started affecting more vital areas such as medicine, energy etc. The recent infamous type of cyber threat – ransomware – is targeting different areas because it is sophisticated and is an untraceable way to get “easy” money via compromising devices and extorting multimillion budget organizations. The risk for the safe and reliable operation of industrial control systems have never been greater. While numerous incidental infections occur in industrial networks on a regular basis, ICS-specific or ICS-tailored malware is rare. However, the recent reports clearly suggest that this sector will be a priority for cybercriminal very soon. Current activity of ICS intrusions is not high/critical enough to state this sector suffers from ransomware but once it “hop on trends” it would be a globally accomplished industry under major threat of losing millions of profits.

Hackers have already begun to shift focus on industries using ransomware type of attack. Having access to industrial buildings and processes, cyber attackers could become more dangerous due to the downtime they may inflict on the businesses which in turn, may impact to vital process and human safety of the companies. Information security around the world is not strong enough to handle this malware if infection of ransomware spread massively across the globe. The best example of it is WannaCry and Petya ransomware that has been attacking globally and was only stopped after numerous times of trials by cyber security specialists. Even though there are many “white” hackers managing to eradicate these malwares, it would still be evolving due to its complexity and its sophisticated implementation. However, researching the taxonomy and strategies it is still possible to apply defensive and preventive countermeasures and move one step forward.

References

[1] J. M. Kevin Finnan, "Cyber Security for Pipelines Other SCADA Systems," 2015. [Online]. Available: https://web-material3.yokogawa.com/2017-09-2253+Cyber+Security+for+Pipelines_Other+SCADA+Systems.pdf.

[2] M. Robinson, "The SCADA Threat Landscape," in Celtics Spings, Newport, Celtics Spings, 2013.

[3] Wolfgang Schwab, Mathieu Poujol, "The State of Industrial Cybersecuity 2018," Trend Study Kaspersky Reports, p. 33, 2018.

[4] Dale Peterson, Ransomware in ICS/SCADA ... It's Happening and Predictions, 2016.

[5] Kaspersky Lab, "The Ransomware revolution," 2016. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07182404/KSB2016_Story_of_the_Year_ENG.pdf. [Accessed 2018].

[6] P. Paganini, "ClearEnergy ransomware aim to destroy process automation logics in critical infrastructure, SCADA and industrial control systems," 5 April 2017. [Online]. Available: https://securityaffairs.co/wordpress/57731/malware/clearenergy-ransomware-scada.html. [Accessed 2018].

[7] FBI.GOV, "Ransomware. What it is and What to do about it.," 2017. [Online]. Available: https://www.justice.gov/criminal-ccips/file/872766/download.

[8] Kaspersky Lab, "Infographic: What you need to know about ransomware," 25 October 2016. [Online]. Available: https://www.kaspersky.com/blog/ransomware-infographics/13315/.

[9] Homeland Security, "RANSOMWARE: GOALS OF MALICIOUS ACTORS AND," 2 June 2017. [Online]. Available: https://content.govdelivery.com/attachments/USDHSCIKR/2017/06/02/file_attachments/825938/OCIA%2B-%2BRansomware_Goals%2Bof%2BMalicious%2BActors%2Band%2BCurrent%2BSystem%2BVulnerabilities%2B%2528FOUO%2529.pdf.

[10] Sentinel One, "SentinelOne: Global Ransomware Study 2," 2017. [Online]. Available: https://go.sentinelone.com/rs/327-mnm-087/images/ransomware%20research%20data%20summary%202018.pdf.

[11] Booz Allen Hamilton, Inc. , "Industrial Cybersecurity Threat Briefing," 2016. [Online]. Available: https://web.kamihq.com/web/viewer.html?file=https%3A%2F%2Fcdn2.hubspot.net%2Fhubfs%2F407136%2FPDFs%2FBooz_Allen%2FIndustrial_Cybersecurity_Threat_Briefing.pdf%3Ft%3D1473881858278&source=extension_open_button. [Accessed 2017].

[12] Symantec Corporation, "Internet Security Threat Report," Symantec Security Threat Report, vol. 22, no. April 2017, 2017.

[13] RSA GROUP, "Future Impacts," 1 November 2016. [Online]. Available: www.rsagroup.com/ media/1911/rsa-future-impacts-researchfindings-30-november-2016.pdf.. [Accessed 1 September 2017].

[14] TrendLabs, Trend Micro, Inc, "The Reign of Ransomware," 2016. [Online]. Available: https://documents.trendmicro.com/assets/rpt/rpt-the-reign-of-ransomware.pdf.

[15] L. Constantin, "S. Korean manufacturing industry targeted with new backdoor program," Computer World, 2015.

[16] Trend Micro, "Kansas Hospital Hit by Ransomware, Extorted Twice," Security News, 2016.

[17] W. J. W. Cox, "“MedStar Health turns away patients after likely ransomware cyberattack," Washington Post, 25 May 2016.

[18] R. Winton, "“Hollywood Hospital pays $17,000 in bitcoin to hackers; FBI investigating," L.A Times, 2016.

[19] T. Fox-Brewster, "Ransomware crroks demand $70,000 after hacking San-Francisco's transport system," Forbes, 2016.

[20] J. Sumalapao, "New Crypto-Ransomware JIGSAW Plays Nasty Games," TrendLabs Security Intelligence Blog, 2016.

[21] Trend Micro, "RANSOM_SURPRISE," Trend Micro Threat Encyclopedia, 2016.

[22] Trend MIiro, "The Rise of SAMSAM Crypto-Ransomware," A Lesson on Patching, 2016.

[23] Trend Micro, "ZCRYPT Crypto-ransomware Attacks Windows 7 and Later, Scraps Backward Compatibility," TrendLabs Security Intelligence Blog, 2016.

[24] The Guardian, "Cadbury's factory cyberattack," The Guardian, 2017.

[25] C. Budd, "Ransomware's newest target: The electric grid," Trend Micro, 2016.

[26] Emerson, "“PETYA” RANSOMWARE CYBER-THREAT," 28 July 2017. [Online]. Available: https://www.emerson.com/documents/automation/openenterprise-security-notification-petya-ransonware-cyber-threat-recommended-actions-en-1060762.pdf.

[27] Z. W. H. C. Aaron Zimba, "Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems," 3 November 2017. [Online]. Available: file:///U:/Download%20Files/1-s2.0-S2405959517303302-main.pdf. [Accessed 10 September 2018].

[28] S. D. R. B. David Formby, "Out of Control: Ransomware for Industrial Control Systems," Fortiphyd Logic, p. 8, 2017.

[29] M. A. M. S. Z. M. S. Bander Ali Saleh Al-rimy, "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions," Science Direct, 2017.

[30] Emsisoft, "Spotlight on ransomware: Ransomware encryption methods," 2018. [Online]. Available: https://blog.emsisoft.com/en/27649/ransomware-encryption-methods/. [Accessed 9 October 2018].

[31] D. Lindskog and M. P. Zavarskya, "Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization," Procedia Computer Science, vol. 2016, no. 94, pp. 465-472, 2016.

[32] Securonix Threat Research Team, "Grandcrab Ransomware Attack," Securonix , USA, 2018.

[33] T. Williams, "The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation," 1992.

[34] C. Forrest, "Report: Manufacturing industry most susceptible to ICS cyberthreats," TechRepublic, 2017.

[35] D. Cohen-Sason, "Ransomware a real risk for SCADA networks," CyberBIT, 2017.

[36] L. Obbayi, "Eye on SCADA," 21 August 2017. [Online]. Available: https://blog.jighi.com/wp-content/uploads/2017/08/SCADA-Systems.pdf. [Accessed 2018].

[37] D. Bisson, "Half of american ransomware victims have paid the ransom," TripWire , 2017.

[38] S. G. Raj Samani, "McAfee Labs Threats Report," McAfee Report, p. 27, June 2018.

[39] HackersEnigma, "McAfee Labs Threats Report – June 2018," McAfee Labs, 2018.

[40] L. Bridges, "The changing face of malware," Network Security, vol. 1, no. 1, pp. 17-21, 2008.

[41] M. Y. A. Young, "Cryptography as an attack technology: proving the RSA/factoring kleprographic attack," The new codebreakers, pp. 243-55, 2016.

[42] S. Z. F. M. N. Andronio, "Helldroid: dissecting and detecting mobile ransomware," Research in Attacks, Intrusions, and Defenses, RAID, vol. 4, no. 94, pp. 382-404, 2015.

[43] Q. L. X. Luo, "Awareness Education as the key to ransomware prevention," Information security, vol. 4, no. 16, pp. 195-202, 2008.

[44] Q. L. X. Luo, "Ransomware: a new cyber hijacking threat to enterprises," Handbook research on information security and assurance, vol. 1, no. 1, pp. 1-6, 2008.

[45] N. K. W. W. S. Zeadally, "Efficient and anonymous mobileuser authentification protocol using self-certified public key cryptography for ,ulto-server architectures," IEEE Trans Information Fornsic Security, vol. 9, no. 11, p. 64, 2016.

[46] H. C. P. T. K. B. N. Scaife, "Stopping ransomware attacks on user data," Cryptolock, 2016.