

# **Killing Me Softly with His Song**

*Understanding Cyber SInS*

*A^2 – Aamir Lakhani, Senior Red Team Researcher*

April 2019

# Why am I here today



```
sudo -u root echo `whoami`
```

## (A^2) Aamir Lakhani

- Hacker, Ninja, Prince
- Red Team Researcher
- Fortinet, FortiGuard Labs
- I am known as that guy that liked the Phantom Menace

Let's Connect!



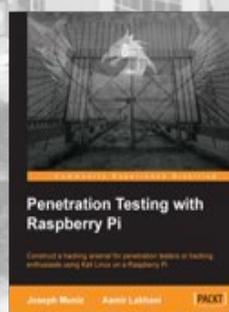
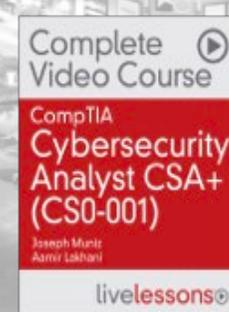
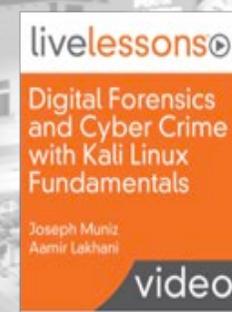
@aamirlakhani



alakhani@Fortinet.com



Blog: [www.DrChaos.com](http://www.DrChaos.com)



# What do you want to be when you grow up?



# Note to teacher

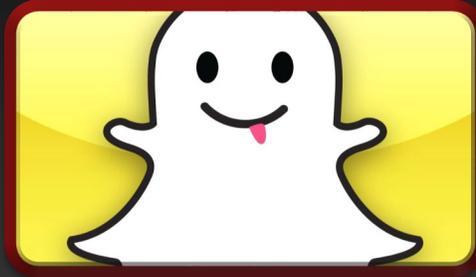
Dear Mrs. Jones,

I wish to clarify that I am not now, nor have I ever been, an exotic dancer.

I work at Home Depot and I told my daughter how hectic it was last week before the blizzard hit. I told her we sold out every single shovel we had, and then I found one more in the back room, and that several people were fighting over who would get it. Her picture doesn't show me dancing around a pole. It's supposed to depict me selling the last snow shovel we had at Home Depot.

From now on I will remember to check her homework more

# My Favorite Social Media Site/App?



# Who are your social friends



# Robin Sage



**What Is The Real Threat?**

**Fictional** American cyber threat hunter created to abstract sensitive information. She graduated from MIT and had 10 years of experience despite she was 25 years old.

Due to her profile, she was offered consulting work with notable companies such as Google and Lockheed Marti. She had friends in the FBI, CIA and even offered dinner invitations from male friends.

# Emily Olivia Williams



**Fictional** CSE created to abstract sensitive information from a specific target. She graduated from MIT and had **10** years of experience despite she was **28** years old.

Despite the fake profile, she was offered sensitive information from our target's AM and CSEs. She had friends in large partner vendors and even offered dinner invitations from male friends.

# The Impact of Social Media

10 minutes:

20 Facebook connections

6 LinkedIn Connections

## NOTIFICATIONS



endorsed you for a skill: Cisco Technologies

1h



endorsed you for a skill: CCNA

1h

tions  
ions

op; 10 EMC;

ends

ments

For Expertise and Experience  
From Partners and co-workers

**Offers:**

4 job offers, Laptop and office  
equipment, network access.

Messages

Reply

Forward

Report Spam

RE: Job Opp

To: Em

You replied to th

The interview is just a formality. I am sure with your qualifications and references it won't be an issue. Besides, it would probably just better if you had an interview at the office.

Emily Williams w

Ahhhh that is so sweet! You look great! I love your profile picture. I hate interviewing because I get really nervous or shy but I am sure you don't ever let me have fun :-(((

Hi Emily,

Any chance would you be interested in a senior SE position? It looks like it would be a perfect fit. If you have a few minutes I would be happy to discuss it with you. I have 10 years of experience.

Reply

Men trust attractive women



# What we did

## *What?*

Created fake FaceBook and LinkedIn profile to gain information using social media.

## *How?*

Social engineering techniques that allowed us to participate as a New Hire

## *What was captured?*

Salesforce Logins, Issued Laptops, Jobs offers, Endorsements, Meet up requests

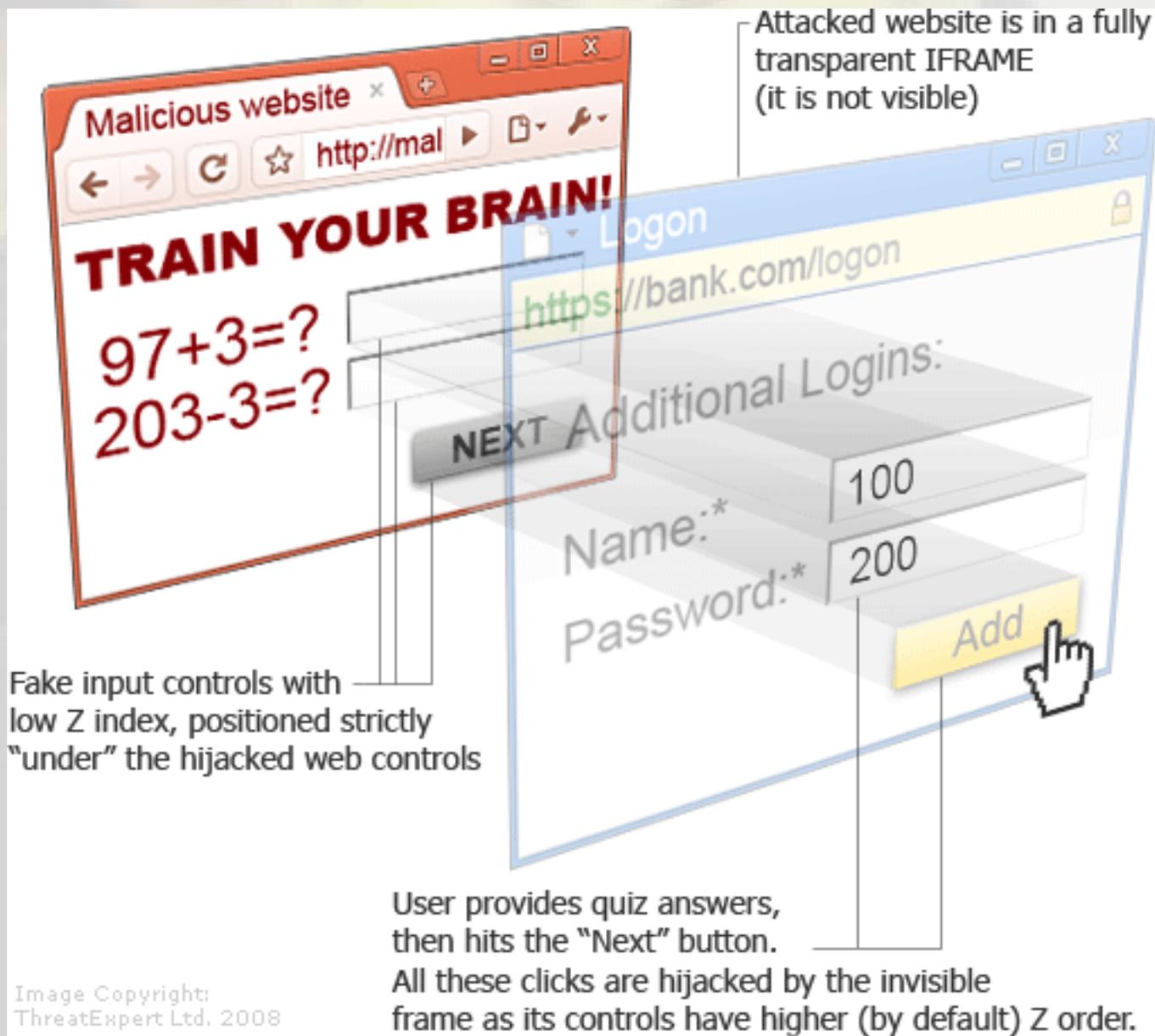
## *What was the real threat?*

Published a Christmas card on social networks that gave us remote access to anyone that clicked on the link. This gave us significant access to devices and data.

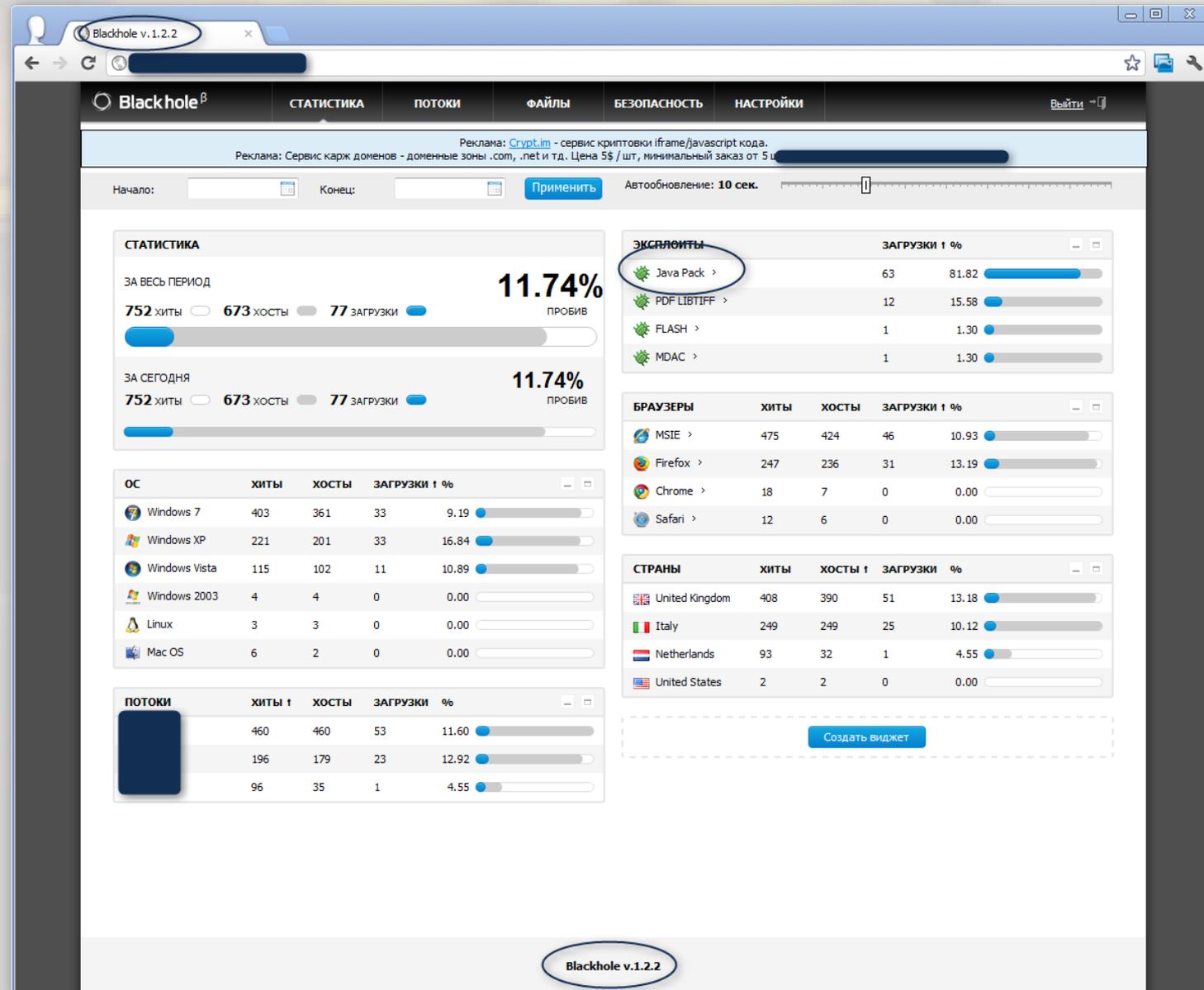
Happy Holidays!



# Other Attacks: Click Jacking



# Other Attacks: Malware



# Other Attacks: SET

## Using Credential Harvester module in SET - Kali Linux



Join us on `irc.freenode.net` in channel `#setoolkit`

The Social-Engineer Toolkit is a product of TrustedSec.

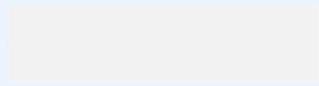
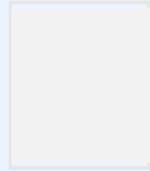
Visit: <https://www.trustedsec.com>

Select from the menu:

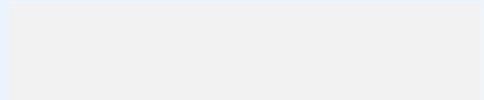
- 1) Spear-Phishing Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Generator Attack Vector
- 10) Powershell Attack Vectors
- 11) Third Party Modules



## RE: Join my network on LinkedIn



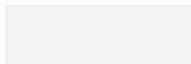
Talent Acquisition Director at



To: Emily Williams

Date: November 1, 2012

Happy to be your valet when you arrive in [REDACTED]! Give me a little notice when your schedule is set. Do you need any help in getting the Service Desk to accelerate the laptop and email issues?



On 11/01/12 12:51 PM, Emily Williams wrote:

-----

Thanks [REDACTED]!

I am still get situated getting my laptop and email. I can't wait to get started! Are you in [REDACTED] [REDACTED]? I think I will be coming up there soon to meet with a customer. You will definitely need to introduce me to everyone up there! :)

Er

'S

S

So

?

 [\[Name\]](#)  
Yesterday

Anyone ever had this happen? A person you don't know adds you that has a new profile with maybe 5 mutual friends – but no other friends. After they add you they start mass adding all of your friends. Other friends also email about the same thing – asking me how I know her. That's why I deleted her. Smells like a troll.

Like · Comment

 4 people like this.

 [View all 11 comments](#)

 [\[Name\]](#) This is why I stopped posting to Friends of Friends and just do it to Friends now.  
Yesterday at 12:35pm · Like ·  1

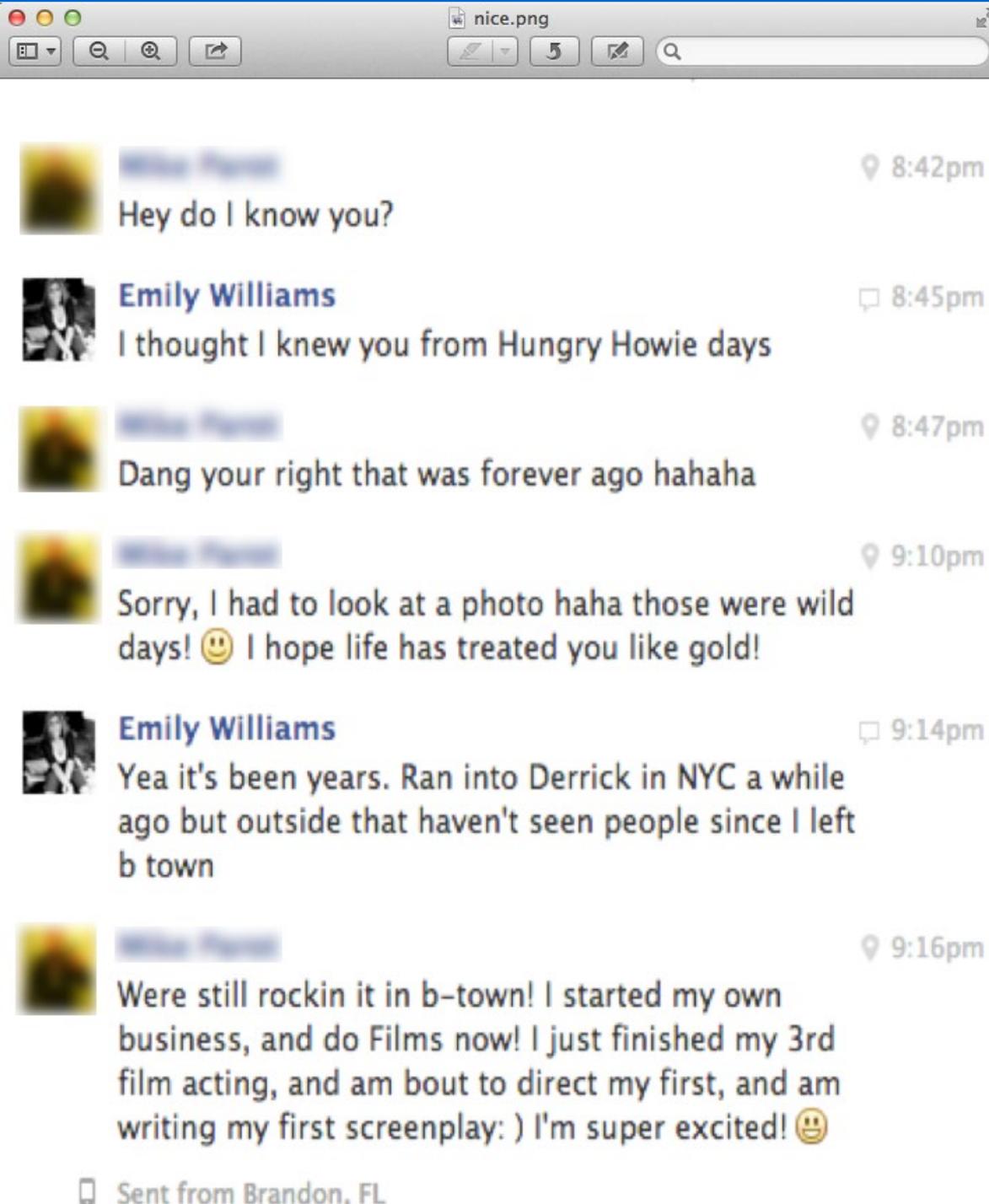
 [\[Name\]](#) Foff posting has definitely expanded my audience, but yeah... I have to deal with the BS sometimes. Fortunately, I've been the Robin Hood of trolls since 89.  
Yesterday at 12:37pm · Like ·  1

 [\[Name\]](#) Yes. Just today I was asked to be friends with 2 people I don't know. We only have one "mutual friend" between both of them. I just ignore them. I am considering thinning down the herd anyway, let alone adding new ones.  
Yesterday at 12:44pm · Like ·  1

 [\[Name\]](#) That is why I don't allow many realtors to be my friend. I am a realtor, I have seen how some of them work.  
23 hours ago via mobile · Like ·  1



We



ou!

What do

d be used

# Hard Drives



# Hard Drive Forensics

Purchased 10 hard drives from online auctions – Total cost \$700

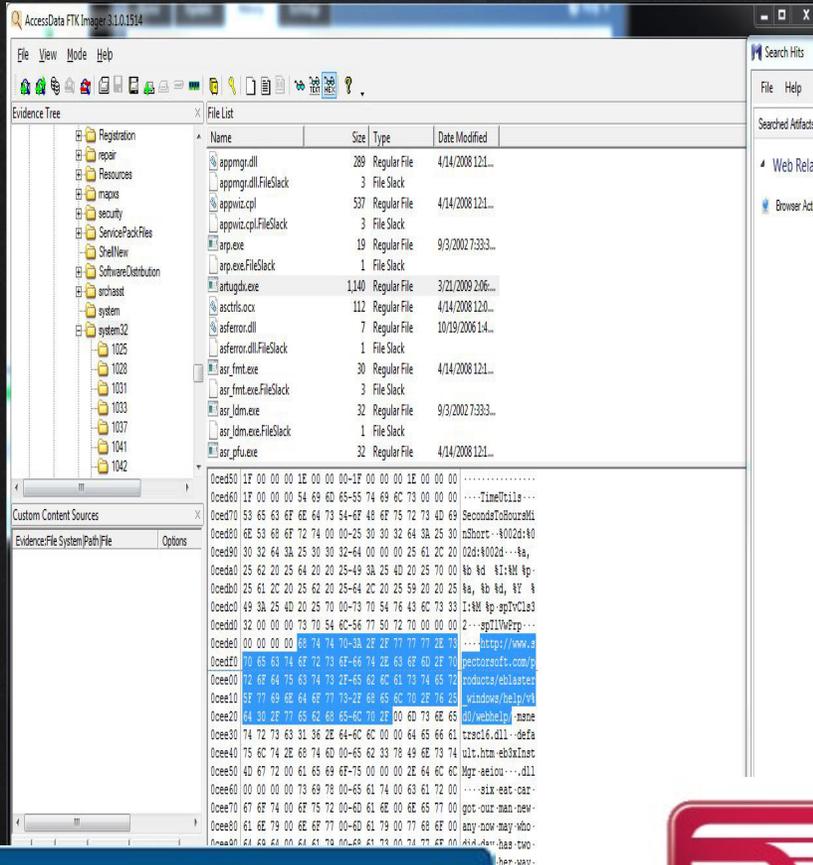
- X 1 Hard Drive forensically clean
- X 1 Hard Drive “floor model”
- X 8 Hard Drive had “interesting data”

Used FTK Imager

- X Show file content (block PII)
- X Show browser history
- X Show pictures



# FTK Imager



- DOTs is no data
- Sometimes all data was there, just hidden partitions
- Lots of drives with infected malware
- Slack space and corrupted clusters



Redline



And We Found



# Amazon Echo – “Alexa”

## Amazon Alexa Coming to Mexico in 2018, Developers Can Start Building Alexa Skills Now

BRET KINSELLA on August 9, 2018 at 1:31 pm



- Alexa Skills Kit is now available to developers to build Alexa skills localized for Mexico
- Amazon Echo smart speakers will launch later in 2018, date not disclosed but November is a good bet
- Sonos and Bose will ship Alexa-powered smart speakers in Mexico in 2018
- This follows a June announcements of forthcoming [Alexa availability in Spain](#) in 2018
- Google Home smart speakers began [shipping in Mexico](#) in June 2018

Amazon announced in a [blog post](#) yesterday that Alexa Skills Kit (ASK) is now available for developers to begin building



**“22 Million devices  
in homes as of  
2017” - Forbes**



# Alexa Skills Student Makes \$10K/Month

S

K

I

L

L

S

The image is a screenshot of a CNBC 'make it' article. At the top, the 'make it' logo is on the left, and 'VISIT CNBC.COM' and a search bar are on the right. Below the logo is a navigation menu with 'HOME', 'ENTREPRENEURS', 'LEADERSHIP', 'CAREERS', 'MONEY', and 'SPECIALS'. To the right of the menu are social media icons for Facebook, LinkedIn, and Twitter. A banner for 'ecobee3 lite SMART THERMOSTAT' is displayed, featuring a smart thermostat and a smartphone, with the text 'Control your smart thermostat from your phone.' and a 'LEARN MORE' button. To the right of the banner is a small advertisement for 'WORKS WITH ROOM SENSORS' with a 'Sold separately.' note. The main article title is 'This 22-year-old college student makes \$10,000 a month off Amazon's Alexa', with a sub-header 'ENTREPRENEURS' in a blue box. Below the title is the author 'Ali Montag | @Ali\_Montag' and the date '9:05 AM ET Thu, 12 April 2018'. The article image shows a young man smiling in front of a chalkboard with technical drawings. At the bottom, there is a long URL: 'https://adclick.g.doubleclick.net/pcs/click?xai=AKAOjssdcluuq2oJL9k\_Bzy2od8iePudfskDYzBfqXfOBPFqKjo0ArwBYXZ-opo4sNIIGPEuO6bMyky532fdp2VLJVymyNFUlagUxb2jZLZgYqHyAgrbsLEz2MRT66\_2SKq76yWrD6\_eRfLGVV...'

# Skill Squatting

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

MAD SKILLZ —

## Researchers show Alexa “skill squatting” could hijack voice commands

Homophones and mistakes in voice processing could be used to phish Echo users, research finds.

SEAN GALLAGHER - 8/30/2018, 5:40 PM



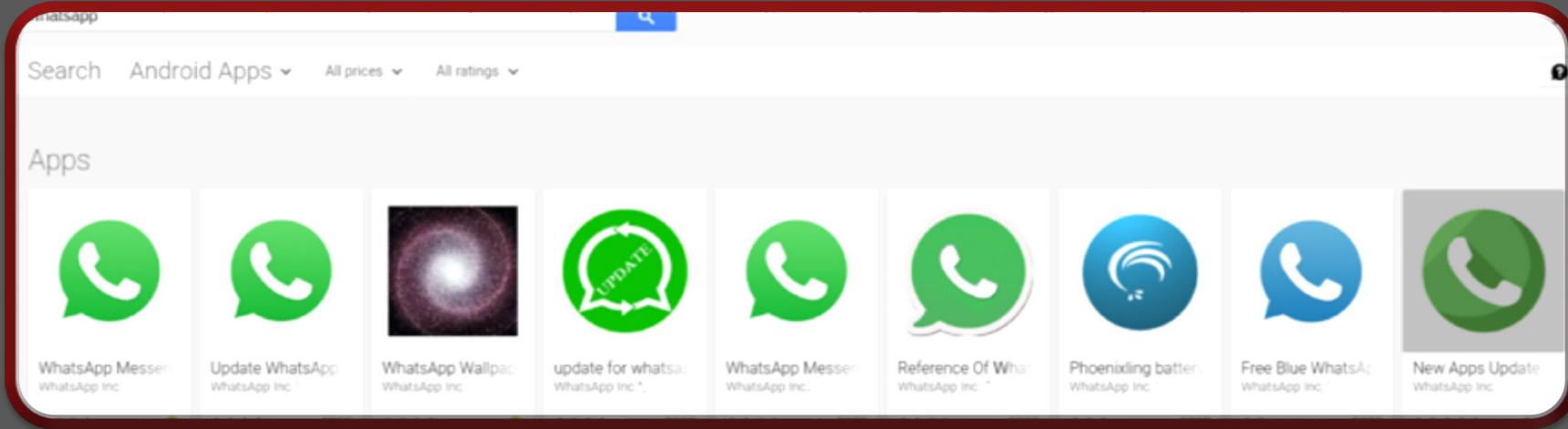
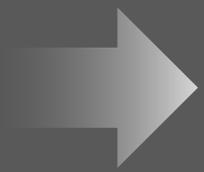
Alexa Skills

New Attack  
Surface

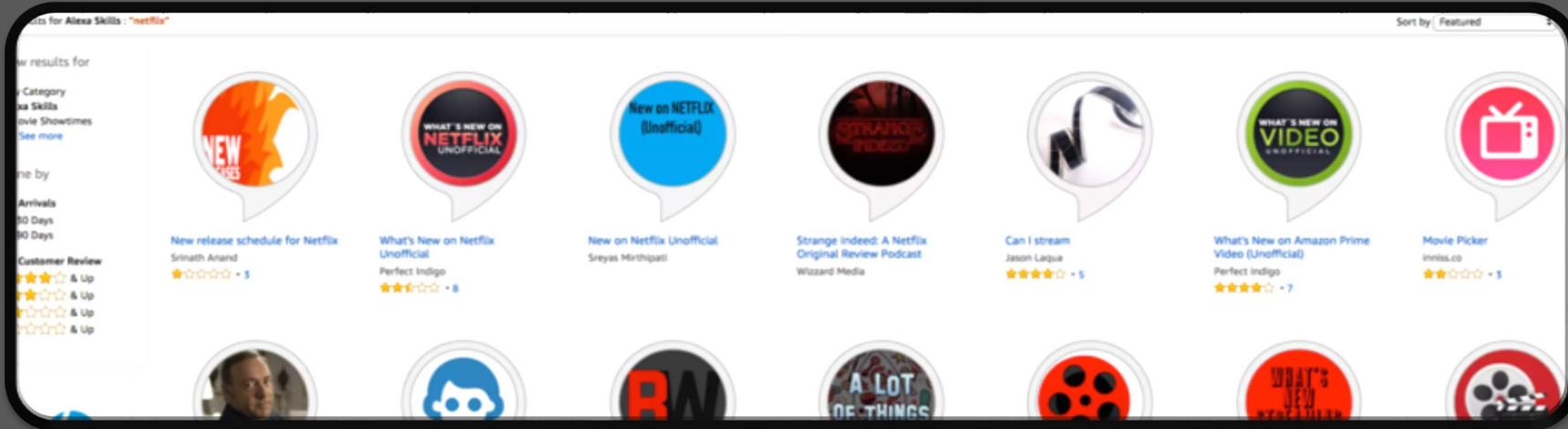
Sound-Alike  
commands

# Skill Squatting vs Mobile Implants

Mobile Implants



Skill Squatting



# Skill Squatting – How It Works

Criminals



Sound-alike  
Skill "Name"



Publish  
Skill

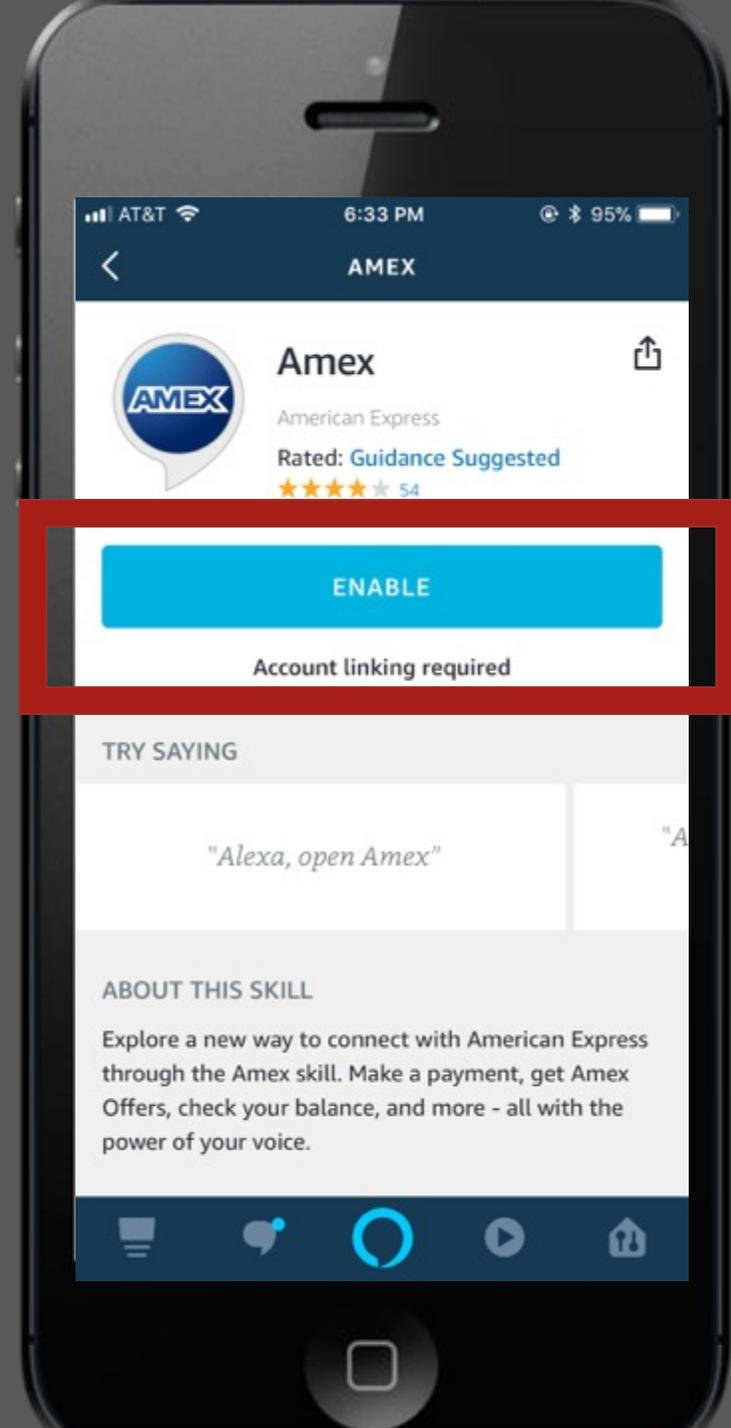
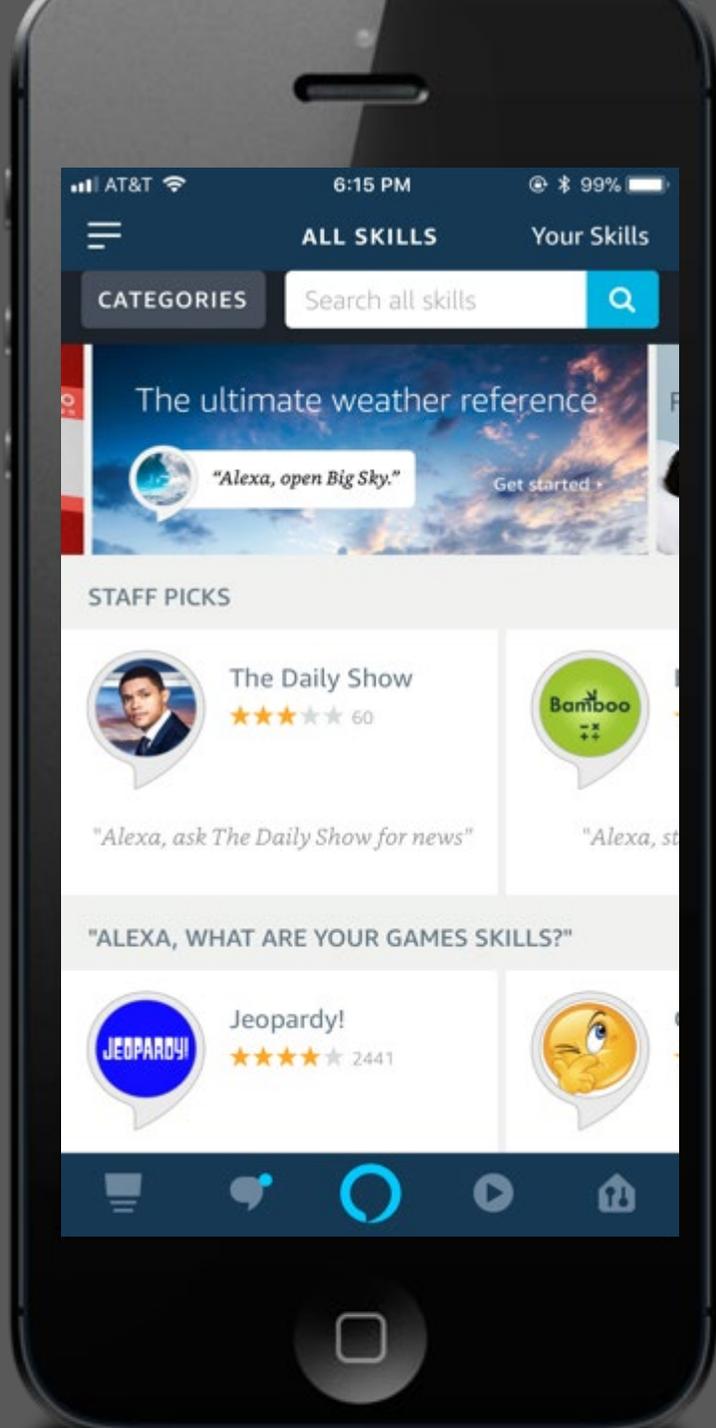


Alexa, open  
"Skill Name"



User enables  
"Skill"





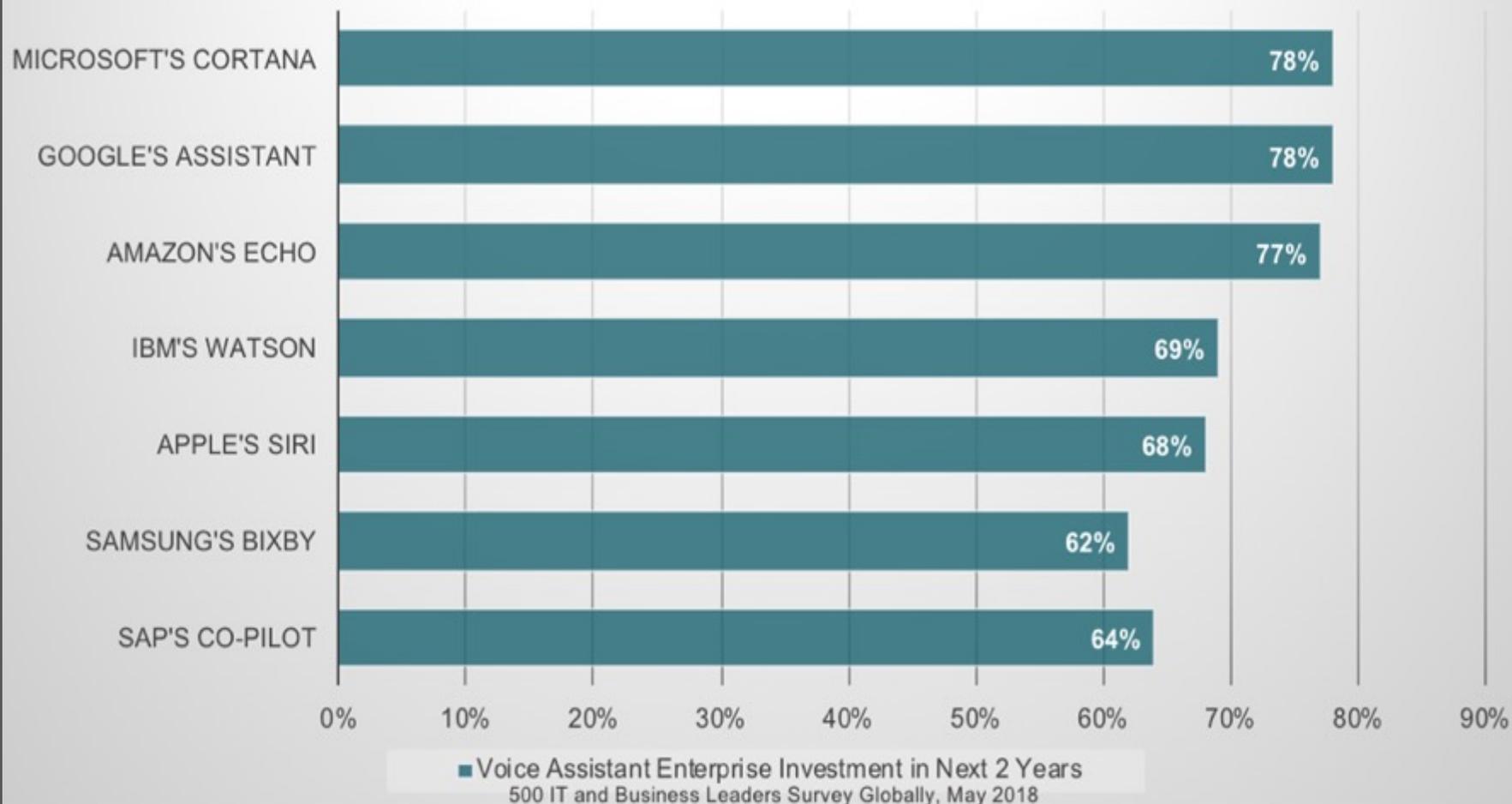
# Voice Assistants For Business

Microsoft

Google

Amazon

## Voice Assistant Enterprise Investment in Next 2 Years



# Open Sesame - Cortana Article



Cortana Voice Assistant

Open Sesame

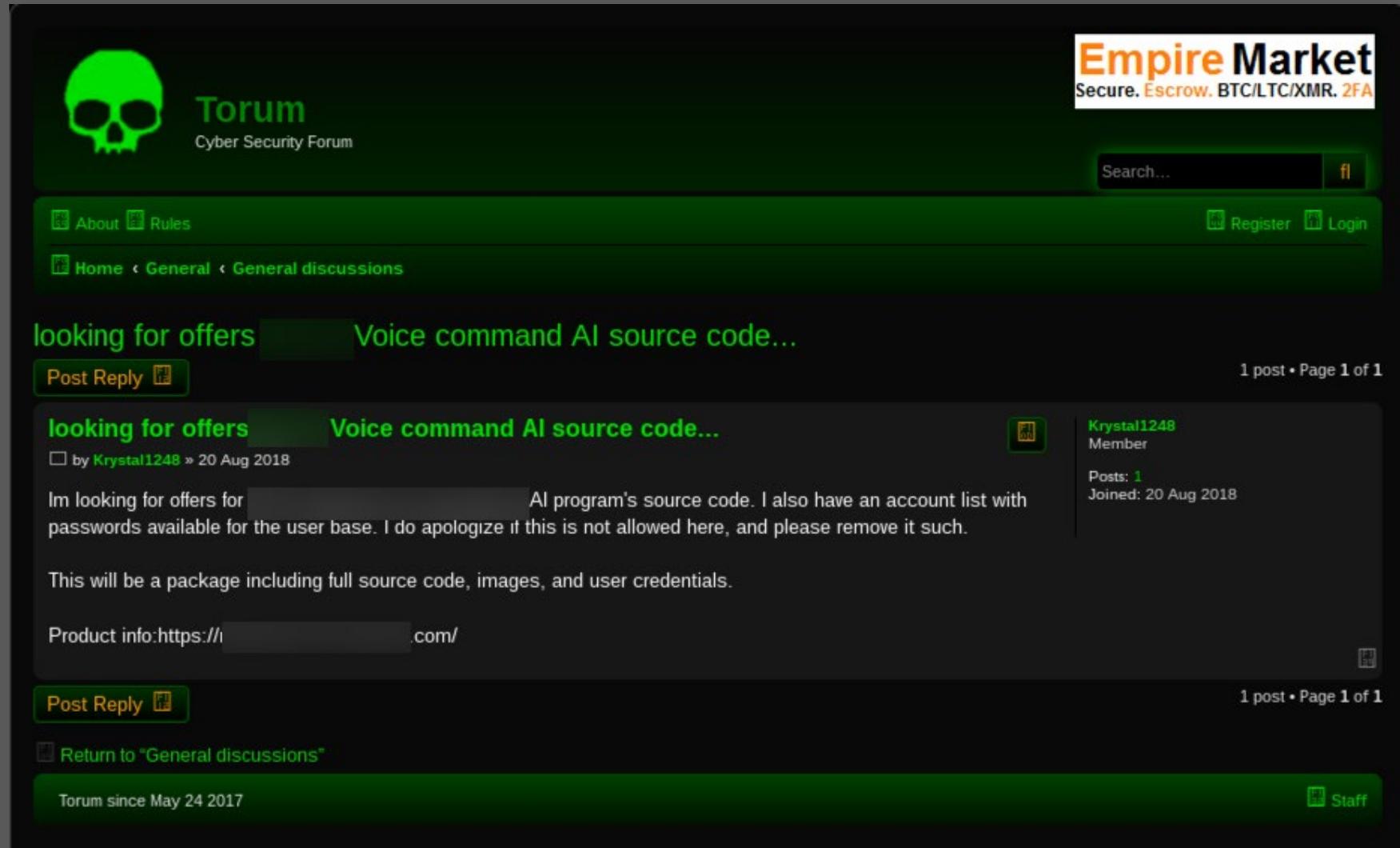
Windows 10 PCs

# Voice AI Source Code – Darknet Chatter

Looking for Offers

Workflow  
Automation

Digital Assistant



The screenshot shows a forum post on the Torum Cyber Security Forum. The forum's header includes a skull logo, the name 'Torum', and the tagline 'Cyber Security Forum'. In the top right corner, there is an advertisement for 'Empire Market' with the text 'Secure. Escrow. BTC/LTC/XMR. 2FA'. Below the header is a search bar and navigation links for 'About', 'Rules', 'Register', and 'Login'. The breadcrumb trail indicates the post is in the 'Home > General > General discussions' section. The post title is 'looking for offers [redacted] Voice command AI source code...'. The post is by user 'Krystal1248', a member who joined on 20 Aug 2018 and has 1 post. The post content reads: 'Im looking for offers for [redacted] AI program's source code. I also have an account list with passwords available for the user base. I do apologize if this is not allowed here, and please remove it such. This will be a package including full source code, images, and user credentials. Product info:https://[redacted].com/'. The forum footer shows 'Torum since May 24 2017' and a 'Staff' link.

# Drones – Bank Roof Top

## Game of Drones: For Criminals and Corporate Spies, the Sky's the Limit

By Rasika Sittamparam  
18TH APRIL 2018

+ INCREASE / DECREASE TEXT SIZE -



★ Add to favorites

**A rogue drone found on Credit Suisse HQ's roof; fears of acid drops into data centres: drones are the latest security threat for businesses. Rasika Sittamparam eyes the aerial battle.**

**Rogue Drones**

**Credit Suisse**

**Acid Drops into  
Data Center**

# How do Data Breaches Affect Me?



Do regular people care about data breaches

Does it really matter

**EQUIFAX**

What is the endgame?

# UBER – Data Breach

UBER Help

We're here to help

 Search Rider Help

TRIP ISSUES AND REFUNDS

ACCOUNT AND PAYMENT  
OPTIONS

A GUIDE TO UBER

SIGNING UP

MORE

ACCESSIBILITY

FOR RIDERS > MORE >

## Information about 2016 Data Security Incident

In October 2016, Uber experienced a data security incident that resulted in a breach of information related to rider and driver accounts.

Rider information included the names, email addresses and mobile phone numbers related to accounts globally. Our outside forensics experts have not seen any indication that trip location history, credit card numbers, bank account numbers, Social Security numbers or dates of birth were downloaded.

When this happened, we took immediate steps to secure the data, shut down further

**57 Million  
Customers**

**October 2016**

**600,000 Drivers  
and License #s**

# Drones – Darknet Listing



## Bypass your Drones No Fly Zone (NFZ) Restriction

Firmware Kill NFZ Drones Yuneec Q500, Q500+ & Q500 4K **IMPORTANT NOTE**

**We are not responsible for any miss use or any bad actions you may do that involves the use of this tool.**

Sick of you the No Fly Zone restrictions ??? You want to be able to fly anywhere you want ??? You want to fly over forbidden areas ??? When you b...

Sold by **WhiteChapel** - 0 sold since Jul 26, 2016 **Vendor Level 4** **Trust Level 5**

	Features		Features
Product class	Digital goods	Origin country	Worldwide
Quantity left	5 items	Ships to	Worldwide
Ends in	Never	Payment	FE Listing 100%

Same Day delivery via Private Message - 1 days - USD +0.00 / item

Purchase price: USD 50.00

Qty:  **Buy Now** **Que**

0.0390 BTC / 3.6206 XMR

Description

Bids

Feedback

Refund Policy

### Product Description

Firmware Kill NFZ Drones Yuneec Q500, Q500+ & Q500 4K

**IMPORTANT NOTE**

NFZ Bypass

\$50

Yuneec Drones

# So What, Now What

# FortiGuard Labs How We Do What We Do

**Advanced  
Research**

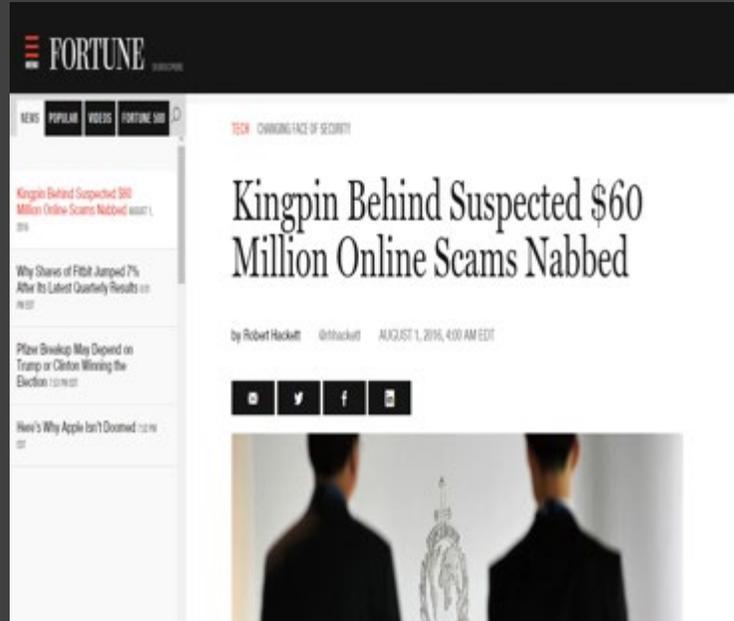
**Actionable  
Threat  
Intelligence**

**Artificial  
Intelligence**



# Fortiguard Labs Why We Do What We Do

**\$61 Million**



**9000 C2 Servers**



**Connected Cars**



The logo for FERTINET is displayed in a bold, white, sans-serif font. The letter 'F' is stylized with three horizontal bars. The letters 'E', 'R', 'T', 'I', 'N', and 'E' are solid. The final 'T' is also solid. A registered trademark symbol (®) is located to the right of the last 'E'. The background is a solid blue color with a complex, white, isometric wireframe pattern of overlapping rectangular and cubic shapes, creating a 3D architectural or technical aesthetic.

**FERTINET®**