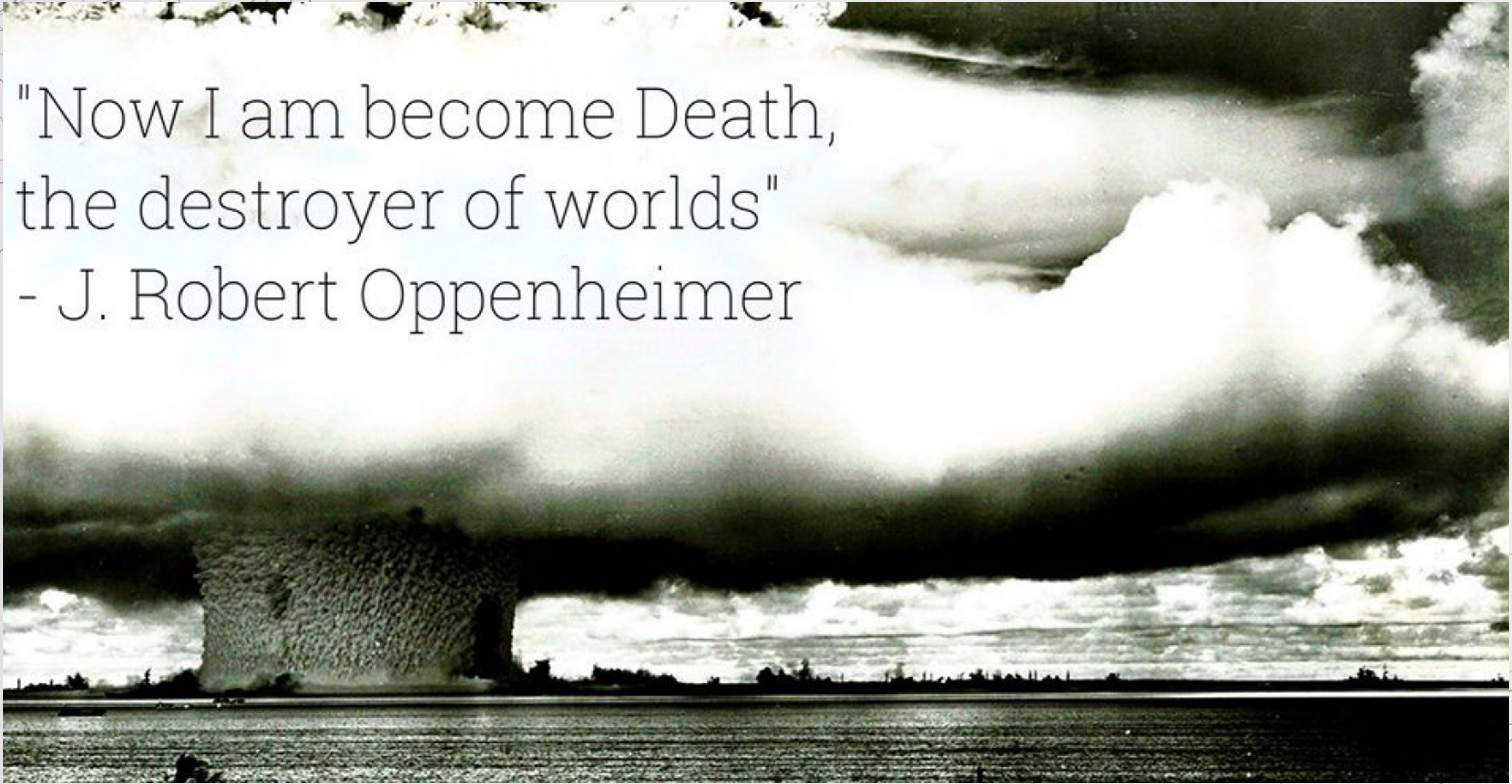
My Oppenheimer Paradox

Responsibilities for the things I create

Silas Cutler
CrisisCon 2020 Keynote

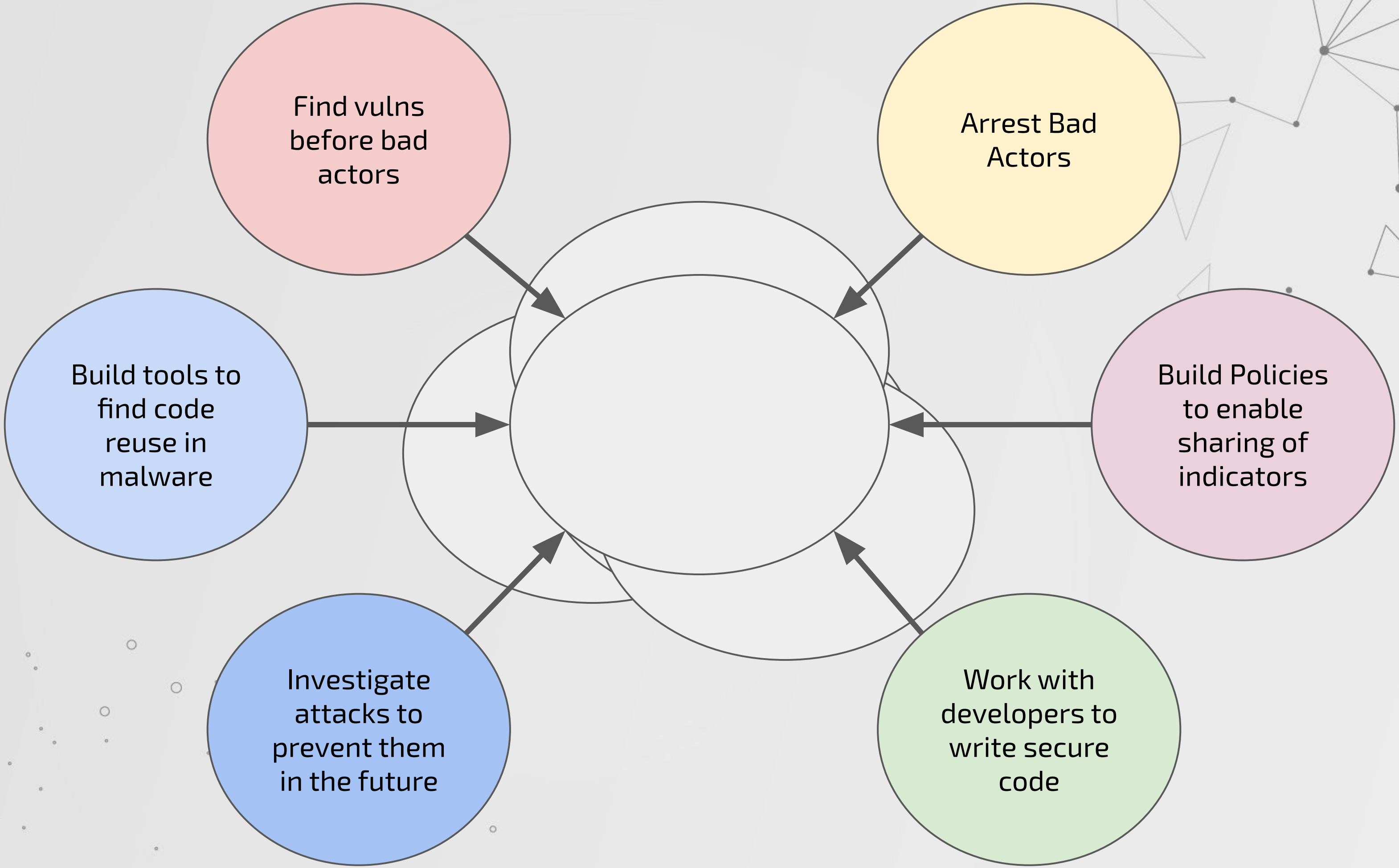


"Now I am become Death,
the destroyer of worlds"
- J. Robert Oppenheimer

Inherently, we’re all working towards a **common goal**…

Just differing views of

How we get there



Find vulns before bad actors

Arrest Bad Actors

Build tools to find code reuse in malware

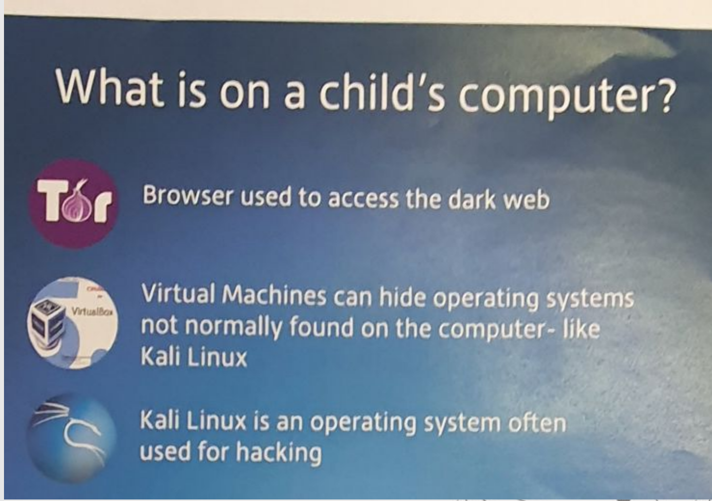
Build Policies to enable sharing of indicators

Investigate attacks to prevent them in the future

Work with developers to write secure code

How changes / evolves

- Always relative and subjective
  - *[what if MSF was released now?]*
- Sometimes they conflict - Sometimes they build off each other
- Together we adjust, tune, etc.
  - often **slowly**



What is on a child's computer?

Browser used to access the dark web

Virtual Machines can hide operating systems not normally found on the computer- like Kali Linux

Kali Linux is an operating system often used for hacking

Tor
VirtualBox

Inherently, we're all working towards a **common goal**…

Just differing views of

How we get there

Which is good

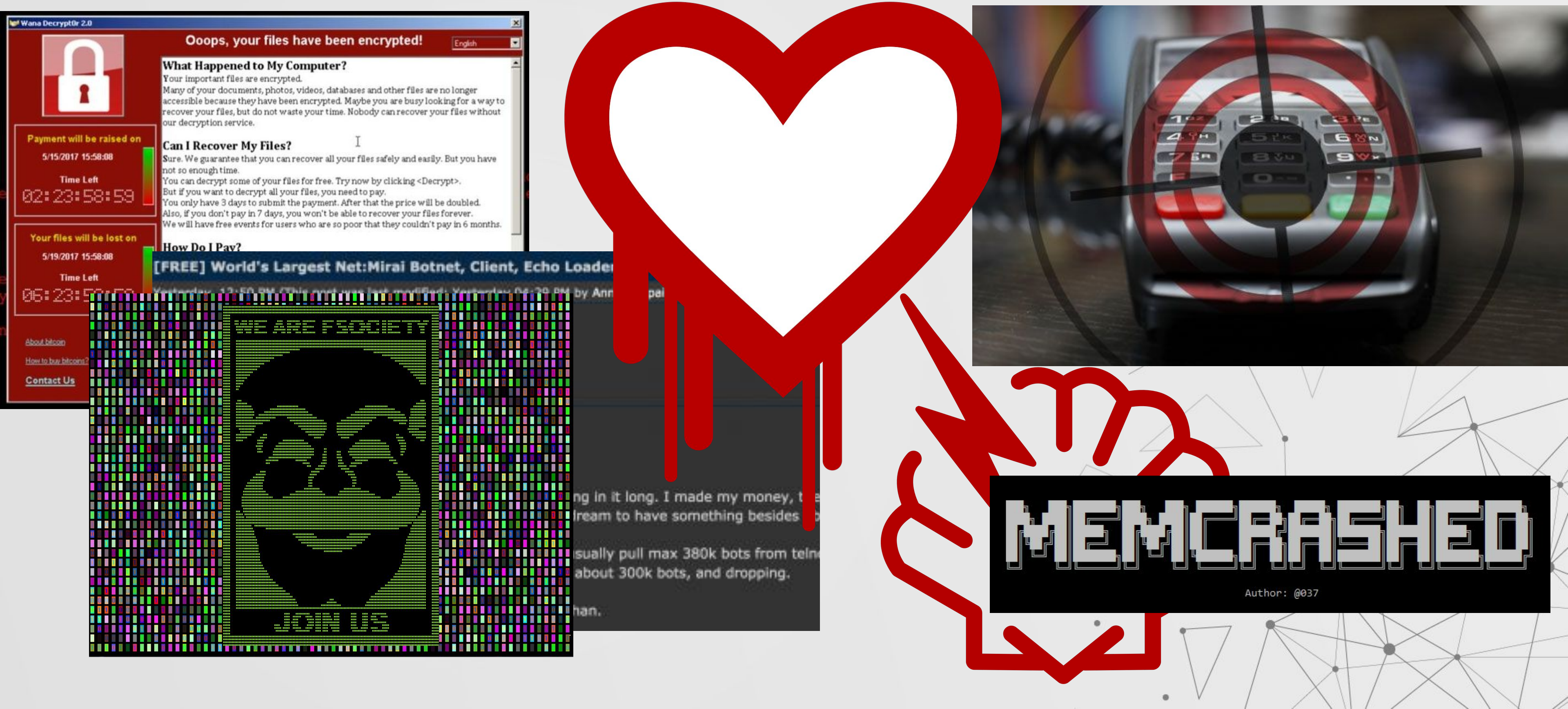
Individuals ability to influence

- Individuals can have a massive impact
  - *DoOcracy*
  - Broad range of views / backgrounds / disciplines

- Sometimes these are positive
  - *Sometimes **not***

- **Delicate**

Crises change things fast



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:5

About bitcoin

How to buy bitcoins?

Contact Us

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

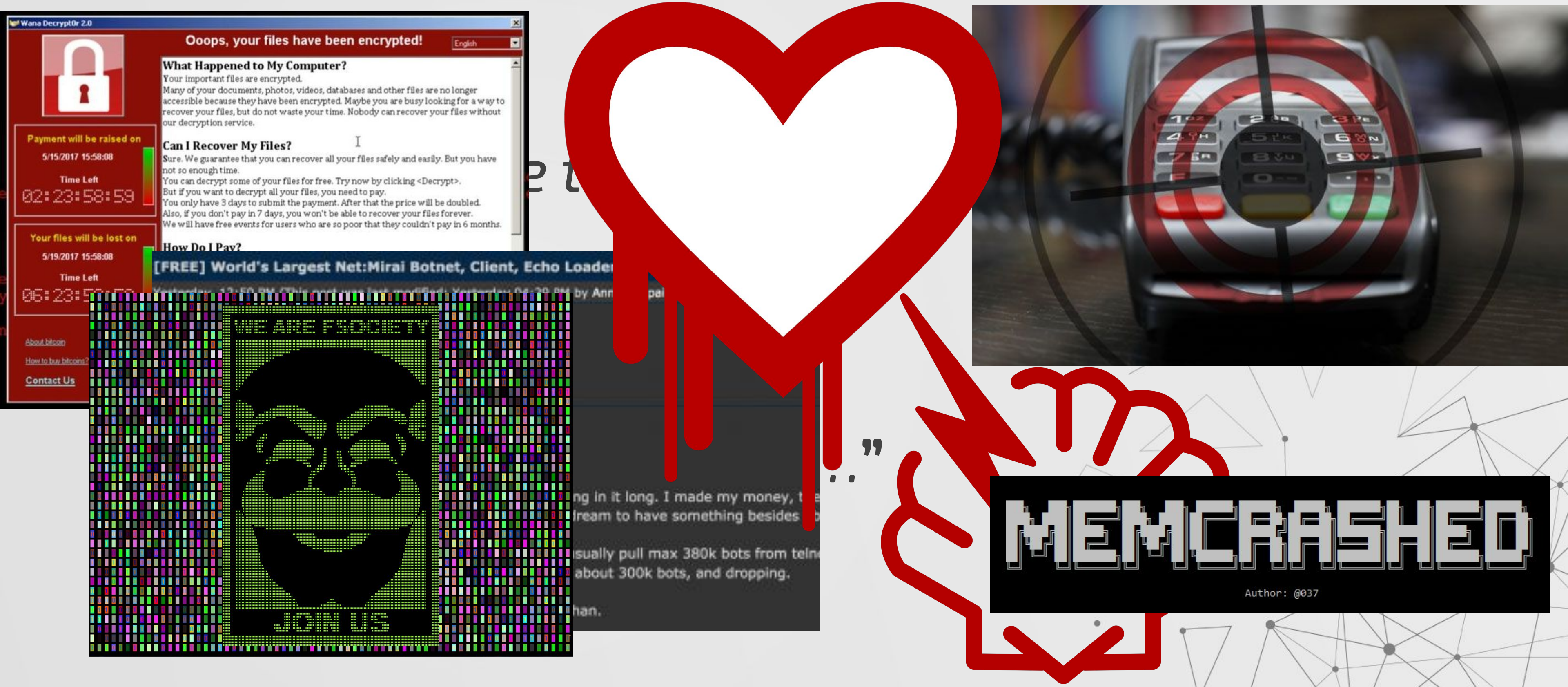
[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader

by Ann pai

ng in it long. I made my money, t e
lream to have something besides

sually pull max 380k bots from teln
about 300k bots, and dropping.

han.



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader

ng in it long. I made my money, t

lream to have something besides

isually pull max 380k bots from teln
about 300k bots, and dropping.

han.

How to create a crisis…101

Northeast Collegiate Cyber Defense Competition (NECCDC) (March 2017)

- College Blue Team exercise
  - Blue Team - Students
  - Red Team - Industry professionals

- **Business Responsibilities + Technical Abilities**

Northeast Collegiate Cyber Defense Competition (NECCDC)

Kobayashi-Maru

The IT Crowd

How do we up the “real” factor?

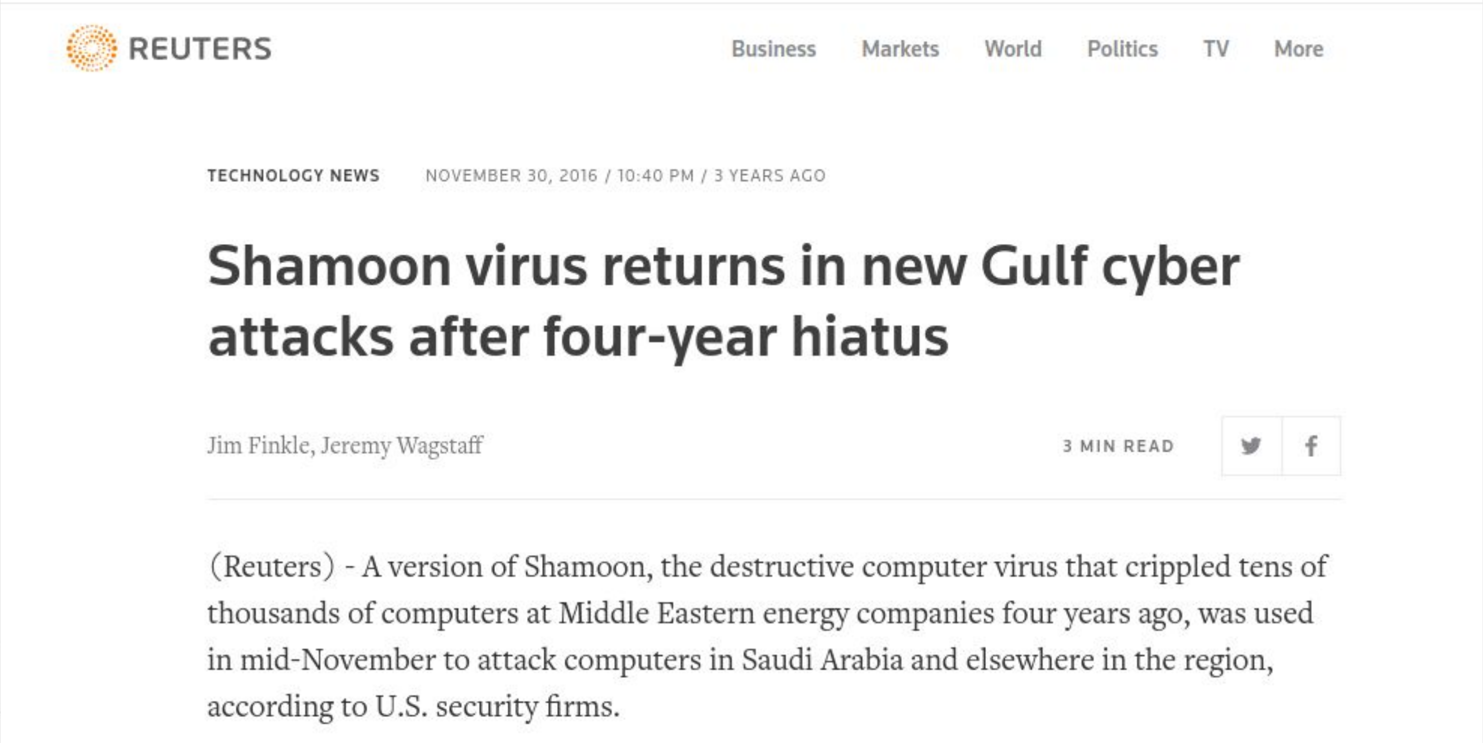
🚫 Simulate a DDoS?

🚫 Sudden hardware loss?

🚫 Intentionally create a vuln in some of their software?

🚫 Sudden Student loss?

Replicate a recent attack?



TECHNOLOGY NEWS NOVEMBER 30, 2016 / 10:40 PM / 3 YEARS AGO

Shamoon virus returns in new Gulf cyber attacks after four-year hiatus

Jim Finkle, Jeremy Wagstaff

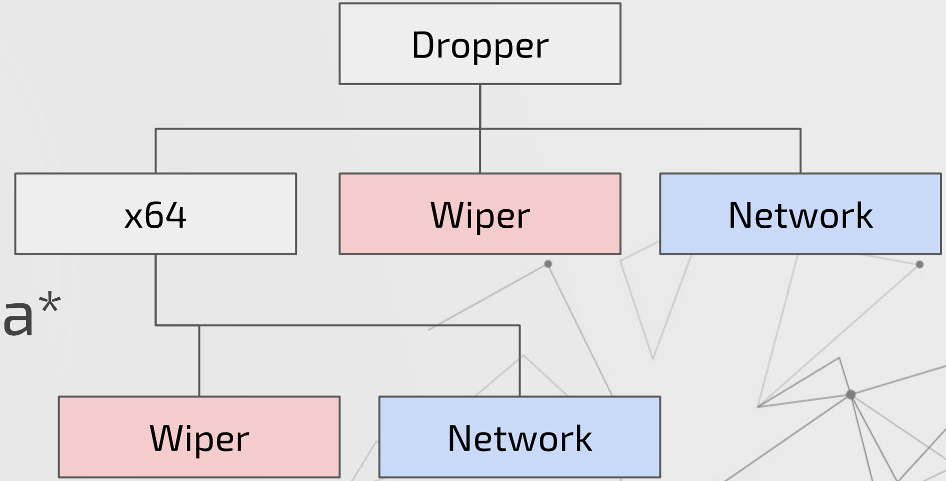
3 MIN READ

(Reuters) - A version of Shamoon, the destructive computer virus that crippled tens of thousands of computers at Middle Eastern energy companies four years ago, was used in mid-November to attack computers in Saudi Arabia and elsewhere in the region, according to U.S. security firms.

Shamoon
(DistTrack)

- Destructive malware
  - Overwrites files with embedded image
- Suspected Iranian
  - Targeting: Saudi Arabia*
- 2012 / 2016-2017 *

- **Usage in 2012 against Saudi Aramco**
  - Wiped 35,000 systems



Shamoon
(DistTrack)

- **What we wanted / What Shamoon would do**
  - *Preventable (ish)*
  - Current / topical
  - Would impact teams - even if they had evicted the Red Team
  - *New technique for the Red Team*

Replication

Tooling

- Can the same tools be used?
- Can we *control* those tools?

Procedures

- Can we recreate the same steps the actor used?

Control

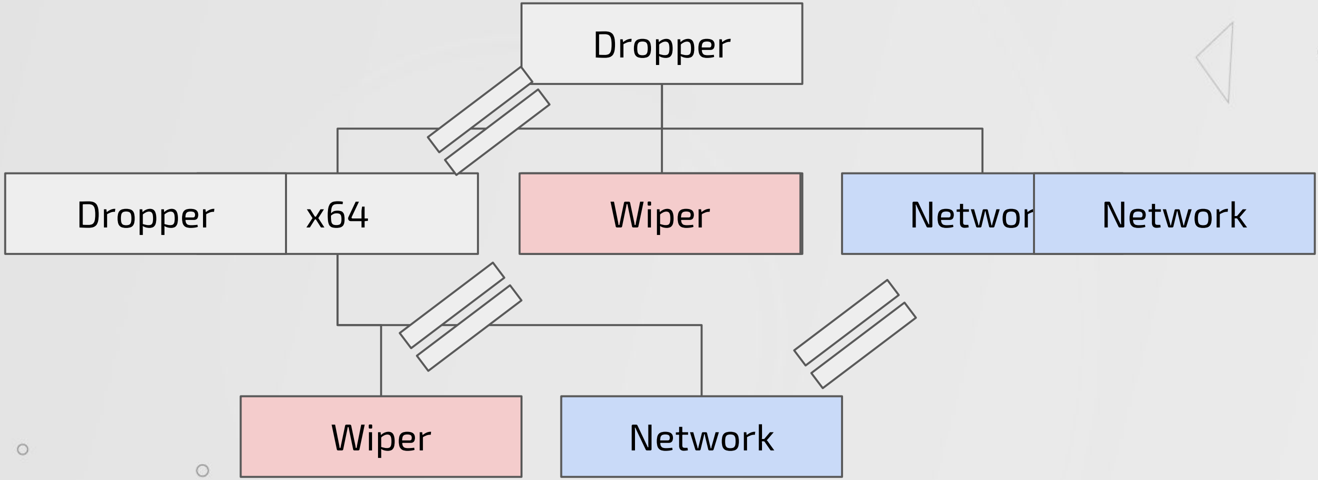
- Can we control the situation to not impact real world research?

Planned outcome

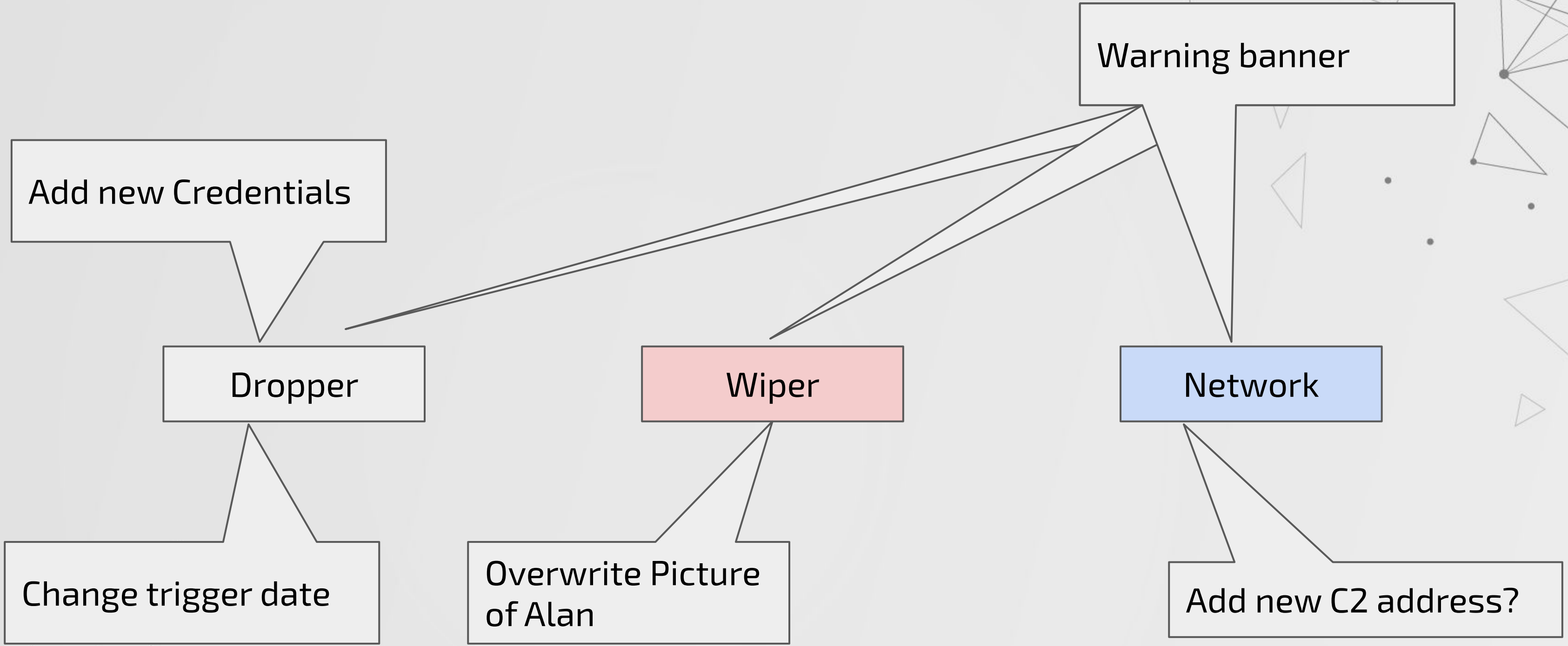
- **Students could say they'd experienced a wiper attack**
  - Recover from backups?
  - What to bring up first?

- If we lost access after the first day
  - Still be able to fulfil objectives

Malware Necromancy



Malware Necromancy



Warning banner

Add new Credentials

Dropper

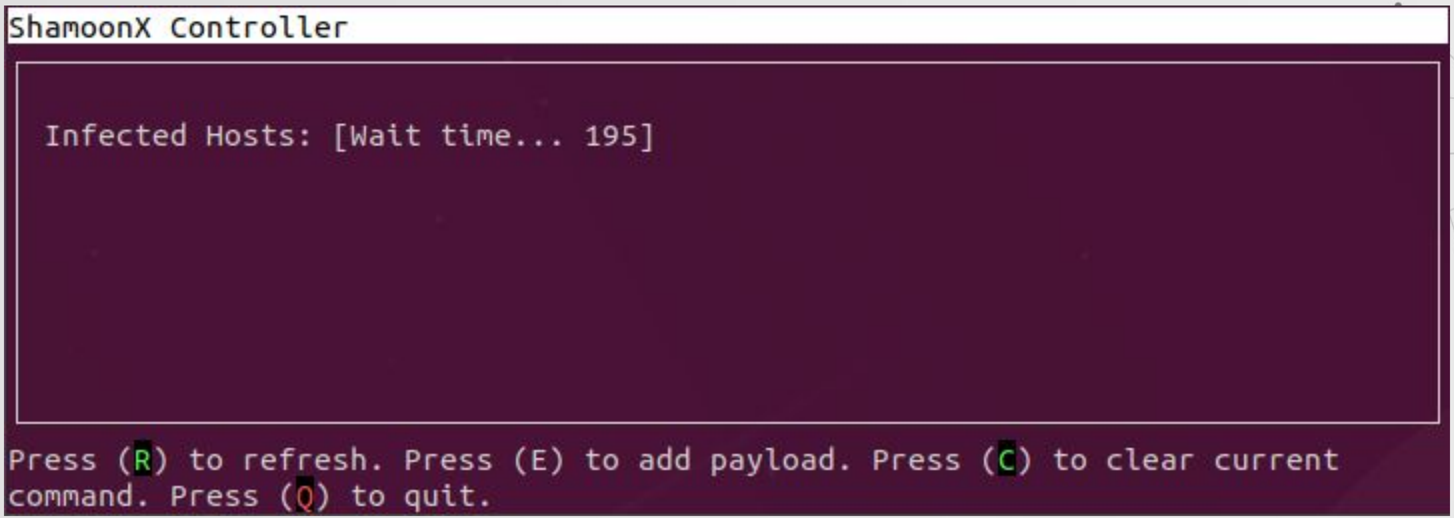
Wiper

Network

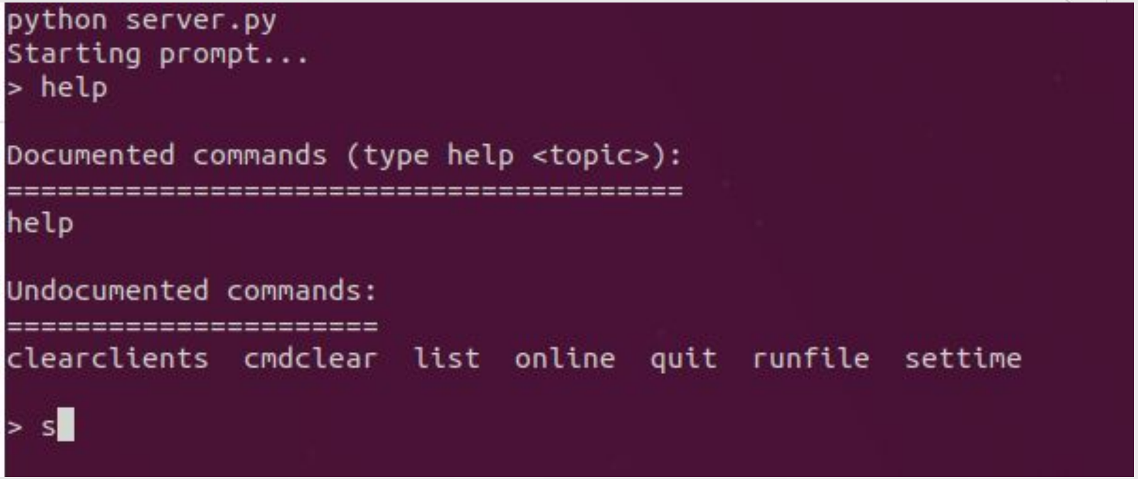
Change trigger date

Overwrite Picture of Alan

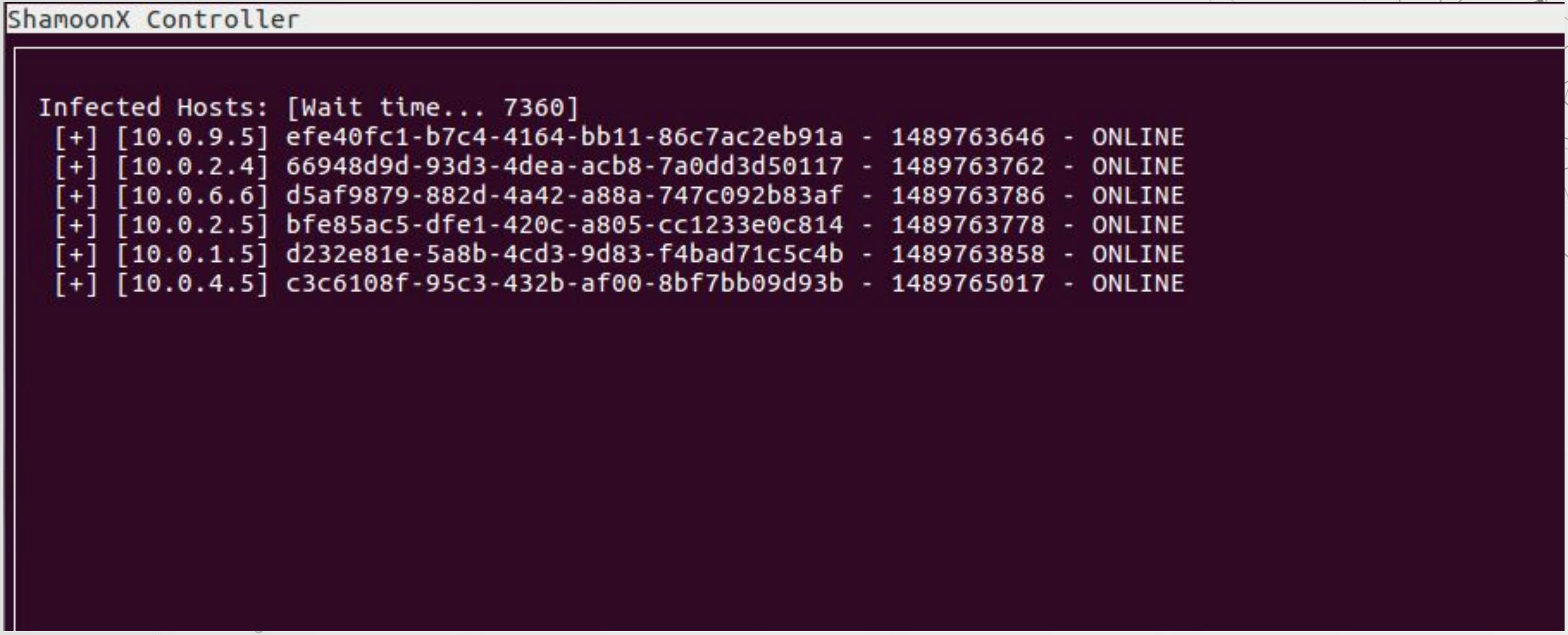
Add new C2 address?



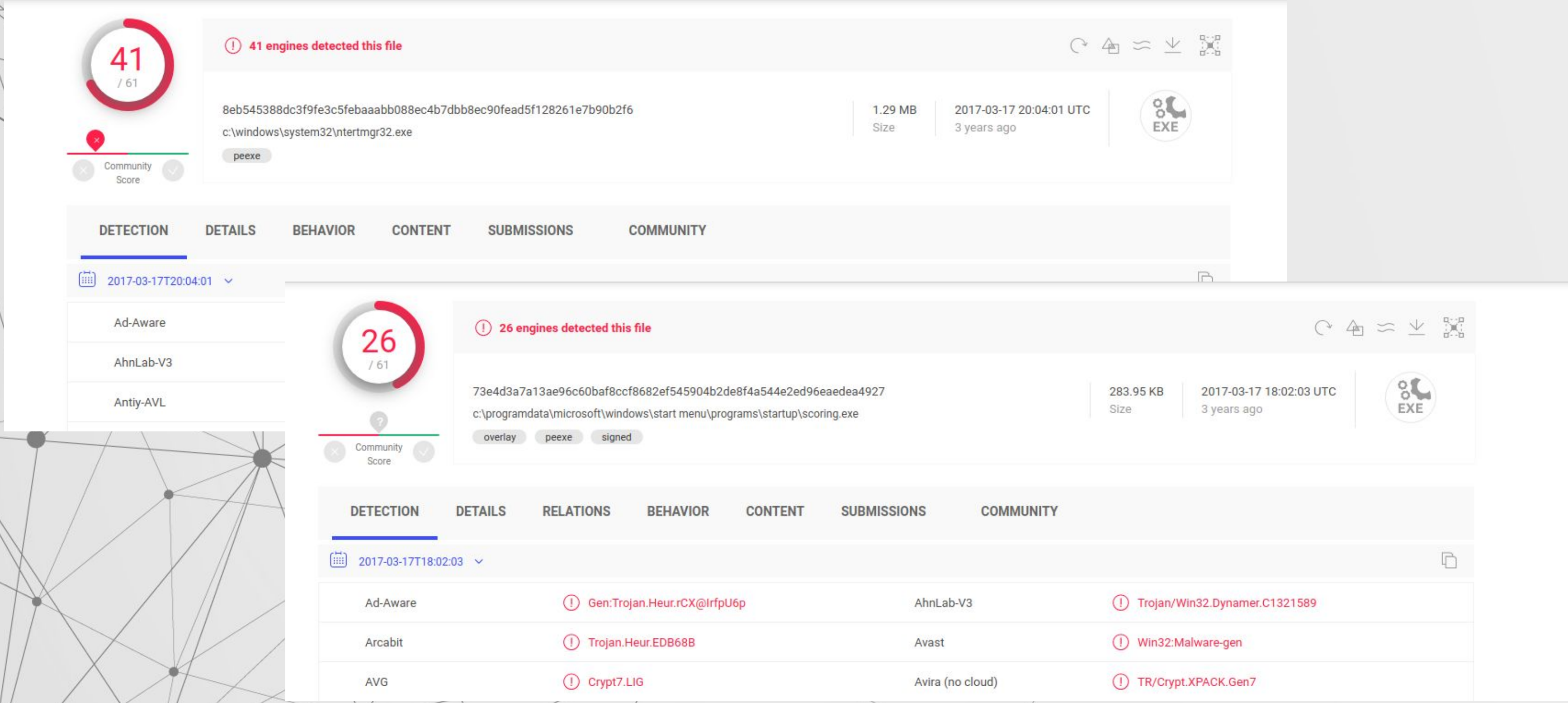
```
ShamoonX Controller

 Infected Hosts: [Wait time... 195]

Press (R) to refresh. Press (E) to add payload. Press (C) to clear current
command. Press (Q) to quit.
```



```
python server.py
Starting prompt...
> help

Documented commands (type help <topic>):
========================================
help

Undocumented commands:
======================
clearclients  cmdclear  list  online  quit  runfile  settime

> s
```



```
Infected Hosts: [Wait time... 7360]
 [+] [10.0.9.5] efe40fc1-b7c4-4164-bb11-86c7ac2eb91a - 1489763646 - ONLINE
 [+] [10.0.2.4] 66948d9d-93d3-4dea-acb8-7a0dd3d50117 - 1489763762 - ONLINE
 [+] [10.0.6.6] d5af9879-882d-4a42-a88a-747c092b83af - 1489763786 - ONLINE
 [+] [10.0.2.5] bfe85ac5-dfe1-420c-a805-cc1233e0c814 - 1489763778 - ONLINE
 [+] [10.0.1.5] d232e81e-5a8b-4cd3-9d83-f4bad71c5c4b - 1489763858 - ONLINE
 [+] [10.0.4.5] c3c6108f-95c3-432b-af00-8bf7bb09d93b - 1489765017 - ONLINE
```



41 / 61

41 engines detected this file

8eb545388dc3f9fe3c5febaaabb088ec4b7dbb8ec90fead5f128261e7b90b2f6

c:\windows\system32\ntertmgr32.exe

peexe

1.29 MB Size

2017-03-17 20:04:01 UTC 3 years ago

2017-03-17T20:04:01

Ad-Aware

AhnLab-V3

Antiy-AVL

26 / 61

26 engines detected this file

73e4d3a7a13ae96c60baf8ccf8682ef545904b2de8f4a544e2ed96eaedea4927

c:\programdata\microsoft\windows\start menu\programs\startup\scoring.exe

overlay peexe signed

283.95 KB Size

2017-03-17 18:02:03 UTC 3 years ago

2017-03-17T18:02:03

Ad-Aware	Gen:Trojan.Heur.rCX@lrfpU6p	AhnLab-V3	Trojan/Win32.Dynamer.C1321589
Arcabit	Trojan.Heur.EDB68B	Avast	Win32:Malware-gen
AVG	Crypt7.LIG	Avira (no cloud)	TR/Crypt.XPACK.Gen7

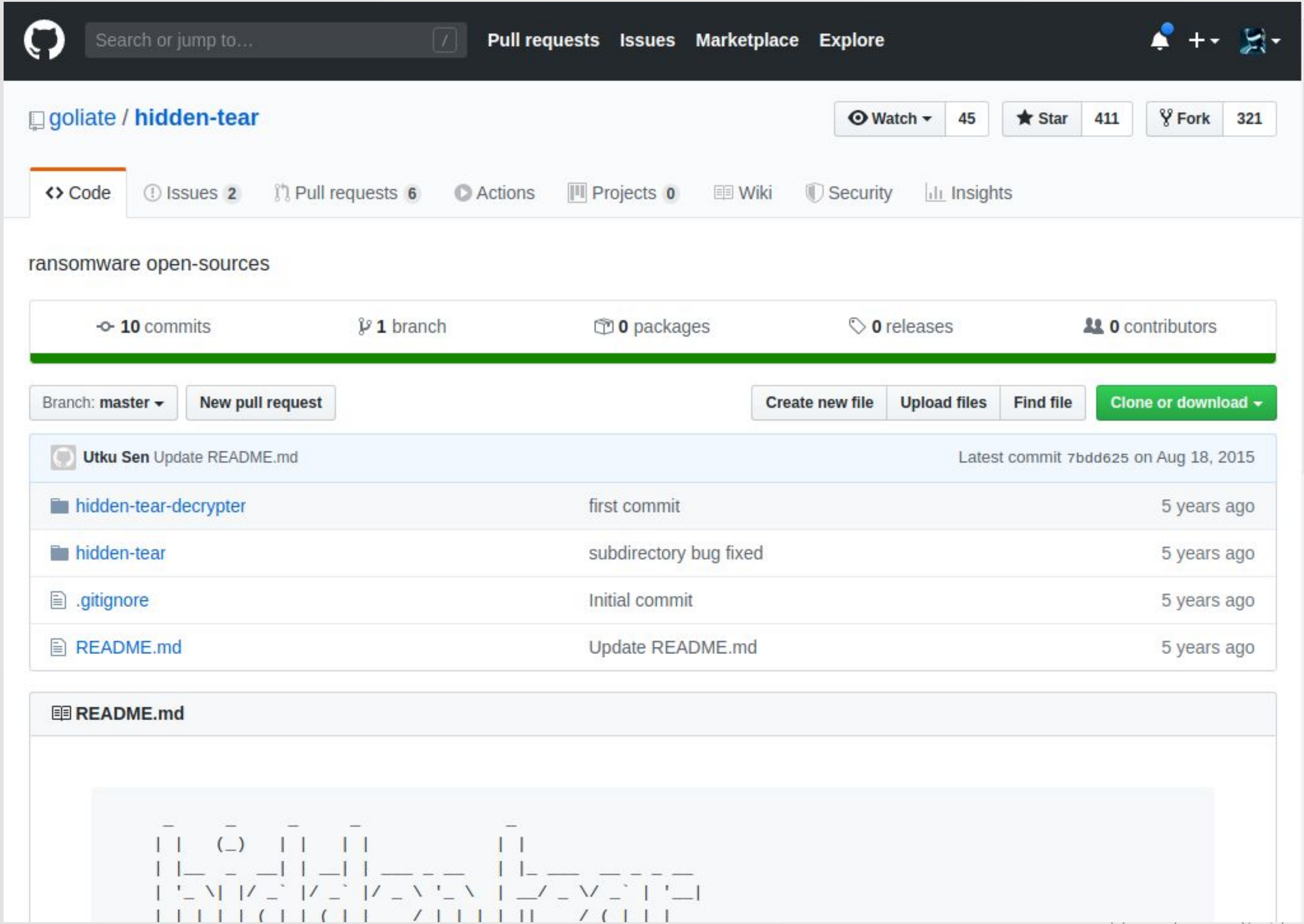
Immediate Fallout

- *Bad hot-takes lead to bad responses*
  - [Rumor] Spread to other university systems
  - [Rumor] External spreading

- **Saudi Arabia late notification**

Fallout

- *~~Never~~ stopped to think if I should*
- Lose ban on future use replayed tooling
- Became a topic I haven’t wanted to talk about in years
- **Request to Open-Source?**



ransomware open-sources

10 commits · 1 branch · 0 packages · 0 releases · 0 contributors

Utku Sen Update README.md — Latest commit 7bdd625 on Aug 18, 2015

hidden-tear-decrypter	first commit	5 years ago
hidden-tear	subdirectory bug fixed	5 years ago
.gitignore	Initial commit	5 years ago
README.md	Update README.md	5 years ago

README.md

```
 _     _     _     _              _
| |   (_)   | |   | |            | |
| |__  _  __| | __| | ___ _ __   | |_ ___  __ _ _ __
| '_ \| |/ _` |/ _` |/ _ \ '_ \  | __/ _ \/ _` | '__|
```

Long Fallout

- Limited (if any) public reporting
    - *Lot of folks **aware***

- Students had a really unique experience

- Could have been (and may be) a lot worse
    - Technical model for future false flag operations?
    - *Would [we] even know?*

Why this matters

My Oppenheimer's Paradox

- The reason I tell this story
  - Good intention -> (nearly) bad outcome
  - Past actions != future results

- Caught up in the moment - the can we do this
  - Not enough should we do this?

- **Open-sourcing now vs then**

Summary

- We all share responsibility for the future
  - Individually capable of massive impacts (Intentionally or accidentally
- **Own and evaluate your actions**

<3 the Crisis

- Look at crises as tests
  - What worked?
  - What can we do better?
  - What can we do to prevent it in the future?

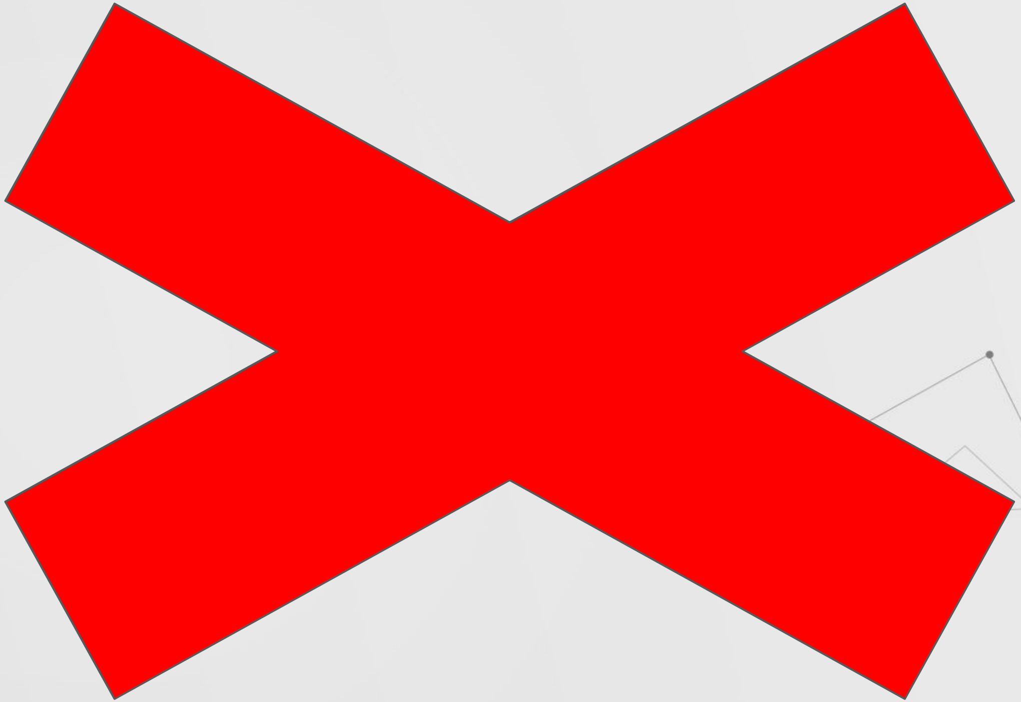
  - See the path through the forest

- **Problems are the first step to solutions**

Thanks

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**.

Please keep this slide for attribution.



How changes

“Hacking Tools” should be illegal

We need more tools to find security flaws

Offsec tools help bad actors over defenders

More Dev-Sec-Ops!

Licensed users only

Indicators are irrelevant. Share TTPs!

Hashes or it didn’t happen

“*Zero-Day Hashes*”

Trusted Partners only

IoCs must openly shared

Actors change we we drop IoCs

Cobalt Strike Beacon Tracker

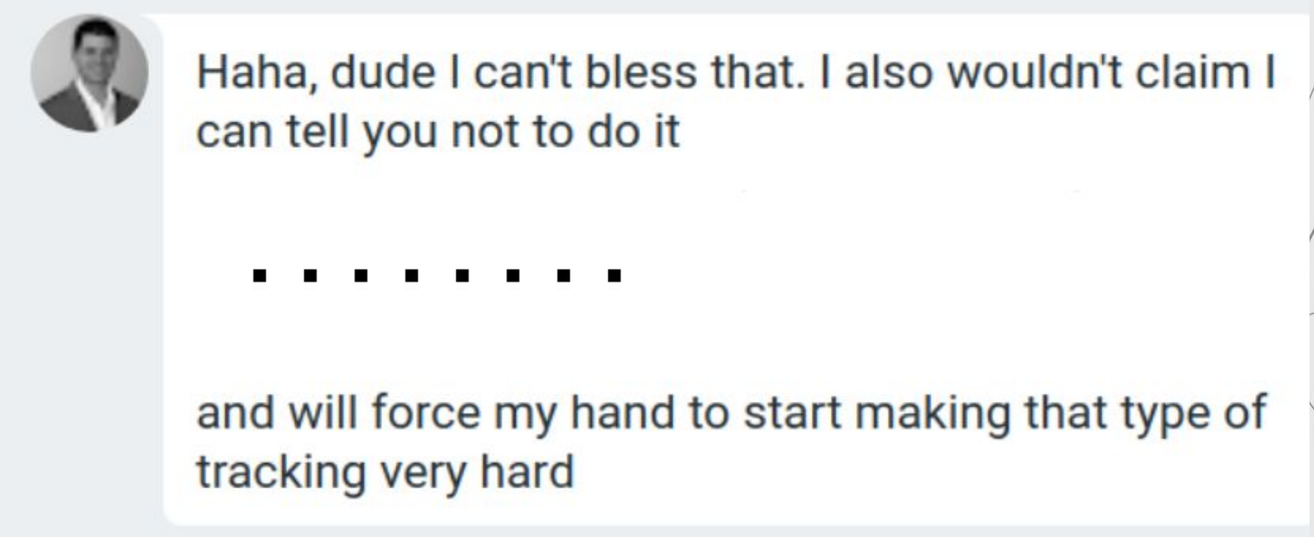
- Public decoding / tracking of Cobalt Strike copies
  - Like ZeusTracker

- Freely provide ongoing & historic indicators

Screenshot?

This will be great! Everyone will find it useful! Open all the data

This will be great! Everyone will find it useful! Open all the data



Haha, dude I can't bless that. I also wouldn't claim I can tell you not to do it

....

and will force my hand to start making that type of tracking very hard

Why am I doing this?

Cobalt Strike Beacon Tracker

- Short Term Win - vs - Long Term Loss
  - *Arms race* with Raphael

- **Am I doing this for me?**
- What provides the greater good?