global cyber liability insurance market is showing such strong growth. Yet, at the same time, if businesses are paying good money to cover their losses in the event of a breach, the last thing they want is a battle with the insurance company to collect in the event of a claim. That's where compliance process automation comes in, helping ensure that businesses with cyber-insurance actually receive a pay-out on their policy, if they are unfortunate enough to fall victim to an attack.

About the author

Michael Mittel is president of RapidFire Tools, a Kaseya company, and has 30 years of experience in the technology industry focusing on the software needs of small to mid-sized businesses.

References

1. 'Cyber security market is estimated to grow at a CAGR of 13.5% over the forecast years (2019 – 2027), with cyber attacks gaining traction as fastest growing type of crime across the globe, says Absolute Markets Insights'. GlobeNewswire, 6 Mar 2019. Accessed Jan 2020. www.globenewswire.com/news-release/2019/03/06/1749113/0/en/Cyber security-Market-is-Estimated-to-Grow-at-a-CAGR-of-13-5-over-the-forecast-years-2019-2027-with-Cyber attacks-Gaining-Traction-as-Fastest-Growing-Type-of-Crime-Across-the-Globe.html.
2. 'Cost of a Data Beach'. IBM/Ponemon Institute, June 2018. Accessed Jan 2020. www.ibm.com/security/data-breach.
3. 'Global cyber insurance market by type (stand-alone cyber insurance, and packaged cyber insurance), by application (financial institutions, retail and wholesale, healthcare, and others), by region and key companies – industry segment outlook, market assessment, competition scenario, trends and forecast 2019 – 2028'. Market.us. Accessed Jan 2020. https://market.us/report/cyber-insurance-market/.

A malicious activity monitoring mechanism to detect and prevent ransomware

Jinal Tailor

Ashish Patel

Ashish Patel and Jinal Tailor, Department of Computer Engineering, SVM Institute of Technology, India

In this digital world, security is the primary concern for users concerned about unauthorised access to their computer systems. At the same time, ransomware – a tool used by cyber criminals to encrypt the contents of a computer's file system without the permission or knowledge of the victim – is becoming increasingly common. Once the system is compromised – that is, the files are encrypted – the attacker forces users to pay a ransom, typically through online payment methods, to get a decryption key. Even if victims pay the ransom, there is no guarantee that the decryption key will be supplied, or access to their computer system restored.

In this article, we propose a solution that prevents such an attack and secures computers using a new mechanism that identifies an attack and takes the necessary steps to defeat it by creating a large dummy file. When a large dummy file is being encrypted by an attacker – which takes some time because of the file size – the remaining contents of the file system are made non-accessible to the malware. The proposed mechanism has been tested in a real-time environment and proved beneficial.

In an article published by Cyberscoop on 20 September 2017, package delivery company Fedex reported an estimated $300m loss due to ransomware known as NotPetya.[1] In 2014, US businesses and consumers experienced a loss of more than $18m because of ransomware called CryptoWall, according to the FBI's Internet Crime Complaint Centre.[2] In 2016, the damage reported was nearly $1.5bn due to ransomware attacks.[3,4] In 2017, cyber risk modelling firm Cyence estimated a loss of $4bn due to the WannaCry ransomware outbreak that attacked computers in more than 150 countries.

The WannaCry ransomware outbreak of 2017 was accidentally stopped in its tracks by a UK-based cyber security researcher, initially known simply by the name 'MalwareTech', but who was later revealed to be Marcus Hutchins.[5] He purchased a domain name to which the malware was connecting during the attack. This domain was intended for use as a killswitch in case the attacker wanted to prevent further spreading of the virus.[6]

These incidents make it clear that there is a serious security issue here that continues in spite of the large amounts organisations spend on security budgets.[7-10] At the same time, in the case of WannaCry, it is apparent that prevention is possible even while our computer systems are under attack.

Theoretical background

As mentioned, ransomware is a kind of encryption tool that encrypts computer files without the user's knowledge. It employs a backdoor route into a computer via malicious email links, email attachments, social media, USB devices, business applications and many other methods. Figure 1 explains the share of each possible vulnerability. Ransomware is spread through the use of email links (31%), email attachments (28%), applications other than email (24%), social media (4%), USB sticks (3%) and business applications (1%). Unrecognised ransom attacks contribute to 9% of incidents. There are two main types of ransomware attack: locker ransomware and crypto-ransomware. Locker ransomware denies or restricts access to a computer or any other resources. Crypto-ransomware blocks files and other records using encryption. In both types, the attacker asks for a ransom, generally via digital transfer, to regain access to the computer or files.[11]

Locker ransomware (computer locker) denies access to the computer or device. It is also designed to deny access to computing resources. Usually, it takes the form of locking the computer or device's user interface and then asking the user to pay a charge to restore admission to it. Locked computers are often left with limited capabilities, such as only allowing the user to work with the ransomware and make the ransom payment. This means access to the mouse might be disabled, and the keyboard functionality might be limited to numeric keys, allowing the victim to type numbers only to indicate the payment code.

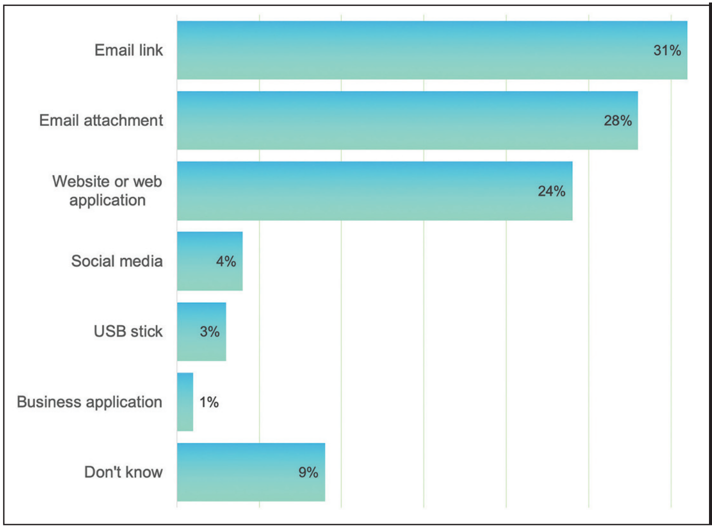


Figure 1: Applications through which ransomware enters into a computer system.

Crypto-ransomware (data locker) prevents access to files or data. This type of ransomware is designed to find and encrypt valuable data stored on the computer, making the data unavailable unless the user obtains the decryption key. As people's lives become increasingly digital, they are saving more essential data on their personal computers and devices.

Ransomware evolution

The first ransomware attack was PC Cyborg in December 1989. It used a combination of a symmetric key and an initialisation vector to encrypt the files present on the computer's drives, which was the first crypto form of ransomware. Figure 2 shows the evolution of ransomware.[12]

There is plentiful information available in the literature to determine the evolution of ransomware over time.[13-16] Fake anti-virus ransomware appeared in 2004 and again in 2005. These malware families included Performance Optimiser, SpySheriff and Registry Care. With the arrival of PGPcoder (aka Gpcode), the crypto-ransom family started to grow from 2005. PGPcoder deployed a custom encryption method for encrypting data. It spread wildly till 2008 and had many variants. In 2006, two other families started spreading – Cry zip and Archiveus. Archiveus used a protected folder to hide all the files. Cry zip searched for files with selected extensions and then located these encrypted files in a zipped folder.

The first major variation was Trojan-Ransom, which has been in use since 2010 and is a form of Master Boot Record (MBR) ransomware. Then 'boot.seftad.a' and (in 2011) 'boot-lock.b' came out with more attacks. This type of ransomware replaces the original MBR with its own code and locks the user from accessing the machine's services. It does not encrypt any files but displays the ransom message at computer boot-up time. In 2004, fake AV malware increased and it became particularly significant in 2005. Some of this malware took the form of 'performance optimiser' software, bogus anti-virus solutions and registry cleaning software. The malware operators offered paid solutions for non-existent machine problems, and these forms of scams were common on the Internet up until 2008.

Fake FBI ransomware arrived in 2011 with the Ransomlock family. Later in 2012, families like Reveton and ACCDFISA started spreading in the wild. These families displayed 'fine payment' notices from official-looking local law enforcement agencies. Many variants of Ransomlock and Reveton were seen in 2013. In 2014, new locker families like Virlock, Kovter and few advanced options of Ransomlock arrived.

When Cryptolocker, Cryptolocker 2, Ransomcrypt, Crilock and Dirty Decrypt arrived in 2013, crypto-ransomware became a challenging problem. Later in 2015, we witnessed new variants of Ransomcrypt, Cryptolocker, Vaultcrypt, Crypto Fortress,

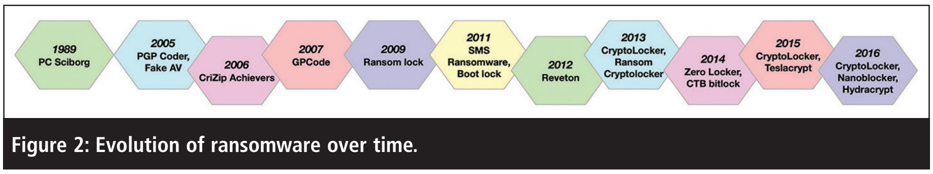


Figure 2: Evolution of ransomware over time.

Troldesh, TelsaCrypt, CryptoTor Locker, Ransomweb, Pclock, Cryptowall 3, Crypto blocker and Cryptowall 4. Cryptowall 3 used the Tor anonymity network for command and control (C&C) communication. Nearly all recent crypto-ransomware families are using very sophisticated encryption techniques. Recently, in 2016, new families of crypto such as PHPRansm.B, Locky, Ransom32, HydraCrypt, Cryptolocker.N and Cerber started to spread.

Targets of ransomware

There are three main types of ransomware target – home users, the business community and public agencies.

Home users often have sensitive information, files and documents that are personally valuable stored on the computer, such as college projects, photographs, videos and video game data. Despite these things being of value to users, home users are still unlikely to have a useful back-up strategy in place to successfully recover from events such as a fire or theft, let alone a crypto-ransomware attack.[17]

Business computers are also likely to contain sensitive data and documents of critical importance, such as customer databases, business plans, proposals, reports, source code, forms and tax compliance documents. Modern crypto-ransomware threats can enumerate all accessible drives, including local fileshare servers, and encrypt files on these as well. This means just a single crypto-ransomware infection can impact more than one system.[18]

Public agencies such as educational institutes, healthcare organisations, local government and even law enforcement entities are not excluded from the attention of these cyber criminals and, in some cases, they may be specifically targeted.[19]

General guidelines are useful to protect computer systems against ransomware attacks.[20-25] The first point to remember is to back up work regularly and encrypt the back-up before storing on any device. Users should be careful with unsolicited email attachments and they must not use super-user privileges until required. They must also be aware of the dangers of hyperlinks. They need to maintain an updated firewall and use the latest anti-virus and anti-malware programs. Also, computer users should never follow links on the Internet that they don't know and trust.

Monitoring mechanism

To detect and prevent a ransomware attack, we designed an attack and then resolved the problem. The mechanism is designed using various modules. Each module consists of several phases. The solution successfully attacked the system and then was subsequently prevented using the proposed approach.

Phase 1: Generate ransomware. This phase generates a module to create a new strain of ransomware. The ransomware attacks the system using websites, USB devices and advertisements. It gets access through the network using a number of malicious activities, such as clicking a link, notifications and phishing emails.

Phase 2: Attack by ransomware on file or directory. After getting access to the system, the ransomware can encrypt any file, directory or an entire system and displays a ransom note.

Phase 3: Verify encryption by ransomware. At the end of a successful attack, the proposed system checks the details of the encrypted contents. For example, if the file is not accessible, there is data loss or there are restricted rights, these would indicate a damaged system. MD5 (Message-Digest algorithm 5) is used for the cryptographic hash function. The idea behind this algorithm is to take up random data (text or binary) as an input and generate a fixed size hash value as the output.

Phase 4: Apply the attack over a LAN. When the compromised system is a part of a local area network (LAN), it finds another system and encrypts the shared files.

Phase 5: Identification of an attack using a ransomware detection module. Ransomware has mainly two types of attack – crypto-ransomware (data locker) or ransom locker (computer locker). Crypto-ransomware prevents access to files or data, and a ransom locker denies access to the computer or device. The module identifies which type of attack is in progress.

Phase 6: Ransomware prevention module protects the system. If one file is affected in the system, the solution provides protection for other data to assure minimum damage. Once the modified file is found in the specific

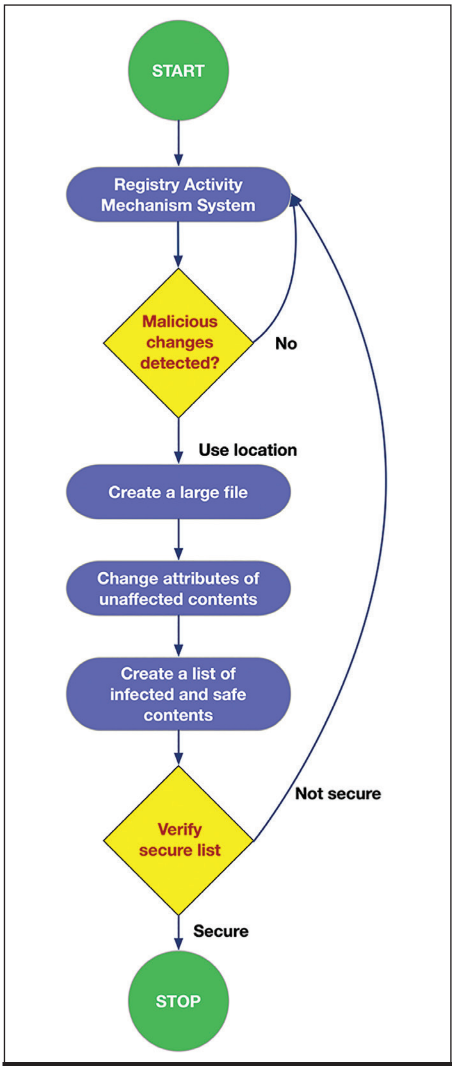

START
Registry Activity Mechanism System
Malicious changes detected?
No
Use location
Create a large file
Change attributes of unaffected contents
Create a list of infected and safe contents
Not secure
Verify secure list
Secure
STOP

Figure 3: Proposed solution to mitigate a ransomware attack.

folder, it generates the list of files with the modifications carried out in that folder. The following steps are applied to counter the ransomware attack:

1. Create a large file to keep the attacker busy with encryption.
2. Identify the encryption algorithm.
3. Change the attributes of remaining data.
4. Create the infected files list.
5. Create the secure files list.

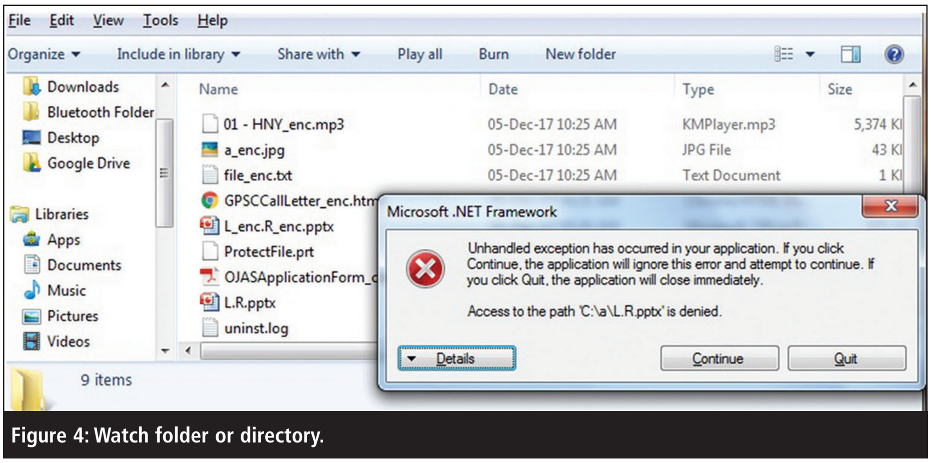
After applying the above procedure, the system does not allow the execution of malicious files. The user-defined threshold works as a trigger and can be used to block any unwanted modification. For example, if the attacker tries to encrypt files in a folder one-by-one and the threshold is set to two, after two encryptions, the protection solution creates a large file. The attacker remains busy processing the large file (thousands of bytes): meanwhile, the solution changes the attributes of the remaining unaffected files, thus preventing further spread of the attack.

Phase 7: Verify prevention module. Finally, the proposed solution checks for effectiveness by examining the remaining files.

Implementation and results

The proposed solution was implemented and tested using Visual C# coding on a Windows platform. There are four modules that stop the spreading of a ransomware attack.

Module 1: Watch folder/directory. This module detects any change in the registry of directory contents. We have used a threshold value for valid changes. If a process tries to change registry values of any file beyond the threshold, it is identified as a possible malicious activity (see Figure 4). The tasks provided by the module include: provide folder/directory path, include subdirectories; use watcher; notify filters; notify creation time; notify directory name, filename, last access, last write, security and size.

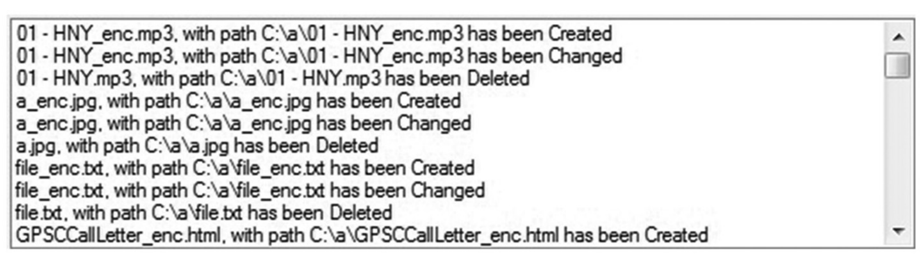


Name	Date	Type	Size
01 - HNY_enc.mp3	05-Dec-17 10:25 AM	KMPlayer.mp3	5,374 KI
a_enc.jpg	05-Dec-17 10:25 AM	JPG File	43 KI
file_enc.txt	05-Dec-17 10:25 AM	Text Document	1 KI
GPSCCallLetter_enc.htm			
L_enc.R_enc.pptx			
ProtectFile.prt			
OJASApplicationForm_c			
L.R.pptx			
uninst.log			

Unhandled exception has occured in your application. If you click Continue, the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.

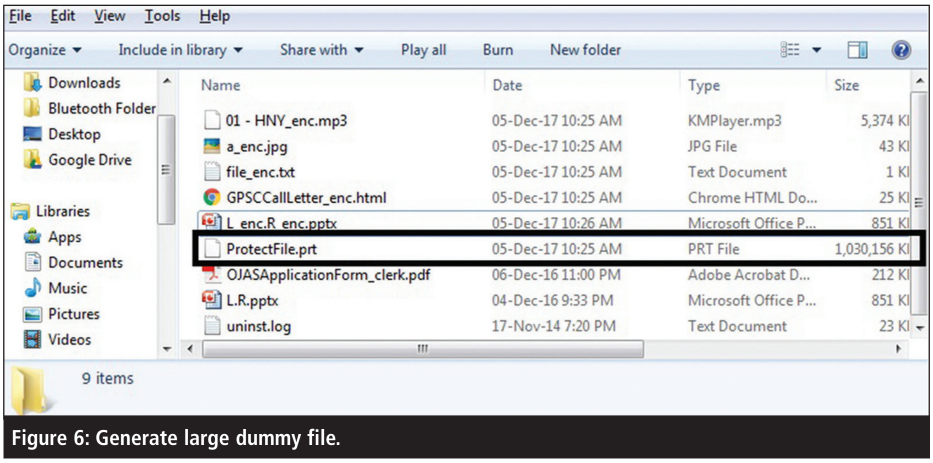
Access to the path 'C:\a\L.R.pptx' is denied.

Figure 4: Watch folder or directory.



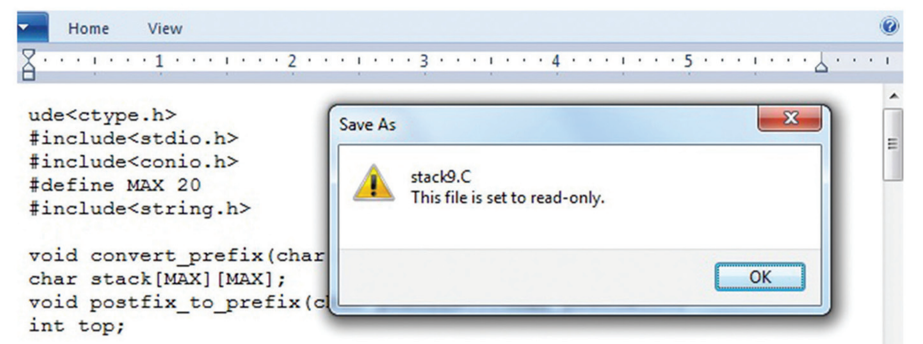
```
01 - HNY_enc.mp3, with path C:\a\01 - HNY_enc.mp3 has been Created
01 - HNY_enc.mp3, with path C:\a\01 - HNY_enc.mp3 has been Changed
01 - HNY.mp3, with path C:\a\01 - HNY.mp3 has been Deleted
a_enc.jpg, with path C:\a\a_enc.jpg has been Created
a_enc.jpg, with path C:\a\a_enc.jpg has been Changed
a.jpg, with path C:\a\a.jpg has been Deleted
file_enc.txt, with path C:\a\file_enc.txt has been Created
file_enc.txt, with path C:\a\file_enc.txt has been Changed
file.txt, with path C:\a\file.txt has been Deleted
GPSCCallLetter_enc.html, with path C:\a\GPSCCallLetter_enc.html has been Created
```

Figure 5: Generate a list of infected files.



Name	Date	Type	Size
01 - HNY_enc.mp3	05-Dec-17 10:25 AM	KMPlayer.mp3	5,374 KI
a_enc.jpg	05-Dec-17 10:25 AM	JPG File	43 KI
file_enc.txt	05-Dec-17 10:25 AM	Text Document	1 KI
GPSCCallLetter_enc.html	05-Dec-17 10:25 AM	Chrome HTML Do...	25 KI
L_enc.R_enc.pptx	05-Dec-17 10:26 AM	Microsoft Office P...	851 KI
ProtectFile.prt	05-Dec-17 10:25 AM	PRT File	1,030,156 KI
OJASApplicationForm_clerk.pdf	06-Dec-16 11:00 PM	Adobe Acrobat D...	212 KI
L.R.pptx	04-Dec-16 9:33 PM	Microsoft Office P...	851 KI
uninst.log	17-Nov-14 7:20 PM	Text Document	23 KI

Figure 6: Generate large dummy file.



```
ude<ctype.h>
#include<stdio.h>
#include<conio.h>
#define MAX 20
#include<string.h>

void convert_prefix(char
char stack[MAX][MAX];
void postfix_to_prefix(c
int top;
```

stack9.C
This file is set to read-only.

Figure 7: Change attributes of remaining contents.

Module 2: Generate list of infected files. The second module uses the information gathered in the first module to generate a list of infected files. The user is informed about suspicious activity and presented with the list of infected files. The user can take appropriate action – eg, by intentionally changing the list within the predefined time frame. If the time frame has elapsed, the activity is considered as malicious or unwanted (Figure 5). The tasks provided by the module are: watching for a change event; generating the user defined string; and checking the count for the threshold.

Module 3: Generate large random

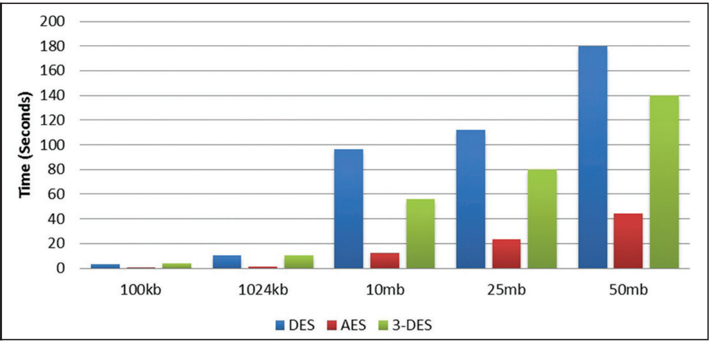


Figure 8: Time comparison – encryption using DES, AES and 3-DES.

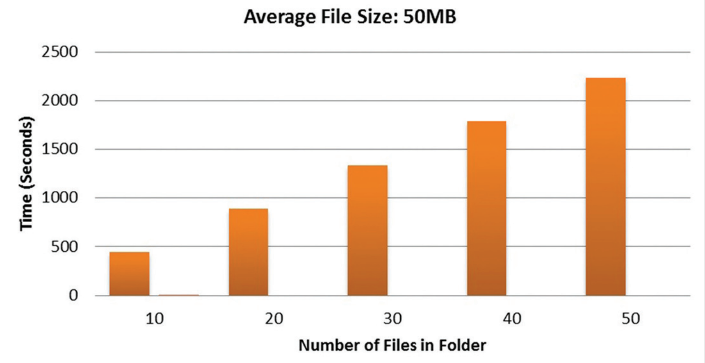


Figure 9: Comparison of the different number of 50MB files.

file. Once the mechanism identifies an attack, it generates a large file – eg, 10GB – at the location of the attack. The intention here is to slow down the attack to take the necessary actions to stop further modification of the file system (Figure 6).

Module 4: Change attributes of remaining contents. When the attacker process is busy with the encryption/modification of the large dummy file, the proposed solution changes the attributes of the remaining contents. It makes the attacker unable to perform further modifications in the system (Figure 7).

The above four modules were implemented and tested for efficiency. We found the solution very useful. The mechanism stops the spreading of the attack by setting a user-defined threshold. After crossing the set limit, the solution creates a large dummy file to keep the attacker busy. Utilising the extra time provided to the system, the solution changes the attributes of the remaining files and directories. Further modification in the system by the attacker is thus not possible.

We assumed the ransomware uses DES (Data Encryption Standard), AES (Advanced Encryption Standard) or the 3-DES algorithm to encrypt the data on the compromised system. We analysed the time taken for all three algorithms, of which AES took the least time for the encryption process (Figure 8).

Figure 9 shows the time consumed for encrypting files. Larger file sizes require more time for encryption, allowing our proposal to prevent further damage. The result confirms that creating a dummy file is a feasible solution against a ransomware attack.

Conclusion

The economy of any country or organisation is greatly affected by malicious electronic activities such as ransomware attacks. Following an attack, it is hard to deal with the aftermath; thus, prevention becomes extremely important. In this work, we first created the ransomware attack and then provided a solution to protect the computer system from significant damage.

The proposed solution can detect such an attack and safeguard computer systems. We demonstrated the use of different encryption algorithms used by ransomware. The time used to encrypt a large file is higher compared to ordinary files typically found on computer systems. A large dummy file is generated to slow down the attack.

Meanwhile, remaining files that have not so far been affected are made secure by changing their attributes. The solution was tested in a real-time environment to determine its effectiveness. By using this approach, although a small number of files cannot be recovered, we may secure other essential contents.

About the authors

Ashish Patel is an assistant professor in the department of computer engineering at the SVM Institute of Technology, India. He is a research fellow at Pandit Deendayal Petroleum University. He is also a certified Microsoft professional and a life member of the Institution of Engineers and Indian Society for Technical Education. His research interests include ambient assisted living, computer security and networking. He has published more than 20 research papers in various international journals and conferences.

Jinal Tailor is a certified professional in creating strong passwords, mobile device security, security awareness training, CEO fraud and social engineering. She has completed a Master of Engineering in Information Technology at the SVM Institute of Technology. She is working on Open Web Application Security Project (OWASP) web application security risks in ASP.NET. Her areas of interest include ransomware attacks, ethical hacking and cyber security.

References

1. Shoorbajee, Zaid. 'Fedex attributes $300 million loss to NotPetya ransomware attack'. Cyberscoop.com, 20 Sep 2017. Accessed Aug 2019. www.cyberscoop.com/fedex-attributes-300-million-loss-notpetya-attack.
2. J Schwartz, Mathew. 'FBI alert: $18 million in ransomware losses, ongoing cryptowall attacks lead to major expenses'. Bank Info Security, 26 Jun 2015. Accessed Aug 2019. www.bankinfosecurity.com/fbi-sees-18m-ransomware-fallout-a-8355.
3. Berr, Jonathan. 'WannaCry ransomware attack losses could reach $4 billion'. CBS News.com, 16 May 2017. Accessed Aug 2019. www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses.

4. Kolodenker, Eugene; Koch, William; Stringhini, Gianluca; Egele, Manuel. 'Paybreak: defence against cryptographic ransomware'. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pp.599-611, ACM, 2017.
5. Mohurle, Savita; Patil, Manisha. 'A brief study of WannaCry threat: Ransomware attack 2017'. International Journal of Advanced Research in Computer Science, 8(5), 2017.
6. Khomami, Nadia; Solon, Olivia. 'Accidental hero halts ransomware attack and warns: this is not over'. The Guardian, 13 May 2017. Accessed Aug 2019. www.theguardian.com/technology/2017/may/13/ accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber attack.
7. Power, Richard. 'Tangled Web: Tales of digital crime from the shadows of cyberspace'. Macmillan Press, 2000.
8. Markoff, John. 'Worm infects millions of computers worldwide'. The New York Times, 22 Jan 2009. Accessed Dec 2019. www.nytimes.com/2009/01/23/technology/Internet/23worm.html.
9. Schneier, Bruce. 'Secrets and Lies: digital security in a networked world'. John Wiley & Sons, 2011.
10. Silver-Greenberg, Jessica; Goldstein, Matthew; Perlroth, Nicole. 'JP Morgan Chase hack affects 76 million households'. New York Times, 2 Oct 2014. Accessed Dec 2019. https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber security-issues/.
11. O'Gorman, Gavin; McDonald, Geoff. 'Ransomware: A growing menace'. Symantec Corporation, 2012. Accessed Dec 2019. www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf.
12. Richardson, Ronny; North, Max. 'Ransomware: Evolution, mitigation and prevention'. International Management Review, 13(1):10, 2017.
13. Kharraz, Amin; Robertson, William; Balzarotti, Davide; Bilge, Leyla; Kirda, Engin. 'Cutting the gordian knot: A look under the hood of ransomware attacks'. In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, pp.3-24. Springer, 2015.
14. Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin RB Butler. 'Cryptolock (and drop it): stopping ransomware attacks on user data'. In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS), pp.303-312. IEEE, 2016.
15. Andronio, Nicol´o; Zanero, Stefano; Maggi, Federico. 'Heldroid: Dissecting and detecting mobile ransomware'. In International Symposium on Recent Advances in Intrusion Detection, pp.382-404. Springer, 2015.
16. Kharaz, Amin; Arshad, Sajjad; Mulliner, Collin; Robertson, William; Kirda, Engin. 'UNVEIL: A large-scale, automated approach to detecting ransomware'. In 25th USENIX Security Symposium, pp.757-772, 2016. Accessed Dec 2019. www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kharaz.
17. Mercaldo, Francesco; Nardone, Vittoria; Santone, Antonella. 'Ransomware inside out'. In 2016 11th International Conference on Availability, Reliability and Security (ARES), pp.628 – 637, IEEE, 2016.
18. Mansfield-Devine, Steve. 'Ransomware: taking businesses hostage'. Network Security, Oct 2016, pp.8-17. Accessed Dec 2019. www.sciencedirect.com/science/article/pii/S1353485816300964.
19. Everett, Cath. 'Ransomware: to pay or not to pay?' Computer Fraud & Security, Apr 2016, pp.8-12. Accessed Dec 2019. www.sciencedirect.com/science/article/pii/S1361372316300367.
20. Brewer, Ross. 'Ransomware attacks: detection, prevention and cure'. Network Security, May 2016. Accessed Dec 2019. www.sciencedirect.com/science/article/pii/S1353485816300861.
21. Zavarsky, Pavol; Lindskog, Dale et al. 'Experimental analysis of ransomware on Windows and Android platforms: Evolution and characterization'. Procedia Computer Science, 94, pp.465-472, 2016.
22. Balaban, David. '22 ransomware prevention tips'. Tripwire, 24 Jan 2016. Accessed Sep 2019. www.tripwire.com/state-of-security/security-data-protection/cyber%20security/22-ransomware-prevention-tips/.
23. Tailor, Jinal; Patel, Ashish. 'A comprehensive survey: ransomware attacks prevention, monitoring and damage control'. International Journal of Scientific Research, Jun 2017.
24. 'How to protect your networks from ransomware'. Technical Guidance Document, US Department of Justice, 2019. Accessed Sep 2019. www.justice.gov/criminal-ccips/file/872771/download.
25. Luo, Xin; Liao, Qinyu. 'Awareness education as the key to ransomware prevention'. Information Systems Security, 16(4), pp.195-202, 2007.