Ransomeware

by Chris G

What is Ransomeware?

- It’s nasty!

- A type of malicious software designed to block access to a computer system until a sum of money is paid.

- To regain access or control of the data, the user must pay a ransom — typically via bitcoin. ~~The encryption is unbreakable~~ and simply removing the malware will not solve the problem.

The Many Names of Ransomeware

Crytolocker

Reveton

Cryptowall

bitcoin

- **What?** An untraceable currency.

- **Why?** So you can’t trace / dispute the charge with your credit card - preventing thieves their hard earned money.

Why do “they” do it?

The Economics of Ransomeware

A **BILLION** dollar a year industry

The average ransom paid in 2016 was **$679**, more than double the $295 demanded at the end of 2015.* Some businesses that experience a ransomware attack are making 4 to 5 digit payments.

*according to a report from Symantec

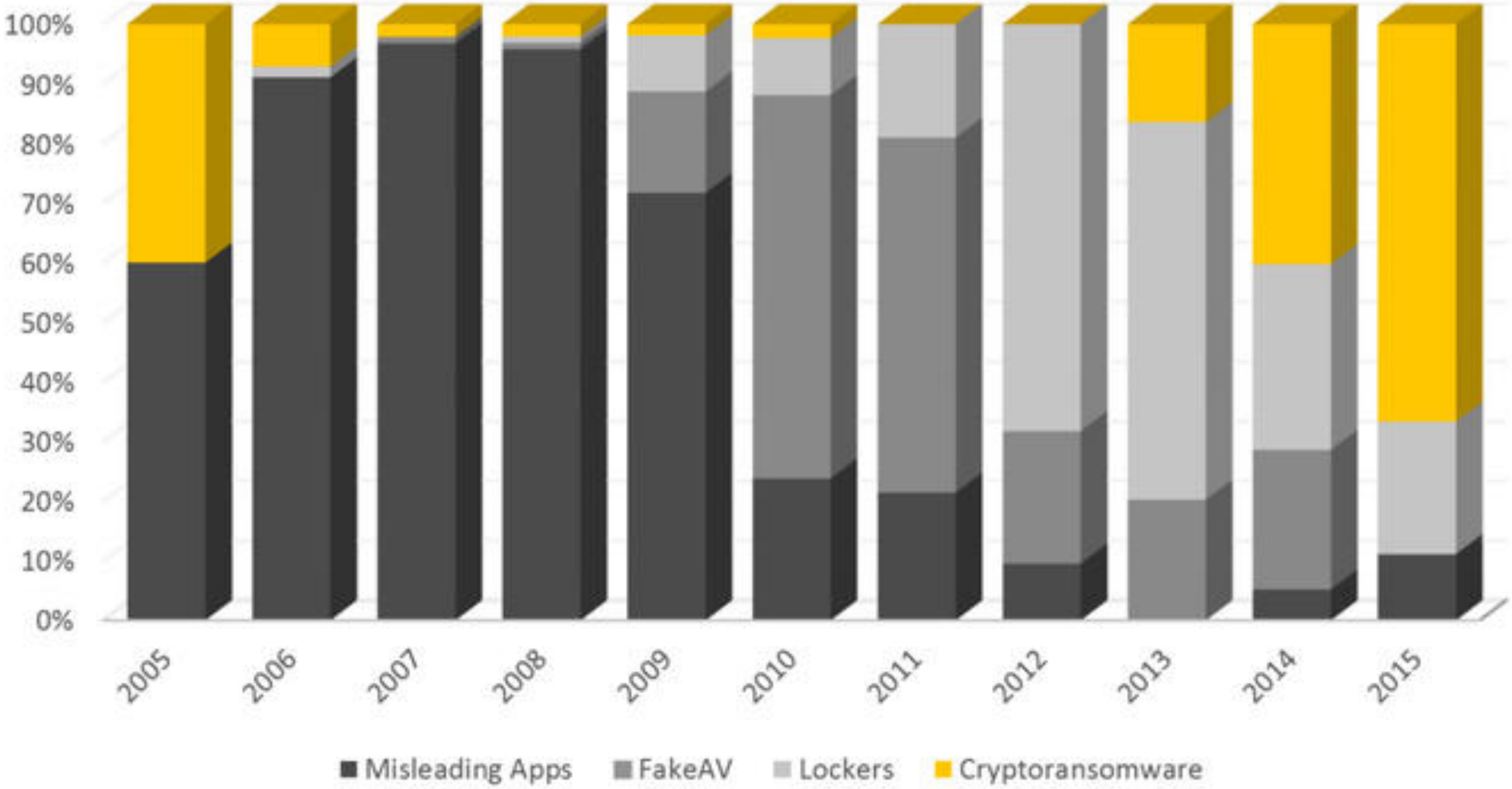


Figure 4. Percentage of new families of misleading apps, fake AV, locker ransomware and crypto ransomware identified between 2005 and 2015

On the Rise

How Do I Get It?

- Often comes from emails under the guise of UPS, USPS, or FedEx trying to update you on tracking information for a package. Remember, tracking information NEVER requires a download or attachment.
- Emails from untrustworthy sources or advertisements.
- Popups and Advertisements. Even on reputable sites like Facebook!

Devices Affected

Windows Devices
Mac Devices
Smart TVs
Android Devices
iOS less likely

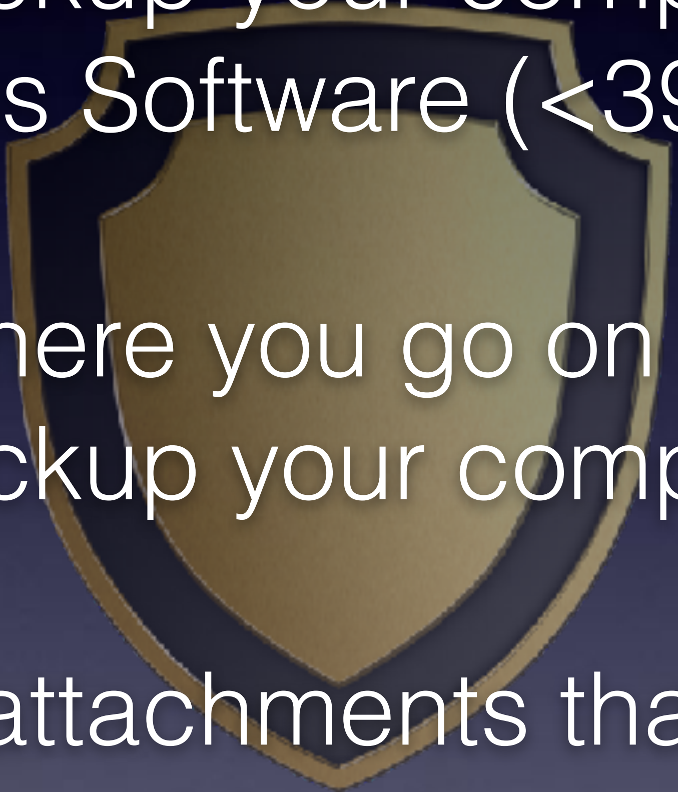
Antivirus Software

It can protect from getting the virus, however once a Cryptovirus is on the computer, AV software will do nothing.

If I Pay?

Reports vary. You may get **nothing** for the exorbitant fee.

How Do I Protect Myself?



- Backup your computer!
- Antivirus Software (<39$ a year)

- Careful where you go on the internet!
- Backup your computer!

- **Don’t** open email attachments that are .ZIP unless you know 100% they’re legit.
- Don’t click on pop-ups or advertisements.
- Backup your computer!

Types of Backup

- Local backup with external drive. Obsolete and not recommended.
- Cloud Based Backup Systems. G. Computer offers exclusive pricing for Carbonite and Backblaze.

If I’m Infected, What Do?

- **Don’t** pay the fee! It encourages this behavior!
- Call your local computer company! They may have solutions.
- DIY: Reformat your hard drive, reinstall your OS, and recover your files with your backup.
- If all else fails, G. Computer has methods to recover encrypted data with a 100% success rate as of this presentation!

Q&A

Chris G
chrisg@g-evo.com
757.291.4515