SOCIAL MEDIA – FRIEND OR FOE?
A COMPOUNDING PROBLEM

Chipotle apologizes for racist tweets during Twitter hack

Facebook Scam Leads to Nuclear Explosion

U.S. military social media accounts apparently hacked by Islamic State sympathizers

LinkedIn-based intelligence gathering the security

Fake job recruit experts on LinkedIn

APT 29 use Twitter to control its Hammertoss data stealer

Malwarebytes Unpacked

Fake Twitter Verification Profile leads to Phishing, Credit Card Theft
A COMPOUNDING PROBLEM

CISCO FACEBOOK SCAMS ARE THE #1 WAY TO BREACH THE NETWORK

EMPLOYEES EXPERIENCE CYBERCRIME ON SOCIAL MEDIA MORE THAN ANY OTHER BUSINESS PLATFORM

OF ALL SOCIAL USERS
92% REPORT RECEIVING SPAM
54% REPORT RECEIVING PHISHING LINKS
23% REPORT RECEIVING MALWARE
1 IN 5 HAVE BEEN HACKED

BARRACUDA

TREND MICRO

NEW YORK POST

160,000 FACEBOOK ACCOUNTS BREACHED EVERY DAY

KASPERSKY LAB

YEARLY COST OF SOCIAL MEDIA PHISHING $1.2 BILLION

INTELL SECURITY
<table>
<thead>
<tr>
<th>TARGET</th>
<th>WHY / IMPACT</th>
<th>TACTICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMPLOYEES</td>
<td>Humans are compromised in order to bypass security defenses and gain access to “protected” systems and sensitive data</td>
<td>HASHTAG HIJACKING</td>
</tr>
<tr>
<td>BUSINESS OPERATIONS</td>
<td>Sensitive, confidential &amp; protected information is published &amp; malicious actions coordinated to damage revenue generating activities &amp; biz trust</td>
<td>ACCOUNT TAKEOVER</td>
</tr>
<tr>
<td>CUSTOMERS</td>
<td>Customers are targeted through fraudulent impersonations of the org and key executives to steal customer data &amp; damage reputation</td>
<td></td>
</tr>
</tbody>
</table>
SOCIAL AS AN INVESTIGATION TOOL

• Use social to get “attribution”
  – Identify posts and other content containing the IP / URL in question
  – Trace back to suspected originating profile
  – Map connections to “attacker” profile
  – Who knows what you’ll find…

• Use social to identify patient zero & other potential infection points
  – Map and identify your organization’s social assets
  – Look for instances where the IP / URL is connected to your employees
  – Map employee connections to attacker & attacker connections
  – Who knows what you’ll find….
SOCIAL AS AN INVESTIGATION TOOL

• Adversary chatter
  – Look for chatter and communication across social networking platforms related to your organization
  – You might find cloaked planning dating back to before the “breach”
  – You might find talks about what was stolen or bragging about the “hack”
GET OUT IN FRONT!

- Identify threat indicators before it’s too late
  - Map your organization’s social footprint
  - Continuously scan posts and communications for targeted phishing & malware attacks
    - Remember, Facebook is #1 way to compromise the corporate network!
  - Integrate threat data into SIEM, perimeter and other security technologies for prevention, correlation and rapid response
- Monitor adversary chatter to get a jump on planned actions
  - Listen for communications that could provide insight
  - Coordination often happens in the open whether blatant or veiled, it’s there
  - Potentially uncover unknown breaches based on data
THE ZEROFOX TECHNOLOGY PLATFORM

DISCOVER & MONITOR

ANALYZE & CONTEXTUALIZE

PROFILE ANALYSIS ENGINE

LINK ANALYSIS ENGINE

CONTENT ANALYSIS ENGINE

PROTECT & INTEGRATE

ZEROFOX SECURITY ENFORCEMENT

ANALYTICS & EVENT MGMT
CONTEXT BREEDS CONFIDENCE

Driven by expert models, supervised machine learning and malware and phishing detection technology, the Security Analysis Engine identifies never before seen attacks and camouflaged threats.

THREAT DATA
- URL and Redirects
- IP Address
- DNS Info
- Geolocation
- Shellcode
- Obfuscation Techniques

SOCIAL CONTEXT
- Social Networks
- Shares
- Hashtags
- Attacker Profile
- Origin Post

SECURITY ANALYSIS
- Executable Analysis
- Username/Password Requests
- Malware File Hash
- Phishing Classification
- Malware Classification
- Spam Classification
SOCIAL PHISH TESTING... SCARY RESULTS

100% PHISHING SUCCESS

RECO
Discover your social media assets & quantify your social media vulnerabilities with a repeatable assessment & phishing simulation