Mike Raggo, ZeroFOX

Attacks on Enterprise Social Media

// OUR AGENDA

- Social Media Threat Landscape
- Anatomy of social media attack
- Social Media Footprinting, Monitor & Profile, Impersonate, Attack
- Topical Social Media Threats
- Countermeasures

#whoami

Mike Raggo (CISSP, NSA-IAM, ACE, CSI)

- •Author, Speaker, Researcher, Governing Bodies Participant
- •Mobile device and Smartwatch ethical hacking
- •18 years research Steganography, Covert Communications
- •Former digital forensics investigator (certified)

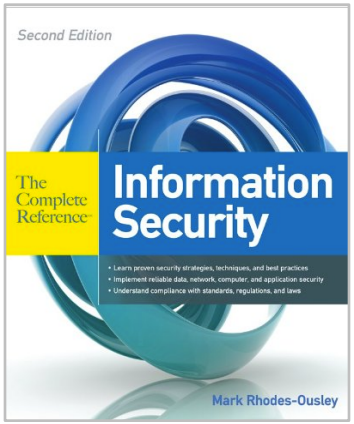
RSA CONFERENCE

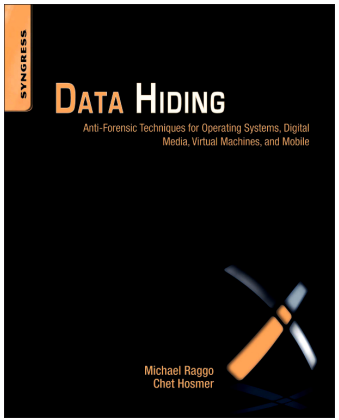
black hat

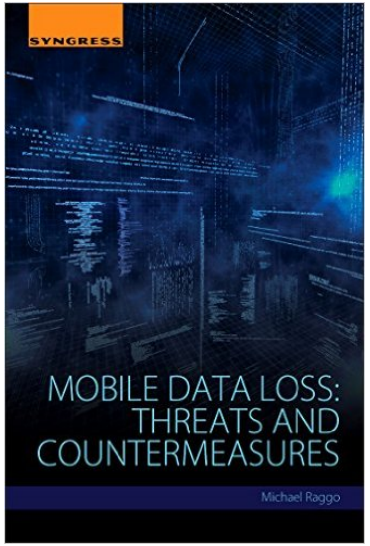
DEF CON

THE UNITED STATES CYBER CRIME CONFERENCE 2014

HackCon





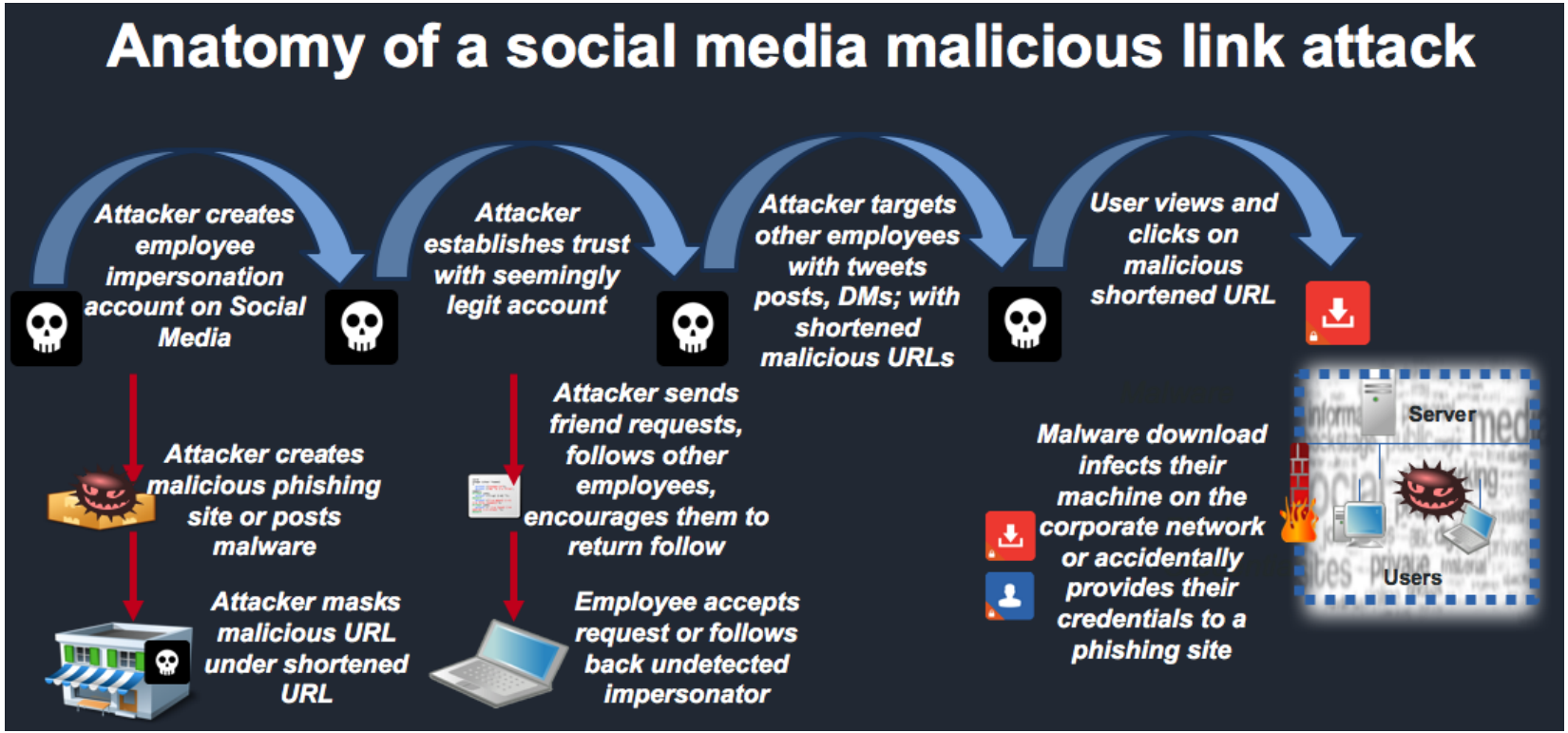


Book signing 3:30 today

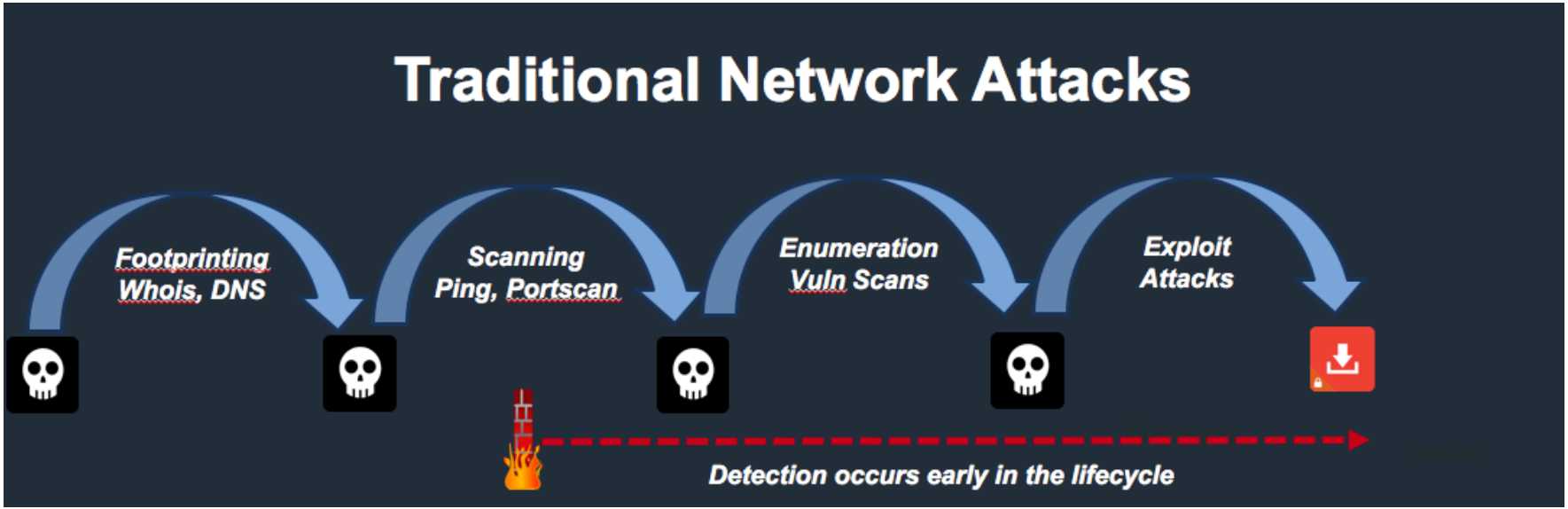
// Social Media Threat Landscape

- **Social media blurs the lines** between our personal lives and work day
- **New threat landscape** is evolving introducing new methods of attack
- Social media attacks are being used to:
  - Impersonate executives, brands, and employees
  - Hijack Accounts
  - Distribute malware
  - Phish credentials
  - Discredit company brands
  - Perform scams
  - Execute cyber attacks
  - Stage violence
  - And more…

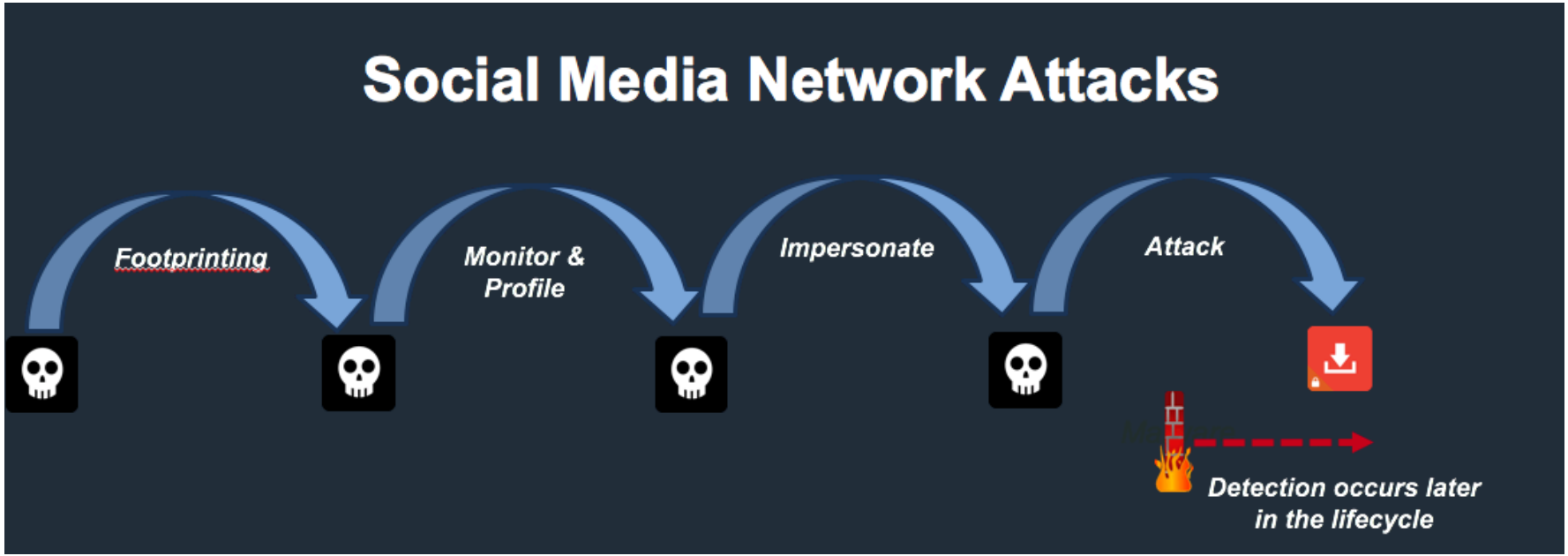
// Social media attack targeting corporate network



// Traditional Network Attacks vs. Social Media Attacks



// Social Media Attacks – Build a network of “trust”



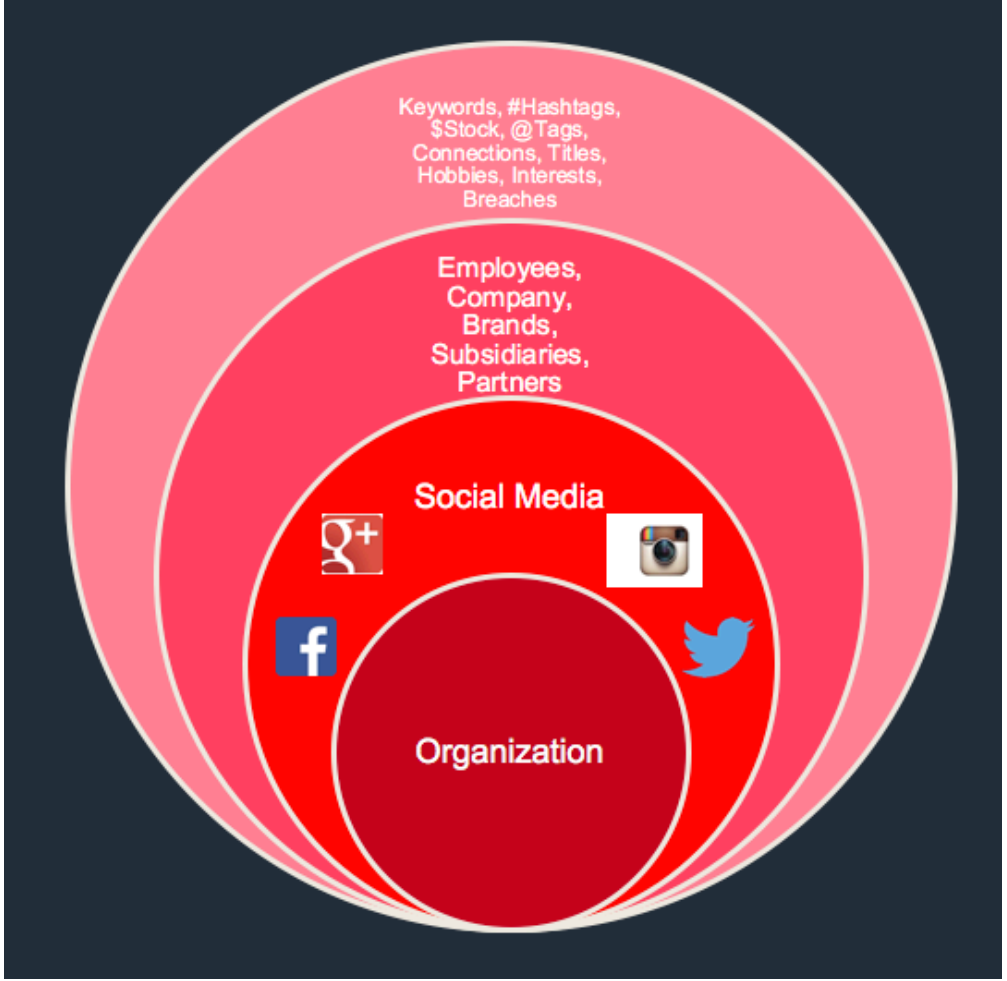
Build a network of ”trust”!!!

// Footprint

LinkedIn	company employees, titles, locations, email addresses, phone numbers, former employees
Twitter	bio, interests, other Twitter accounts they own, other brands/sub-brands, employees responsible for managing brand accounts, followers
Facebook	bio, birthday, interests, hobbies, connections
Google+	corporate ID or login, interests, hobbies, connections

// Monitor & Profile

- Social Media Accounts
- Dormant accounts
- Subsidiaries
- Responsible people for those accounts
- Partners
- Keywords
- #Hashtags
- @<mentions>
- $Stock
- Hobbies, interests
- Titles



// Monitor & Profile

// IMPERSONATIONS

- Our sampling of approximately ***100 enterprises shows more than 1000 impersonation accounts are created weekly*** by perpetrators.

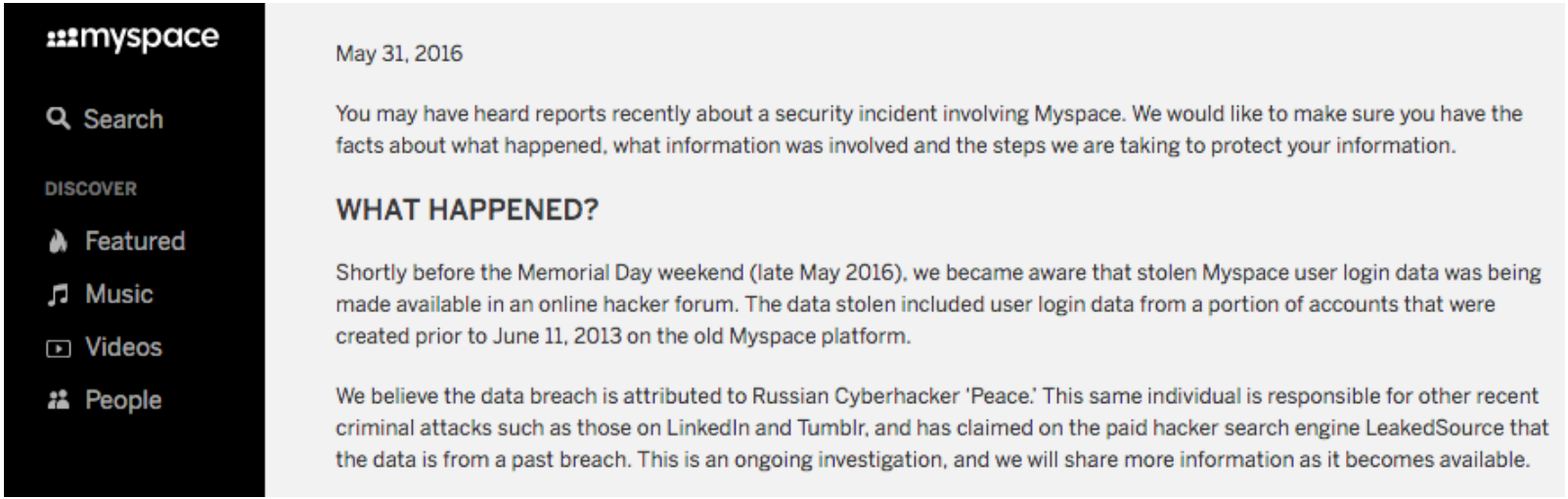
- Attackers creating homoglyph spelling of handles, name, and bio.
- Image analysis can identify identical or photoshopped images

// Impersonations – entice followers and connections

- @<mentions> of targets
- #hashtags common to targets
- Keywords targets use
- Follow targets
- Further campaign

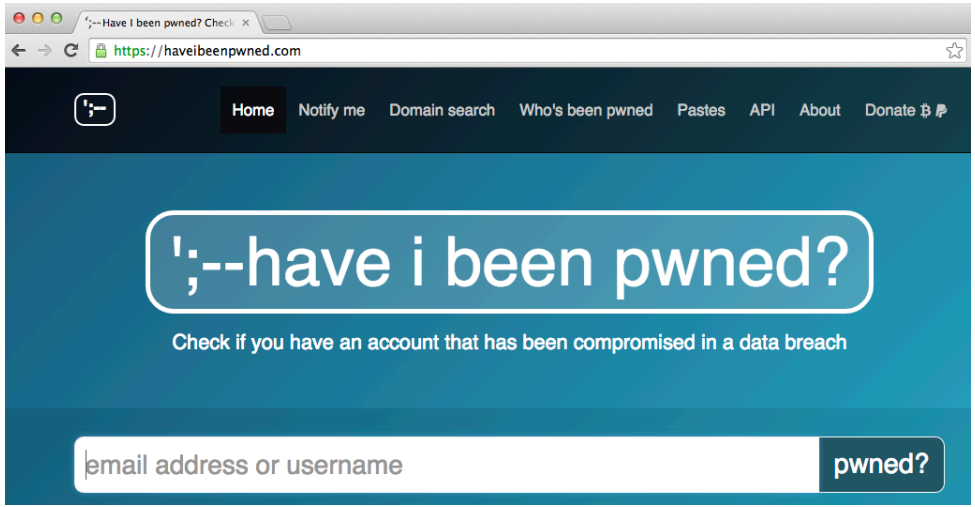
// Hijacking – How?

- Reuse of exposed passwords on other social networks



// Hijacking – How?

- Other sources of possible passwords on Social Web (Pastebin, Troy)



// Attack Methods - TTPs

- **Establishing trust** is fundamental
- Without connections, followers, or friends; the attack surface is limited
- **Connected targets increases the success of an attack** and compromise
- Social Media automates **shortened URLs**
- While a benefit to social media in general, it also allows attackers to **obfuscate** malicious and phishing URLs.

// Attack Methods – URL Shorteners

- **Shortened URLs come in many forms:**

Company	Legitimate Shortened URL
Bitly	bit<dot>ly
Google	goo<dot>gl
Hootsuite	ow<dot>ly
TinyURL.com	tinyurl<dot>com
Tiny.cc	tiny<dot>cc

- **Many (but not all) do not check for bad URLs**

// Attack Methods – Obfuscated Malicious URL

ALERT DETAILS

Retweets: 2

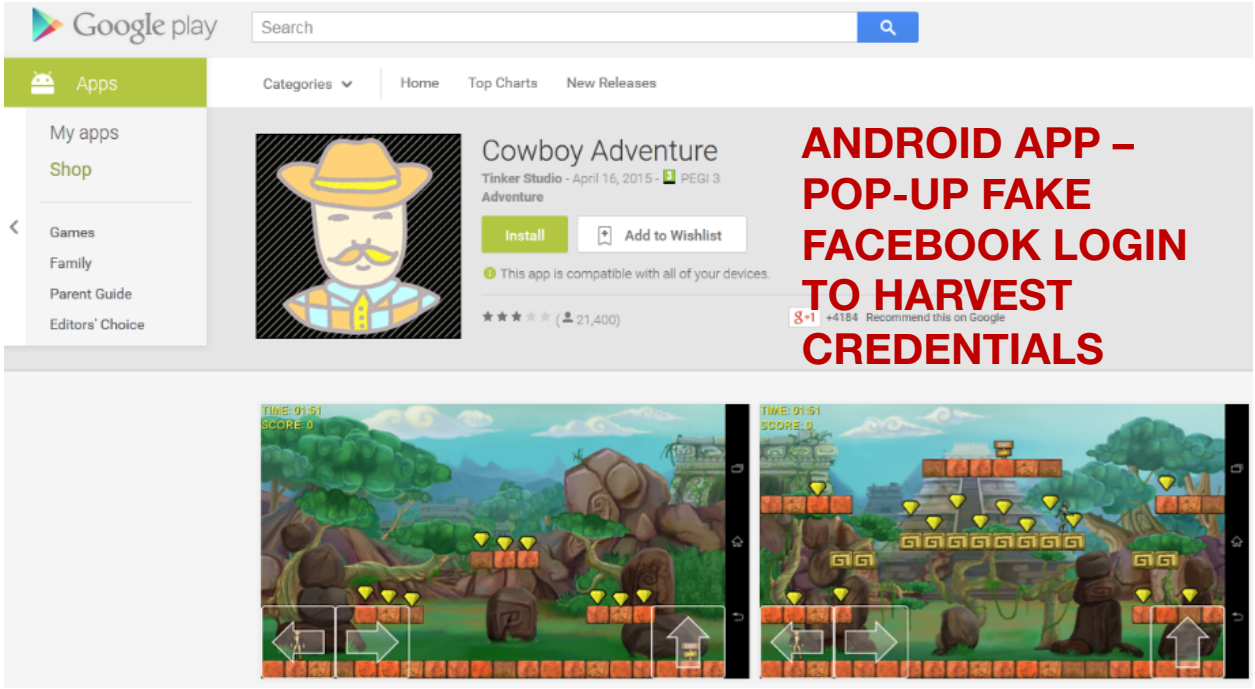
RT @fondieuropei20: #**PMI** #innovazione Macchinari ed emozioni, la rivoluzione umana di Techshop - La Stampa http://bit.ly/1XEN5li

Destination URL: http://3488fns.com/c/d?i=4lIZaBKQyam

» View Offending Content Source

// Attack Methods – Malicious URLs

- **Malware**
- **Phishing Link**
- **Malicious Browser Plug-in**
- **Bad App**



http://fossbytes.com/cowboy-adventure-game-malware-affecting-1-million-android/

// SCAMS, SCAMS & MORE SCAMS

"SPONSORED" SCAMS
Scammers pay Instagram to feature their content to more people

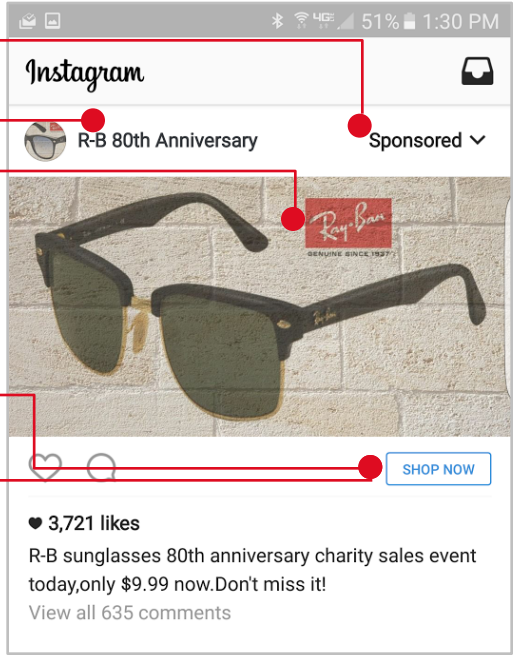
TRADEMARKED IMAGE
Copyrighted content repurposed for malicious activity

BRAND IMPERSONATION
Company name and logo abused to make the scam appear legitimate

CUSTOMER SCAM
Scam post designed to compromise customer credentials and damage brand

PHISHING LINK
Malicious link redirects to a phishing page intended to harvest credentials

COUNTERFEIT GOODS
Fake good being sold online undermines an organization's bottom line

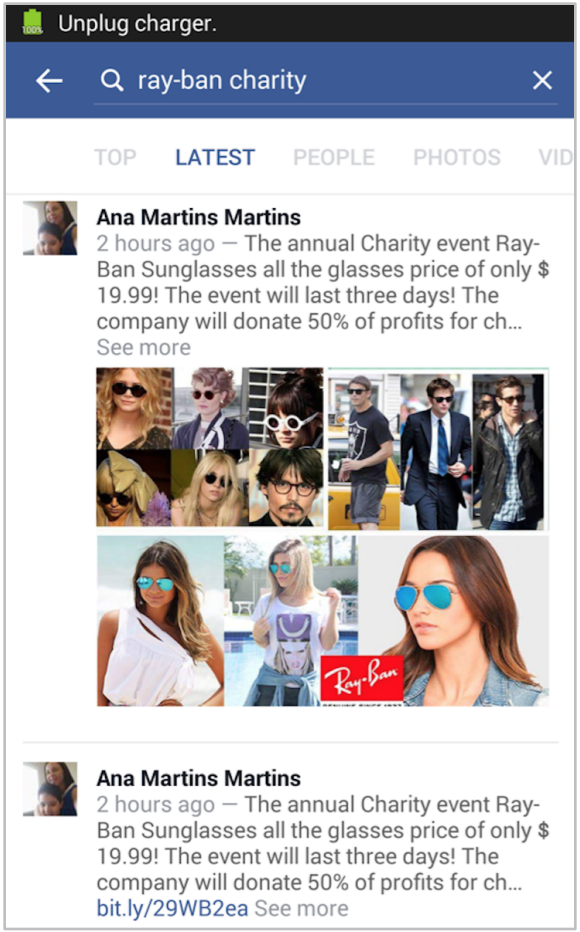


// RAY-BAN SUNGLASSES

PHISHING & FRAUD CONTINUE…

CRITICAL ISSUE

- What: Fake Ray-Ban Charity Events scams and account hijacking
- When: still active… seen activity since at least 2014
- How: Fake event offering sunglasses up to 90% off, fools users into purchasing sunglasses through malicious link, also hijacks Facebook account to send event out to more people



// RAY-BAN SUNGLASSES

PHISHING & FRAUD CONTINUE...

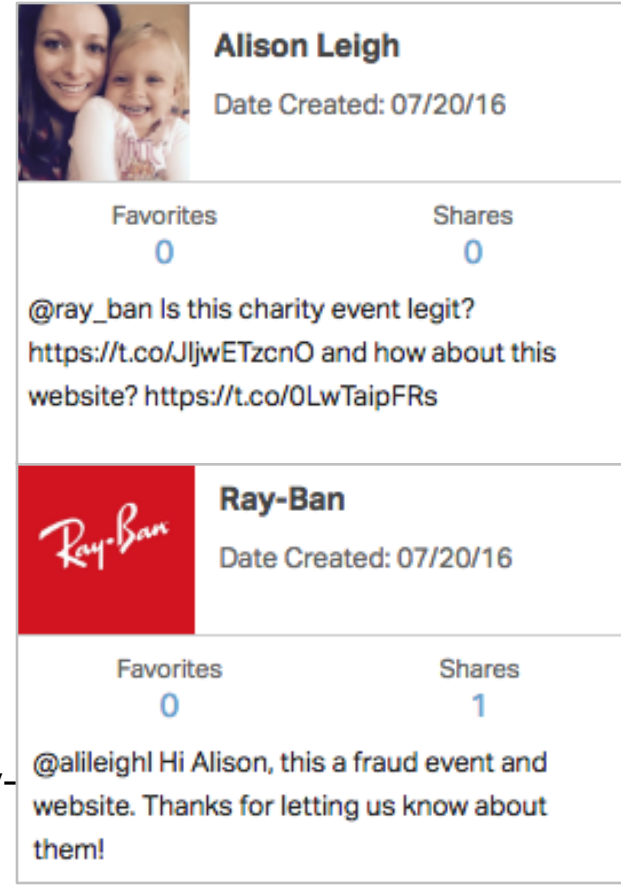

```
                "display_url": "facebook.com/R%D0%B0%D1%83-\u2026",
                "expanded_url": "https://www.facebook.com/R%D0%B0%D1%83-
B%D0%B0n-summer-charitable-eventsAll-colors-for-2499-1248946518484005/",
                "indices": [
                    38,
                    61
                ],
                "url": "https://t.co/JljwETzcn0"
            },
            {
                "display_url": "rbvim.com/ray-ban-rb4161\u2026",
                "expanded_url": "http://www.rbvim.com/ray-ban-rb4161-sun
glasses-havana-crystal-frame-brown-polarized-l-p-242.html",
```

// RAY-BAN SUNGLASSES

PHISHING & FRAUD CONTINUE…

RECOMMENDATIONS

- Avoid clicking unidentified Events on Facebook
- Change password immediately if a victim
- Update blacklists on perimeter and endpoint security with *known bad domains*
  - www.<rbvim>.com
  - Many more listed on site below: http://www.welivesecurity.com/2016/04/06/buying-ray-bans-dont-fall-for-this-facebook-scam/



// FACEBOOK

MALWARE CLICK FRAUD…

CRITICAL ISSUE

- What: Facebook malware targets Windows PCs running Chrome browser
- When: July 19, 2016
- How: User Likes a friend's Liked item, prompts "Verify Age" and install of a malicious Verify Content Age Chrome extension in Chrome store. Downloads a malicious payload, directs user to a malicious page that steals their Facebook (access) tokens

Source: http://www.scmagazine.com/chrome-browser-extensions-discovered-engaging-in-facebook-click-fraud/article/510843/

// FACEBOOK
MALWARE CLICK FRAUD…

RECOMMENDATIONS

- Google has removed the Chrome extension from their store, and removed from the ~132,000 impacted user's Chrome browsers
- Remove other unnecessary extensions

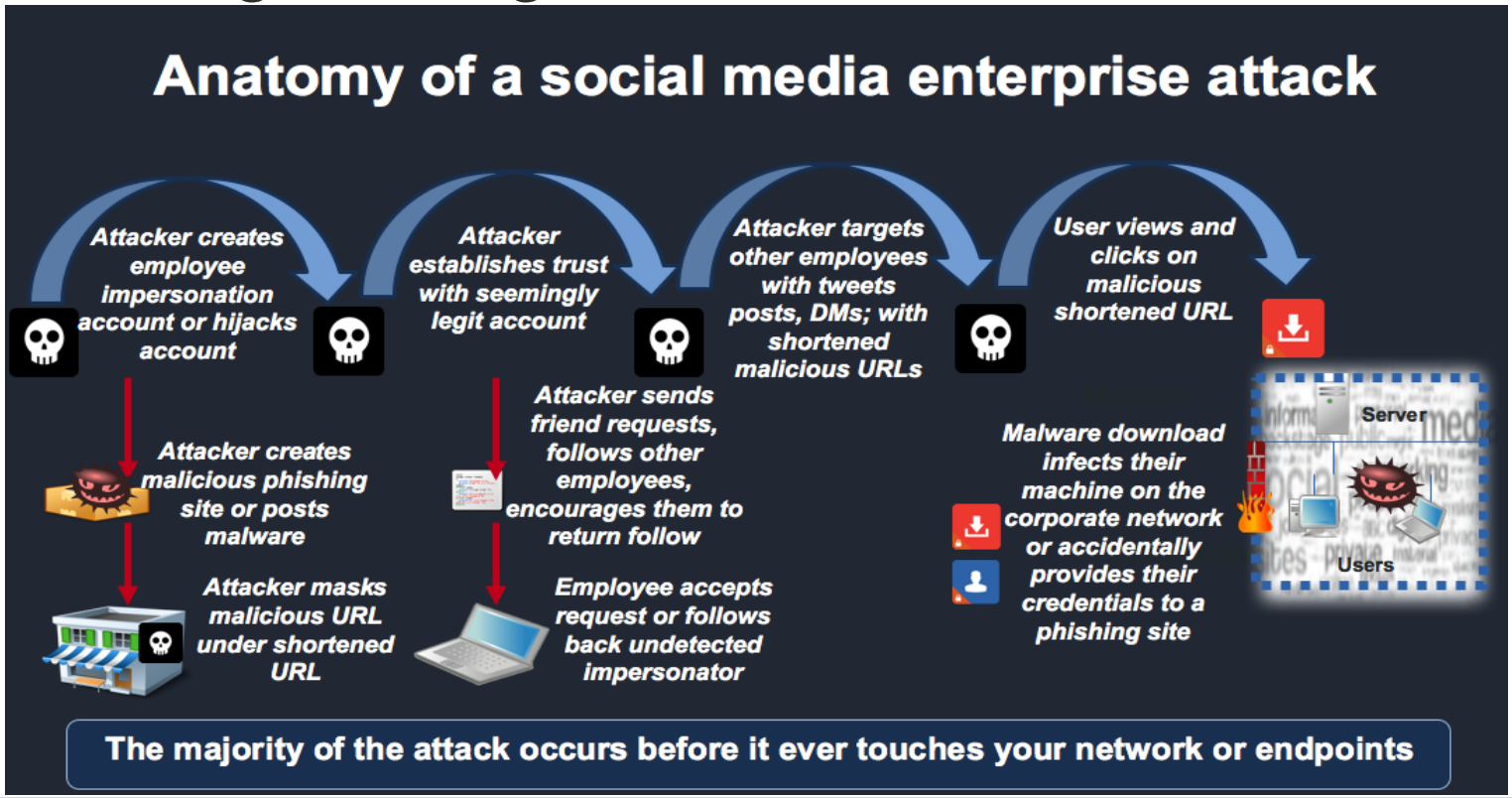
// FACEBOOK MESSENGER *MALWARE…*

CRITICAL ISSUE

- What: Malware bot targeting Facebook Messenger
- When: July 7, 2016
- How: User receives a message from a Friend, clicks on link and infects machine (Windows PC with Chrome) with a trojan and hijacks victim's Facebook account and spreads it to other users.

Source: http://www.digitaltrends.com/computing/facebook-messenger-virus-malware-windows-chrome/

// Putting it all together…



// Countermeasures – Fortifying your Social Media

- Identify your organization's social media footprint (companies, accounts, and key individuals)
- Monitor for impersonation accounts, and, when malicious, arrange for takedown.
- Enable two-factor authentication for social media accounts to deter hijacking
- Enhance security intel by feeding social media context, such as malicious and phishing URLs, into perimeter (firewalls, IDS, MPS, or proxy), endpoint security solutions, and SIEM
- Augment your incident response plan and process to encompass social media and include a takedown process.

// Q&A

Thank you