

CRYPTOVIRUS

A RELATIVELY NEW GENRE OF VIRUS

TOBY SCOTT, TECH GURU
CHANNEL ISLANDS PCUG



Virtual Technology
Conference
Saturday, 05/06/17
@ 1 PM ET

Conference Description
& Registration Links go to

apcug2.org/content/virtual-conferences

WHAT IS A CRYPTOVIRUS?

It's a virus that once installed on your computer, attempts to find all your data files, including the ones on shared and attached drives and encrypt them with a strong encryption key that only the hacker knows. Then they will leave you a message demanding payment, usually via bitcoin, in order to unlock your data.

Cryptovirus is a form of Ransomware

HOW WILL I KNOW IF I GET A CRYPTO VIRUS?

- It won't be difficult
- The virus will crypto lock all your data files so you cannot open them
- It may take up to three days (depending on the amount of data you have)
- And then you will see something like . . .

YOUR ENCRYPTED SCREENSHOT



HOW DANGEROUS IS THIS?

Companies and organizations that were forced to pay

- Hollywood Presbyterian Medical Center
- Melrose Police Department
- New Jersey Spine Center
- Marin Healthcare District, CA
- Los Angeles Valley College
- University of Calgary

Companies that were hacked to bring in unsuspecting web traffic

- The Chinese Government website was hacked and infected visitors' computers
- BBC, AOL, NY Times all had infections for users who clicked on ads on their sites

HOW PROFITABLE IS IT?

- CNBC reports that:
 - Ransomware emails spiked 6,000% in 2016
 - 40% of all email had ransomware
 - 70% of businesses paid hackers for decryption, with 20% paying more than \$40,000
 - Industry estimates are that total payments in 2016 amounted to more than

\$1 Billion

WHY CAN'T LAW ENFORCEMENT GET RID OF IT?

- There are only a few creators of cryptovirus scripts
- But the creators never use the software themselves
- They invite hackers to share in the bounty of what they have created
- So that maybe 25 cryptovirus scripts are delivered by thousands of hackers who just put a wrapper on the original scripts. They need no significant computer or programming skills
- Law enforcement has taken down dozens of sites and arrested quite a few, but more replace them

HOW ARE THE VIRUSES DELIVERED?

- The most common are email zip file attachments
- Infected websites (you click on a link that installs the virus)
- Hacked Remote Desktop sites (Windows)
- Infected email PDF files with embedded Word.doc files running the virus scripts
- Updates to apps originally downloaded via Google and iOS app stores (the originals are checked for viruses, but no checks are done on updates)
- Email attachments of Word and Excel files

WHO IS AT RISK?

The following platforms have been targets of Cryptoviruses

- Windows XP and later, including all Server variants
- Mac OSX
- Linux (especially Red Hat)
- Oracle databases
- Android phones and tablets
- Apple phones and tablets (iOS)
- That means basically everyone is a target

HOW TO PROTECT YOURSELF

Protection comes in layers: First, don't get infected

- Don't open email attachments
- Don't click on links in email
- If you click on a link on a webpage and it wants to install anything, shut your browser down immediately using Alt-F4 or Program Manager
- If a PDF asks for permission to open a Word or Excel document, click No and delete the PDF
- If an Office document asks to run scripts, click No and delete the document (there are a few exceptions)

IF YOU USE ADOBE READER FOR PDF FILES

- Open Adobe Reader
- Click Edit > Preferences
- Under Categories, select Trust Manager
- Uncheck “Allow opening of non-PDF file attachments with external applications”
- Click OK
- If you use other default applications for PDF’s do a Search to see if you can disable opening of non-PDF files

BACKUP YOUR COMPUTER

- For Windows, use Windows Backup or third party program such as Acronis
- For Macs use Time Machine
- For Linux, almost anything will do
- Do a full system backup, sometimes called an image backup, onto a removable drive (flash drives won't work)
- Unplug the drive and put it in a safe place (not connected to your computer)

BACKUP YOUR COMPUTER

- If you make any significant changes to the programs and apps on your computer, redo or update the backup
- Make sure your phones and tablets are syncing with the cloud
- Cloud backups are too slow for system restores, so use local solutions for full system backups

SOLUTIONS FOR DATA BACKUP

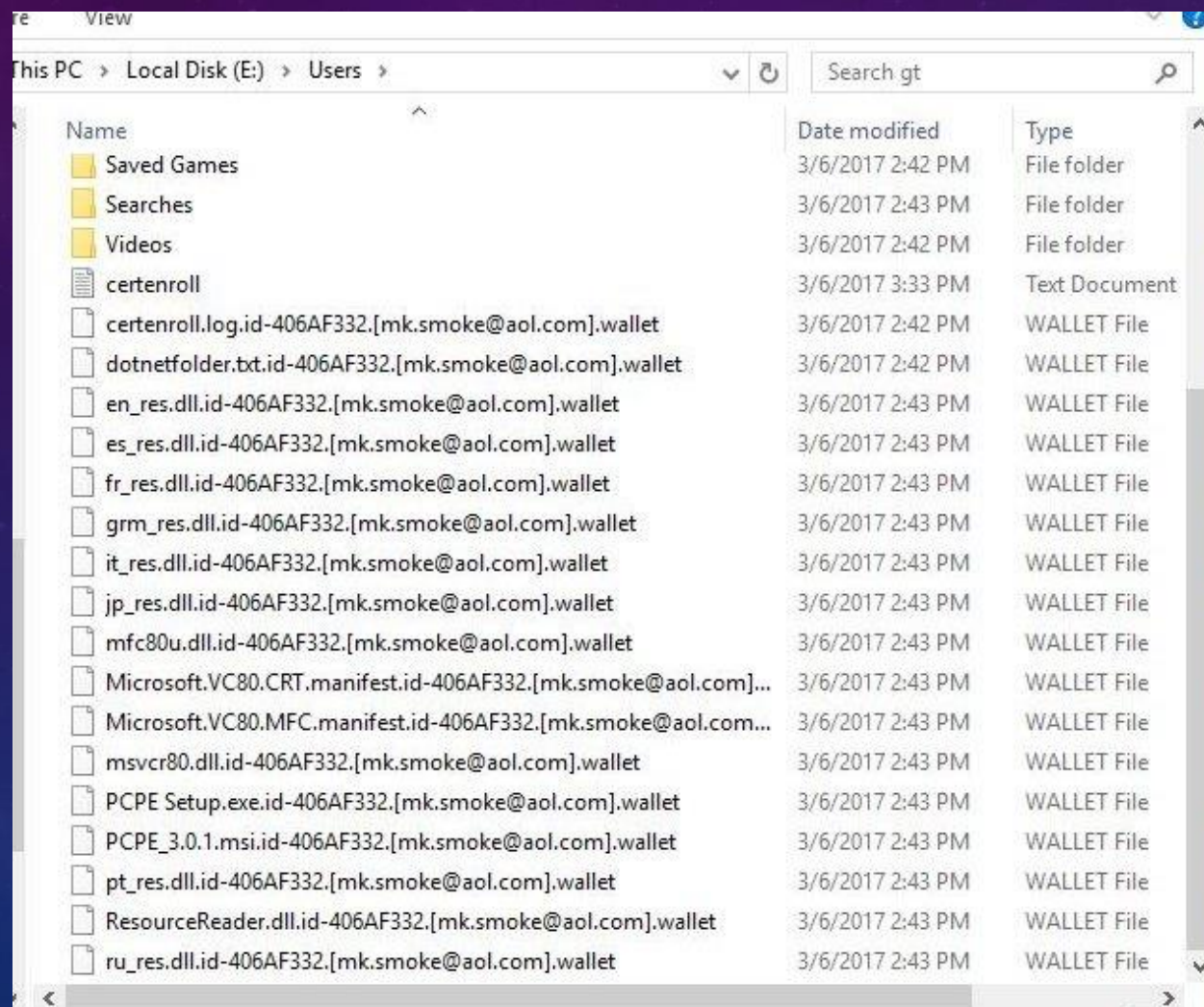
Once your operating system is safe,
you need to backup the data that changes daily

- Best solution is to buy and install automatic backup programs like Carbonite or Mozy
- Office 365 subscriptions come with a terabyte of cloud backup
- Configure OneDrive and put all your data in it
- Buy Google Drive space and backup everything there
- Subscribe to a Cloud sync system that has Versioning

SOLUTIONS FOR DATA BACKUP

- Get several large flash drives and rotate them, doing manual backups
- Network Attached Storage (NAS) devices aren't recommended as the Virus can find and encrypt network data, including NAS
- There are ways around this, but they are geeky and beyond the scope of this presentation

WHAT DO THE FILES LOOK LIKE?



Name	Date modified	Type
Saved Games	3/6/2017 2:42 PM	File folder
Searches	3/6/2017 2:43 PM	File folder
Videos	3/6/2017 2:42 PM	File folder
certenroll	3/6/2017 3:33 PM	Text Document
certenroll.log.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:42 PM	WALLET File
dotnetfolder.txt.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:42 PM	WALLET File
en_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
es_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
fr_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
grm_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
it_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
jp_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
mfc80u.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
Microsoft.VC80.CRT.manifest.id-406AF332.[mk.smoke@aol.com]...	3/6/2017 2:43 PM	WALLET File
Microsoft.VC80.MFC.manifest.id-406AF332.[mk.smoke@aol.com]...	3/6/2017 2:43 PM	WALLET File
msvcr80.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
PCPE Setup.exe.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
PCPE_3.0.1.msi.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
pt_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
ResourceReader.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File
ru_res.dll.id-406AF332.[mk.smoke@aol.com].wallet	3/6/2017 2:43 PM	WALLET File

MISCELLANEOUS INFORMATION

- Nearly all variants will crypto lock all data they can find, including all forms of backups
- Most will disable antivirus programs (or at least try to)
- Hackers migrate to the most lethal package, so plan for the worst
- If you use POP3 email programs, don't forget to backup your email files
- Remember: If you can see where your files are backed up, so can the hackers

MISCELLANEOUS INFORMATION

- Several variants leave a hidden VPN tunnel so they can re-infect you as soon as you've restored
- Several variants also leave the operating system so it will boot but not do other basic functionality
- You may have to restore the OS as well as the data

RESOURCES

- <https://www.bleepingcomputer.com/>
Best general info site
- <https://www.foolishit.com/cryptoprevent-malware-prevention/>
Excellent prevention tool
- <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>
They have decrypter tools for several of the older forms of Cryptoviruses
- <https://noransom.kaspersky.com/>
More decrypter tools
- Most of these sites have Forums where you can search for your particular virus and get up-to-date info

QUESTIONS?

Cryptovirus

Toby Scott, Tech Guru
Channel Islands PCUG

Tech (at) cipcug.org

