CYREN

PHISH GUTS

The Anatomy of a Phishing Attack

While most folks know what phishing is, few realize the lengths to which a criminal will go to initiate a phishing attack. More than just distributing emails with fake corporate logos like LinkedIn or Facebook, cybercriminals design attacks carefully by using fake clickable advertising, spoofing well-known online brands, and creating legitimate-looking phishing websites to capture the sensitive data that the unsuspecting victim enters.

STEP 1 VICTIM IDENTIFICATION

Mass Phishing Attack

- Untargeted, large group of victims.

Targeted Phishing Attack

- Specific group, or high profile victim.

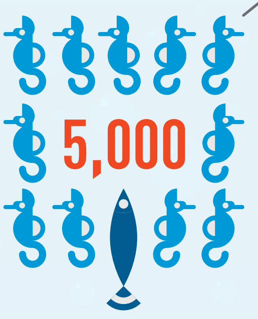
$2.3 BILLION

Amount lost to corporations in the last three years due to targeted spear phishing of CEOs, according to an FBI report.

STEP 2 SOURCE SETUP

Brand Names

- Phisher selects a brand name for mass email distribution, such as LinkedIn, PayPal, or FedEx.
- Using a newly created domain or a hacked website, phisher builds webpages that resemble those of trusted brand name.



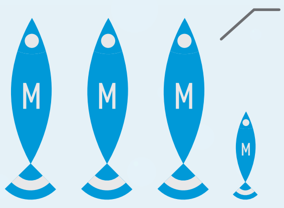
5,000

Number of fake phishing pages found on just one hacked website

Sophisticated Content

- Phisher develops an email with legitimate-looking content requesting legal or financial information.
- Spoofs the email address of someone at the target organization or of a contact known to the target.

STEP 3 ATTACK DISTRIBUTION



4.44 MILLION

Number of phishing URLs distributed in the 2nd quarter of 2016

Mass Distribution

- Phisher sends a mass distribution email containing brand logos/name and links to fake webpages.
- Places links to fake web pages in banner ads, on social media, or in text messages.

Targeted Distribution

- Phisher sends email to specific target victim or group.

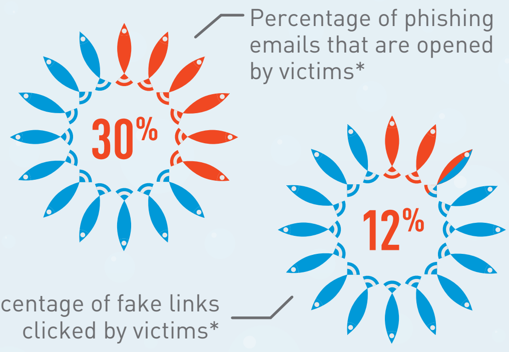
STEP 4 HOOK VICTIMS

Click Fake Links

- Victims click on link in the email and enter sensitive credential information into fake web page.

Respond Directly To Email Request

- Victim responds directly to email with requested information, such as login credentials or financial information.



Percentage of phishing emails that are opened by victims*

Percentage of fake links clicked by victims*

*SOURCE: 2016 Verizon Data Breach Investigations Report

STEP 5 EXPAND / MONETIZE

Develop Additional Attacks

- Phisher uses stolen credentials for the next phase of the attack (such as an APT).
- Collects additional email addresses from hacked accounts for future attacks.

Financial Gain

- Phisher sells the stolen credentials on the black market.
- Phisher steals money using credentials from bank, PayPal account, or fake wire transfer.

.

$60 MILLION

Amount stolen from SMBs in financial phishing scams by a single cybercriminal recently arrested by Interpol