THE ANATOMY OF AN ENTERPRISE

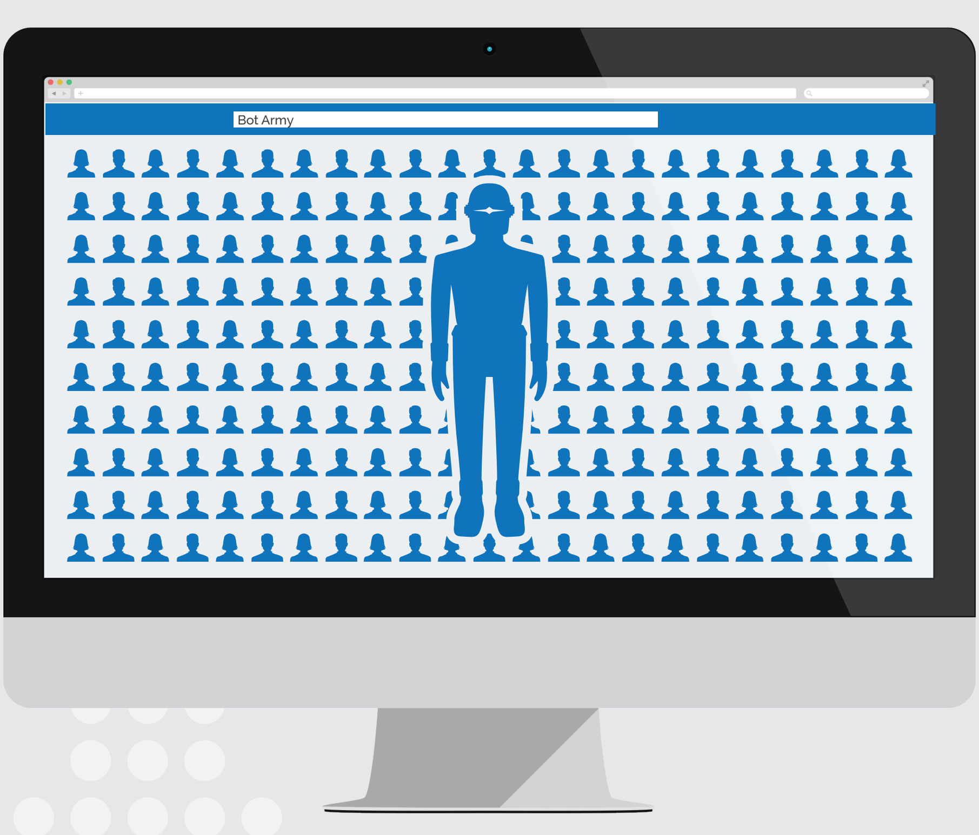
SOCIAL MEDIA CYBER ATTACK

When new technology becomes mainstream, it's sure to quickly attract the cyber criminal. Social media has become part of our every day lives, both personally and professionally. It has changed the way we communicate with our friends, family, colleagues and customers...and it also has become one of the fastest growing cyber attack vectors. Cyber criminals use social networks, including sites such as LinkedIn, Facebook, Twitter, Skype, and VKontakte as mediums for launching targeted malware and phishing schemes.

THE PREP » CYBER CRIMINALS BUILD AND PREPARE SOCIAL MEDIA BOT ARMIES

Bot Armies* are key to Enterprise Social Cyber Attacks. Cyber criminals aim to masquerade their bots as trustworthy social media profiles. To achieve this goal, they populate their bots with relevant popular content. By posting viral videos and popular articles, and even buying 'likes', cyber criminals create social media profiles that potentially reach millions of users.

millions of users



*There are essentially two types of bots. One is a bot account that is created and operated remotely via software. The other is a "sock puppet" – a false account operated by an individual pretending to be someone or something they're not. Facebook estimates that between 5-6 % of all accounts are bogus. When a group of these bogus accounts are created together to accomplish a common goal, the output is a bot army.

Lazy criminals can buy software-controlled bot armies for as cheap as 6¢ per bot; human-verified social bots can fetch a price as high as $1.25.

SELECTING A TARGET

targets

Once bots are created, the next step in the preparation phase is selecting a target. In order to increase effectiveness, the cyber criminal will either focus attacks against specific organizations, an organization's customers or against the general public via popular topic hijacking (trendjacking)*.

**Trendjacking is a common PR tactic that subverts trending topics and discussions to inject a different message into the conversation. Much like a PR team, the cyber criminal injects malware and phishing attacks, masquerading as another interested party (e.x. #MileyCyrus is trending and the attacker posts – "#MileyCyrus OMG did you see this video of Miley?! http://bit.ly/@&Dkdl@")*

MAKING CONNECTIONS

connections

In order to initiate an attack, the cyber criminal needs to connect his bots with the targeted victims. More bot connections mean more potential victims. To make connecting more successful, the manager of the bot armies will fill the bots profiles with attractive photos, funny images or anything else to draw the attention of the targets based on their interests.

Even the most savvy can fall victim, think about the business development or sales rep that gets enticed by a bot pretending to want to do business.

DISTRIBUTION! » CYBER CRIMINAL PICKS MODE OF ATTACK: PHISHING OR MALWARE

PHISHING VS. MALWARE

PHISHING

The cyber criminal sets up a phishing website disguised as a reliable site. For example, the phishing site could look just like a bank's, and ask customers to enter their login credentials.

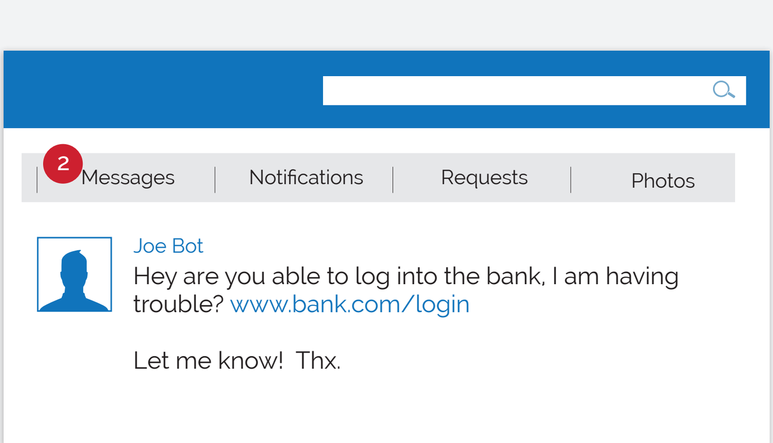
Phishing is the act of attempting to acquire sensitive information (usernames, passwords, credit card info and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

MALWARE

Cyber criminals hide Malware on websites that can consequently launch or download without the target even knowing! All it takes is one errant visit or click to the malicious URL and the attacker has hooked another victim.

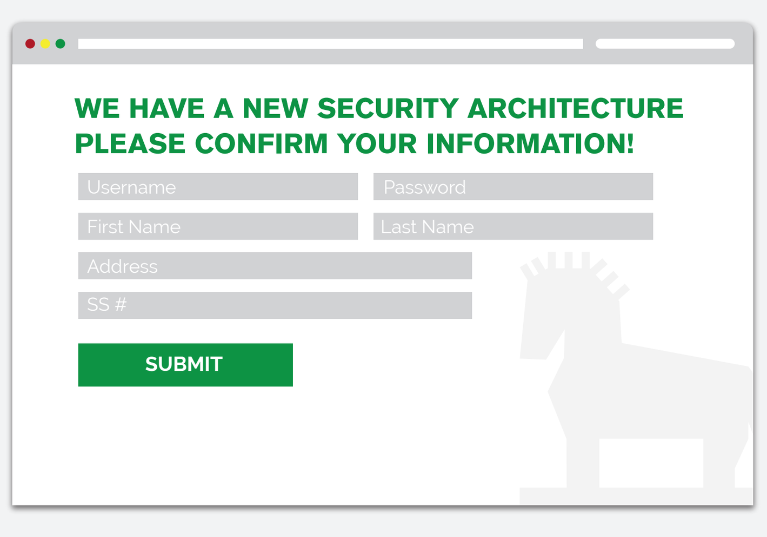
Malware is a file that infects devices, networks and systems and is usually repackaged and hidden from traditional anti-virus and anti-malware technologies.

A FRAUDULENT WEBSITE IS BUILT



MALWARE IS BOUGHT OR CREATED

WEBSITE IS SHARED WITH THE TARGET



A SHORTENED LINK TO THE DISGUISED MALWARE IS SHARED WITH TARGET

WEBSITE PROMPTS THE TARGET TO ENTER SENSITIVE INFORMATION

TARGET CLICKS LINK THAT EXECUTES MALSCRIPT/ DOWNLOADS MALWARE

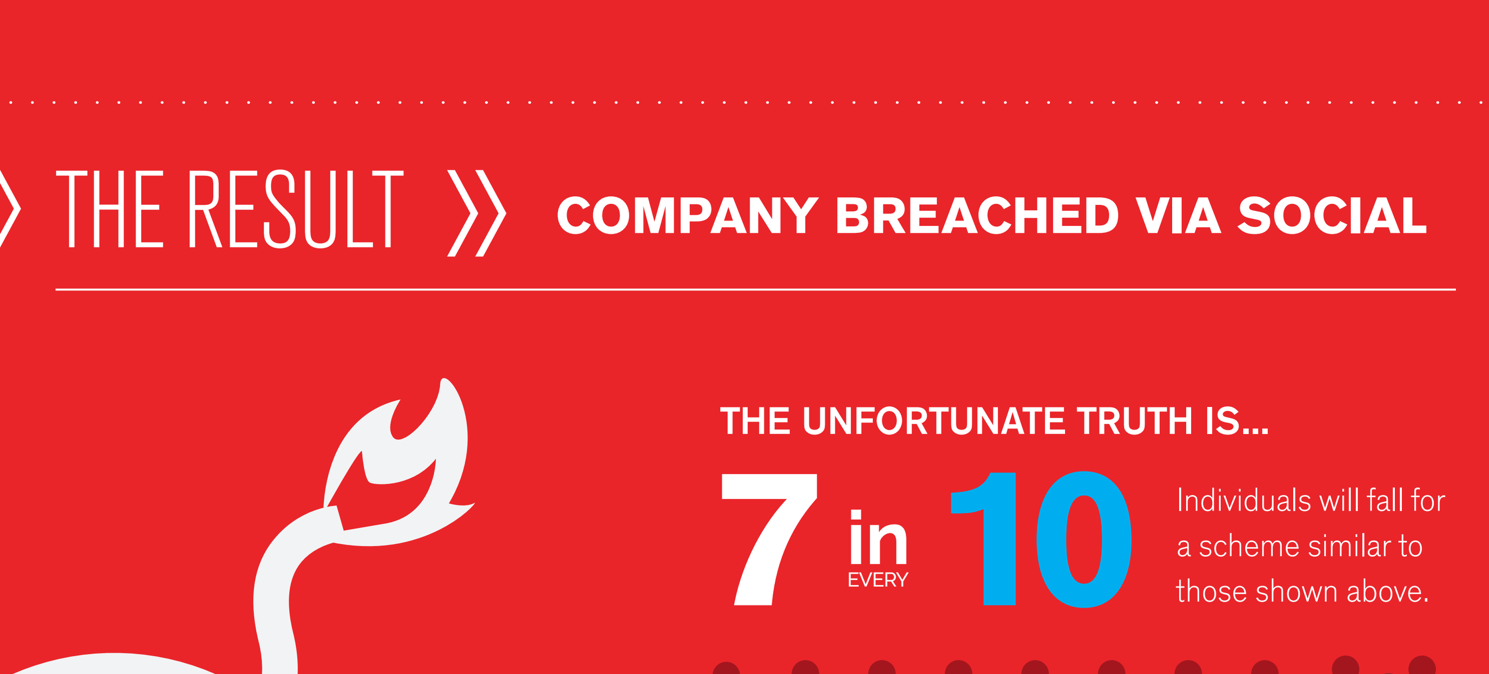
THE CYBER CRIMINAL EITHER USES "CLEAN" DOMAINS (NO BAD REPUTATION DATA) TO HOST THESE MALICIOUS PAGES OR RAPIDLY CHANGES THE END LOCATION SO AS TO AVOID DETECTION BY TRADITIONAL WEB FILTERS OR ADVANCED FIREWALLS.

CYBER CRIMINAL NOW HAS ACCESS TO ACCOUNT AND PERSONAL INFORMATION*

*People will commonly use the same passwords for work accounts and personal accounts. Even a personal phishing attack is of concern to organizations as this might result in privileged access credentials leaking out.

CYBER CRIMINAL NOW HAS ACCESS TO YOUR DEVICE*

Malware can be written for any platform and can effect anything from cell phones, tablets, laptops and desktops as well as servers and storage devices.



THE RESULT » COMPANY BREACHED VIA SOCIAL

THE UNFORTUNATE TRUTH IS...

7 in EVERY 10 Individuals will fall for a scheme similar to those shown above.

Whether it's a work laptop or a personal device that gets infected, malware now has access to data, passwords and anything else worth stealing! In fact, when malware is introduced to an environment, it typically tries to replicate and infect any other systems on the network, even home networks.

Once infected targets connect to the company network, malware can capture data from anywhere across the enterprise.

THIS MEANS IMPORTANT COMPANY DATA COULD BE EASILY TRANSMITTED BACK TO THE CYBER CRIMINAL.

CONSEQUENTLY IN 2013:

ONE-THIRD OF DATA BREACHES ORIGINATED VIA SOCIAL MEDIA

RESULTING IN AN AVERAGE LOSS OF 5.4 MILLION DOLLARS PER ATTACK

GET PROTECTED! » LEARN MORE ABOUT THE RISE OF SOCIAL CYBER ATTACKS AT

ZEROFOX.COM

BROUGHT TO YOU BY

ZEROFOX®

— & —

National Cyber Security Awareness Month