Cyber-threats in Perspective.

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

Three Segments
Three Segments

Complex Hacks

[Images of logos: Bangladesh Bank and 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.)

Wow! Looks official, right? It says IRS, it has the logo... etc.

If it sounds too good to be true, then it probably is too good to be true.

Social Engineering

Social Engineering Attacks

Machine learning will accelerate social engineering attacks.

1. Data collection
   - Data breaches, social media, public disclosures

2. Attack
   - Initial contact
     - Employ social engineering techniques
   - Target acquisition
     - Persuade with machine learning

3. Extract, transform, and load; feature selection; and generation
   - Training machine learning models

4. Initial contact
   - Employ social engineering techniques

Now observe the actual link you would be taken to!
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:

UYYINZ7R9nmlzlwHtrpKM4jWG1gUL2zzyHGTGdzvRDM
Crime-as-a-Service

- Software-as-a-Service
- Platform-as-a-Service
- Infrastructure-as-a-Service
Deep Fakes and AI
Objectives

What Gets Stolen?
Three Segments

![Image of a fish underwater]

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

* According to Statista.com
Equifax
Three Segments

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

![Image of an email message]