

Hacking Apple to Hack Dropbox

RIPET78

Theodor

Ragnar

Gíslason



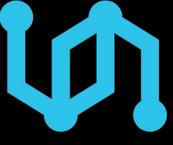
Hack different.

 **SYNDIS**
Creative[In]Security

 **Adversary**

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!

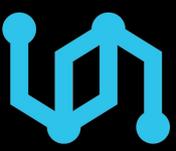
CLINT EASTWOOD GENE HACKMAN ED HARRIS
LAURA LINNEY JUDY DAVIS SCOTT GLENN E.G. MARSHALL DENNIS HAYSBERT



ABSOLUT POWER



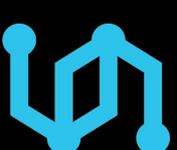
CASTLE ROCK ENTERTAINMENT PRESENTS A MARSHO PRODUCTION CLINT EASTWOOD GENE HACKMAN ED HARRIS "ABSOLUTE POWER"
STARRING CLINT EASTWOOD GENE HACKMAN ED HARRIS LAURA LINNEY JUDY DAVIS SCOTT GLENN E.G. MARSHALL DENNIS HAYSBERT
DIRECTED BY JOHN DAHLER
CASTING BY JILL COX
EXECUTIVE PRODUCERS HENRY JACOBSON AND JACK V. GREEN, S.C.
PRODUCED BY TOM ROONER AND KAREN SPIGEL
WRITTEN BY DAVID BALDWIN
EDITED BY WILLIAM GOLDMAN
MUSIC BY CLINT EASTWOOD
DISTRIBUTED BY PIONEER
CASTLE ROCK ENTERTAINMENT
ABSOLUTE POWER
CASTLE ROCK ENTERTAINMENT
ABSOLUTE POWER
CASTLE ROCK ENTERTAINMENT
ABSOLUTE POWER



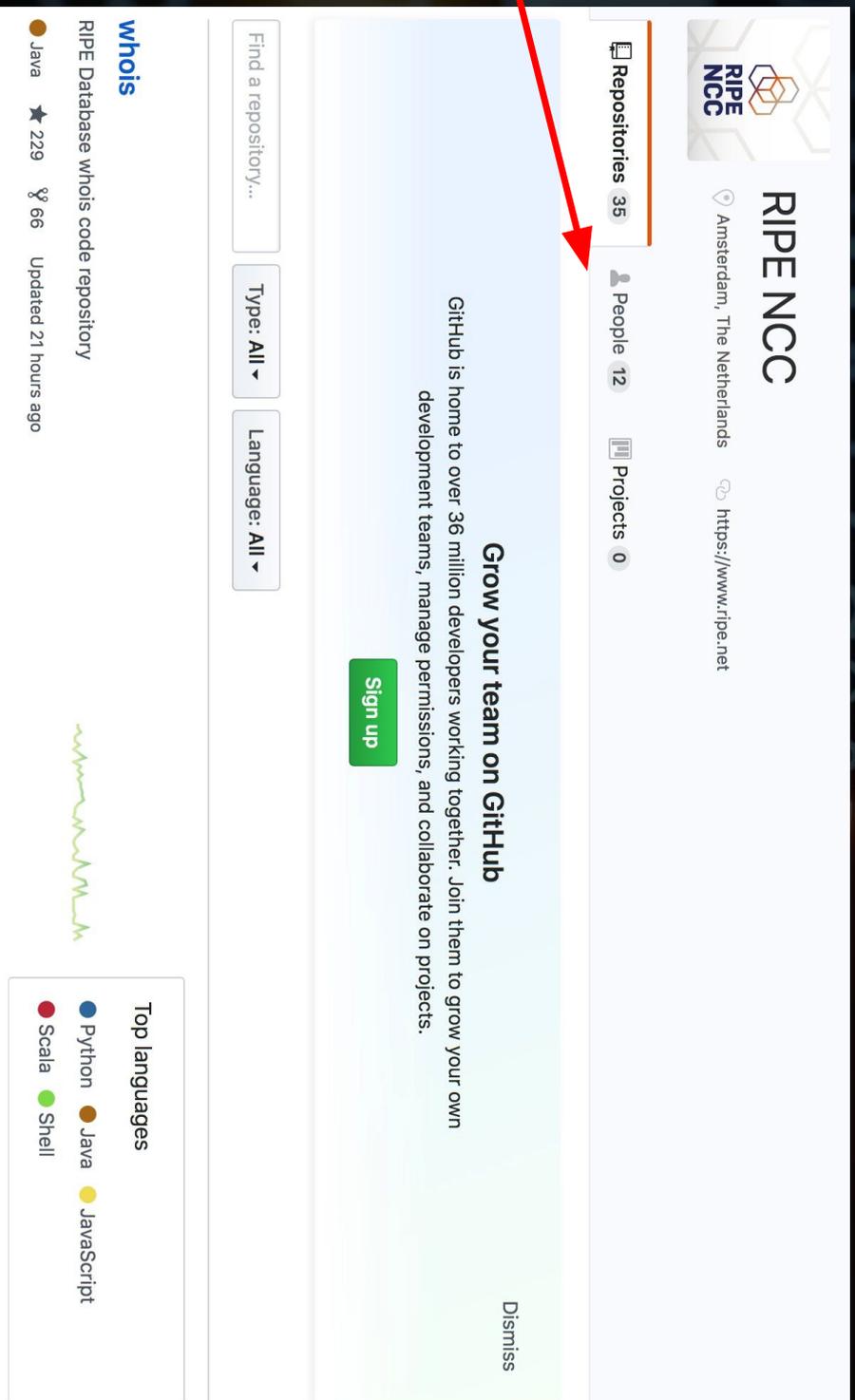
You are the target!



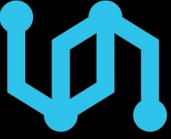
RIPE NCC
RIPE NETWORK COORDINATION CENTRE



You are the target!



The screenshot shows the GitHub profile page for RIPE NCC. At the top, the profile name 'RIPE NCC' is displayed, along with the location 'Amsterdam, The Netherlands' and the website 'https://www.ripe.net'. Below this, a navigation bar shows 'Repositories 35', 'People 12', and 'Projects 0'. A red arrow points to the 'Repositories 35' link. The main content area features a light blue background with the text: 'Grow your team on GitHub' and 'GitHub is home to over 36 million developers working together. Join them to grow your own development teams, manage permissions, and collaborate on projects.' A green 'Sign up' button is positioned below this text. At the bottom right of the main content area, there is a 'Dismiss' link. On the left side, there are filters for 'Find a repository...', 'Type: All', and 'Language: All'. Below these filters, the 'whois' section is visible, showing 'RIPE Database whois code repository' with a star count of 229 and an update time of 'Updated 21 hours ago'. At the bottom left, there is a 'Top languages' section with a legend for Python (blue), Java (orange), JavaScript (yellow), Scala (red), and Shell (green).



You are the target!

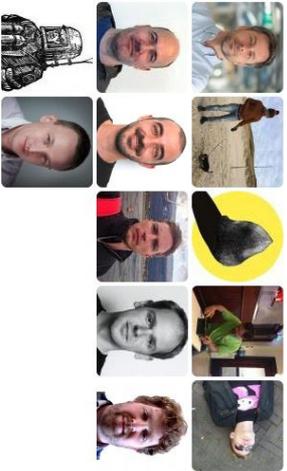
Top languages

- Python
- Java
- JavaScript
- Scala
- Shell

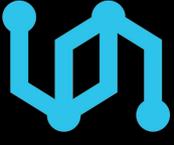
Most used topics

- python
- ripe-atlas
- ripe-ncc

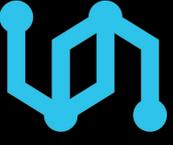
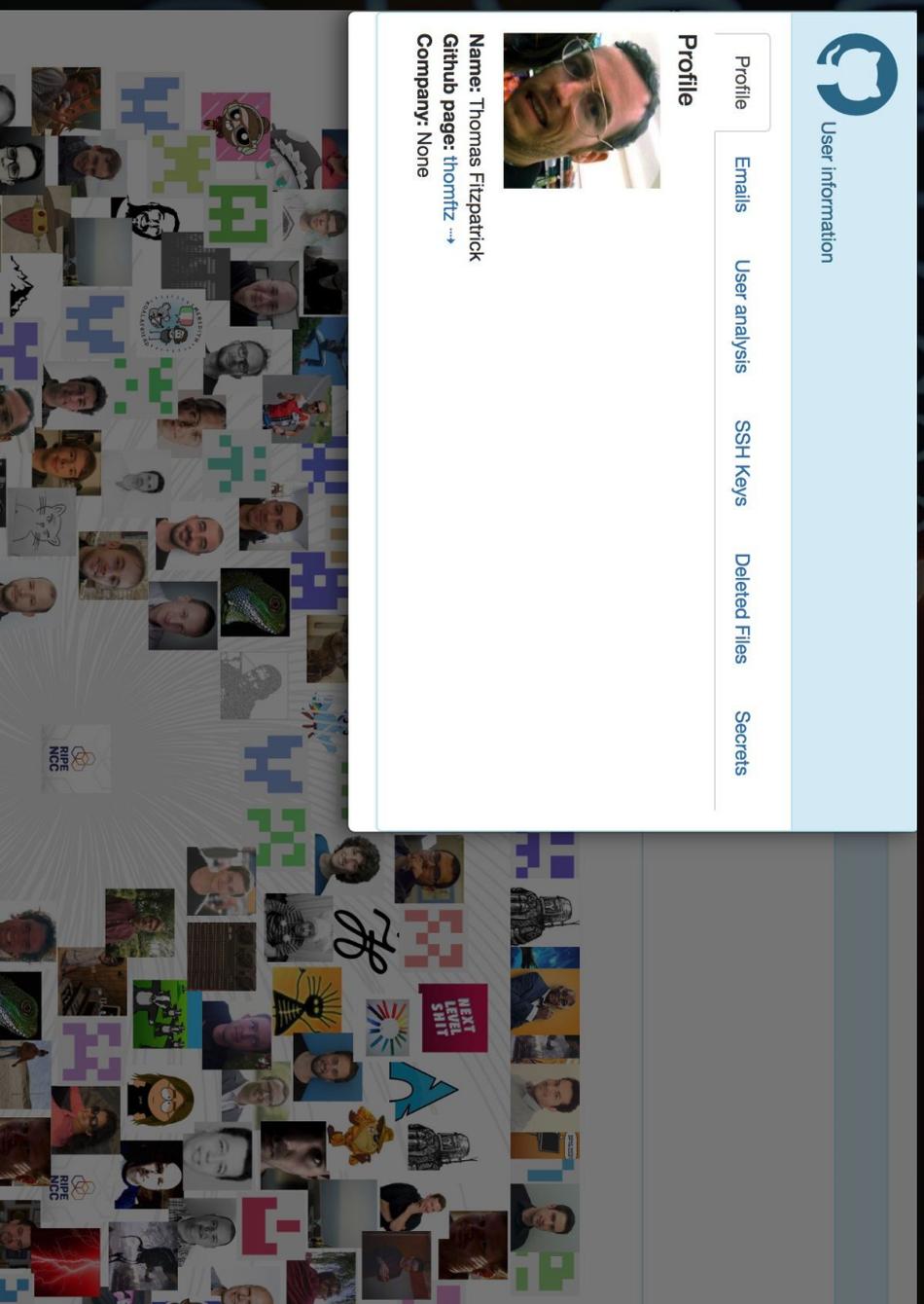
People



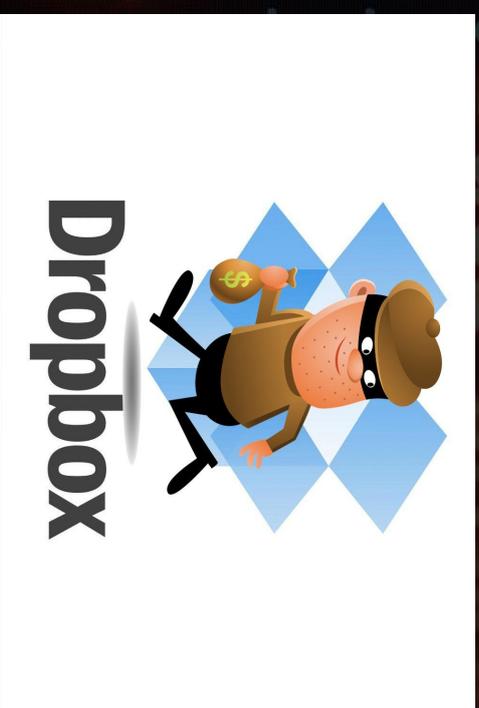
12 >



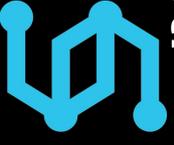
What do engineers do? We build things(tools) of course



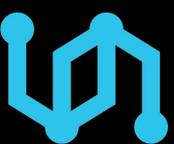
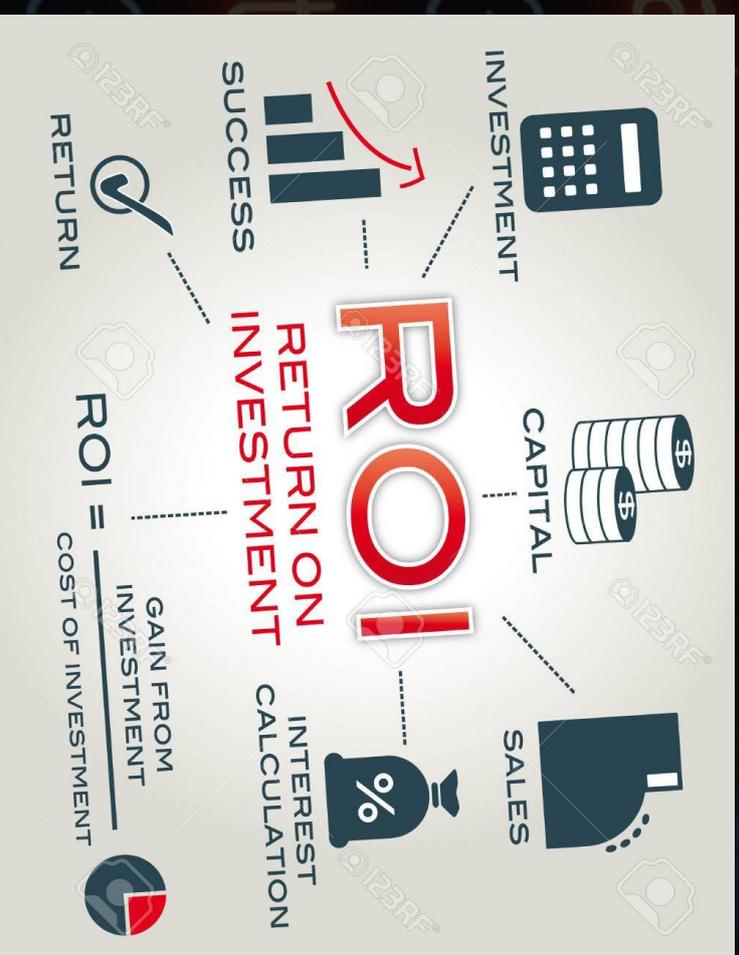
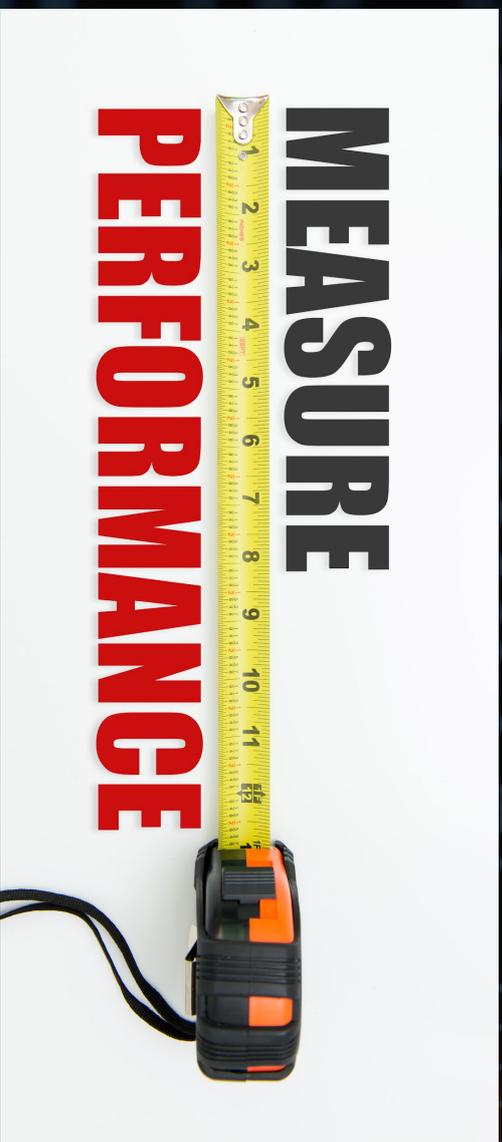
Dropbox red team engagement



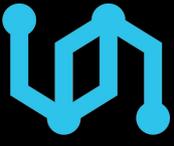
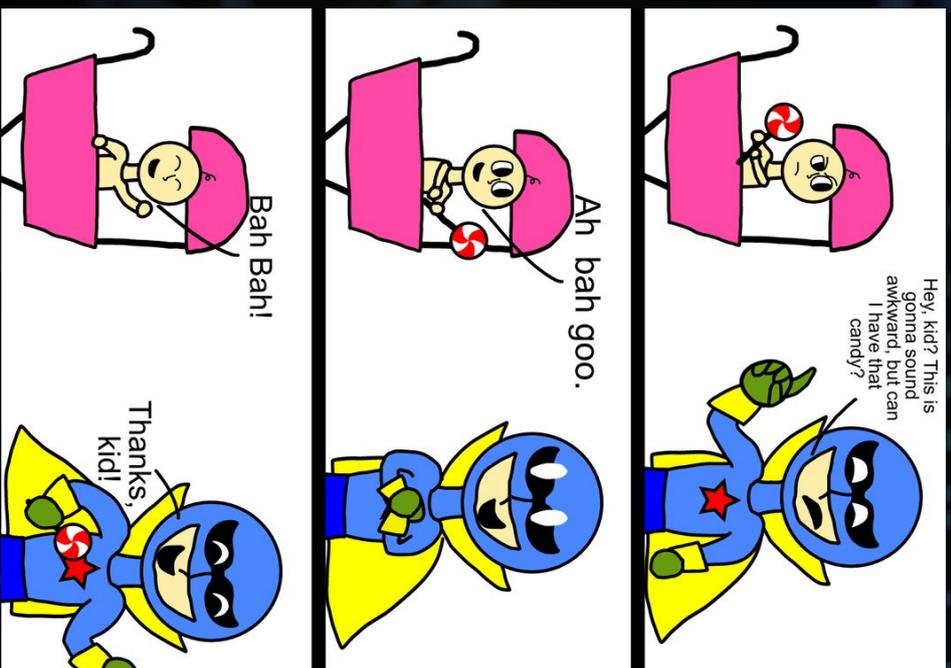
<https://blogs.dropbox.com/tech/2018/11/offensive-testing-to-make-dropbox-and-the-world-a-safer-place/>



Dropbox red team engagement

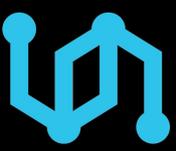
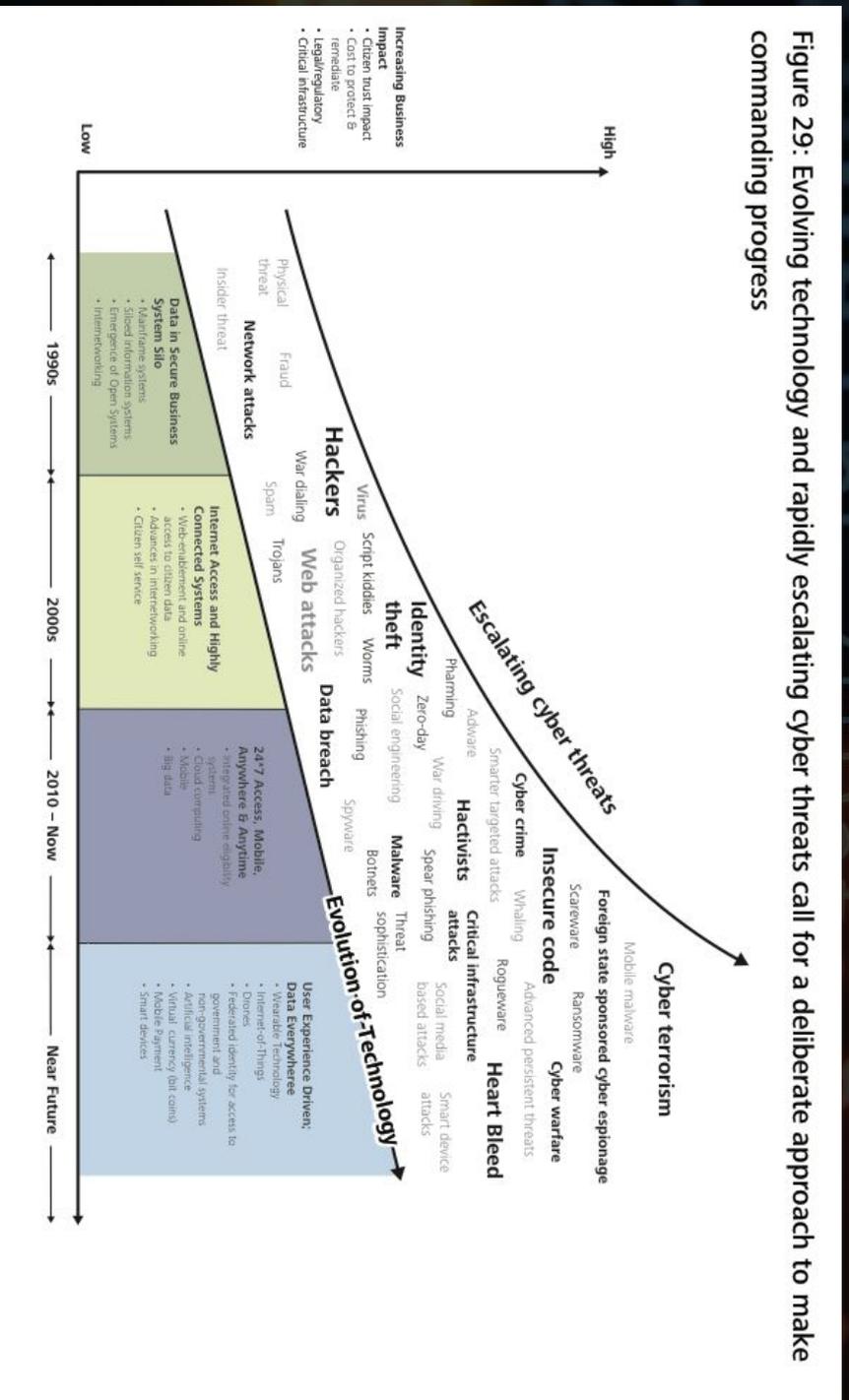


Dropbox red team engagement

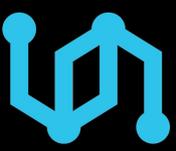


The continually evolving cyber battlefield

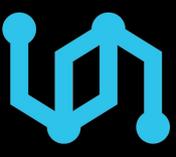
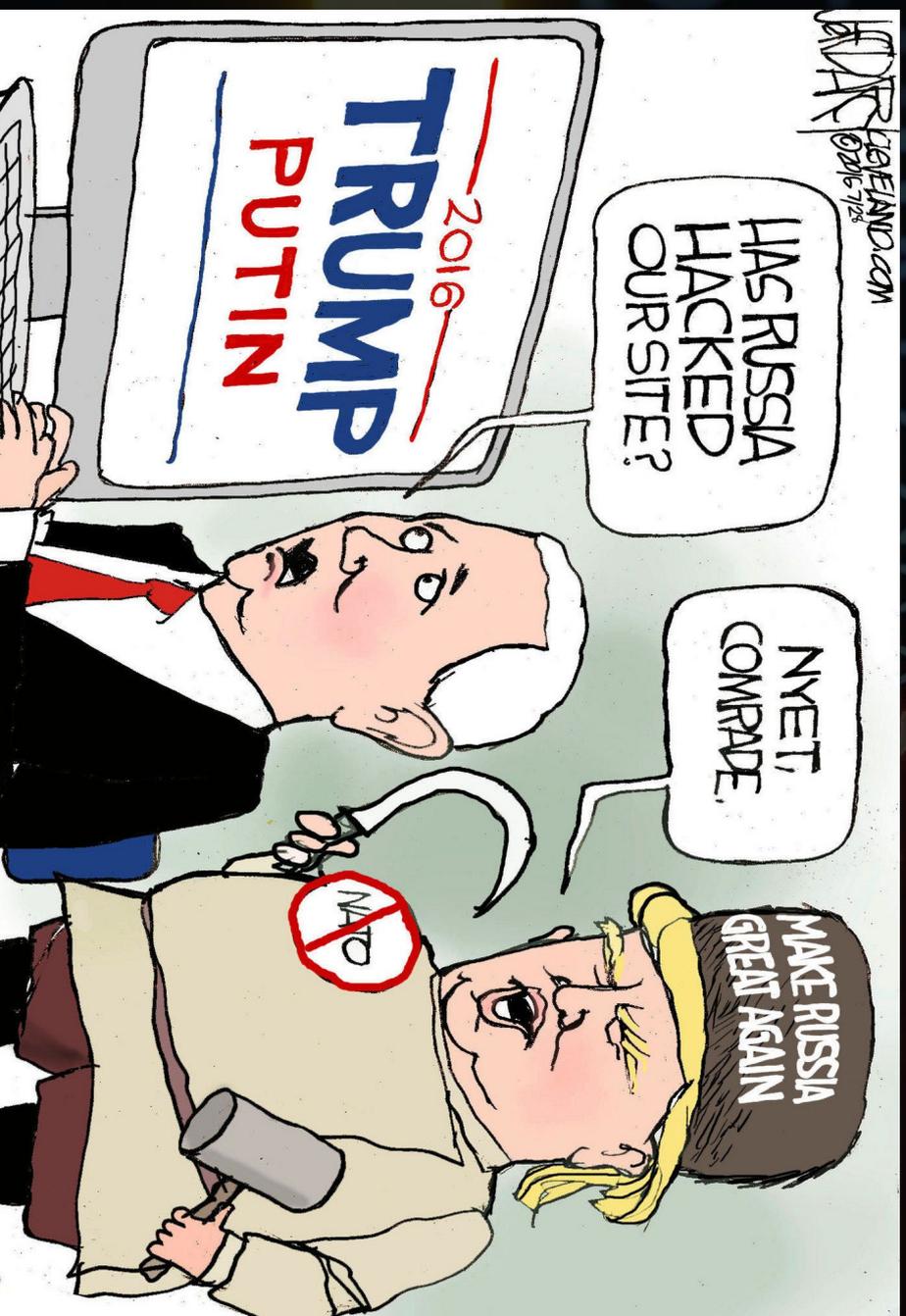
Figure 29: Evolving technology and rapidly escalating cyber threats call for a deliberate approach to make commanding progress



Organized crime and fraud is rampant



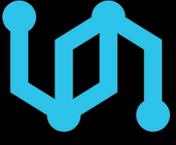
Nation state attack teams can change history



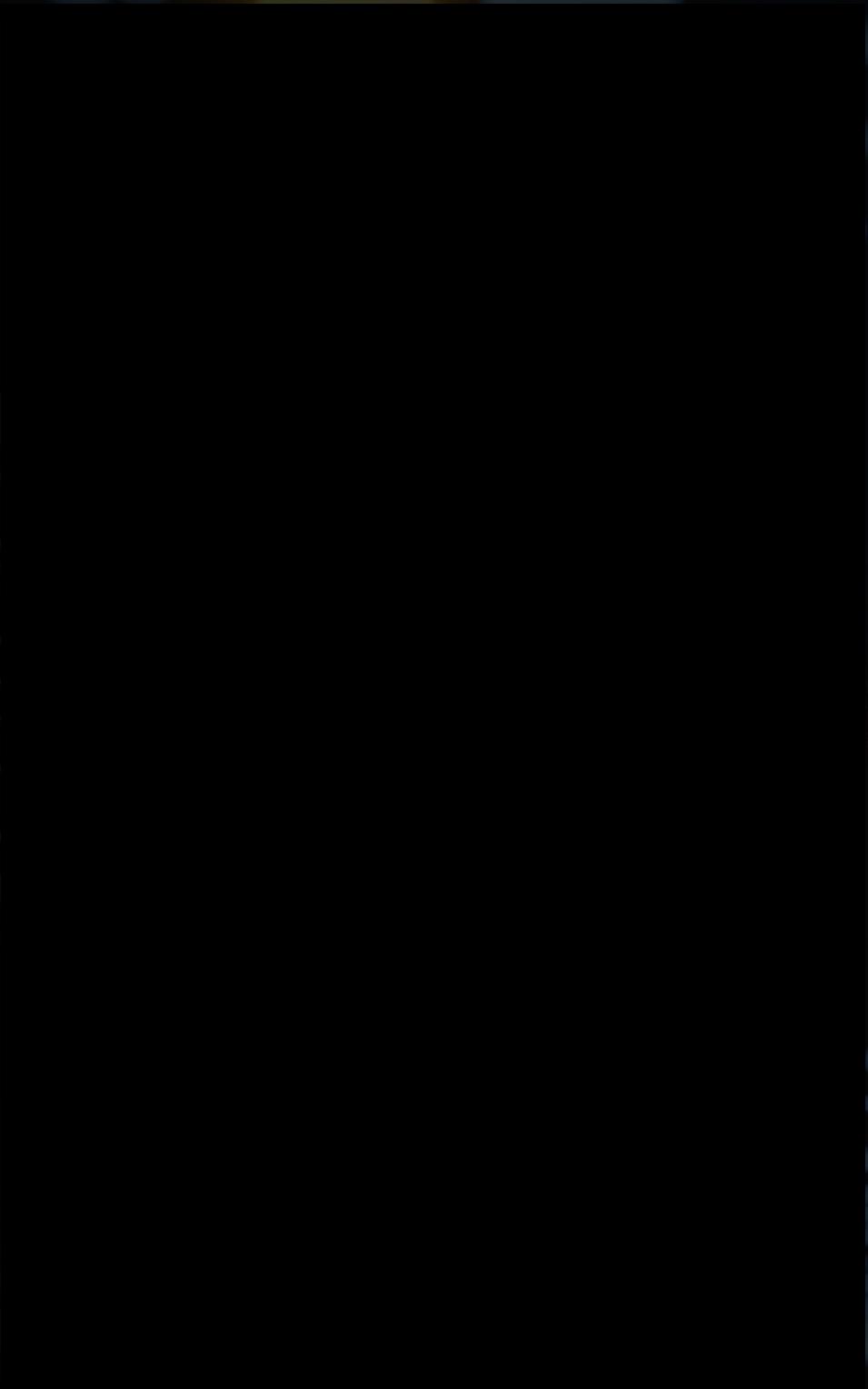
The fruits are RIPLE for the picking



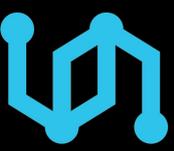
<https://safeatlast.co/blog/iot-statistics/>



A trend is emerging?



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



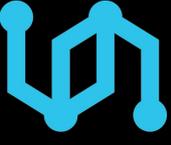
Hackers are realizing that data itself is valuable

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)



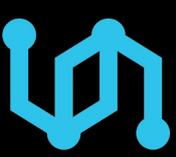
IDEA OF THE DAY 

WHY MACS ARE MORE SECURE

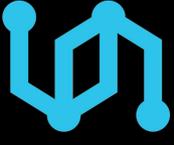
Here's Why...

IDEAOFTHEDAY.COM 

The image shows a man with a beard and long hair, wearing a dark shirt, speaking in a video frame. The background is a room with a blue sofa and a wooden table. The text 'IDEA OF THE DAY' is at the top left, and 'WHY MACS ARE MORE SECURE' is in large yellow letters across the middle. A yellow banner at the bottom left says 'Here's Why...'. The website 'IDEAOFTHEDAY.COM' and a lightbulb icon are at the bottom right.



“Oday” (Zero day) vulnerabilities in a project



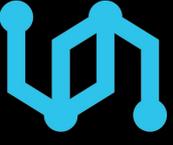
What is this “Zero-day” word anyway?



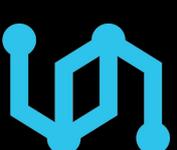
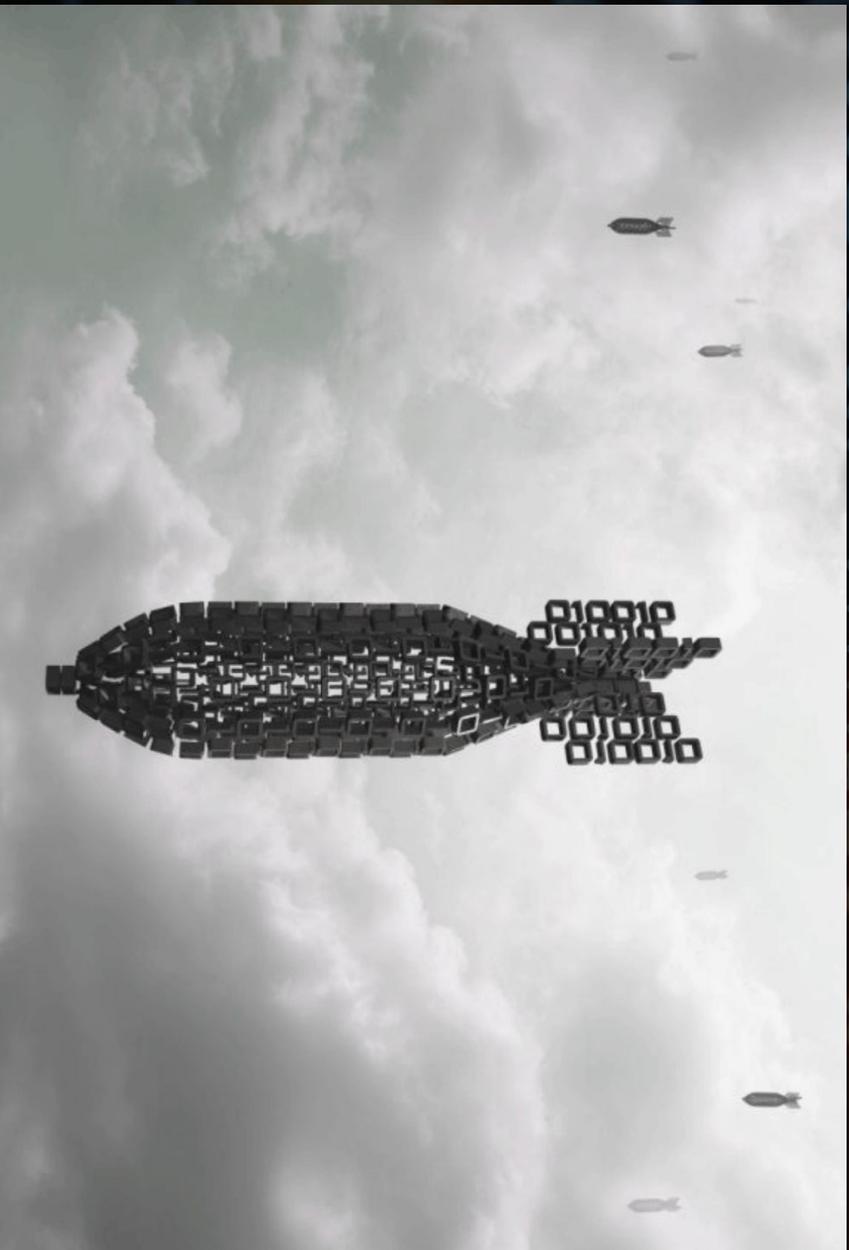
The global battle to steal your secrets is turning hackers into



“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.”



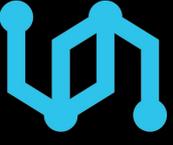
It's a cyber bomb



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

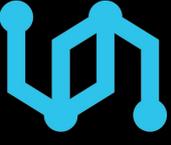
Available for: OS X El Capitan 10.11.6, macOS Sierra 10.12.6, macOS High Sierra 10.13.3

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

Description: A logic issue was addressed with improved validation.

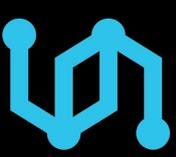
CVE-2018-4175: Theodor Ragnar Gislason of Syndis

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



Demo Time!





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>



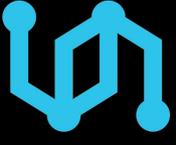
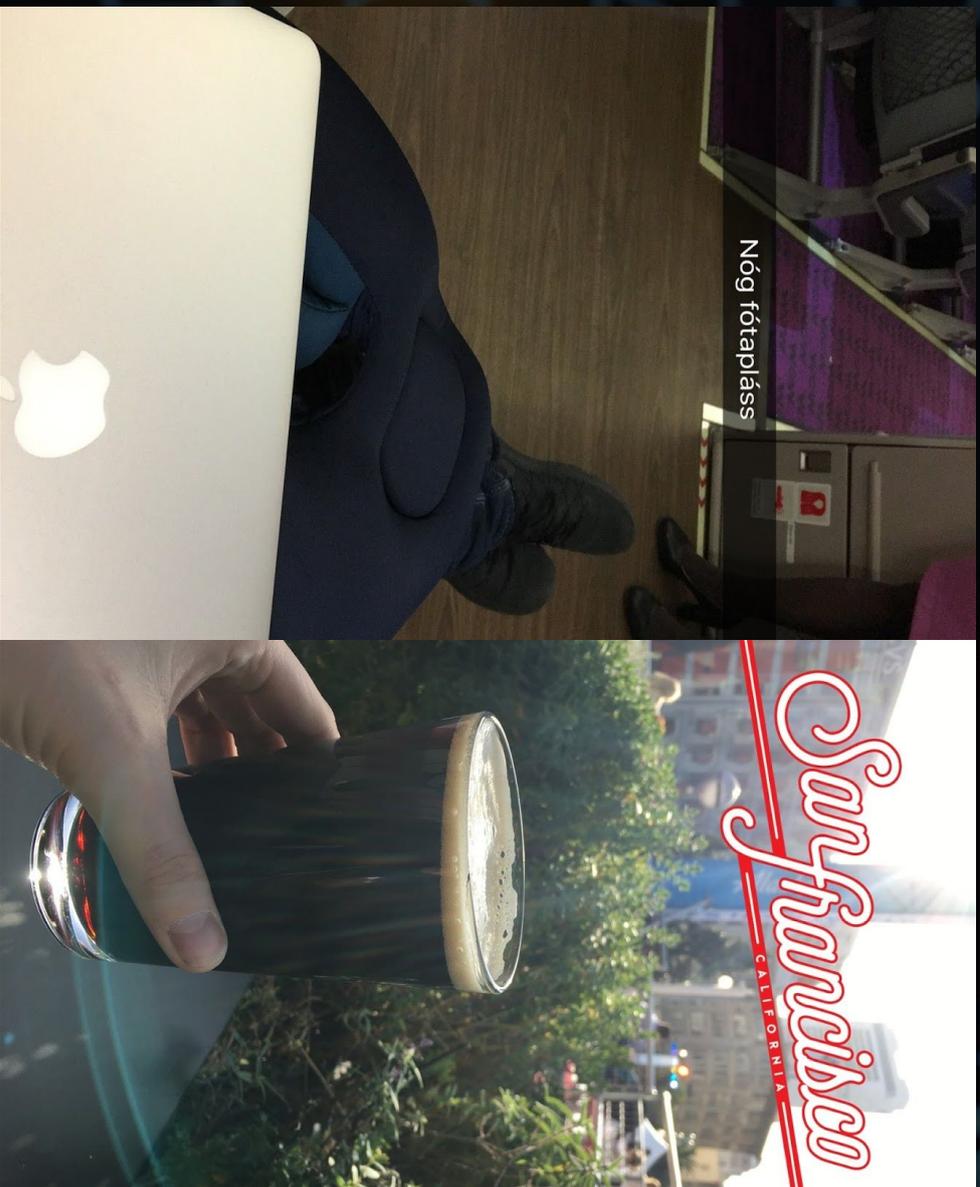
Was this a highly expensive process with a dedicated team of cyber hackers?



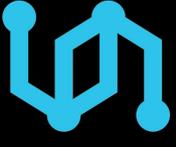
www.china-defense-mashup.com



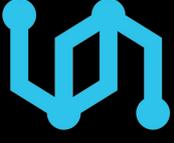
No.... This was done during a long haul flight to SFO



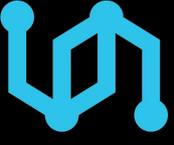
Final words



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



Questions?

@theorg1