Crypted_Pony Ransomware- A Mysteries Entity in Cyber World

Krunal A. Gandhi
Assistant Professor, I.T Department
Laxmi Institute of Technology
Sarigam, Valsad

Viral D. Patel
Assistant Professor, I.T Department
Laxmi Institute of Technology
Sarigam, Valsad

Siba Ram Raut
Assistant Professor, C.S.E Department
Laxmi Institute of Technology
Sarigam, Valsad

Kavita A. Joshi
Assistant Professor, I.T Department
Laxmi Institute of Technology
Sarigam, Valsad

ABSTRACT
In today's cyber world, it is difficult to trap the hackers and for the innocent users who are unaware of this kind of crimes can be easily trapped. The world had already seen the effect of ransomware where professionals were also trapped and company lost huge amount of money in terms of bit-coins. So in this study paper, the post effects of ransomware are discussed.

Keywords
Ransomware, bitcoins, Crypted_pony, Payment, Education

1. INTRODUCTION
1. **Ransomware**: It is a malware which is used by attackers by covertly installing into victim's system through mail attachment (most of the time) and after installation it will encrypt all the files of the victim's system and then demands a ransom payment (in bit-coins) in return for the decryption key which is required to decrypt the encrypted file. Not only can encrypt the files on victim's system but it is smart enough that it will travel across the network and encrypt any files which are located both on mapped and unmapped drive. This can lead to critical situation whereby one user's infection brings entire department or an organization to a halt. The first known ransomware was coded in 1989. Thus, this paper main objective is to aware all the peoples who uses internet nowadays and maybe they might encounter it in future [1].
2. **Bit-Coins**: It is the form of crypto-currency; it is a virtual currency which does not have physical representation. The main benefits of bit-coins are they are stored in anonymous digital wallets. It can be transferred around the globe via web. It can be paid from anywhere, to anywhere with total anonymity. It is commonly abbreviated as BTC [1].
3. **TOR**: It is an anonymity network, which stands for "The Onion Router". It is developed by considering the anonymity over internet traffic as prime objective. It uses a special browser that is configured to use a worldwide connected network of relays. All traffic is encrypted and the network was designed to hide the origin and ending destination of the traffic. It also using onion domain. You need TOR browser to use onion domain websites [1].

2. WORKING OF RANSOMWARE
There are steps of being affected by the one of the six ransomwares.

How Ransomwares Works?

1. End user receives an email that appears to be from their boss. It contains a URL to a SaaS application such as Salesforce, Workday or ZenDesk.
2. The link opens a browser window and directs the user to a website that seems legitimate. It's actually a landing page for an exploit kit hosted in a.co.cc top level domain (TLD).
3. Upon loading the page, the web server hosting the exploit kit begins communicating with the victim machine. The server sends requests about versions of software such as Java to find a vulnerable version for which the kit has an exploit.
4. When a vulnerable version is confirmed, the kit attempts to exploit the vulnerability. Once successful, the exploit kit pushes down a malicious .EXE file – let's call it "ransomware.exe." The malicious binary on the victim machine then attempts to execute.
5. From this beachhead, the binary spawn's child processes, including vssadmin.exe (shadow copy), to delete existing shadows on the victim machine and create new ones to hide in. The attacker does this to limit the possible recovery of files by the victim using Shadow Copies that Windows stores on a system.
6. The binary uses a PowerShell executable to propagate copies of itself throughout the filesystem. The executable also searches the filesystem for files of specific extensions and begins to encrypt those files.
7. The powershell.exe child process creates three copies of the originating malware binary, first in the AppData directory, next in the Start directory, and finally in the root C:\ directory[1]

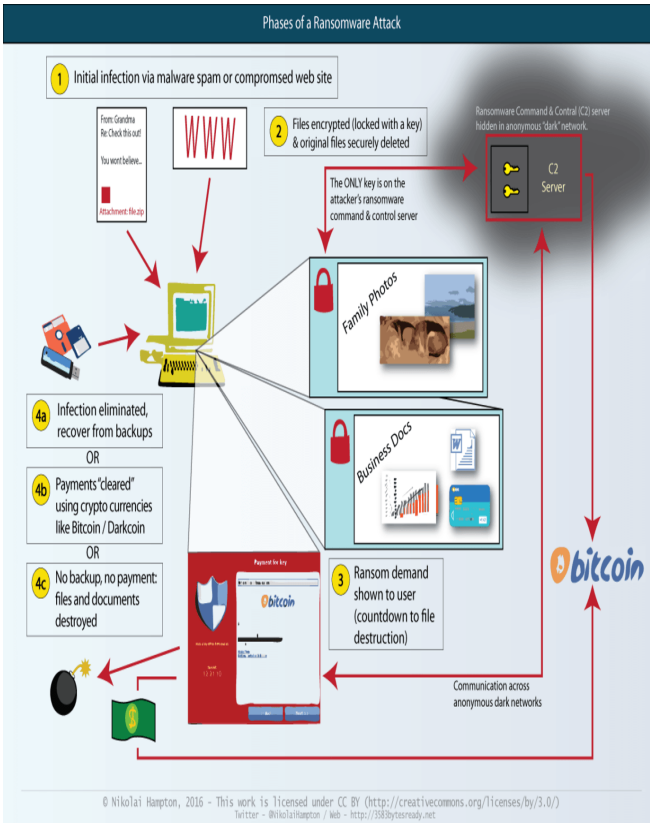

Fig 1. Working of Ransomware

These copies are used in conjunction with the registry modifications to restart the malware upon reboot and login events.

8. After encrypting the victim's files, the malware sends the encryption key and other host- specific information back to the command-and-control server.

9. The server then sends a message to the victim. This could be a simple "alert user of encryption and directions on paying us." It could also include directions that result in downloading additional malware, which enables the attacker to steal credentials from the victim as well.

To amplify the victim's distress, ransomware often includes a countdown clock with a deadline for paying the ransom – or else the decrypt key will be destroyed, eliminating any chance of recovery.

Paying the ransom often means the attacker will unlock the victim's machine or provide the key to decrypt files. However, it rarely means the originating malicious binary, "ransomware.exe" in the case above, has been removed. That will require IT and SecOps support.

And the attack doesn't necessarily end there. Attackers often load additional malware on a user's machine, allowing them to harvest personal information, intellectual property, and credentials to sell for additional revenue.[2]

3. CRYPTED_PONY

3.1 Introduction

Crypted Pony ransomware virus is one of many crypto-demanding threats that use the AES encryption method for the file locking process. It mainly focuses on file encryption and demanding the 0,5 BTC for the alleged decryption key. Typically ransomware type threats mark encoded files, in this case with an appendix in a pattern **crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx**.[2]

The virus also adds a long-named ransom note too, called **IF_YOU_WANT_TO_GET_ALL_YOUR_FILES_BACK_PLEASE_READ_THIS.HTML.** The ransom note contains a ransom message that aims to convince victims to pay ransom in order to get their files to work once again.

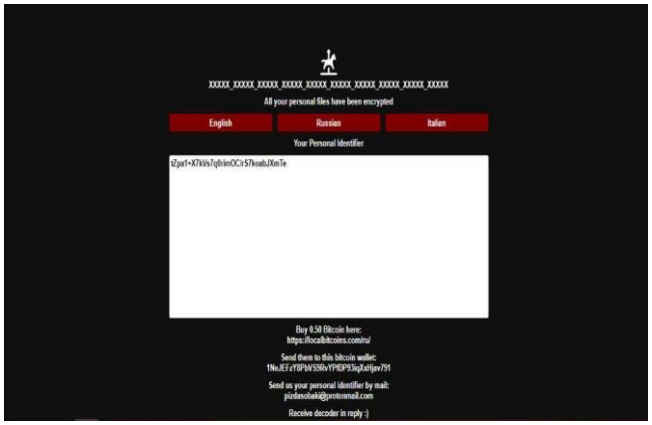

Fig 2. Crypted_Pony Ransom Message

Crypted Pony ransomware virus is also called other names like Pony ransomware, Pony_XXX ransomware and all those names come from the file extension that victims' files get after encryption process. The appendix in a pattern .crypted_pony_test_build_xxx_xxx_xxx_xxx_xxx marks files that are no longer usable because encryption is the process when the original code of the file gets changed.[1]

Additionally, when analyzing the main ransomware payloads and executables from malware samples, various researchers that discover these threats call this particular virus 05ntoar0 ransomware. Executable files associated with the attack at the time of writing: 05ntoar0.exe; pony.exe; chrome.pif.exe, or even any other random file name.

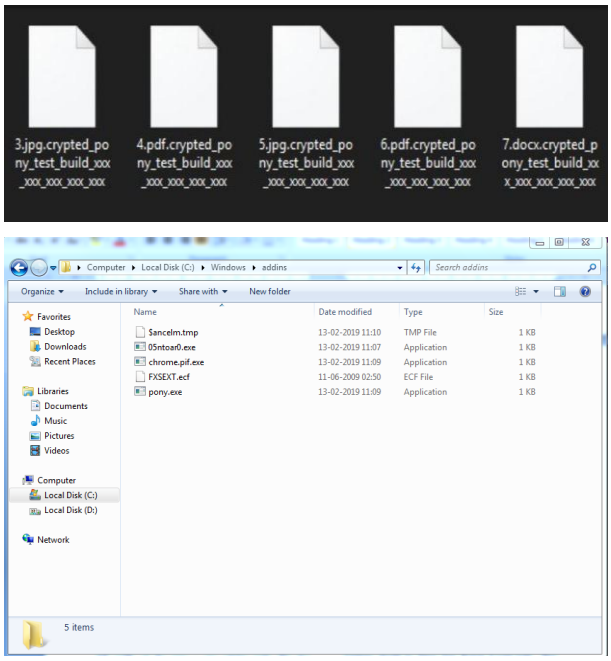

Fig 3. Encrypted File Names

In addition to this, the .crypted_pony virus may also interfere with the Run and RunOnce registry keys of Windows, located in the following directories [3]:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

In addition to this, the .crypted_pony ransomware may also delete the shadow copies on the computers, compromised by it by obtaining administrative privileges and running the following commands in Windows Command Prompt as an administrator.

sc stop VVS

sc stop wscsvc

sc stop WinDefend

sc stop wuauserv

sc stop BITS

sc stop ERSvc

sc stop WerSvc

cmd.exe /C bcdedit /set {default} recoveryenabled No

cmd.exe /C bcdedit /set {default} bootstatuspolicy ignoreallfailures

C:\Windows\System32\cmd.exe" /C vssadmin.exe Delete Shadows /All /Quiet

4. HOW TO PROTECT?

There are various steps to remove this ransomware and some of them are listed below:

1) Reboot your pc in safe mode with networking.

- Click *Start → Shutdown → Restart → OK*
- When your computer becomes active, start pressing F8 multiple times until you see the Advanced Boot Options window.
- Select Safe Mode with Networking from the list.

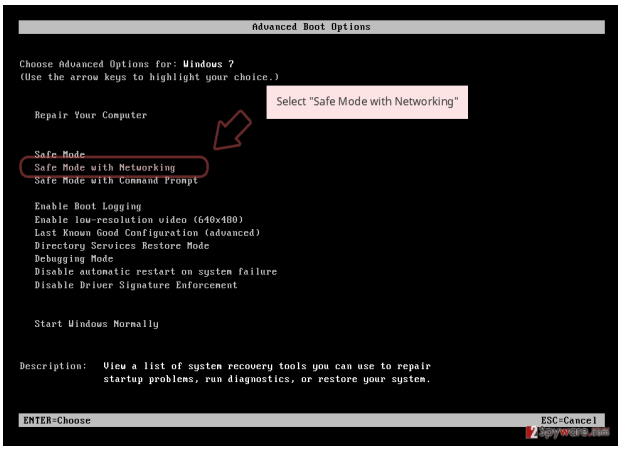

Fig 4. Protection Trick 1

- Once the Command Prompt window shows up, enter **cd restore** and click Enter.
- Now type **rstrui.exe** and press Enter again.
- When a new window shows up, click Next and select your restore point that is prior the infiltration of Crypted Pony. After doing that, click Next.

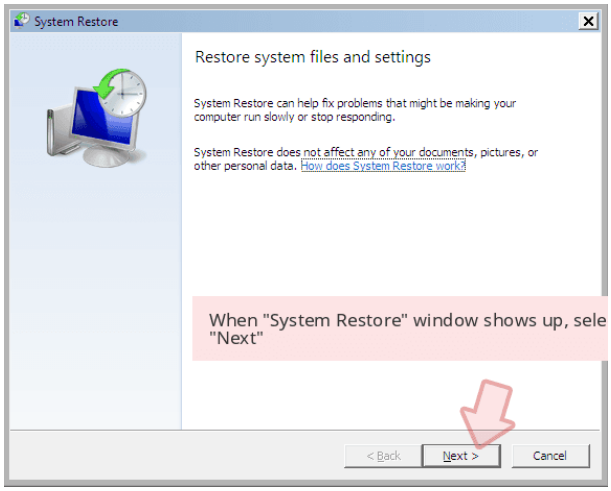

Fig 4. Protection Trick 2

- Now click Yes to start system restore.

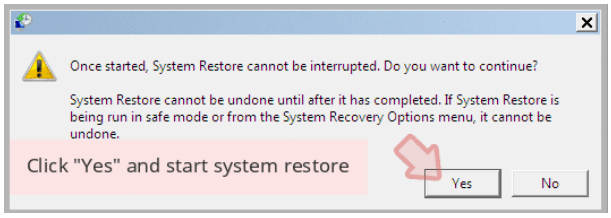

Fig 4. Protection Trick 3

2) **From Registry**.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msseces.exe "Debugger" = 'svchost.exe'

HKEY_LOCAL_MACHINE\SOFTWARE\.crypted_pony Files Virus

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\virus name

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings "WarnOnHTTPSToHTTPRedirect" = '0′

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore "DisableSR " = '1′

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msascui.exe "Debugger" = 'svchost.exe'

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "xas"

HKEY_CURRENT_USER\Software\.crypted_pony Files

ViruS.

3) From Task manager.[2]

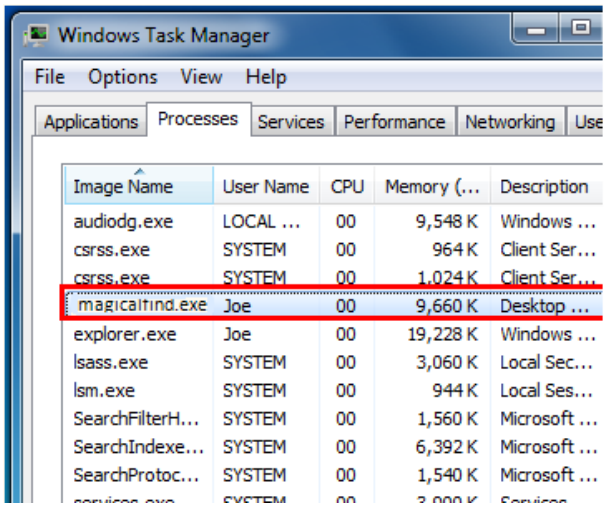

Fig 4. Protection Trick 4

4) **Remove From Google Chrome**.

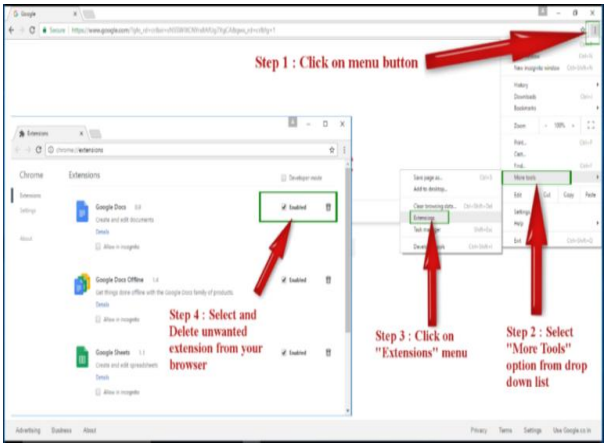

Fig 4. Protection Trick 5

4.1 Tips to Prevent from Crypted pony in Future

- Always select Custom Installation while installing any new application.
- Uncheck any hidden options which attempt to secretly install.
- Check Windows Firewall security and turn it on.
- Use a powerful anti-virus program and keep it updated.
- Scan all downloaded files, applications or email attachments before opening.
- Never download cracked software, themes and similar products.
- Do not visit Torrent/adult / porn websites to stay safe online.
- Keep backup of all your important files and data.
- Create a system restore point for security purpose.

5. ANALYSIS

1) PAYMENT: From the survey results and the literature, it can be concluded that only a very small portion of the victims actually pays the attacker. There are most likely multiple reasons for this, such as a deep distrust of the instructions to download the TOR browser [REF] and buy Bitcoins (both technologies with a seedy reputation). Furthermore, it seems likely that a significant portion of the victims do not possess the necessary technical skills to install and manage these technologies, even if they did have the intention to pay.approach' in the hope of reaching some viable targets and, in process, create a lot of collateral damage. The role of Internet is also a pressing threat for easier spread of ransomware.[1]

2) TRANSFER: Victims which can, from the attacker's point of view, be seen as viable targets are a small subset of the total group of victims. Viable targets are victims who have lost important data, require the technical skills to make a payment and are also willing to do so. It can therefore be assumed that most ransomware distributors use a 'shotgun.[1]

6. CONCLUSION

This paper will spread the awareness about ransomware, especially for the common peoples. With the increasing use of internet, ransomware can be easily spread. In industries, due to the latest attack the lack of awareness among the employees is confirmed. Lastly, from the possible solutions will ensure that an internet user will stay safe and far away from ransomware.

7. FUTURE SCOPE

As this paper will provide enough countermeasures for the ransomware, but in this fast internet world new attack may introduce at any moment. So, in future as the new attack introduces we will back with the countermeasures of it too.

8. REFERENCES

[1] Gandhi Krunal A., Patel Viral D. " Ransomware- A New Era of Cyber Attack https://www.ijcaonline.org/archives/volume168/number3/krunal-2017-ijca-914446.pdf

[2] Remove .crypted_pony Files Virus from Windows 7 : Clean .crypted_pony Files Virus.[online]: https://www.stepstoremovevirus.com/remove-crypted_pony-files-virus-from-windows-7-clean-crypted_pony-files-virus

[3] crypted_pony Files Virus (Pony) – How to Remove Itby Ventsislav Krastev [online]: https://sensorstechforum.com/remove-pony-ransomware/

[4] G. O'Gorman and G. McDonald, "Ransomware: a growing menace," Symantec Corporation, 2012.

[5] B. N. Giri, N. Jyoti and M. AVERT, "The Emergence of Ransomware," AVAR, Auckland, 2006.

[6] J.-L. Richet, "Extortion on the internet: the rise of cryptoransomware.," Harvard , 2016. International Journal of Computer Applications (0975 – 8887) Volume 168 – No.3, June 2017 41

[7] A. Bhardwaj, G. Subrahmanyam, V. Avasthi and H. Sastry, "Ransomware: A rising threat of new age digital extortion.," in arXiv preprint arXiv:1512.01980, 2015.

[8] X. Luo and Q. Liao, "Awareness education as the key to ransomware prevention.," Information Systems Security,

vol. 16, no. 4, pp. 195-202, 2007.

[9] A. Gazet, "Comparative analysis of various ransomware virii," Journalin computer virology, vol. 6, no. 1, pp. 77-90, 2010.

[10] M. Fossi, G. Egan, K. Haley, E. Johnson, T. Mack, T. Adams, J.Blackbird, M. Low, D. Mazurek, D. McKinney and P. Wood, "Symantec internet security threat report trends for 2010," Symantec, 2011.

[11] B. Foster and Y. Lejins, "Ehealth security Australia: The solution lies with frameworks and standards.," 2013.

[12] J. C. a. E. A. B. Hernandez-Castro, "UK has little to be proud of assurvey reveals sorry state of European cybersecurity," University of Kent, 2015. [Online]. Available: https://kar.kent.ac.uk/51071/1/uk-haslittle-tobe-proud-of-as-survey-reveals-sorry-state-of european cyber security-37505. [Accessed 2016].

[13] K.-K. R. Choo and R. G. Smith, "Criminal exploitation of online systems by organised crime groups," Asian journal of criminology, vol. 3, no. 1, pp. 37-59, 2008.

[14] K. Gradon, "Crime science and the internet battlefield: Securing the analog world from digital crime.," Security & Privacy, IEEE, vol. 11, no. 5, pp. 93-95, 2013.

[15] T. Zhang, H. Antunes and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework.," Internet of Thing