



HACKING SOCIAL

*Driving Visibility to Support
Monitoring & Incident Response*

CSO – SOCIAL IS A TOP 5 CONCERN



SECURITY ADVISER

By [Roger A. Grimes](#), Columnist, CSO | AUG 21, 2017 4:32 AM PT

TODAY'S TOP STORIES

The 5 cyber attacks you're most likely to face

Don't be distracted by the exploit of the week. Invest your time and money defending against the threats you're apt to confront

CYBER ATTACK NO. 4: SOCIAL MEDIA THREATS

“Our online world is a social world led by Facebook, Twitter, LinkedIn or their country-popular counterparts. Social media threats usually arrive as a rogue friend or application install request...**Many of today's worst hacks started out as simple social media hacking.** Don't underestimate the potential.”

FORBES – TARGETED ATTACKS VIA SOCIAL



“The lovely and disarming ‘Mia Ash’ is a fictional female created by the highly-active hacker crew known as OilRig, which... SecureWorks believes is sponsored by the Iranian regime. In July 2016, Mia's puppeteers **targeted a Deloitte cybersecurity employee**, engaging him through [Facebook] in conversations about his job.”

CISCO – SOCIAL IS #1 SOURCE OF MALWARE



“Facebook is now the #1 source of malware...Unsurprisingly, ‘social media’ saw the largest jump from last year’s report on the list of top 24 concerns; **social is now ranked #3 overall**...Facebook malware is just one example of this dangerous new confluence.”

BUSINESS.COM – DON'T FORGET TO SECURE SOCIAL

Yes, Malware is Bad. But Your Biggest Security Threat May Come From Your Social Media Accounts.

BY JONATHAN FURMAN

Business.com / Security / Last Modified: September 13, 2017

SHARE THIS



“Businesses already know how important security and protection is in today’s digital world. However they often leave out social media not realizing **how porous [social media] can be when it comes to hacks and breaches.** There are several ways in which things can go wrong.”

IMPACT OF SOCIAL, DIGITAL & COLLABORATION

SOCIAL & DIGITAL IMPACT

83%

Global organization's use social
as key business platform

22.4%

of total enterprise marketing
budgets spent on social in next 4
years

\$1.2B

Annual targeted social phishing
cost to organizations

SOCIAL BUSINESSES

200 Million

Facebook Business Pages Alone!

61% More

than all ".coms" in the world

<1%

Currently have protection

COLLABORATION IMPACT

80%

of global businesses use
enterprise collaboration

97%

of collaboration users service
more clients

28%

Employees use collaboration for
data exfiltration

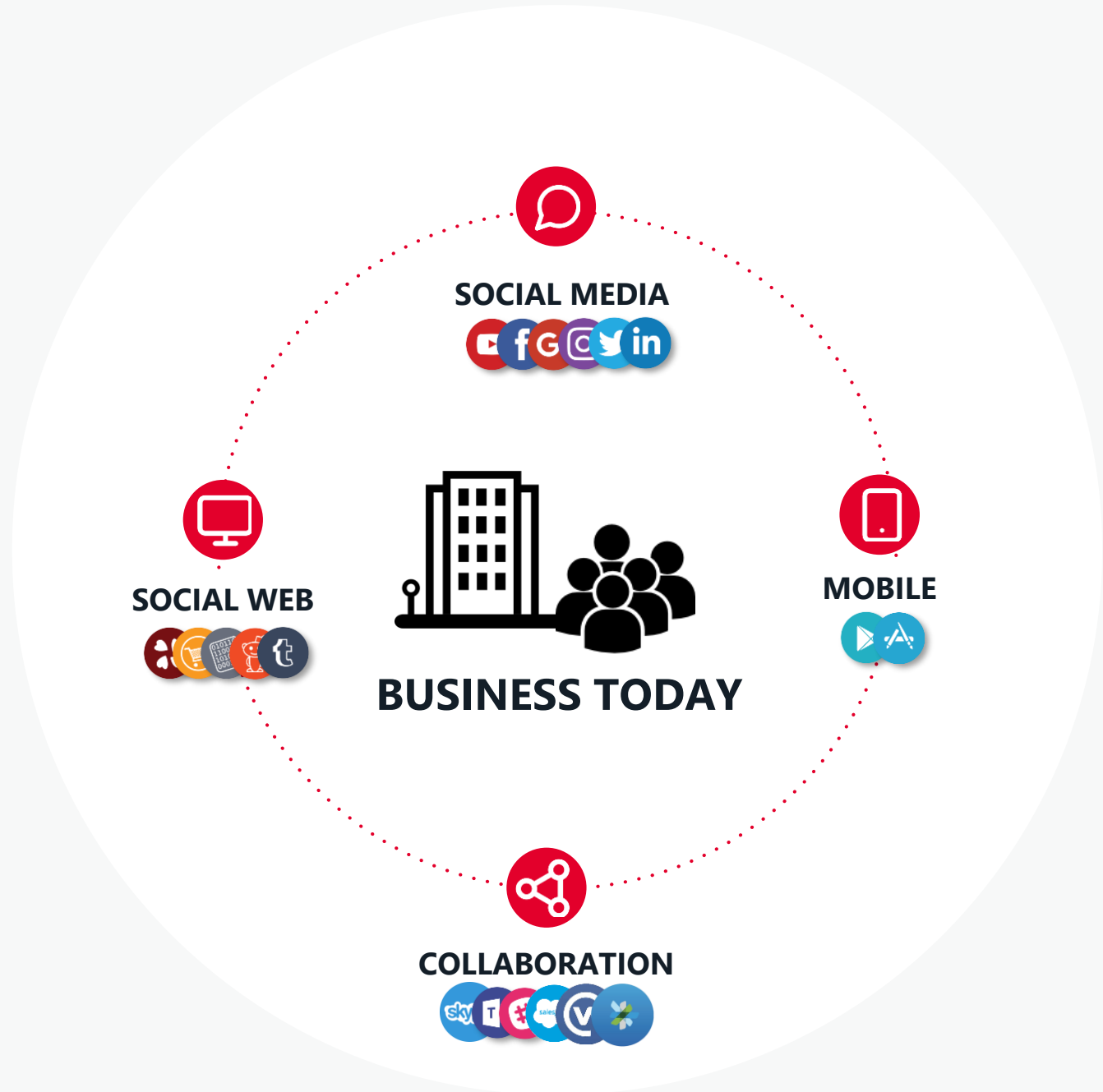
<12%

Organization's have visibility into
data activity

ASSET PROTECTION INSIDE THE FIREWALL



SOCIAL & DIGITAL - THE NEW RISK VECTORS



1. Social is Everywhere

- 1/3 people are on social globally
- 27% of all internet time is spent on social
- 50% of Americans make purchase decision w/ Facebook
- 83% of global org use social as a "key business platform"

2. Hacking is Easy

- Easy to use; create a profile in minutes
- Low cost
- Global scale; find any target globally or use at scale
- Build "trusted relationships"
- End-to-end profiling & engagement platform

3. Limited Visibility

- Security Teams are not monitoring Social Media
- Social Media Teams are not trained to look for security threats
- 43% of Security professionals listed social media as a top concern

WHAT WE KNOW

1

More walled gardens, harder attribution

2

Business & personal blur, defense gets distributed

3

AI hits social

3 TRENDS



How Twitter Bots Are Shaping the Election

Between the first two presidential debates, a third of pro-Trump tweets and nearly a fifth of pro-Clinton tweets came from automated accounts.

DOUGLAS GUILBEAULT AND SAMUEL WOOLLEY | NOV 1, 2016 | TECHNOLOGY

POPULAR

QUARTZ

Twitter admits that as many as 23 million of its active users are automated

TACTIC #1: ACCOUNT HIJACKING

NEW YORK POST

1.8 Facebook accounts
hacked every second;
600,000 every day

HARRIS POLL

2 in 3 social media users
have had their accounts
hijacked



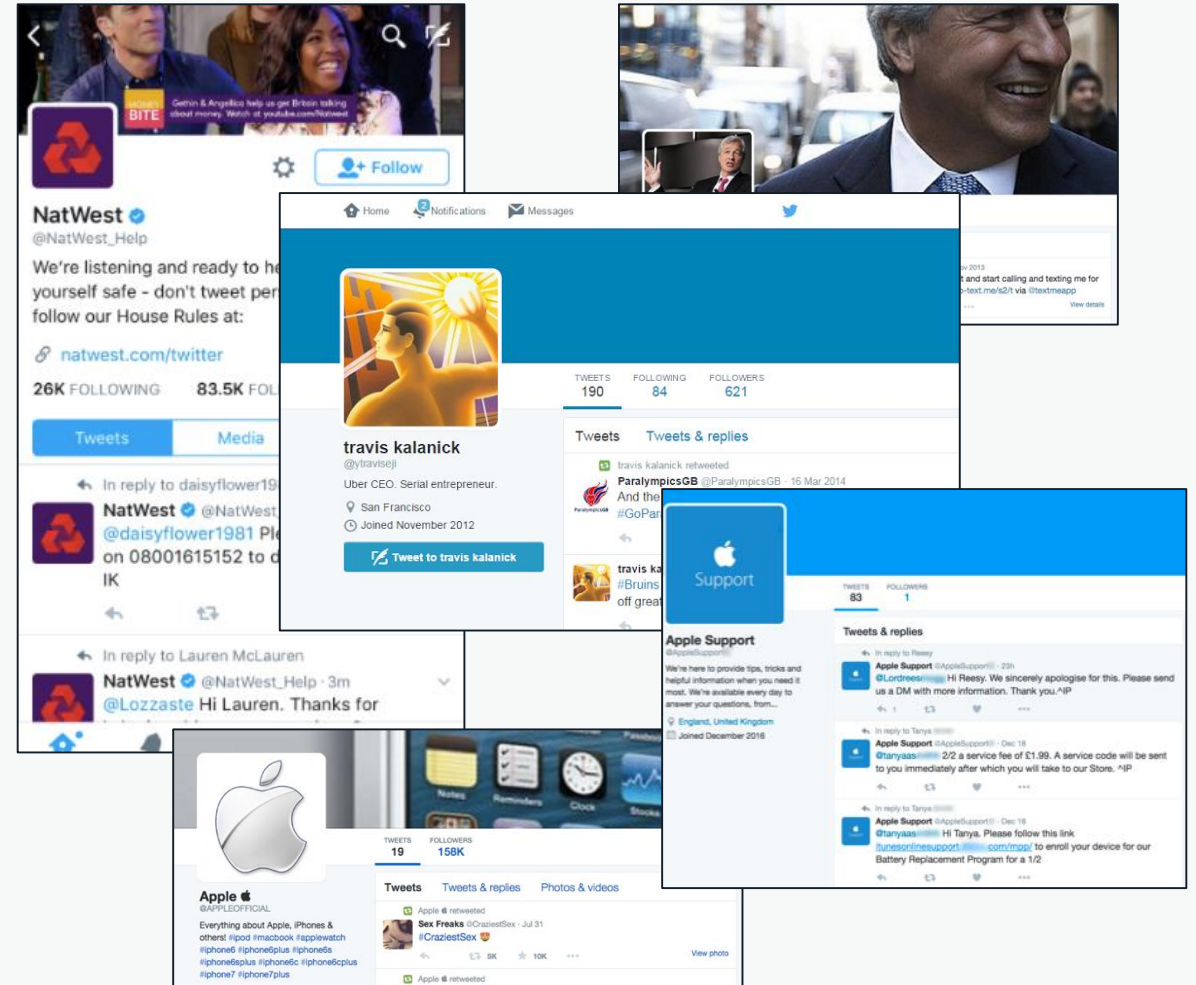
ZEROFOX

Instances of fraudulent accounts increased 11x in the past 24 months

ZEROFOX

38% of brand impersonations drive users to phishing pages

TACTIC #2: FRAUDULENT ACCOUNTS



TACTIC #3: SOCIAL PHISHING & MALWARE

KASPERSKY

7.57 million victims of social phishing annually

CISCO

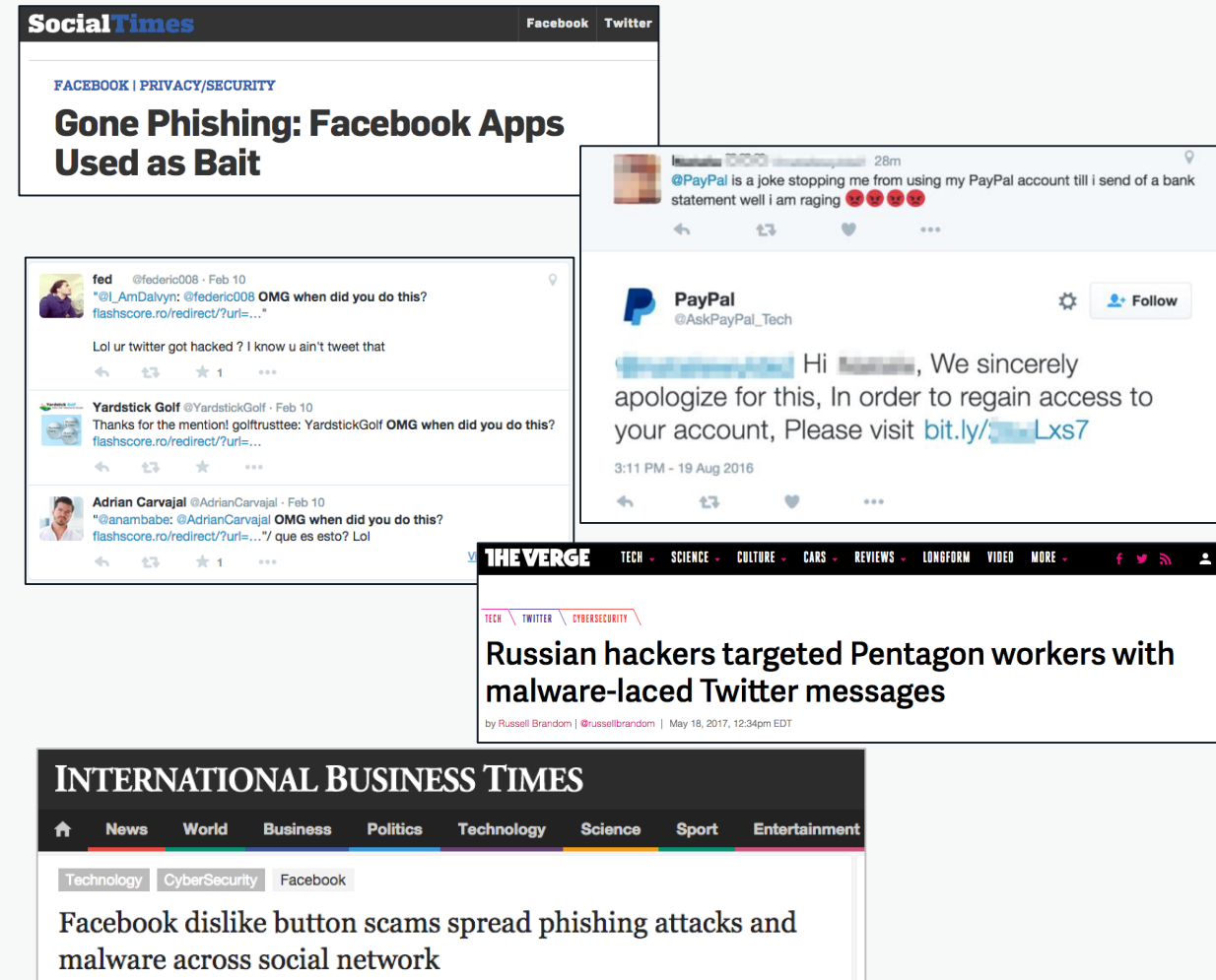
Facebook is the most common delivery mechanism for malware; *the #1 way to breach the network*

RSA

Global cost of social media phishing is \$1.2 billion

PONEMON

\$3.2 million to remediate web based malware



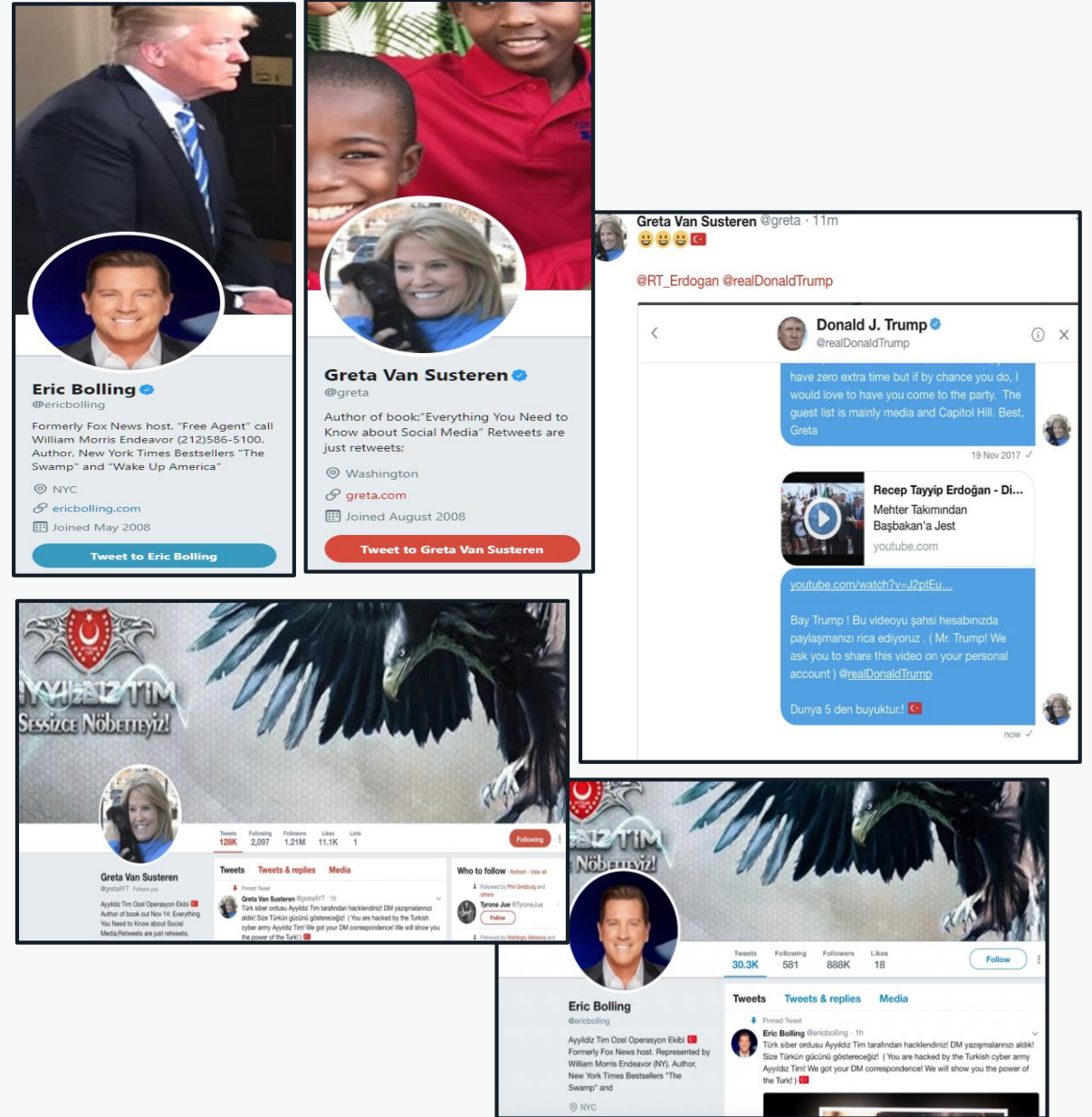
CISCO

Facebook is the most common delivery mechanism for malware; the #1 way to breach the network

FBI

Social Media complaints on the rise, up to 92/day (32k/year)

TACTIC #4: DIRECT MESSAGE SCAMS & FRAUD



Eric Bolling @ericbolling
Formerly Fox News host. "Free Agent" call William Morris Endeavor (212)586-5100. Author, New York Times Bestsellers "The Swamp" and "Wake Up America"

Greta Van Susteren @greta
Author of book: "Everything You Need to Know about Social Media" Retweets are just retweets:

Donald J. Trump @realDonaldTrump
have zero extra time but if by chance you do, I would love to have you come to the party. The guest list is mainly media and Capitol Hill. Best, Greta

Recep Tayyip Erdoğan - Di... Mehter Takımından Başbakan'a Jest youtube.com

Bay Trump ! Bu videoyu şahsi hesabınızda paylaşmanızı rica ediyoruz. (Mr. Trump! We ask you to share this video on your personal account) @realDonaldTrump
Dunya 5 den buyuktur!

Eric Bolling @ericbolling
Aylık Tim Ozel Operasyon Ekibi
Türk siber ordusu Aylık Tim tarafından hacklendi! DM yazmalarını istedik! Size Türkün gücünü göstereceğiz! (You are hacked by the Turkish cyber army Aylık Tim. We will show you the power of the Turk!)

IMPACT

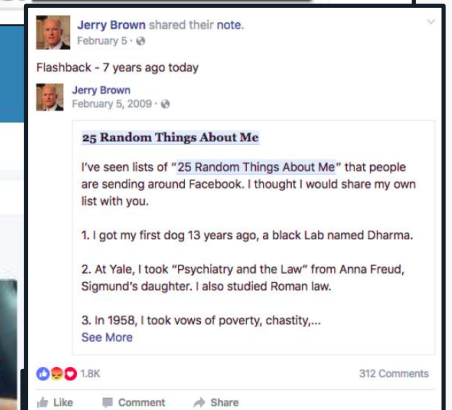
- Bruteforce Password Attacks
- Social Engineering Attacks
- Physical Theft
- Brand Damage
- Competitive Intelligence
- Social Account Compromise
- Network Compromise

INFOWATCH

Over 1500 data leaks occur every year and 72.8% are from insiders

E & Y

The average cost per record lost is \$214, data breach is > \$7M



TACTIC #5: ACCIDENTAL INFORMATION LEAKAGE

TACTIC #6: PHYSICAL SECURITY

AIG
40,000 kidnap and ransom cases involving business travelers are reported annually

US STATE DEPT
70% of overseas kidnappings of US citizens goes unreported.



WHAT'S IMPORTANT TO YOU?



INFORMATION SECURITY

SPOOFED DOMAIN

TARGETED PHISHING & EXPLOIT

COMPROMISED CREDENTIALS

INSIDER, DLP & COMPLIANCE



BRAND RISKS

BRAND PROTECTION

REPUTATION DAMAGE

CUSTOMER ATTACKS

COUNTERFEIT & PIRACY



CORPORATE SECURITY

SITUATIONAL AWARENESS

EXECUTIVE PROTECTION

EVENTS & TRAVEL THREATS

LOCATION PROTECTION

LEGAL // HR // FINANCE // COMPLIANCE // RISK & FRAUD



THE ONLY COMPLETE
SOCIAL MEDIA AND DIGITAL PROTECTION PLATFORM BUILT FOR ENTERPRISES



PROTECT

Corporate Social Media
Assets & Brands



SAFEGUARD

Business & Customer
Engagement



SECURE

Employees & the Business
from Cyber & Physical
Threats



FOR SECURITY

- Reduce **operational** costs
- Reduce time to **identify** a threat
- Reduce time to investigate and **clean up** an issue
- Increase the **breadth** of your defense-in-depth program

THE VALUE

#1

Targeted social media malware is the #1 method for breaching an enterprise network

40%

40% of enterprises have fallen victim to social media spearphishing attacks

20%

1 in 5 businesses have been infected with malware sent via social media

TARGETED DATA COLLECTION

- SOCIAL MEDIA**
 - Open Networks (Facebook, Google+, Instagram, LinkedIn, Reddit, Tumblr, Twitter, YouTube)
 - Closed Networks (Discord, Facebook, Messenger)
 - Collaboration Networks (Slack, Trello)
- DEEP/DARK/WEB**
 - TLD Registrations (.com, .co.uk, .org, .net, .biz, .uk)
 - Bin & Dump Sites (Gh0stbin)
 - Custom Sites
- MOBILE STORES**
- NEWS/BLOGS/FORUMS**
- END USER ACCOUNTS**
 - Open/Closed Social
 - Breach Notifications

API



INTELLIGENT ANALYSIS

Artificial Intelligence Classifiers

Out-of-the-box Rulesets

FoxThreats



API



CUSTOM RULES & POLICIES



REMEDiation & INTEGRATIONS



AUTOMATED REMEDIATION
Automatically remove malicious content and profiles from the social networks directly



SECURITY INTEGRATION
Integrate threat indicators into existing security tools, empowering existing defense against digital attacks



MANAGED SERVICES
Expert digital risk analysts provide 24x7x365 coverage



ZEROFOX

HOW IT WORKS



DEFINE WHAT'S IMPORTANT



CREATE A POLICY



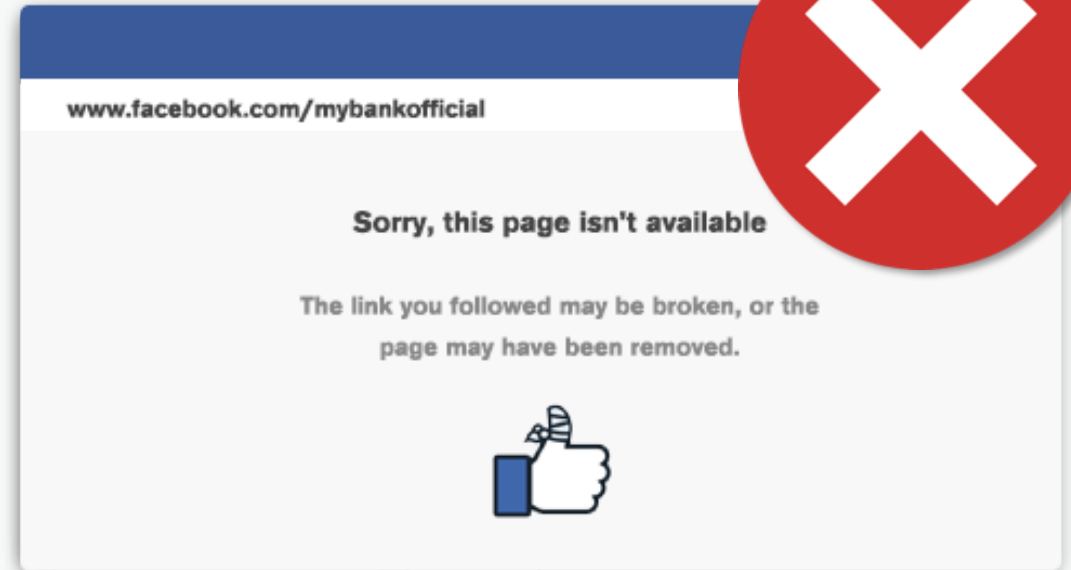
MONITOR SOCIAL CHANNELS



ALERT ON RISKS



REMEDiate MALICIOUS CONTENT



THE INDUSTRY'S ONLY COMPREHENSIVE COLLECTION OF SOCIAL MEDIA THREATS AND INDICATORS

- ZeroFOX's social media threat data and the ability to **correlate social media incidents**
- Enable your security team throughout different phases of an attack
 - Prevent
 - Detect
 - Respond
 - Recover

ZEROFOX THREAT FEED



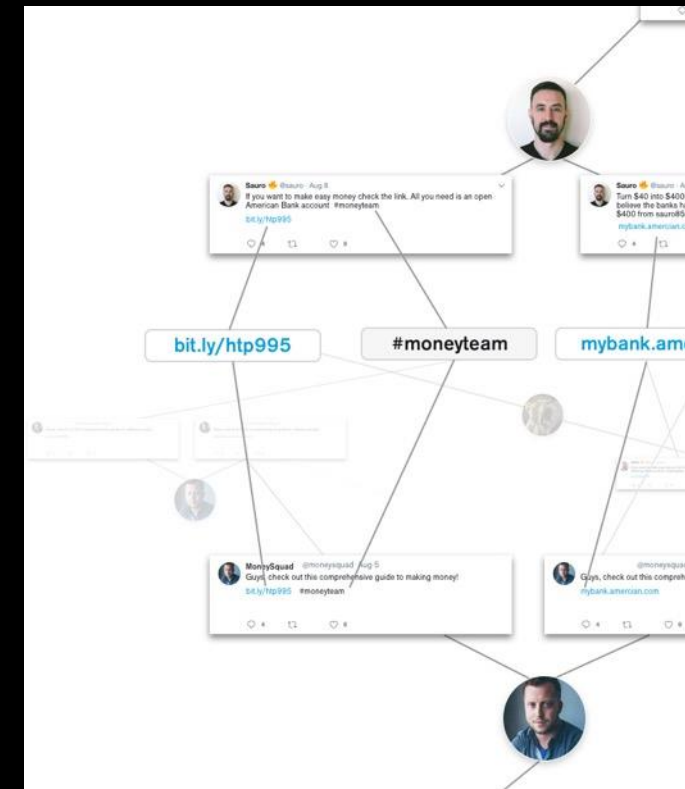
ANOMALI



MALTEGO



splunk >



Three Pillars of Protection



Visibility



Automation



Remediation





SOCIAL MEDIA SECURITY CHECKLIST

1. Identify Social Media Footprint
2. Obtain “**Verified Accounts**”
3. Enable **Two-Factor Authentication**
4. Monitor for **Spoofed & Impersonating Accounts**
5. **Identify Scams**, Fraud, Money-flipping, and More by Monitoring Your Corporate and Brand Social Media Pages
6. Monitor for signs of Social Media **Account Hijacking**
7. **Train Employees** on Social Media Hygiene
8. **Incorporate Strategy** for Social Media & Digital Threat Detection



THANK YOU

www.zerofox.com