Hack different.

SYNDIS
Creative[in]Security

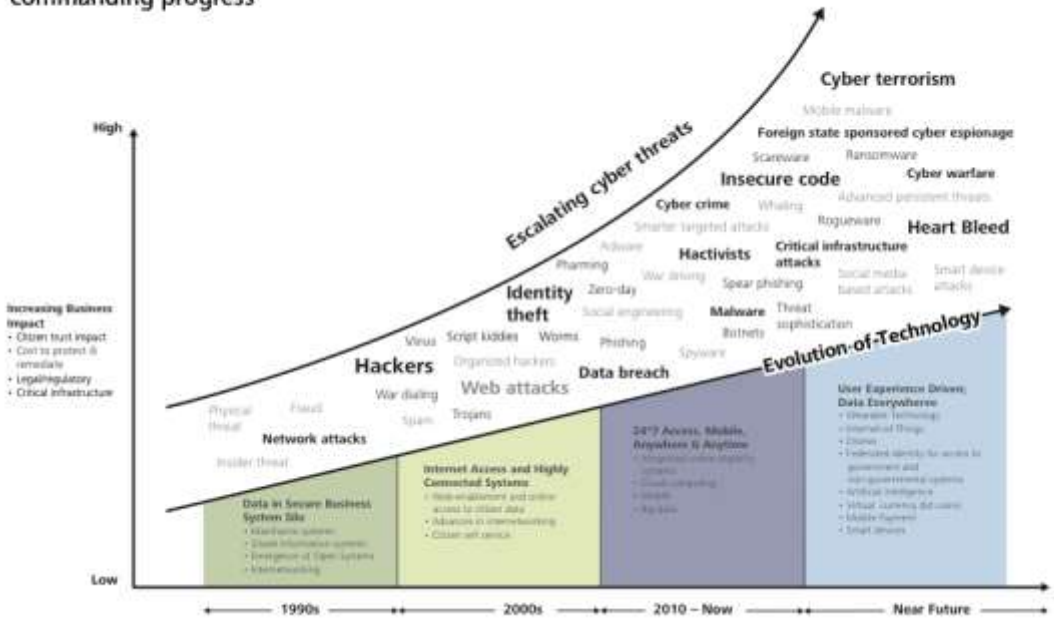
Adversary

Inngangur

- Stafrænn vígvöllur
- “Núlldagsveikleiki” í Apple MacOS stýrikerfinu
- Lokaorð

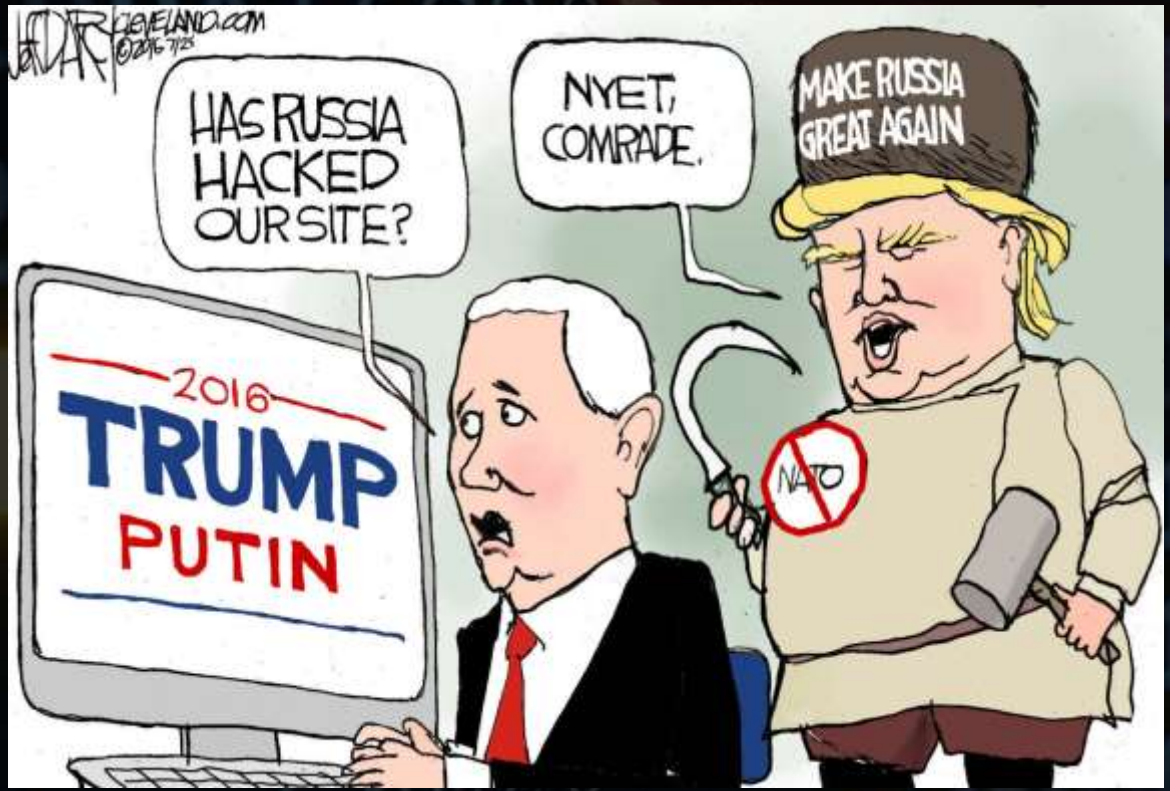
Stafrænn og síbreytilegur vígvöllur

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



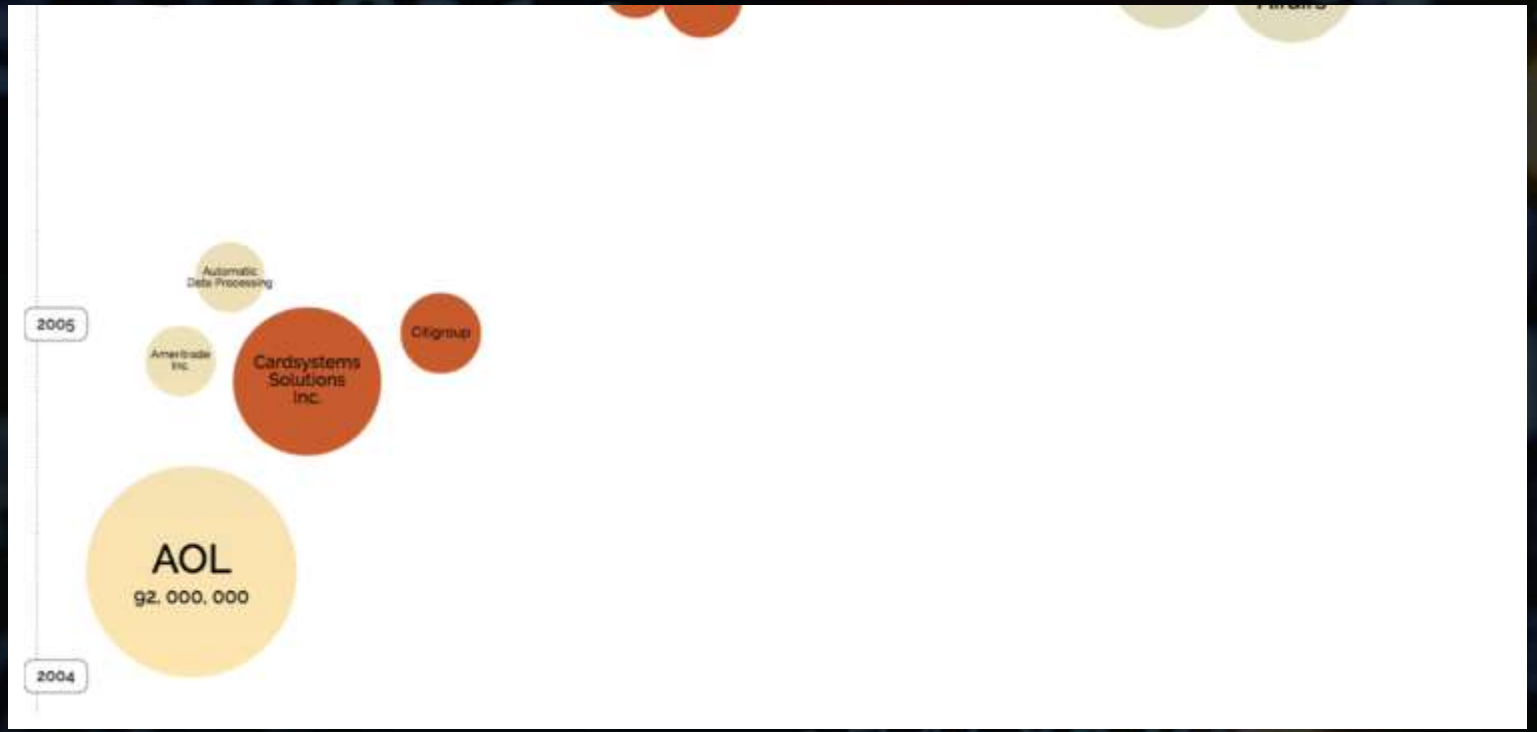
Skipulögð glæpastarfsemi hefur haslað sér völl

Stafræn árásarteymi breyta gangi sögunnar



Fyrirtæki þurfa að aðlagast stafrænu samfélagi

Ansi áhugaverð þróun á gagnalekum.



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

Hugarvelta - gögnum breytt eða stolin?

Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data

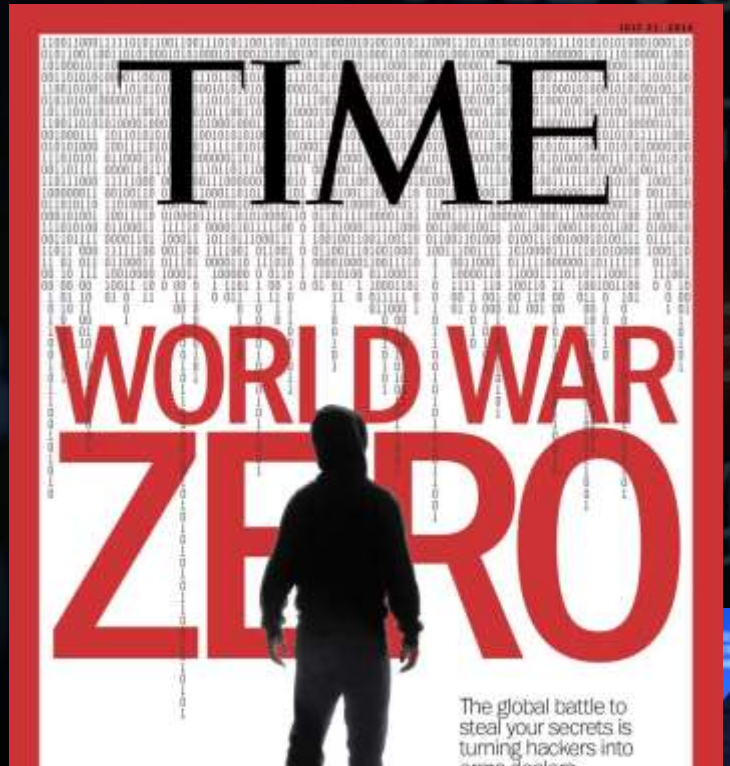
Uber's headquarters in San Francisco. The ride-hailing company said information on driver and rider names, emails and telephone numbers had been compromised in a data breach.

Ryan Young for The New York Times

Öryggi Apple stýrikerfisins (*MacOS X*)

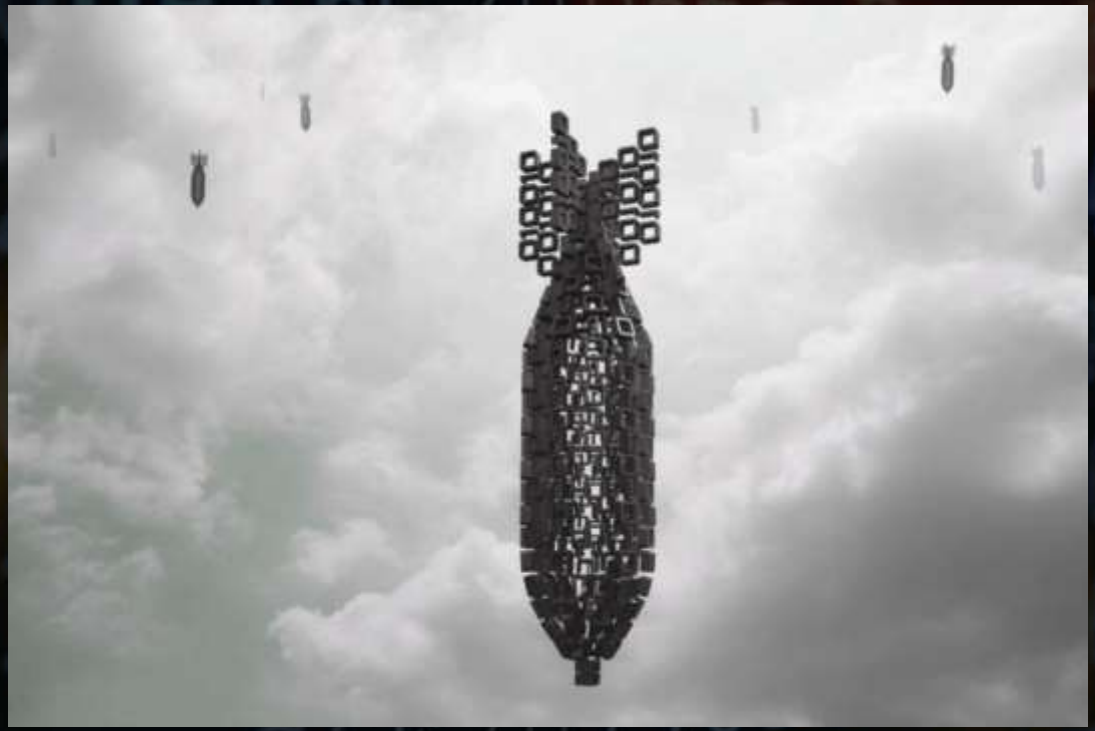
“Núlldags” (*Zeroday*) veikleikar í verkefni

Hvað er þetta “*Núlldags*” orðtiltæki eiginlega?

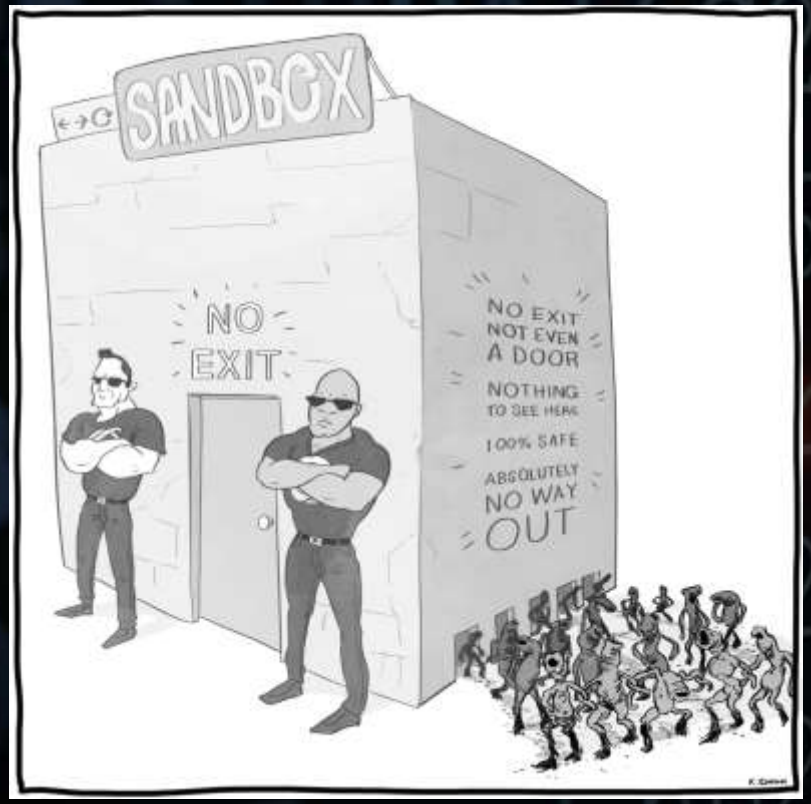


“A zero-day (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer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

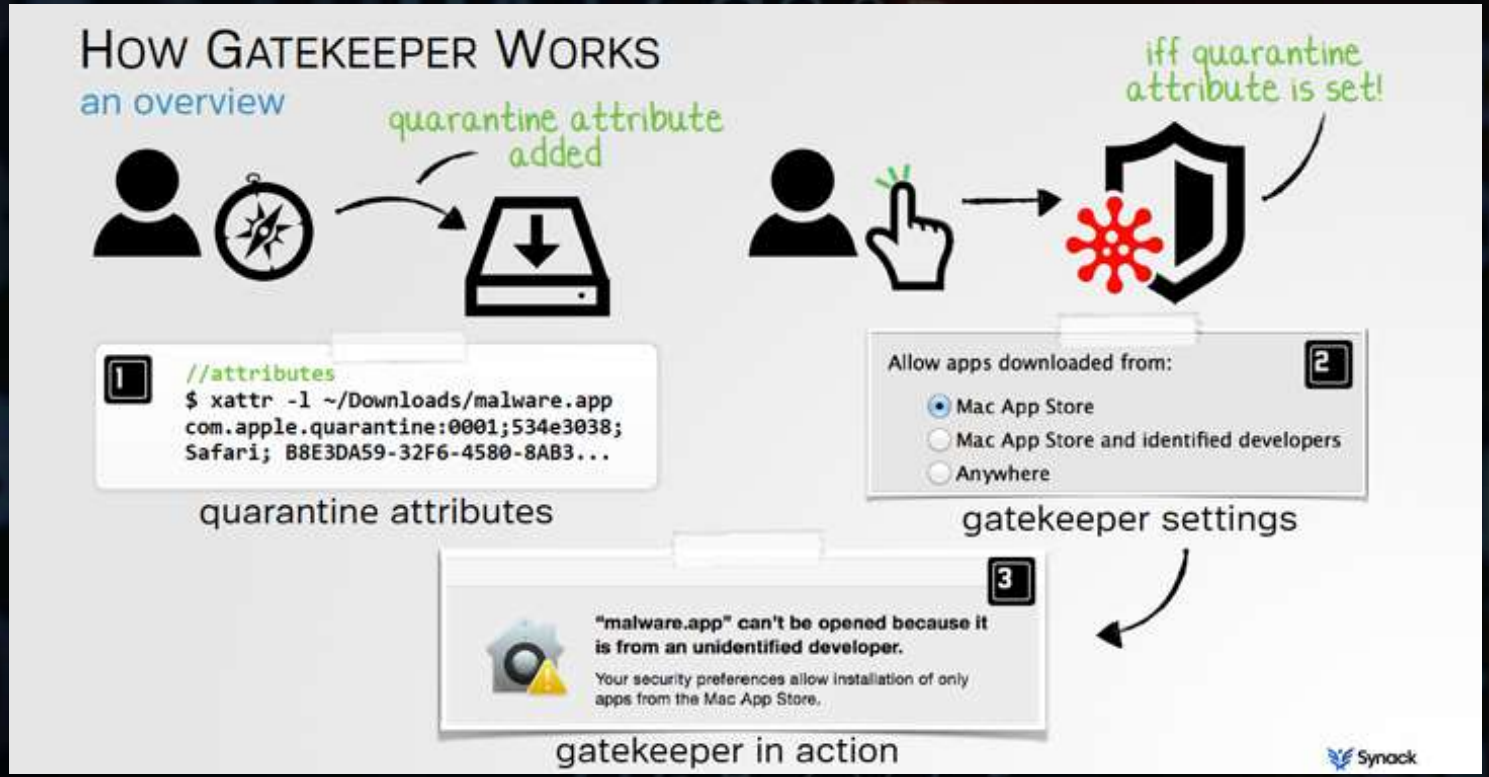
Stafrænt vopn?



Hvað með varnir, eru þær ekki öflugar?



Öflugar varnir í flestum nútíma stýrikerfum



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

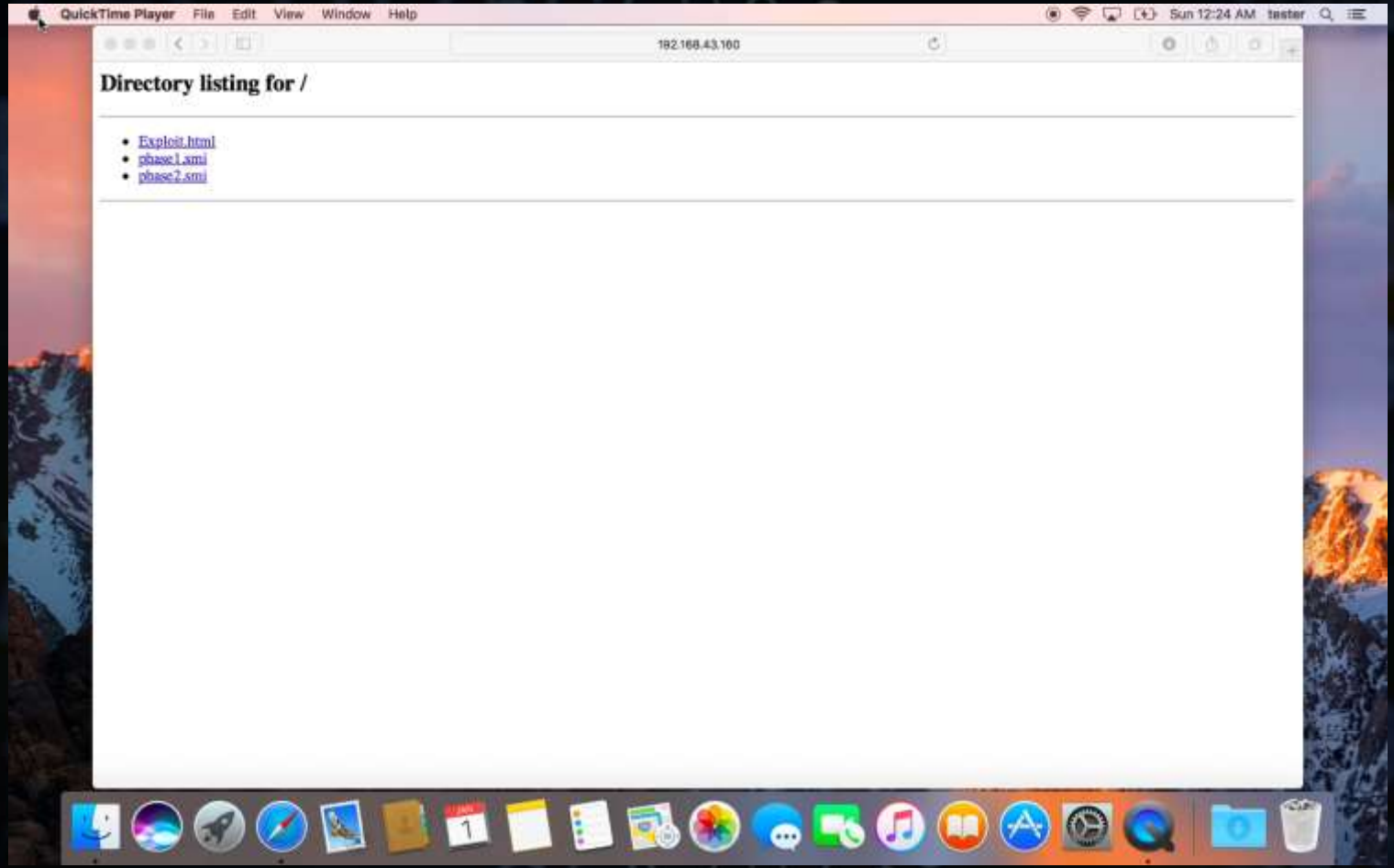
Impact: A maliciously crafted application may be able to bypass code signing enforcement

Description: A logic issue was addressed with improved validation.

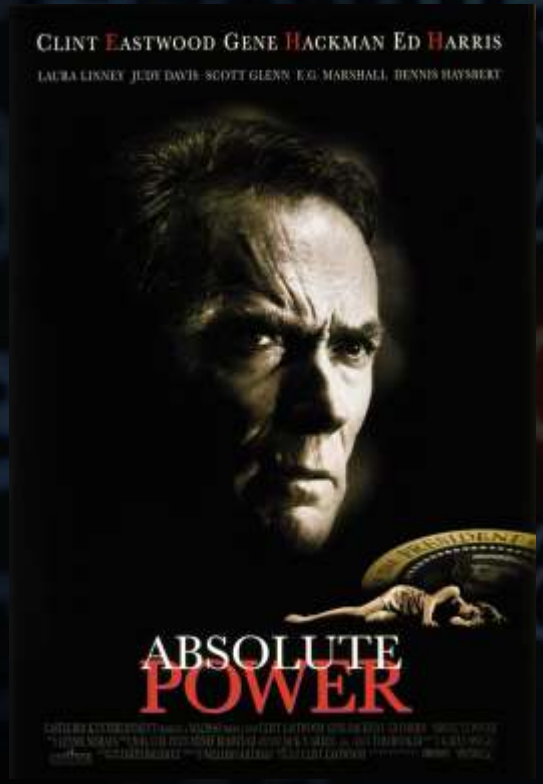
CVE-2018-4175: Theodor Ragnar Gislason of Syndis

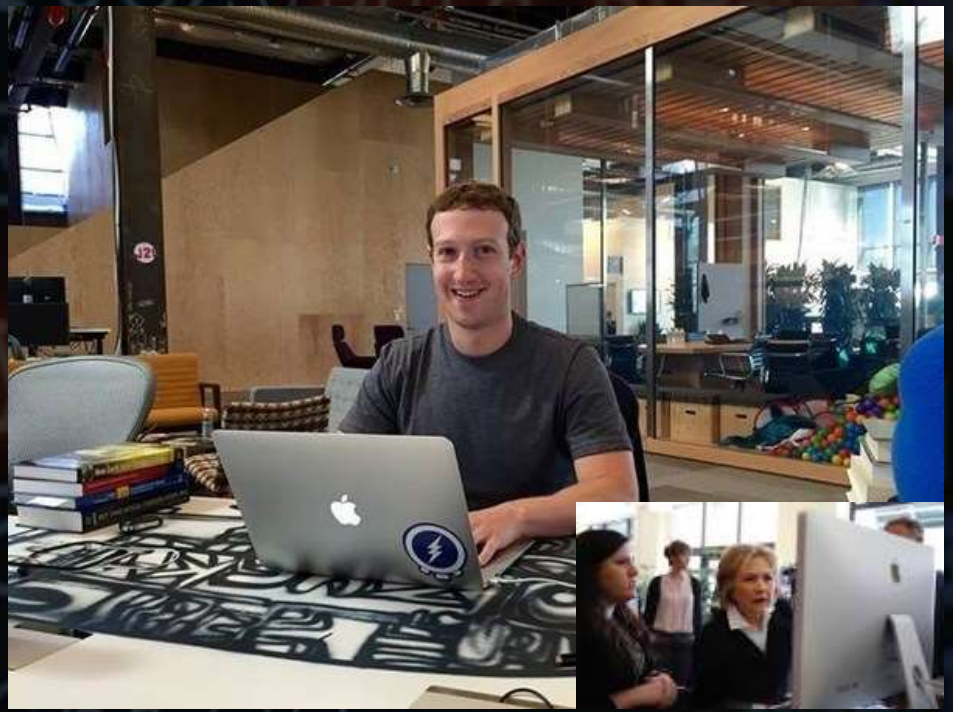
Þrjár öryggisvillur til að fara framhjá vörnum stýrikerfisins

Demo Time!


QuickTime Player File Edit View Window Help
Sun 12:24 AM tester
192.168.43.160
Directory listing for /
Exploit.html
phase1.smi
phase2.smi

Með þessu hefðum við geta hakkað alla Makka í heiminum!





Hvers virði var þetta?

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

Hátæknileg framleiðsla í marga mánuði?

Nei, þessu var “*reddað*” í flugi til SFO

Lokaorð

Ekki spyrja hvort eitthvað sé öruggt.

Ekkert er öruggt.

Betra að mæla öryggi í tíma (kostnaði) sem það tekur að brjóta eitthvað

Hverjum ertu svo að reyna að verjast?

Takk fyrir

@theorg1