Cyber-threats in Perspective.

Presented by: Gilles HILARY
gilles.hilary@georgetown.edu

GEORGETOWN UNIVERSITY
McDonough SCHOOL of BUSINESS

Three Segments

GEORGETOWN UNIVERSITY
McDonough SCHOOL of BUSINESS

Three Segments

Complex Hacks

BANGLADESH BANK
Central Bank of Bangladesh

TARGET

Target

- Install malware that steals credentials (HVAC vendor)
- Connect to Target's system (payroll,,…)
- Exploit a web application vulnerability

- Explore network
- Obtain admin privileges and persistent privileges

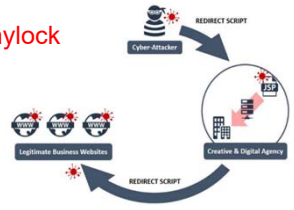
- Steal 70 million PII, no credit card (PCI-compliant)

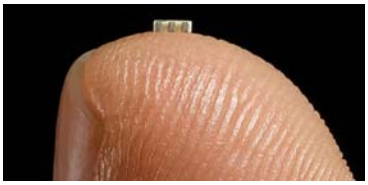
- Install malware steal 40 credit cards at PoS (the only custom malware)

- Send stolen data through the network and extract through FTP.

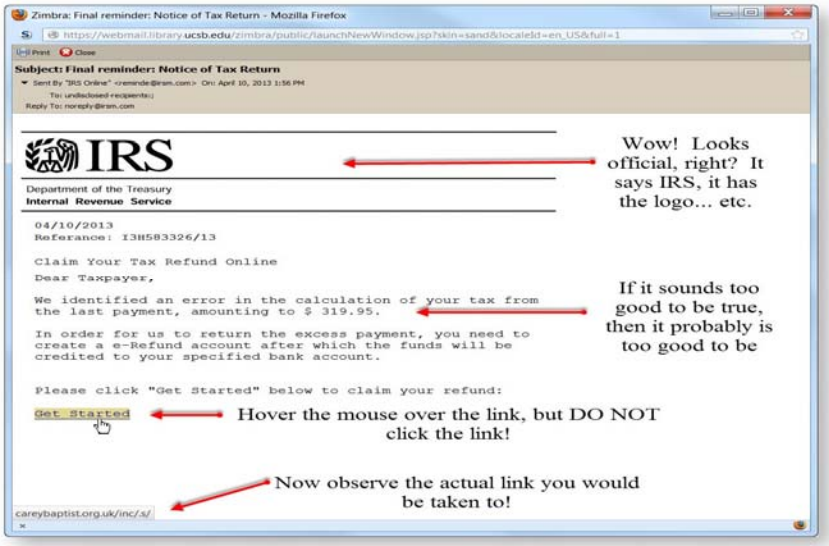
Wholesale Hacks

Shylock

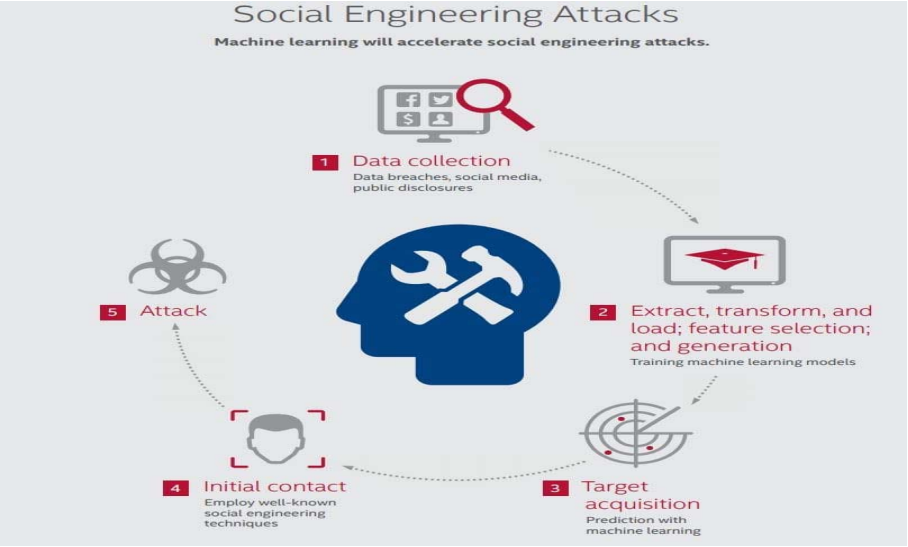




Phishing and Malware (cont.)



Social Engineering



Three Segments

DDoS Letter from Hackers – Real Example

From: Kadyrovtsy Sent: Wednesday, June 29, 2016 9:26 AM
To: customerservice; Subject: DDoS Attack Imminent - Important information

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Kadyrovtsy and we have chosen your Firm as target for our next DDoS attack.

All of your servers will be subject to a DDoS attack starting at Tuesday the 5th of July, 2016.

Right now we are running a small demo attack on YOUR IP 162.xxxx.x02 to prove that this is not a hoax.

What does this mean?
This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation amongst your clients.

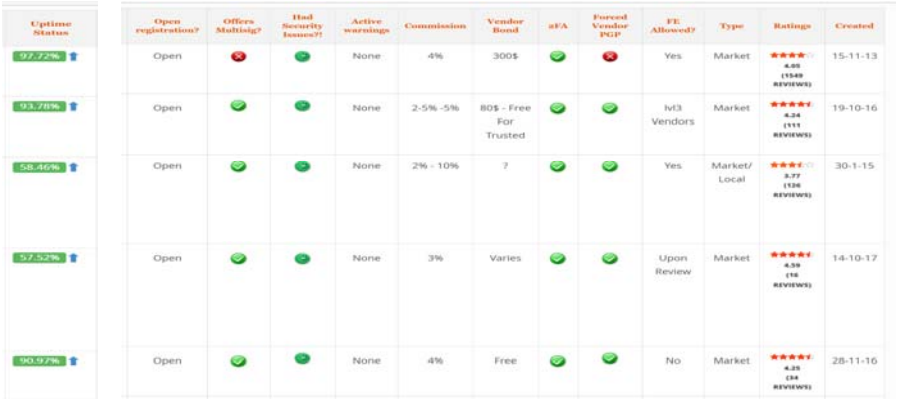
How do I stop this?
We are willing to refrain from attacking your servers for a small fee. The current fee is 20 Bitcoins (BTC). The fee will increase by 20 Bitcoins ($12,000) for each day (after Tuesday) that has passed without payment.

Please send the bitcoin to the following Bitcoin address:

UYY1NZ7R9sm1dvHtpKM4jWG1gU2zzyHGTGdvRDM

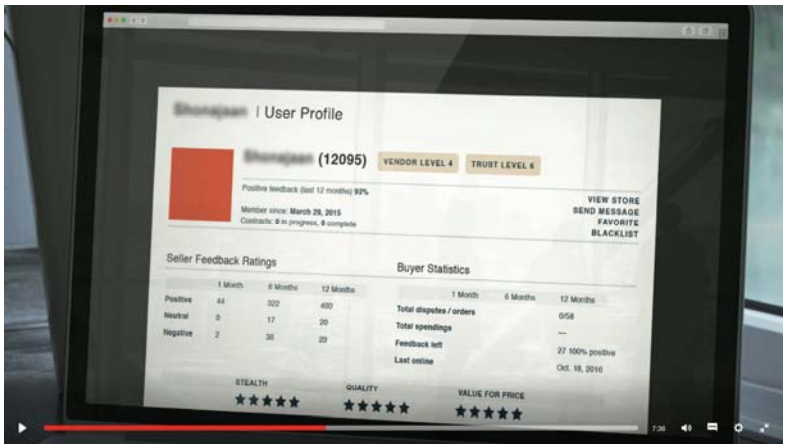
Crime-as-a-Service

- **Software-as-a-Service**
- **Platform-as-a-Service**
- **Infrastructure-as-a-Service**



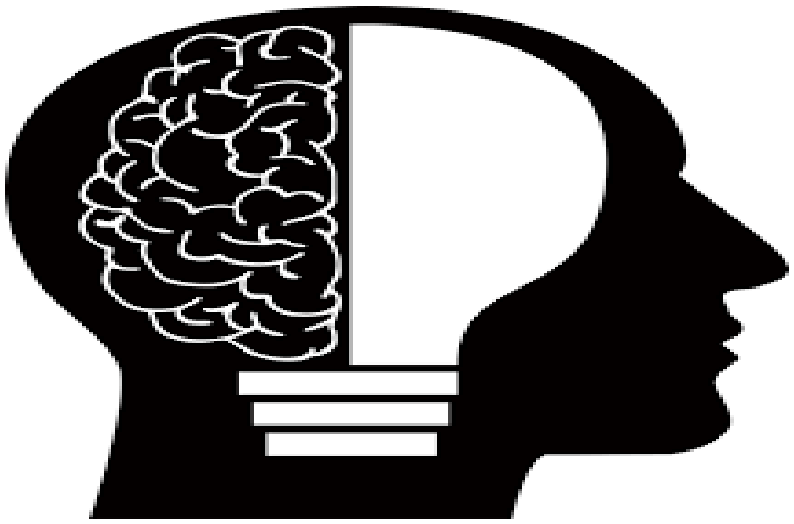
Uptime Status	Open registration?	Offers Multisig?	Had Security Issues?!	Active warnings	Commission	Vendor Bond	2FA	Forced Vendor PGP	FE Allowed?	Type	Ratings	Created
97.72%	Open	✗	✓	None	4%	300$	✓	✗	Yes	Market	4.05 (1549 REVIEWS)	15-11-13
93.78%	Open	✓	✓	None	2-5% -5%	80$ - Free For Trusted	✓	✓	lvl3 Vendors	Market	4.24 (111 REVIEWS)	19-10-16
58.46%	Open	✓	✓	None	2% - 10%	?	✓	✓	Yes	Market/ Local	3.77 (126 REVIEWS)	30-1-15
57.52%	Open	✓	✓	None	3%	Varies	✓	✓	Upon Review	Market	4.59 (16 REVIEWS)	14-10-17
90.97%	Open	✓	✓	None	4%	Free	✓	✓	No	Market	4.25 (34 REVIEWS)	28-11-16

12



13

Deep Fakes and AI



Objectives

GEORGETOWN UNIVERSITY
McDonough SCHOOL of BUSINESS

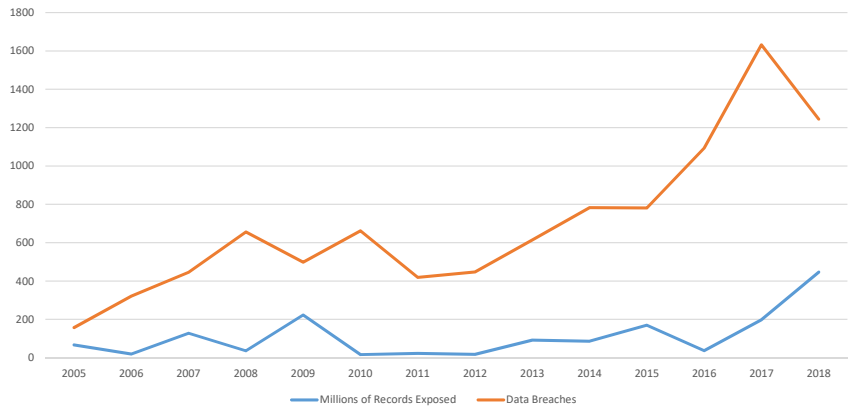
15

What Gets Stolen?

GEORGETOWN UNIVERSITY
McDonough SCHOOL of BUSINESS

Three Segments

Annual Number of **Reported** Data Breaches & Exposed Records in the United States *



* According to Statista.com


Graph 5a - Sony (SNE) : 24/11/14


Graph 5c - Home Depot (HD): 8/09/14 & 06/10/14


Graph 5d - Anthem (ANTM): 4/02/15

Equifax


160
140
120
100
80
60
2017
2018

Three Segments

21

Thank You !

Gilles.Hilary@georgetown.edu

FINRA's Small Firm Guidance

FINRA has created a Checklist for a Small Firm's Cybersecurity Program to assist in the establishment of the program including:

- Identify and assess cybersecurity threats, protect assets from cyber intrusions
- Detect when their systems and assets have been compromised
- Plan for the response when a compromise occurs
- Implement a plan to recover lost, stolen or unavailable assets

This checklist is primarily derived from the National Institute of Standards and Technology (NIST) Cybersecurity Framework and FINRA's Report on Cybersecurity Practices

Use of this checklist does not create a "safe harbor" with respect to FINRA rules, federal or state securities laws, or other applicable federal or state regulatory requirements.

Executive Email Compromise & Wire Fraud