Evolution of Ransomware, Attacks and Prevention.

Rohan Dhadge[1]

[1]U.G. Student, SOE, ADYPU, Lohagaon, Pune, Maharashtra, India.

Abstract:

In today's era cyber-attacks are in demand where users are having trouble in performing their tasks. One of these cyber-attacks is Ransomware which has the potential to cause large scale damage to the user or the company which has been attacked. This attack can cost a company its fortune. Basically ransomware encrypts the files or system so that user are blocked from the access. The attackers ask ransom in exchange of decryption key. Here we discuss what was the first attack of ransomware and the evolution of the same. Even how we can prevent a ransomware attack. The vectors that play major role in vulnerability of the system or company. Backup of data and system plays major role in prevention of ransomware attack as files and system are encrypted the user looses access of data. The backup services come in action when the system is attacked as user already have data backed up and ready to use.

I. Introduction:

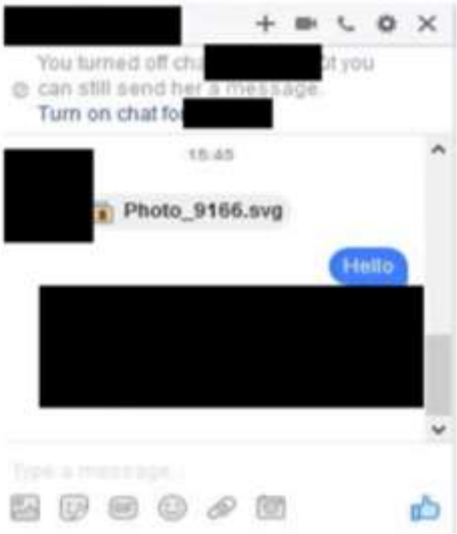
Ransomware is categorized as a spiteful software that gains approach to files or systems and enciphers the files and blocks user approach to systems. All files are then encrypted by the attackers and ransom is asked in exchange for the decryption key. Once the ransom is paid to the attackers and the key is released the users can access to the files and system that are blocked. In this current time ransomware comprise a consolidation of advanced circulation attempt advanced growth techniques using enciphers to assures the reverse engineering is exceptionally hard as well as pre-built framework used for distributing the new variety with ease and widely. The use of offline encipher techniques are becoming prominent in which ransomware takes the profit of authorized system options such as Microsoft CryptoAPI, excluding the demand for Command and Control connection. As ransomware is becoming one of the durable attacks, businesses and self-employed are having trouble facing threats and it is not surprising that attacks are becoming more complex, and it is more difficult for preventing and even more harmful to victim.

II. Working of Ransomware Attack:

To elicit users or businesses for economic earnings this function of a software is known to be as 'ransomware'. The penetration is done through infecting or attack vectors. The program then penetrated to the data or system that it will hold ransom. Malware and virus software consist similarities to some biological issues. Due to those similarities only, filtered entering points are called as "vectors," same as the world of epidemiology uses the term for carriers of harmful pathogens. Like the biological world, there are a many way for systems to be affected and ransomed. Technically, an attack or infection vector is the only means through which ransomware gains access.

III. Example of vector types

Messages: A common means of deception employed by ransomware assailants is to message victims on social media. And on of the most prominent means approach is Facebook Messenger. Accounts are created to mimic a user's current friend and is used to send a message with file attachments. Once opened, ransomware could gain access and lock down network connection to infect the device.



[redacted]

You turned off cha[redacted]t you
can still send her a message.
Turn on chat fo[redacted]

15:45

[redacted]

Photo_9166.svg

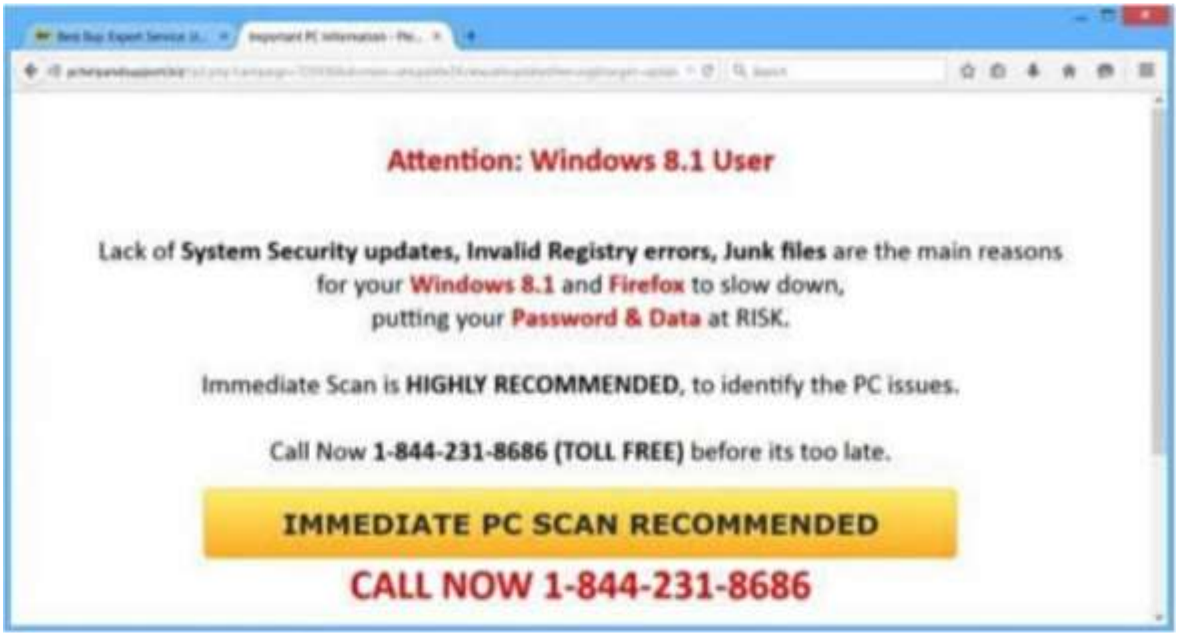
Hello

[redacted]

Type a message...

Fig 1 Screenshot via The Windows Club.

Pop up's: Another common yet older ransomware vector is the online "Pop-ups". Pop-ups are made to mimic currently-used software so that users will feel more comfortable following prompts, which are ultimately designed to hurt the user.



Attention: Windows 8.1 User

Lack of System Security updates, Invalid Registry errors, Junk files are the main reasons for your Windows 8.1 and Firefox to slow down, putting your Password & Data at RISK.

Immediate Scan is HIGHLY RECOMMENDED, to identify the PC issues.

Call Now 1-844-231-8686 (TOLL FREE) before its too late.

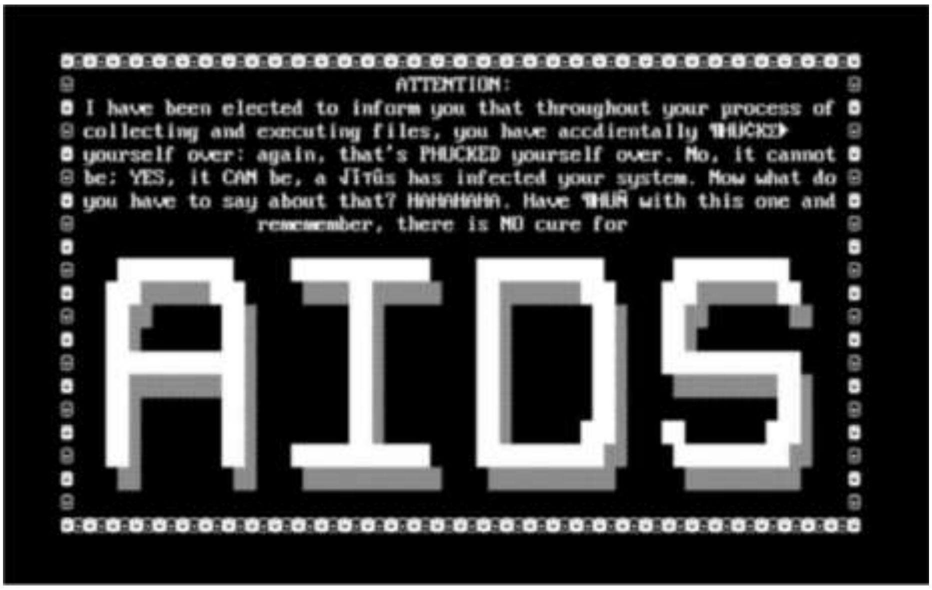
IMMEDIATE PC SCAN RECOMMENDED

CALL NOW 1-844-231-8686

Fig no 2 Screenshot via Fixyourbrowser.

IV. First Ransomware Attack:

The first ever known ransomware attack was recorded in 1989 which targeted the healthcare industry. Today after 30 years healthcare industry remains at the top target for ransomware attack. The first ever known attack was deployed by an AID researcher named Joseph Popp, who carried the attack by making 20,000 floppy disks available to AID researchers spanning more than 90 countries. Claiming the disk contained a program that had questionnaires which analysed individual's risk of acquiring AIDs. As the disk also consisted a malware which at the start behaves as a dormant in computers and was programmed to triggered only after a computer is powered 90 times. After the 90th start was reached the malware displayed a dialog message which demands a amount of $189 and other $378 for a software validity plans. This attack was also known as AIDs Trojan or PC Cybor



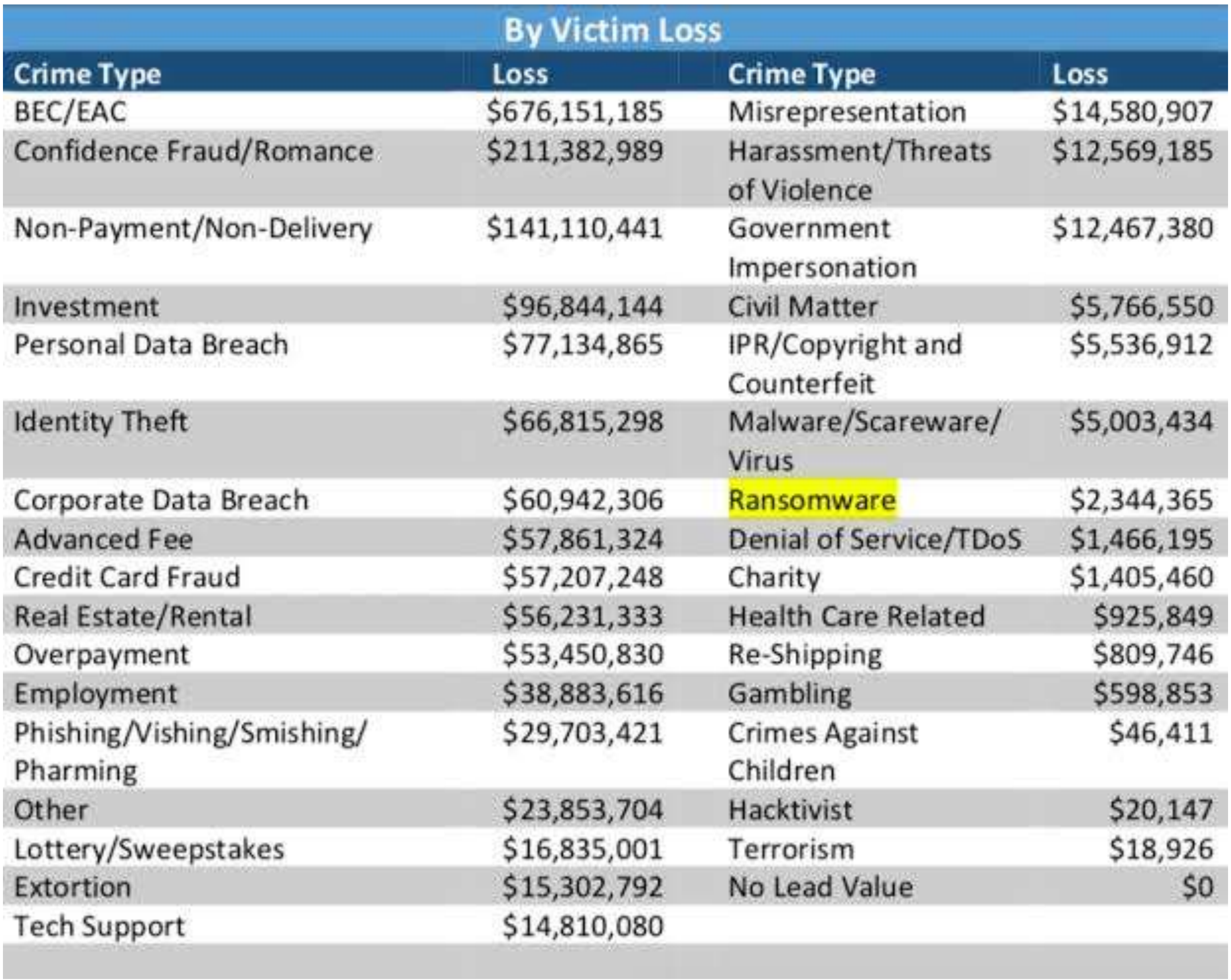
```
                        ATTENTION:
I have been elected to inform you that throughout your process of
collecting and executing files, you have accdientally ¶HUCKED
yourself over: again, that's PHUCKED yourself over. No, it cannot
be: YES, it CAN be, a √ïτûs has infected your system. Now what do
you have to say about that? HAHAHAHA. Have ¶UÑ with this one and
              remember, there is NO cure for

                          AIDS
```

Fig 3 The message floppy disk recipients received.

V. Evolution of Ransomware:

Early ransomware developers typically created their own encryption code, but today's generation attackers are reliable off the shelf library that are significantly harder to crack. Which is leveraging more complicated methods of delivering such as spear-phishing rather than traditional phishing email blasts, which are filtered out by email spam filter today. Some users have created toolkits which can be downloaded and used to attack by attacker with less technical skills. There are cybercriminals who are providing ransomware by offering ransomware as a service program. Which has induced the rise of infamous ransomwares like Crypto Locker, Crypto wall, Locky and Tesla Crypt. Where $320 million revenue has been generated by Crypto wall itself. The ransomware remained infrequent until mid-2000's when the attacks begin applying more difficult and hard to break encryption such as RSA algorithms. TROJ.RANSOM.A, Krotten, MayArchive were some famous during this time. Then in 2011 a ransomware surfaced imitating Widows Product Activation notice making it more challenging for users to tell difference between genuine notifications and threats.



By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$676,151,185	Misrepresentation	$14,580,907
Confidence Fraud/Romance	$211,382,989	Harassment/Threats of Violence	$12,569,185
Non-Payment/Non-Delivery	$141,110,441	Government Impersonation	$12,467,380
Investment	$96,844,144	Civil Matter	$5,766,550
Personal Data Breach	$77,134,865	IPR/Copyright and Counterfeit	$5,536,912
Identity Theft	$66,815,298	Malware/Scareware/Virus	$5,003,434
Corporate Data Breach	$60,942,306	Ransomware	$2,344,365
Advanced Fee	$57,861,324	Denial of Service/TDoS	$1,466,195
Credit Card Fraud	$57,207,248	Charity	$1,405,460
Real Estate/Rental	$56,231,333	Health Care Related	$925,849
Overpayment	$53,450,830	Re-Shipping	$809,746
Employment	$38,883,616	Gambling	$598,853
Phishing/Vishing/Smishing/Pharming	$29,703,421	Crimes Against Children	$46,411
Other	$23,853,704	Hacktivist	$20,147
Lottery/Sweepstakes	$16,835,001	Terrorism	$18,926
Extortion	$15,302,792	No Lead Value	$0
Tech Support	$14,810,080		

Fig 4 History of Ransomware

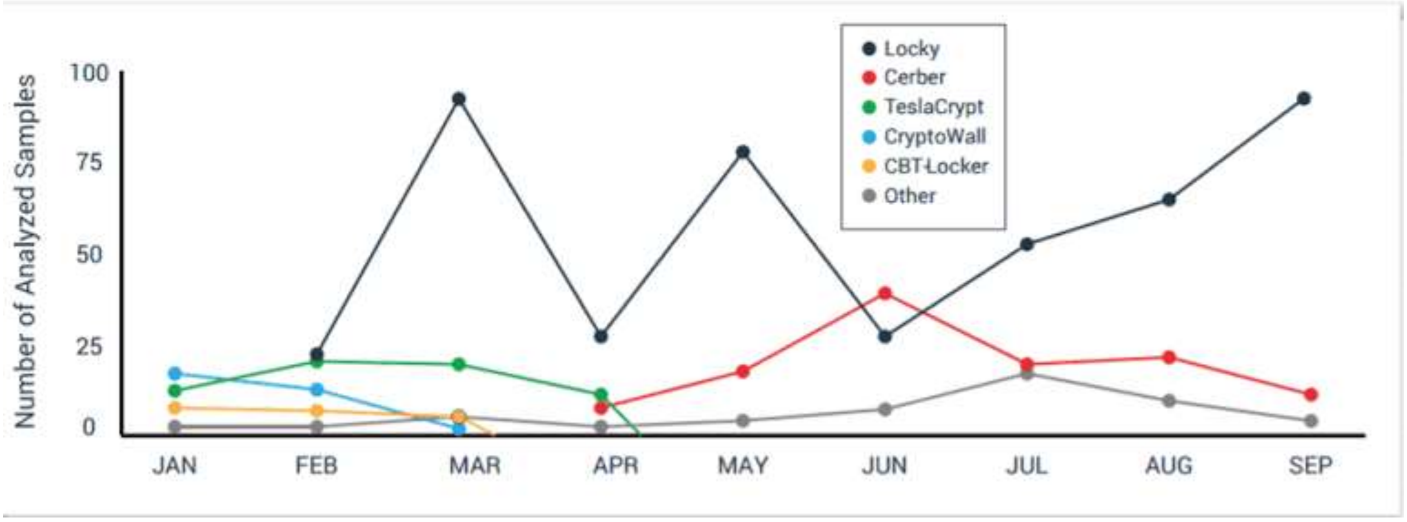


Fig 5 Relative proportions of ransomware varieties analysed

Prevention against Ransomware:

As to reduce the risk of falling into ransomware there are steps that can be taken care by the end-user or companies. There are four vital cybersecurity practices to minimise the damage of ransomware and they are as follows:

a. Frequent tested backups: To backup important files and system are one of the robust defences against ransomware. The backup should be tested to ensure that data is not corrupt to be ready for restoration when needed.
b. Sensible Restrictions: There should be limitations and restriction to the people who have access to the company systems which contains company files, records/programs. Use devices attached to company network that could be made vulnerable should be restricted or limitations should be applied.
c. Proper Credentials Tracking: Any person who is given access to the system can have potential of vulnerability point of ransomware. If the company fails to update password and improper restriction can result in higher possibilities of attacks at this point.
d. Structured regular updates: A company uses different software which can have patches or loop holes that can be a potential point of threat. The software should be updated on time. Even the company should appoint an employee for software updating. The less people involved in this process the less are the chances of attack vectors for criminals.

Conclusion:

In past few years ransomware had evolved significantly and for the criminals the internet is like an enormous ocean of opportunities where they can carry out their criminal activities. Internet itself has created a environment that supports the development and financial backup for creation of a malware. As the criminals have strived to bulletproof their anonymity, they have used money-laundering services that have popped up as part of the criminal ecosystem. These money laundering services are also known as ‘mixing services’, where the ransom payment is passed through multiple Bitcoin wallets, performing money laundering, to further cover the criminals’ tracks. User should have updated software and should have restriction based on the users. Safety guidelines should be followed by companies to keep a step ahead of a ransomware attack. As the ransomware has evolved as so the attackers have started to take advantages of them. As the resource are increased for the malwares so we have to be updated for the preventions against them. Backup services should be checked and updated for the recovery when needed.

References:

1. ISSN 2047-4954Received on 20th September 2017 Evolution of ransomware.
2. IEEE LETTERS OF THE COMPUTER SOCIETY, VOL. 2, NO. 2, APRIL-JUNE 2019
3. 10.1109/ACCESS.2019.2945839 A Survey on Detection Techniques for Cryptographic Ransomware