RANSOMEWARE ATTACK IN CYBER SECURITY :A CASE STUDY

Gaurav Kumar Sharma[1], Kamal Kant Verma[2]
[1]B.Tech, Student, Dept. of CSE, Quantum School of Technology, Roorkee, Uttarakhand India
[2]AP Department of Computer Science Quantum School of Technology Roorkee India

Abstract
Nowadays cybercrime is common problem of this world. Crime committed using a computer and the internet to steal a person's identity or illegal imports or malicious programs cybercrime is nothing but where the computer used as an object or subject of crime. To protect this issue we have Cyber Security. Sometimes the security is not good. It break by attackers, Here in this paper, consider a case study of attacks what was the cause or vulnerability of the System who were Victim. Mainly ransomware attacks.
Keywords: Cybercrime, Cyber Security, malicious, Attacker, Vulnerability, Victim, ransomware.

I. INTRODUCTION

Ransomware is a malicious code that is used by cybercriminals to launch data kidnapping and lock screen attacks. The motive for ransomware attacks is monetary, and unlike other types of attacks. The victim is usually notified that an exploit has occurred and is given instructions for how to recover from the attack. Payment is often demanded in virtual currency to protect the criminal's identity. Ransomware malware can be spread through malicious e-mail attachments, infected software apps, infected external storage devices and compromised websites. In a lock screen attack, the malware may change the victim's login credentials for a computing device; in a data kidnapping attack, the malware may encrypt files on the infected device as well as other connected network devices [1].

Types of Ransomware Known:
Till now 12 Ransomware identified [3]:

1. Goldeneye - taking parts of Ukraine offline.
2. WannaCry -decrypt0r wreaks havoc on NHS England.
3. Crypto Locker – where ransomware took off
4. Locky - well engineered, ruthless, clever
5. Petya - locking down the whole system
6. Crysis - Locky copycat with big ambitions
7. zCrypt – ransomware that behaves like a virus
8. PowerWare – PowerShell hijacker
9. HydraCrypt – ransomware can be beaten
10. Cerber – ransomware-as-a-service
11. RAA ransomware – ransomware meets JavaScript
12. Crypto Wall – it's everywhere

II. FACTS ABOUT RANSOMWARE [2]

Typical ransomware software uses RSA 2048 encryption to encrypt files. Just to give you an idea of how strong, this is, an average desktop computer is estimated to take around 6.4 quadrillion years to crack an RSA 2048 key.
Crypto Locker was followed up by the variant Crypto Wall, which made $325 million dollars in 18 months, half of that in the United States. By now there are thousands of ransomware victims, including a New Jersey School district, police departments in Maine, Massachusetts & Chicago.

III. SYSTEM AFFECTED FROM RANSOMWARE (WANNACRY) 2017

Windows XP, Windows 8, and Windows Server 2003,Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012, Windows 10,

Windows Server 2012 R2, Windows Server 2016.

After system got affected from wannacry ransomware Microsoft release the patch for the system which have Outdated security.[4]

Figure 1 Ransomware screen

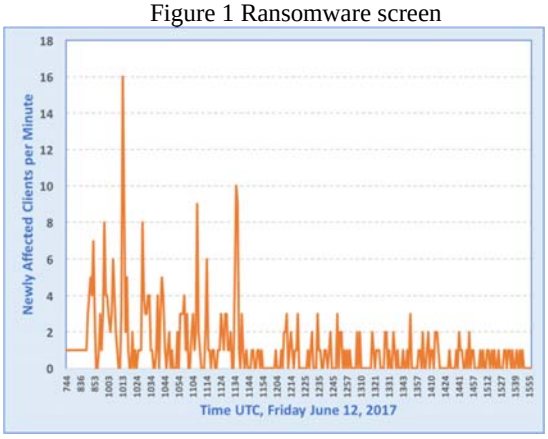


Figure 2 Wannacry Graph

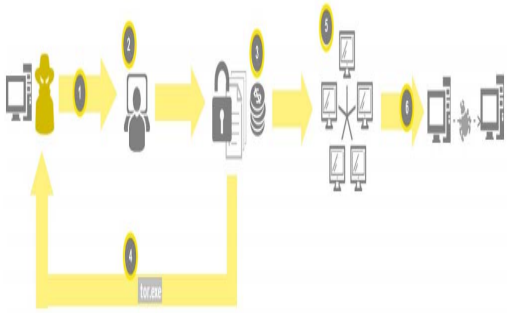
A.The Biggest Cyber-Attacks in History [5]

Cyber-attacks have become more and more frequent as the world becomes ever connected by technology. Millions of attacks take place ever year as cyber criminals target critical data and finances. Quite often the attacks will target individuals but what about those on a larger scale? Take a look at five of the biggest cyber-attacks in history.

1. Google China (2009).
2. Heart bleed (2012-2014)
3. PlayStation Network (2011)
4. Sony Pictures Entertainment (2014)
5. Yahoo (2012-2014)
6. Wannacry Ransomware (2017)

B. Attacker uses a yet-to-be-confirmed initial attack vector [6]

1. WannaCry encrypts files in the victim's machine using AES-128 cypher, deletes shadow copies.
2. It then displays a ransom note requesting $300 or $600 in bit coin
3. Tor.exe is used by wannadecryptor.exe, initiating connections to tor nodes in order toconnect back to the attacker (therefore making this extremely difficult, if not impossible, totrack)
4. IP address of the infected machine is checked; then IP addresses of the same subnet are
5. scanned for additional vulnerable machines and connected to via port 445 TCP
6. When a machine is successfully connected, data containing the exploit payload is transferred



First Ransomware was discovered in 1989 and targeted the health care industry.[6]

s.no	Name	year	Comment
1.	Tesla Crypt	Feb 2015	Initially targeted online games later it become one of the most seen ransomware.
2.	Fusob	Apr 2015	It accounted more for more than half of the Infected mobile phones.
3.	Tox	May 2015	It is free to use but the developers get a percentage of ransom.
4.	Sleeper ransom -ware Locker	May 2015	Infected windows machines.

5.	Chimera	Sep 2015	Leak the encrypted file if the ransom is not paid.
6.	Ransom ware 32	Jan 2016	Written in JavaScript so it can affect windows, mac OS, and Linux.
7.	7ev3n	Jan 2016	First to destroy files if the ransom is not paid. It ask for the highest ransom(13 BitCoins about $5000).
8.	Locky	Feb 2016	It is part of an aggressive phishing campaign that uses the Dridex infrastructure. It is one of the most notorious ransomware
9.	Locky	Mar 2016	Two more hospital in California hit with locky.
10.	Samsam	Mar 2016	It is first ransomware to target Jboss Server. It allows for attacker to communicate to the victim in real time using tor browser.
11.	Petya	Apr 2016	Overwrite the systems master boot record. It is delivered by Drop box.
12.	Petya	Jul 2016	Developers releases chimeras decryption key to reduce completion.
13.	Shadow Breaker	Aug 2016	First campaign leaking tools and exploits used by the Equation Group (or the NSA)
14.	Shadow Brokers	Apr 2017	Shadow Brokers have a fifth dumping campaign which exposes the Double Pulsar and the External Blue exploits.
15.	Wannac ry	May 2017	Impacted over 300,000 systems at least 150 countries.

C.GLOBAL IMPACT OF WANNACRY [6]

There are approximately 30–40 publicly named companies among the likely thousands that were impacted by this ransomware. Examples include the Russian Interior Ministry, Telefonica (Spain's largest telecommunications company) and FedEx. The UK National Health Service (NHS) was badly hit, with 16 of the 47 NHS trusts being affected, and routine surgery and doctor appointments being canceled as the service recovers. There are reports that in China over 40,000 organizations have been affected, including over 60 academic institutions.

Figure 4 Twitter Malware Tech - Ransomware country target mapping

IV. SECURITY LOOP HOLE [7][8]

WannaCry propagates using EternalBlue, an exploit of Windows' Server Message Block (SMB) protocol. Much of the attention and comment around the event was occasioned by the fact that the U.S. National Security Agency (NSA) had already discovered the vulnerability, but used it to create an exploit for its own offensive work, rather than report it to Microsoft.

V.HOW TO SECURE YOURSELF FROM CYBER ATTACKS [9][10]

1.Set one day a week to monitor your credit card statements
2. Sign up for real-time alerts.
3. Keep your private information private
4. Routinely change passwords and make them strong
5. Subscribe to identity protection
6. System security update before vulnerability release.

HOW TO PROTECT FROM RANSOMWARE ATTACKS:

1. Update your software
2. Install antivirus software
3. Be wary of suspicious emails and pop-ups.
4. Create backups of your data
5. Create a security plan for your business

What to do if already infected?

If you are already a victim of ransomware, the first thing to do is disconnect your computer from the internet so it does not infect other machines. Then report the crime to law enforcement and seek help from a technology professional who specializes in data recovery to see what your options might be. If there are none,

don't lose hope: There may be new security tools to unlock your files in the future.
In some extreme cases, it might make sense to pay a ransom if you have no backups and the encrypted files are valuable, Mr. Wysopal said. But he added that with WannaCry, people definitely should not pay the ransom. That's because the hackers are apparently overloaded with requests from victims asking for their data to be released — and many who have paid the ransom are not hearing back.

VI. CONCLUSION

The purpose of this paper is to analyze and to make aware of ransomware and Cyber Crime. So that, they will not be the victim of these crime by using proper security policies.
We come to the conclusion WannaCry Ransomware Attack 2017 is one of the catastrophic attack among the attack were happened in past years.

References:

[1]http://searchsecurity.techtarget.com/definition/ransomware

[2]https://www.wired.com/wpcontent/uploads/2016/03/RansomwareManual-1.pdf .

[3]http://www.computerworlduk.com/galleries/security/worst-ransomware-attacks-we-name-internets-nastiest-extortion-malware-3641916/ .

[4]https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/ .

[5]https://superfast-it.com/five-biggest-cyber-attacks-history/ .

[6]http://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf.

[7]http://www.independent.co.uk/news/uk/home-news/nhs-cyber-attack-edward-snowden-accuses-nsa-not-preventing-ransomware-a7733941.html .

[8]http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/ .

[9]https://www.forbes.com/sites/realspin/2014/02/07/5-ways-to-protect-yourself-from-cyber-attacks/#55a14f445afb .

[10]https://www.nytimes.com/2017/05/15/technology/personaltech/heres-how-to-protect-yourself-from-ransomware-attacks.html?mcubz=0 .