CANDYLAND

A MODERN DAY MALWARE PRIMER

WARNING

This talk may contain comments or opinions that at times may differ with those of cisco systems. The views expressed here do not necessarily reflect those of cisco systems. Audience discretion is advised.

MOSES@MOSES.IO

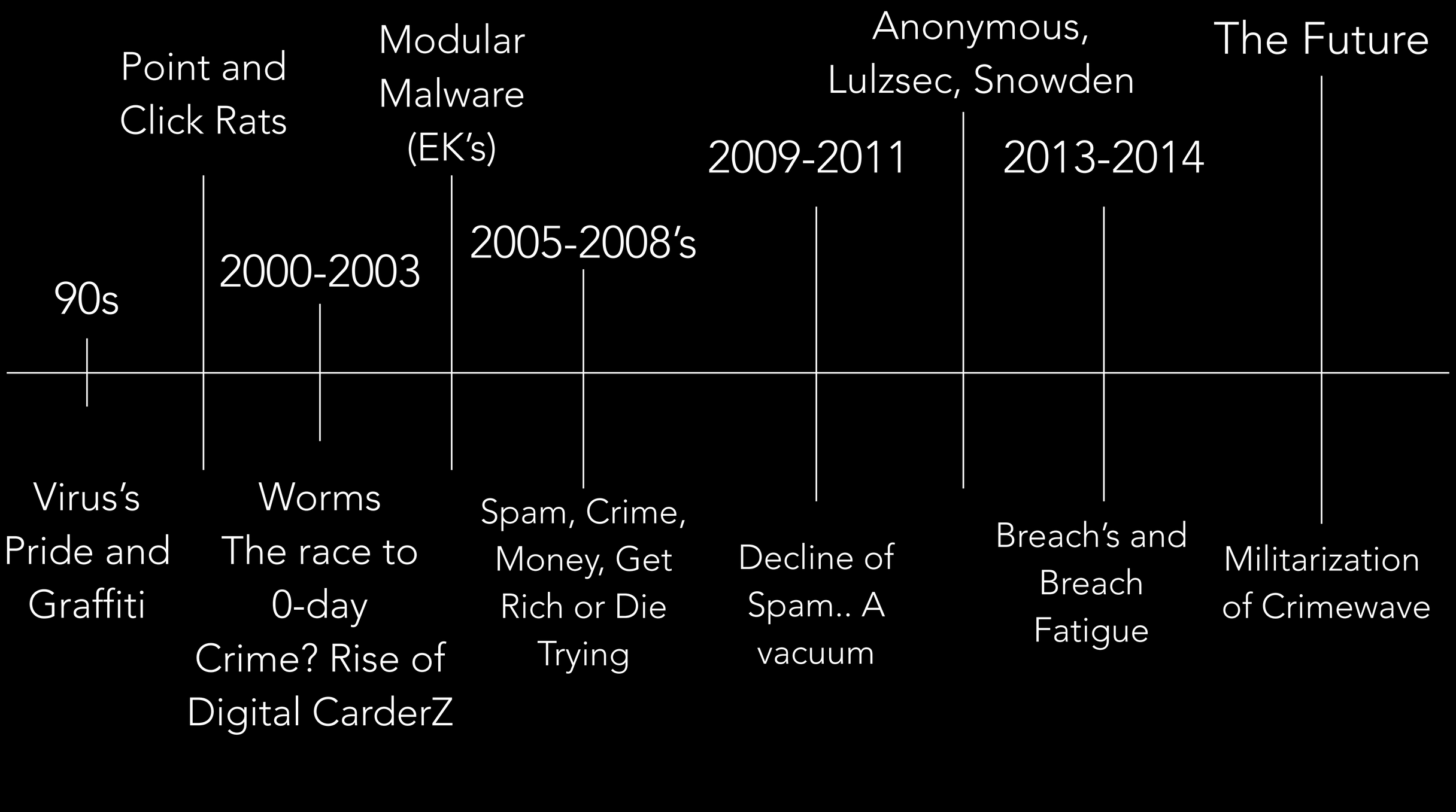
AS SEEN AT CISCO
AND SANS
AND SEVERAL OTHER PLACES

ABOUT.ME/MOSESHERNANDEZ
@MOSESRENEGADE

Malware? Or Software? It’s all how you look at it

“Where are you going, where have you been”

-JOYCE CAROL OATES.


90s
Virus's
Pride and
Graffiti
Point and
Click Rats
2000-2003
Worms
The race to
0-day
Crime? Rise of
Digital CarderZ
Modular
Malware
(EK's)
2005-2008's
Spam, Crime,
Money, Get
Rich or Die
Trying
2009-2011
Decline of
Spam.. A
vacuum
Anonymous,
Lulzsec, Snowden
2013-2014
Breach's and
Breach
Fatigue
The Future
Militarization
of Crimewave

MALWARE ECONOMICS?

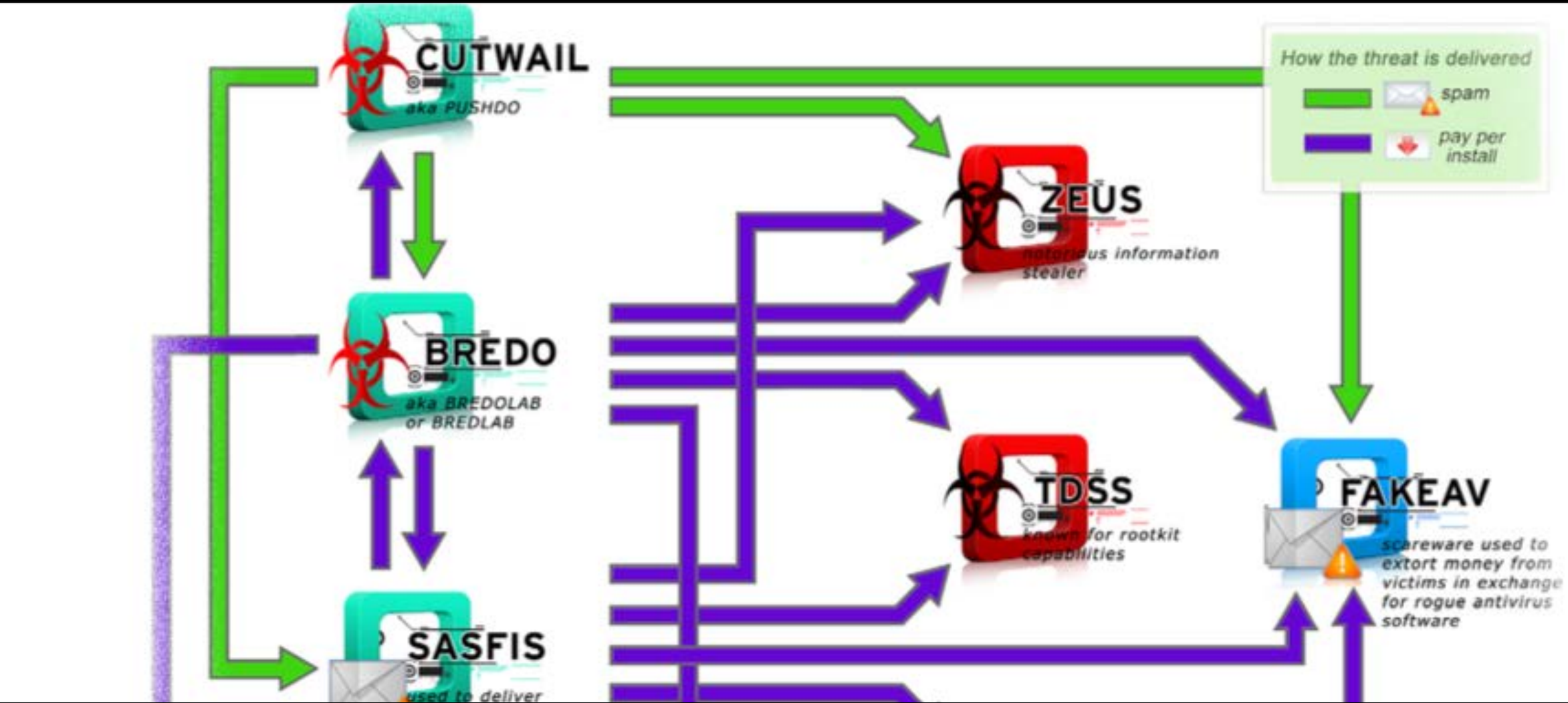
- A market economy
  - Investment - through R&D
  - Production - through Development
  - Distribution - through compromise
  - Supply and Demand - Obvious
  - “Free Market”

AN ECOSYSTEM OF WIN.

- The Service Economy:
  - Stressers / Booters (DDoS as a Service)
  - Need to attack new victims? Phishing/Vishing/Spam/Blackhat SEO/ Malvertising - as a service
  - Exploit Kit’s and RATS/Trojans - Payload Delivery, and Payloads
  - Cashing Out Services - Laundering, Processing, Etc.

IMAGE: HTTP://LA.TRENDMICRO.COM/MEDIA/WP/FAKEAV-AFFILIATE-NETWORKS-WHITEPAPER-EN.PDF

HISTORY - FAKE A/V

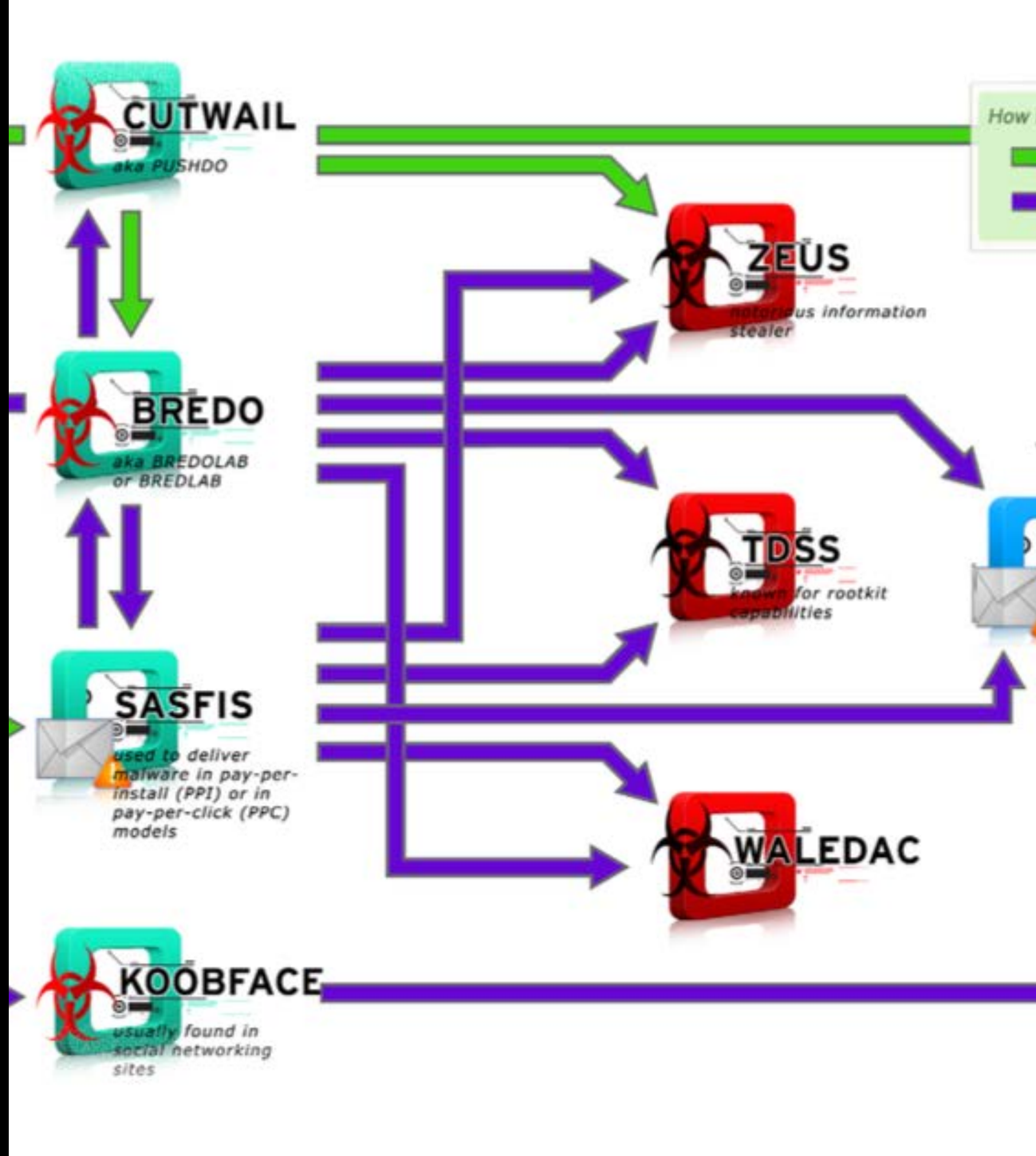


MMM. CANDY.

- Fake A/V Research from UCSD
- http://krebsonsecurity.com/wp-content/uploads/2011/07/ue_fakeav.pdf
- Researchers where looking at how the system goes from ‘Fake A/V’ to Cash $$$$.
- One or Few Payment Processors would handle all the business.

REAL WORLD EXAMPLES

- Consider the eco system on the right:
  - The owner of a bot net
  - Delivers a Trojan
    - To push out Fake A/V
    - Makes money.



THE QUEST FOR MORE CANDY

ERR MONEY.

A NOTE ON: NATION STATE ATTACKS

If a nation state is after you… truly.

There isn’t much you can probably do.

On your own.

NOW THAT WE HAVE NO MORE PHARMA... RANSOM!

Sell Exploit Kits

Sold to, Delivered, etc

Exploited Servers

victim browses to this.

User is Popped
Data is Encypted

Victim has to Pay Up!

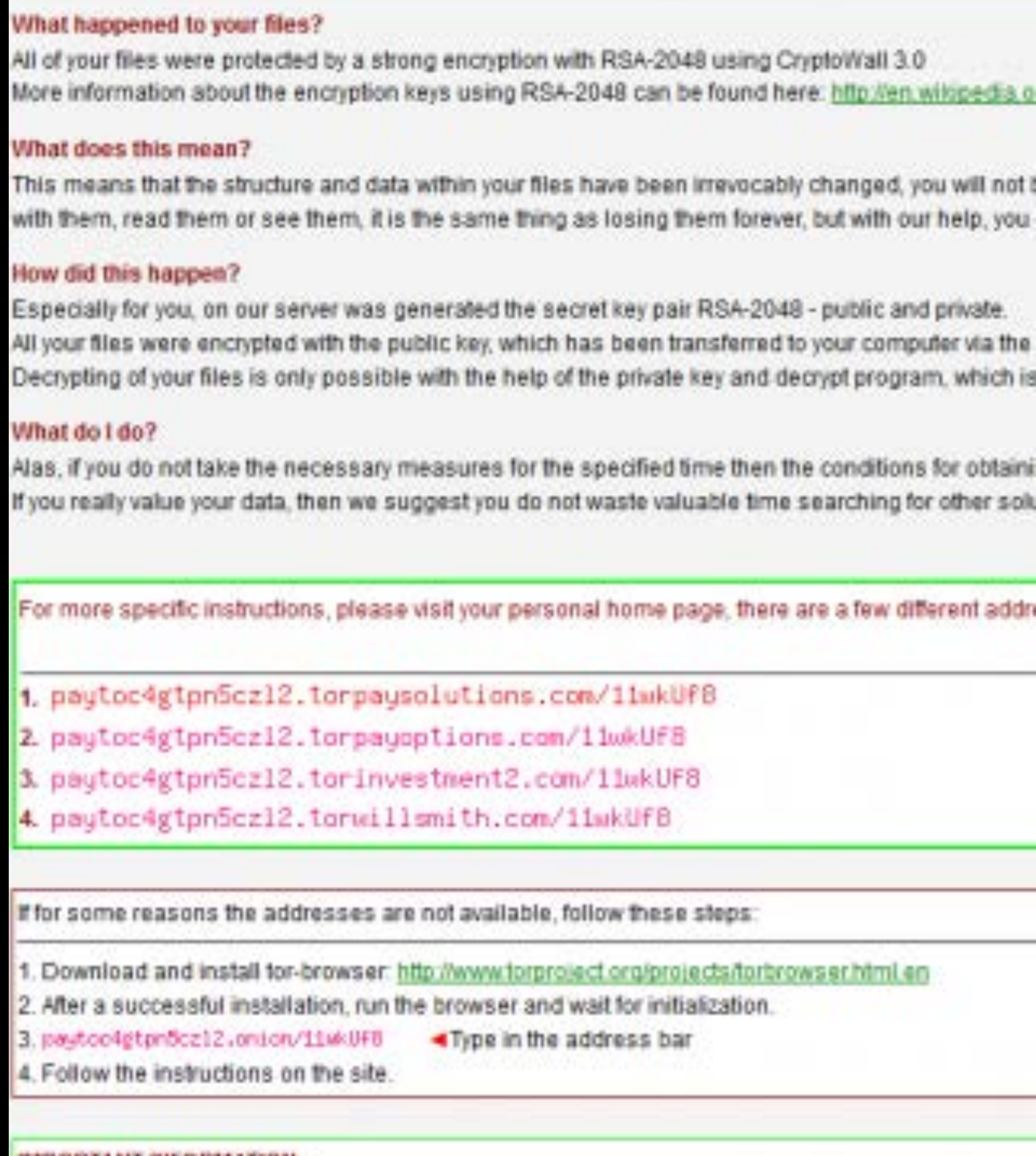
Through Tor

BitCoin*

Obligatory Villain

HELP YOUR CUSTOMERS!

- Its a FAQ and Techsupport.
- From Victim (Customer) to Business (Hacker).
- How to pay, via ToR and BitCoin.



BITCOINS, TOR, AND ANONYMITY

- The crime individuals learned from the ‘Pharma wars’ that getting processing going is critical.
- Moving to BitCoin makes it ‘harder’ to bring down their network (more distribute). In theory
- It also makes cashing out harder.

WHERE ARE WE GOING?

- Our dystopian malware future?!

THE FUTURE

- Three distinct areas:
  - Low-Tech criminals will start learning for nation state actors (currently trending)
  - Low-Tech nation states will learn from advanced nation state attackers (somewhat could be happening).
  - An acceleration in what Nation States are doing. (How would we know?)

NOT QUITE THIS BAD

END ON A HAPPY NOTE!

- It’s not too bad!
- Think of the progress that has been made:
  - Apple App Store. Less Malware than other App Stores.
  - Not perfect, nothing is.
  - It’s one example of a working eco-system.

THOUGHTS? QUESTIONS?

moses[at]moses.io

@mosesrenegade on twitter.

Tweets to me!