RSAConference2015
San Francisco | April 20-24 | Moscone Center

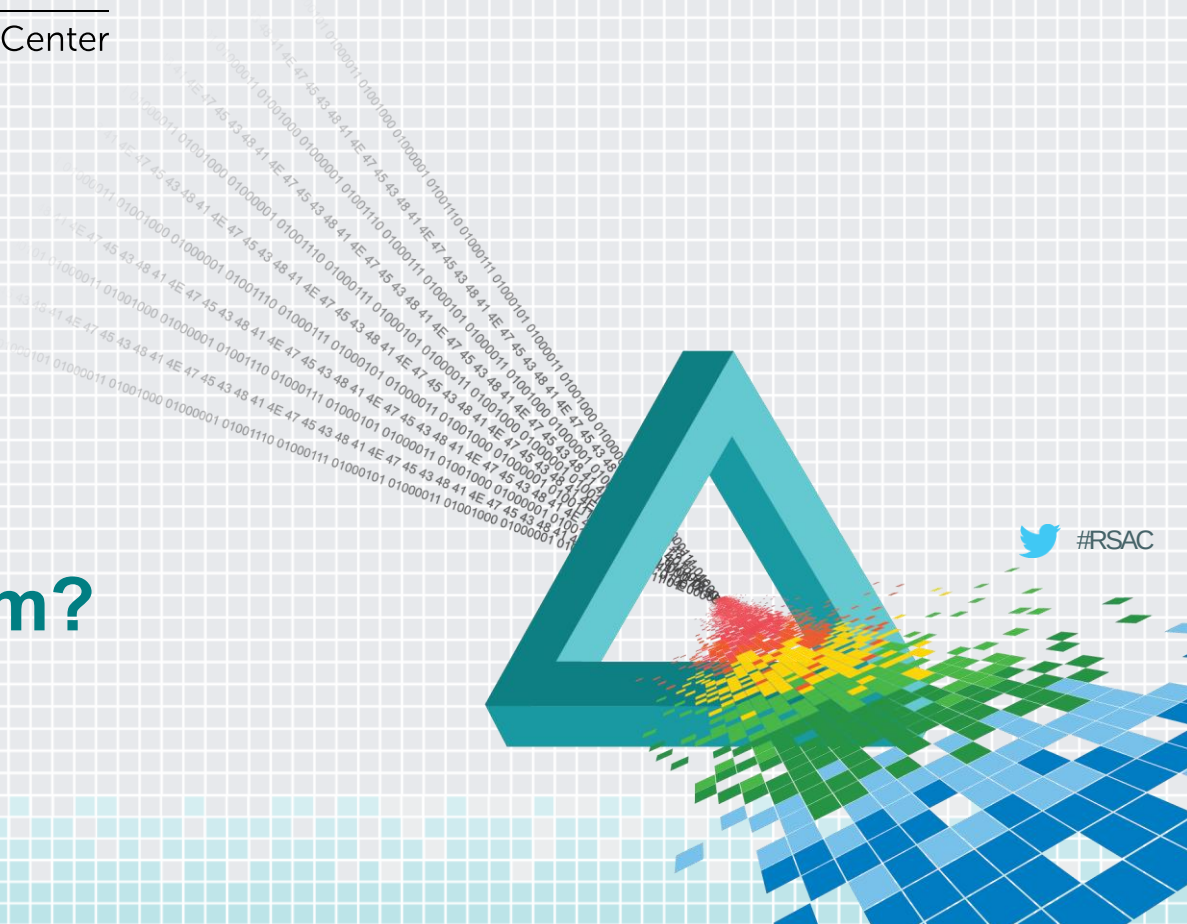
SESSION ID: SPO3-T09

Defense in Depth to Coordinated Defense: Organizing against Our Common Enemy

Chester Wisniewski
Sr. Security Advisor
SOPHOS
@chetwisniewski

John Shier
National Channel SE
SOPHOS
@john_shier

What's the problem?



2-D view

Complex threats

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

HOME | ABOUT US | PUBLICATIONS | ALERTS AND TIPS | RELATED RESOURCES

C³ VP

Alert (TA15-098A)
AAEH

More Alerts

Original release date: April 09, 2015

Print | Tweet | Send | Share

Systems Affected

- Microsoft Windows 95, 98, Me, 2000, XP, Vista, 7, and 8
- Microsoft Server 2003, Server 2008, Server 2008 R2, and Server 2012

Overview

AAEH is a family of polymorphic downloaders created with the primary purpose of downloading other malware, including password stealers, rootkits, fake antivirus, and ransomware.

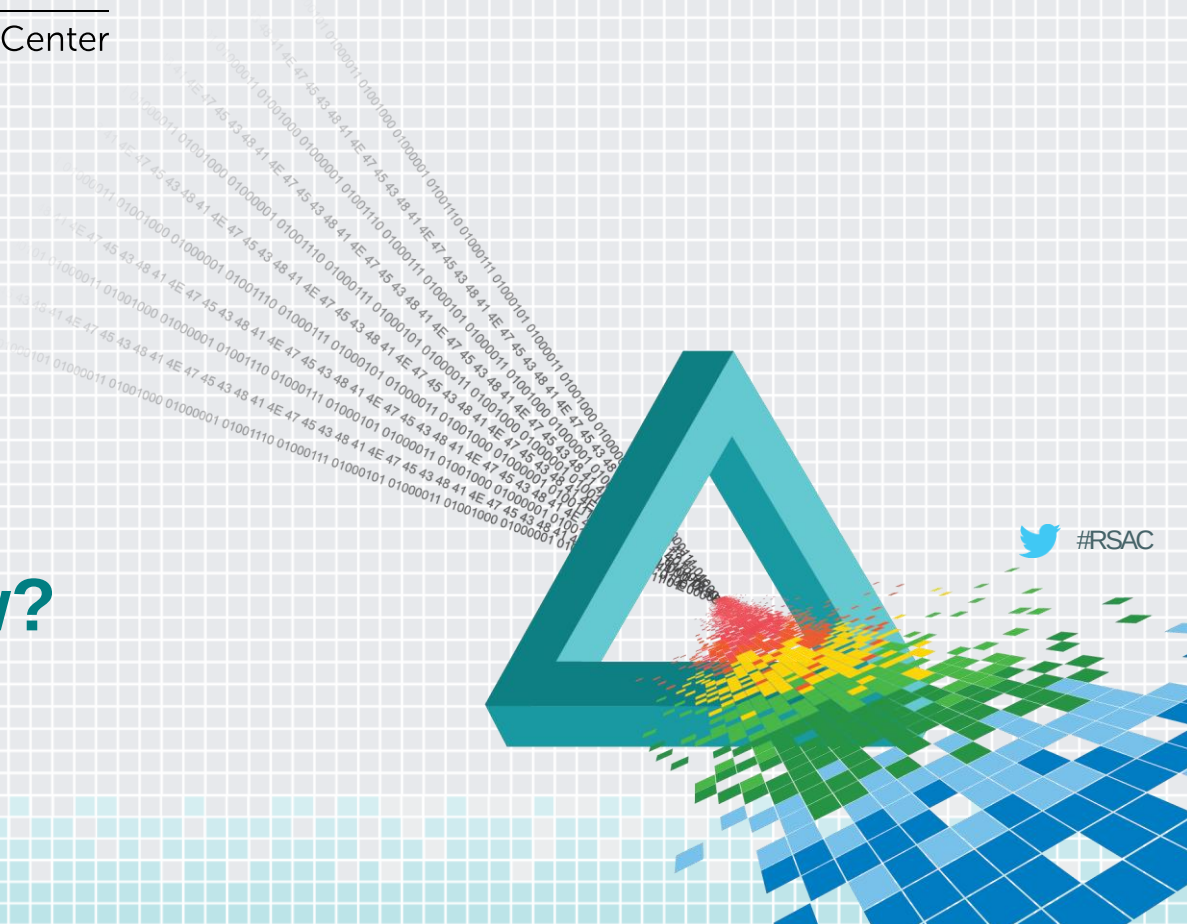
The United States Department of Homeland Security (DHS), in collaboration with Europol, the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ), released this Technical Alert to provide further information about the AAEH botnet, along with prevention and mitigation recommendations.

Description

AAEH is often propagated across networks, removable drives (USB/CD/DVD), and through ZIP and RAR archive files. Also known as VObfus, VBObfus, Beebone or Changeup, the polymorphic malware has the ability to change its form with every infection. AAEH is a polymorphic downloader with more than 2 million unique samples. Once installed, it morphs every few hours and rapidly spreads across the network. AAEH has been used to download other malware families, such as Zeus, Cryptolocker, ZeroAccess, and Cutwail.

Current situation

Where are we now?



Cryptowall 3.0

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/wiki/RSA_(cryptosystem)

What does this mean?

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

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 on our secret server.

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 changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

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

1. paytoc4gtpn5czl2.torforall.com/vRRRbw
2. paytoc4gtpn5czl2.torman2.com/vRRRbw
3. paytoc4gtpn5czl2.torwoman.com/vRRRbw
4. paytoc4gtpn5czl2.torroadsters.com/vRRRbw

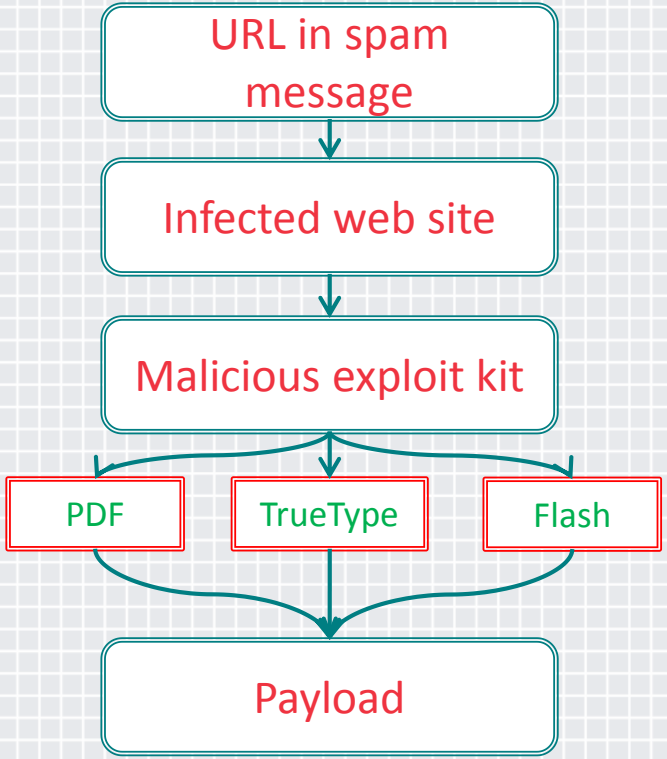
If for some reasons the addresses are not available, follow these steps:

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/vRRRbw ◄Type in the address bar
4. Follow the instructions on the site.

IMPORTANT INFORMATION:

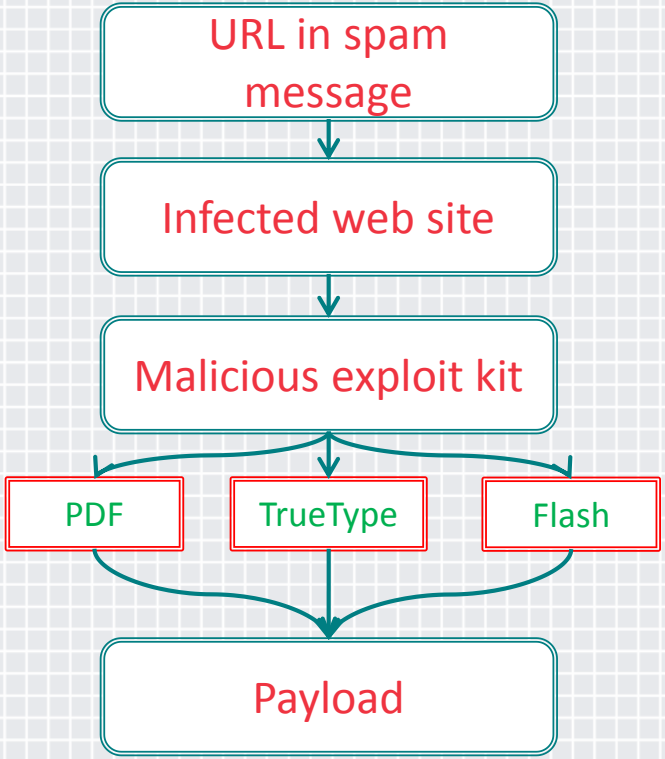
paytoc4gtpn5czl2.torforall.com/vRRRbw ◄Your Personal PAGE
paytoc4gtpn5czl2.onion/vRRRbw ◄Your Personal PAGE(using TOR)
vRRRbw ◄Your personal code (if you open the site (or TOR 's) directly)

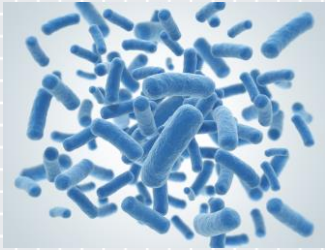
Defense in depth



Bob and weave

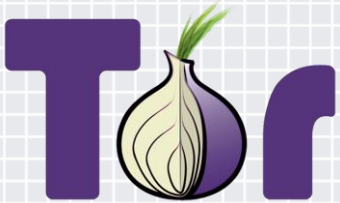
Designed to defeat





Sjhjkhgdubf.biz
Ecubfg34da.info
Oerujnsgb3n.ru
Asdbn3dnd.com

ssh-rsa
AAAAB3NzaC1yc2
EAAAABIwAAAgEA
2MxpV3LdkG4OS7
MHXbG4kXvlYn



Executive Order 13691

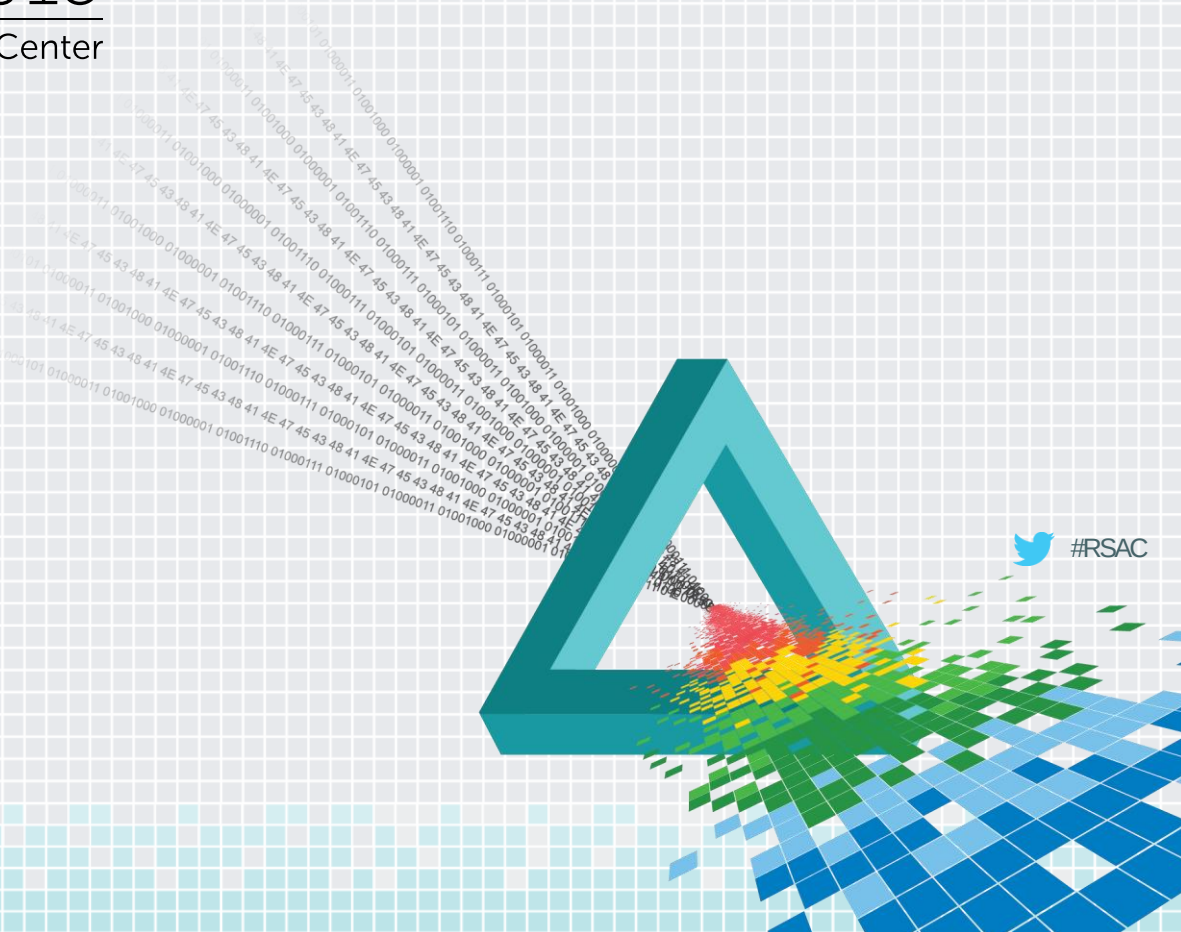
“In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible.”

Single point of success?

Suite spot?

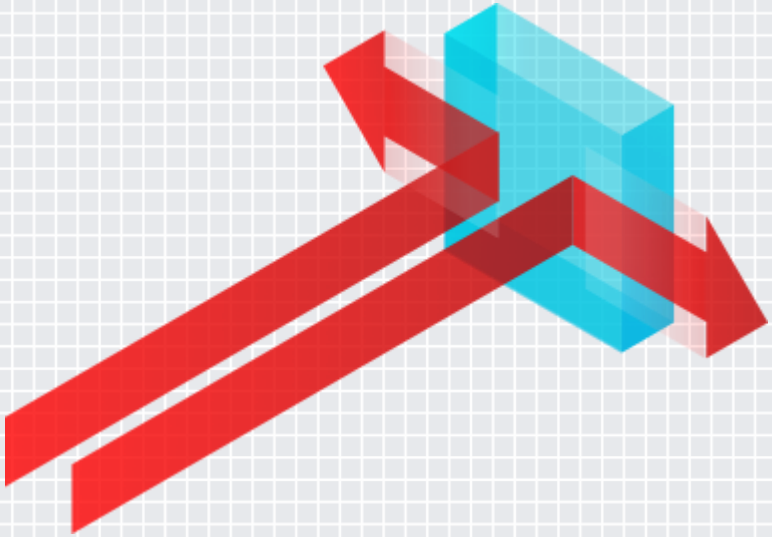
Best of breed

Making it better



Malicious traffic detection

- Suspicious traffic detected
- Alert sent to other components
- Related activities considered suspicious

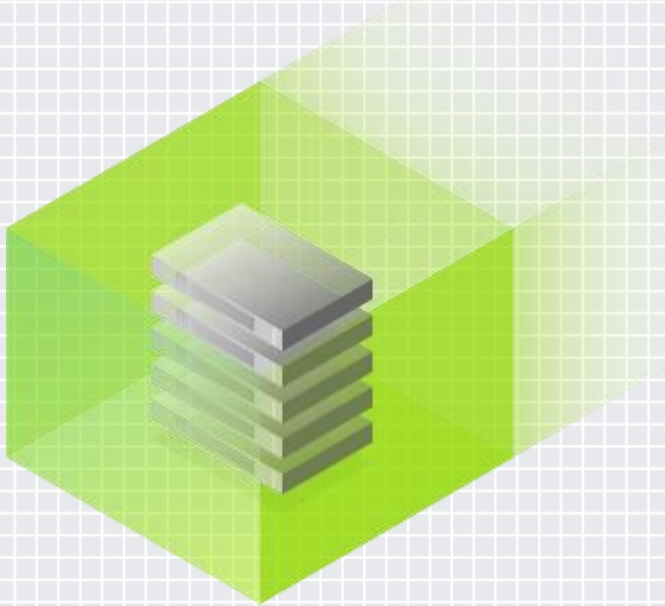


Application tracking

- Detect unknown applications generating traffic
- Discover which computers share the same process
- Use lockdown locally and on the network to quarantine host

Lockdown

- Identify known good processes and files
- Whitelist processes
- Block unauthorized modifications and applications

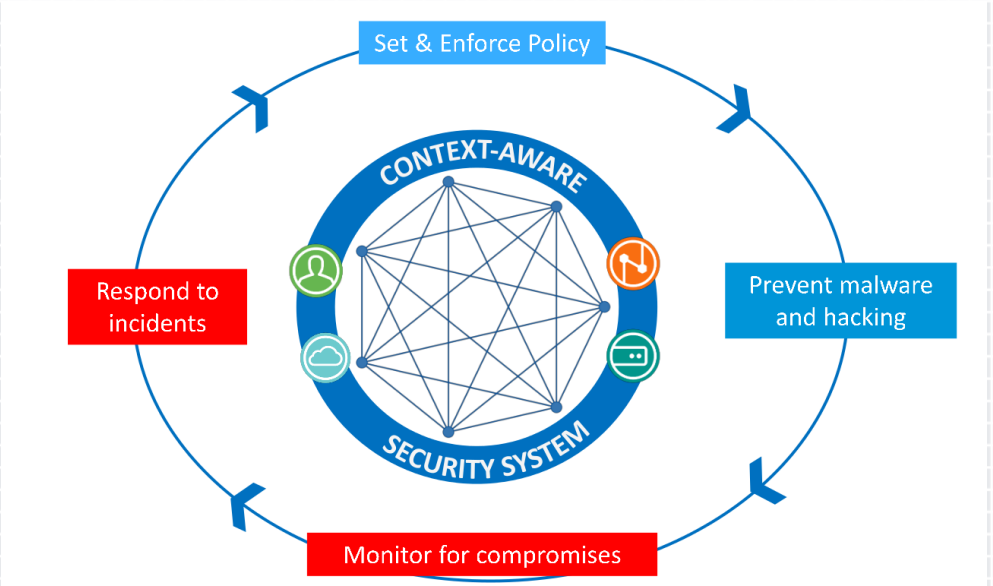


Heartbeat

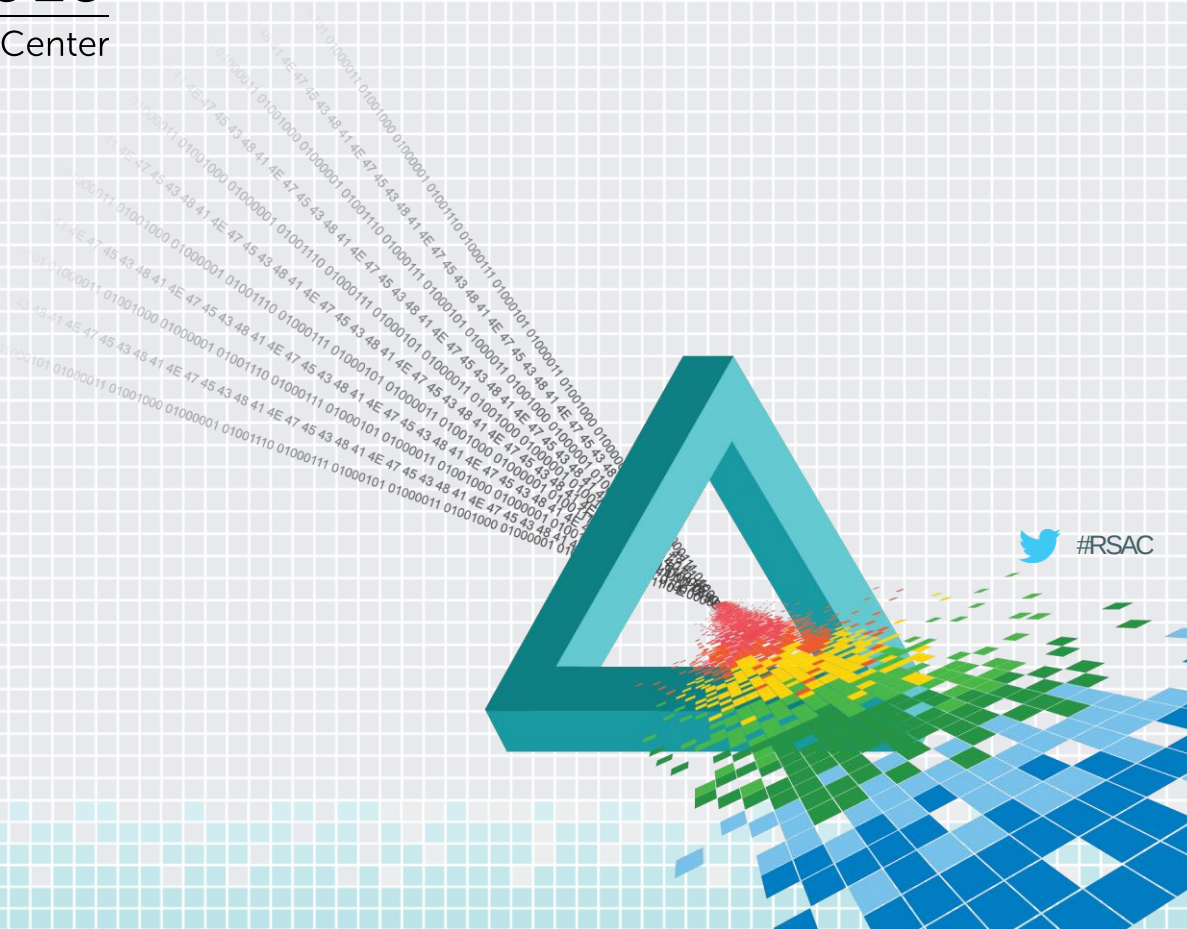
- Gather health of devices
- Gather health of network
- React to compromise
- Coordinate communication to all components to enable organized defense

Wash, rinse, repeat

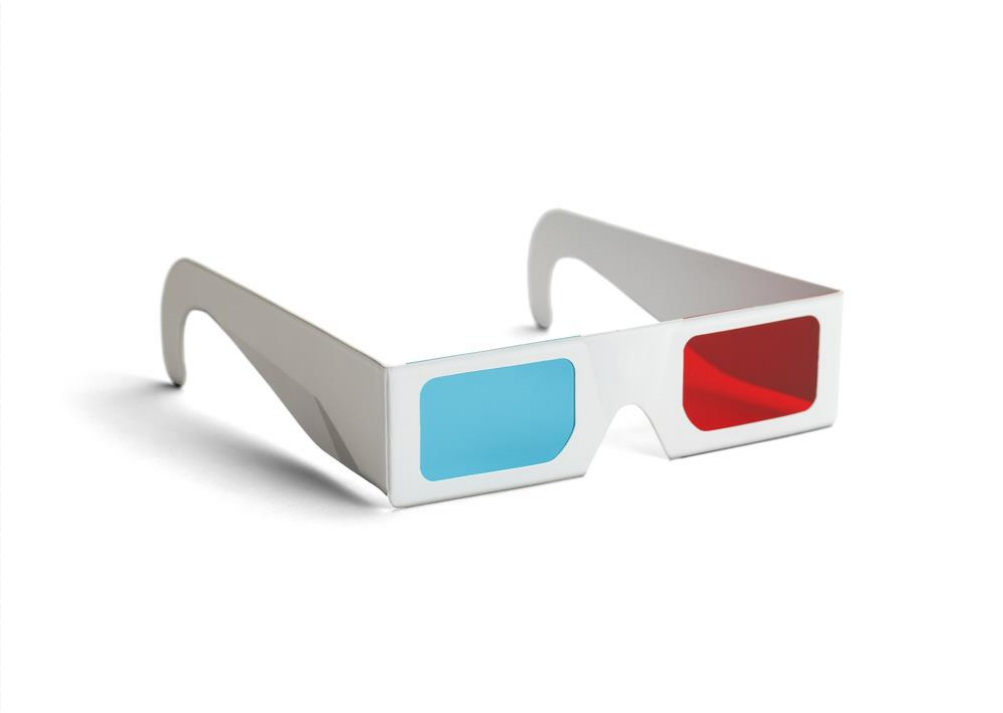
- Gather data from various sources
- Correlate events
- Replay events
- Trace sequence of events
- Write policy based on events



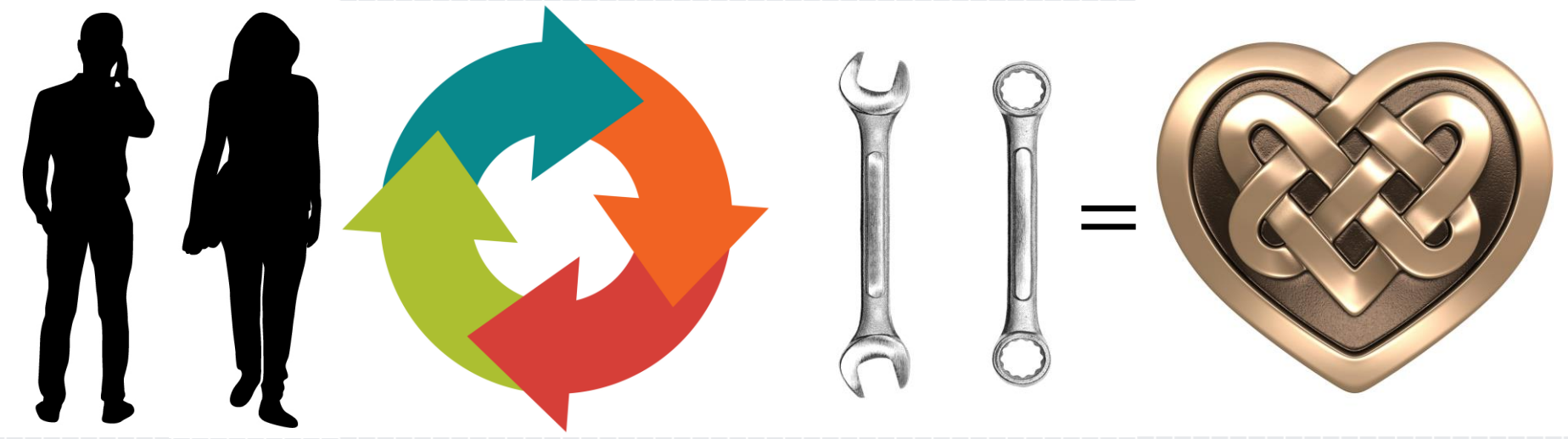
Conclusion



3-D view



Sounds great, what now?



State of bliss