

Mike Rago, ZeroFOX

Attacks on Enterprise Social Media

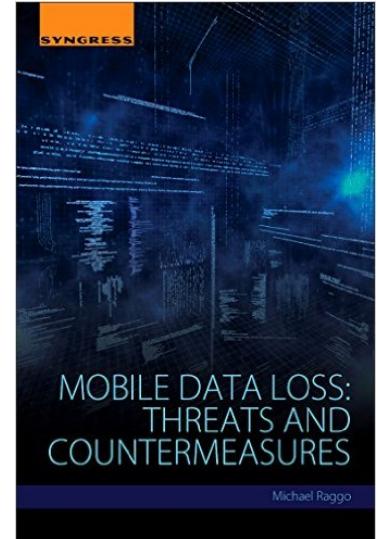
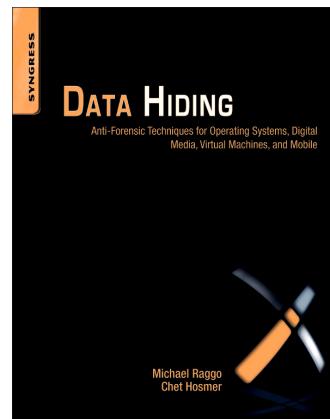
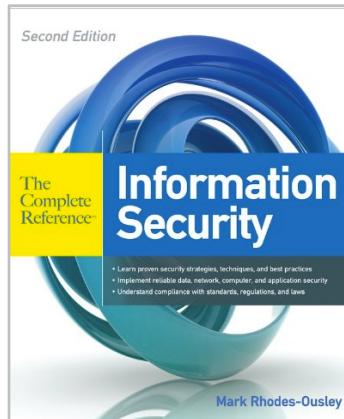
// OUR AGENDA

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

#whoami

Mike Rago (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)



**Book signing
3:30 today**

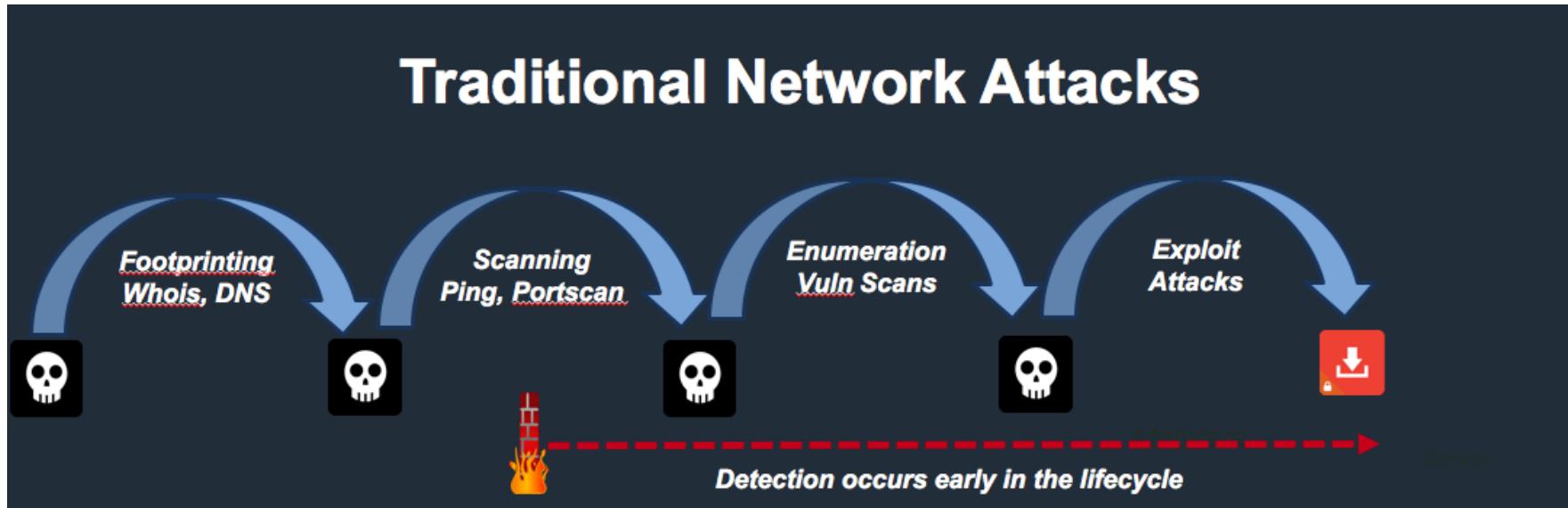
// Social Media Threat Landscape

- **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...

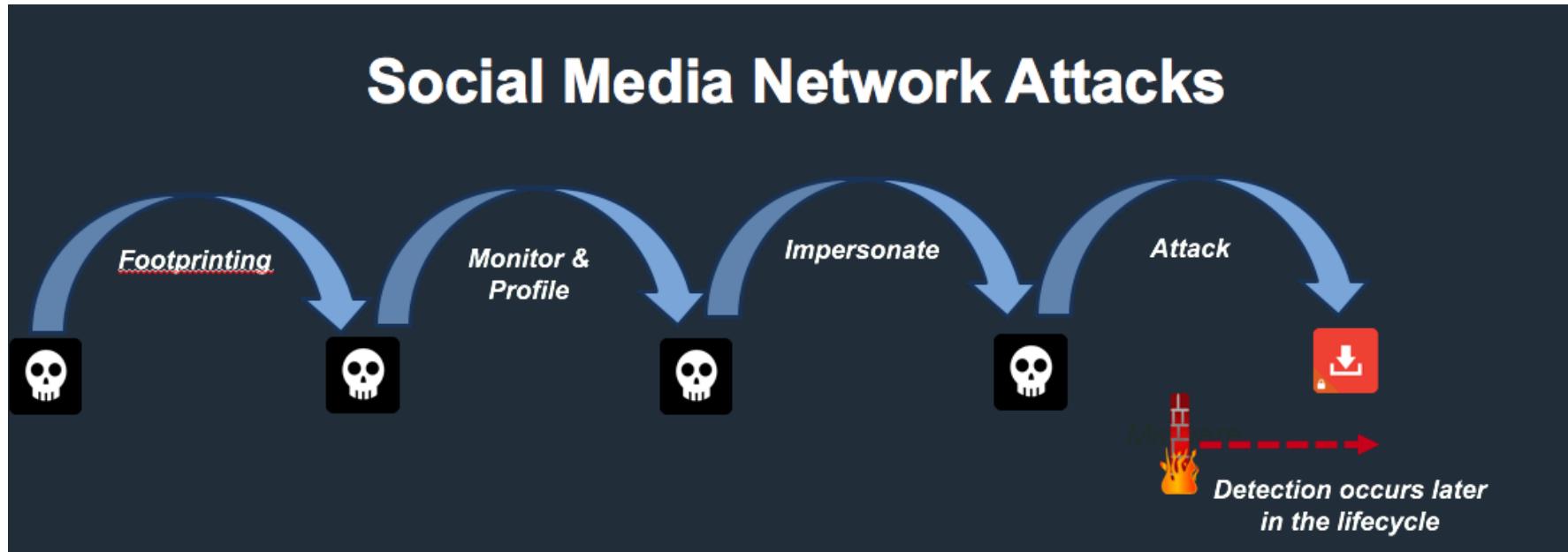
// Social media attack targeting corporate network



// Traditional Network Attacks vs. Social Media Attacks



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



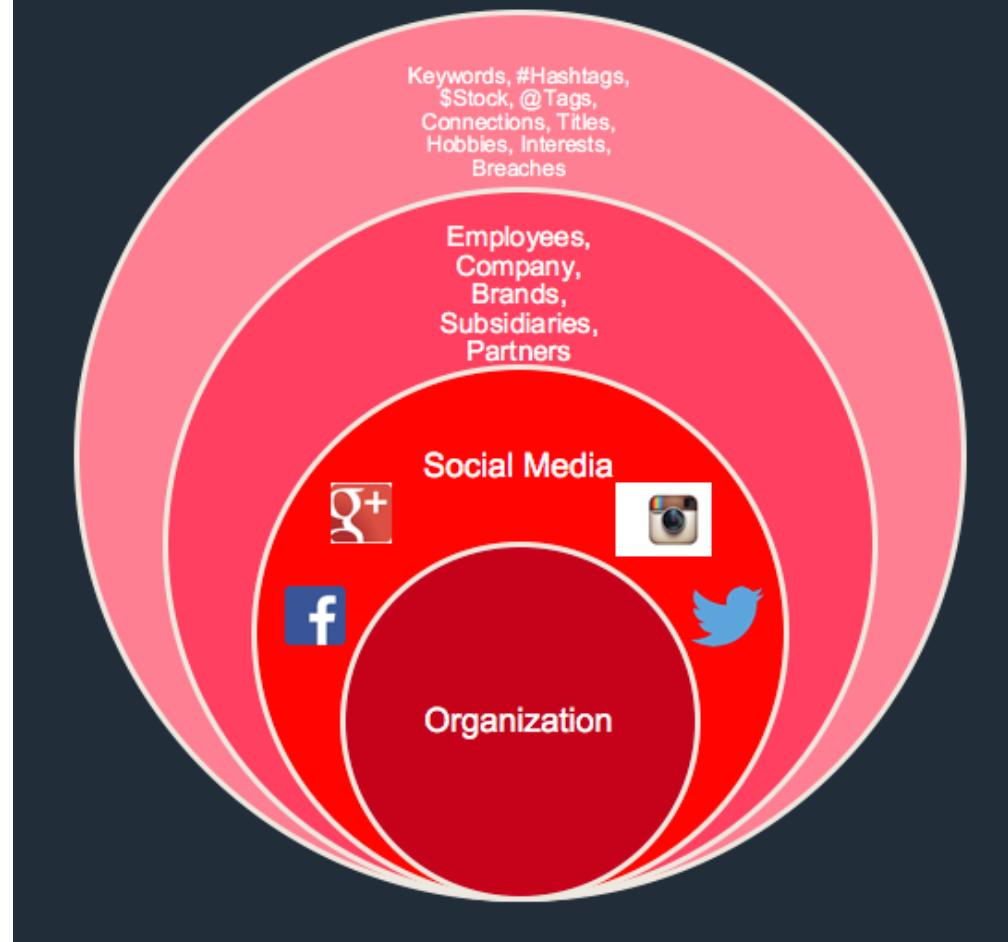
Build a network of "trust"!!!

// 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



ZENPRISE

FOLLOWING 1 FOLLOWERS 2

[Follow](#)

Zenprise   @Zenprise_Inc

Zenprise is now part of Citrix. You can follow us at [@XenMobile](#)

 Joined February 2013

@Zenprise_Inc's Only confirmed followers. Click the "Follow" button

 **Sudheesh Nair** 

RT [@pvdwerken](#): Today enjoying my last working day at [#Zenprise](#) (now part of [#Citrix](#)). Has been a truly great ride. Starting [@nutanix](#)...

RETWEET 1 

3:25 AM - 15 May 2013

1 0

// 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

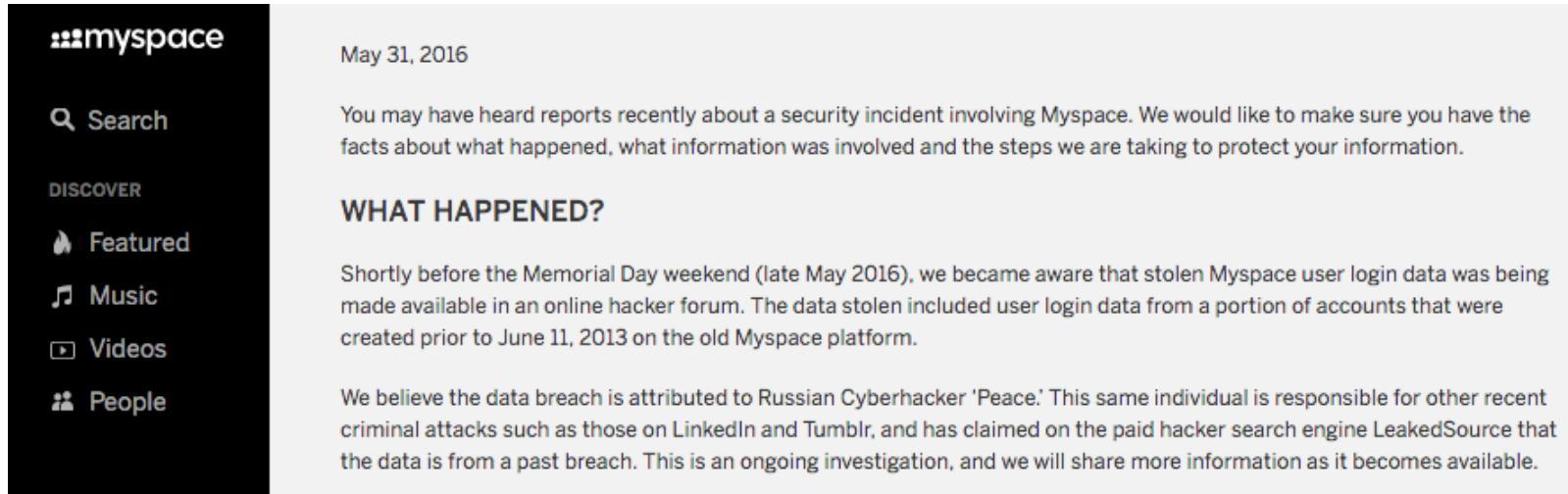
- @<mentions> of targets
- #hashtags common to targets
- Keywords targets use
- Follow targets
- Further campaign

The screenshot shows a Twitter search results page for the query '@WarrenBuffett'. At the top is a profile card for 'Warren Buffet' (@WarrenBuffett), which includes a photo of him, 0 tweets, 1 following, 40 followers, and a 'Follow' button. Below the profile card are five tweets from users who have impersonated Warren Buffett:

- A Reader** (@A_Reader_FT) - 4 Nov 2015: 'Buffett's @WarrenBuffett BNSF railway helped lead fight to delay US train safety technology for years reut.rs/1Nra7Ys via @Reuters'
- veracarvalho** (@vhcarvalho) - 30 Jul 2015: 'Eu amaria sentar para um longo papo com @WarrenBuffett'
- Venilton Leal** (@venilton_leal) - 20 Jul 2015: '@WarrenBuffett hello sir good evening, we can talk please? I live in Brazil. I am musician. Thanks.'
- White Feather** (@amiraclestory) - 18 Feb 2014: '@WarrenBuffett Its me.Sister Shirley Lopez.The Beatles,'
- marcialarsonpeiffer** (@marcialarson) - 13 Dec 2013: '"Honesty is an expensive gift. Do not expect it from cheap people" - @WarrenBuffett'

// Hijacking – How?

- Reuse of exposed passwords on other social networks



The screenshot shows a news article from Myspace. The left sidebar has a black background with white icons and text: 'myspace' logo, 'Search', 'DISCOVER', 'Featured', 'Music', 'Videos', and 'People'. The main content area has a white background. At the top, it says 'May 31, 2016'. The article starts with: 'You may have heard reports recently about a security incident involving Myspace. We would like to make sure you have the facts about what happened, what information was involved and the steps we are taking to protect your information.' Below this is a section titled 'WHAT HAPPENED?'. It continues: 'Shortly before the Memorial Day weekend (late May 2016), we became aware that stolen Myspace user login data was being made available in an online hacker forum. The data stolen included user login data from a portion of accounts that were created prior to June 11, 2013 on the old Myspace platform.' At the bottom, it says: 'We believe the data breach is attributed to Russian Cyberhacker 'Peace.' This same individual is responsible for other recent criminal attacks such as those on LinkedIn and Tumblr, and has claimed on the paid hacker search engine LeakedSource that the data is from a past breach. This is an ongoing investigation, and we will share more information as it becomes available.'

// Hijacking – How?

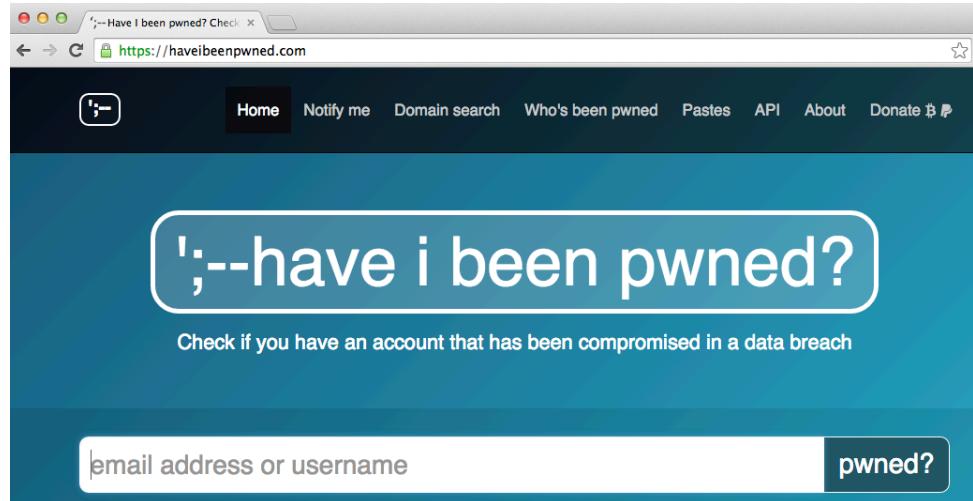
- Other sources of possible passwords on Social Web (Pastebin, Troy)

<https://twitter.com/#!/passfile>

Guest posted to Pastebin
06/14/12 16:46

Please use pastebin/paste2 for the hashes... dont want a flood of single hashes....i will, sr y... ;-)
user & password

878f1 [REDACTED]
aa3a2abae:I8love



The screenshot shows a web browser window with the URL <https://haveibeenpwned.com>. The page has a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Pastes, API, About, and Donate. Below the header is a large white button with the text ':--have i been pwned?'. Underneath the button, the text 'Check if you have an account that has been compromised in a data breach' is displayed. At the bottom is a search bar with the placeholder 'email address or username' and a blue button labeled 'pwned?'.

// 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

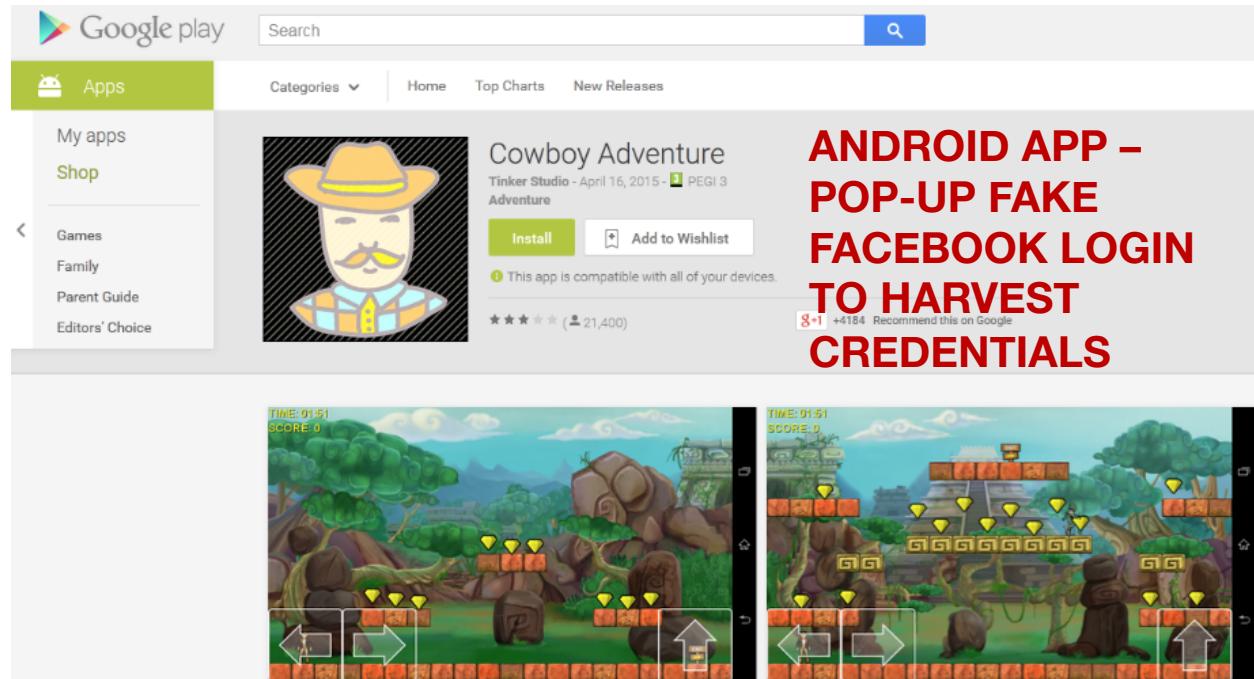
di Techshop - La Stampa <http://bit.ly/1XEN5li>

Destination URL: <http://3488fn.com/c/d?i=4lIZaBKQyam>

[» View Offending Content Source](#)

// Attack Methods – Malicious URLs

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



// 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

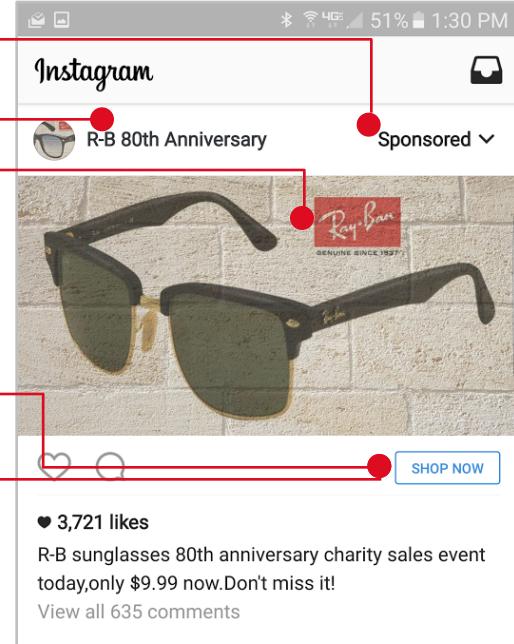
Scam post designed to compromise customer credentials and damage brand

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

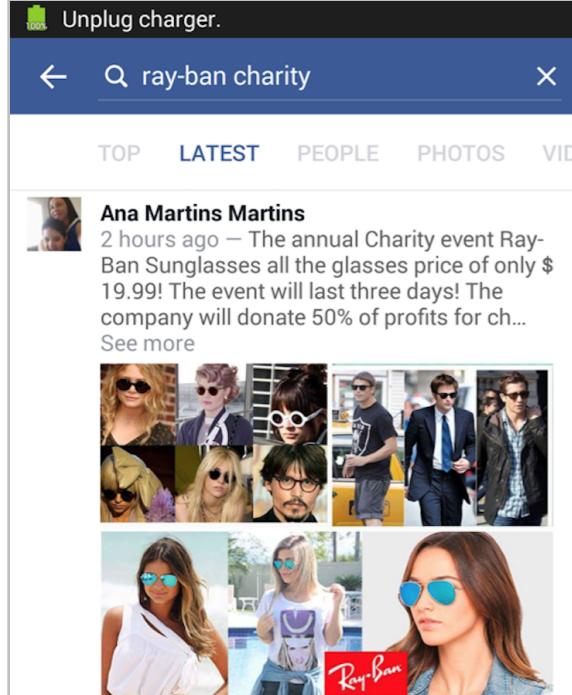


// RAY-BAN SUNGLASSES

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



Unplug charger.

← Q ray-ban charity ×

TOP LATEST PEOPLE PHOTOS VID

Ana Martins Martins
2 hours ago — The annual Charity event Ray-Ban Sunglasses all the glasses price of only \$19.99! The event will last three days! The company will donate 50% of profits for ch... See more



Ana Martins Martins
2 hours ago — The annual Charity event Ray-Ban Sunglasses all the glasses price of only \$19.99! The event will last three days! The company will donate 50% of profits for ch... bit.ly/29WB2ea See more

// 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-sur-
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/>



Alison Leigh

Date Created: 07/20/16

Favorites

0

Shares

0

@ray_ban Is this charity event legit?

<https://t.co/JljwETzcnO> and how about this website? <https://t.co/0LwTaipFRs>



Ray-Ban

Date Created: 07/20/16

Favorites

0

Shares

1

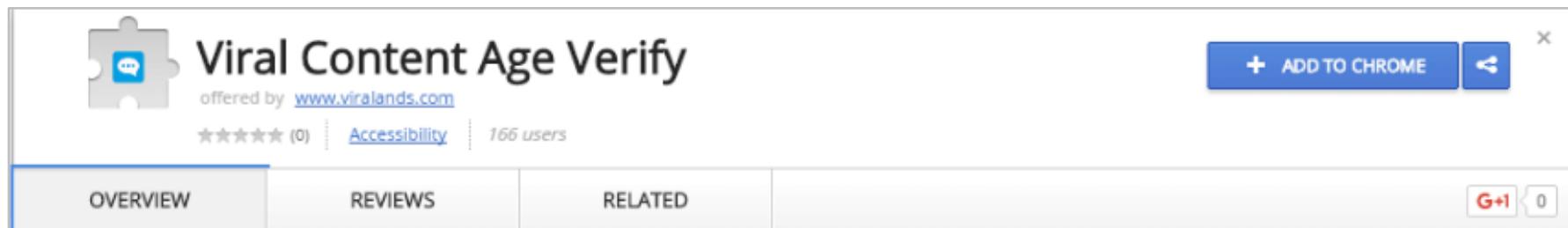
@alileigh Hi Alison, this a fraud event and website. Thanks for letting us know about them!

// 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

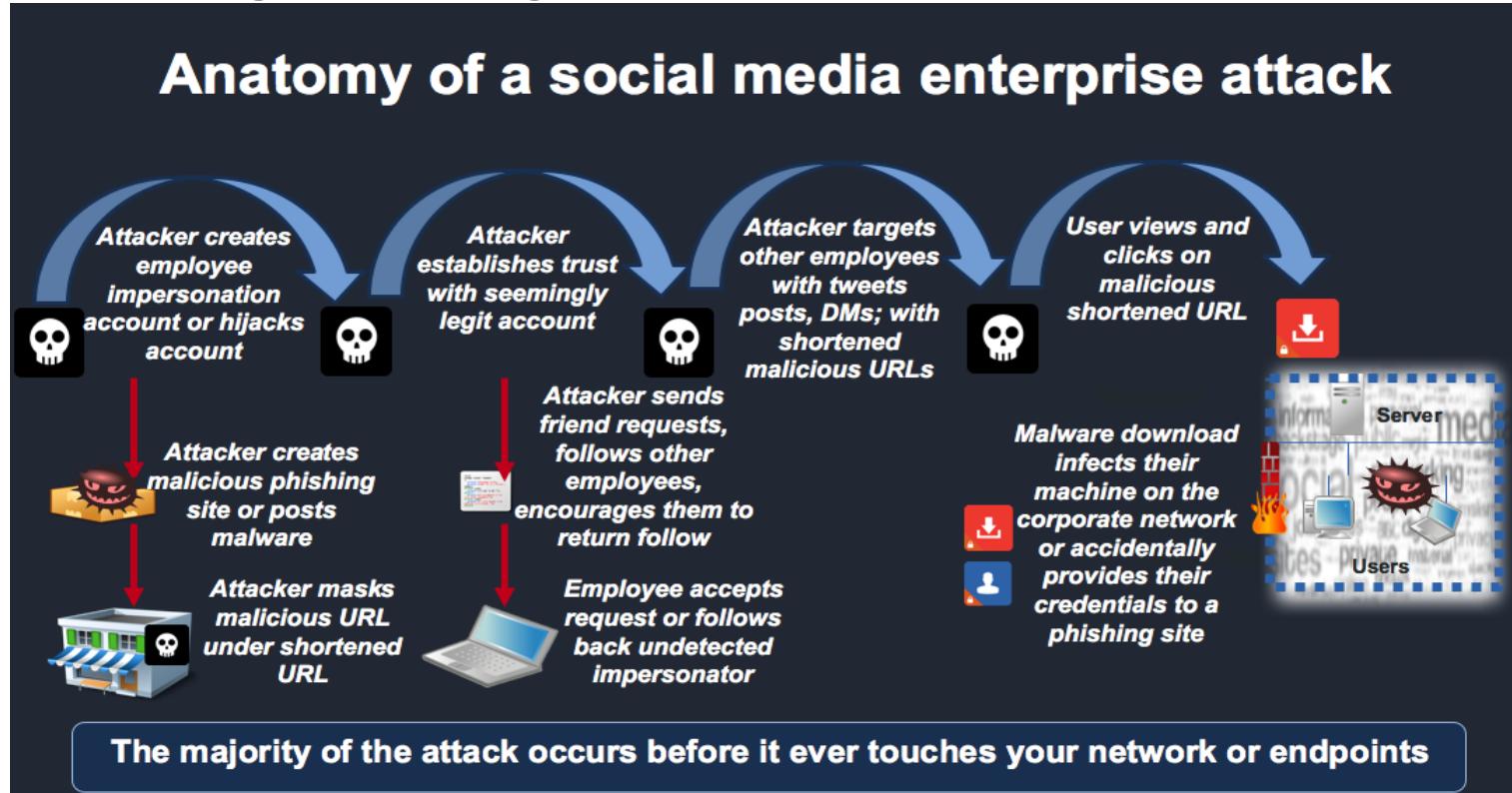
MALWARE...

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.

Thank you