Ransomware: How serious is it?

Craig Heptinstall

PRIFYSGOL ABERYSTWYTH UNIVERSITY

Introduction

Ransomware has been a quite prominent type of malware that has been on the rise since 2013, but is it all as bad as it seems?

“A bully stuffing a student into a locker is apocryphal, but on the Internet the reality is far worse” - Bromium ransomware report [1].

Ransomware has been making its way onto countless news stories in recent times, so what is it, how bad is it, and what can be done to stop it?

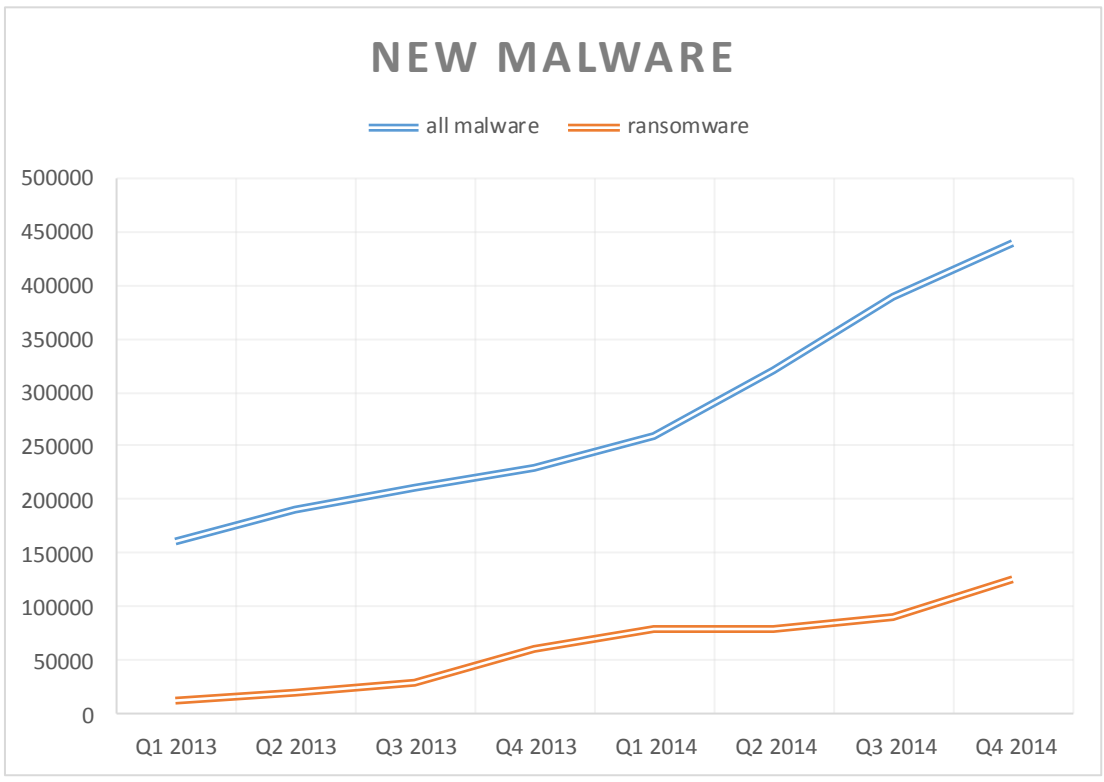

Figure 1. Malware increase statistics depicting the amount of new malware and ransomware families detected. Data: mcAfee 2014.

What is ransomware?

Viruses or malware have sub categories, ranging from spyware, to adware, and in this case: **scareware**.

Scareware has the intention of taking advantage of a user’s fear of revealing or deleting private data in an attempt to gain payment from them.

Users are usually presented with either:

Lock-screen ransomware– Prevents access to a machine until payment.

Crypto-ransomware– Encrypts user’s data until payment has been made.

“Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication”

- James Scott, Sr. Fellow, Institute for Critical Infrastructure Technology

A common case of ransomware

1.

- Ransomware finds it victims in various means.

Not limited to: Email attachments, web links, SMS, fake software or apps.

2.

- The malware then encrypts all their personal data of that user.
- Presents them with a message similar to this.
- The user then must pay the attacker to release a key.

3.

- Attackers usually only allow payment via bitcoin.
- Bitcoins allow anonymity of payee, and make it harder to trace attackers.

Ransomware: How serious is it?

Craig Heptinstall

PRIFYSGOL ABERYSTWYTH UNIVERSITY

Statistics and findings

Ransomware attacks have grown exponentially over the past 2 years [2], but just how much?

- 500% increase in attacks in 2013 compared to previous year. [3]
- Cryptolocker ransomware infected around 250,000 machines alone in the same year, including a police department.
- 39% of variants target more than just desktops [4].

Figure 2. Android ransomware detection trend. ESET. LiveGrid. 2016.

File type targeting

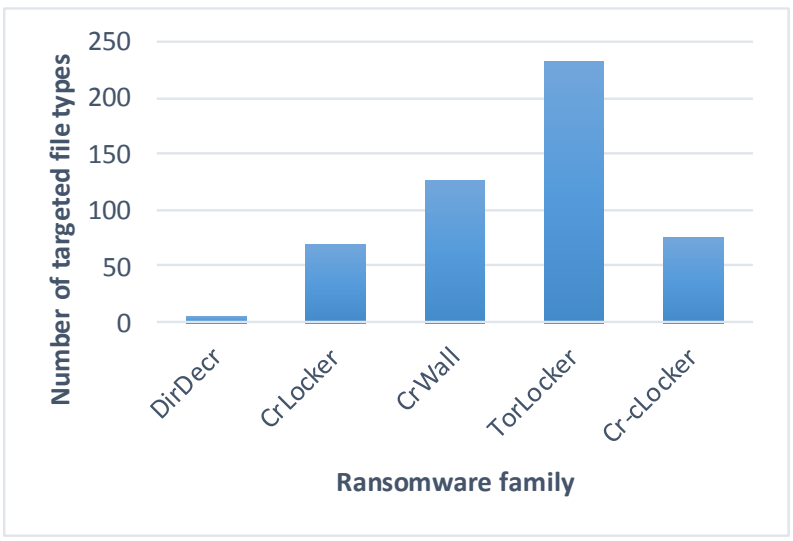

Figure 3. File type targeting per each ransomware family. Data: Bromium Security 2015.

From 1300 samples, there are two distinct ransomwares:

CryptoWall

- Uses unbreakable AES encryption
- Activity over Tor network
- Provide one free key to unlock a file to prove they hold real keys

TorrentLocker

- Exclusively distributed via email
- Also uses AES encryption
- Spreads further by harvesting a victims emails
- HTTPS POST requests

Ransomware mitigation

Most ransomware acts abnormally, so **should be detectable.**

Following a look at how the most popular ransomware works, there were some mitigation strategies suggested [3]:

1. API call monitoring
2. Monitoring file system activity
3. Using decoy resources

Some papers [5] suggest that no matter how well equipped machines are to protect users, they will always be the weak spot.

Further reading

[1] V. Kotov, M. S. Rajpal. *Understanding Crypto-Ransomware.* Bromium. 2015.

[2] Webroot. *A Guide to Avoid Being a Crypto-Ransomware Victim.* 2015.

[3] A. Kharaz, W. Robertson. *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks.* 2015.

[4] E. Kirda. *Most Ransomware isn't as complex as you might think.* Lastline labs. 2014.

[5] A. Price, Y. C. *Human Factors in Information Security. International Journal of Computer and Information*