RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PDAC-R09

Third-Party Code: Where Data Breaches, Election Meddling & Ad Fraud Converge

Mark Grantz

Assistant to the Special Agent in Charge
U.S. Secret Service – Technical Security Division

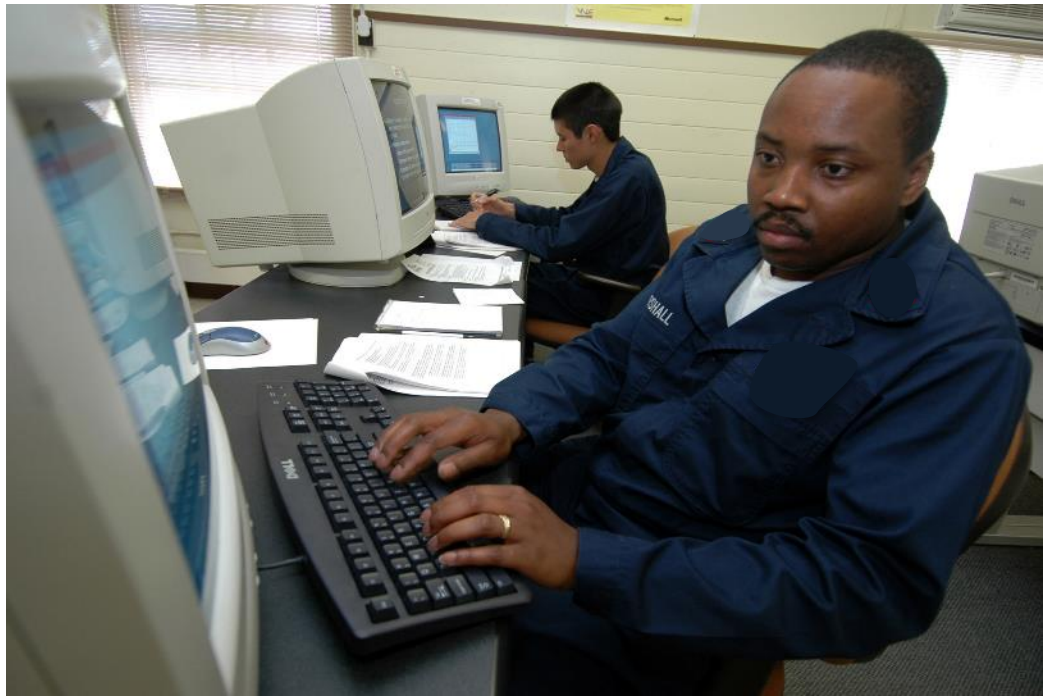
Chris Olson

Founder and CEO
The Media Trust
@3pc_ChrisOlson

Accountability for the digital world we inhabit

CONSUMER PERSPECTIVE

ENTERPRISE PERSPECTIVE



Changing communication infrastructure

ONE-TO-ONE

ONE-TO-MANY

Third-party Code: It's what makes the internet work

Advertising

Content recommendation

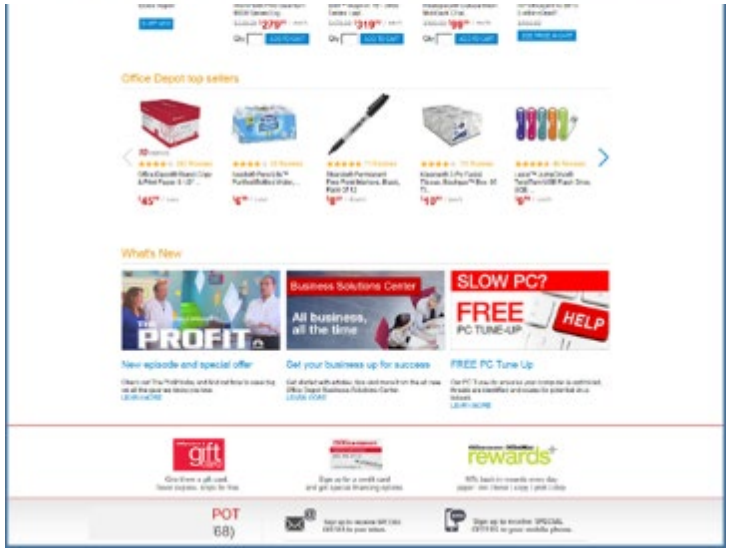
Image Lib

Social sha

Video

Customer Identification/ login

Shopping cart



Analytics

Content Management

ment

Device Recognition

Cookies

Fingerprinting

Third-party Code: It's what makes the internet work

50-90% executing digital code is from third parties

Advertising

Content recomme

Image Library

Video

Customer Identification

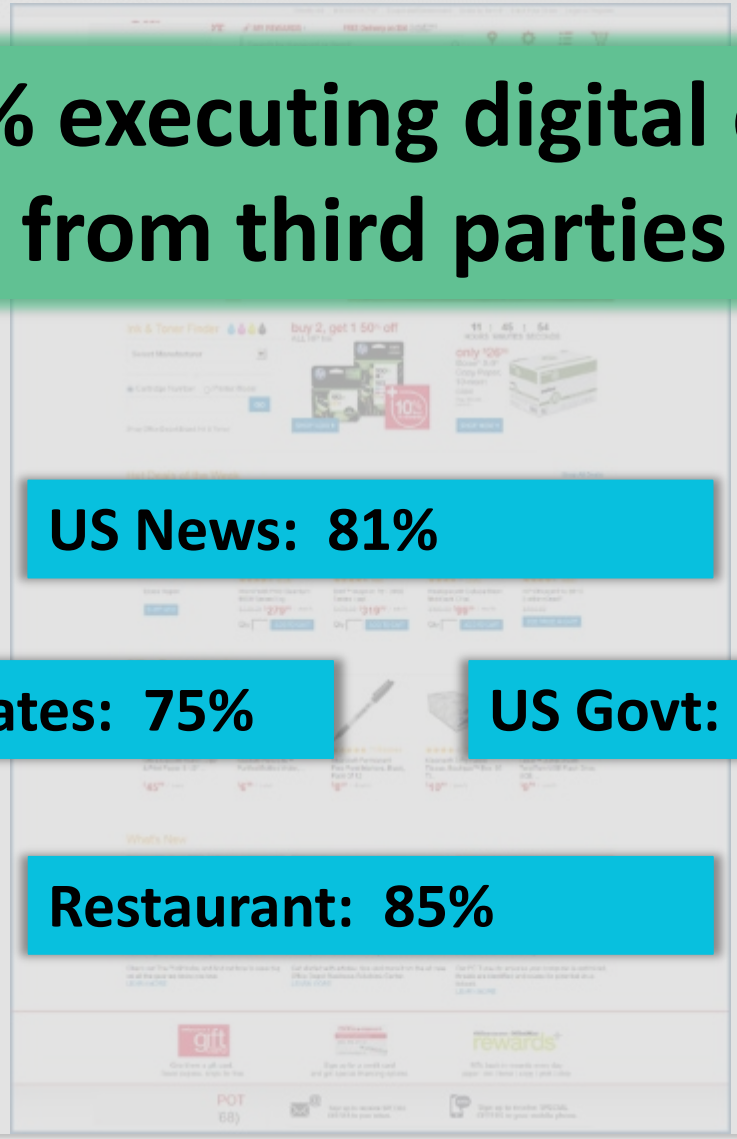
tics

nt Management

Data Management

Device Recognition

Cookies



Hotel & Gaming: 84%

US News: 81%

Banking: 82%

Presidential Candidates: 75%

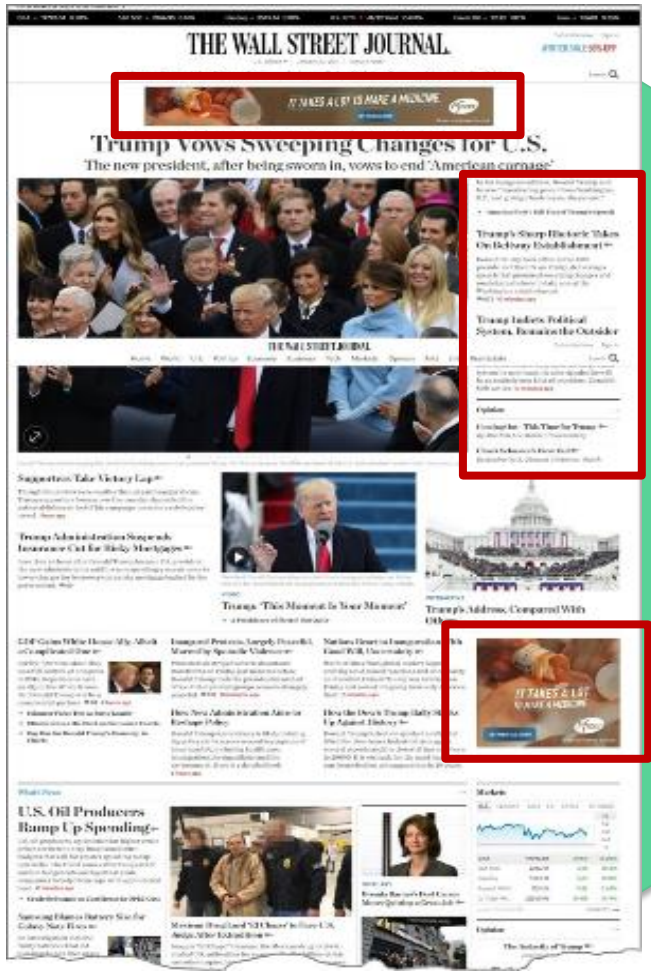
US Govt: 78%

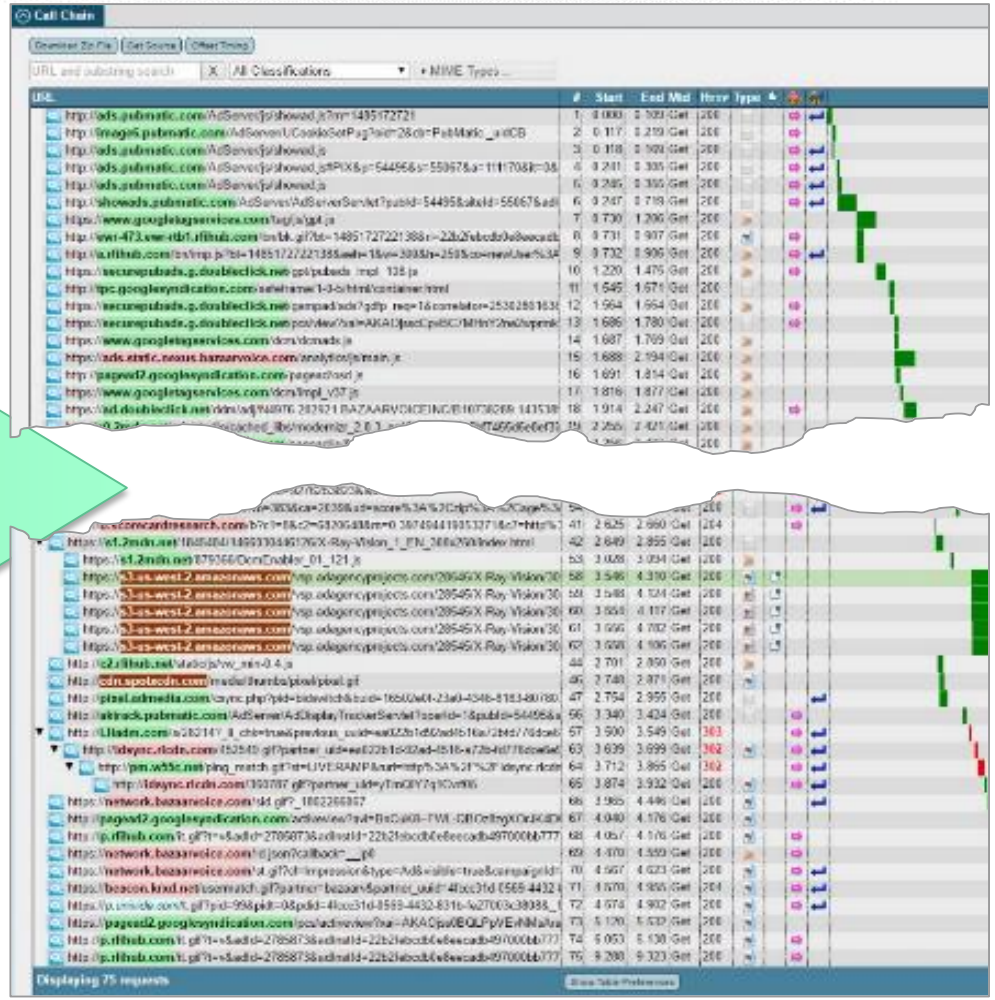
Retail: 82%

Restaurant: 85%

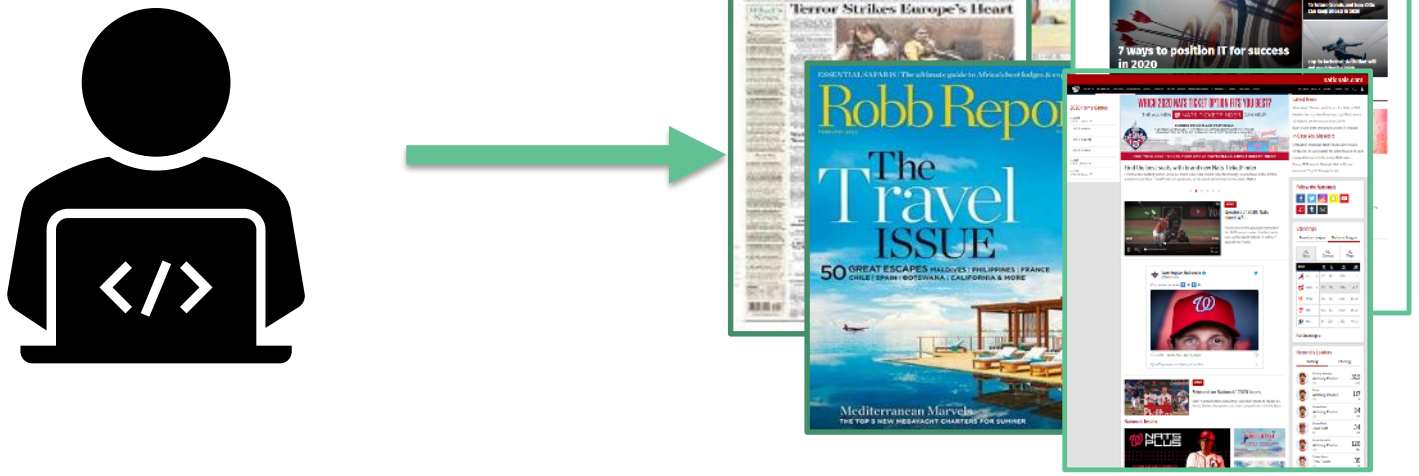
Healthcare: 84%

What you see isn't what you get

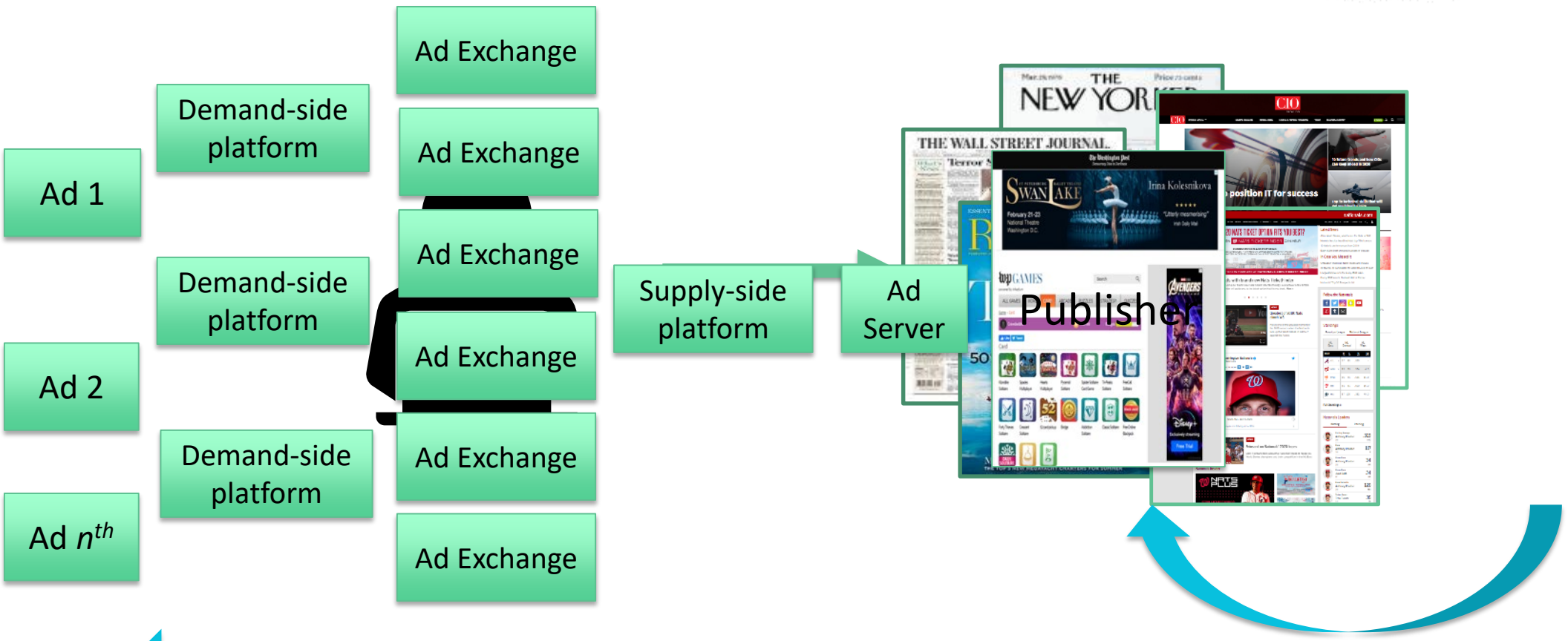




Deciphering the purpose of a digital footprint



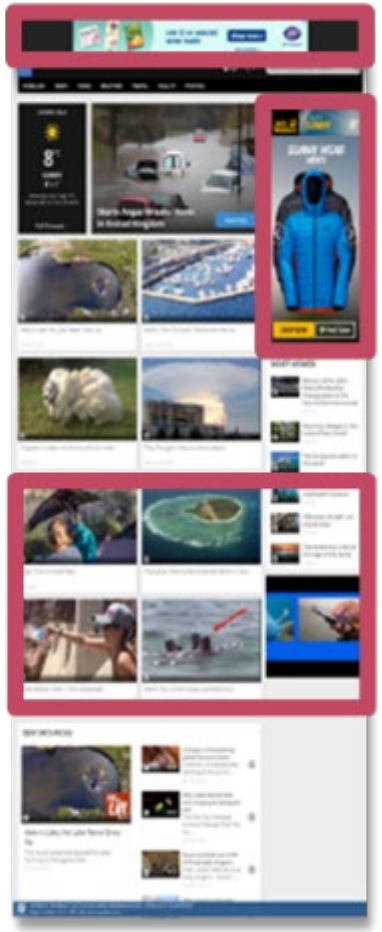
Deciphering the purpose of a digital footprint



Third-party code used to target…

Weather

Male, 22 Years.
McLean, VA (USA), iOS



Female, 40 Years.
London. Desktop. Safari.

USA Today

Male, 22 Years.
McLean, VA (USA), iOS

Female, 40 Years.
London. Desktop. Safari.

...and harm

Smart Krampus-3PC Malware Targets iPhone Users

Facebook disables some misleading ads on HIV prevention drugs, responding to growing outcry

Report: Ryuk ransomware impacts websites of DOD contractor

US Agency Hit With N. Korean-Themed Phishing: Report

Online Threats Targeting Unprepared Retailers Ramp up Dramatically During the Holiday Shopping Season

FBI says hackers are targeting US auto industry

U.S. Army bans TikTok on military devices, signaling growing concern about app's Chinese roots

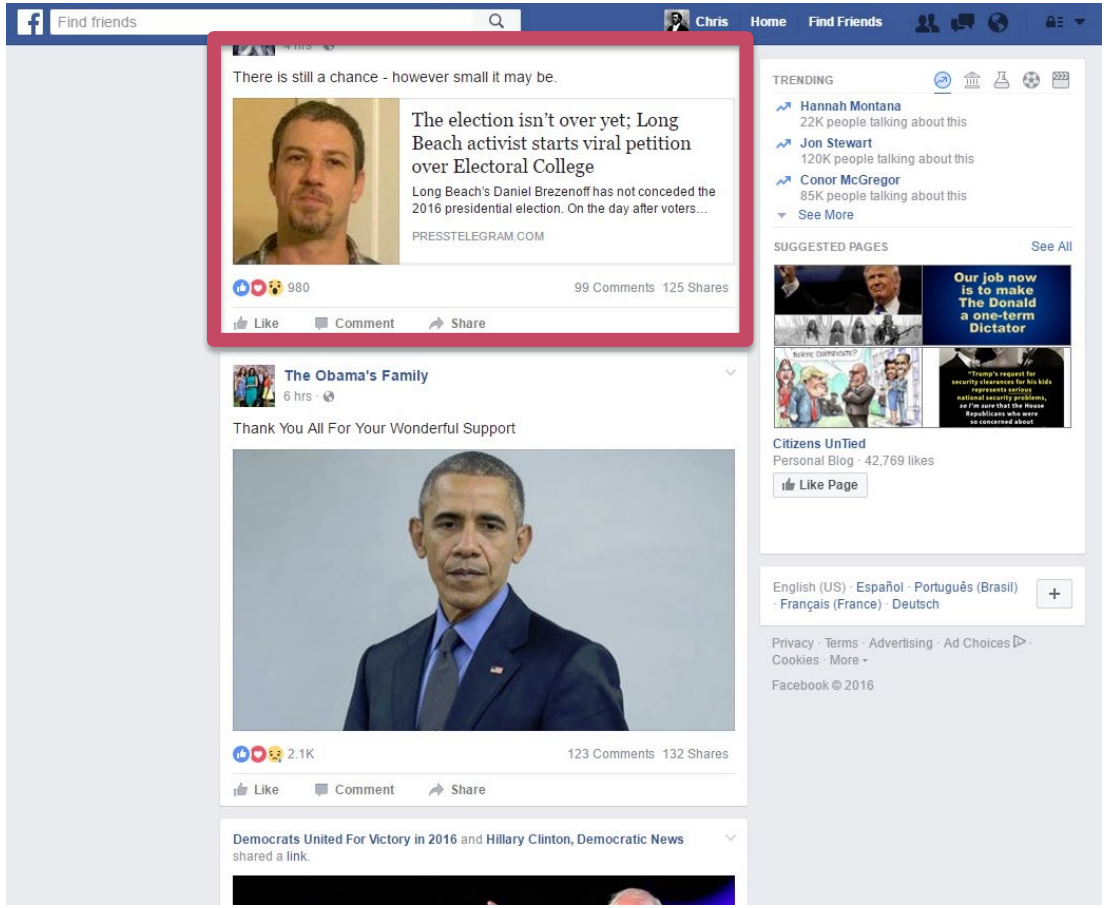
Senate Intelligence report finds 'extensive' Russian election interference

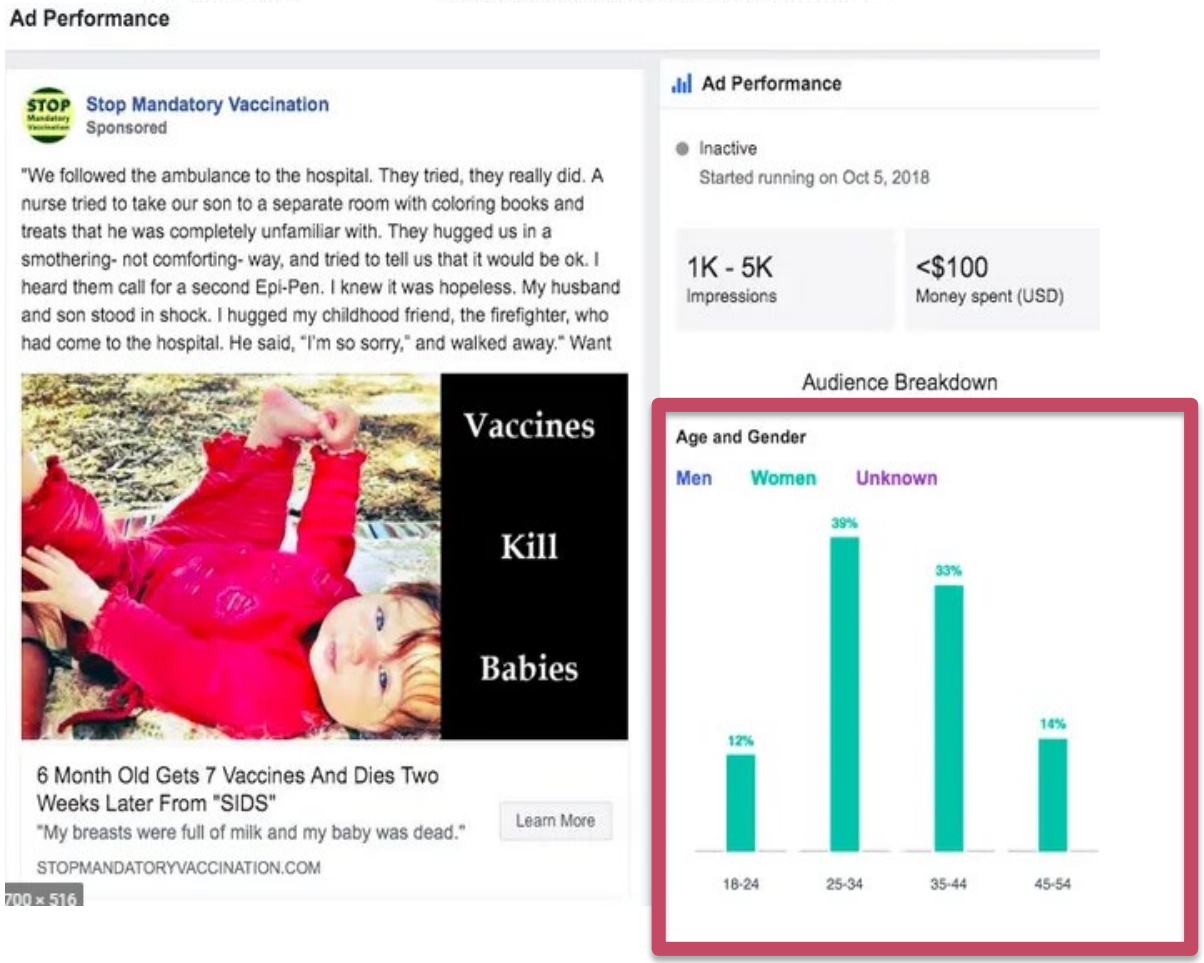
Ransomware attack on construction company raises questions about federal contracts

Card Skimmer Group Replaces Checkout Page to Steal Payment Info

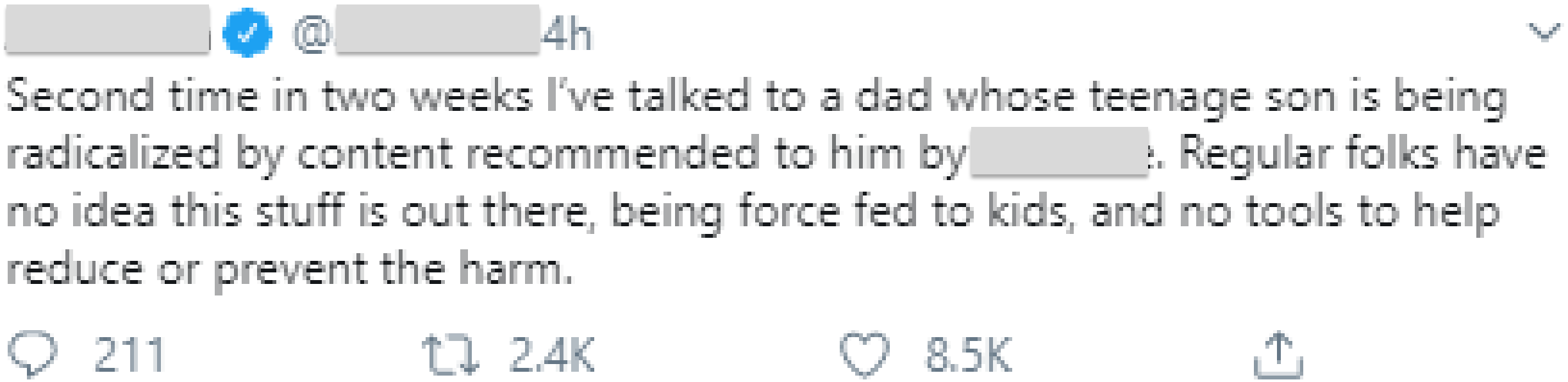
Zynga data breach exposed 200 million Words with Friends players

…and misinform consumers





Case in point



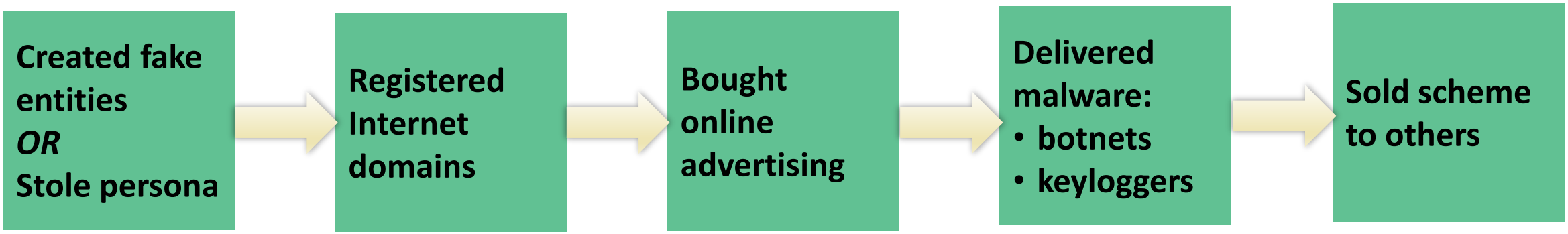
RSAConference2020

The Incident

Ukrainian malvertiser exploited digital advertising ecosystem to target American consumers and defraud

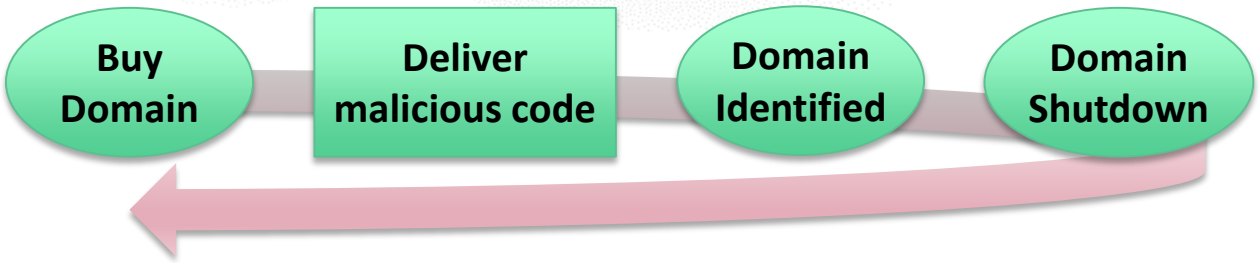
Background

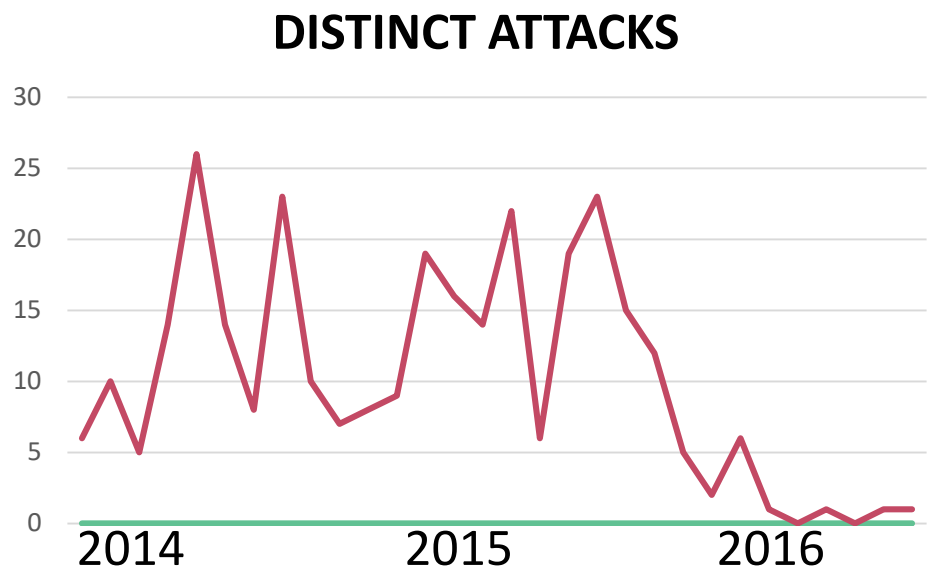
- October 2013 – May 2018 [4½ years]
- Goal: Unlawfully enrich by launching malicious advertisements
- Affected: 100 million+ US consumers



How it worked: Trial & Error

- Digital advertising campaigns with compromised code
- Code checks:
  - Geography
  - Device parameters
  - Real human (cookies)
- 300+ distinct incidents with thousands of domain combinations





Sample attack…

http://ib[.]adnxs[.]com/cr?id=31151433 **AD SERVER**

http://12[.]csdevgrp[.]com/WhiteLabelBidRequestHandlerServlet?oid=12&width=728&height=90&pubid=123178&tagid=736988&pstn=ETER_PLACEMET_ID_HERE&noaop=1&revmod=ISERT_COTET_TYPE&encoded=1&cb=1433563870&keywords=ISERT_COMMA_SEPARATED_KEYWORDS&callback=document[.]write&urlonly=1&cirf=

http://cpm[.]ranch2market[.]com/advertising[.]html **BAD DOMAIN**

http://cpm[.]ranch2market[.]com/media/ads[.]js **REDIRECT**

http://cpm[.]ranch2market[.]com/5559e5cc00c42[.]jpg **IMAGE**

http://cdn[.]adnxs[.]com/v/s/20/trk[.]js

http://ib[.]adnxs[.]com/favicon[.]ico#-moz-resolution=16,16

http://ib[.]adnxs[.]com/favicon[.]ico

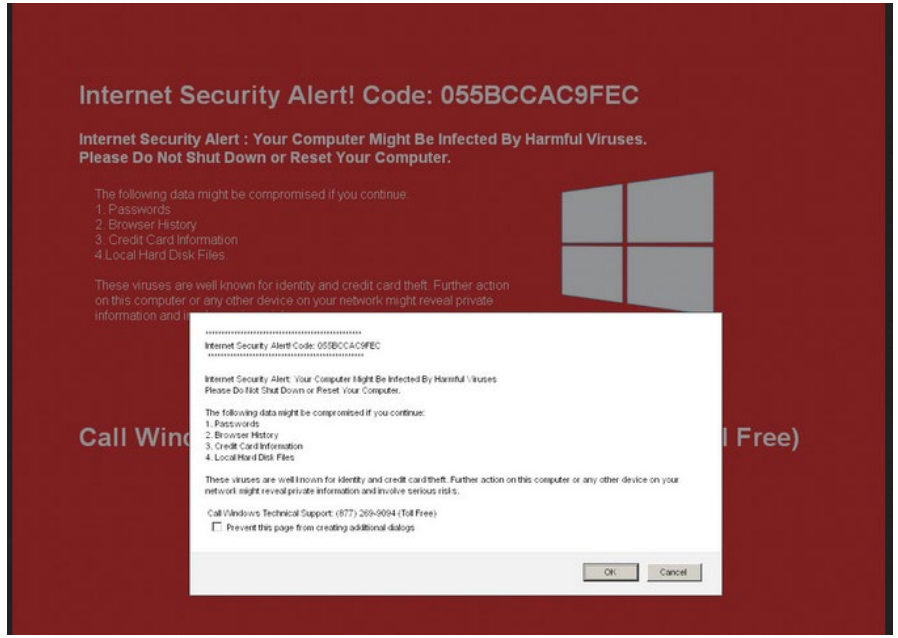
https://goo[.]gl/c5L2ak **URL SHORTENER**

http://poakkddhdjs[.]net[.]ru/rebmiw[.]html?9694429786a=HiCMrgems7cQ%2BwEt23ZgSaxv%2FzpKTn3vLuLYrW9ho4%3D **PAYLOAD 1**

https://goo[.]gl/Lyc31

http://best[.]funeralsrip[.]com/evasion-muses-disinterested-sitters/450808331995180 **PAYLOAD 2**

IMAGE PRESENTED



What we know about the domains

DOMAIN	CREATED	SEEN	OVERT	REPORTED
MEDIASRV23	2013-0911	2014-1128	2014-1205	2015-1205 (3)
STEALTH-MEDIA	2013-0913	2015-0120	2015-0120	2016-0220 (1)
ONLINE-MARKETING-MAVEN	2013-0927	2015-0127	2015-0127	2019-0328 (2)
ADS-GEEK	2012-1231	2015-0318	2015-0525	---
RANCH2MARKET*	2012-0125	2015-0526	2015-0608	2019-1213 (3)
TITHOREBREPREN*	2015-0528	2015-0601	2015-0609	---
STARSTRAFFIC.EU	2015-0617	2015-0617	2015-0617	---
TRIVAGOAD	2015-1005	2015-1005	2015-1011	---

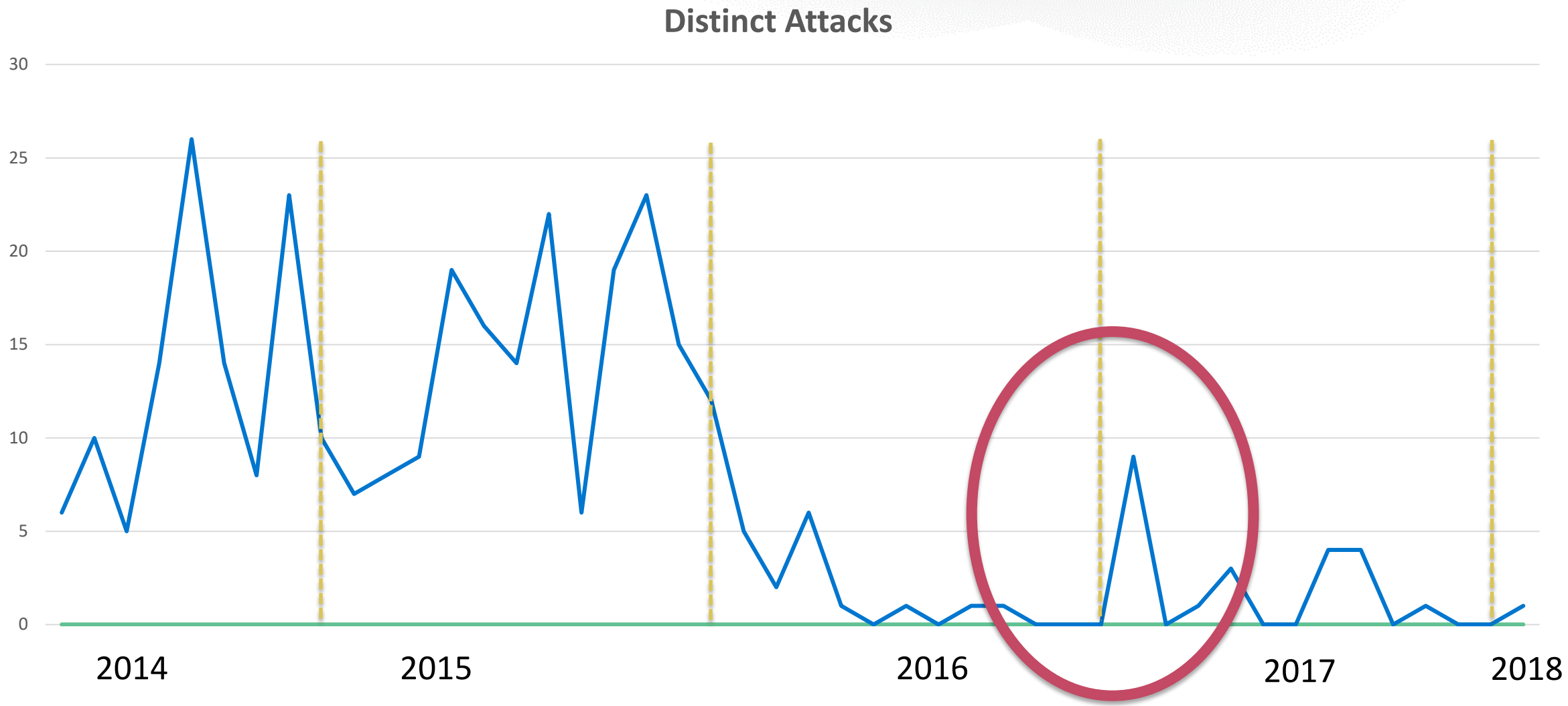
What we know about the domains

DOMAIN	CREATED	SEEN	OVERT	REPORTED
MEDIASRV23	2013-0911	2014-1128	2014-1205	2015-1205 (3)
STEALTH-MEDIA	2013-0913	2015-0120	2015-0120	2016-0220 (1)
ONLINE-MARKETING-MAVEN	2013-0927	2015-0127	2015-0127	2019-0328 (2)
ADS-GEEK	2012-1231	2015-0318	2015-0525	---
RANCH2MARKET*	2012-0125	2015-0526	2015-0608	2019-1213 (3)
TITHOREBREPREN*	2015-0528	2015-0601	2015-0609	---
STARSTRAFFIC.EU	2015-0617	2015-0617	2015-0617	---
TRIVAGOAD	2015-1005	2015-1005	2015-1011	---

What we know about the domains

DOMAIN	CREATED	SEEN	OVERT	REPORTED
MEDIASRV23	2013-0911	2014-1128	2014-1205	2015-1205 (3)
STEALTH-MEDIA	2013-0913	2015-0120	2015-0120	2016-0220 (1)
ONLINE-MARKETING-MAVEN	2013-0927	2015-0127	2015-0127	2019-0328 (2)
ADS-GEEK	2012-1231	2015-0318	2015-0525	---
RANCH2MARKET*	2012-0125	2015-0526	2015-0608	2019-1213 (3)
TITHOREBREPREN*	2015-0528	2015-0601	2015-0609	---
STARSTRAFFIC.EU	2015-0617	2015-0617	2015-0617	---
TRIVAGOAD	2015-1005	2015-1005	2015-1011	

Changing focus: Attribution



…They're back for more

xhttp://a[.]yesadsrv[.]com/displayb[.]php?nid=4&w=728&h=90&zone=76907&pid=4155&sid=56662&subid=&cnt=1&b1=&b2=&b3=&b4=&opt1=&opt2=&opt3=&random=9855	AD SERVER
http://pub[.]clicksor[.]net/newServing/js/ui[.]js	
http://tithorebrepren[.]us/advertising[.]html	BAD DOMAIN
http://tithorebrepren[.]us/media/ads[.]js	REDIRECT
http://tithorebrepren[.]us/553eaf30ac9f7[.]png	IMAGE
http://a[.]yesadsrv[.]com/newServing/tracking_id[.]php?b=1&UID=1433804611288O&TRSTR=1&RTID=	AD SERVER
https://goo[.]gl/lBL3eD	URL SHORTENER
http://hernotherabsup[.]eu/watersheds[.]html?7928103389a=mo%2FsVe3bJaUsoZXm7%2B5pFODC%2F5OHUYdYyD474%2BqIfY%3D	CHECK
https://goo[.]gl/RJ1M09	
http://psoid98iu2hg[.]howhertwatersu[.]in/baloneyallowing/962753024137308	PAYLOAD 1
http://psoid98iu2hg[.]howhertwatersu[.]in/HMoUs3245Ut_TWeT1koCkw0LAWojfUgJk5qQIU9LUruGCK9Z[.]java?five=FWIKVKHLSXO&four=vnd&four=3651676&four=2934&six=o5UWYGx	PAYLOAD 2

RSAConference2020

Changing Enforcement Environment

Bad boys, bad boys whatcha gonna do when they come for you?

Is digital compromise or manipulation illegal?

COPPA
Children's Online Privacy Protection Act

CCPA
California Consumer Privacy Act

CFAA 1990
Computer Fraud and Abuse Act

GDPR
EU's General Data Protection Regulation

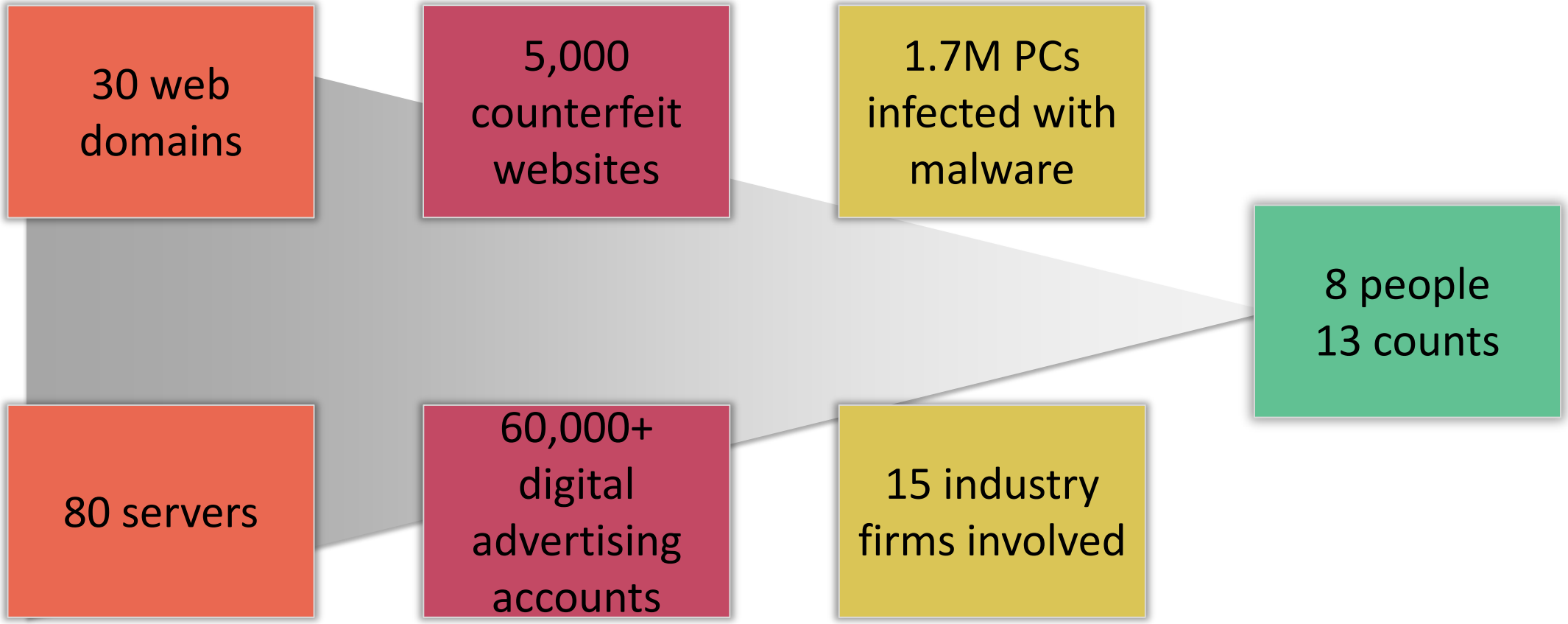
SAFETY Act

FERPA
Family Educational Rights and Privacy Act

PCI DSS
Payment Card Industry Data Security Standard

HIPAA
Health Insurance Portability and Accountability Act

Protecting consumers is a priority: 3ve & FBI



RSAConference2020

Being a Good Digital Citizen

Steps to protect & defend yourself, your family & your business from online manipulation

Basic tenets to being a good corporate digital citizen

1. **Know your digital supply chain**
2. **Identify/Research/Track *anything* new**
3. **Comply with industry best practices & regulations**
4. **Report suspicious activity**

Your Next Steps: Apply these learnings

30 DAYS	90 DAYS	120 DAYS
ASSEMBLE	**AUDIT**	**ENFORCE**
Digital Risk Tiger Team • Cross-department • Document needs	Digital environment • Quantify risks • Review contracts • Communicate expectations	Compliance • Flag violations • Correct errors • Apply legal weight

RSAConference2020

THANK YOU!

Stop the delivery mechanism.

Protect your business.

Enhance public safety.

Primum non nocere.

APPENDIX: Regulation & Industry Standards

- COPPA (Children's Online Privacy Protection Act) The Children's Online Privacy Protection Act ("COPPA") specifically protects the privacy of children under the age of 13 by requesting parental consent for the collection or use of any personal information of the users.
- Computer Fraud and Abuse Act, also known as the CFAA, is the federal anti-hacking statute that prohibits unauthorized access to computers and networks.
- SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by creating systems of risk and litigation management.
- PCI DSS is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.
- CCPA is a state statute intended to enhance privacy rights and consumer protection for residents of California, United States.
- GDPR is a new set of rules designed to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizens and businesses in the European Union can fully benefit from the digital economy.
- FERPA is a federal privacy law that gives parents certain protections with regard to their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules.
- HIPAA rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically.