Not another phishing presentation

1

Not another phishing presentation

2

Phishing presentations are boring

- Don't open that email
- Don't click on that link
- Only go to links you trust
- Look for the green bar

Not another phishing presentation

3

What we'll talk about

- This isn't about you, this is for your organization
- What do actual attacks look like?
- Where does that data/money, go?
- How do we protect our organizations?

Not another phishing presentation

4

What do attackers want

- Trick victim into sending money
- Send money via extortion/faketortion
- Send them information
- Access to an account
- Execute a malicious program

Not another phishing presentation

5

How are businesses actually compromised

Phishing

- Broad attack focusing on a businesses customers or company wide attack
- Two types of attacks to worry about
  - Brand Reputation attack – Attacking the customer
  - Malware installs – Attacking the organization

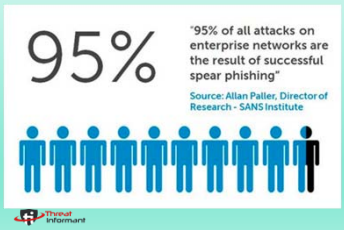
Not another phishing presentation

6

How are businesses actually compromised

Spear Phishing

- Directed and well researched attack against an individual or small group



Not another phishing presentation

7

How are businesses actually compromised

Whaling

- Business Email Compromise (BEC)
  - On the rise
  - Not a volume play. Attacks are carefully researched
  - FBI shows $5.3 billion lost to BEC over October 2013 to Dec 2016
  - Incidents knows to FBI are estimated to be 20% of total

72% of whaling attackers pretended to be the CEO, while 36% were attributed to the CFO.

Not another phishing presentation

8

What does an attack actually look like?

AFGlobal Corp (-$480k)

Glen,

I have assigned you to manage file T521, this is a strictly confidential financial operation, to which takes priority over other tasks. Have you already been contacted by Steven Shapiro (attorney from KPMG)?

This is very sensitive, so please only communicate with me through this email, in order for us not to infringe SEC regulations. Please do no speak with anyone by email or phone regarding this.

Regards,
Gean Stalcup

- 30 minutes later, Mr Wurm was contacted by Mr shapiro stating that due diligence fees regarding the China acquisition were needed.
- The company attempted to recover the money but the account had already been zeroed out shortly after the transfer
  - 30 minutes later, Mr Wurm was contacted by Mr shapiro stating that due diligence fees regarding the China acquisition were needed.
  - The company attempted to recover the money but the account had already been zeroed out shortly after the transfer

Not another phishing presentation

9

What happens after?

- Darkweb markets
  - Most of this you can actually find on the normal web
- Malware attacks
  - System compromise

Not another phishing presentation

10

What happens after?

Perfect for:
TAX SEASON
OBTAINING NEW LINES OF CREDIT
GETTING LOANS
GETTING VEHICLES
OPENING BANK ACCOUNTS
OPENING VENMO OR PAYPAL

You will find no better on any other place other than here.

These are WITHOUT credit card info
BUT, these do come with acct number and routing number

Tax season is around the corner friends, let's make as much money as we can

YOU WILL RECEIVE THE FOLLOWING

first name
last name
ssn
date of birth
bank name
account type
account #
routing #
mmn
dl_number
dl_state
gender
residence_type
residence_length
address1

address1
city
state
zip
phone_home
phone_cell
email
ip_addr
net_income
employer_name
job_title
phone_work
direct_deposit
reference1_firstname
reference1_lastname
reference1_relationship
phone_reference1
reference2_firstname
reference2_lastname
reference2_relationship
phone_reference2

Threat Informant

www.threatinformant.com

Not another phishing presentation

11

What happens after?

Threat Informant

www.threatinformant.com

Not another phishing presentation

12

What happens after?

Threat Informant

www.threatinformant.com

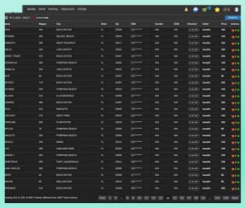
Not another phishing presentation

13

What happens after?

W2 Markets and Drop Sites

Name	Wagers	City	State	Zip	SSN	Gender
JOAN	44K	BOCA RATON	FL	33486		N/A
ARTEMIO	28K	DELRAY BEACH	FL	33444		N/A
ROBERTO	19K	WEST PALM BCH	FL	33417		N/A
EMILIO	32K	LAKE WORTH	FL	33461		N/A
SIDNEY TRANT	57K	BOCA RATON	FL	33487		N/A
NORMAN W	26K	POMPANO BEACH	FL	33060		N/A
DANIELLE	24K	LAKE WORTH	FL	33461		N/A
JACK	6K	BOCA RATON	FL	33487		N/A



Threat Informant
www.threatinformant.com

Not another phishing presentation

14

How to protect our organizations?

Culture

- Employees should feel they won't get fired
- It's okay to double check with superior if something doesn't feel right
- You should double check with superior on major financial transactions
- Explain, there are certain things I will never ask you to do over email
- Check with security just to make sure..

Training Is Great

- Organizations that invest in phishing training see great ROI
- Training will reduce users that take unwanted actions, but it doesn't eliminate the risk
- Know your risk – phishing assessments

When training fails, and it will fail

- Tag external emails so that it is obvious to users
- DLP (Data loss prevention)
  - Scans data in messages before sending out
  - Enforces encryption to USB
- Email firewall rules/detections
  - Detect and quarantine suspicious emails
- Why doesn't my organization have this?
  - You probably do
  - It's a lot of work to monitor and configure

Threat Informant
www.threatinformant.com