Rise of Ransomware and the Readiness of Bangladesh

Samantha Haque[1] and Touhid Bhuiyan[2]

***Abstract*—**Security threats in cyberspace is growing exponentially with the dramatic growth of the use of Internet. Ransomware is special types of malware that usually blocks a user's access to their data or programs by using encoding techniques with a key and allow decode those until a ransom payment is made to cybercriminals. Many of world giant companies rank Ransomware among their top cyber threats for 2016. To achieve the government's goal of Vision 2021, Bangladesh is going forward with digitization of public and private sectors. Like the private services, many of the government services now also available online. The rapid growth of digital contents on cyberspace, without taking proper security measure increases the risk of vulnerability of those sites. Cybercriminal may take these opportunities to collect Ransomware by attacking these vulnerable sites. This paper investigates the global trends of rise of Ransomware and the potential risk of the sites in Bangladesh. Several vulnerability of these sites have been detected and to make the cyberspace of Bangladesh more secure, specific recommendations have been made. The findings of this research will help the government and private sector to understand the level of risk due to these vulnerabilities and will help them to fight against the cybercriminals.

***Keywords*—**Cybercriminal, Ransomware, Security, Vulnerability.

I. INTRODUCTION

SECURITY threats in cyberspace is growing exponentially with the dramatic growth of the use of Internet. Ransomware is special types of malware that usually blocks a user's access to their data or programs by using encoding techniques with a key and allow decode those until a ransom payment is made to cybercriminals. Many of world giant companies rank Ransomware among their top cyber threats for 2016.

To achieve the government's goal of Vision 2021, Bangladesh is going forward with digitization of public and private sectors. Like the private services, many of the government services now also available online. The rapid growth of digital contents on cyberspace, without taking proper security measure increases the risk of vulnerability of those sites. Cybercriminal may take these opportunities to collect Ransomware by attacking these vulnerable sites. This paper investigates the global trends of rise of Ransomware and the potential risk of the sites in Bangladesh. Several vulnerability of these sites have been detected and to make the cyberspace of Bangladesh more secure, specific recommendations have been made. The findings of this research will help the government and private sector to understand the level of risk due to these vulnerabilities and will help them to fight against the cybercriminals [1].

Ransomware is a type of malware that's main determination is simply extortion. It is actually a cyber-security attack and its main objective is to take control of any devices including android mobile, software even Macs as well. It is basically a type of malware that prevents or limits the users from accessing their systems. Here access is regained by paying ransom money to the hackers who have penetrated your device. It works silently by encrypting the files, games, software or any important documents before demanding payment for their return, often with a time limit.

The most common and popular infection method used in Ransomware campaign is spam or phishing emails [2]. It can also be downloaded by visiting malicious or comprised websites and sometimes different attachments to email. The email contains an attached word document which contains a malicious macro. When the user opens the files it becomes encrypted.

Once a file or device or system is encrypted, the victim is shown a ransom note, asking for payment in return for a decryption key to regain access to their files. The users may encounter this threat through a variety of means. However paying for the ransom does not guarantee that users can eventually assess the infected system. When the system is properly executed in Ransomware it can lock the computer screen or encrypt predetermined files with a password [3]. On the very first scenario, there shows a full screen image or notifications which mainly prevent and at the same time make the users understand that they are now under threat. Then it shows some guide lines for paying ransom money to decrypt their affected items. Second type of Ransomware mainly locks the files like documents, spreadsheets and other file types.

II. BACKGROUND

The first Ransomware virus was originated in 1989 by evolutionary biologist Joseph L. Popp and since then named as AID Trojan and later it known as PC Cyborg after 17 years in 2006, the first Ransomware was again distributed by the named Archiveus Trojan which used RSA (Rivest Shamir Adleman) encryption. Near about 30,000 new Ransomware samples detected in each of the first two quarters of 2011 and surprisingly it became double just after third quarter of 2011[4].

In 2012, another toolkit named as Citadel that aims was to

Samantha Haque[1] is a student of the Department of Software Engineering, Daffodil International University, Bangladesh.

Dr. Touhid Bhuiyan[2] is the Head of the Department of Software Engineering, Daffodil International University, Bangladesh.

infect the systems. Cyber criminals then brought a new crime kits named Lyposit that mainly pretends to be a local law enforcement authority and threatens customer by using different laws. Both Citadel and Lyposit's main intention is to take extortion from the users by using different innovative techniques [5].

Banker Trojans were one of the most prominent threats in the cyber world. It was actually a mirror of the bank's website which main intention is to capture user's credentials; however there are some weaknesses over there. It requires the banking malware to keep a live channel during attack and if the command and control server is shutdown during the process, the attacker may not be successful anymore. Even the attacker has some risks during the transaction as it may trigger a silent alert to catch the attacker while withdrawing the funds. Actually the ability to recognize a retrieval or electronic movement of funds that creates a real risk for the attacker [6, 7].

There are many types of Ransomware. For example screen locking Ransomware was first originated in Russia near about 2010. It extended to 2014 until users learned how to get past lock screens by restarting personal computer's in safe mode and then running antivirus software to eliminate the malware. Scareware, another type in comparison to other types of Ransomware, not so scary. Scareware includes rogue security software and tech support scams. You might receive a pop-up message claiming that bajillion pieces of malware were discovered and the only way to get rid of them is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe. A quick scan from your security software should be able to clear out these suckers [8].

'Police Trojan', another common variant of Ransomware aims to tell the victims that they have violated the law by visiting child pornography websites and for this reason they must have to pay a fine to regain their system unlocked.

Another type of locker Ransomware informs the user that they are now using pirated version of windows and demands payment for a legitimate Microsoft license to restore access to the computer [9].

Other well-known variants include Tesla Crypt that's targets gaming PCs. CryptoWall, which spreads via malicious online ads or 'malvertising'; Linux Encoder, which attacks Linux based web servers and keyRanger that infects Macs via a corrupted BitTorrent installer [10].

III. THREATS FOR BANGLADESH

Investigators suspect unknown hackers installed malware in the Bangladesh central bank's computer systems and watched, probably for weeks, for how to go about withdrawing money from its U.S. account, two bank officials briefed on this matter. More than a month after hackers breached Bangladesh Bank's systems and attempted to steal nearly $1 billion from its account at the Federal Reserve Bank of New York, cyber security experts are trying to find out how the hackers got in. FireEye Inc's Mandiant forensics division is helping investigate the cyber heist, which netted hackers more than $80 million before it was uncovered [11].The hackers appeared to have stolen Bangladesh Bank's credentials for the SWIFT messaging system, which banks around the world use for secure financial communication [12]. Like most industries, the cyber threat to the financial sector continues to grow at an unprecedented rate, but the financial industry has a unique factor to consider: this is where the money is. A financial organization of any size is an ideal target for attacks at the hands of any number of malicious actors. Attackers vary widely – from cybercriminals to hacktivism to nation-state-sponsored Advanced Persistent Threat (APT) actors.

Attackers have become more sophisticated in their methods, while still relying on social engineering (primarily phishing campaigns) to gain access, as these methods remain quite effective. Though social engineering remains relatively unsophisticated, detection has grown increasingly complex, and once the financial institution realizes what has happened it's often too late [13].

At the same time, many banks are greatly increasing their attack surfaces, expanding online payment options and mobile apps, thereby opening up new vectors for would-be attackers. Researchers are also noticing a growth in various types of threats over the last several months:

- Increased use of Ransomware.
- Whaling and spear-phishing campaigns, the first step in targeting financial institution employees for Business Email Compromise.
- Targeting banks directly, rather than individual user accounts.
- Accessing systems to alter exchange rates which could lead to a cascade of events affecting global markets.

The use of banking-specific malware like Dridex, as well as repurposing other malware to target financial organizations.

IV. CURRENT SITUATION OF RANSOMWARE IN BANGLADESH

As we know, only few months ago 81M dollar was stolen by the hackers called three boys and the authority could rarely get back a bit of that which was a big loss for our country's economy. Only this one hacking from our national bank our national bank shows the situation of our cyber security whereas we are trying to make our country a digital country.

It seems like we are making a big house without a door from where anyone can come from outside can steal all our important things. An accident like this has become very common in abroad but it was the first time our country got attacked. As our present situation of our cyber communication based economy is just like a growing child and that little attack even was a deep wound on our backbone. We all need be more and more aware about the security because how rich we are doesn't matter if we cannot secure our assets.

Under this circumstances do we think, is our country prepared for a Ransomware attack? Ransomware has become the most unhealthy threat in cyber world and till 2015 the amount of lose for Ransomware was 24.1M.and FBI estimates that the loses for Ransomware will touch 1 billion in 2016

what is a bloodcurdling news for the whole world.so according to this survey we can undoubtedly say that Ransomware in also knocking our door. If once it starts in our country it will get viral which can be a big disaster for our economy. So it's better to take precaution before getting attacked [14].

The good news for us is till now we didn't have heard any demand from hacker but we don't have enough time to make our shield strong steadily.

V. How Does It Work

In the first life of ransomware it was only about the PC from where all the data had got encrypted or locked .as a result the user couldn't be able to use his important stuffs. Then the criminals started to hack peoples phone, servers and other internet based connections also.in some cases the cybercriminals can be able to take under control an entire office or all the machines of a house. The cost of attackers differs of each according to importance. Although there have been a handful of high profile arrests in the Netherlands, Spain and the UK and US. They always try to play a very safe game and high prosecution [15, 16].

There has same specific phases of ransomware attack. "understanding what happens to each phase and knowing the indicators of compromise to look for, increases the likelihood of being able to successfully defend against or at least mitigate the effects of-an attack," says Sommers [17].

The phases are

- Exploitation and infect
- Delivery and execution
- Backup spoliation
- File encryption
- User notification and clean up.

Here is a diagram of the method of Ransomware:

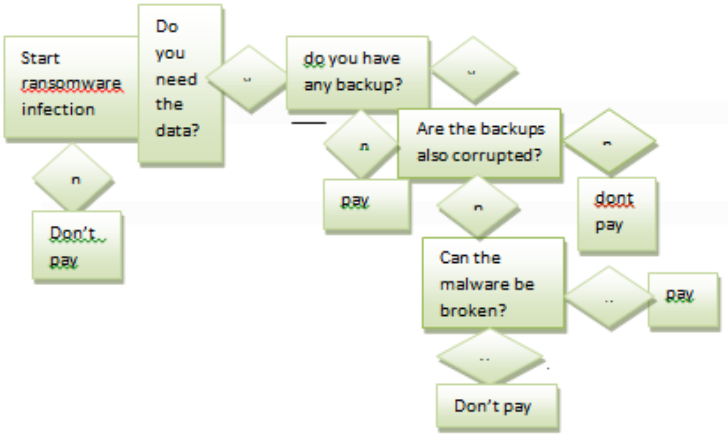

Fig. 1 The Basic Method of Ransomware

VI. Ransomware All Over The World

In the beginning it was based on one user. Hackers attacked one single PC, took all information and demand for money what turns into bit-coin after a while what makes it more risky and undetectable. Suddenly victims saw he couldn't access in his system and got a notification only if he wants his stuff back he had to pay some bit-coin when he doesn't even know what bit-coin is. For the sake of files they fulfilled the demand of criminals. Subsequently they get aware and started to store backups also day by day the attack shifted from one user to organizations [18]. The arrival of bit-coin in the ransomware world was for the low risk, high profitability and lower use of bit-coin. The transaction of this crypto-currency is just unidentifiable from where it's coming or going .The amount of bit-coin also increasing according to the amount and importance of information not only offices it has been seen many times the entire system of hospitals get attacked by ransomware. So the risk is not only about data, it's about human life also. In February 2016 the computer network at Hollywood Presbyterian medical center was down for more than a week. A campaign presented the advertisement achieved 13,491installs and 116 ransom payments earning a total of $34,800.74 between April and May 2016 [19].

Statistics

Date	Installs	Encryption started good	Encryption started bad	Encrypiton completed	Visit landing	Number of payments	CRV	CRI	Profit	
5/8/2016	22	3	4	4	92	1	1.09%	4.55%	0.9731	445.27
5/7/2016	36	4	7	4	249	8	3.21%	22.22%	5.3871	2465.1
5/6/2016	148	36	18	26	262	9	3.44%	6.06%	6.8622	3140.09
5/5/2016	290	102	23	91	602	15	2.49%	5.36%	9.5242	4558.19
5/4/2016	3583	2200	367	1716	643	18	3%	0.49%	12.1432	5556.62
5/3/2016	3454	2165	344	1565	291	16	2.49%	0.46%	10.2516	4591.02
5/2/2016	85	10	3	8	32	7	2.41%	8.14%	5.5179	2524.92
5/1/2016	65	2	1	2	102	0	0.00%	0.00%	0	0
4/30/2016	26	7	7	10	485	2	1.95%	3.64%	1.7419	797.08
4/29/2016	55	34	14	43	500	18	3.71%	9.54%	15.1289	6922.82
4/28/2016	183	3987	538	2895	143	10	2.00%	0.17%	7.6064	3480.63
4/27/2016	5792	1	0	9	140	4	2.80%	8.70%	0.356	162.89
4/26/2016	45	3	0	7	120	3	2.14%	8.11%	0.2263	103.53
4/25/2016	37	6	0	19	61	3	2.34%	7.09%	0.2368	109.27
4/24/2016	38	14	1	28	641	2	3.28%	3.64%	0.0947	43.33
Total	13941	8574	1329	6417	4371	116	2.65%	1.35%	76.0522	34800.74

Fig. 2 Growth of Ransomware attacks (Nov'15-Mar'16)

The cycle of ransomware all over the world getting strong day by day.it has become an industry, service and a competition also among the hackers. The unity fixed rules among their black society making it stronger. It has been almost a decade the ransomware is spreading but during last three years the emergence of ransomware was significant. The sophistication level and the way of targeting has changed. The most important reason of the explosion is RaaS (Ransomware as a Service). It is a system of buying and selling system in the dark web in line with capability where the terms of ransom are set. It helps to improve the skills of cybercriminals also. For this they are getting more skillful and diverging the way of their works.

VII. Findings And Discussion

If it would get spread in our country –

- It can be a big reason of our economic fall
- In so many areas people have started to get attached with mobile banking and other digitalized systems. If it would happen, it will make a fear among them about internet based works
- As most of the people of our country is not IT literate, many of them doesn't even know the ABC of IT. If this kind of attack will happen they can never attempt to come up. Which can be a big blockage in the rapid growth of digitalization.
- As our security system is not stable enough yet. If we let it be as it is, it can be harmful for our governmental information also.
- Question paper, results can be attacked through it, as it is a very sensitive part of our country.
- Many other corruption will increase because of this.
- Black hat Hackers of our own country can be the part of it rather than recuing own country.
- Attacks in the healthcare center and the hospital can be the reason of the toll of human lives. The loss of data can be the reason of their financial lose also.

Overall situation can be more worst if we don't get active in our security system and public awareness. The ransomware is just ramping up now world widely. The situation is so bad that we cannot pass a week even without hearing a new news with new diversion about ransomware. Strongly secure country like US is also spending tough time to cope with this infection, thus we can perceive that how safe and aware we need to be.

VIII. Recommendations

For a country like us it's not only about to aware the people of IT but also the people who are the main user. At first we need to aware the people all over the country in school and high school levels.

- At first we need to teach the teachers through trainings about the bit-coin, cyber criminals, how they works, ransomware etc.
- We need to teach all students the proper use of google drive and other drives. Authority needs to get more active to make students inspired in IT.
- Attacked even we all computers and the systems need to make secure and people need to learn to keep backup files so that if we get can deny the ransom
- We need to let people learn to say no to ransom which helps to discourage the criminals.
- Government need to be more conscious about the security system of our administrative data. They should keep a backup of everything also. Because the amount of ransom can be unimaginable in accordance with the importance of data.

Knowing how the ransomware came onto your system can help you better prime your defense system and direct your detection mechanisms in the future.

IX. Conclusion

There is no guaranteed defense against ransomware because in recent years, it is found that different organization with heavy cyber security budget fall victim to ransomware attacks. Maybe the best and only defense is to be setup so that anyone can wipe any affected machine clean at any time and for this you need to reinstall your system from your last cleanup. Now cyber criminals see an easy opportunity for getting a good profit which combined with new methodologies in targeting their attacks. Now the age of self-propagate and move semi autonomously throughout a network to devastating effect. So when the ransomware attacks, it can easily elevate from a potential data loss to potential identity theft to a data breach in the form of extortion. According to FBI report criminal are netting an estimated $150 million a year through these scams and they said ransomware I the actually scarier than the Scareware scams. So this is the high time to start making strides towards defensible architecture today, massive ransoms may end up getting paid tomorrow.

Acknowledgment

The authors acknowledge the support from the researchers of DIU Cyber Security Centre for their time and resource support.

References

[1] Anderson,R.,Barton,C.,Bohme, R.,Clayton, R.,van Eeten,M.J. G.,Levi,M.,Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime.

[2] Exploring E-readiness on E-commerce adoption of SMEs: Case study South-East Asia.

[3] Antonio Pooe ; L Labuschagne A conceptual model for digital forensic readiness.

[4] W. Sutopo ; R. W. Astuti ; A. Purwanto ; M. Nizam. Commercialization model of new technology lithium ion battery: A case study for smart electrical vehicle.

[5] K. Mohitmafi ; P. Hanafizadeh . A selection framework of e-business model by assessing organizational e-readiness.

[6] J. Puustjärvi ; L. Puustjärvi . Practicing information therapy in self-care: A solution to the rise in health care costs.

[7] Jinxue Zhang; Rui Zhang; Yanchao Zhang; Guanhua Yan. The Rise of Social Botnets: Attacks and Countermeasures.

[8] Vincent Micheal Kiberu; Vincent Micheal Kiberu. E-Health Readiness Assessment in Uganda: Integration of Telemedicine Services into Public Healthcare System.

[9] Krzysztof Cabaj; Wojciech Mazurczyk. Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall.

[10] Bora Tüccaroğlu ; Müesser Nat. The readiness of banks for the application of Business Intelligence solutions.
[11] Shewangu D. (2015), Cyber-banking fraud risk mitigation- conceptual model, Banks and Bank Systems, Volume 10, Issue 2, 2015.
[12] Fedaral Bureau of Investigation, Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer credit Washington, D.C. September 14, 2011.
[13] Defeating crypto-locking with threat-cloud and gateway threat prevention
[14] Florencio, D., & Herley, C. (2010). Phishing and money mules. In Information Forensics and Security WIFS,IEEE International Workshop on pp.1-5.IEEE
https://doi.org/10.1109/WIFS.2010.5711465
[15] ISTR and symentic intelligent recources; http://www.symentic.com /security/responsecontent/2016/02/Rise_of_Android_Ransomware.pdf
[16] http://www.symantec.com/content/en/us/enterprise/media/security_response/white papers/ISTR2016_Ransomware_and_Businesses.pdf
[17] http://icitech.org/wp-content/uploads/2016/03/ICIT-Brief-The-Ransomware-Report2.pdf
[18] https://go.crowdstrike.com/rs/281-OBQ-2266/images/ WhitepaperRansomware.pdf
[19] Mohammad Mehdi Ahmadian ; Hamid Reza Shahriari ; Seyed Mohammad Ghaffarian. Connection-monitor & connection-breaker: A novel approach for prevention and detection of high survivable ransomwares.

Ms. Samantha Haque is a BSc student of the Department of Software Engineering, Daffodil International University, Bangladesh. She is also working as a part time researcher at the Cyber Security Center of the same University. Her research interest includes ransomware, data security, data mining for counter-terrorism, secure cloud computing, healthcare and social networks, cryptography etc. Ms. Samantha Haque is also associated with www.bugsbd.com as an independent contributor to support cyber security related issues. Her future plan is to study in the area of Information Security and become a Cyber Security professional.

Dr. Touhid Bhuiyan is the Founder Director of the Cyber Security Center, Daffodil International University (DIU), Bangladesh. His research interests are in cyber security, intelligent recommendations, social network, trust management, database management, e-Learning etc. He is the recipient of Australian Postgraduate Award and Deputy Vice-Chancellor's Initiative Scholarship from QUT, Australia. Before joining at DIU, he has employed by several renowned organizations including The University of Western Australia, Central College Sydney, Queensland University of Technology and University of Western Sydney. He has more than 18 years' experience in teaching, research and working at the IT industry in Australia, Singapore, Malaysia and Bangladesh.