

CANDYLAND

# A MODERN DAY MALWARE PRIMER

# CANDYLAND

A child's first game





# 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](mailto:MOSES@MOSES.IO)

AS SEEN AT CISCO  
AND SANS  
AND SEVERAL OTHER PLACES

[ABOUT.ME/MOSESHERNANDEZ](http://ABOUT.ME/MOSESHERNANDEZ)  
[@MOSESRENEGADE](https://twitter.com/MOSESRENEGADE) 



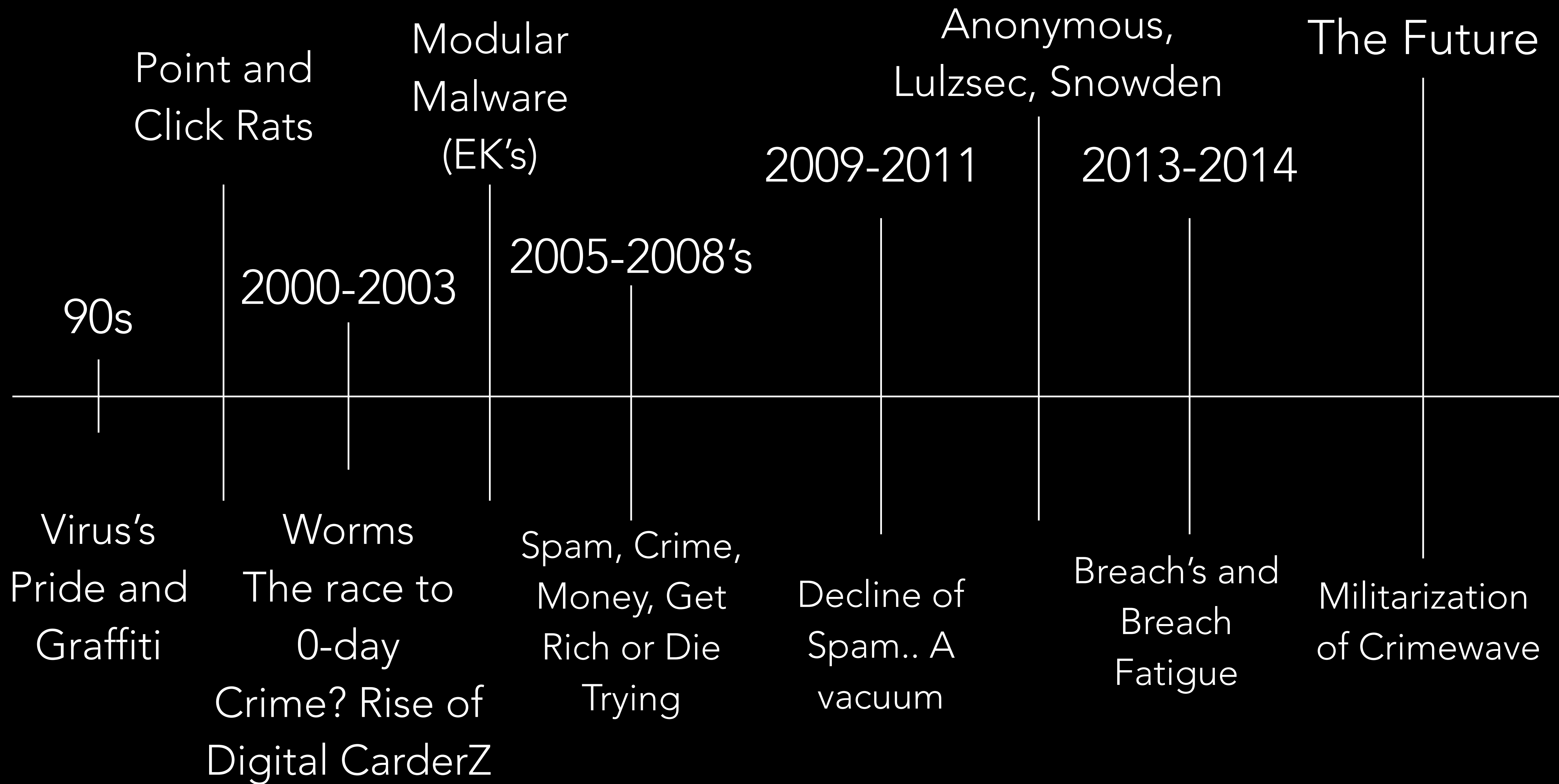


Malware? Or Software? It's all how you look at it



“Where are you going, where have you been”

-JOYCE CAROL OATES.





# MALWARE ECONOMICS?

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

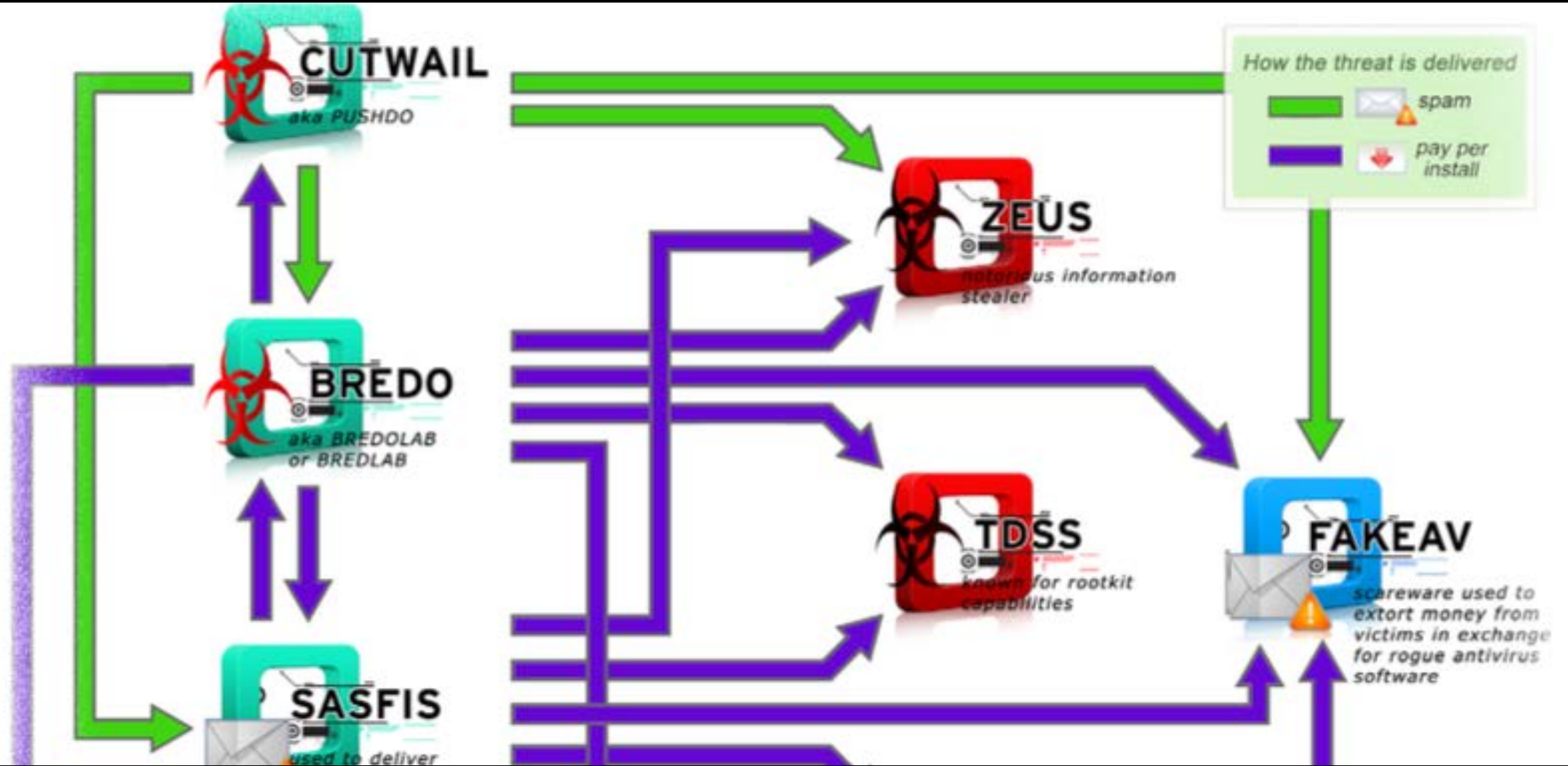


# AN ECOSYSTEM OF WIN.

- 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.



# HISTORY - FAKE A/V





# MMM. CANDY.

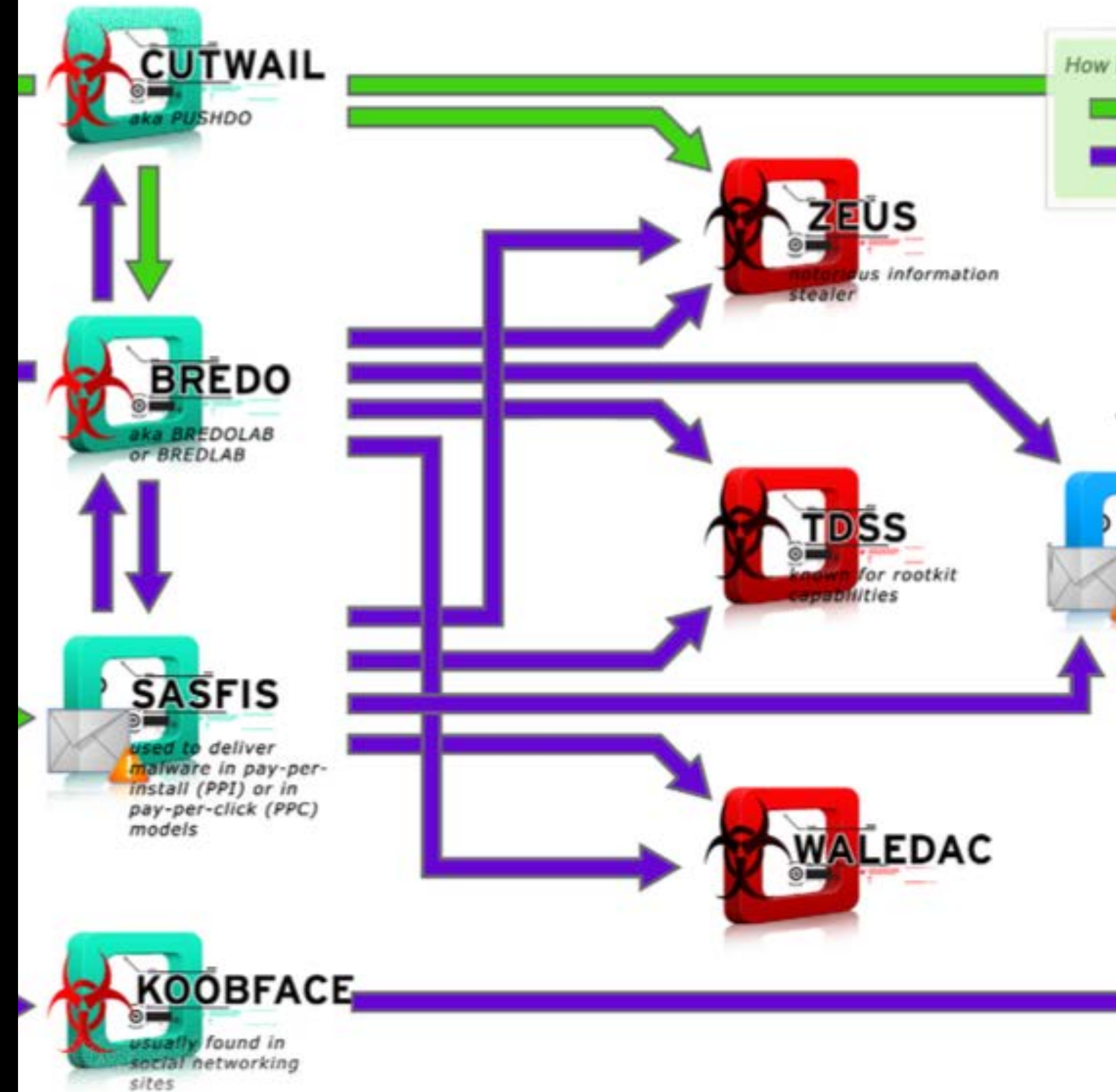
- Fake A/V Research from UCSD
- [http://krebsonsecurity.com/wp-content/uploads/2011/07/ue\\_fakeav.pdf](http://krebsonsecurity.com/wp-content/uploads/2011/07/ue_fakeav.pdf)
- Researchers where looking at how the system goes from 'Fake A/V' to Cash \$\$\$\$.
- One or Few Payment Processors would handle 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.

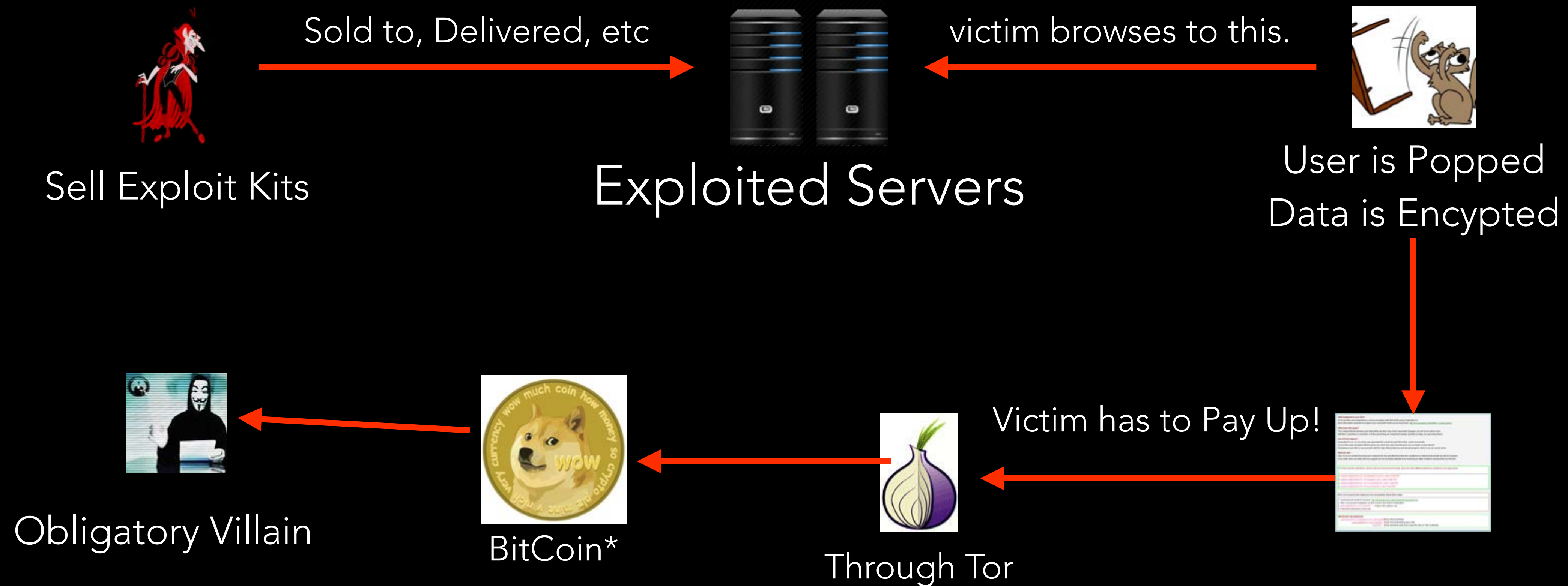
On your own.

**KEEP CALM AND EAT  
YOUR MILK SANDWICH**





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





# HELP YOUR CUSTOMERS!

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

## What happened to your files?

All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0  
More information about the encryption keys using RSA-2048 can be found here: <http://en.wikipedia.org>

## What does this mean?

This means that the structure and data within your files have been irrevocably changed, you will not be able to edit, delete, copy, move, with them, read them or see them, it is the same thing as losing them forever, but with our help, you can get them back.

## How did this happen?

Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.  
All your files were encrypted with the public key, which has been transferred to your computer via the internet.  
Decrypting of your files is only possible with the help of the private key and decrypt program, which is available on our website.

## What do I do?

Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be more difficult.  
If you really value your data, then we suggest you do not waste valuable time searching for other solutions.

For more specific instructions, please visit your personal home page, there are a few different addresses:

1. [paytoc4gtpn5czl2.torpaysolutions.com/11wkUF8](http://paytoc4gtpn5czl2.torpaysolutions.com/11wkUF8)
2. [paytoc4gtpn5czl2.torpayoptions.com/11wkUF8](http://paytoc4gtpn5czl2.torpayoptions.com/11wkUF8)
3. [paytoc4gtpn5czl2.torinvestment2.com/11wkUF8](http://paytoc4gtpn5czl2.torinvestment2.com/11wkUF8)
4. [paytoc4gtpn5czl2.torwillsmith.com/11wkUF8](http://paytoc4gtpn5czl2.torwillsmith.com/11wkUF8)

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. [paytoc4gtpn5czl2.onion/11wkUF8](http://paytoc4gtpn5czl2.onion/11wkUF8) ◀ Type in the address bar
4. Follow the instructions on the site.



# 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!