Social Threats – Social Media as an Attack vector for Cyber Threats

Stewart Cawthray

General Manager, Enterprise Security Products & Solutions

February 10, 2017

#WHOAMI

- **General Manager Security Products – Rogers Enterprise**
- 15 Year **Security Veteran**
- **Industry Speaker** & Cybersecurity Evangelist
- Devoted Father & Field Hockey Coach

- Twitter: **@StewartCawthray**

#WhatWeDo

Rogers Security Services

Enterprise Cybersecurity Protection for Businesses of All Sizes

THE SOCIAL REVOLUTION

GLOBAL SCALE OF SOCIAL MEDIA

95%

US WORKING AGE ARE **ACTIVE** ON SOCIAL MEDIA

3/4

WORLDWIDE INTERNET USERS HAVE **ACTIVE** SOCIAL PROFILES

IMPACT ON DAILY LIVES

27%

INTERNET TIME SPENT
ON SOCIAL MEDIA

3 HOURS

EVERY **DAY** SPENT ON
SOCIAL MEDIA

IMPACT ON ECONOMY

50%

OF AMERICAN'S LEVERAGE **FACEBOOK** FOR PURCHASE DECISIONS

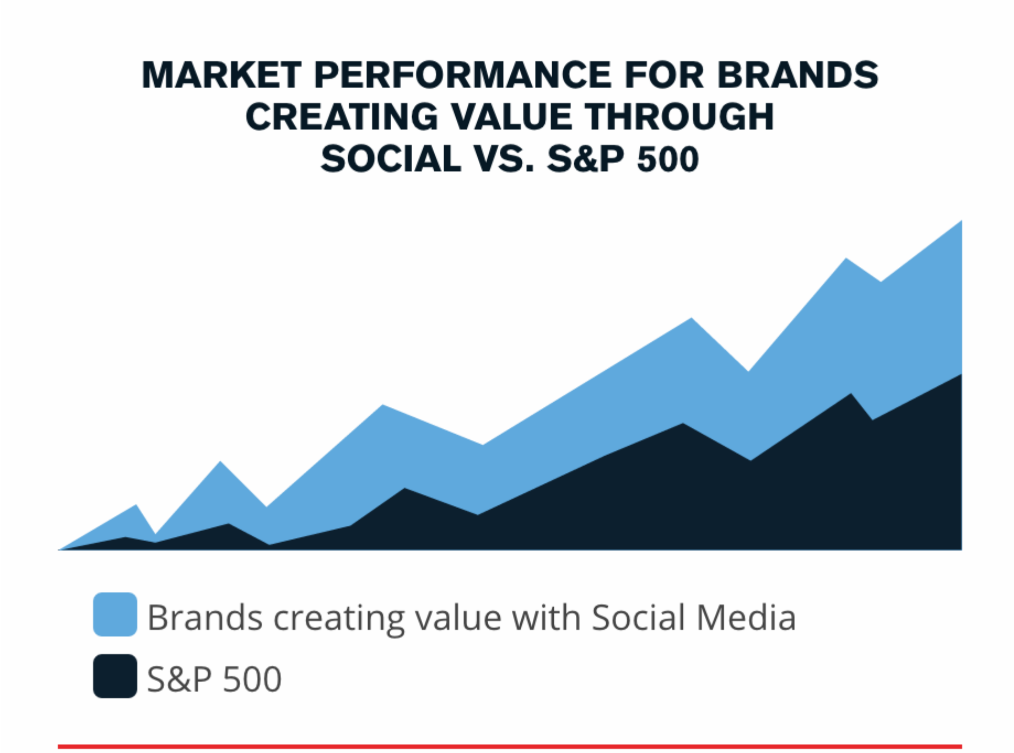
25%

IS **PINTEREST'S** SHARE OF INTERNET RETAIL REFERRAL TRAFFIC

SOCIAL MEDIA

THE BUSINESS PLATFORM

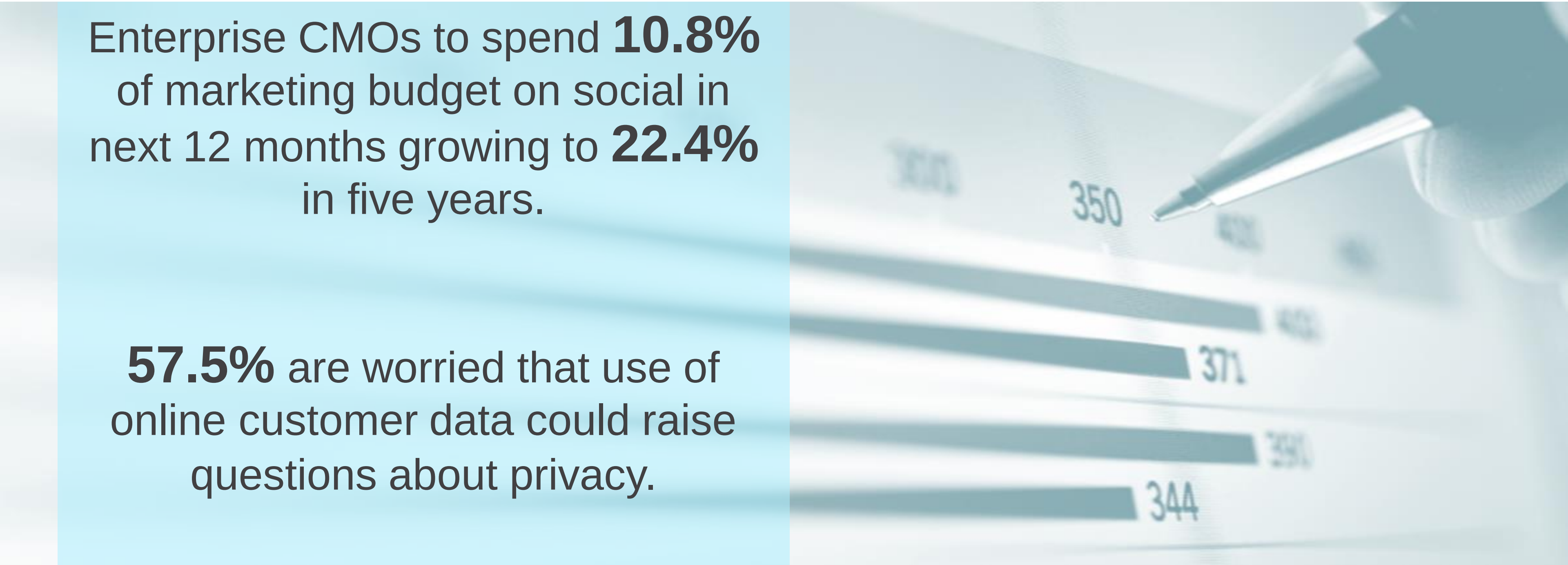
SOCIAL CREATES BUSINESS VALUE



40% Increase in performance for social brands vs. S&P 500

60% buying decisions made on perception of brand vs. product or service quality

MASSIVE INVESTMENT INTO SOCIAL



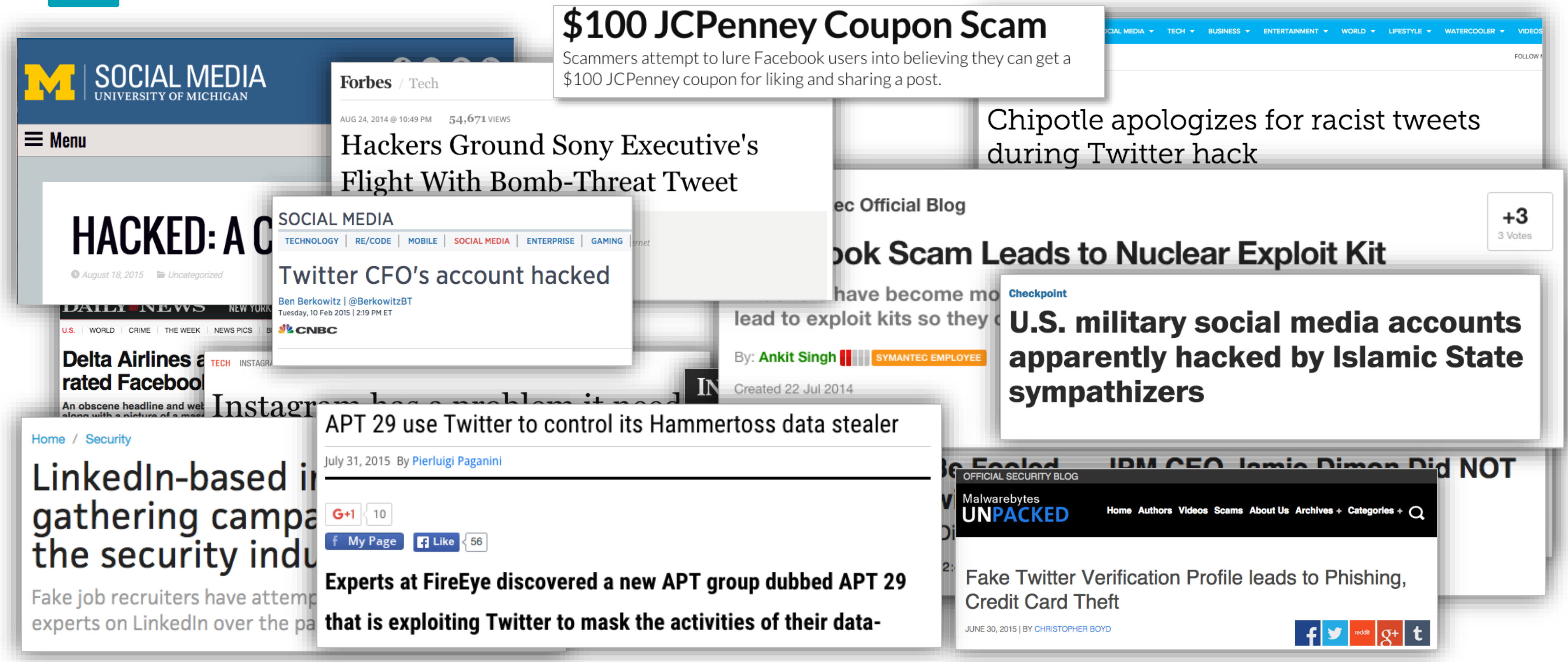
Enterprise CMOs to spend **10.8%** of marketing budget on social in next 12 months growing to **22.4%** in five years.

57.5% are worried that use of online customer data could raise questions about privacy.

YIKES!

SOCIAL MEDIA CAN BE DANGEROUS

IT'S ALL OVER THE NEWS



SOCIAL MEDIA UNIVERSITY OF MICHIGAN

Menu

HACKED: A C

August 18, 2015 Uncategorized

Forbes / Tech

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

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

$100 JCPenney Coupon Scam

Scammers attempt to lure Facebook users into believing they can get a $100 JCPenney coupon for liking and sharing a post.

CIAL MEDIA TECH BUSINESS ENTERTAINMENT WORLD LIFESTYLE WATERCOOLER VIDEOS

Chipotle apologizes for racist tweets during Twitter hack

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

ec Official Blog

ook Scam Leads to Nuclear Exploit Kit

+3 3 Votes

have become mo lead to exploit kits so they

By: Ankit Singh SYMANTEC EMPLOYEE

Created 22 Jul 2014

DAILY NEWS NEW YORK

U.S. WORLD CRIME THE WEEK NEWS PICS

Delta Airlines a rated Faceboo

An obscene headline and wel

TECH INSTAGR

Instagram has a problem it need

Checkpoint

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

Home / Security

LinkedIn-based i gathering campa the security indu

Fake job recruiters have attemp experts on LinkedIn over the pa

APT 29 use Twitter to control its Hammertoss data stealer

July 31, 2015 By Pierluigi Paganini

G+1 10 My Page Like 56

Experts at FireEye discovered a new APT group dubbed APT 29 that is exploiting Twitter to mask the activities of their data-

IBM CEO Jamie Dimon Did NOT

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

ROGERS

AND IT'S NOT HYPE

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

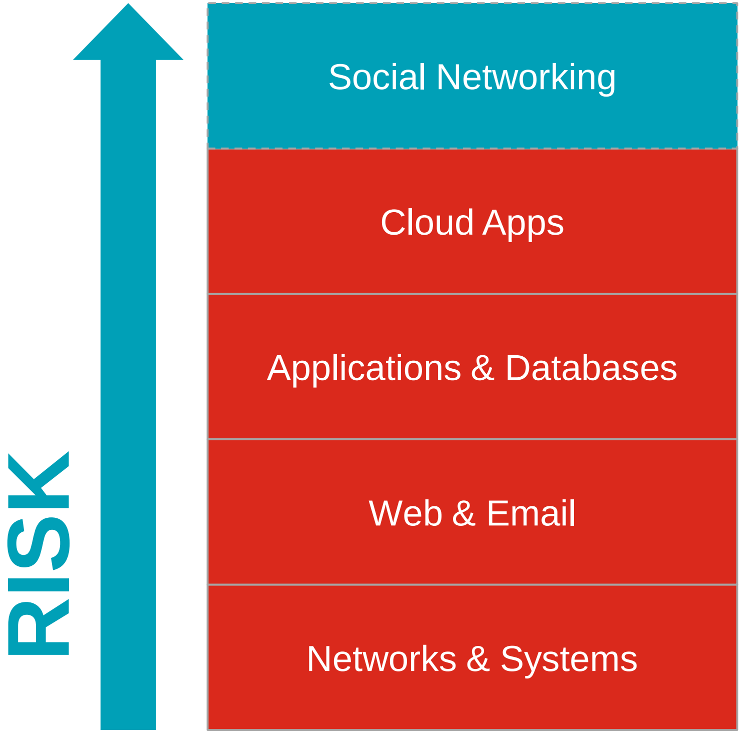
TREND MICRO™

29MILLION 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

TIME TO TREAT SOCIAL AS A RISK SURFACE



RISK

Social Networking

Cloud Apps

Applications & Databases

Web & Email

Networks & Systems

Today we need Social Media Security

In 2015 the CASB vendors enabled security for 3rd party cloud apps

In 2007 you bought Next-Gen Firewalls & DB Security Tools

In 2003 you bought Web & Email Gateway Appliances

“Viruses reach epidemic proportions, infecting millions of desktops” - June 2000

THE PROBLEM WITH SOCIAL

BUSINESS RISKS

- External **Fraud** & Customer **Data Loss**
- Impersonations & **Reputation Damage**
- **Counterfeit,** Piracy & **Trademark** Usage

“Due to the amplification effects of social media, [reputational risk] operational losses can greatly exceed the value of the physical loss from a risk event.” Gartner

SECURITY THREATS

- Targeted Attacks & **Social Engineering**
- **Insider Threat** & Data Loss
- **Executive Protection** & Threat Intelligence

“Social media scams are the #1 method to breach the network, far more common than traditional email phishing, and Facebook is the #1 source of malware.” CISCO

DO YOU HAVE VISIBILITY?

ANATOMY OF AN ATTACK: ENTERPRISE SOCIAL MEDIA

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 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

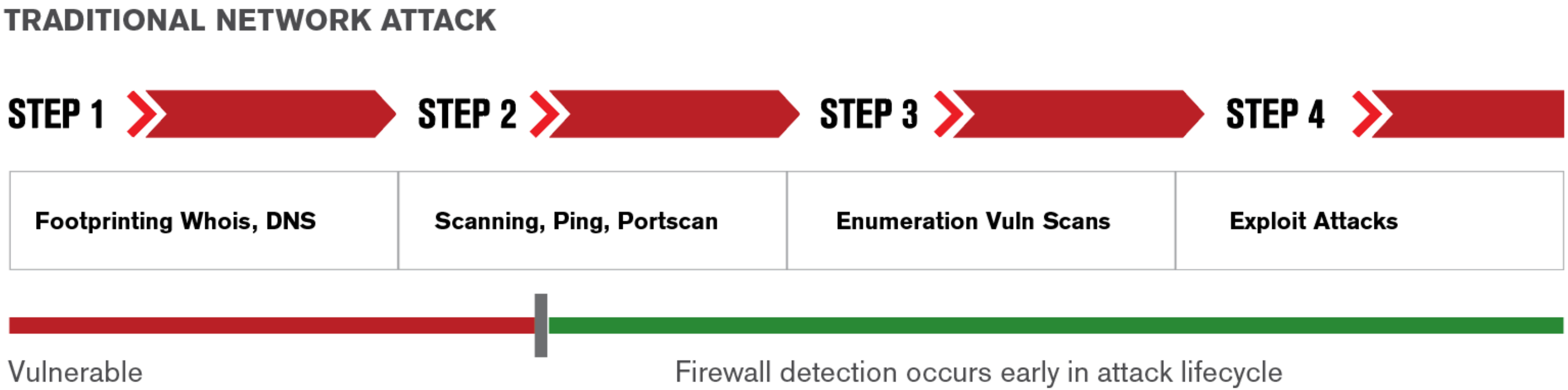
✓ Perform scams

✓ Execute cyber attacks

✓ Stage violence

✓ And more…

TRADITIONAL NETWORK ATTACK VS. SOCIAL MEDIA ATTACK



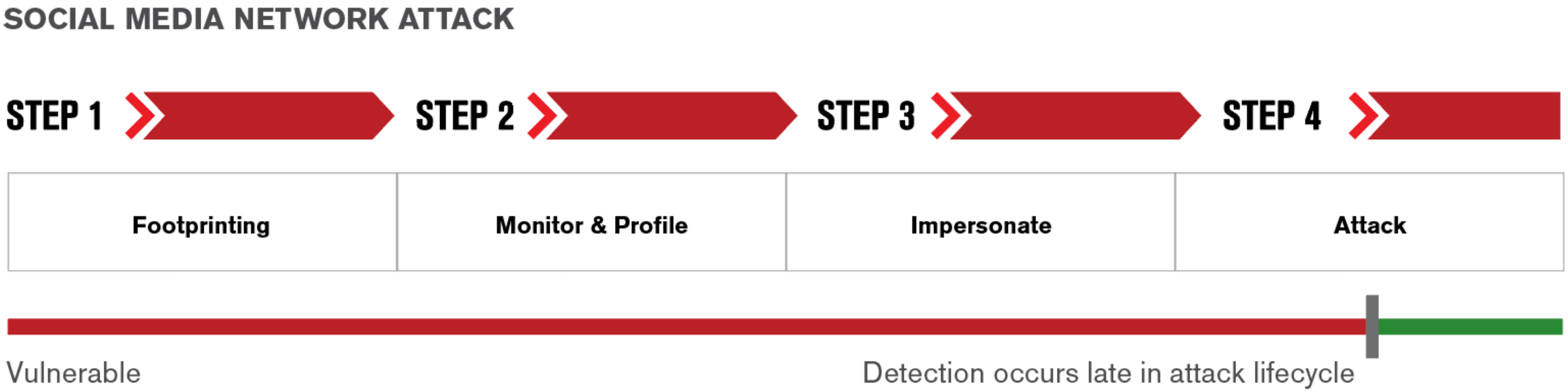
TRADITIONAL NETWORK ATTACK

STEP 1	STEP 2	STEP 3	STEP 4
Footprinting Whois, DNS	Scanning, Ping, Portscan	Enumeration Vuln Scans	Exploit Attacks

Vulnerable

Firewall detection occurs early in attack lifecycle

SOCIAL MEDIA ATTACK – BUILD A NETWORK OF TRUST



SOCIAL MEDIA NETWORK ATTACK

STEP 1 — Footprinting

STEP 2 — Monitor & Profile

STEP 3 — Impersonate

STEP 4 — Attack

Vulnerable

Detection occurs late in attack lifecycle

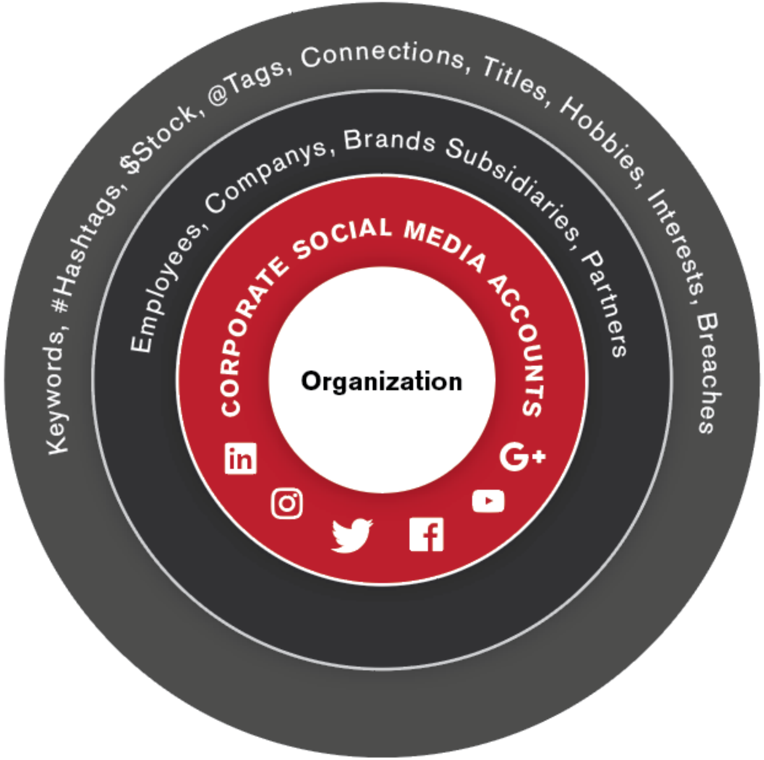
Build a network of “trust”!!!

FOOTPRINT

LinkedIn	company employees, titles, locations, email addresses, phone numbers, former employees
Twitter	bio, interests, other Twitter accounts they own, other brands/sub-brands, employees responsible for managing brand accounts, followers
Facebook	bio, birthday, interests, hobbies, connections
Google+	corporate ID or login, interests, hobbies, connections

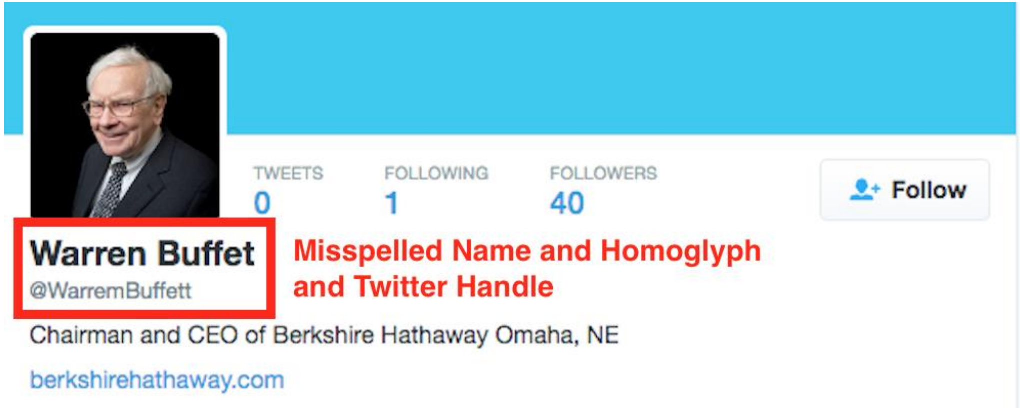
MONITOR & PROFILE

- Social Media Accounts
- Dormant accounts
- Subsidiaries
- Responsible people for those accounts
- Partners
- Keywords
- #Hashtags
- @<mentions>
- $Stock
- Hobbies, interests
- Titles


Keywords, #Hashtags, $Stock, @Tags, Connections, Titles, Hobbies, Interests, Breaches
Employees, Companys, Brands Subsidiaries, Partners
CORPORATE SOCIAL MEDIA ACCOUNTS
Organization

IMPERSONATIONS

- Sampling of approximately ***100 enterprises shows more than 1000 impersonation accounts are created weekly*** by perpetrators.



Warren Buffet
@WarremBuffett

Misspelled Name and Homoglyph and Twitter Handle

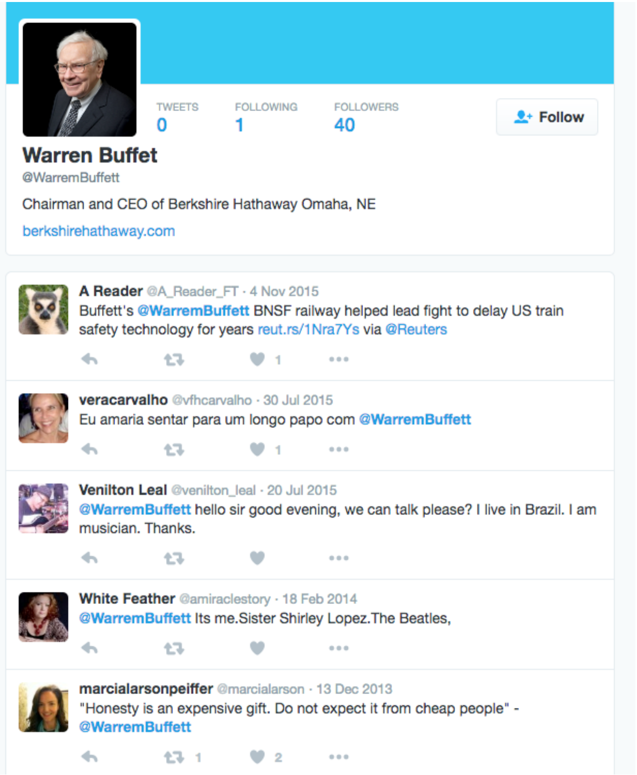
Chairman and CEO of Berkshire Hathaway Omaha, NE

berkshirehathaway.com

- 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



TWEETS 0 FOLLOWING 1 FOLLOWERS 40

Warren Buffet
@WarremBuffett

Chairman and CEO of Berkshire Hathaway Omaha, NE

berkshirehathaway.com

A Reader @A_Reader_FT · 4 Nov 2015
Buffett's @WarremBuffett BNSF railway helped lead fight to delay US train safety technology for years reut.rs/1Nra7Ys via @Reuters
♥ 1

veracarvalho @vfhcarvalho · 30 Jul 2015
Eu amaria sentar para um longo papo com @WarremBuffett
♥ 1

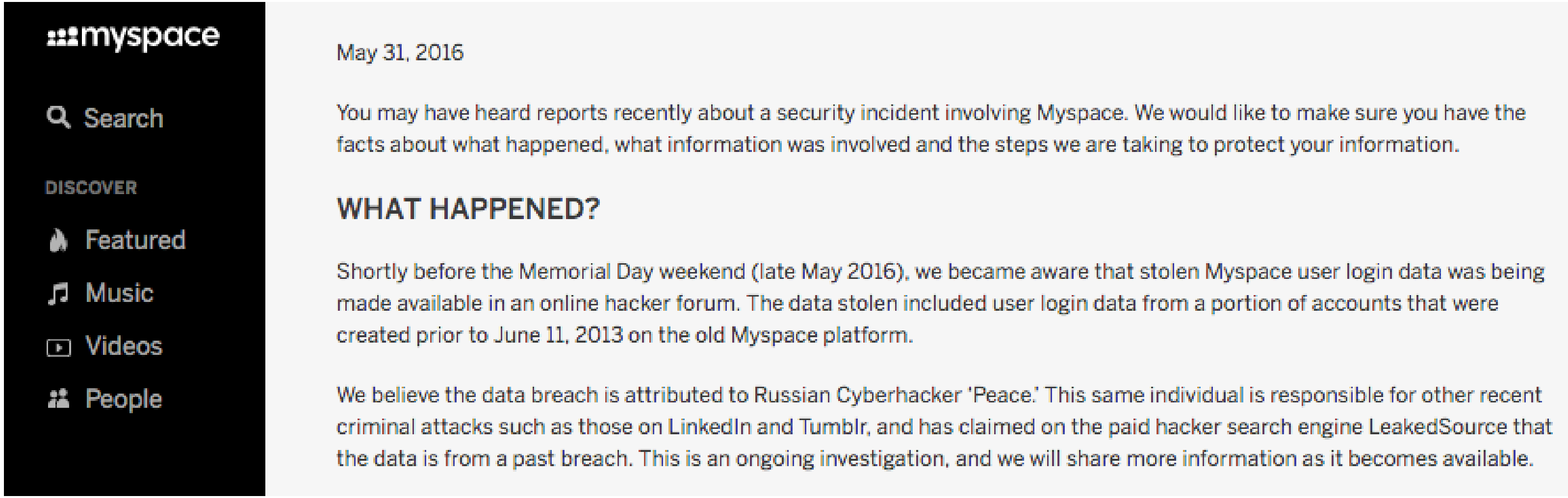
Venilton Leal @venilton_leal · 20 Jul 2015
@WarremBuffett hello sir good evening, we can talk please? I live in Brazil. I am musician. Thanks.

White Feather @amiraclestory · 18 Feb 2014
@WarremBuffett Its me.Sister Shirley Lopez.The Beatles,

marcialarsonpeiffer @marcialarson · 13 Dec 2013
"Honesty is an expensive gift. Do not expect it from cheap people" - @WarremBuffett
1 ♥ 2

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.

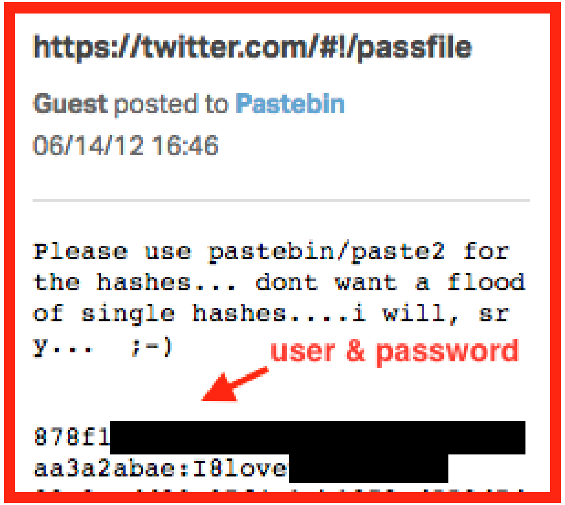
WHAT HAPPENED?

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)



https://twitter.com/#!/passfile

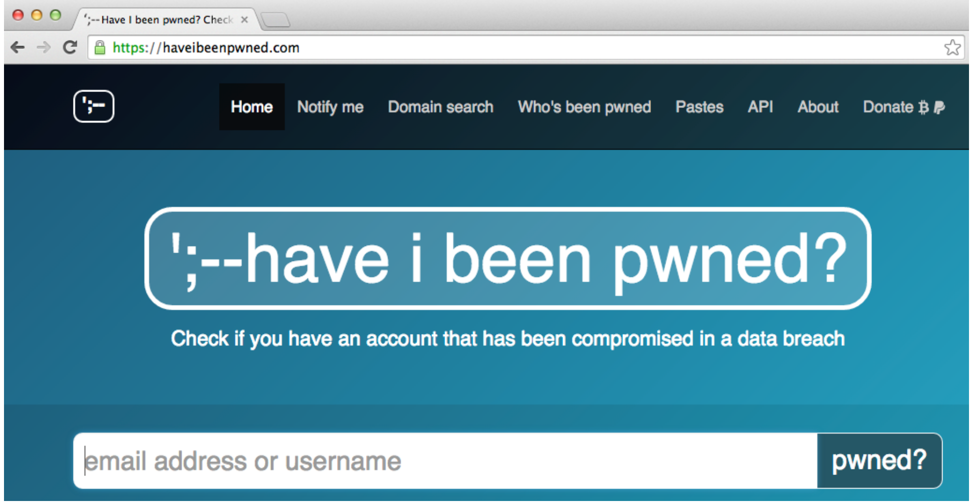
Guest posted to Pastebin

06/14/12 16:46

```
Please use pastebin/paste2 for
the hashes... dont want a flood
of single hashes....i will, sr
y...  ;-)

878f1[redacted]
aa3a2abae:I8love[redacted]
```

user & password



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

pwned?

ATTACK METHODS – Tactics Techniques Procedures

- **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
- We can also reverse footprint social media URL security and serve good/bad content based on this

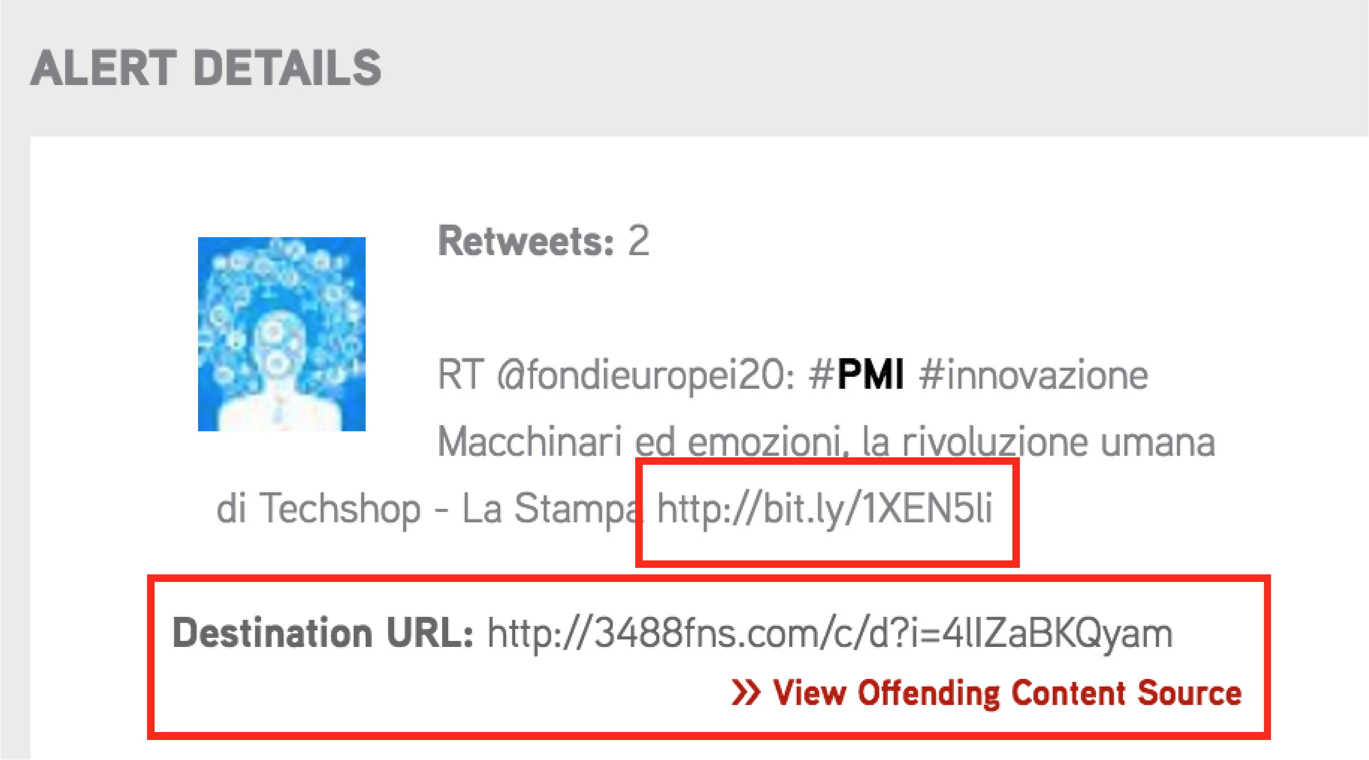
ATTACK METHODS – URL SHORTENERS

- Shortened URLs come in many forms:

Company	Legitimate Shortened URL
Bitly	bit<dot>ly
Google	goo<dot>gl
Hootsuite	ow<dot>ly
TinyURL.com	tinyurl<dot>com
Tiny.cc	tiny<dot>cc

- Many (but not all) do not check for bad URLs

ATTACK METHODS – OBFUSCATED MALICIOUS URL



ALERT DETAILS

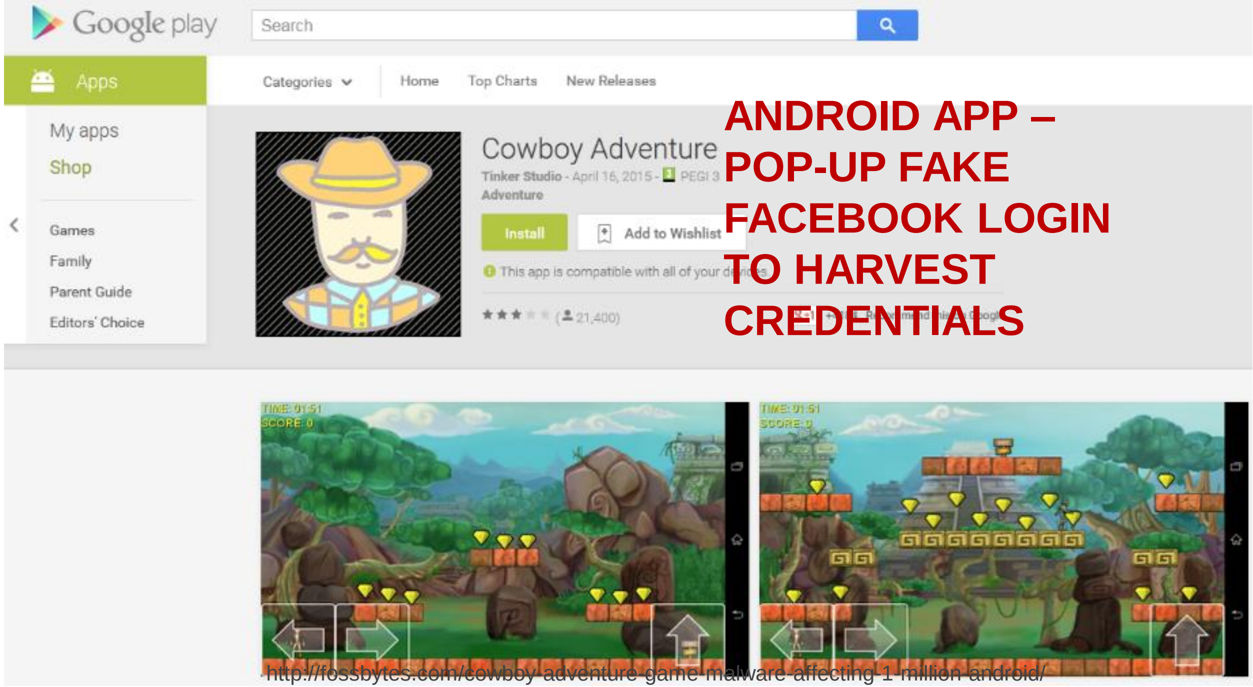
Retweets: 2

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=4lIZaBKQyam

ATTACK METHODS – MALICIOUS URLS

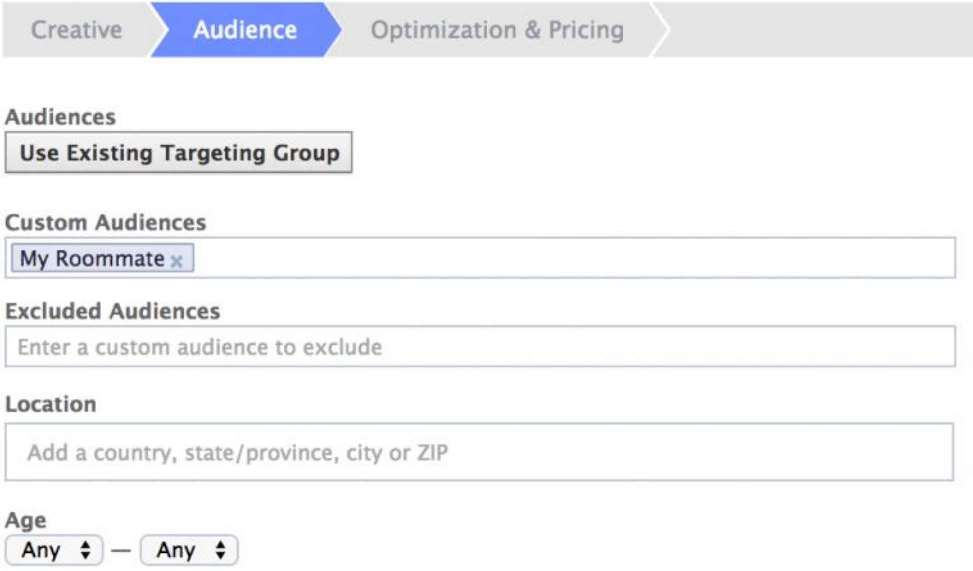
- Malware
- Phishing Link
- Malicious Browser Plug-in
- Bad App



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

http://fossbytes.com/cowboy-adventure-game-malware-affecting-1-million-android/

ATTACK METHODS – MALICIOUS ADVERTISING



Audiences

Use Existing Targeting Group

Custom Audiences

My Roommate ×

Excluded Audiences

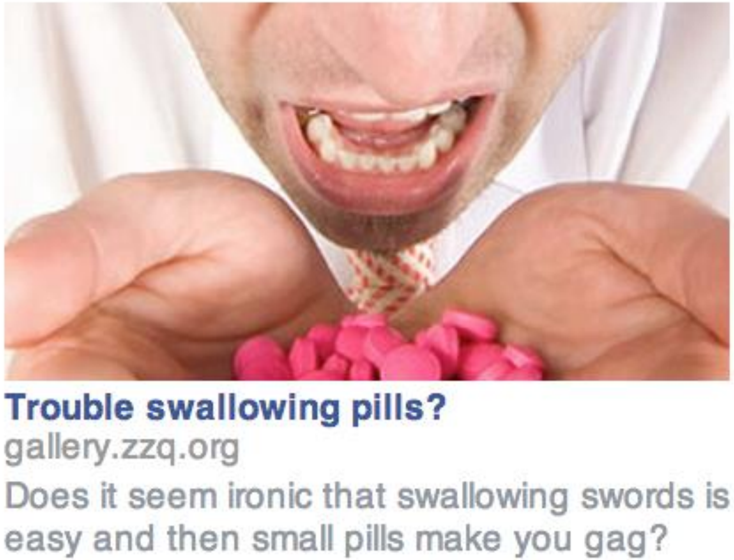
Enter a custom audience to exclude

Location

Add a country, state/province, city or ZIP

Age

Any — Any

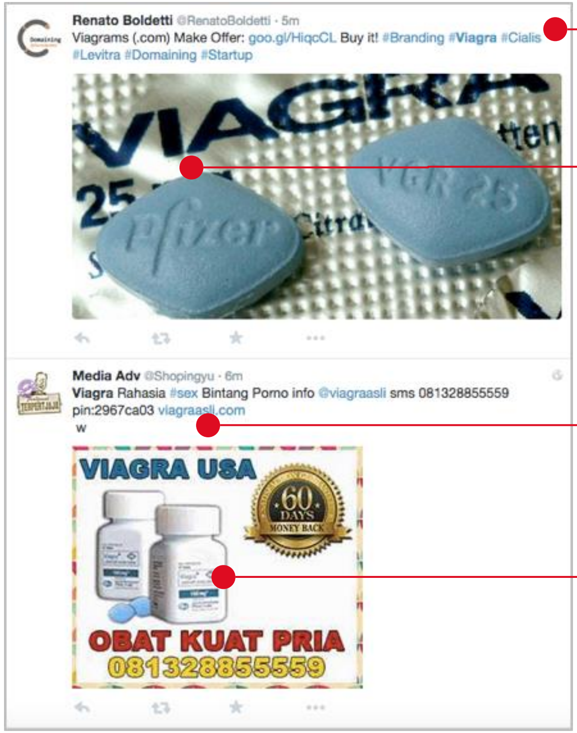


Trouble swallowing pills?

gallery.zzq.org

Does it seem ironic that swallowing swords is easy and then small pills make you gag?

SCAMS, SCAMS & MORE SCAMS



Renato Boldetti @RenatoBoldetti · 5m
Viagrams (.com) Make Offer: goo.gl/HiqcCL Buy it! #Branding #Viagra #Cialis #Levitra #Domaining #Startup

Media Adv @Shopingyu · 6m
Viagra Rahasia #sex Bintang Porno info @viagraasli sms 081328855559 pin:2967ca03 viagraasli.com
w

"SPONSORED" SCAMS
Scammers pay Instagram to feature their content to more people

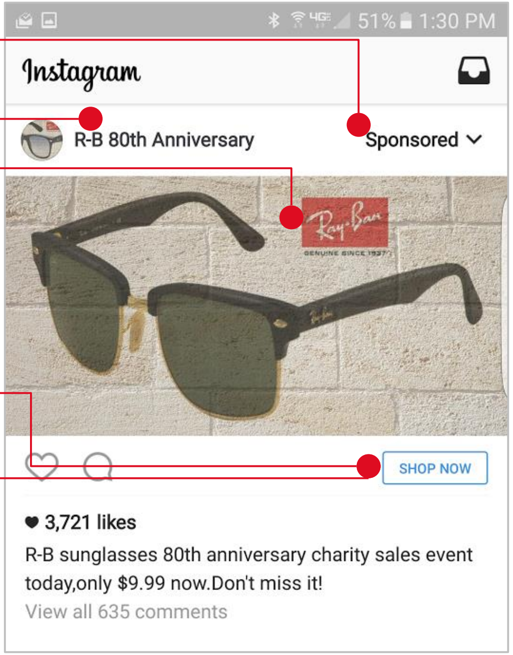
TRADEMARKED IMAGE
Copyrighted content repurposed for malicious activity

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



51% 1:30 PM

Instagram

R-B 80th Anniversary Sponsored

3,721 likes

R-B sunglasses 80th anniversary charity sales event today,only $9.99 now.Don't miss it!

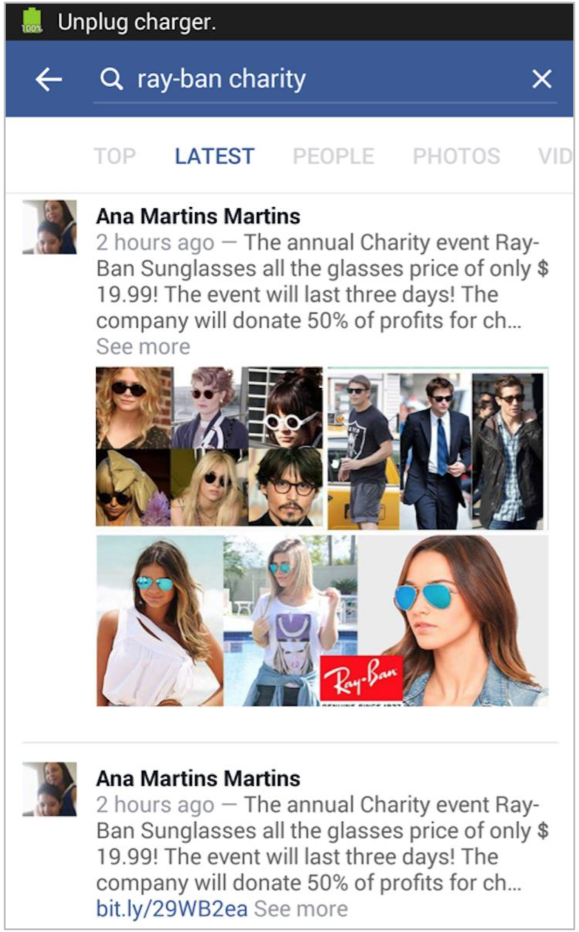
View all 635 comments

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

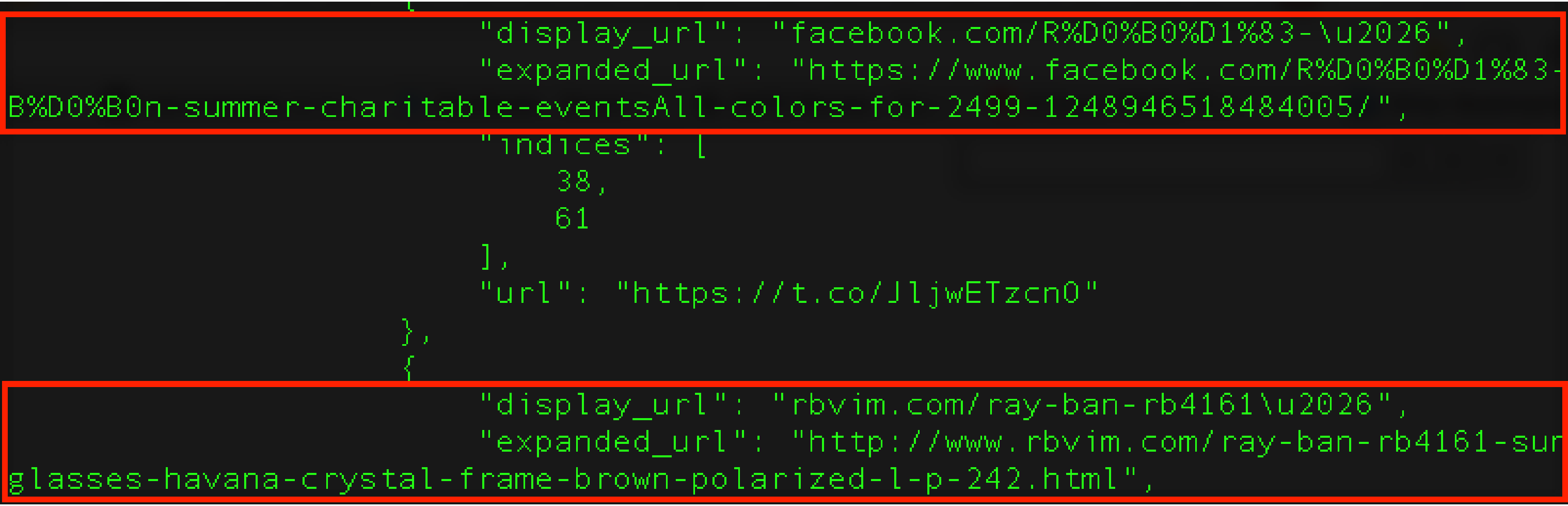


Ana Martins Martins
2 hours ago — The annual Charity event Ray-Ban Sunglasses all the glasses price of only $ 19.99! The event will last three days! The company will donate 50% of profits for ch...
See more

Ana Martins Martins
2 hours ago — The annual Charity event Ray-Ban Sunglasses all the glasses price of only $ 19.99! The event will last three days! The company will donate 50% of profits for ch...
bit.ly/29WB2ea See more

RAY-BAN SUNGLASSES

PHISHING & FRAUD CONTINUE…



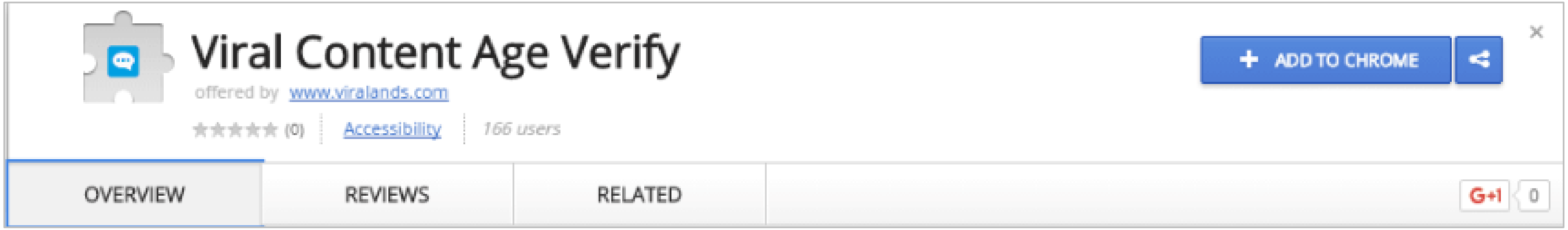
```
                    {
                        "display_url": "facebook.com/R%D0%B0%D1%83-\u2026",
                        "expanded_url": "https://www.facebook.com/R%D0%B0%D1%83-
B%D0%B0n-summer-charitable-eventsAll-colors-for-2499-1248946518484005/",
                        "indices": [
                            38,
                            61
                        ],
                        "url": "https://t.co/JljwETzcn0"
                    },
                    {
                        "display_url": "rbvim.com/ray-ban-rb4161\u2026",
                        "expanded_url": "http://www.rbvim.com/ray-ban-rb4161-sun
glasses-havana-crystal-frame-brown-polarized-l-p-242.html",
```

FACEBOOK

MALWARE CLICK FRAUD…

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



Viral Content Age Verify

offered by www.viralands.com

★★★★★ (0) | Accessibility | 166 users

Source: http://www.scmagazine.com/chrome-browser-extensions-discovered-engaging-in-facebook-click-fraud/article/510843/

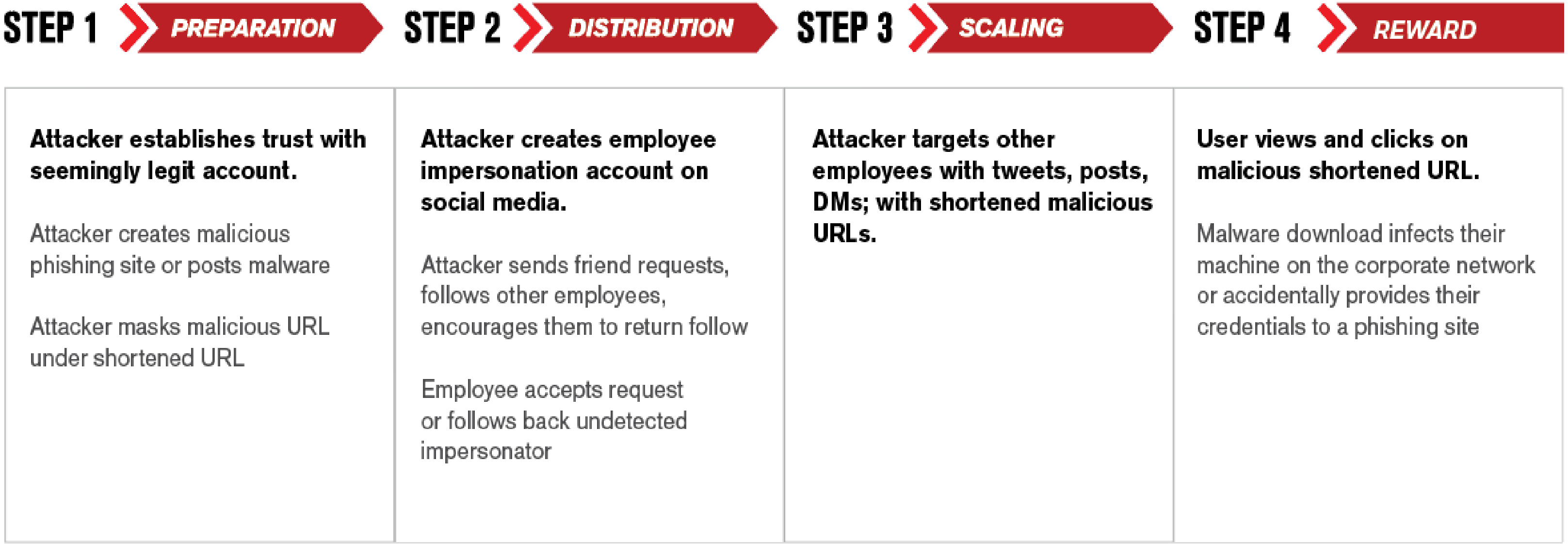
FACEBOOK MESSENGER *MALWARE…*

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.

Source: http://www.digitaltrends.com/computing/facebook-messenger-virus-malware-windows-chrome/

PUTTING IT ALL TOGETHER

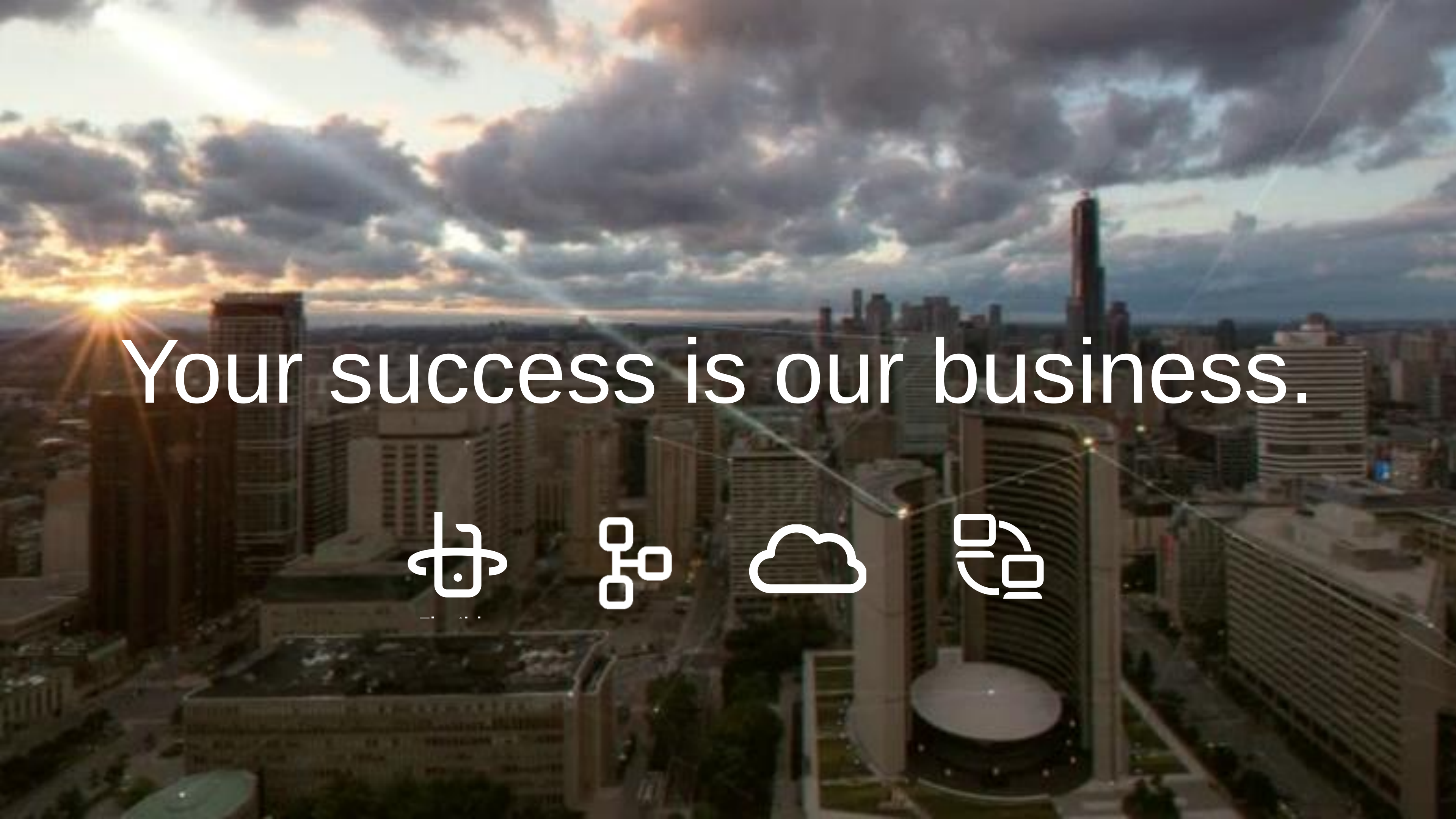


STEP 1 PREPARATION	STEP 2 DISTRIBUTION	STEP 3 SCALING	STEP 4 REWARD
Attacker establishes trust with seemingly legit account. Attacker creates malicious phishing site or posts malware Attacker masks malicious URL under shortened URL	**Attacker creates employee impersonation account on social media.** Attacker sends friend requests, follows other employees, encourages them to return follow Employee accepts request or follows back undetected impersonator	**Attacker targets other employees with tweets, posts, DMs; with shortened malicious URLs.**	**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

COUNTERMEASURES – FORTIFYING YOUR SOCIAL MEDIA

- **Identify and improve 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 and other settings** 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!



Your success is our business.