



THIS WEEK IN SECURITY

`gak@thessSec:~# ./week_1`



What does your browser know about you?

<http://webkay.robinlinus.com/>

Make x86 hardware secure again!

Processors:

- AMD – Platform Security Processor (**PSP**)
- Intel – Management Engine (**IME**)

Access to:

- Memory (without the parent CPU knowing)
- Full access to TCP/IP
- Bypasses firewall – can send/receive packets freely
- Can be active when the system is hibernated or **turned off**

**TL;DR: A hardware built-in backdoor that
your computer cannot work without**

Release the source of PSP

- Eliminate security through obscurity. A secure system must be secure even if every detail but the key is known by untrusted individuals or organizations.
- Give users control over their own systems. It generates confidence in AMD.
- Give FSF and other similar organizations a great reason to recommend AMD for purchases of supporters.
- Increase presence in key security systems on companies and governments.

<https://www.change.org/p/advanced-micro-devices-amd-release-the-source-code-for-the-secure-processor-psp>

Pwn2Own 2017



Vault 7 (less than 1% of Year 0)

- Did WhatsApp and Signal break?

NO. Tools allow:

- Complete access to the device
- Data gets intercepted before it is encrypted

That's worse

- Remote control of smart vehicles (2014 research document)
- Samsung TVs “fake-off” mode → Covert recording of conversations
- Malware Library : “The goal of this repository is to provide functional code snippets that can be rapidly combined into custom solutions”

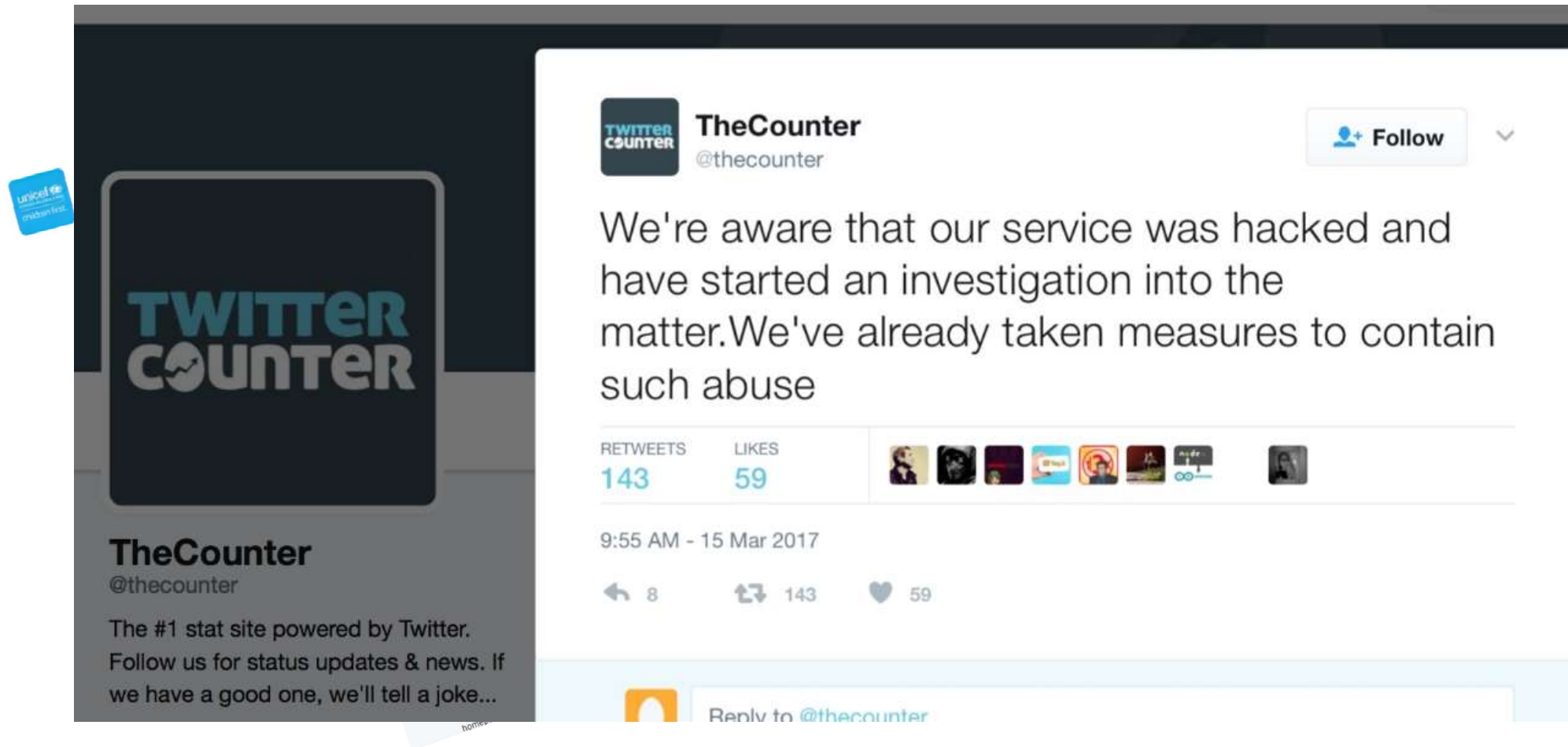
Ransomware-As-A-Service


- Encrypts your data in return for BTC
- Estimated 2016 damage: 1B\$
- Spreads through phishing/malicious links

Satan

- Provides a working ransomware sample
- Attacker can tailor to his needs (Type of encryption etc.)
- Provider keeps 30% of revenue

Twitter are you OK?






TheCounter


@thecounter

The #1 stat site powered by Twitter.
Follow us for status updates & news. If
we have a good one, we'll tell a joke...



TheCounter

@thecounter

 Follow


We're aware that our service was hacked and have started an investigation into the matter. We've already taken measures to contain such abuse

RETWEETS


143

LIKES


59




9:55 AM - 15 Mar 2017




8



143



59



Reply to @thecounter

Yahoo hack : 4 people charged

- Who: Karim Baratov, Alexsey Belan, Dmitry Dokuchaev, Igor Suschchin
- What: Hacked 500M Yahoo Accounts
- Result: 47 criminal charges each
 - Conspiracy
 - Computer fraud
 - Economic espionage
 - Theft of trade secrets
 - Aggravated identity theft

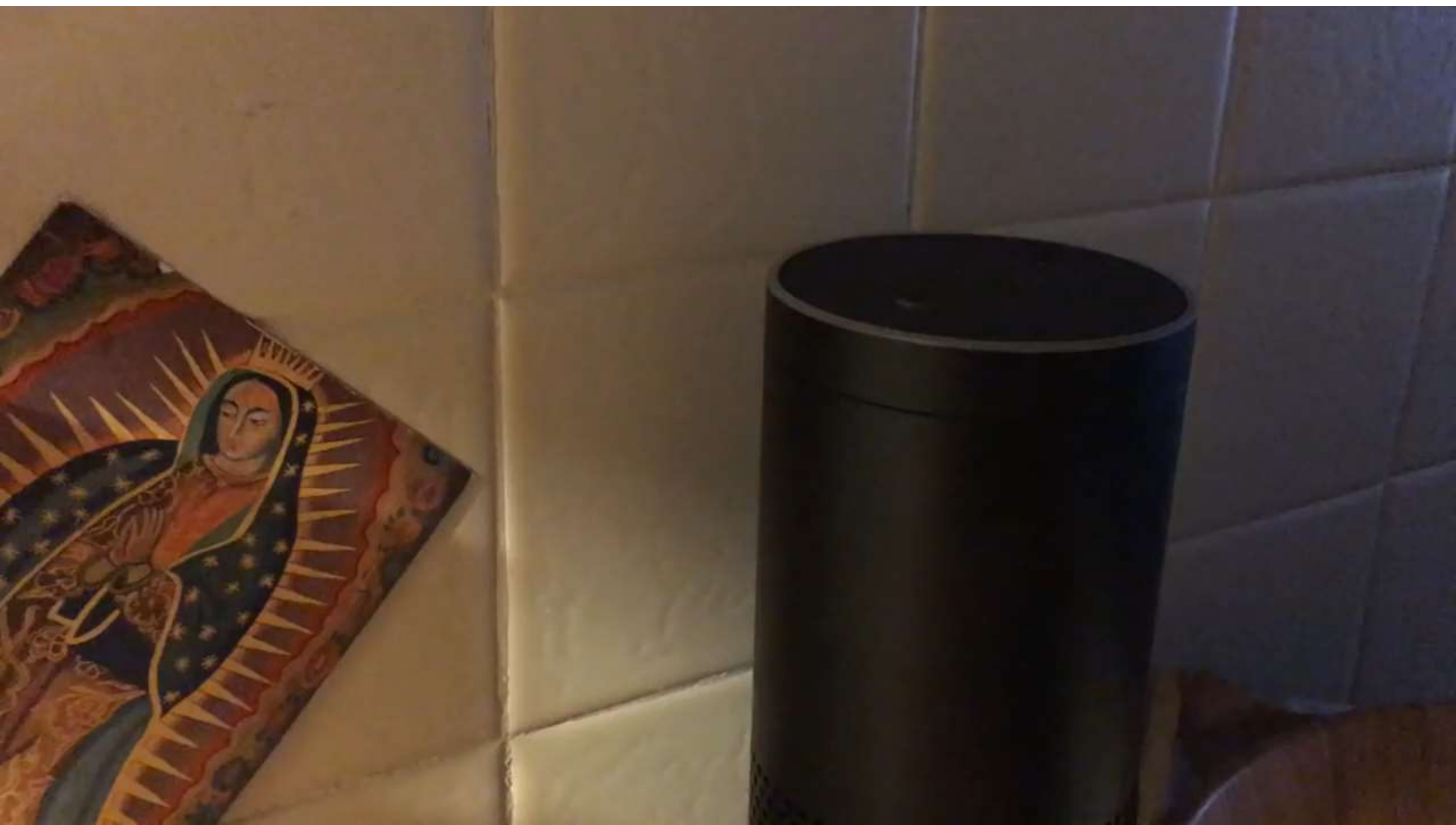
<https://krebsonsecurity.com/2017/03/four-men-charged-with-hacking-500m-yahoo-accounts/>

Yahoo hack : 4 people charged

“In or around November and December 2014, Belan stole a copy of at least a portion of Yahoo’s User Database (UDB), a Yahoo trade secret that contained, among other data, subscriber information including users’ names, recovery email accounts, phone numbers and certain information required to manually create, or ‘mint,’ account authentication web browser ‘cookies’ for more than 500 million Yahoo accounts.

“Belan also obtained unauthorized access on behalf of the FSB conspirators to Yahoo’s Account Management Tool (AMT), which was a proprietary means by which Yahoo made and logged changes to user accounts. Belan, Dokuchaev and Sushchin then used the stolen UDB copy and AMT access to locate Yahoo email accounts of interest and to mint cookies for those accounts, enabling the co-conspirators to access at least 6,500 such accounts without authorization.”

<https://krebsonsecurity.com/2017/03/four-men-charged-with-hacking-500m-yahoo-accounts/>





Till next time.

Animal Tra(fi)cking

- Chinese medical science : Tiger parts (Also high status & wealth)
- First seen : 2013 @Panna Tiger Reserve → Cyber Poaching
- GPS intercepted to find locations of wild tigers

Failure to adopt more proactive thinking about the unintended consequences of electronic tagging could lead to malicious exploitation and disturbance of the very organisms researchers hope to understand and conserve.