A Survey of Ransomware as a Service (RaaS) and Methods to Mitigate the Attack

Ali Ahmed Mohammed Ali Alwashali
School of Technology
Asia Pacific University
Technology Park Malaysia, Bukit Jalil
Kuala Lumpur, Malaysia
TP062148@mail.apu.edu.my

Nor Azlina Abd Rahman
Forensic and Cyber Security Research Centre
Asia Pacific University
Technology Park Malaysia, Bukit Jalil
Kuala Lumpur, Malaysia
nor_azlina@apu.edu.my

Noris Ismail
School of Technology
Asia Pacific University
Technology Park Malaysia, Bukit Jalil
Kuala Lumpur, Malaysia
noris.ismail@apu.edu.my

2021 14th International Conference on Developments in eSystems Engineering (DeSE) | 978-1-6654-0888-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/DESE54285.2021.9719456

***Abstract* - Industries all around the world seek realistic predictions for new threats that might appear in new future that will affect their business and the security of their data. Year 2020 was full of uncertainty due the Covid19 pandemic, entire world had to change the way they do business by shifting to the digital world. The new working methods introduced new threats which will persist, and potential continue to grow in coming few years. Cyber security predictions address challenges and threats caused by the pandemic such as the huge increase of ransomware attacks in the coming year. Almost every organization changed their option to access work and used new software that will allow them to operate from home. Education sector for example uses virtual classes, healthcare sector use web to deliver and communicate with patients and so on. The more individuals and business rely on technology, the more it becomes part of their lives and cannot be replaced. Cyber criminals realized this fact and increased the demand for higher ransom.**

The goal of this paper is to study the trend and the influence of Ransomware as a service in today era. This paper is proposed steps to reduce the impact of Ransomware attack to individuals and organizations. The discussion on how ransomware as a service work, statistic of ransomware cases, methods of improving operational security of the organizations and technical countermeasures that should be taken by organization and also individuals are included in this research paper.

***Index Terms*— Malware, Ransomware, RaaS, Ransomware Kit, Ransomware Services.**

1. Introduction – Ransomware

Ransomware is a malicious software that if it is run on a system, it will encrypt all the data and preventing the user from using the system. The motivation from the attack is to demand for ransom to return the system back to its normal state or decrypt the files.

The first malware used encryption to block users from working normally on their systems is PC Cyborg in 1980. The malware monitored the infected system for reboot count and encrypt the files in C: drive after 90 reboots, then demanded for license renew. There were few malwares that tried to ask for payments to decrypt the files but overall, encryption and demanding payment was not common due to the money transfer difficulties from 1980 up till digital cryptocurrencies were invented. Bitcoin for example hide the identity of the person and cannot be blocked by any central authority, hence it was the savor for cyber criminals to use it for their illegal activities. Currently, ransomware attacks demand ransom in form of bitcoins [1].

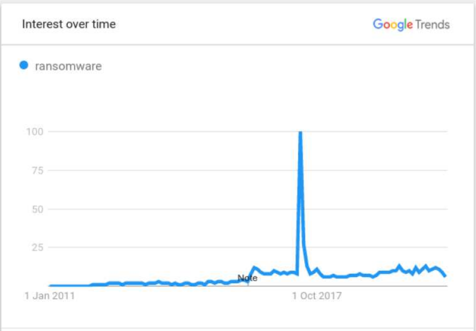


Figure 1: Google Trend for Ransomware Search [11]

The first use of the word ransomware started in 2012 and was in its peak in 2017 when WannaCry ransomware hit business. Figure 1 shows google trending search about ransomware. Ransomware infection is not different from any type of malware, most of the attacks were conducted over spear phishing emails. With the proliferation of Ransomware as a Service (RaaS) platforms, insider threats such as a disgruntled employee or sysadmin can use RaaS services to damage their employee business and gain commission form the ransom.

FireEye report also show that Ransomware as a service will have a tremendous increase in coming years since many businesses adapted the options of remote work [2]. In addition to the emphasis made by FireEye, Verizon company publish a report called 2020 Data breaches investigations report that accurately study cybercrimes from events of previous incidents collected from 81 countries. The report collected 157,525 incidents records. 32,002 met the quality standards put by the company to be used in the study. The data collected from incidents analyzed by Verizon cybersecurity team and by the community through a framework made public for everyone, the framework collects the incidents through a web application [3].

Impact of Ransomware

Chainalysis Insights has published a statistic of total cryptocurrency value received by ransomware from the year 2016 - 2021. The graph in figure 2 has shown that ransomware victims paid over $406 million worth of cryptocurrency to attackers in 2020 and this shows no signs of slowing down nearly five months into 2021 [4].

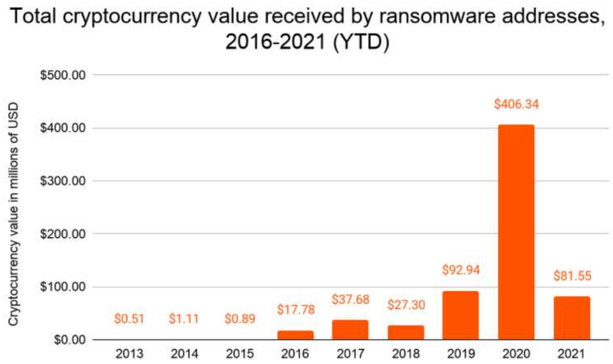


Figure 2: Total Cryptocurrency Value by Ransomware (Ransomware 2021: Critical Mid-year Update [REPORT PREVIEW], 2021). [4].

The high impact is in the spreading capabilities of the malware causing most of the business to be encrypted and blocked from work. For long time FBI rule was not to pay the ransom [5]. Due the high damage to the business, FBI soften their guidelines stating that business owners should study their options in regard paying the ransom [6]. The renowned incidents of WannaCry in May 2017 were the most devastating ransomware malware. It spread over 150 countries. The malware exploited a RCE vulnerability in SMB protocol. The total losses of WannaCry estimated to be $4 billion [7].

2. Ransomware as a service

The academic literature is lacking in the content about ransomware as a service (RaaS), probably because the researchers focus more on the root cause of the problem which ransomware itself as a malware rather than how it was delivered to the target or market trends. Most of the academic papers discussed on the prevention strategies and detection methods for ransomware. The business impact of RaaS services and malware families were found more in reports and blog posts published by cybersecurity companies. Therefore, this paper will focus on how the Ransomware services are provided to the target users.

Ransomware as A Services

The difference between RaaS or any other cybercrime as a service (CaaS) is that ransomware threat actors developed payment systems and technical support platforms for the attacks in case the victim want to discuss the deal for decrypting the data.

How RaaS works?

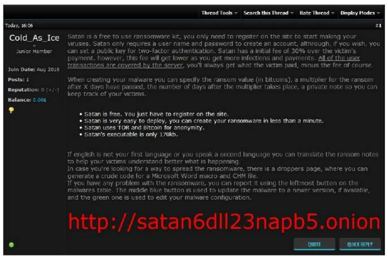
Cyber criminals realize that organizations value their data and intellectual property as much as they value physical property. Cyber-attack including ransomware focus on stealing the data to make profit from extortion. In the past it was not easy for a normal person to perform cybercrimes due to the amount of knowledge it requires to build malware and underlying attack infrastructure. However, currently, there are some attack groups adopted a business model where they can profit from selling malwares to everyone. Either Individual or group buying the ransomware platform (called ransomware kit) or just help spreading the malware and they will get portion of the ransom.

Buying ransomware

There are ransomware platforms available for sale in the dark web. Astonishingly, most of the platforms do not cost much. For example, Stampado's license costs $39 for lifetime license, the same for Cerber, MacRansom and Philadelphia. However, there are other malwares that costs thousands of dollars such as locky ransomware. It depends on the attack target, platform is selected. Most of RaaS operators offer customer service to the malware and help cyber criminals.

Satan Ransomware Kit

Malware kit developers made Satan available to everyone to use for free. They can create their own custom ransomware to fit the target and distribute it in the target network. The platform handles everything from Command-and-control servers (C2 servers) to payment and negotiation. Once the payment is done, developers of the platform cut 30% of the payment and remaining goes to the user [8].



Today, 16:06 #1

Cold_As_Ice
Junior Member

Join Date: Aug 2016
Posts: 1
Reputation: 0 [+/-]
Balance: 0.00$

Satan is a free to use ransomware kit, you only need to register on the site to start making your viruses. Satan only requires a user name and password to create an account, althrough, if you wish, you can set a public key for two-factor authentication. Satan has a initial fee of 30% over the victim's payment, however, this fee will get lower as you get more infections and payments. All of the user transactions are covered by the server, you'll always get what the victim paid, minus the fee of course.

When creating your malware you can specify the ransom value (in bitcoins), a multiplier for the ransom after X days have passed, the number of days after the multiplier takes place, a private note so you can keep track of your victims.

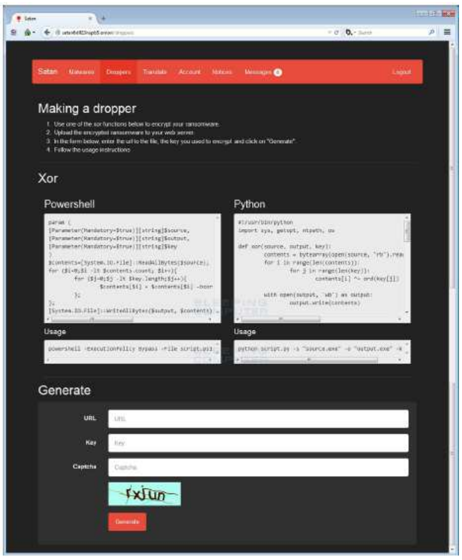
- Satan is free. You just have to register on the site.
- Satan is very easy to deploy, you can create your ransomware in less than a minute.
- Satan uses TOR and Bitcoin for anonymity.
- Satan's executable is only 170kb.

If english is not your first language or you speak a second language you can translate the ransom notes to help your victims understand better what is happening.
In case you're looking for a way to spread the ransomware, there is a droppers page, where you can generate a crude code for a Microsoft Word macro and CHM file.
If you have any problem with the ransomware, you can report it using the leftmost button on the malwares table. The middle blue button is used to update the malware to a newer version, if available, and the green one is used to edit your malware configuration.

http://satan6dll23napb5.onion

Figure 3: Highest Ransomware Payments [8].

The platform is hidden behind tor network. Figure 3 shows the promotion advertisement in one of the underground websites. The following screenshots in figure 4 and figure 5 are used to create a dropper using Powershell and Python. Cyber criminals must copy paste the code and perform the distribution. Such platforms made cybercrimes easy to perform, insider threats now can profit from their revenge against their employees and not just harm them.



Satan
satan6dl23napb5.onion/dropper
Satan Malwares Droppers Translate Account Notices Messages 0 Logout

Making a dropper

1. Use one of the xor functions below to encrypt your ransomware.
2. Upload the encrypted ransomware to your web server.
3. In the form below, enter the url to the file, the key you used to encrypt and click on "Generate".
4. Follow the usage instructions

Xor

Powershell

```
param (
[Parameter(Mandatory=$true)][string]$source,
[Parameter(Mandatory=$true)][string]$output,
[Parameter(Mandatory=$true)][string]$key
)
$contents=[System.IO.File]::ReadAllBytes($source);
for ($i=0;$i -lt $contents.count; $i++){
        for ($j=0;$j -lt $key.length;$j++){
                $contents[$i] = $contents[$i] -bxor
        };
};
[System.IO.File]::WriteAllBytes($output, $contents)
```

Usage

```
powershell -ExecutionPolicy Bypass -File script.ps1
```

Python

```
#!/usr/bin/python
import sys, getopt, ntpath, os

def xor(source, output, key):
        contents = bytearray(open(source, "rb").rea
        for i in range(len(contents)):
                for j in range(len(key)):
                        contents[i] ^= ord(key[j])

        with open(output, 'wb') as output:
                output.write(contents)
```

Usage

```
python script.py -s "source.exe" -o "output.exe" -k
```

Generate

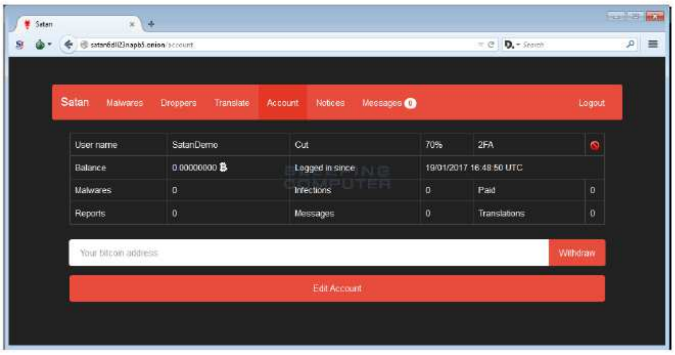
URL: URL

Key: Key

Captcha: Captcha

Figure 4: Custom Malware Page [8].

All payment is done via bitcoin. Users of the platform can follow their payment and how much they made from ransomware distribution.



Satan
satan6dl23napb5.onion/account
Satan Malwares Droppers Translate Account Notices Messages 0 Logout

User name	SatanDemo	Cut	70%	2FA	⊘
Balance	0.00000000 ₿	Logged in since	19/01/2017 16:48:50 UTC		
Malwares	0	Infections	0	Paid	0
Reports	0	Messages	0	Translations	0

Your bitcoin address

Figure 5: Custom Malware Page [8].

3. Methods to Improve Operational Security

Improving operational security to reduce the impact of ransomware mandate taking certain steps that will prevent malwares from propagating across the network. Most of the hardening and prevention tactics address lateral movement techniques. If the network is secured against lateral movements, attackers will find it difficult to move from network to another for manual deployments. Additionally, for the automated deployment, group policy and firewall are used along with endpoint hardening to reduce the likelihood to stop spreading capabilities.

Containment and Prevention Strategies

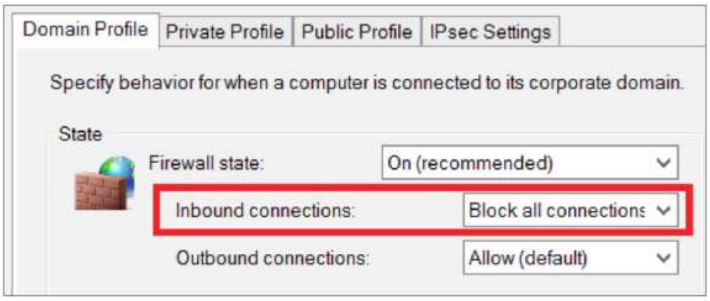
This part presents all the strategies that should be followed by security consultants to stop spread of ransomware. The same can be applied before incidents as a preparation plan [9].

a) Endpoint Hardening

During incidents, attackers leveraged protocols such as SMB, RDP and WMI to move across endpoints.

- SMB Ports: 445, 135, 139
- RDP Ports: 3389
- WMI Ports: 80, 5985, 5986

Endpoint hardening can reduce the spread of ransomware by using group policy to block any communication between workstations. Endpoints will be allowed to communicate with servers but no other endpoints. In addition, users should be prevented from changing windows firewall settings, only group policy or domain administrator account should have the permission to do so.



Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block all connections

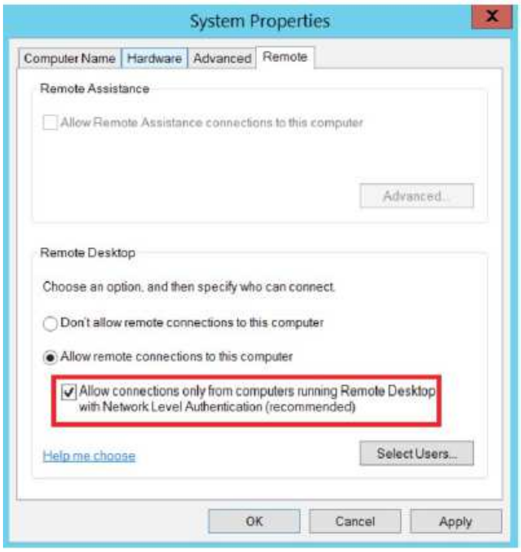
Outbound connections: Allow (default)

Figure 6: Local Firewall Hardening

Endpoint inbound communication should be blocked as shown in figure 6. Inbound communication to any endpoint (non-Server) should be blocked unless there is a business need for that. Windows firewall support options to write custom rules that allow certain port from specific binaries. These options should be utilized to restrict other binaries to receive any inbound communications.

b) Remote Desktop Protocol (RDP) Hardening

If RDP service must be exposed to the internet, multi factor authentication should be used to maximize the security. Enforcing Network level authentication as a second layer of security to connect to RDP as shown in figure 7 and figure 8. Users will be having to tunnel to the network and using network credentials to RDP to the server.



System Properties

Computer Name | Hardware | Advanced | Remote

Remote Assistance

□ Allow Remote Assistance connections to this computer

Advanced...

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

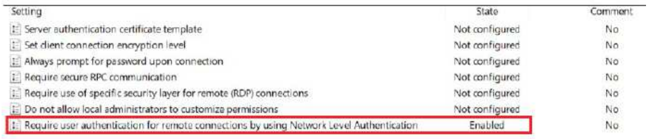
☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Help me choose

Select Users...

OK | Cancel | Apply

Figure 7: Local Firewall Hardening

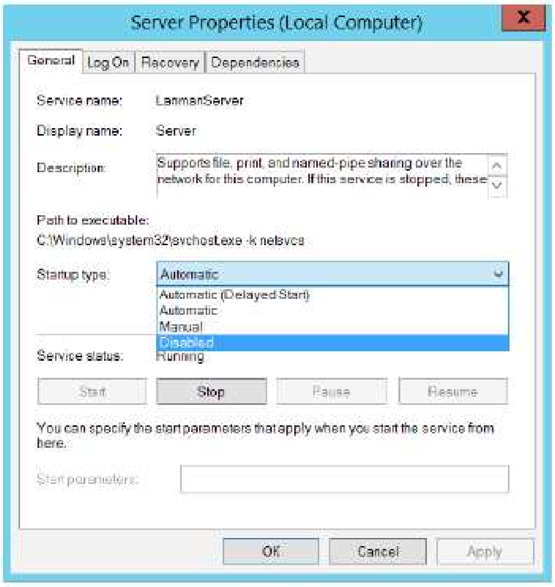


Setting	State	Comment
Server authentication certificate template	Not configured	No
Set dient connection encryption level	Not configured	No
Always prompt for password upon connection	Not configured	No
Require secure RPC communication	Not configured	No
Require use of specific security layer for remote (RDP) connections	Not configured	No
Do not allow local administrators to customize permissions	Not configured	No
Require user authentication for remote connections by using Network Level Authentication	Enabled	No

Figure 8: Enforce LNA Only

c) Disabling Administrative Shares

Administrators may need to disable hidden shares as shown in figure 9. This is because malware may use them to spread and move in the network.



Server Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: LanmanServer

Display name: Server

Description: Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these

Path to executable:
C:\Windows\system32\svchost.exe -k netsvcs

Startup type: Automatic

Automatic (Delayed Start)
Automatic
Manual
Disabled

Service status: Running

Start | Stop | Pause | Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK | Cancel | Apply

Figure 9: Disable Hidden Shares

Other operational security hardening:

- Disabling SMBv1
- Disabling powershell remoting
- Use jump box to access high critical servers
- Randomize local administrator password using LAPS

Incident Response Plan

In addition to the guide published by FireEye in above section, IBM Security team published 46 pages document about ransomware readiness and response, the document contains a playbook step to face and response ransomware attack [10]. The response plan as in figure 10 is in the guide followed the NIST incident response structure.

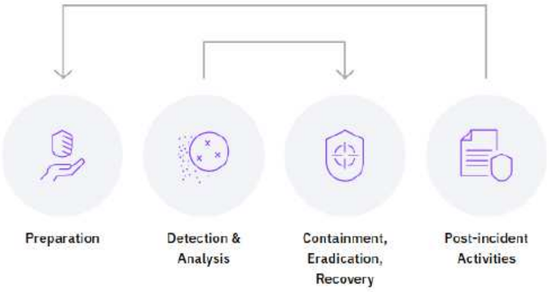


Figure 10: Incident Response Structure

a) Preparation

Organizations should perform the hardening in the above steps mentioned in containment and preventions strategies. In addition, email security hardening and prevention technologies. Email is the attack vector of infection for most of the incidents, hence educating users about spear phishing and deploying sandbox technology is the most important factors for success against ransomware attacks.

b) Detection

Following table summarised the four possible scenarios for ransomware detection. All the scenarios are at endpoint level, neglecting threat intelligence platform and C2 communication if any.

Table 1: Four Possible Scenarios for Ransomware Detection [10].

Scenarios	Detection
Encrypted file over network	User notify IT staff that he is not able to access a file over network because it is encrypted or corrupted
Encrypted local file	User notify IT staff that he is not able to access a file over network because it is encrypted or corrupted
Ransomware message	When entire encryption (infection) process is complete, user will see a message notifying that he has been compromised and need to pay ransom.
Massive file changes	When security staff receive alerts through security controls such as SIEM that massive number of files changed unlike to normal daily operations

c) Analysis And Containment

Security analyst should perform the analysis which starts by identifying the malware and scoping the infection. Malware variant is very important to be identified, there might be chance to find a decryptor or response tactic from community content or threat intelligence platforms.

Scoping the incident can be done over the network or endpoint solutions like EDR. Monitoring the traffic of the infected machine can reveal the IP address or domain name of the infected machine. Then, through SIEM or NSM all devices that already communicated with the C2 server can be enumerated. The same method at endpoint level but with greater flexibility by searching for certain name of file type to be identified across the network. Finally enumerated infected machines should be isolated and backup restoration process should start if the data should be resumed immediately. Root cause analysis as Digital forensics analysis is performed to understand the root cause of the infection and take the necessary steps to patch the vulnerability or harden the weakness in the network security defenses.

d) Recovery

There are incidents where business operation can wait for some time before restoring data from backup, this delay allows security staff perform the analysis and understand the incident better. Later, data can be restored as part of the recovery phase.

Patching the found vulnerability, if the forensics analysis showed that the initial infection was because of unlatched vulnerability. Other scenarios might be because of drive by compromise or phishing email. Regardless the initial infection method, the security staff should take all necessary steps to make sure the same incident does not reoccur again.

4. Conclusion

Ransomware reputation has been well known since the year 2017. All the users are aware on the impact of Ransomware towards the individuals and organizations, but most likely users are not aware of the services to buy the ransomware easily on the net. There are ransomware platforms available for sale in the dark web. Most of RaaS operators offer customer service to the malware and help the cyber criminals too in launching the attack. Since the RaaS are getting popular among all the users, several steps on how to improve the operational security has been explained to reduce the impact of ransomware from propagating across the network.

Today, RaaS are attractive and inherently lure not only the cybercriminals but also to normal users to use their services with minimal fees. For an organization, lack of adequate security, which makes them vulnerable for attackers to launch the ransomware attack to steal private and sensitive information, or to disrupt an individual's smart home or organization environment. Nowadays, individuals and organizations need to be equipped with minimal knowledge on how to secure their environment from being attack by the ransomware malware.

The trend of the ransomware needs to be analysed and understand the pattern of changes that being done. By understanding this pattern several countermeasures can be proposed and awareness can be given to the users so that precaution steps can be taken in protecting their data t be attacked by ransomware.

References

[1]. "Ransomware - What is it & how to remove it?," *Malwarebytes*, 2019 [Online]. Available at: https://www.malwarebytes.com/ransomware/ [Accessed: 15th March 2021]

[2]. "A GLOBAL RESET Cyber Security Predictions 2021," *FireEye* Nov 12, 2020 [online]. Available at: https://www.fireeye.com/blog/executive-perspective/2020/11/a-global-reset-cyber-security-predictions-2021.html [Accessed: 19th March 2021]

[3]. "2021 Data Breach Investigations Report," *Verizon Business*, 2021 [online] Available at: https://enterprise.verizon.com/resources/reports/dbir/. [Accessed: 15th March 2021]

[4]. "Ransomware 2021: Critical Mid-year Update," Blog.chainalysis.com, 2021 [online] Available at: https://blog.chainalysis.com/reports/ransomware-update-may-2021 [Accessed: 15th March 2021]

[5]. "FBI - Ransomware, Federal Bureau of Investigation," FBI, 2016 [online] Available at: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware [Accessed: 15th March 2021]

[6]. "2020 Cyber Security Report," Checkpoint, 2020 [online]. Available at: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf [Accessed: 15th March 2021]

[7]. "What is WannaCry ransomware?," Kaspersky, 2020 [online]. Available at: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry [Accessed: 15th March 2021]

[8]. Abrams, L, "New Satan Ransomware available through a Ransomware as a Service," *Bleeping Computer*, Jan. 19, 2017 [online]. Available at: <https://www.bleepingcomputer.com/news/security/new-satan-ransomware-availablethrough-a-ransomware-as-a-service-/> [Accessed 7 March 2021].

[9]. "Ransomware Protection and Containment Strategies," *FireEye*, 2020 [online]. Available at: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomwareprotection-and-containment-strategies.pdf. [Accessed 7 March 2021].

[10]. "The definitive guide to ransomware: Readiness, response, and remediation," IBM Security - X-force, 2020 [online]. Available at: https://www.ibm.com/downloads/cas/EV6NAQR4 [Accessed: 15th March 2021]

[11]. John Livingston, "5 Steps to Improve Cyber Security Awareness in Manufacturing and OT/ICS," Verve, Oct. 30, 2020 [Online]. Availabe at: https://verveindustrial.com/resources/blog/5-steps-to-improve-cyber-security-awareness-in-manufacturing-and-ot-ics/ [Accessed: 15th March 2021]