International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

GoldenEye Ransomware Attack

Prakruti Joshi[1], Akshit Kurani[2], Hrisha Yagnik[3]

[1-3]*Student, Department of Computer Engineering, Indus University, Ahmedabad, India*

Abstract : *In this new cyber era on one side, the internet facilities have made the world wiser and quicker with thoughts, and on the other hand the same internet is letting the planet on the verge of destruction by making it transparent and prone to* ***cyber-threats****. Amongst these* ***Ransomeware*** *now poses a significant challenge to the world of web, most tech businesses, universities in the world, corporations and organisations are trying to make warning choices to stop ransomware attacks like* ***GoldenEye*** *Ransomware Attack. This study will review the background knowledge of cyber-crime and ransomware; the cases of* ***Petya*** *attack around the world; and enlighten the concerns and recovery measures for such threats.*

Keywords: *Cyber attacks, Ransomware, GoldenEye, Petya, Prevention, Solutions.*

1. INTRODUCTION

Nowadays cybercrime is a common problem in this world. A crime committed using the internet and the computer to steal an individual's identity or illegal imports or malicious programs. Cybercrime is nothing but where the computer is used as a subject or an object of crime. Experts view that cyber-crime is a new category of crime requiring a comprehensive new legal framework to address a unique nature of emerging technologies and the unique set of challenges that traditional crime do not deal with.[1]

To protect this issue we have cybersecurity. But sometimes the security is not good. It is broken by attackers and there are some attacks that were the cause of vulnerability mainly ransomware attacks. The aim of cyber-attack is to get the information system of an individual or a management.[2]

1.1 Ransomware

Ransomware is a malicious code used by cybercriminals to initiate the abduction of data and lock down screen attacks. The motive for ransom ware attacks is monetary, and unlike other types of attacks.[3]In this case, usually, the victim is notified that an exploit has occurred and hence given instructions for how to recover from the attack. There are different types of ransomware known among which GoldenEye is one.

GoldenEye attack was the follow-on attack after the mass ransomware attack called WannaCry attack which was designed as a 'worm' to increase the speed of the attack allowing the infection to spread to over 300,000 end-points in over 150 countries in 2017 'The year of Ransomware' as per the headlines concerning cyber-security.

1.2 Background

After a few months cyber-security professionals had got their attention on WannaCry, next was the Petya ransomware strain identified as 'GoldenEye' and was expected to be a large-scale attack across the globe. WannaCry ransomware attacks were to begin with Detailed on 12th May 2017 and Petya on 27th June 2017.[4]

WannaCry was utilizing two programs for the attack by the cyber-criminals. Those behind the GoldenEye attacks added another prong to their attack; GoldenEye had two layers of encryption. While ransomware has always targeted files and encrypted them to stop the user from being able to use their computers, GoldenEye encrypts both the files and file structures known as NTFS structures.

Unlike most ransomware, the latest GoldenEye version has two types of encryption, one that independently encrypts target files on the device and another that encrypts NTFS (New Technology File System—a proprietary file system of Microsoft) structures. This approach prohibits victims computers from booting up and downloading stored information or samples in a live operating system (OS) environment.

2. CASES

Less than two months after the spread of the WannaCry ransomware in May, Ukraine faced yet another cyberattack, perhaps the most serious one in its history. Referred to as "Petya", "Petya.A", "PetrWrap", "GoldenEye", "Diskcoder.C", etc.[5] On June 27, 2017, a large-scale attack using a version of the ransomware family known as GoldenEye hit most of the world. Around 37 incidents of ransomware attacks were reported to the Indian Computer Emergency Response Team (CERT-In). Of these, 34 incidents were found of WannaCry and Petya ransomware.[4]

In addition to encrypting files on the computer, this ransomware family is distinguished by encrypting the MBR when it has authorization, thereby blocking complete access to the computer. The attack can nearly be seen as a replica of the much-feared WannaCry attack that rocked the world a little over a month ago. This version of the malware is distributed as a DLL with an EXPORT, which is

named with a parameter that varies with each sample to start the device encryption process. When the malware runs, it encrypts certain files on compromised system drives. In exchange, if it has user permissions, the device boot sector is often encrypted by blocking entry to the computer until an access key is inserted that decrypts the system.

- Once payment of the ransom has been made, the key is presumed to be delivered.
- The sample produces a scheduled operation for the computer to shut down afterward.
- GoldenEye shows a fake window after restarting the device, suggesting that a disk issue is being fixed.

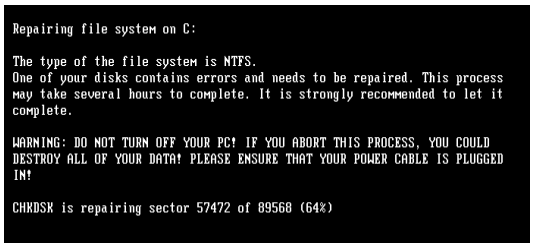

Fig-1: dummy window[6]

- Afterwards it reveals the window seeking the ransom.

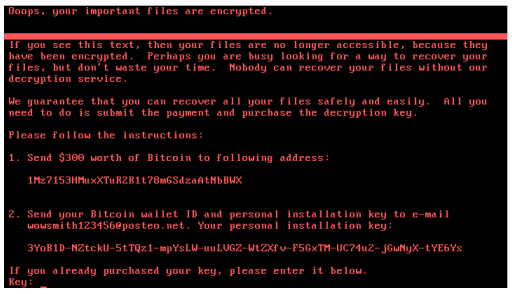

Fig-2: window displaying for ransome[6]

- Just as companies began to think that WannaCry, the malware that put over 200,000 people to ransom across 10,000 organizations in over 100 nations, was on the wane, ransomware again raised its ugly head. The ransomware is labeled as the most comprehensive cyber attack. To fix the 'EternalBlue' exploit in Windows, Microsoft had issued a security patch. [7]
- Although the scale of the cyber-attack is yet to be determined, the virus christened GoldenEye by security firm Bitdefender Labs has had its biggest impact on organizations in Ukraine. And while the target mainly appears to be European countries, the ransomware is also reported to be making inroads in countries like India.

2.1 GoldenEye ransomware attack hit operations at Pipavav Port, JNPT, India

The GoldenEye ransomware attack on the JNPT and Pipavav port may result in the bundling of inbound and outbound cargo, according to the Shipping Ministry. A global ransomware attack interrupted operations at one of three terminals at India's largest container port, Jawaharlal Nehru Port Trust (JNPT), operated by AP Moller-Maersk, near Mumbai, the port said on Wednesday. The variant that triggered the disruption was named by security firm Bitdefender Labs as GoldenEye. On Tuesday, ransomware struck the global operations of the integrated transport and logistics business across its 75 terminals. The JNPT official said The JNPT's IT (information technology) department became aware of the attack on Tuesday at around 4.30pm." The Windows server began to dominate and the master file was encrypted and no data could be accessed. The processes came to a standstill immediately.

Gateway Terminals India operated by APM was absolutely shut down. The JNPT port's APM terminal was affected by the global attack. The processes at the terminal had decelerated and were manually entered. By diverting traffic to other airports, they have been struggling to tackle the situation. Anil Diggikar, JNPT chairman, said, "JNPT operations have not been affected to a large extent." Clearing the backlog took about 24 hours.

Gujarat Pipavav Port told stock exchanges that "At this point in time, the ransomware did not have any major impact on the business."

3. CONCERNS

Concerns have been raised regarding the protection of Indian infrastructure projects with high-level terrorism attack lists for power generation and transmission projects.

The Indian Computer Emergency Response Team (CERT-In), the agency coordinating efforts on cybersecurity issues, in a 27 June advisory warned, "It has been reported that variants of Petya ransomware with work-like capabilities are spreading."

Transportation and shipping companies are ill-prepared for cyberattacks said by Amit Jaju, executive director, fraud investigation and dispute services, EY.

Cybersecurity Ventures estimated global annual cybercrime costs will rise from $3 trillion in 2015 to $6 trillion by 2021. Also experts believe India is ill-equipped to face such attacks.

Space technology is one field which is fully dependent on computers for its functionalities which in turn makes it highly vulnerable to cyber-attacks. [8] Such ransomware attackers are well aware of this dependence, so any significant assault on a nation's satellite grid is necessary to be taken under consideration as a major concern.

4. PROPOSED CHANGES / SOLUTIONS

Traditional security has become inefficient to combat new kinds of virus and malware, so whitelisting a new approach that allows only trusted programs, if anything doesn't match his own database then it will completely discard other things.[9]

"These cases of malware attacks highlight the need for proper cybersecurity planning at all levels particularly for government infrastructure networks," said Pranesh Prakash, policy director at the Bengaluru-based think tank's Centre for Internet and Society.

Since it is a well-funded and rapidly evolving threat, cyber-security should be a top priority for all organizations. The rate in which the danger grows makes it much harder to defend against illegal practices once they are in operation.

Ransomware threats are capable of triggering mass outages and disrupting networks, which can be expensive for organizations that are unable to return to operating capability.

Educating customers on the threats they pose and getting them to realize how they can mitigate the risk of cyber-attack is a major part of putting proper cyber-security measures in place.

A big cause of downtime is human error and this is something that hackers depend on. One of the key reasons why threats like GoldenEye have been so destructive in their success is malicious connections or attachments being opened in emails. It will go a long way to securing systems for the whole company by educating users to be more diligent about their personal protection.

When a ransomware attack cannot be prevented, the only alternative remains to rebound from it. Yet the IT programs will have no prior operating state to return to without an isolated, up-to-date archive of records, and the enterprise will have no alternative but to pay up in the expectation of recovering access or acknowledging that the data is lost permanently. It might be necessary to assist with an onsite archive, but if the infection extends to this nearby copy, it too will be unavailable.

If data is already compromised, installing a new recovery solution is not useful-a backup will be able to take place, but the repair may not be able to get past the encryption that is already there. Your recovery will be fast just by providing up-to-date, isolated data backup and all traces of the ransomware infection will be deleted. Therefore, attacks could not be avoided, but with sufficient information and instruction, they may be retrieved.

CONCLUSION

This study of risks represents a detailed examination of Ransomware, including some of the most common Variant called "GoldenEye", its evolution, vectors, noteworthy threats, and how to work to prevent a company from being the next one casualty. It is obvious that ransomware will evolve. In complexity and as it becomes more generalized, individual users will continue to be troubled, as well as entrepreneurship. The accomplishment thus far in the extortion of the cash from victims opens the way for more Cyber attackers to use ransomware as a form of main tactic.

REFERENCES

[1] NEELESH JAIN, VIBHASH SHRIVASTAVA, "CYBER CRIME CHANGING EVERYTHING – AN EMPIRICAL STUDY",International Journal of Computer Application, ISSN: 2250-1797 , Volume 1, Issue 4, February 2014
[2] Jibi Mariam Biju, Neethu Gopal, Anju J Prakash, "CYBER ATTACKS AND ITS DIFFERENT TYPES", e-ISSN: 2395-0056. Volume: 06 Issue: 03 | Mar 2019.
[3]Gaurav Kumar Sharma, Kamal Kant Verma, "RANSOMEWARE ATTACK IN CYBER SECURITY: A CASE STUDY",Indian Technical research Organization, ISSN(ONLINE):2394-0697, VOLUME-4, ISSUE-10, 2017
[4]Saurabh Kumar Sen, Nidhi Chourey, "A Study of Ransomware Detection and Prevention at Organizations" International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056, Volume: 07 Issue: 07 | July 2020.
[5] Lev Streltsov, "The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments", Eur J Secur Res (2017) 2:147–184 DOI 10.1007/s41125-017-0020-x
[6]https://www.pandasecurity.com/en/mediacenter/malware/goldeneye-petya-ransomware/
[7] Anusha Chandrasekharan, Bhavana Malviya," Ransomware: A Review", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056 , Volume: 05 Issue: 06 | June 2018.
[8] Rohit Sharma, Dr. Mona Purohit, "Emerging Cyber Threats and the Challenges Associated with them", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395-0056 , Volume: 05 Issue: 02 | Feb-2018.
[9] Abhay pratapsingh, "RANSOMEWARE: A HIGH PROFILE ATTACK", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395 -0056, Volume: 04 Issue: 02 | Feb -2017