Hacking Apple to Hack Dropbox

RIPE78
Theodor
Ragnar
Gíslason

SYNDIS
Creative[in]Security

Adversary

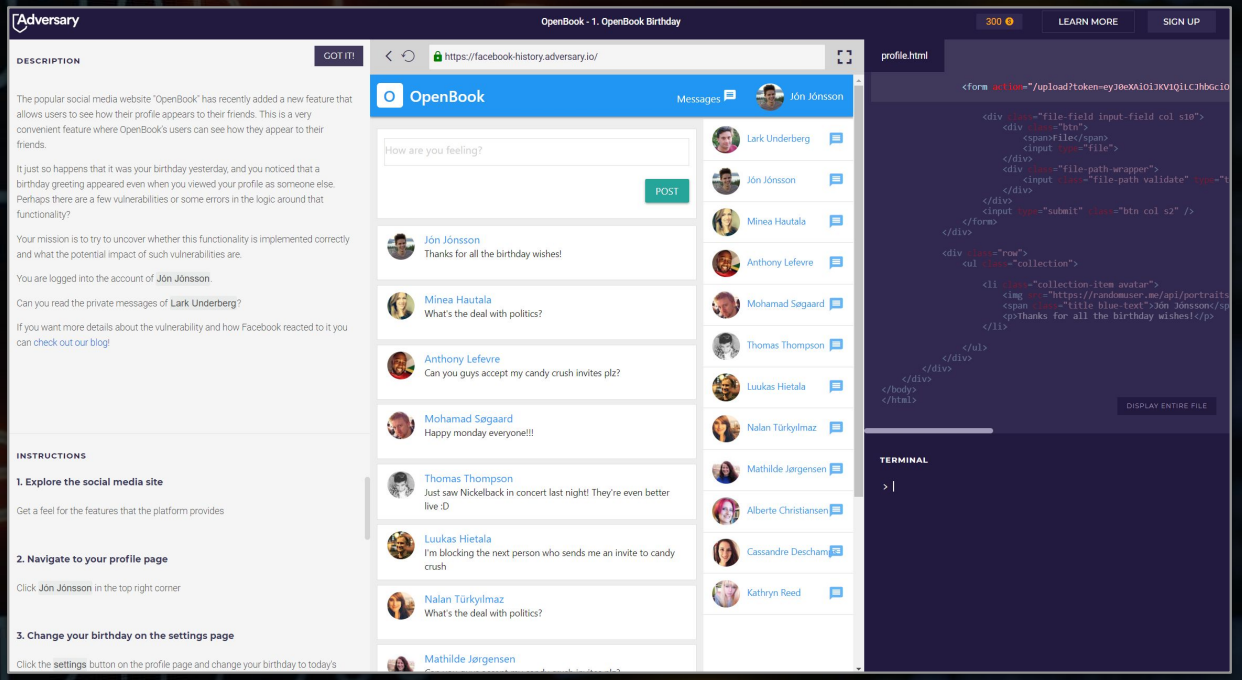
SYNDIS

Creative[in]Security

SERVICES TEAM LABS

https://syndis.is

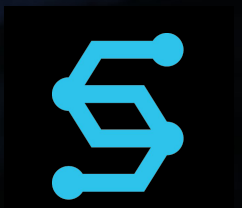
Adversary



https://adversary.io

This talk today

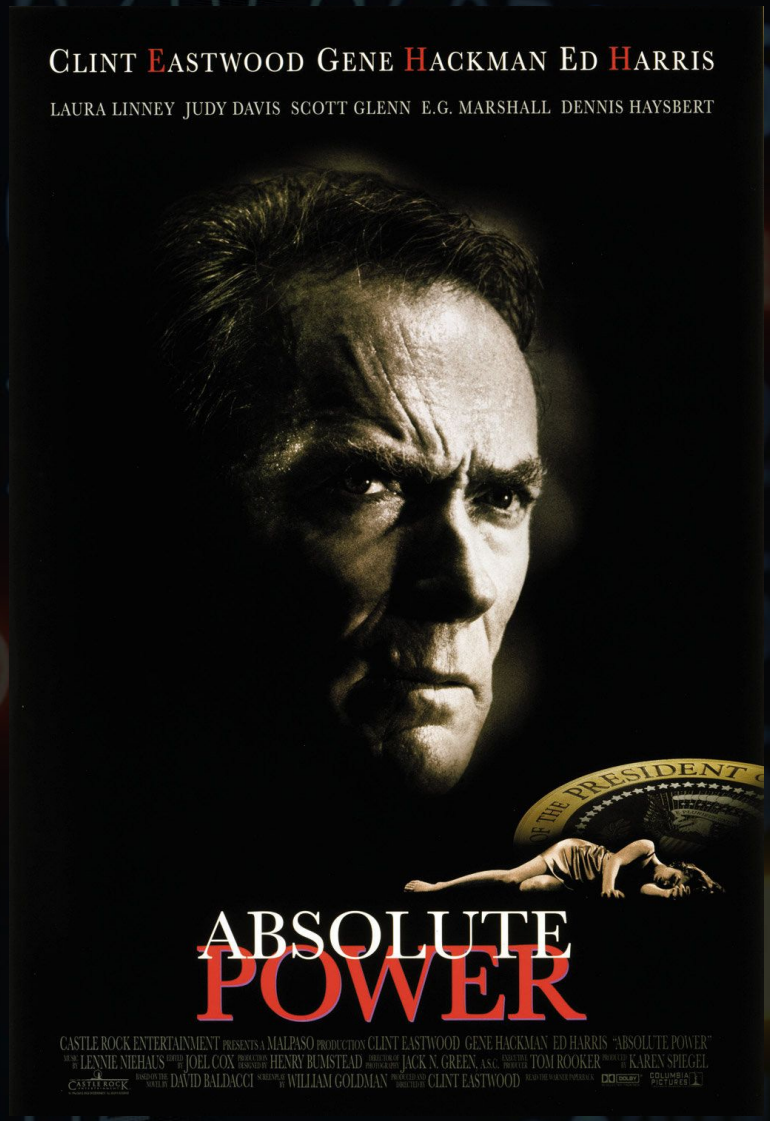
- You are the target!
- Dropbox red team engagement
- Constantly evolving cyber battlefield
- The cost of finding and exploiting a 0-day vulnerability
- Who are you defending against



You are the target!

Cambridge Analytica

You are the target!



You are the target!

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

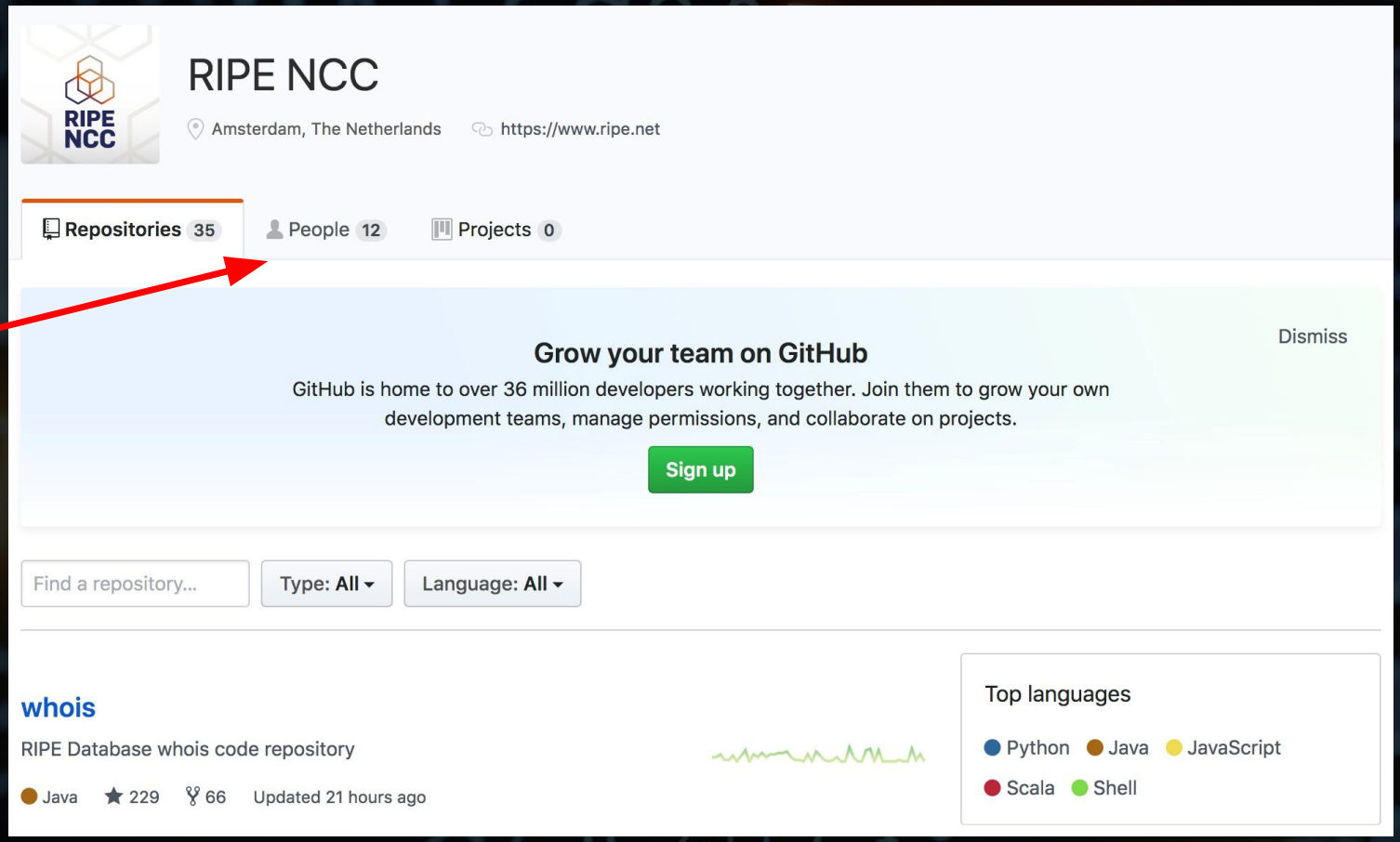
HashiCorp Vagrant

GitLab

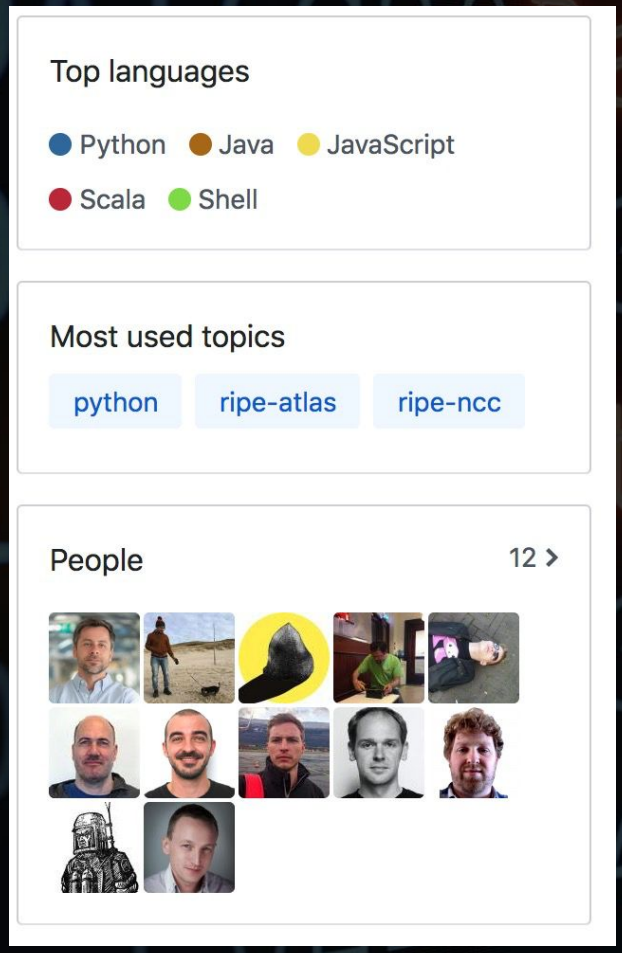
You are the target!

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

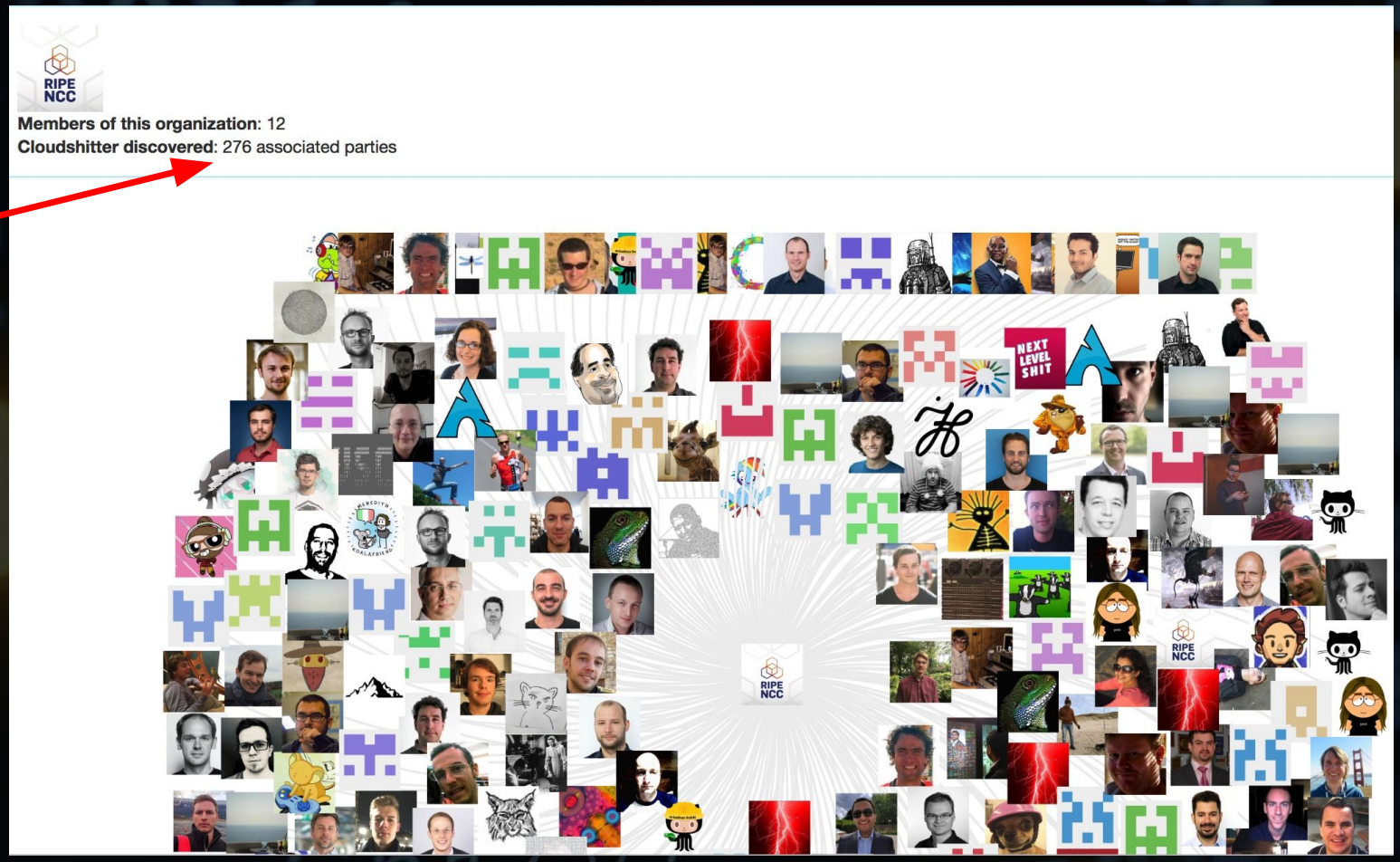
You are the target!



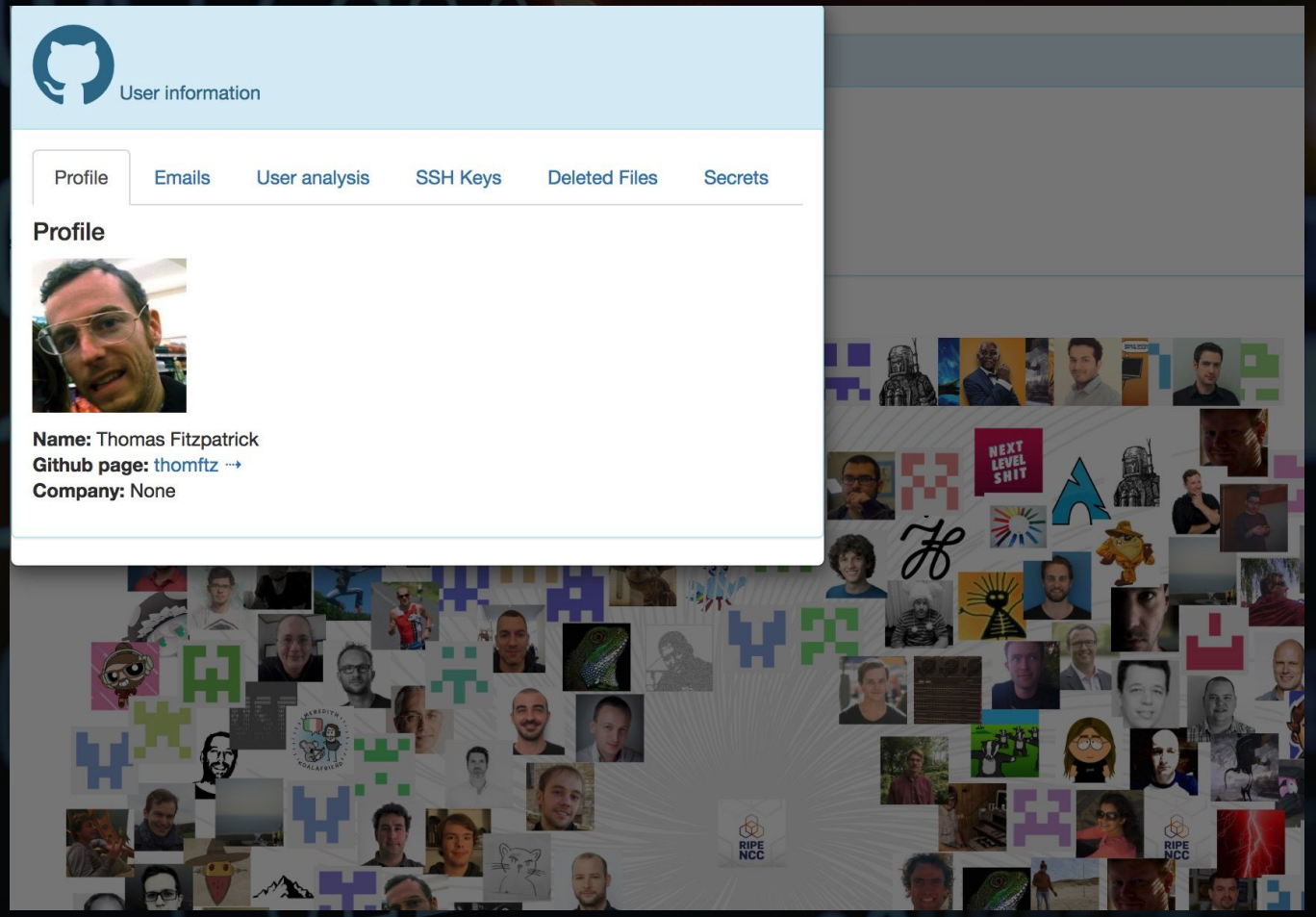
You are the target!



What do engineers do? We build things(tools) of course



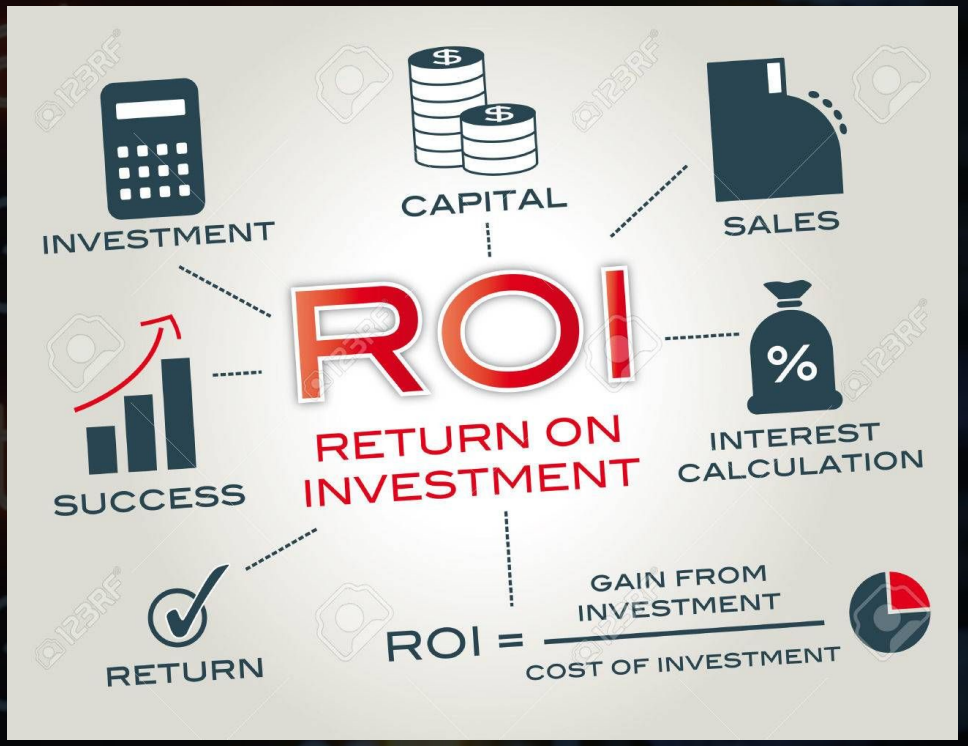
What do engineers do? We build things(tools) of course



Dropbox red team engagement

https://blogs.dropbox.com/tech/2018/11/offensive-testing-to-make-dropbox-and-the-world-a-safer-place/

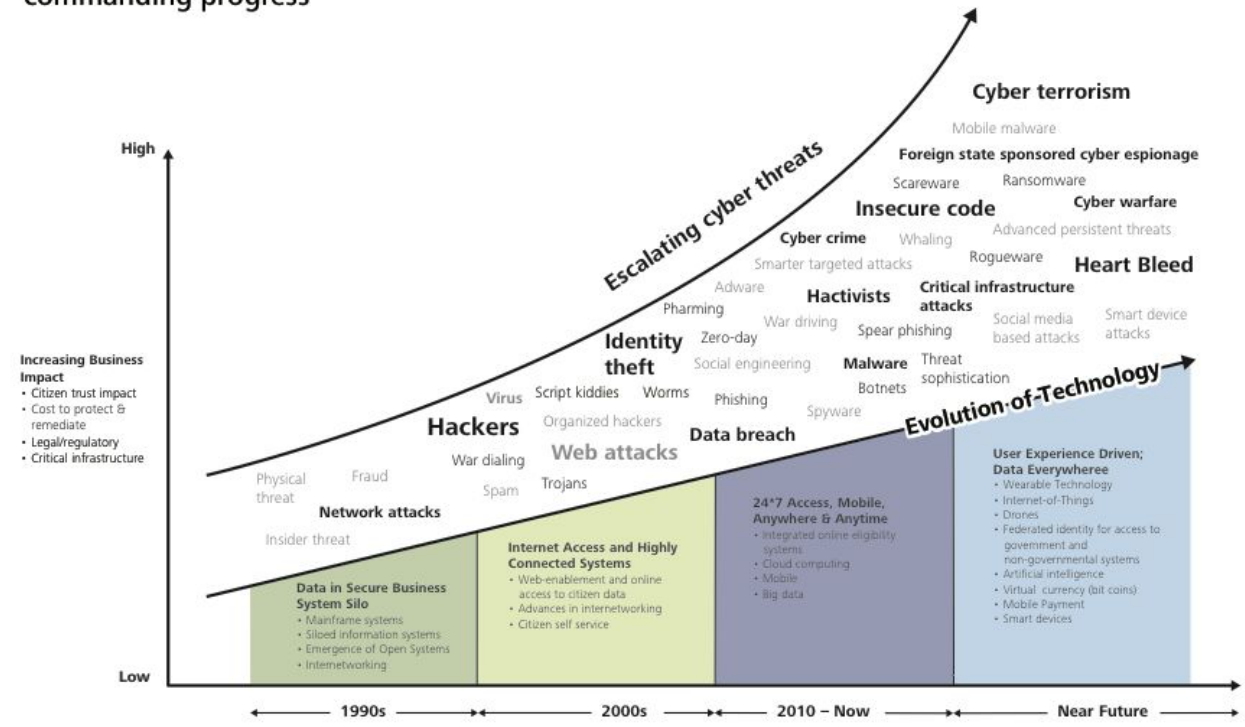
Dropbox red team engagement



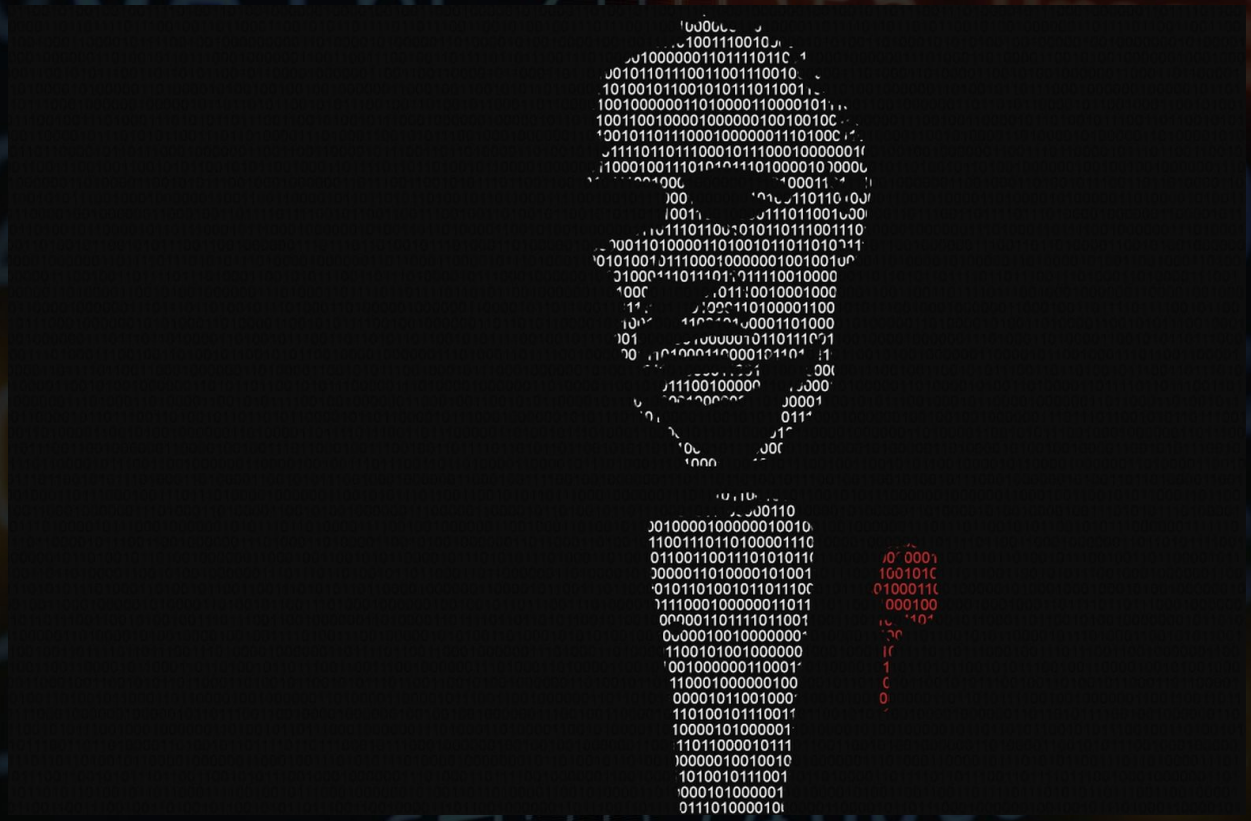
Dropbox red team engagement

The continually evolving cyber battlefield

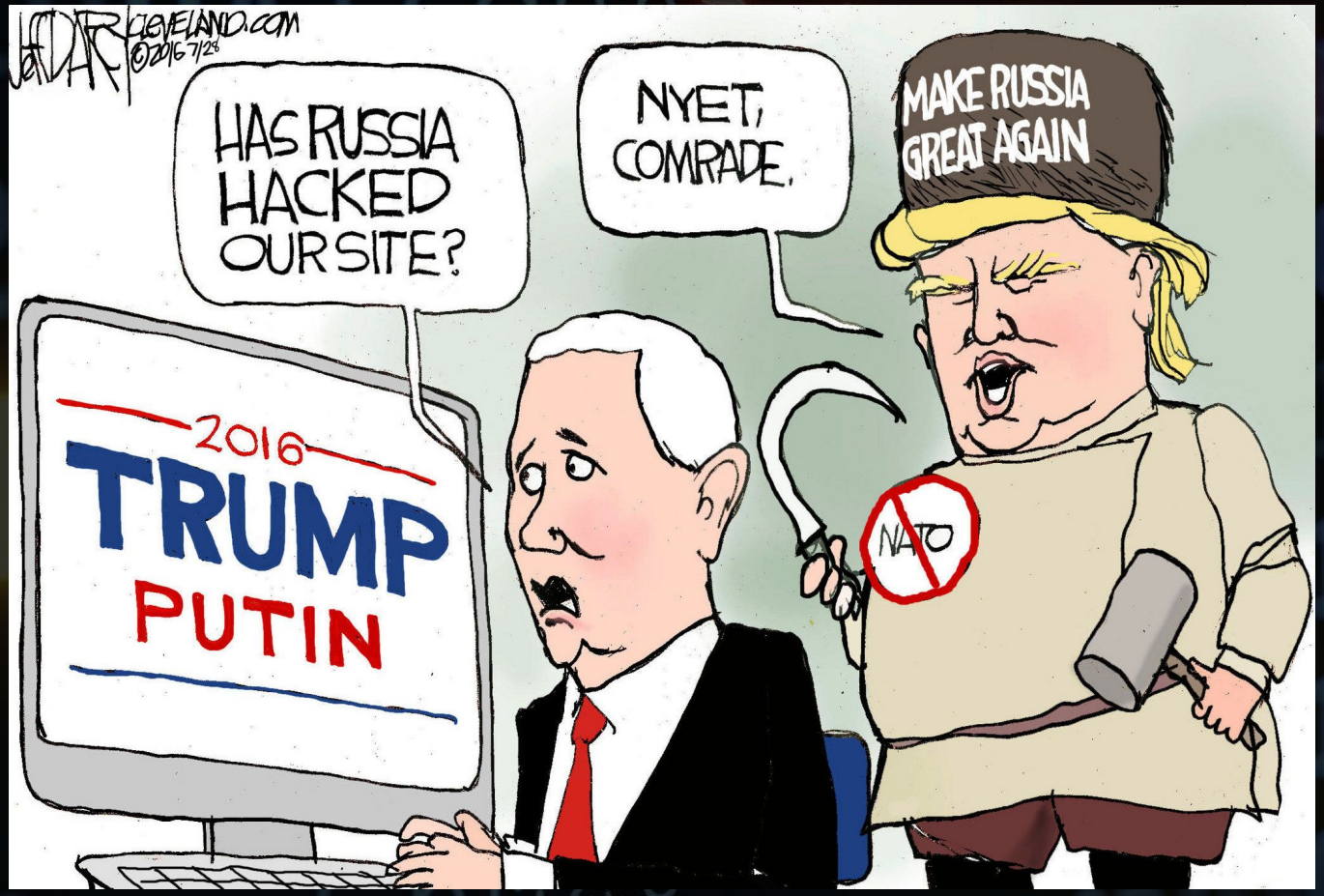
Figure 29: Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress



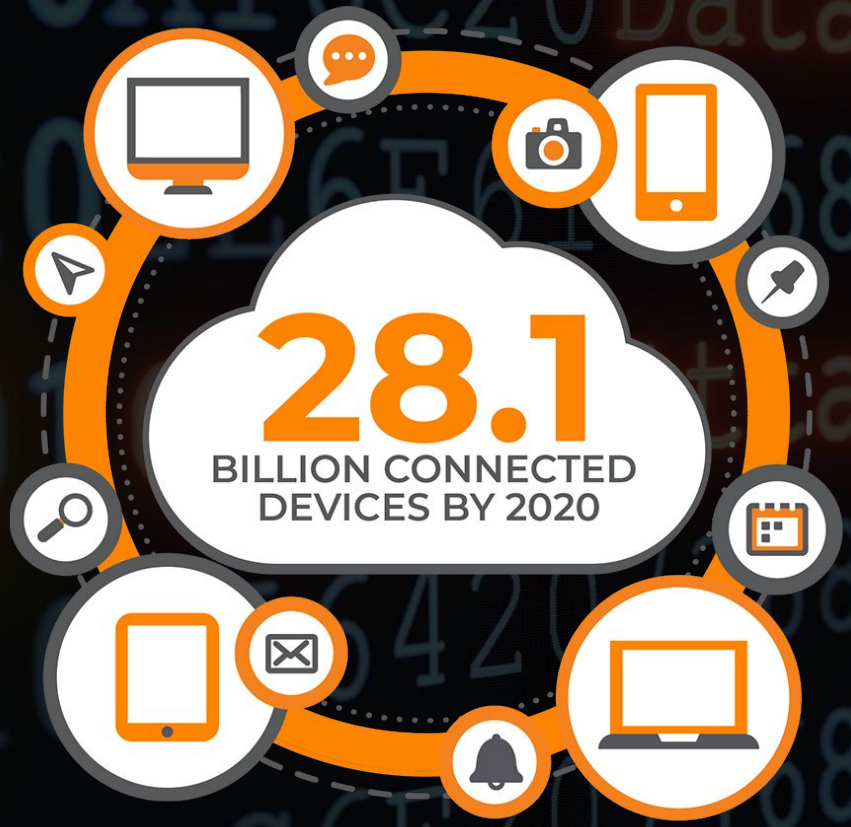
Organized crime and fraud is rampant



Nation state attack teams can change history



The fruits are RIPE for the picking



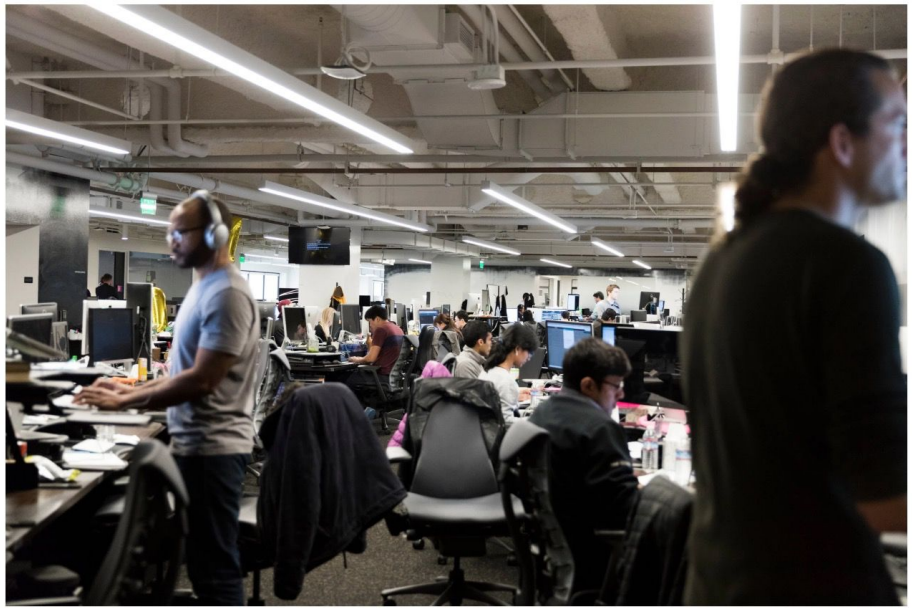
https://safeatlast.co/blog/iot-statistics/

A trend is emerging?

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Hackers are realizing that data itself is valuable

Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data



Uber's headquarters in San Francisco. The ride-hailing company said information on driver and rider names, emails and telephone numbers had been compromised in a data breach.

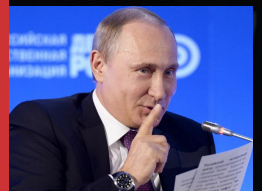
Ryan Young for The New York Times

Lets turn our attention to Apple (*MacOS X*)

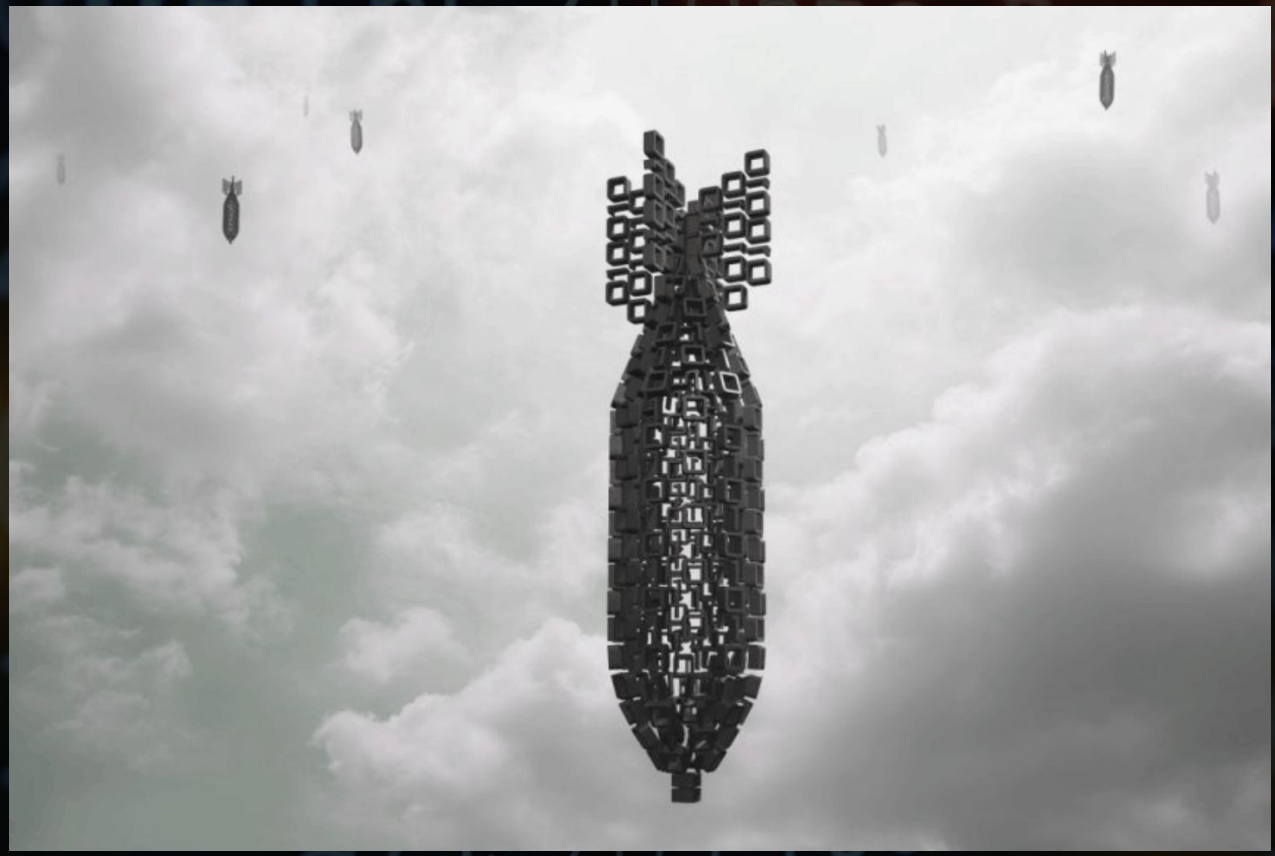
“0day” (*Zeroday*) vulnerabilities in a project

What is this “*Zeroday*” word anyway?

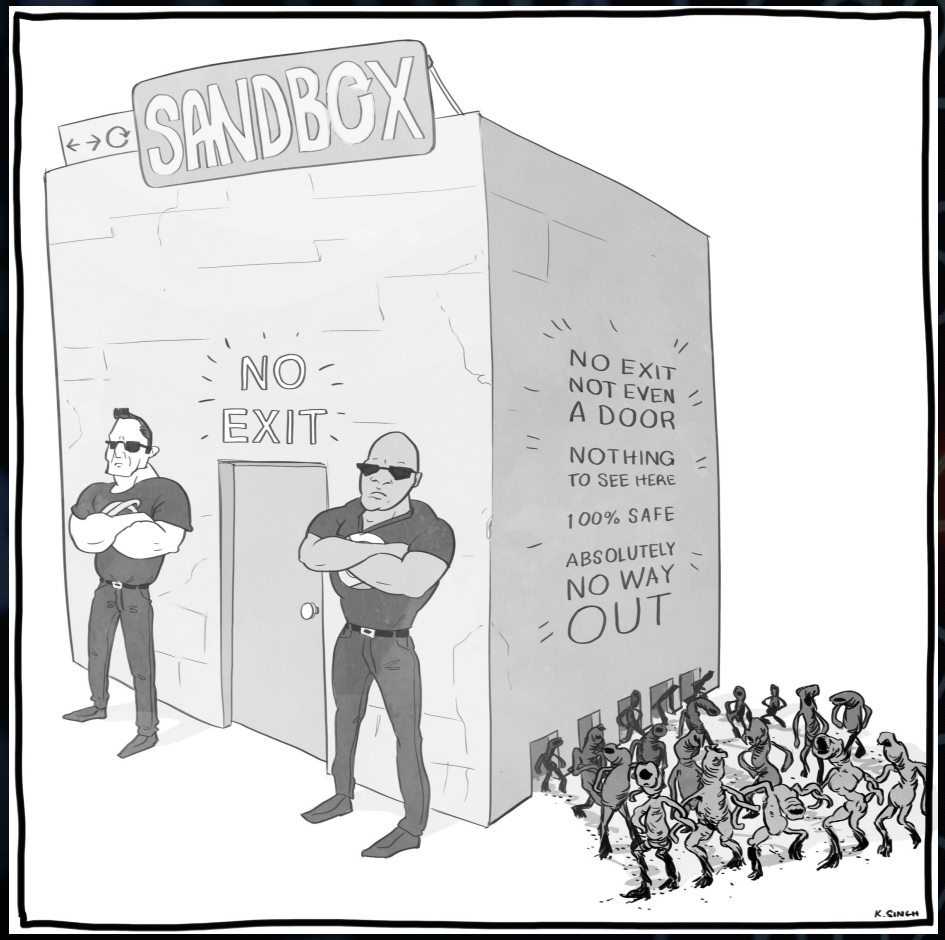
“A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network. An exploit directed at a zero-day is called a zero-day exploit, or zero-day attack.”



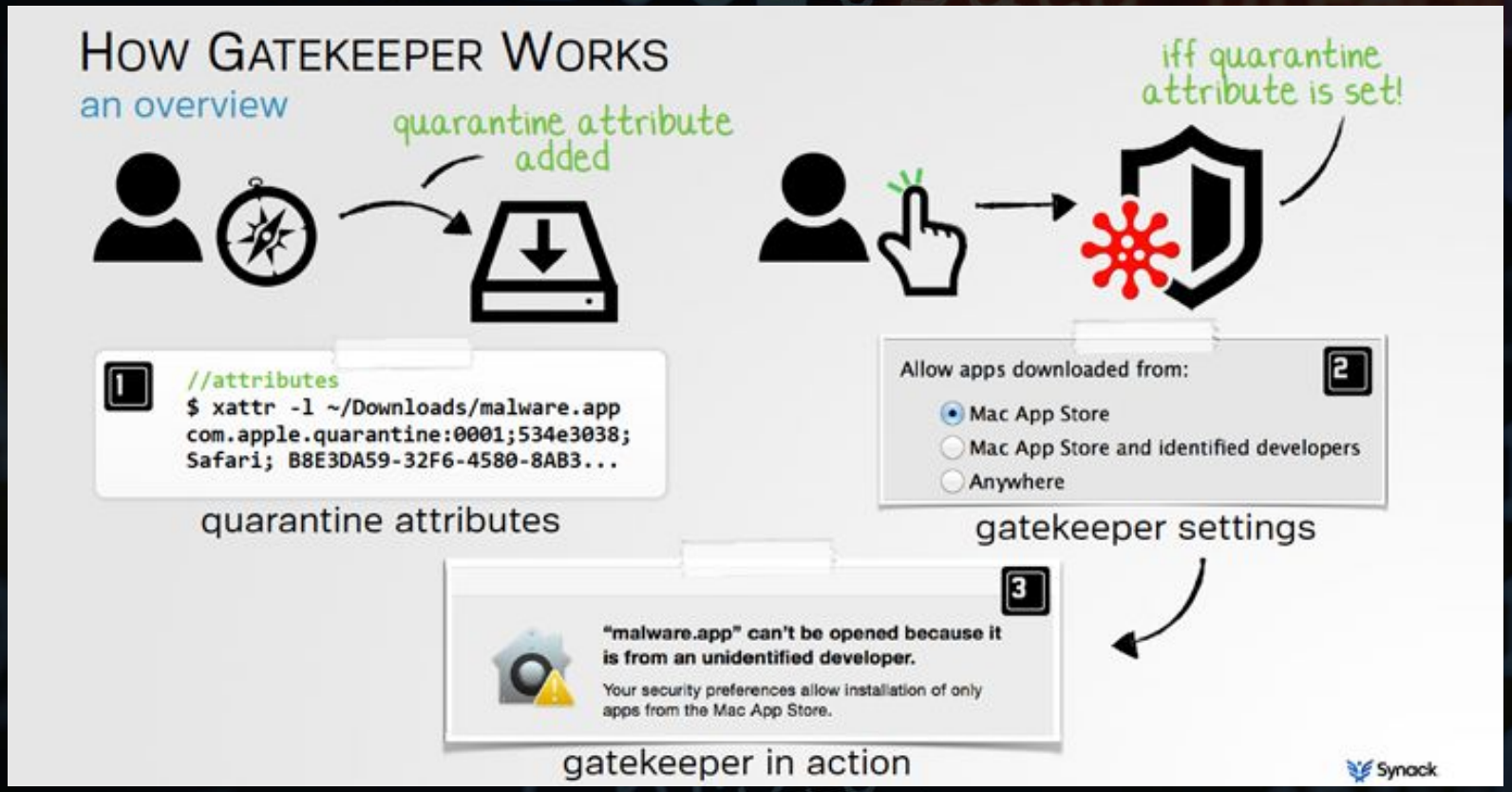
It’s a cyber bomb



What about defenses, they are pretty good?



Modern operating systems have pretty strong security controls that need to be bypassed



https://support.apple.com/en-us/HT208692

CoreTypes

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6

Impact: Processing a maliciously crafted webpage may result in the mounting of a disk image

Description: A logic issue was addressed with improved restrictions.

CVE-2017-13890: Apple, Theodor Ragnar Gislason of Syndis

Disk Images

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6, macOS High Sierra 10.13.3

Impact: Mounting a malicious disk image may result in the launching of an application

Description: A logic issue was addressed with improved validation.

CVE-2018-4176: Theodor Ragnar Gislason of Syndis

LaunchServices

Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6, macOS High Sierra 10.13.3

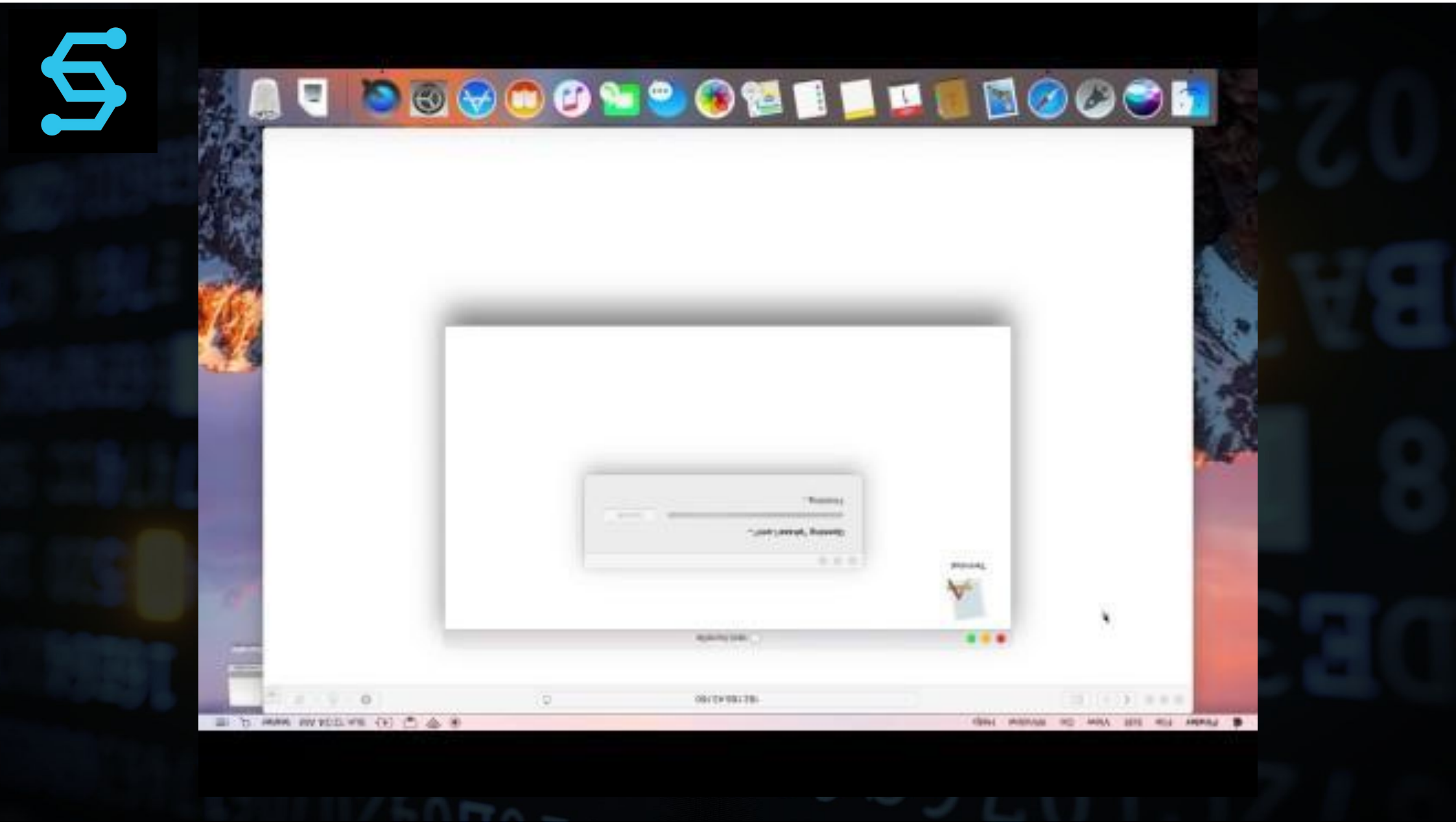
Impact: A maliciously crafted application may be able to bypass code signing enforcement

Description: A logic issue was addressed with improved validation.

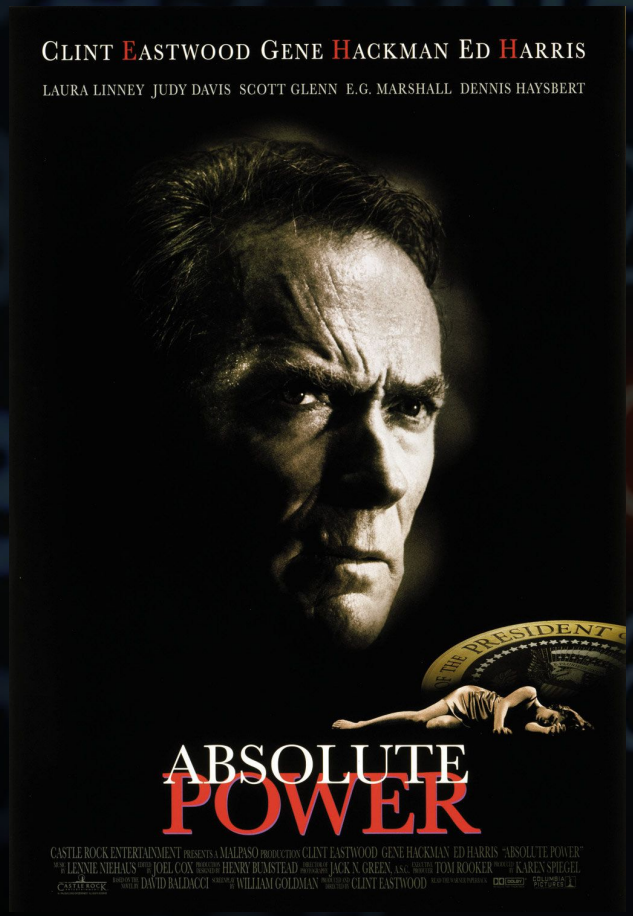
CVE-2018-4175: Theodor Ragnar Gislason of Syndis

And indeed it required three different vulnerabilities to create this “cyber bomb”


Demo Time!



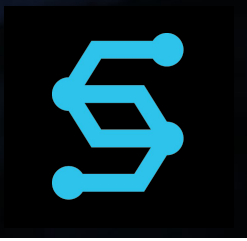
With that we could have broken into practically EVERY Mac on the planet!



How much is it worth on the open market (not for weapons sales)

Target	Escape Options	Prize	Master of Pwn Points	Eligible for Add-on Prize
Google Chrome	Sandbox Escape	$60,000	6	Yes
	Windows Kernel Escalation of Privilege	$70,000	7	Yes
Microsoft Edge	Sandbox Escape	$60,000	6	Yes
	Windows Kernel Escalation of Privilege	$70,000	7	Yes
Apple Safari	Sandbox Escape	$55,000	5	No
	macOS Kernel Escalation of Privilege	$65,000	6	No
Mozilla Firefox	Sandbox Escape	$40,000	4	No
	Windows Kernel Escalation of Privilege	$50,000	5	No

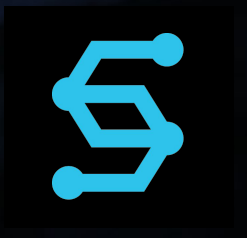
https://www.zerodayinitiative.com/Pwn2Own2018Rules.html



How much is it worth on the open market (not for weapons sales)

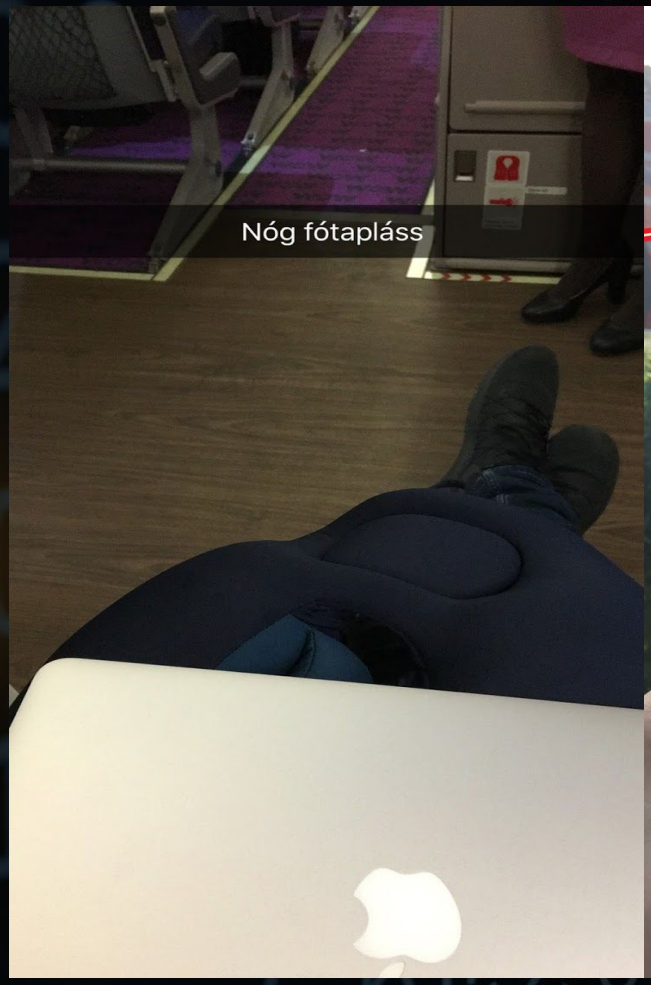
Target	Escape Options	Prize	Master of Pwn Points	Eligible for Add-on Prize
Google Chrome	Sandbox Escape	$60,000	6	Yes
	Windows Kernel Escalation of Privilege	$70,000	7	Yes
Microsoft Edge	Sandbox Escape	$60,000	6	Yes
	Windows Kernel Escalation of Privilege	$70,000	7	Yes
Apple Safari	Sandbox Escape	$55,000	5	No
	macOS Kernel Escalation of Privilege	$65,000	6	No
Mozilla Firefox	Sandbox Escape	$40,000	4	No
	Windows Kernel Escalation of Privilege	$50,000	5	No

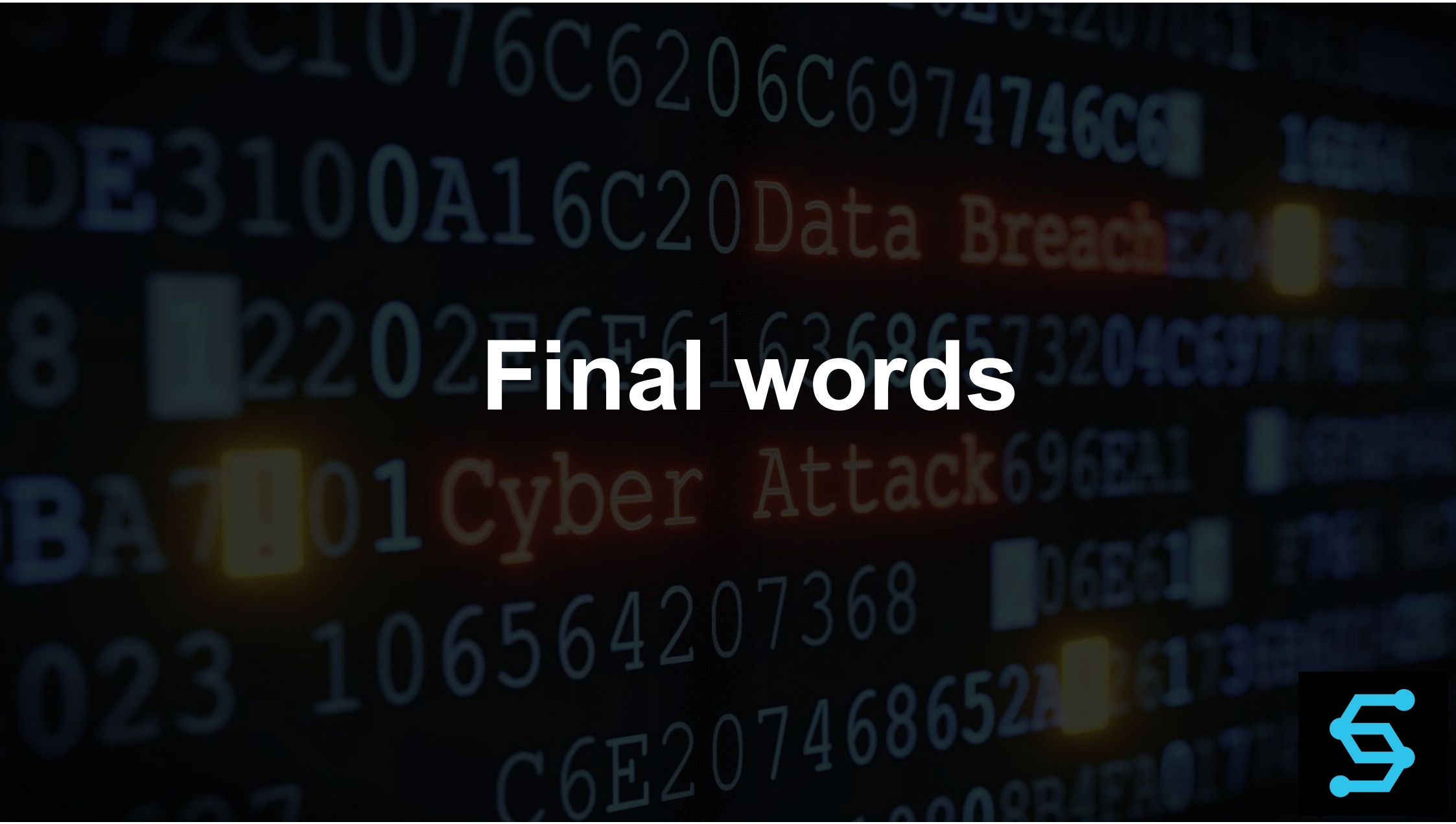
https://www.zerodayinitiative.com/Pwn2Own2018Rules.html



Was this a highly expensive process with a dedicated team of cyber hackers?

No…. This was done during a long haul flight to SFO




Final words

Stop asking whether something is secure

NOTHING IS SECURE

It’s much better to measure security through the time (cost) that it takes to break it

It’s also important to understand who your defending against


Questions?
@theorg1
SYNDIS
Creative[in]Security