RANSOMWARE PREVENTION
AN ANTI DOT
FOR RANSOMWARE REMOVAL

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 RANSOMWARES

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

RESEARCH WORK FOR RANSOMWARES

Presenting a cheap solution oriented and logical solution for fighting against ransomware attacks.

ANTI DOT PREPARED FOR RANSOMWARES

A tool that will help organization to secure their 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 RANSOMWARES

INTRODUCTION TO RANSOMWARES

Ransomware is not a new terminology in the area of Malwares, the only difference between the todays ransomware and the previous once is they didn't ask for Ransom amount, crypto currency was not introduced. Today's ransomware are demanding and even more fascinating because of there working.

Ransomware Evolution: Timeline from 1989 to Present

RANSOMWARE HITS THE BIG TIME

	1989 AIDS Trojan	2006 Archiveus Cryzip	2012 Reveton	2013 CryptoLocker Cryzip	2014 Virlock	2015 Chimera	2016 Petya	2016 Kovter	2017 WannaCry
THREAT	Local Symmetric Crypto	Asymmetric Crypto	Threats of Criminal Prosecution	Online Asymmetric Crypto	Polymorphic Self-replicating	Encryption and Doxing	Disable System Time Based Increases		
DELIVERY	Physically Mailed Floppy Disks	Trojans	Trojans	Email	Viral	Email	Multiple	Fileless	Exploit-based propagation
PAYMENT	Payoff to banks	Website purchases	Prepaid cash services	Bitcoin	Bitcoin	Bitcoin	Bitcoin	Bitcoin	Bitcoin

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

RESEARCH WORK FOR RANSOMWARES

RESEARCH WORK IN RANSOMWARES

In recent years, the attack of ransomware become a very serious threat to the organization, specially in Pharmaceutical & Health care sectors where patient had lost their live due to unavailability of the systems and data encrypted by these ransomware. I have been wo rking to collect, identify and discover the behavior of each ransomware. The consistency found in these ransomware can be defined as:

STEPS	1	2	3	4	5	6
	For Every Ransomware once landed in the system irrespective which is coming from any source demands some amount in order to process the Decryption of the data hosted in the machine.	Each Ransomware uses an Encryption Algorithm using different encryption keys and SALT in their malicious payloads.	Each Ransomware encrypt a File associated with an Extension may be it can be .PDF, .PPTX, .XLSX, .DOCX, .ZIP To .PDF.Lock, .PPTX.Lock, .XLSX.Lock etc.	Once the files are locked it shows a message stating that YOUR PERSONAL FILES ARE ENCRYPTED 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)...

The environment on which the testing had been conducted contains the following details:

S. No	Operating System	x86 / x64	Privileges	OS Type	Error Identified
1	Windows 10 Pro N Build(1809)	x64	Standard	Licensed	Nil
2	Windows 7 Professional	x64	Standard	Unlicensed	Nil
3	Windows 10 Pro Build(18364)	x64	Standard	Unlicensed	Nil

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