
SOCIAL MEDIA – FRIEND OR FOE?



A COMPOUNDING PROBLEM

M SOCIAL MEDIA UNIVERSITY OF MICHIGAN

Menu

HACKED: A

August 18, 2015 Uncategorized

Forbes / Tech

5 Billionaire-Owned Energy Stocks With Triple Digit Potential

AUG 24, 2014 @ 10:49 PM 54,671 VIEWS

Hackers Ground Sony Executive's Flight With Bomb-Threat Tweet



Paul Tassi, CON
News and opinion at

FOLLOW ON FORBE
Opinions expressed by Fo

SOCIAL MEDIA

TECHNOLOGY | RE/CODE | MOBILE | SOCIAL MEDIA | ENTERPRISE | GAMING

Twitter CFO's account hacked

Ben Berkowitz | @BerkowitzBT
Tuesday, 10 Feb 2015 | 2:19 PM ET
CNBC

Mashable

SOCIAL MEDIA TECH BUSINESS ENTERTAINMENT WORLD LIFESTYLE WATERCOOLER VIDEOS

Business

Chipotle apologizes for racist tweets during Twitter hack



Symantec Official Blog

Facebook Scam Leads to Nuclear Explo

Attackers have become more aggressive and are now using lead to exploit kits so they can control a user's system.

Checkpoint

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

Delta Airlines apologizes for apparent Facebook

TECH INSTAGRAM
An obscene headline and well along with a picture of a mas
BY DOYLE MURPHY Follow

Instagram has a problem

Home / Security

LinkedIn-based intelligence gathering the security

APT 29 use Twitter to control its Hammertoss data stealer

July 31, 2015 By Pierluigi Paganini

G+1 10

f My Page Like 56

Technology CyberSecurity Facebook
Facebook dislike button scams spread phishing attacks and malware across social network

FLASH UPDATE, INFECTS 110K

OFFICIAL SECURITY BLOG

Malwarebytes UNPACKED

Home Authors Videos Scams About Us Archives + Categories +

Fake Twitter Verification Profile leads to Phishing, Credit Card Theft

JUNE 30, 2015 | BY CHRISTOPHER BOYD

f t reddit + f

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



29 MILLION
TWEETS
EVERY DAY
ARE MALICIOUS



160,000 facebook ACCOUNTS BREACHED EVERY DAY



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

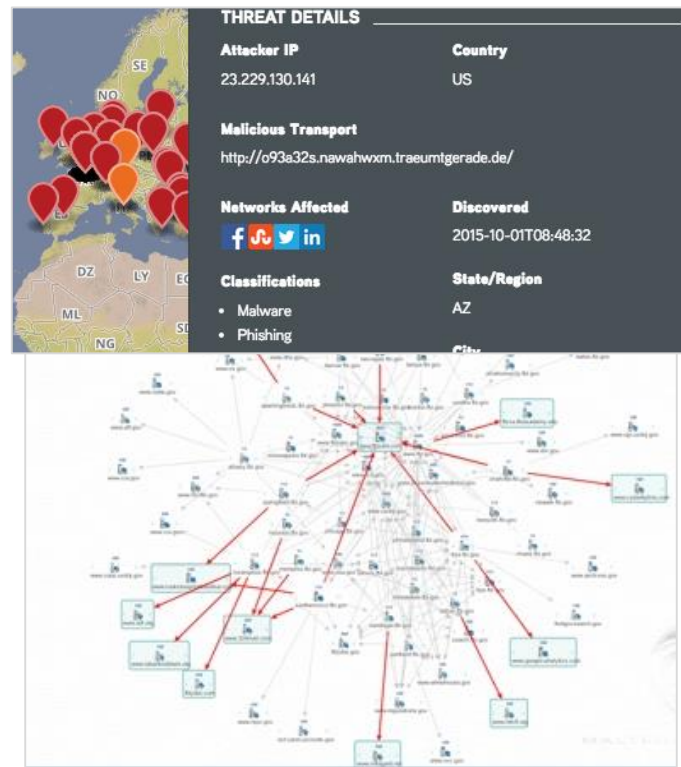
Sensitive, confidential & protected information is published & malicious actions coordinated to damage revenue generating activities & biz trust

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....



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

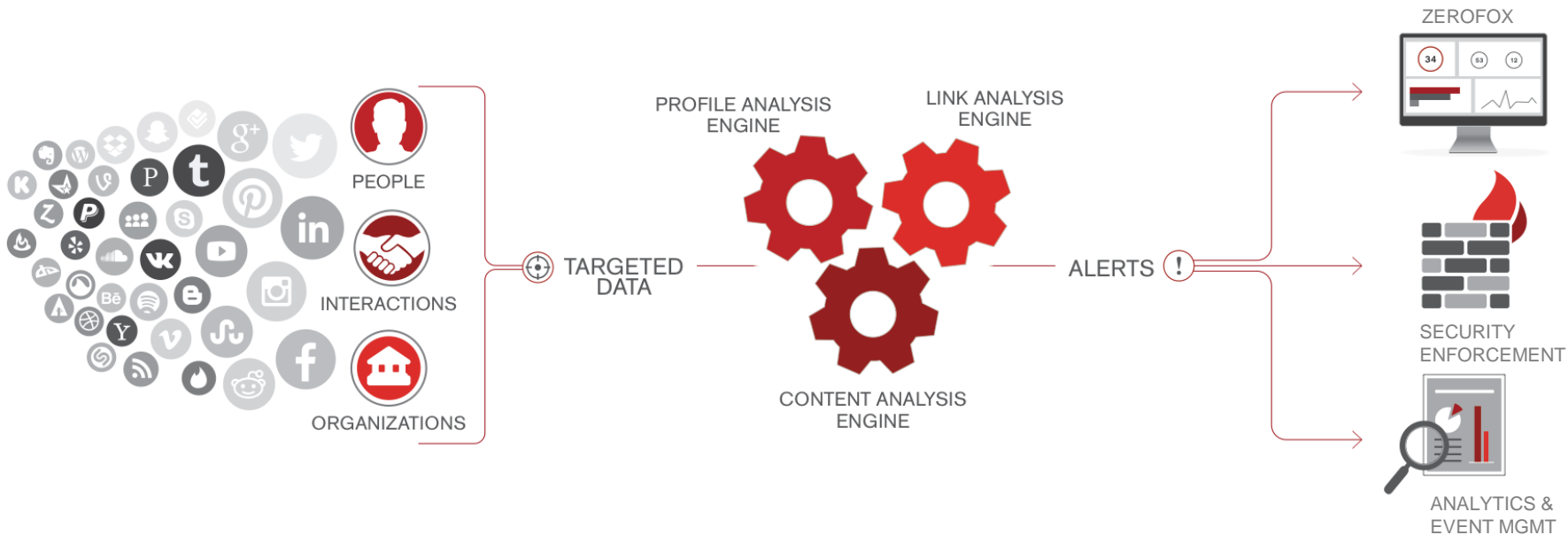


THE ZEROFOX TECHNOLOGY PLATFORM

DISCOVER & MONITOR

ANALYZE & CONTEXTUALIZE

PROTECT & INTEGRATE



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

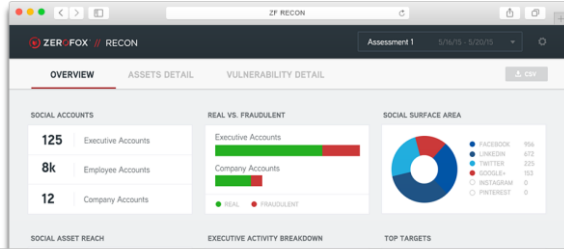
- Social Networks
- Shares
- Hashtags
- Attacker Profile
- Origin Post



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

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

ZEROFOX.COM

Talk to a solutions expert:
844.369.7259