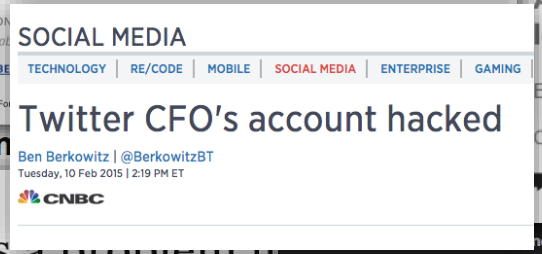
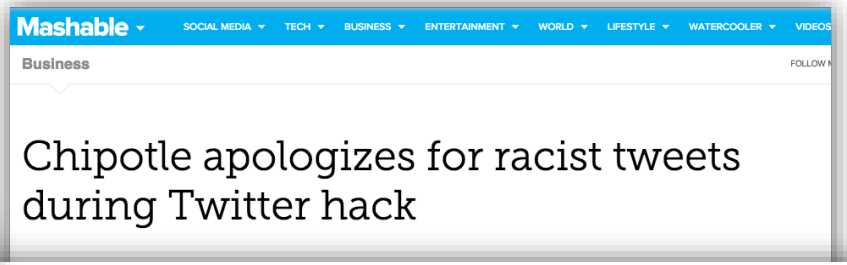
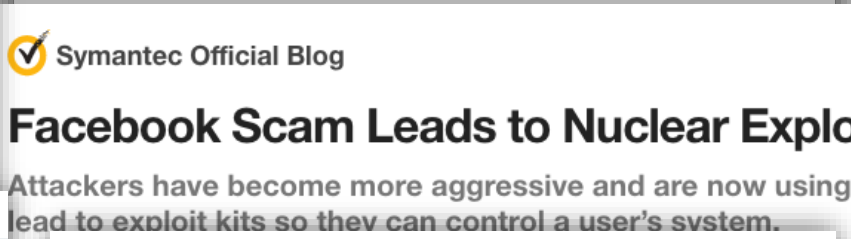
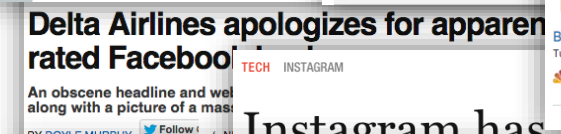
SOCIAL MEDIA – FRIEND OR FOE?

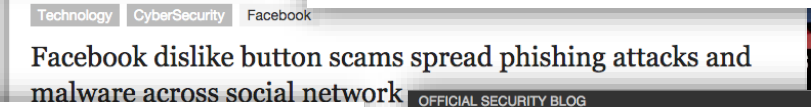
A COMPOUNDING PROBLEM

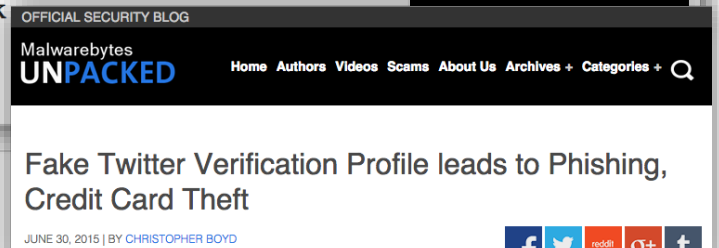












A COMPOUNDING PROBLEM

CISCO™

FACEBOOK SCAMS ARE THE #1 WAY TO BREACH THE NETWORK

intel Security

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

Barracuda

OF ALL SOCIAL USERS

92% REPORT RECEIVING SPAM

54% REPORT RECEIVING PHISHING LINKS

23% REPORT RECEIVING MALWARE

1 IN 5 HAVE BEEN HACKED

TREND MICRO™

29 MILLION TWEETS EVERY DAY ARE MALICIOUS

NEW YORK POST | 160,000 facebook ACCOUNTS BREACHED EVERY DAY

KASPERSKY lab | RSA SECURITY | YEARLY COST OF SOCIAL MEDIA PHISHING $1.2 BILLION

TARGET	WHY / IMPACT	TACTICS
EMPLOYEES	Humans are compromised in order to bypass security defenses and gain access to “protected” systems and sensitive data	HASHTAG HIJACKING ACCOUNT TAKEOVER IMPERSONATIONS ATTACK PLANNING SOCIAL PHISHING SOCIAL ENGINEERING INFORMATION LEAKAGE
BUSINESS OPERATIONS	Sensitive, confidential & protected information is published & malicious actions coordinated to damage revenue generating activities & biz trust	
CUSTOMERS	Customers are targeted through fraudulent impersonations of the org and key executives to steal customer data & damage reputation	

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….

ZEROFOX

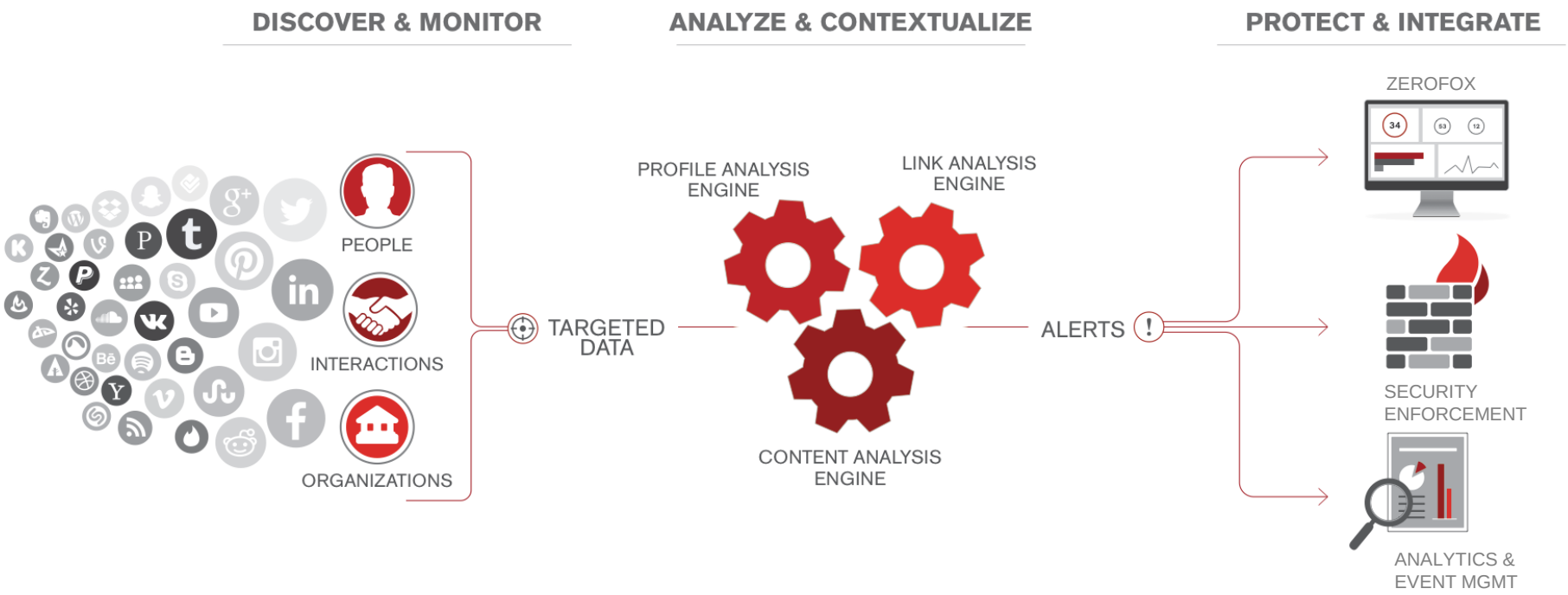
SOCIAL AS AN INVESTIGATION TOOL

- **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



ZEROFOX

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

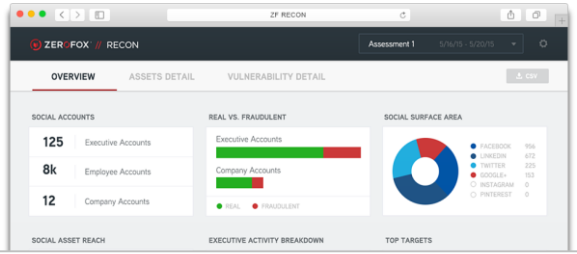
SOCIAL CONTEXT

- 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



RECON

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

100%

PHISHING SUCCESS

ZEROFOX

Evan Blair, Co-Founder, ZeroFOX
evan@zerofox.com | @evanlblair

ZEROFOX.COM

Talk to a solutions expert:
844.369.7259