Attacks on Enterprise Social Media

Mike Raggo, ZeroFOX
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)

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

Anatomy of a social media malicious link attack

1. Attacker creates employee impersonation account on Social Media
2. Attacker establishes trust with seemingly legit account
3. Attacker targets other employees with tweets posts, DMs; with shortened malicious URLs
4. User views and clicks on malicious shortened URL

Attacker creates malicious phishing site or posts malware
Attacker masks malicious URL under shortened URL
Attacker sends friend requests, follows other employees, encourages them to return follow
Employee accepts request or follows back undetected impersonator

Malware download infects their machine on the corporate network or accidentally provides their credentials to a phishing site

Server

Users

Malware
Traditional Network Attacks vs. Social Media Attacks

- Footprinting (Whois, DNS)
- Scanning (Ping, Portscan)
- Enumeration (Vuln Scans)
- Exploit Attacks

Detection occurs early in the lifecycle
Social Media Attacks – Build a network of “trust”!!!

Social Media Network Attacks

- Footprinting
- Monitor & Profile
- Impersonate
- Attack

Build a network of ”trust”!!!
## Footprint

<table>
<thead>
<tr>
<th>Platform</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn</td>
<td>company employees, titles, locations, email addresses, phone numbers, former employees</td>
</tr>
<tr>
<td>Twitter</td>
<td>bio, interests, other Twitter accounts they own, other brands/sub-brands, employees responsible for managing brand accounts, followers</td>
</tr>
<tr>
<td>Facebook</td>
<td>bio, birthday, interests, hobbies, connections</td>
</tr>
<tr>
<td>Google+</td>
<td>corporate ID or login, interests, hobbies, connections</td>
</tr>
</tbody>
</table>
// Monitor & Profile

- Social Media Accounts
- Dormant accounts
- Subsidiaries
- Responsible people for those accounts
- Partners
- Keywords
- #Hashtags
- @<mentions>
- $Stock
- Hobbies, interests
- Titles
RT @pvdwerken: Today enjoying my last working day at #Zenprise (now part of #Citrix). Has been a truly great ride. Starting @nutanix...
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

May 31, 2016

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.

WHAT HAPPENED?

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.

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)
// 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:

<table>
<thead>
<tr>
<th>Company</th>
<th>Legitimate Shortened URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitly</td>
<td>bit&lt;dot&gt;ly</td>
</tr>
<tr>
<td>Google</td>
<td>goo&lt;dot&gt;gl</td>
</tr>
<tr>
<td>Hootsuite</td>
<td>ow&lt;dot&gt;ly</td>
</tr>
<tr>
<td>TinyURL.com</td>
<td>tinyurl&lt;dot&gt;com</td>
</tr>
<tr>
<td>Tiny.cc</td>
<td>tiny&lt;dot&gt;cc</td>
</tr>
</tbody>
</table>

- 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=4llZaBKQyam

» View Offending Content Source
Attack Methods – Malicious URLs

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

[Image of Google Play Store with a fake app named Cowboy Adventure]

- ANDROID APP – POP-UP FAKE FACEBOOK LOGIN TO HARVEST CREDENTIALS

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...
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/
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 Age Chrome extension in Chrome store. Downloads a malicious payload, directs user to a malicious page that steals their Facebook (access) tokens

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.

Putting it all together…

Anatomy of a social media enterprise attack

1. Attacker creates employee impersonation account or hijacks account
2. Attacker establishes trust with seemingly legit account
3. Attacker targets other employees with tweets, posts, DMs; with shortened malicious URLs
4. User views and clicks on malicious shortened URL

- Malware download infects their machine on the corporate network or accidentally provides their credentials to a phishing site

The majority of the attack occurs before it ever touches your network or endpoints
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