Ransomware and Cryptojacking – The Two Biggest Threats to User Security

Hardik Prajapati

Asst. Professor, Department of Electronics & Communication, Indus University, India

Abstract : ***Ransomware is a type of cyber attack, which take control over a computer and prevents the user to access data until ransom is paid. The attacker encrypts the data and stops other software and apps from running. Such malware is causing millions of dollars financial loss [1]. Users are given instructions for how to pay ransom to get the decryption key. The costs can range a few hundred dollars to thousand payable to cybercriminals in Bitcoin. Cryptojacking is emerging as a more cost-effective and efficient alternative to ransomware, in ransomware attack there is no guarantee that the attacker will get ransom. On the other hand Cryptojacking empowers hackers to make use of infected computers and assures financial gain. Cryptojacking is the illegal practice of accessing and using the resources of a target computer, mobile device, or server to mine cryptocurrencies [2].***

IndexTerms – Bitcoin, Encryption, Identity theft, Crypto

I. INTRODUCTION

As the technology is growing cyberattack has become profiteering business for hackers. Cyber attack uses infected programs change computer logic, data or code, which results in troublesome consequences which leads to cybercrime like information and identity theft. The Wanna Cry ransomware attack is one of the largest ever cyber attacks affecting computers across the globe [3]. On 12th May 2017, media reports started highlighting that a ransomware attack had brought down computer systems in UK hospitals. It soon emerged that the attack was global with reports of affected computers coming in from all over the globe. The ransomware - Wanna Cry - infected computers and encrypted all the data stored on the hard drives. In lieu of decrypting the data, Wanna Cry demanded payment ranging between $300 (around Rs 19,000) to $600 (around Rs 39,000) in Bitcoin [3]. Fig. 1 shows how Ransomware works.

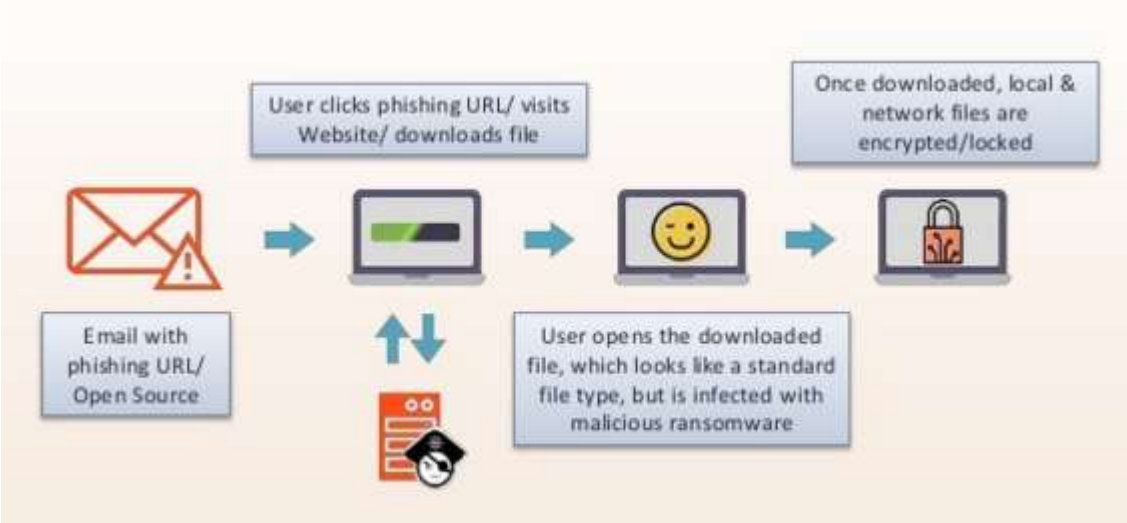

Figure: 1 How Ransomware works

II. TYPES OF RANSOMWARE

There are two main types of ransomware in circulation today:
1. Locker ransomware (computer locker): Denies access to the computer or device
2. Crypto ransomware (data locker): Prevents access to files or data. Crypto ransomware doesn't necessarily have to use encryption to stop users from accessing their data, but the vast majority of it does [4].
Both types of ransomware are aimed fairly at today's digital lifestyle. They are designed to deny the users to access what they need and offer to return what is rightfully users' on payment of a ransom. Despite having similar objectives, the approaches taken by each type of ransomware are quite different.

Locker Ransomware:
Locker ransomware is designed to deny access to computing resources. This typically takes the form of locking the computer's or device's user interface and then asking the user to pay a fee in order to restore access to it. Locked computers will often be left with limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom. This means access to the mouse might be disabled and the keyboard functionality might be limited to numeric keys, allowing the victim to only type numbers to indicate the payment code.
Locker ransomware is typically only designed to prevent access to the computer interface, largely leaving the underlying system and files untouched. This means that the malware could potentially be removed to restore a computer to something close to its original state. This makes locker ransomware less effective at extracting ransom payments compared with its more destructive relative crypto ransomware.

Because locker ransomware can usually be removed cleanly, it tends to be the type of ransomware that goes to great lengths to incorporate social-engineering techniques to pressure victims into paying. This type of ransomware often masquerades as law enforcement authorities and claims to issue fines to users for alleged online indiscretions or criminal activities. Locker ransomware can particularly be effective on devices that have limited options for users to interact with. This is a potential problem area considering the recent boom in wearable devices and the Internet of Things (IoT), where millions of connected devices could potentially be at risk from this type of ransomware [4].

Crypto ransomware:

This type of ransomware is designed to find and encrypt valuable data stored on the computer, making the data useless unless the user obtains the decryption key. As people's lives become increasingly digital, they are storing more important data on their personal computers and devices. Many users are not aware of the need to create backups to guard against hard disk failures or the loss or theft of the computer, let alone a possible crypto ransomware attack. This could be because users don't realize the value of the data until it is lost. Setting up an effective backup process requires some work and discipline, so it's not an attractive proposition for the average user. Crypto ransomware targets these weaknesses in the typical user's security posture for extortion purposes. The creators of crypto ransomware know that data stored on personal computers is likely to be important to users. For example, the data could include things like memories of loved ones, a college project due for submission, or perhaps a financial report for work. The ransomware victims may be desperate to get their data back, preferring to pay the ransom to restore access rather than simply lose it forever and suffer the consequences.

After installation, a typical crypto ransomware threat quietly searches for and encrypts files. Its goal is to stay below the radar until it can find and encrypt all of the files that could be of value to the user. By the time the victim is presented with the malware's message that informs them that their data is encrypted, the damage is already done. With most crypto ransomware infections, the affected computer continues to work normally, as the malware does not target critical system files or deny access to the computer's functionality. This means that users can still use the computer to perform a range of activities apart from accessing the data that has been encrypted [4].

Figure:2 Screen which appear after ransomware attack

III. COUNTERMEASURES AGAINST RANSOMWARE

There is no any technique which gives guarantee against malware, some precautions must be taken by users [6].

1. Stop ransomware before the endpoint: The most proactive method of protecting a network from ransomware attack (other than the human firewall) is to keep ransomware from reaching the endpoint in the first place. Consider a web-filtering technology.
2. Apply all current operating system and application patches: Many ransomware strategies take advantage of vulnerabilities in the operating system or in applications to infect an endpoint. Having latest operating system and patches will reduce the chances of attack.
3. Spam filtering and web gateway filtering: Again, the ideal approach is to keep ransomware off the network and the network and the endpoint. Spam filtering and web gateway filtering are great ways to stop ransomware that tries to reach the endpoint through malicious IPs, URLs, and email spam.
4. Allow only white listed items to execute: Use an "application control" method that offers centrally administered white listing to block unauthorized executables on servers, corporate desktops, and fixed-function devices, thus dramatically reducing the attack surface for most ransomware.
5. Limit privileges for unknown processes: This can be done easily by writing rules for host intrusion prevention systems or access protection rules.

IV. CRYPTOJACKING:

Cyber criminals who have been firmly focused on ransomware for revenue generation are now starting to explore other opportunities [7] . During the past year, the astronomical rise in crypto currency values inspired many cyber criminals to shift to coin mining as an alternative revenue source. With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are using coin miners to steal computer processing power and cloud CPU usage from consumers and enterprises to mine crypto currency. While the immediate impact of coin mining is typically performance related—slowing down devices, overheating batteries, and in some cases, rendering devices unusable—there are broader implications, particularly for organizations. Corporate networks are at risk of shutdown from coin miners aggressively propagated across their environment. There may also be financial implications for organizations who find themselves billed for cloud CPU usage by coin miners. As malicious coin mining evolves, IoT devices will continue to be ripe targets for exploitation. Symantec already found a 600 percent increase in overall IoT attacks in 2017 [7].

4.1 How Cryptojacking works:

Cryptocurrencies have skyrocketed in the recent years, which leads the hackers to 'cryptojacking'. Cryptojacking refers to secretly mining cryptocurrency (generating digital cash) by a website using the resources of users' computers usually without their knowledge. It is estimated that a single Bitcoin transaction (which happens in cryptojacking) consumes 215 kilowatt-hours (KWh) of energy causing significant system slowdown and spiked electricity bills [8] . Now, cryptojacking might be used by legitimate sites as a revenue stream instead of serving their visitors with pesky advertisements – which makes sense in a way. But, the fact that, this entire thing goes on without the user's consent still makes it malicious. Looking at cryptojacking from an angle of cybercrime – there is another side to it. Hackers might inject mining codes into legitimate websites (without the website owner's nor its visitor's knowledge) to generate cryptocurrency and fill their wallet. Now, all this might not look as harmful as a phishing or traditional malware attack, but at the end of it all users are being robbed of their money indirectly without their knowledge or will [8]. As opposed to ransomware, cryptojacking attacks remain almost undetected, enabling attackers to use the compromised systems to mine cryptocurrencies for as long as they want.

4.2 Types of Cryptojacking:

There are two forms of cryptojacking:
Like other malware attacks and involves tricking a user into downloading a mining application to their computer. It's far easier, however, just to lure visitors to a webpage that includes a script their web browser software runs or to embed a mining script in a common website [9].
Another variant of this latter approach is to inject cryptomining scripts into ad networks that legitimate websites then unknowingly serve to their visitors. The mining script can be very small – just a few lines of text that download a small program from a web server, activate it on the user's own browser and tell the program where to credit any mined cryptocurrency. The user's computer and electricity do all the work, and the person who wrote the code gets all the proceeds. The computer's owner may never even realize what's going on [9].

IV. CONCLUSION

Today, cybercrime has become more serious matter than real life crime, as it affects millions of web users. When the Internet services are interrupted it leads to huge amount of losses. Ransomware and Cryptojacking are the biggest threats against consumers' valuable data. The users need to take all precautions to protect their data like taking back up regularly, keeping all software up to date. For cryptojacking users may be able to recognize on their own. Because it involves increasing processor activity, the computer's temperature can climb and the computer's fan may activate or run more quickly in an attempt to cool things down. Users who are concerned their computers may have been subjected to cryptojacking should run an up-to-date antivirus rogram. Installing software updates may also help users block attacks that try to download cryptojacking software or other malicious programs to their computers

REFERENCES

[1] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler, CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data, 2016 IEEE 36th International Conference on Distributed Computing Systems
[2] Cryptojacking, Threat Bulletin, May 2018
[3] K.V.G.N. Naidu, P.Sireesha, A STUDY ON WANNACRY RANSOMWARE ATTACK, International Journal of Recent Innovation in Engineering and Research, Volume: 02 Issue: 05 May– 2017 (IJRIER)
[4] Kevin Savage, Peter Coogan, Hon Lau, The Evolution of Ransomware, Security Response, Symantec
[5] Azad Ali , RANSOMWARE: A RESEARCH AND A PERSONAL CASE STUDY OF DEALING WITH THIS NASTY MALWARE, Issues in Information Science + Information Security, Volume 14 2017
[6] The Global Technical Support & R&D Center of TREND MICRO, Ransomware: Past, Present and Future
[7] Executive Summary, 2018 Internet Security Threat Report, Symantec
[8] QUICK HEAL ANNUAL THREAT REPORT | 2018