All Points

MARS SUITE

Evolution of Cyber Attacks & Defending Against Cyber Adversaries

National Cyber Summit

September 22, 2022

www.allpointsllc.com

All Points Logistics

SDVOSB

CMMIDEV/3

Speaker Background

All Points
www.allpointsllc.com

Mark Dallmeier:

Industry Veteran, Researcher, President/CSO/CMO for Various Cyber & Risk Consulting Firms, MSSPs, MSPs.

- 27+ Years in the Industry
- Turn Around, Transformation Consultant
- CEO, President, CSO, CMO
- Serial Entrepreneur
- Board Director, Advisor
- Industry Researcher, Analyst, Speaker

HP
Hitachi Global Services
Verizon Business
XO Communications
Avnet
Qwest
3 Sigma
IT Partners
Sage Software
Stach & Liu
BishopFox
Terra Verde Security
Avertium
Vertek
Xceptional
New Genesis Solutions
All Points Logistics

Confidential

Previous Research, Presentations

2020 – 2022 (40+) Cyber, Risk, Compliance Trends & Best Practices Panels/Webinars

2019 Cybersecurity Trends, Best Practices:
"Cybersecurity & Compliance Trends in Healthcare" (AT&T Cybersecurity)
"Managing 3rd Party Vendor Risk" (ISC2 Phoenix)

2018, 2017 Cybersecurity Trends & Predictions:
"Cyber Attack Trends & Industry Predictions."
"Future Impact of the Equifax Breach."

2018, 2017, 2016 Phoenix SAC Conference:
"Beyond Ransomware"
"The Future of Ransomware."

2017, 2016 TribalNet:
"The Mind of a Hacker."
"Ransomware."

Disclaimer: The research, comments and opinions presented are the sole opinion of the presenter and do not represent the opinions of All Points Logistics

Conversation Set Up / Context

14,000+
Conversations
on Cyber, Risk,
Compliance

400+
Cyber, Risk,
Compliance
Customers
20,000+
Deployments

2000+
Assessments.
200+
CISO/CIO/CXO
Interviews

Trends

The more things change the more they appear to stay the same. Industries and organizations have nuances but most face similar challenges, issues.

Lessons

Failures, successes, best practices are valuable. Best practices can be shared, modified, and enhanced for various organizations to use across industries.

Observations

Many business, cyber, and risk executives have similar issues, experiences, opinions, outlooks, and biases.

Agenda

1 Evolution of Cyber Crime, Previous Attack Predictions

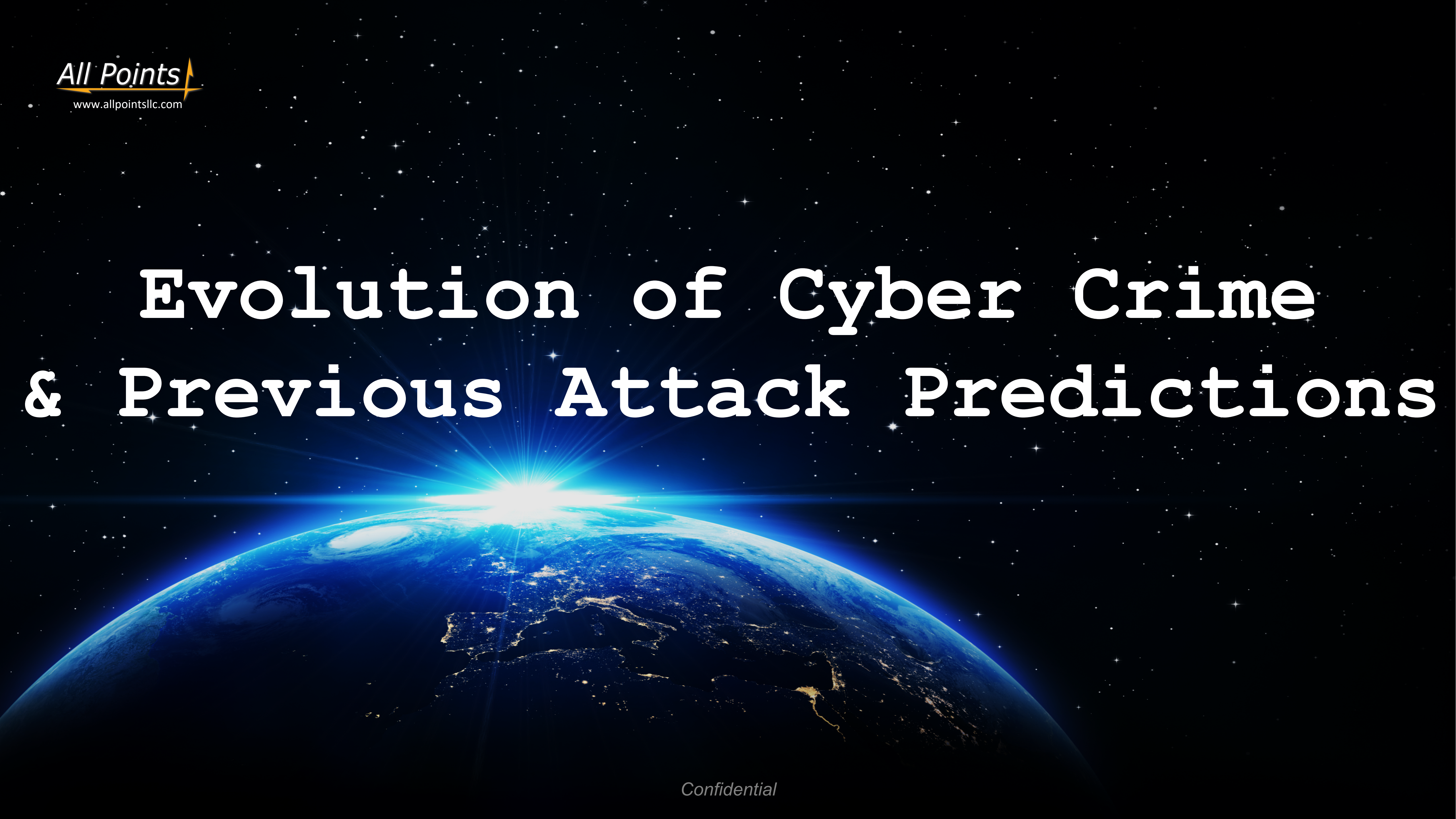
2 The Mind of the Hacker and Adversary

3 Evolution of Adversaries

4 Social Media Platforms & Risks

5 Current Protection & Defense Methods

6 Observations, Best Practices, Key Takeaways



Evolution of Cyber Crime & Previous Attack Predictions

Evolution of Cyber Crime + 201 Predictions

All Points
www.allpointsllc.com

RANSOM

Julius Ceasar, Chas Lindbergh Jr., John Paul Getty III
Frank Sinatra Jr.

1970's: Patty Hearst Kidnapping

2016-17: Ransomware + As a Service

2018 +: **As a Service** Factories

2018 & Beyond: Cyber Hostage Human, Physical, IT

LARCENY

1940s: Capone Mob Theft, Coercion Laundering

2016-17: BEC Targeting Tool Kit Integration

2018 +: **Cyber & Physical** Integration, Orchestration

2018 & Beyond: Criminal Enterprise 2.0

FRAUD

1930s: Victor Lustig Impersonation Counterfeiting

2016-17: BPC Cyber + Physical Attack Integration

2018 +: Business Disintermediation, Storefronts

2018 & Beyond: Business & Brandjacking

These Attacks Represent the Technical Weaponization of Criminal Acts that Have Been Around for Thousands of Years.

2017 Predictions Continued

Beyond:
Cyber Hostage
Human, Physical, IT

- *Targeting Business, Individuals, IT*
- *Utilizes IoT Exploits to Gain Full Situational Control:*
- *Physical Buildings, Transportation Devices w/ People Involved*
- *Acceptance of Various Payment Types*

Utilities, Research, Development, Manufacturing, Supply Chain:

- Systems down

- Access down

- Manufacturing down

- Communications controlled, down

Airplanes, Airports, Travel, Automobiles, Buses, other:

- Systems down

- Access down

- Travel down

- Communications controlled, down

Held hostage by hackers - latest computer virus infecting the valley | WDAZ

Buildings, Stadiums, Public Transportation, Logistics:

- Systems down

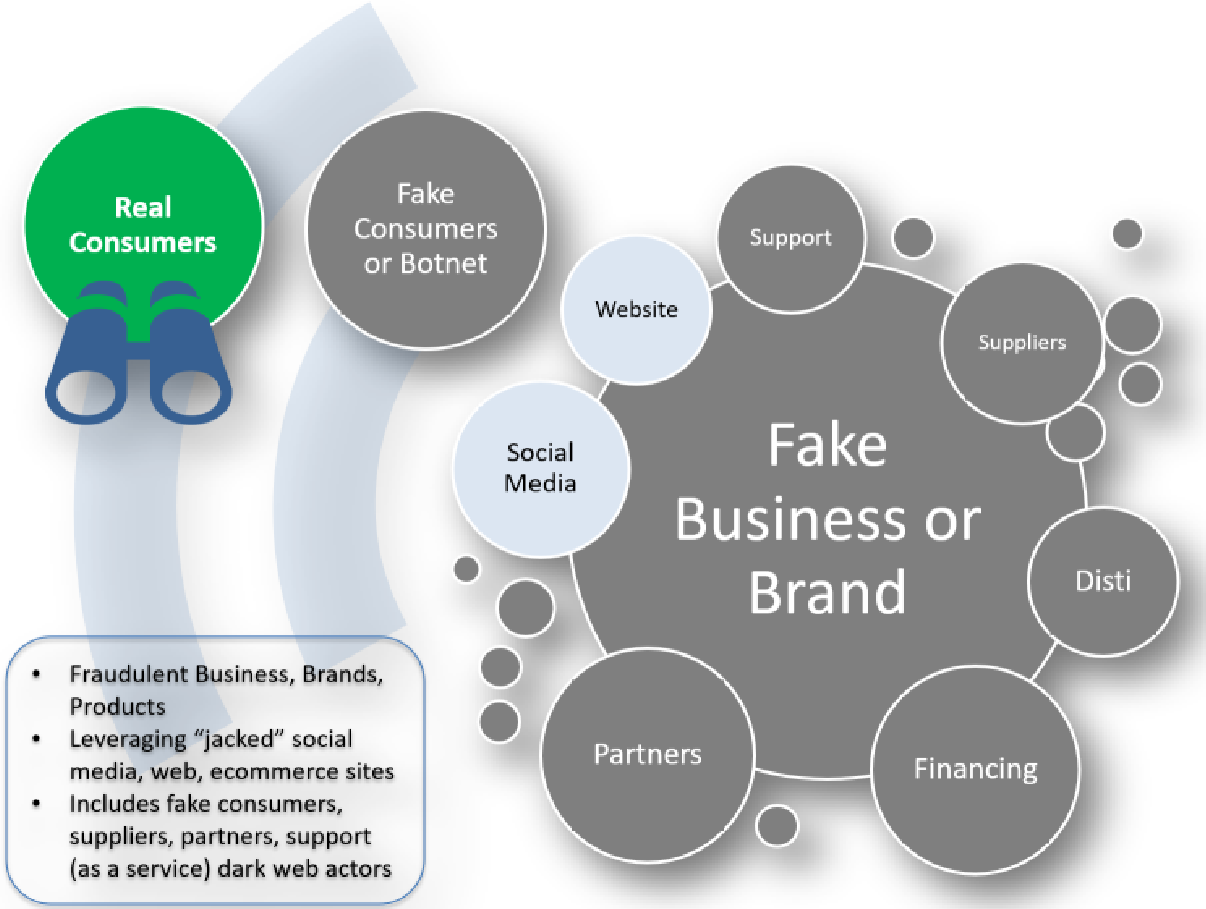
- Access down

- Travel down

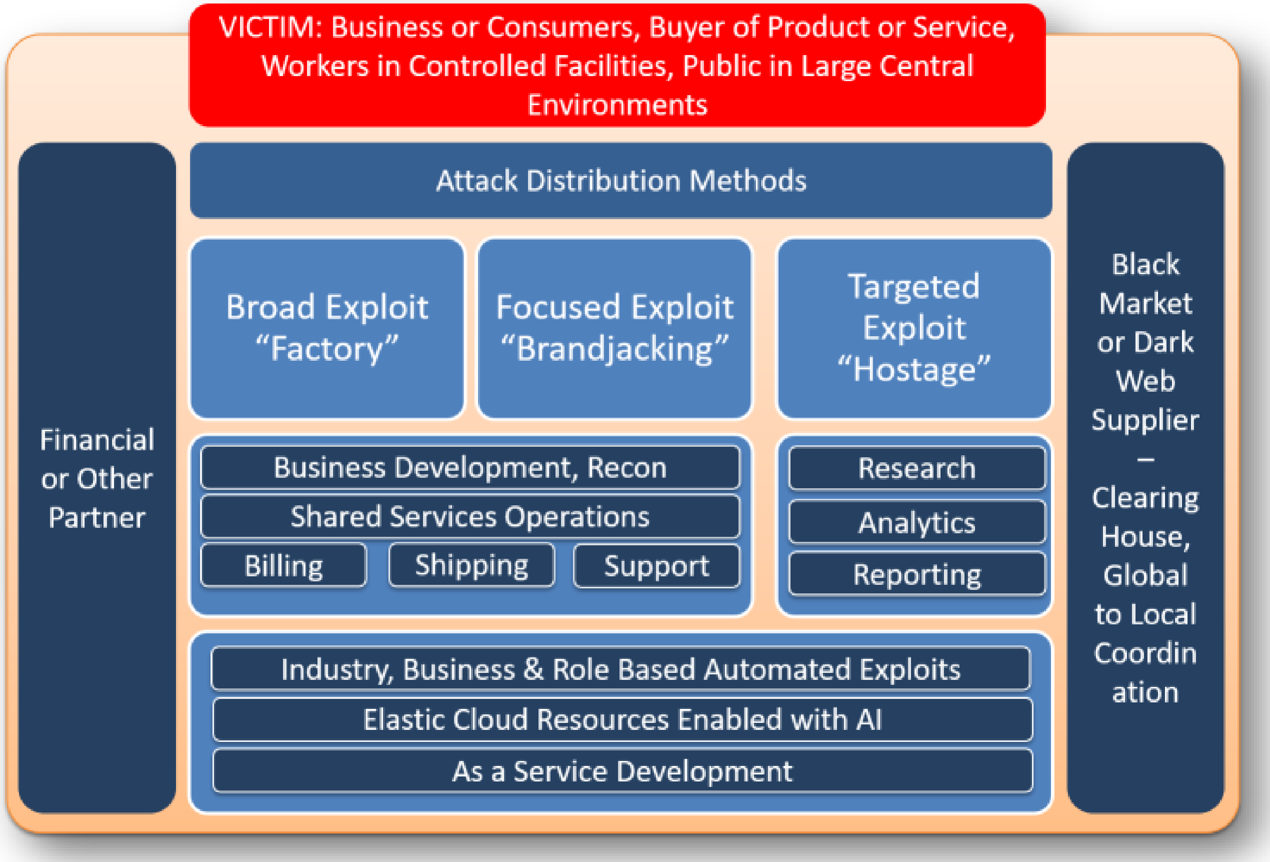
- Communications controlled, down

Evolution of Cyber Attacks & Dark Web 2018

All Points
www.allpointsllc.com



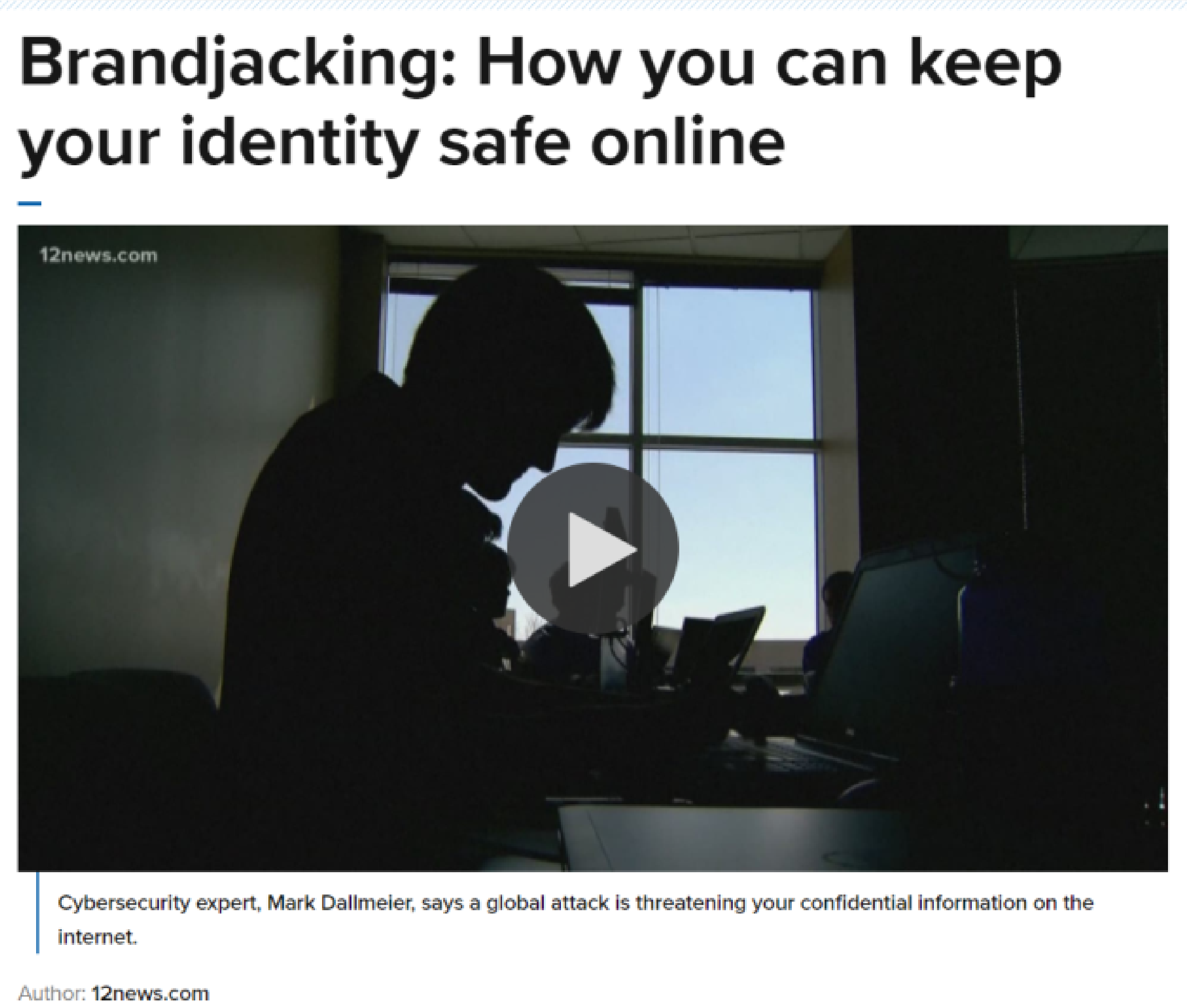
- Fraudulent Business, Brands, Products
- Leveraging "jacked" social media, web, ecommerce sites
- Includes fake consumers, suppliers, partners, support (as a service) dark web actors


VICTIM: Business or Consumers, Buyer of Product or Service, Workers in Controlled Facilities, Public in Large Central Environments
Financial or Other Partner
Attack Distribution Methods
Broad Exploit "Factory"
Focused Exploit "Brandjacking"
Targeted Exploit "Hostage"
Business Development, Recon
Shared Services Operations
Billing
Shipping
Support
Research
Analytics
Reporting
Industry, Business & Role Based Automated Exploits
Elastic Cloud Resources Enabled with AI
As a Service Development
Black Market or Dark Web Supplier – Clearing House, Global to Local Coordin ation

Brandjacking 2018 – Now Commonplace

AllPoints
www.allpointsllc.com

https://www.12news.com/video/news/local/brandjacking-how-you-can-keep-your-identity-safe-online/75-8106218

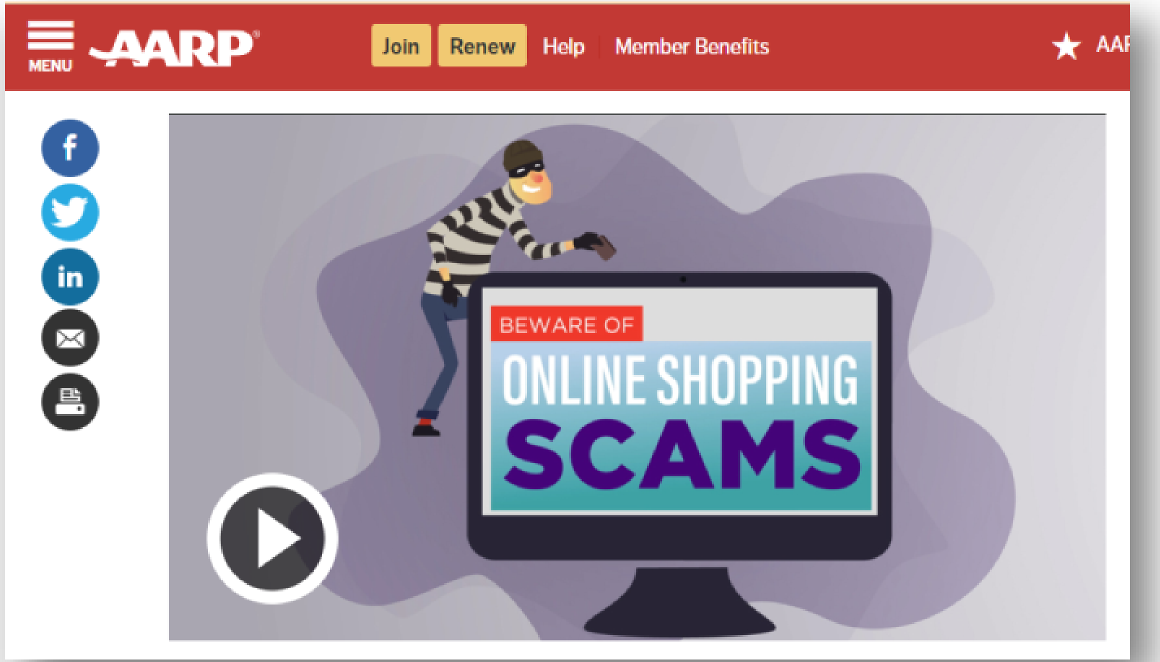


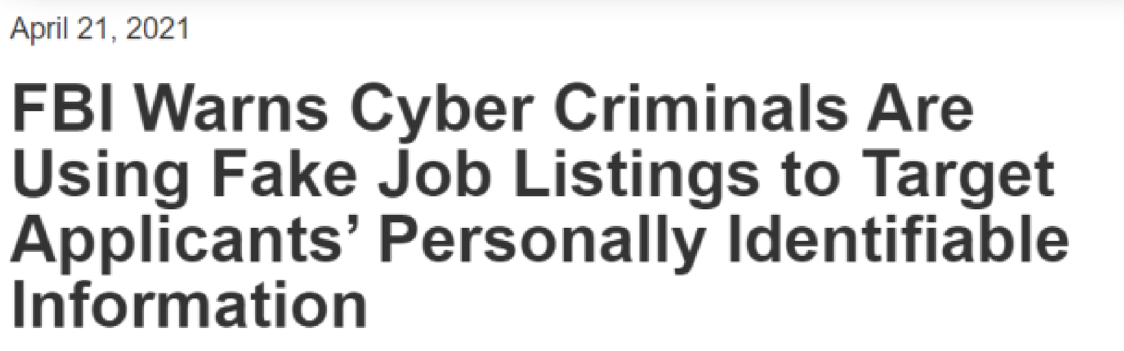
Brandjacking: How you can keep your identity safe online

Cybersecurity expert, Mark Dallmeier, says a global attack is threatening your confidential information on the internet.

Author: 12news.com

https://www.aarp.org/money/scams-fraud/info-2019/online-shopping.html



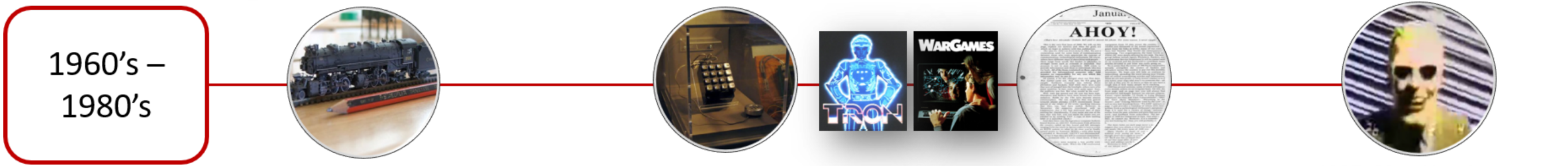


April 21, 2021

FBI Warns Cyber Criminals Are Using Fake Job Listings to Target Applicants' Personally Identifiable Information

Hacking Evolution Timeline, Propagation 1960-2018

All Points
www.allpointsllc.com



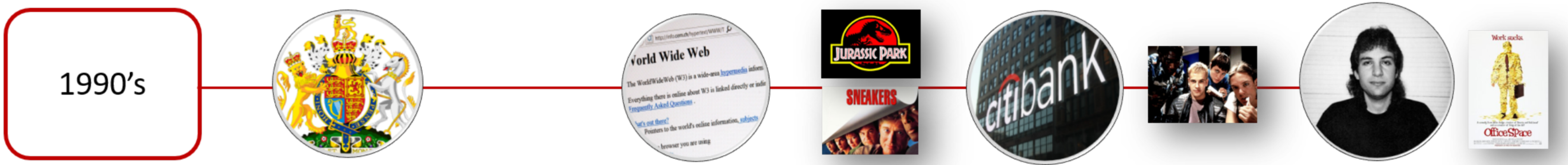
1960's – 1980's

1960: M.I.T.
Hacking Trains, Tech to enhance

1971: Blue Box
Telecom LD Hacking for free service

1984-86: 2600 Magazine
Hacker's Manifesto

1987: Max Headroom
Television broadcast hacking


World Wide Web
The WorldWideWeb (W3) is a wide-area hypermedia information
Everything there is online about W3 is linked directly or indirectly
Frequently Asked Questions
What's out there?
Pointers to the world's online information, subjects
browser you are using
Jurassic Park
Sneakers
citibank
Work sucks.
Office Space

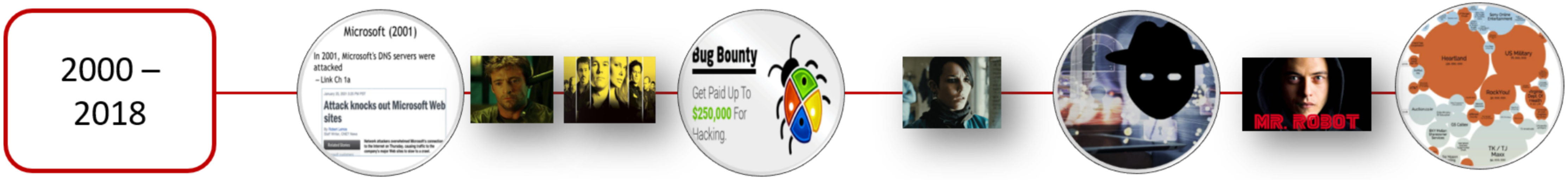
1990's

1990: U.K. Computer Misuse Act
Operation Sundevil

1991: Internet is Created

1994: Citibank Hacked

1995: Kevin Mitnik Arrested


Microsoft (2001)
In 2001, Microsoft's DNS servers were attacked
– Link Ch 1a
Attack knocks out Microsoft Web sites
Bug Bounty
Get Paid Up To $250,000 For Hacking.
Mr. Robot
Heartland
US Military
RockYou!
TK / TJ Maxx

2000 – 2018

2001-03: MSFT DDOS Attack
Formation of Anonymous

2003: MSFT Bounty

2013: 30K Websites
Hacked Daily

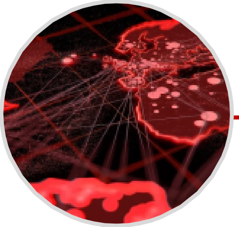
2014 – 18: Ebay, Target, Equifax,
EDGAR, IRS, Sony, Etc All Hacked
Hackers Get Hacked

Hacking Evolution Timeline, Propagation 2019-22

All Points
www.allpointsllc.com

2019 - 2022

2019: **Targeted Attacks** on Social Media, States, Education, Healthcare Labs, Manufacturers, Fed Agencies.

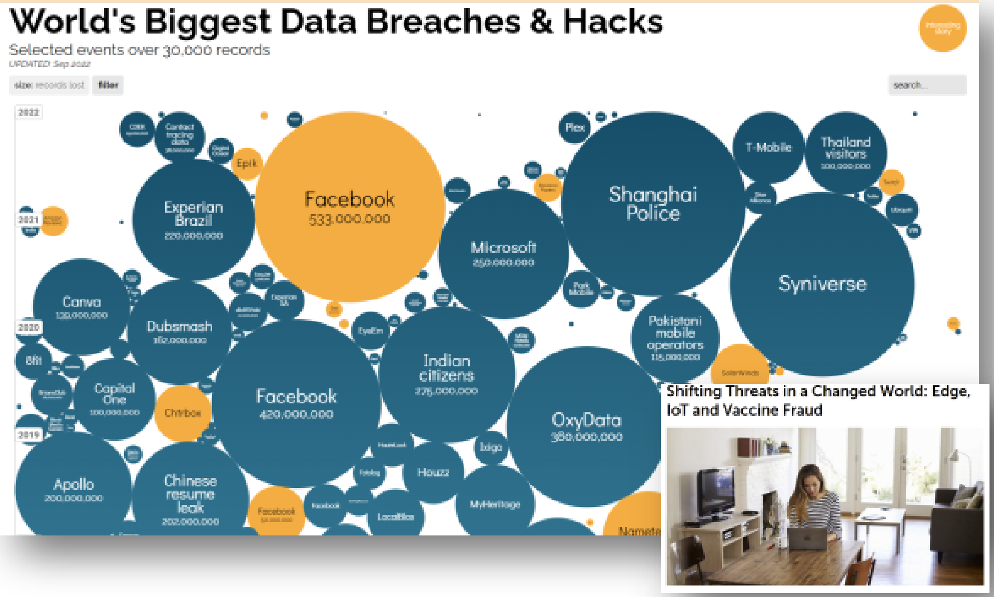


2020: Covid & Election Mis-Dis-Mal Information & Fraud Attacks. Remote Workers, Clinics, Supply Chain, Election Site Attacks.

2021: Ransomware, Extortion, BEC, Phishing, Critical Infrastructure, Water, Pipeline, Supply Chain, Media, Remote Workers.

2022: Targeted & Orchestrated DDoS, Botnet, Ransomware, Phishing on Ukraine, U.S., Allies, Business, General Public

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



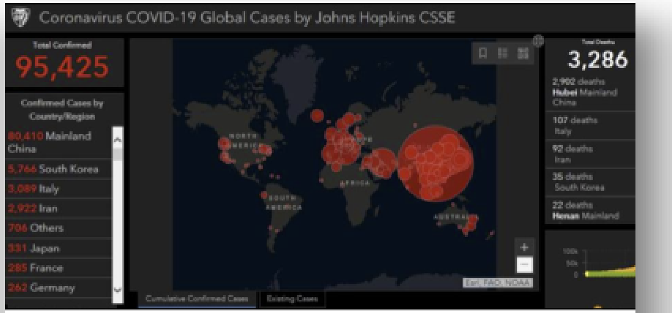
World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Sep 2022

Shifting Threats in a Changed World: Edge, IoT and Vaccine Fraud

https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf



Coronavirus COVID-19 Global Cases by Johns Hopkins CSSE

Total Confirmed 95,425

Confirmed Cases by Country/Region

80,410	Mainland China
5,766	South Korea
3,089	Italy
2,922	Iran
706	Others
331	Japan
285	France
262	Germany

Total Deaths 3,286

2,902 deaths Hubei Mainland China

107 deaths Italy

92 deaths Iran

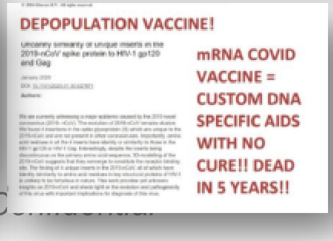
35 deaths South Korea

22 deaths Henan Mainland

Figure 13 - Fake COVID map used in phishing to deliver malware

Figure 1 – Timeline of cyber-attacks on Ukraine

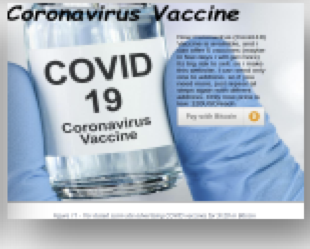
Source: Data compiled by EPRS; Graphic by Lucille Killmayer.



DEPOPULATION VACCINE!

Uncanny similarity of unique inserts in the 2019-nCoV spike protein to HIV-1 gp120 and Gag

mRNA COVID VACCINE = CUSTOM DNA SPECIFIC AIDS WITH NO CURE!! DEAD IN 5 YEARS!!



Coronavirus Vaccine

The Mind of Hackers & Adversaries

All Points
www.allpointsllc.com

WHAT MOTIVATES

WHITE HAT	GRAY HAT	BLACK HAT	CRIMINALS	INSIDERS
Desire to Learn	Desire to Protect	Self Gratification	Malicious Intent	Revenge
Desire to Protect	Altruistic Reason	Ideology	Personal Gain	Personal Gain
Altruistic Purpose	Desire to Learn	Personal Gain	Entitlement	Espionage

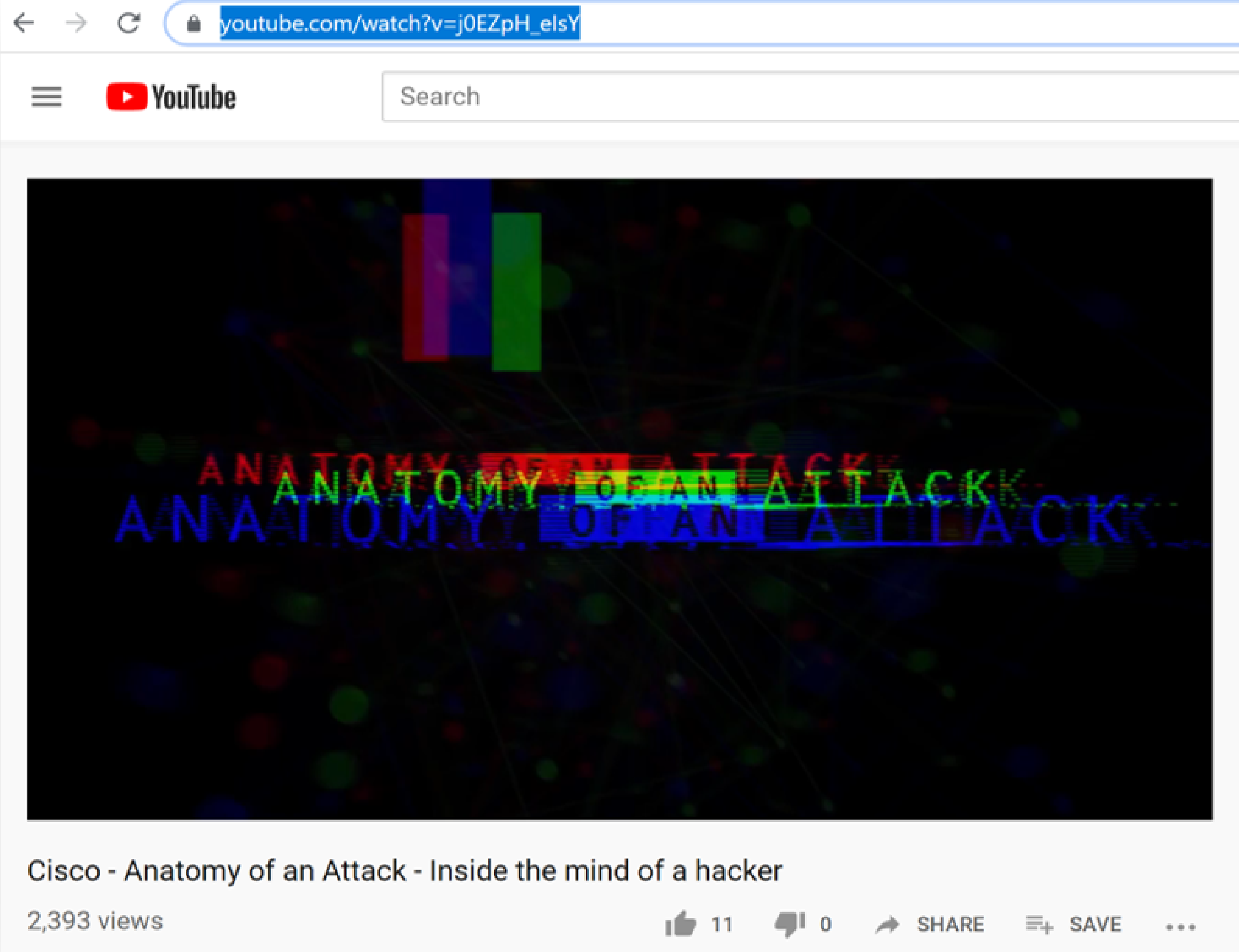
WHAT DRIVES BEHAVIOR

WHITE HAT	GRAY HAT	BLACK HAT	CRIMINALS	INSIDERS
Altruistic Purpose	Personal Ideology	Self Gratification	Personal Gain	Personal Gain
Desire to Protect	Altruistic Reason	Personal Gain	Malicious Intent	Entitlement
Desire to Learn	Desire to Protect	Malicious Intent	Ideology	Revenge

Inside the Mind of a Hacker

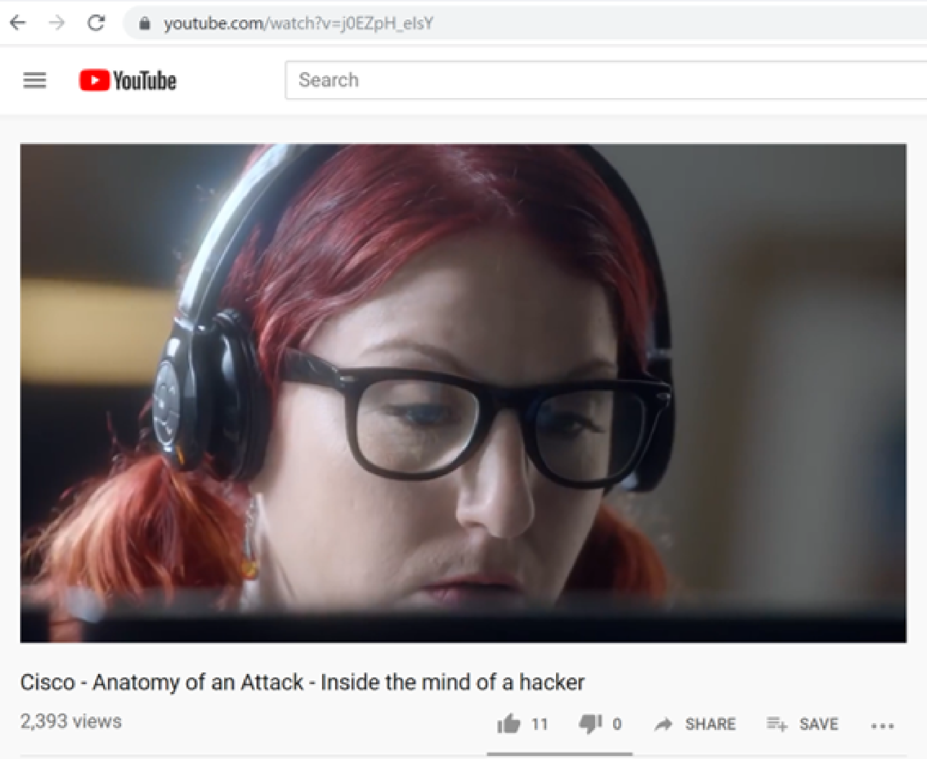
All Points
www.allpointsllc.com

https://www.youtube.com/watch?v=j0EZpH_eIsY


youtube.com/watch?v=j0EZpH_eIsY

Cisco - Anatomy of an Attack - Inside the mind of a hacker

2,393 views


youtube.com/watch?v=j0EZpH_eIsY

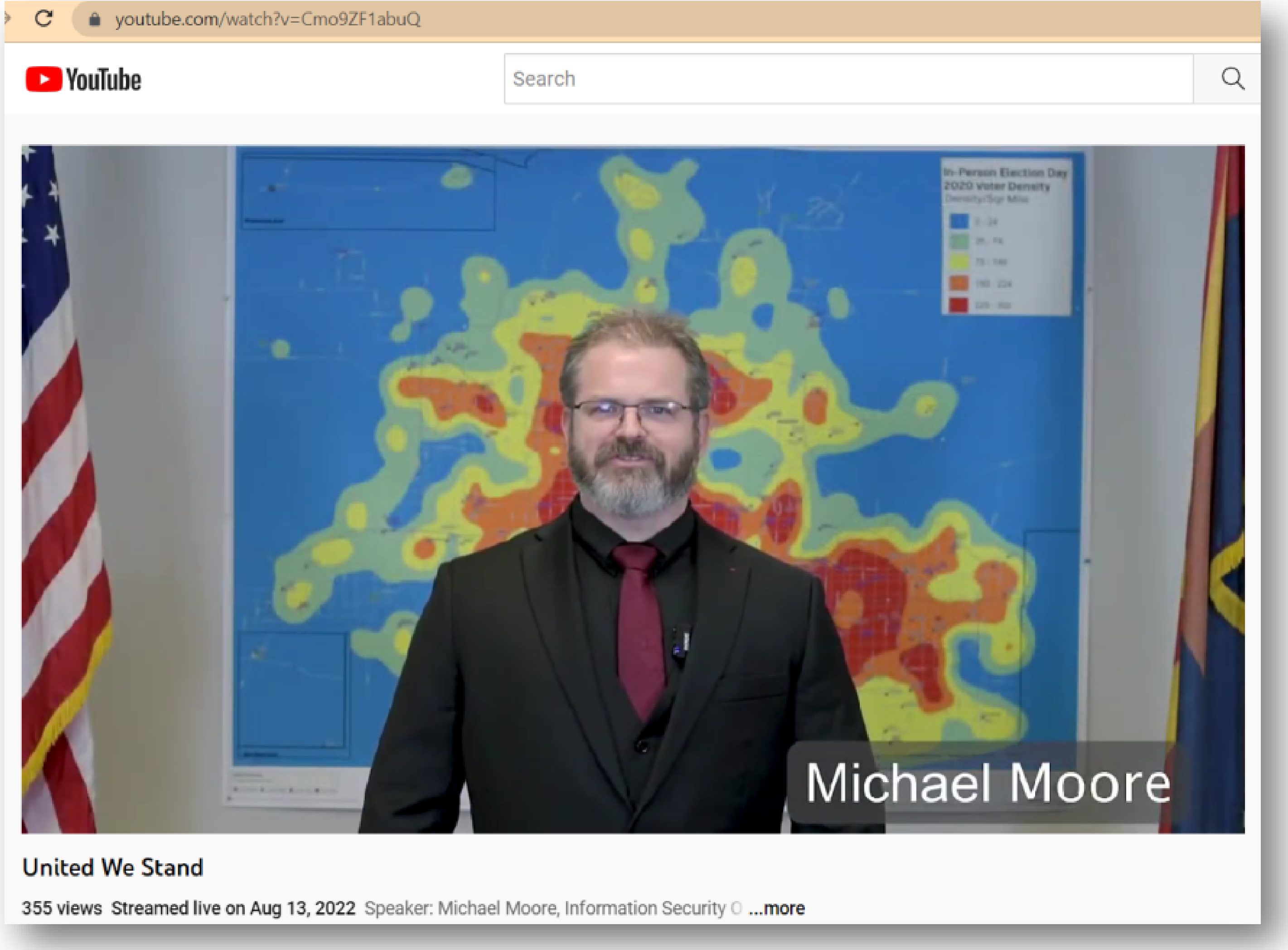
Cisco - Anatomy of an Attack - Inside the mind of a hacker

2,393 views

A great video from Cisco Systems illustrating the Anatomy of an Attack and includes the thoughts of one of the hacker team members that completed the reconnaissance on the company.

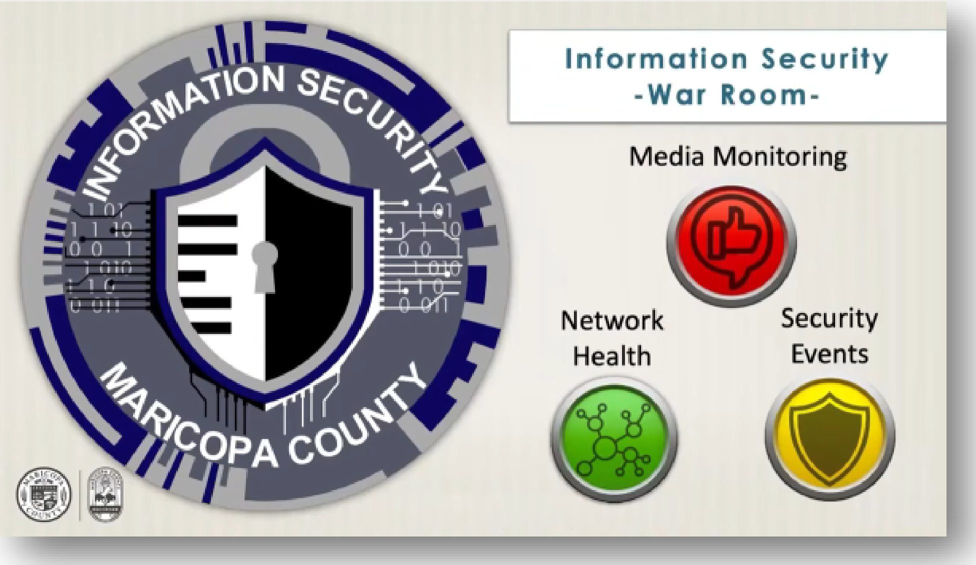
Growth of Mis-Dis-Mal-information

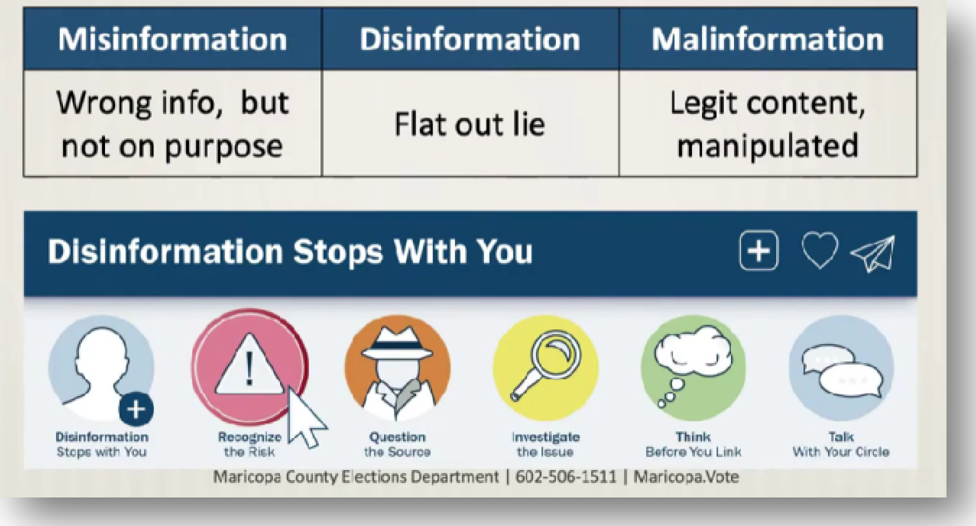
https://www.youtube.com/watch?v=Cmo9ZF1abuQ


youtube.com/watch?v=Cmo9ZF1abuQ
YouTube
Search
In-Person Election Day 2020 Voter Density
Michael Moore

United We Stand

355 views Streamed live on Aug 13, 2022 Speaker: Michael Moore, Information Security O ...more





Misinformation	Disinformation	Malinformation
Wrong info, but not on purpose	Flat out lie	Legit content, manipulated

Disinformation Stops With You

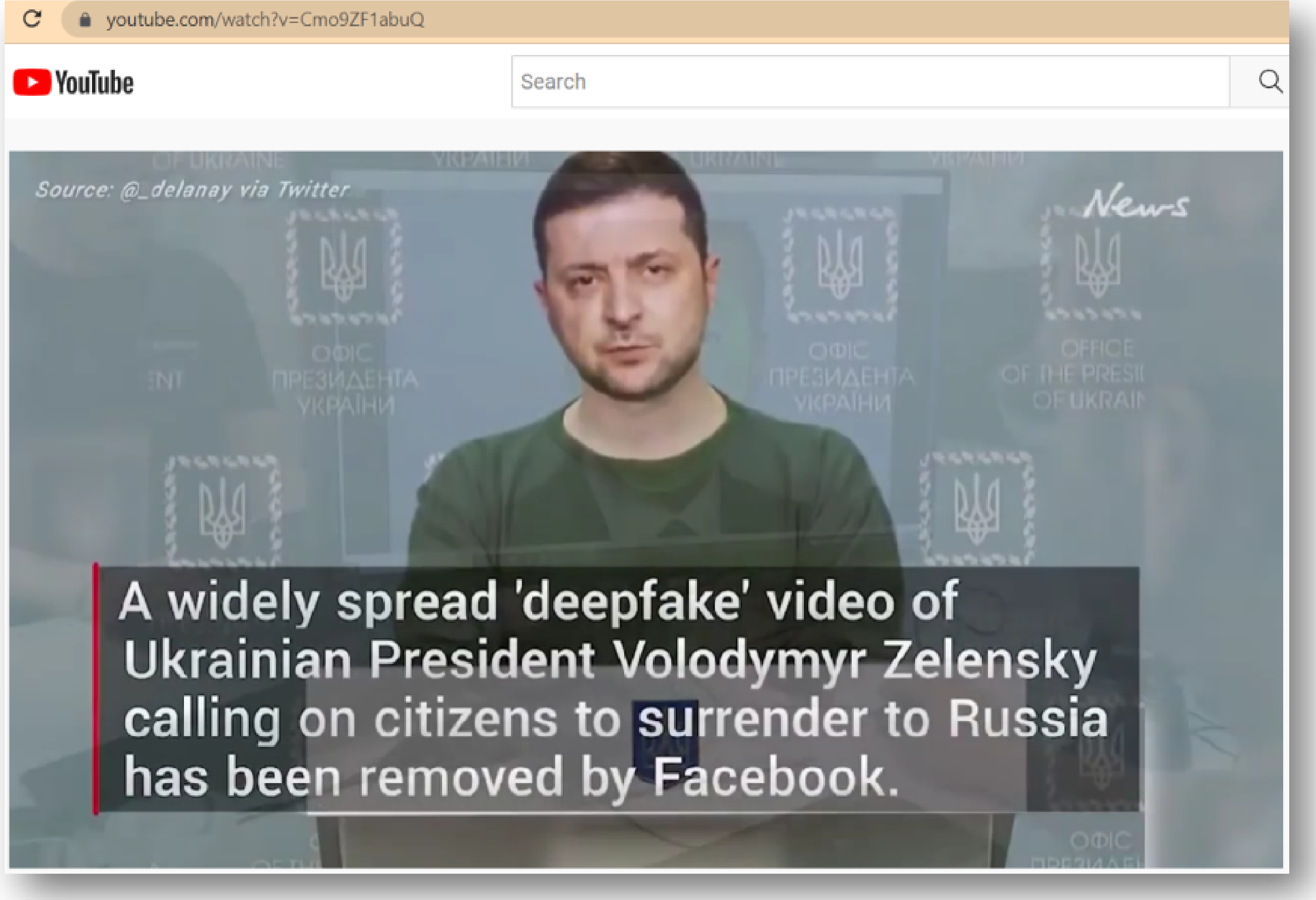
Disinformation Stops with You
Recognize the Risk
Question the Source
Investigate the Issue
Think Before You Link
Talk With Your Circle

Maricopa County Elections Department | 602-506-1511 | Maricopa.Vote

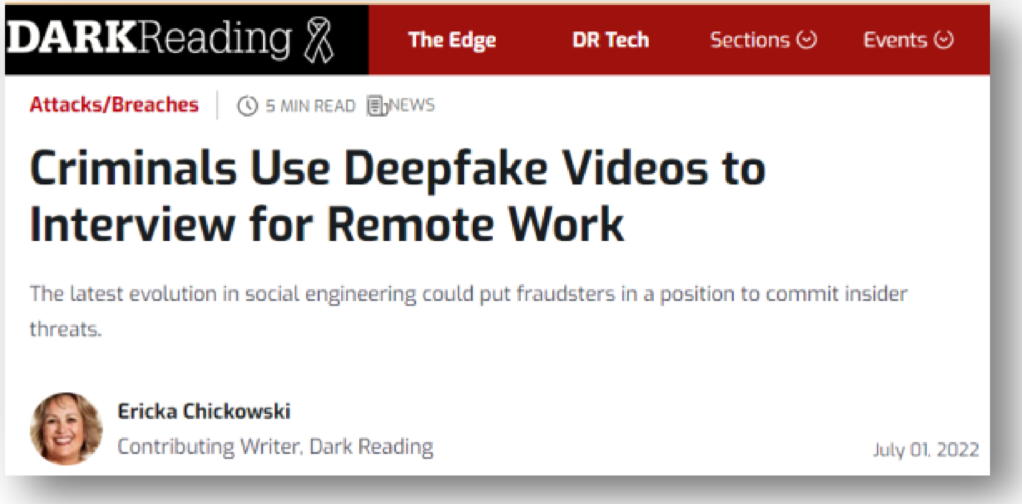
Growth of Synthetic Content, Deepfakes

All Points
www.allpointsllc.com

https://www.youtube.com/watch?v=Cmo9ZF1abuQ


youtube.com/watch?v=Cmo9ZF1abuQ
YouTube
Search
Source: @_delanay via Twitter
News

A widely spread 'deepfake' video of Ukrainian President Volodymyr Zelensky calling on citizens to surrender to Russia has been removed by Facebook.



Criminals Use Deepfake Videos to Interview for Remote Work

The latest evolution in social engineering could put fraudsters in a position to commit insider threats.

Ericka Chickowski
Contributing Writer, Dark Reading

July 01, 2022

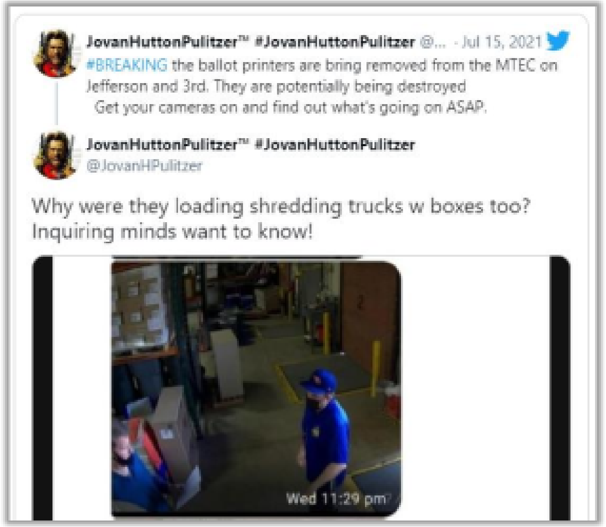
Evolution of Adversaries

1. Nation States
2. White Hats
3. Gray Hats
4. Black Hats
5. Hacktivists
6. Cyber Criminal Syndicates
7. Opportunists/Public (Ideology Driven & Malicious)

Observation

This is not just a technology war. We are fighting against embedded human behavior and ideologies.

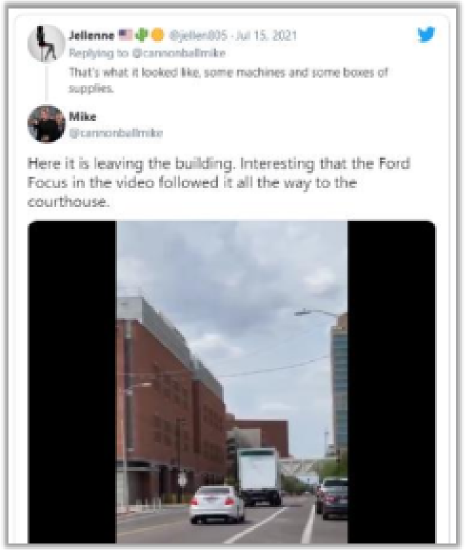
New Adversaries on Social Media = New Threats, Risks


JovanHuttonPulitzer™ #JovanHuttonPulitzer @... · Jul 15, 2021

#BREAKING the ballot printers are bring removed from the MTEC on Jefferson and 3rd. They are potentially being destroyed
 Get your cameras on and find out what's going on ASAP.

JovanHuttonPulitzer™ #JovanHuttonPulitzer
@JovanHPulitzer

Why were they loading shredding trucks w boxes too? Inquiring minds want to know!


Jellenne 🇺🇸🌵🟡 [redacted] · Jul 15, 2021
Replying to [redacted]

That's what it looked like, some machines and some boxes of supplies.

Mike
[redacted]

Here it is leaving the building. Interesting that the Ford Focus in the video followed it all the way to the courthouse.

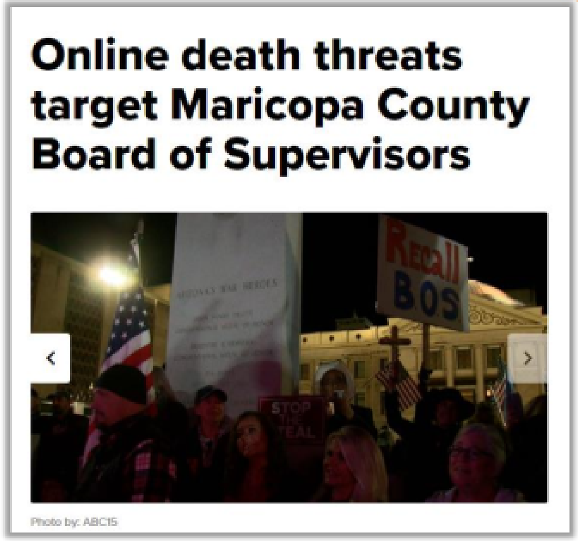
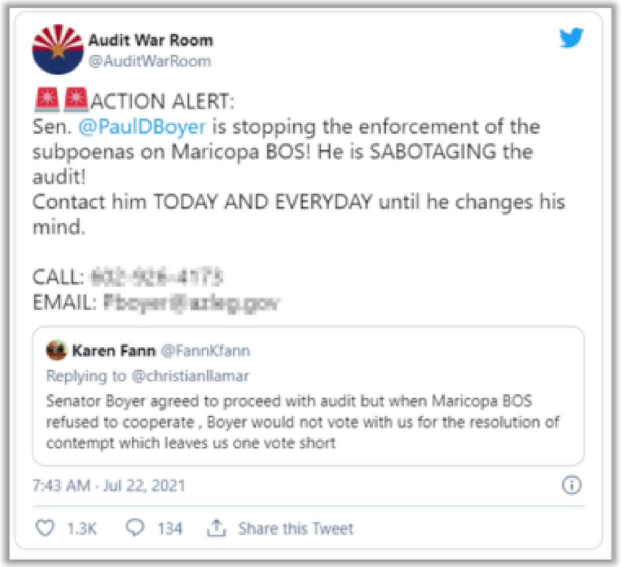

Online death threats target Maricopa County Board of Supervisors

Photo by: ABC15


Audit War Room
@AuditWarRoom

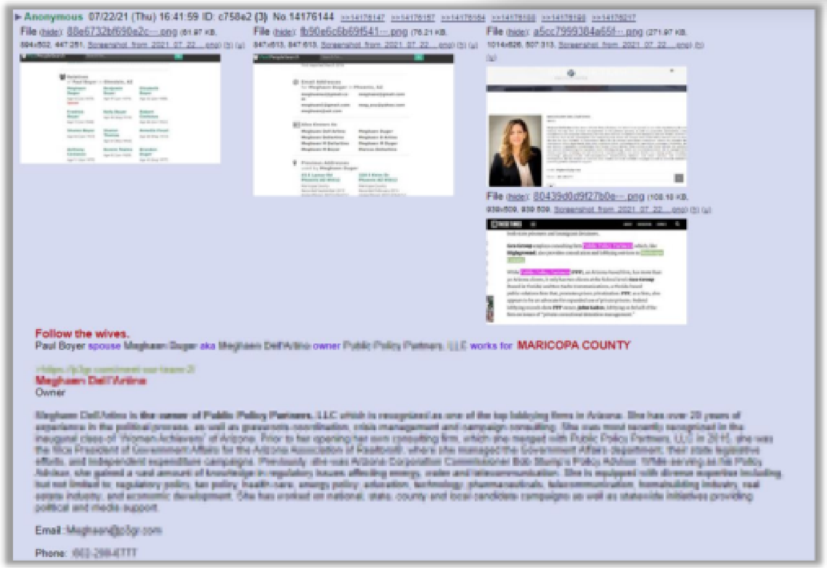
🚨🚨ACTION ALERT:
Sen. @PaulDBoyer is stopping the enforcement of the subpoenas on Maricopa BOS! He is SABOTAGING the audit!
Contact him TODAY AND EVERYDAY until he changes his mind.

CALL: [redacted]
EMAIL: [redacted]

> Karen Fann @FannKfann
> Replying to @christianllamar
>
> Senator Boyer agreed to proceed with audit but when Maricopa BOS refused to cooperate , Boyer would not vote with us for the resolution of contempt which leaves us one vote short

7:43 AM · Jul 22, 2021

♡ 1.3K 134 Share this Tweet


▸ Anonymous 07/22/21 (Thu) 16:41:59 ID: c758e2 (3) No.14176144 >>14176147 >>14176157 >>14176164 >>14176169 >>14176180 >>14176217

File (hide): 88e6732bf690e2c---.png (61.97 KB, 694x502, 847:251, Screenshot from 2021-07-22 ... .png) (f) (u)

File (hide): fb90e6c6b69f541---.png (76.21 KB, 847x613, 847:613, Screenshot from 2021-07-22 ... .png) (f) (u)

File (hide): a5cc7999384a65f---.png (271.97 KB, 1014x626, 507:313, Screenshot from 2021-07-22 ... .png) (f) (u)

File (hide): 80439d0d9f27b0e---.png (108.16 KB, 939x509, 939:509, Screenshot from 2021-07-22 ... .png) (f) (u)

Follow the wives.
Paul Boyer spouse [redacted] aka [redacted] owner [redacted] works for MARICOPA COUNTY

[redacted]
Owner

[redacted]

Email: [redacted]

Phone: [redacted]

- ✓ Maricopa Election Audit drove social media support
- ✓ Served to rally conspiracy theorists
- ✓ Used for donations
- ✓ Routinely posted unofficial findings
- ✓ Armed Citizens tracking and reporting on ballot movement
- ✓ Threats being made to officials
- ✓ Attack planning against spouses, families

Social Media Platforms & Risk Realities

1. **Not only a measure of engagement, sentiment…but**
2. **Brands and reputations are being targeted, impacted**
3. **Is leveraged for targeting, planning, mobilization**
4. **Can be a rich source of intelligence**

- ✓ *Cyber threats*
- ✓ *Kinetic threats*
- ✓ *Adversarial intent*
- ✓ *Threat actor identification*

All Points
www.allpointsllc.com

- ✓ Social media is a business
- ✓ Profit is driven by user engagement, data
- ✓ Conflict = more engagement, data
- ✓ Can be used to drive negative sentiment
- ✓ Nation-states have employed social media with great effect
- ✓ It is easier to hack minds than computers…"We will defeat you from within".

All Points
www.allpointsllc.com

Current Protection & Defense Methods

Protection & Defense Methods

1. **Assets & Players:** *Validate Assets, Identities*
2. **Lock the Doors, Windows:** *Email, Network, Cloud, Data*
3. **Control the Assets:** *Vuln, Config, Access*
4. **Backup the Business:** *BCDR, Immutable BU*
5. **Always be Watching:** *SIEM/SOC/Automation*
6. **Program Procedures:** *Legal, Compliance, Training*
7. **Governance:** *Tops Down, Bottoms Up, Cross Matrix*

- ✓ Hacking the Human is pervasive; SETA is commonplace
- ✓ MFA has become required for cyber insurance coverage
- ✓ Layered approach to security is needed
- ✓ Zero Trust approach is required

- ✓ How are we addressing new adversaries, social media risks, threats?

Questioning the Status Quo

1. **Assets & Players:** *Asset Inventory & Identity Management*
2. **Lock the Doors, Windows:** *Air Gapped, Segmentation, Quantum Encryption*
3. **Control the Assets:** *Configuration Standards, Vulnerability Prioritization, MFA*
4. **Backup the Business:** *Operations & IT Continuity, Simulations*
5. **Always be Watching:** *Social Media, Physical, Geo, 3rd Party, Mining - Intelligence*
6. **Program Procedures:** *Financial, Operations, Suppliers, Partners*
7. **Governance:** *Cyber Declaration-Culture, Mastering Change Management*

Observations, Best Practices, Key Takeaways

Observations

1. Cyber Criminal Industrial Revolution is Underway & Accelerating
2. 2024 Election Could Be Worse Thank 2020 – Increased Polarization, Attacks
3. Continue to Track, Monitor, be Mindful of Emerging Adversaries
4. Watch for Brandjacking, Social Media Mobilization from Adversaries
5. Investigate Social Media Crawling Tools to Track Adversary Activities
6. Use Artificial Intelligence to Sort, Analyze Social Media & Large Pools of Data
7. Training, Skill Development, Counseling for Social Media Threat Hunting, Analysis

Best Practices

ACKNOWLEDGE TRENDS

- □ Hacking the Human Works – Phishing/Social Engineering Attacks, Losses Are Growing.
- □ Ransomware & Malware Attacks Are Pervasive.
- □ Scans & Attacks Are Automated 24/7/365.
- □ Once Breached, Attacks Increase.
- □ No Org is Too Small To Be Attacked.
- □ Cyber Insurance Coverage is Not a Viable Strategy - is More Costly & Difficult to Attain.

HOW TO BEGIN

- □ **Program:** Deploy a Cyber Plan/Program/Resources with Communication Plan.
- □ **Patch:** Scan and Update Systems/Vuln Management.
- □ **People:** Train, Educate, Incent Employees, Counseling for Infosec.
- □ **Passwords:** Update, Change and Manage Passwords.
- □ **Zero Trust Approach** to IT Network/System Access.
- □ **Secure and Harden** IT Systems/Applications.

PROGRAM

- □ Zero Trust with Multi-Factor Authentication.
- □ Continuous Monitoring, Detection, Alerting, Response to Risks, Threats, Attacks.
- □ Social Media Review, Intel Gathering, Monitoring.
- □ Inventory, Scan, Patch, Fix or Remove Old Systems.
- □ Train, Educate, Phish, Incent People.
- □ Encrypt Data.
- □ Corporate-Wide & 3rd Party Scans, Assessments.

TRUSTED PARTNERS

- □ Managed Threat Detection, Alerting, & Response (SIEM, SOC).
- □ End Point Detection & Response (Anti-Malware, Anti-Ransomware).
- □ Security and Risk Assessments.
- □ Backup as a Services.
- □ Security as a Service.
- □ Compliance as a Service.
- □ Managed IT Services.

The first step in reducing the risk of a cyber-attack, data breach, or compliance action is to acknowledge the trends and the realities impacting your industry. Employees and 3rd Party Vendors are the weakest links in terms of data privacy and cybersecurity and are being targeted by cybercriminals and hackers. **The next critical step is to deploy a data privacy and cybersecurity plan and program that includes implementing continuous risk, threat, and attack monitoring, detection, and response capability inside your organization**. *This enables visibility into real-time risks and threats and provides specialized resources and support to remove and remediate threats.*

Key Takeaways – Next 6 Months

1 Determine Capabilities/Gaps Around Best Practices + Social Media Monitoring

2 Engage with Executives, Educate on Best Practices & Emerging Risks

3 Update BCDR/IR Plans, Protocols to Address Ransom, Extortion, BEC, Social Media & Physical Attacks and Risks

4 Watch for Brandjacking, Social Media Mobilization from Adversaries

5 Document & Report the Team's Progress & Positive Impact on the Organization

6 Continue to Assess, Refine Capabilities Including Social Media Risk Monitoring

Questions? Thank You!
Visit us at Booth 613

National Cyber Summit

September 22, 2022