FILELESS RANSOMWARE(S)

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

TABLE OF CONTENTS

INTRODUCTION TO FILELESS RANSOMWARES

Highlight the key threats associated with Fileless Ransomware attacks and the occurrence of this event which caused financial data loss to many organization

RESEARCH WORK ON FILELESS RANSOMWARES

Research for the work performed for making of Fileless Ransomware,

ANTI DOT PREPARED FOR RANSOMWARES

A tool that will help organization to secure there Servers from ransomware attacks

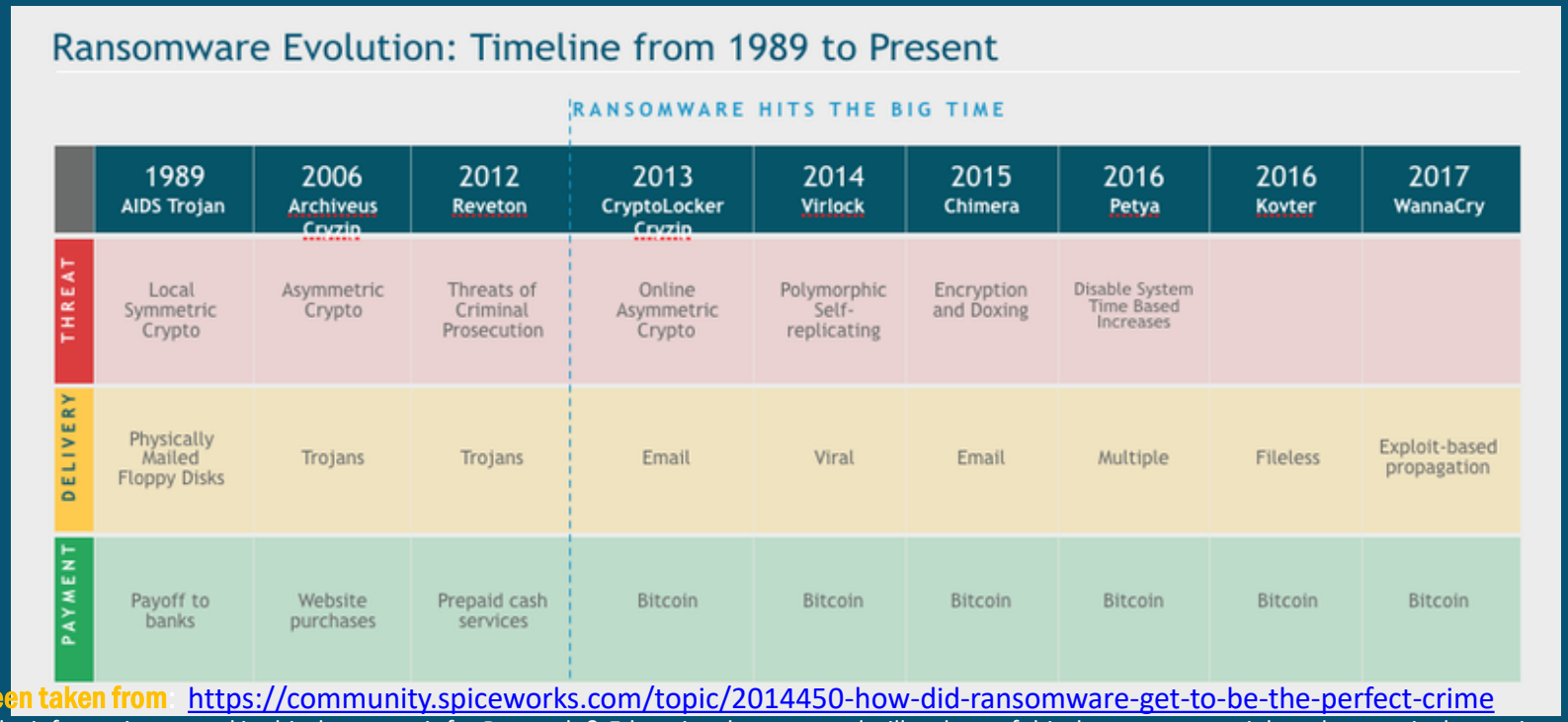
LIMITATION & CHALLANGES

Limitation & challenges which are currently not covered in this tool, continuous research will help to mitigate those risk associate with Ransomwares.

INTRODUCTION TO FILELESS RANSOMWARES

INTRODUCTION TO FILELESS RANSOMWARES

Fileless malwares are those malwares which works without transferring the suspicious files in the system. Organized crime groups are expanding their operations to reach more victims and extract more ransoms. Meanwhile, security measures are getting better at detecting and blocking ransomware, forcing cybercriminals to constantly develop new techniques to evade detection. One of these advanced techniques involves “fileless”, where malicious code is either embedded in a native scripting language or written straight into memory using legitimate administrative tools such as PowerShell, without being written to disk.



Source image has been taken from: https://community.spiceworks.com/topic/2014450-how-did-ransomware-get-to-be-the-perfect-crime

RESEARCH WORK ON FILELESS RANSOMWARES

RESEARCH WORK ON FILELESS RANSOMWARES

There are several test that were conducted to make a File based malware into Fileless, this would allow our assessment to be carried out not only for file based Ransomwares but for Fileless ransomware as well.

STEPS	1	2	3	4	5	6
	User receive Malicious email attachment, drive by download URL. Victim user clicks link or opens document, Website downloads legitimate Flash, and Flash launches PowerShell.	Once the PowerShell script is downloaded & executed it requires a Decryption key to undo the process of Files Encryption.	Executing through cmd and operating only in memory PowerShell can download malware, contact C&C, encrypt files on computer, delete backups etc.	The Ransomware then encrypt all the files associated with an Extension it can be .PDF, .PPTX, .XLSX, .DOCX, .ZIP To .PDF.Lock, .PPTX.Lock, .XLSX.Lock etc.	If an organization really want to have those file to be recovered from Ransomware they pay ransom by sending money through Bitcoin as instructed in the message	Depend upon the attacker, if they transfer the decryption key to the same machine and execute it through process then decryption will take place, otherwise money & data both lost

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

ANTI DOT PREPARED FOR RANSOMWARES

ANTI DOT PREPARED FOR RANSOMWARES

After doing a comprehensive research I along with my team members prepared an Anti Dot which is the life saving Anti Dot for Ransomware and the major part it does not cost a lot, by assessing environment and organizational scale the Anti Dot for the Ransomware is cost effective.
Note: One thing that we should keep in our mind is that the anatomy of all Ransomware lies upon triggering the file extension which is of .PDF, .TXT, .DOCX, .ZIP etc.

STEPS 1	2	3	4	5	6
We will not be building any solution, Hardware Box or device which prevent Ransomware attack.	A combination of scripts along with customized methods that doesn't affect Server performance has been prepared. The current tool is only prepared for Microsoft Windows Environment.	A simple but very aggressive approach I am come up with, we will be changing the Extension of the File before a Ransomware got it. For Example if the original File is .PDF we would be changing its extension to .PPDDFF and allowing the reader to read .PPDDFF file.	A scheduler will be continuously working to search any file hosted in the system containing an extension of .PDF, .XLS, .TXT, .DOCX will be automatically converted to our desired extension. Whenever a file is landed in the machine it will auto change its extension	The tricky part is that when we need to depart the file outside our system to external network or machine, for this A Standard folder on the Desktop will be created where the customized extensions file will be uploaded, a scheduler for every minute will be running to revert back the extension to .PPDDFF to .PDF	This whole activity doesn't require any high end configuration of the hardware nor any software solution, the only thing is the steps performed by the users.

ANTI DOT FOR RANSOMWARES (CONTD)...

Research has been conducted on the following environments and results were generated successfully while conducting the POC for the same approach.

S. No	Operating System	x86 / x64	Ransomware Tested	Anti Dot Result(s)
1	Windows Server 2012 R2	x64	WannaCry	Successful
2	Windows 10 Pro Build (1809, 1909) Windows 10 Pro N Build (1809, 1909)	x64 x64	Petya	Successful
3	Windows 7 Pro, Ultimate	x64	Loki	Successful
4	Windows Server 2016	x64	Crypto	Successful

LIMITATIONS & CHALLANGES

LIMITATION & CHALLANGES

Ransomwares usually occurred due the mistake done by user or any vulnerability in the system which would allow an attacker to upload malicious content in the system, the attack use that element to gain advantage by uploading Ransomware and demand ransom as per organization size and confidentiality of the data.

Here are some list of limitation which are temporary barriers and we hope that continues research will bridge that GAP

1. Anti Dot of Ransomware will only be able to work on Windows Based Operating system;
2. Linux, Unix and Solaris server are still vulnerable with this attack;
3. The behavior which is in build in the system doesn't cover network components or security appliances;
4. The Tool has been prepared in accordance with the assessment of historical incidents and consistent approach of ransomware occurred in the organizations;
5. Network Traffic or bandwidth monitoring has not been measured while using this technique;

THANK YOU