**Project Proposal Synopsis**

**Index**

|  |  |  |
| --- | --- | --- |
| Sr. No. | Content | Page No. |
| 1 | **Introduction** | **2** |
| 2 | **Objectives** | **3** |
| 3 | **Project Category** | **5** |
| 4 | **Overview of research methodology** | **6** |
| 5 | **Scope of the solution** | **8** |
| 6 | **Tools and Technology Used** | **9** |
| 7 | **Future Scope and further enhancement of the project** | **11** |
| 8 | **Bibliography and Literature survey** | **12** |
|  |  |  |

**Introduction:-**

Ransomware is a particular class of malwares that demands payment in exchange for a stolen functionality, mostly data. This class of malware has been identified as a major threat to computer and network security across the globe. Ransomware installs covertly on a victim's device to either mount the cryptoviral extortion attack from cryptovirology that holds the victim's data hostage, or the cryptovirology leakware attack that threatens to publish the victim's data. The real target of this form of attack is critical data that are very important to individuals and enterprises alike. In fact, the attack has spread to mobile devices and mobile malware detection approaches are not so effective because of the subtle nature of the malicious programs. Therefore, billions of mobile device users are susceptible to this attack.

Most of the ransomware variants depend on file encryption as a strategy for extortion. Data stored on victim’s device are encrypted while the hacker demands for ransom before the files can be decrypted. Ransomware may encrypt the Computer's Master File Table (MFT) or entire hard drive. It is a denial-of-access attack that prevents computer users from accessing files since it is intractable to decrypt the files without the decryption key. Ransomware attacks are typically carried out using a Trojan that has a payload disguised as a legitimate file. Although advanced encryption algorithms are useful for effective protection of vital enterprise data, they have become tools for malicious attacks in the hand of cyber-criminals. Data protection is, therefore, under serious threat as hackers continue to utilize enhanced algorithms in ransomware attacks.

Digital extortion has significantly increased in the last six years as the number of online applications and services, and smart mobile devices continue to grow exponentially. The impact of ransomware has become so tremendous to the point that it is now rated as the biggest cyber scam to hit businesses. About 80% of ransomware attacks exploit vulnerabilities in Flash that firms should have patched. Destructive ransomware can spread by itself and hold entire networks (i.e. companies) hostage.

Ransomware attacks are shifting focus from individuals to organizations. For instance, the Hollywood Presbyterian Medical Center in the United States was attacked in February 2016. The health care organization was forced to shut down when it was hit by Crypto Ransomware. The malicious program encrypted the files on their databases, denying medical staff the access to patients’ health records. In another occasion, the Methodist Hospital in Henderson, Kentucky only managed to recover its patient records with backups after surviving a ransomware attack. Stolen administrative credentials were used to infect servers with ransomware variant dubbed ‘SamSam’. Active directory credentials were harvested to break into other servers. Overall, nearly half (46%) of firms have encountered ransomware attacks: 57% of medium-size organizations and; 53% of large organizations. Willingness to pay is surprisingly high. IBM found that 20% of executives would be prepared to pay over $40,000 each; 25% would shell out $20,000-$40,000 and; 11% would pay $10,000-$20,000.

Ransomware are now delivered as Word macros and PowerShell scripts. ‘Petya’ encrypted hard drive master boot record (MBR), as well as files, rendering computers completely unusable. The MBR is replaced with the malware’s own bootloader so that the ransom note can be displayed. The most common method of delivering ransomware is the phishing attack and it is not easily recoverable.

According to the Federal Bureau of Investigation (FBI), estimated losses of about one billion US dollars ($1 billion) were incurred to ransomware attacks in the year 2016. The boom recorded by this crime shows that a good number of victims eventually pay the ransom to have their data unlocked. Nearly 40 percent of ransomware victims paid the ransom. Three out of four ransomware gangs are willing to negotiate prices for decryption. On average, they will give a 29% discount on the fee initially demanded. Unfortunately, traditional preventive and reactive security measures are not adequate to handle the effect of ransomware attacks.

**Objectives:-**

The main objective is to design an application which will work as a File Encryptor and behaves like a file encryptor ransomware. The intention here is to use this application to secure our local file storage from unwanted access. We are aware of the loopholes presents in the operating systems whether it is windows or the Linux OS to bypass the user login when the machine is physically available and in some cases when it is turned on.

The application will also be useful to secure any personal data or the sensitive information to be disclosed when the system goes into the wrong hands, by stolen or by any other means.

The unintended person will be required a key to see the actual information of the files, and if someone tries to decrypt the files with the wrong keys, the files will be unrecoverable.

**Project Category:-**

The project domain is cryptography, when we make best use of cryptography for the data at rest to hide the personal information from the intruders.

We can also say that the special type of file encryptor which will let us choose which directory needs to be sourced to the application and then it will encrypt all the files of the same directory and of all the subdirectories.

**Overview of Research Methodology:-**

**1 PyCrypto:**

PyCrypto is a library, which provides secure hash functions and various encryption algorithms. It supports Python version 2.1 through 3.3.

**2 Crypto.Hash package**

Cryptographic hash functions take arbitrary binary strings as input, and produce a random-like fixed-length output (called digest or hash value).

It is practically infeasible to derive the original input data from the digest. In other words, the cryptographic hash function is one-way (pre-image resistance).

Given the digest of one message, it is also practically infeasible to find another message (second pre-image) with the same digest (weak collision resistance).

Finally, it is infeasible to find two arbitrary messages with the same digest (strong collision resistance).

Hash functions can be simply used as integrity checks. In combination with a public-key algorithm, you can implement a digital signature.

**3 Crypto.Cipher package**

The Crypto.Cipher package contains algorithms for protecting the confidentiality of data.

There are three types of encryption algorithms:

Symmetric ciphers: all parties use the same key, for both decrypting and encrypting data. Symmetric ciphers are typically very fast and can process very large amount of data.

Asymmetric ciphers: senders and receivers use different keys. Senders encrypt with public keys (non-secret) whereas receivers decrypt with private keys (secret). Asymmetric ciphers are typically very slow and can process only very small payloads. Example: PKCS#1 OAEP (RSA).

Hybrid ciphers: the two types of ciphers above can be combined in a construction that inherits the benefits of both. An asymmetric cipher is used to protect a short-lived symmetric key, and a symmetric cipher (under that key) encrypts the actual message.

**Scope of the solution:-**

The scope of the project is any stand alone machine running Linux OS, MAC OS or the Windows Operating System. Once the execution starts the application will encrypt all the files in the selected directory and it’s all the subdirectories.

**Tools and Technology Used:-**

To develop this application we are using **python 2.7** version on a **Kali Linux** machine. The tools we will be using the usual editor (nano) and sublime as well for better coding and design experience.

**Future scope and further enhancements of the project:-**

In the current scenario the application encrypts only the single machine on which it is being executed. It will also be able to encrypt any shared directories with respect to the permissions of the host machine.

Further it can be extended to work upon the machines available in the network – network level file encryption.

Also the key management framework can be improved. Currently we input one password and the application creates a valid key to encrypt all the files with the same key. To make the application run as quickly as possible without much user intervention, in future we can work upon the automatic key generation and management algorithms.

**Bibliography and Litrature survey:-**

URL and Links referred:

1. <https://www.symantec.com/security-center/writeup/2017-051310-3522-99>