Eat’n Park OSINT

By Eric Miller and Zarek Rush
For Emerging Topics in Cybersecurity (CYBS-4360-A),
Robert Morris University

Intro

- Open Source Intelligence (OSINT) - The gathering of publicly available information and data for any kind of intelligence purpose.
- Done to understand an organization's security landscape better, how it handles risks, and defend against attacks.
- Our group consisting of Eric Miller and Zarek Rush conducted an OSINT assessment against Eat’n Park.
- This assessment will include information gathered from online tools, websites, and in person gatherings to gather as much information as possible from every angle.

Rationale

- Family-Owned Local company with large amounts of locations.
  - Not as knowledgeable in security standards
  - Large attack surface
  - Not as much money to spend on security as big companies
- Over 8,000 employees.
  - Higher employee amount means higher change of social engineering attacks being successful
- Easily accessible to conduct in person OSINT reconnaissance.

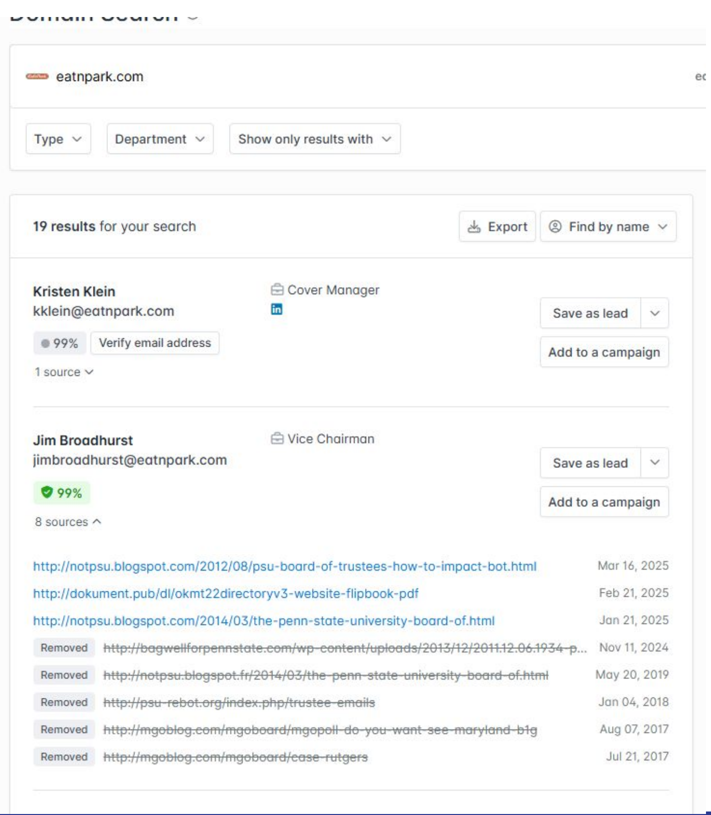
Methodology

- Physical
    - Acting as a regular customer use tools such as bluetooth scanners and Wi-Fi scanners.
- Digital
    - Use websites and tools such as Hunter.io, Nikto, URLscan, and Hudson Rock to discover publicly available information about Eat’n Park and it’s security landscape.

Targets

- Known problems in security.
- Employee email addresses.
  - For social engineering attacks or involvement in data breaches
- Weakness in Wi-Fi security or bluetooth devices.
  - Such as weak or default passwords
- Known Eat’n Park systems.
  - See if any exploits exist for them

Information Gathered - Hunter.io



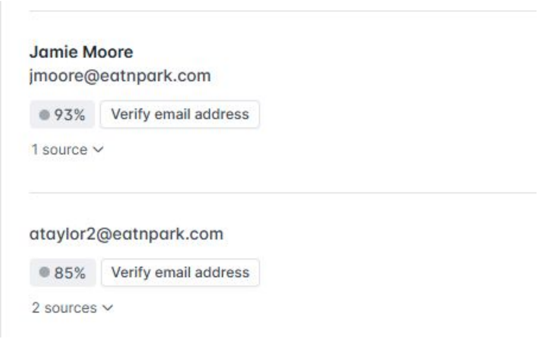
eatnpark.com

19 results for your search

Kristen Klein — Cover Manager
kklein@eatnpark.com
99%
1 source

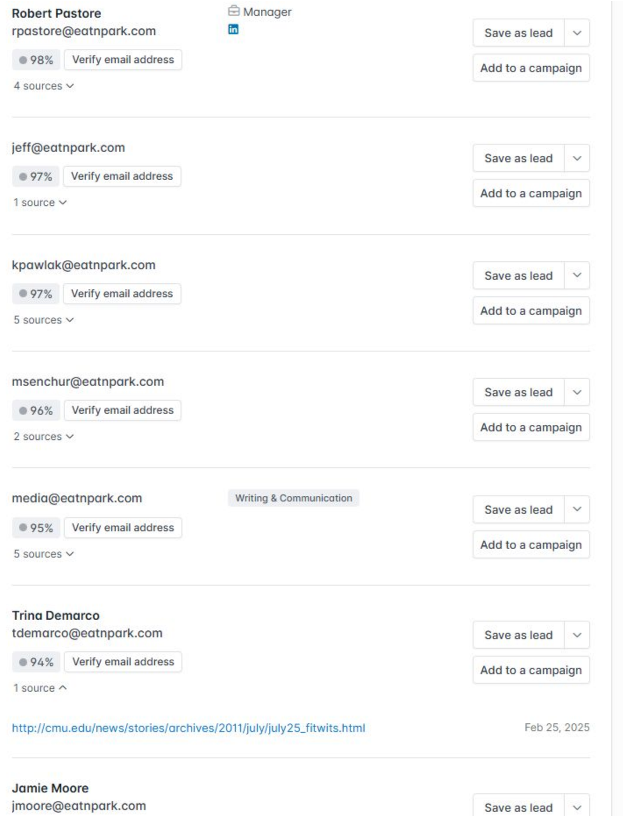
Jim Broadhurst — Vice Chairman
jimbroadhurst@eatnpark.com
99%
8 sources

	http://notpsu.blogspot.com/2012/08/psu-board-of-trustees-how-to-impact-bot.html	Mar 16, 2025
	http://dokument.pub/dl/okmt22directoryv3-website-flipbook-pdf	Feb 21, 2025
	http://notpsu.blogspot.com/2014/03/the-penn-state-university-board-of.html	Jan 21, 2025
Removed	~~http://bagwellforpennstate.com/wp-content/uploads/2013/12/2011.12.06.1934-p...~~	Nov 11, 2024
Removed	~~http://notpsu.blogspot.fr/2014/03/the-penn-state-university-board-of.html~~	May 20, 2019
Removed	~~http://psu-rebot.org/index.php/trustee-emails~~	Jan 04, 2018
Removed	~~http://mgoblog.com/mgoboard/mgopoll-do-you-want-see-maryland-b1g~~	Aug 07, 2017
Removed	~~http://mgoblog.com/mgoboard/case-rutgers~~	Jul 21, 2017



Jamie Moore
jmoore@eatnpark.com
93%
1 source

ataylor2@eatnpark.com
85%
2 sources



Robert Pastore — Manager
rpastore@eatnpark.com
98%
4 sources

jeff@eatnpark.com
97%
1 source

kpawlak@eatnpark.com
97%
5 sources

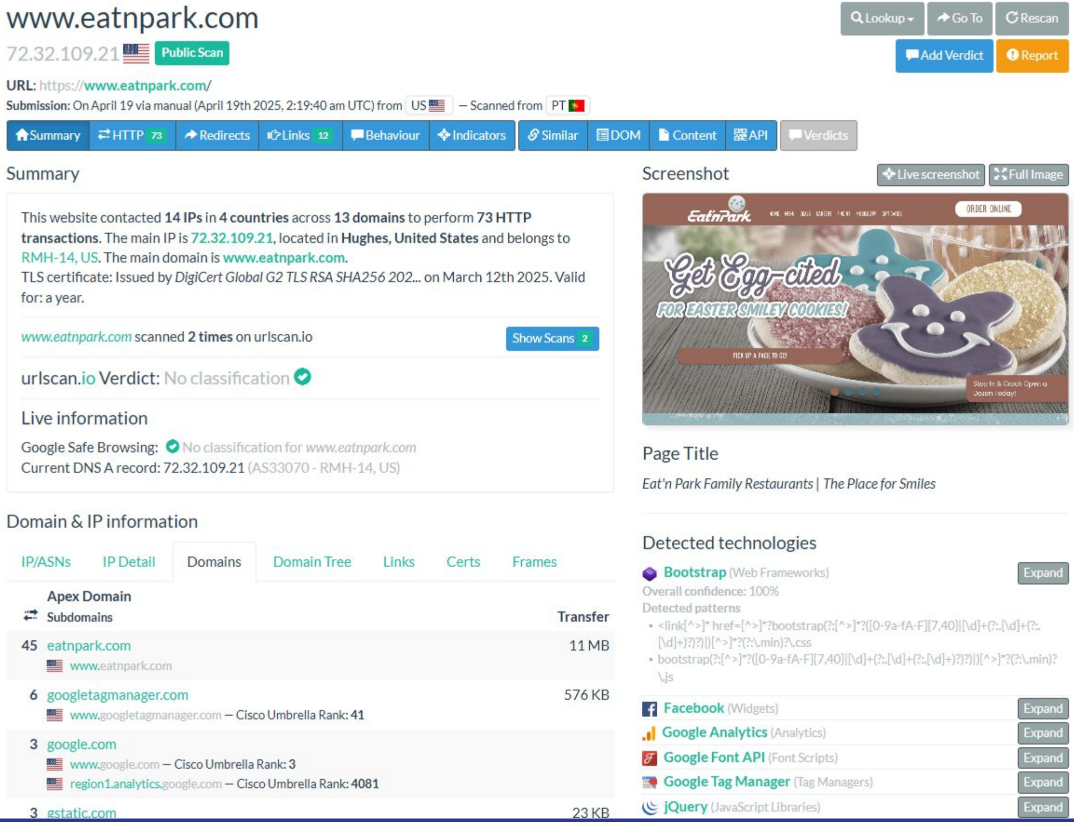
msenchur@eatnpark.com
96%
2 sources

media@eatnpark.com — Writing & Communication
95%
5 sources

Trina Demarco
tdemarco@eatnpark.com
94%
1 source
http://cmu.edu/news/stories/archives/2011/july/july25_fitwits.html — Feb 25, 2025

Jamie Moore
jmoore@eatnpark.com

Information Gathered - URLscan



www.eatnpark.com

72.32.109.21 Public Scan

URL: https://www.eatnpark.com/

Submission: On April 19 via manual (April 19th 2025, 2:19:40 am UTC) from US — Scanned from PT

Summary

This website contacted **14 IPs** in **4 countries** across **13 domains** to perform **73 HTTP transactions**. The main IP is 72.32.109.21, located in **Hughes, United States** and belongs to RMH-14, US. The main domain is www.eatnpark.com.
TLS certificate: Issued by *DigiCert Global G2 TLS RSA SHA256 202...* on March 12th 2025. Valid for: a year.

www.eatnpark.com scanned **2 times** on urlscan.io

urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *www.eatnpark.com*
Current DNS A record: 72.32.109.21 (AS33070 - RMH-14, US)

Screenshot

Page Title

Eat'n Park Family Restaurants | The Place for Smiles

Domain & IP information

	Apex Domain Subdomains	Transfer
45	eatnpark.com www.eatnpark.com	11 MB
6	googletagmanager.com www.googletagmanager.com — Cisco Umbrella Rank: 41	576 KB
3	google.com www.google.com — Cisco Umbrella Rank: 3 region1.analytics.google.com — Cisco Umbrella Rank: 4081	
3	gstatic.com	23 KB

Detected technologies

Bootstrap (Web Frameworks)
Overall confidence: 100%
Detected patterns

- <link[^>]* href=[^>]*?bootstrap(?:[^>]*?([0-9a-fA-F]{7,40}|[\d]+(?:.[\d]+(?:.[\d]+)?)?)|)[^>]*?(?:\.min)?\.css
- bootstrap(?:[^>]*?([0-9a-fA-F]{7,40}|[\d]+(?:.[\d]+(?:.[\d]+)?)?)|)[^>]*?(?:\.min)?\.js

Facebook (Widgets)
Google Analytics (Analytics)
Google Font API (Font Scripts)
Google Tag Manager (Tag Managers)
jQuery (JavaScript Libraries)

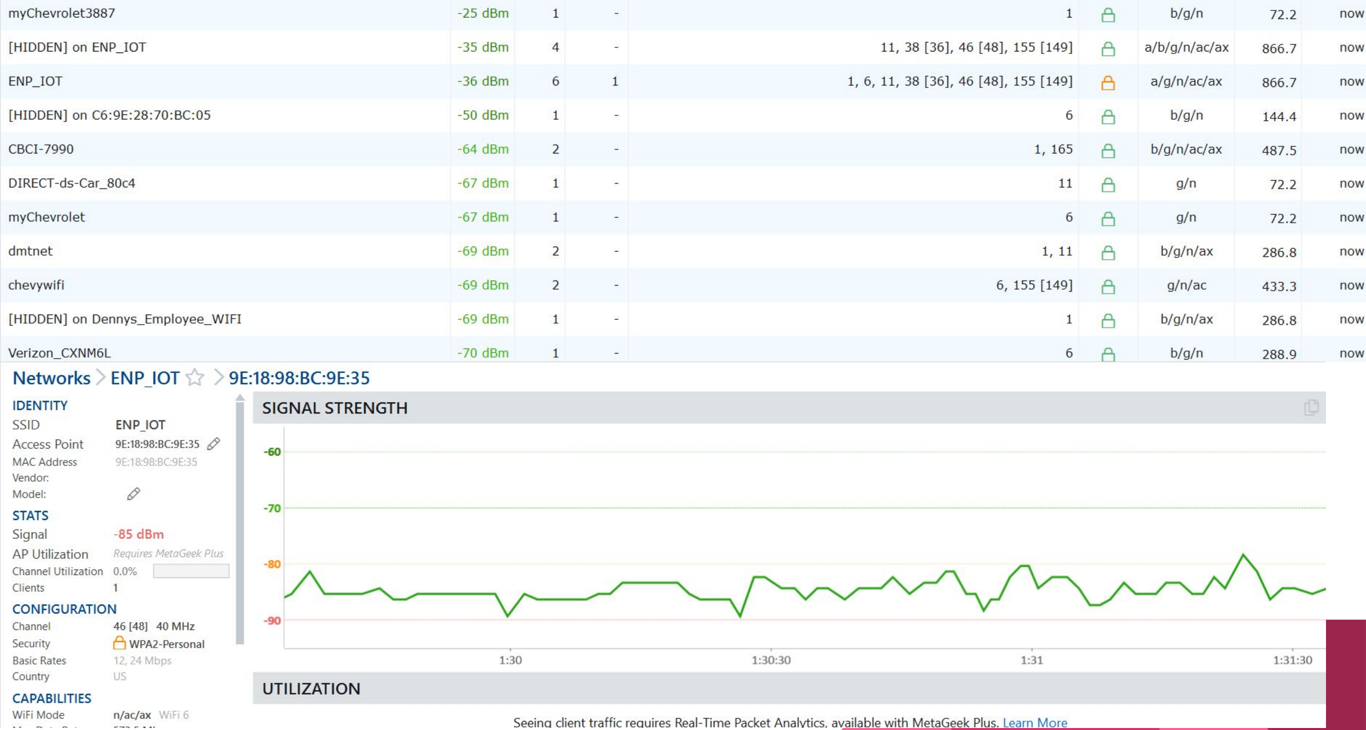
- Notable Information: Bootstrap is known for having XSS exploits across numerous software versions, as seen here: https://security.snyk.io/package/npm/bootstrap

Information Gathered - In Person Gathering

- Location used - 7370 McKnight Rd. Pittsburgh PA.
- LightBlue bluetooth scanner revealed nothing.
- No public Wi-Fi.
    - Was told to use Denny’s Wi-Fi from across the street.
- IoT network was not hidden.
    - Weak passwords and default passwords guessed, did not work
    - Used inSSIDer to gather information

Information Gathered - In Person Gathering: inSSIDer

- [HIDDEN] on C6… suspected to be managerial or employee Wi-Fi.
- IoT network uses WPA2.



myChevrolet3887	-25 dBm	1	-	1	🔒	b/g/n	72.2	now
[HIDDEN] on ENP_IOT	-35 dBm	4	-	11, 38 [36], 46 [48], 155 [149]	🔒	a/b/g/n/ac/ax	866.7	now
ENP_IOT	-36 dBm	6	1	1, 6, 11, 38 [36], 46 [48], 155 [149]	🔒	a/g/n/ac/ax	866.7	now
[HIDDEN] on C6:9E:28:70:BC:05	-50 dBm	1	-	6	🔒	b/g/n	144.4	now
CBCI-7990	-64 dBm	2	-	1, 165	🔒	b/g/n/ac/ax	487.5	now
DIRECT-ds-Car_80c4	-67 dBm	1	-	11	🔒	g/n	72.2	now
myChevrolet	-67 dBm	1	-	6	🔒	g/n	72.2	now
dmtnet	-69 dBm	2	-	1, 11	🔒	b/g/n/ax	286.8	now
chevywifi	-69 dBm	2	-	6, 155 [149]	🔒	g/n/ac	433.3	now
[HIDDEN] on Dennys_Employee_WIFI	-69 dBm	1	-	1	🔒	b/g/n/ax	286.8	now
Verizon_CXNM6L	-70 dBm	1	-	6	🔒	b/g/n	288.9	now

Networks > ENP_IOT ☆ > 9E:18:98:BC:9E:35

IDENTITY

SSID ENP_IOT
Access Point 9E:18:98:BC:9E:35
MAC Address 9E:18:98:BC:9E:35
Vendor:
Model:

STATS

Signal -85 dBm
AP Utilization *Requires MetaGeek Plus*
Channel Utilization 0.0%
Clients 1

CONFIGURATION

Channel 46 [48] 40 MHz
Security 🔒 WPA2-Personal
Basic Rates 12, 24 Mbps
Country US

CAPABILITIES

WiFi Mode n/ac/ax WiFi 6

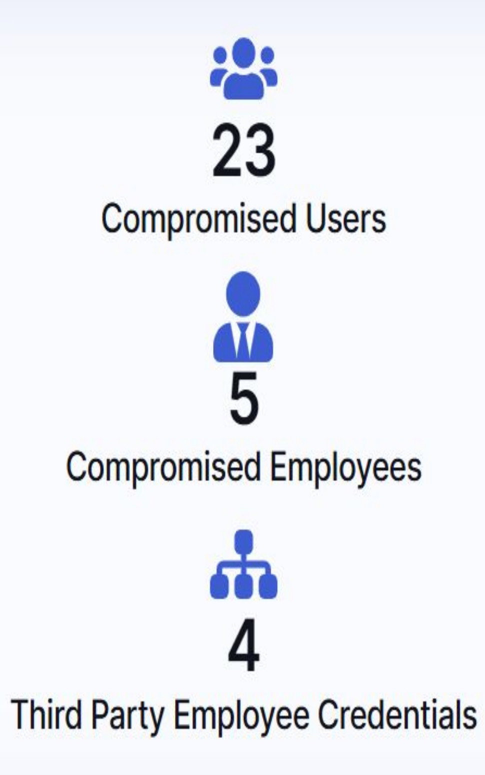
Seeing client traffic requires Real-Time Packet Analytics, available with MetaGeek Plus. Learn More

Information Gathered - Nikto Network Scan

Overall Risk Assessment of Network

Issue	Severity	CVE/Exploit Potential
TRACE method enabled	Medium–High	XST
Internal IP leakage	Medium	CVE-2000-0649
Server/version disclosure	Low–Medium	Reconnaissance
Missing security headers	Low	Browser-side abuse
Unrestricted HTTP methods	Low–Medium	Recon, method abuse

Information Gathered - Hudson Rock



23

Compromised Users

5

Compromised Employees

4

Third Party Employee Credentials

Infostealer Malware Used

A total of 56 infections were linked to eatnpark.com credentials:

- RedLine – 36 infections
- Lumma – 10 infections
- StealC – 2 infections

External Attack Surface

- https://sso.eatnpark.com/adfs/ls/ - Employee
- https://sso.eatnpark.com/adfs/ls - Employee
- https://order.eatnpark.com/checkout - User
- https://order.eatnpark.com - User
- https://order.eatnpark.com/login - User

Information Gathered - ';--have i been pwned?

The employee emails gathered from hunter.io:

- 6 out of the 10 were involved in numerous data breaches
- Half of the breached emails included passwords and personal data
  - Credit status information, Ethnicities, Family structure, Financial investments, Home ownership statuses, Income levels, IP addresses, Marital statuses, Net worth, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages, Geographic Locations

- All of the emails were involved in multiple breaches
  - The most breached one was involved in 18

Analysis

- Hunter.io revealed multiple high-level and low-level employee emails.
- URLscan revealed the IP address used to host Eat’n Park’s website and the detected technologies used in the website.
    - Bootstrap, a web framework has been known to have XSS vulnerabilities in the past
- On site gathering was lackluster.
    - No information gained from LightBlue
    - No public Wi-Fi
    - Little information gained with inSSIDer
    - Discovered probable hidden network
    - Samsung and Cisco devices were connected to the IoT network

Analysis

Nikto Network scan revealed an array of vulnerabilities

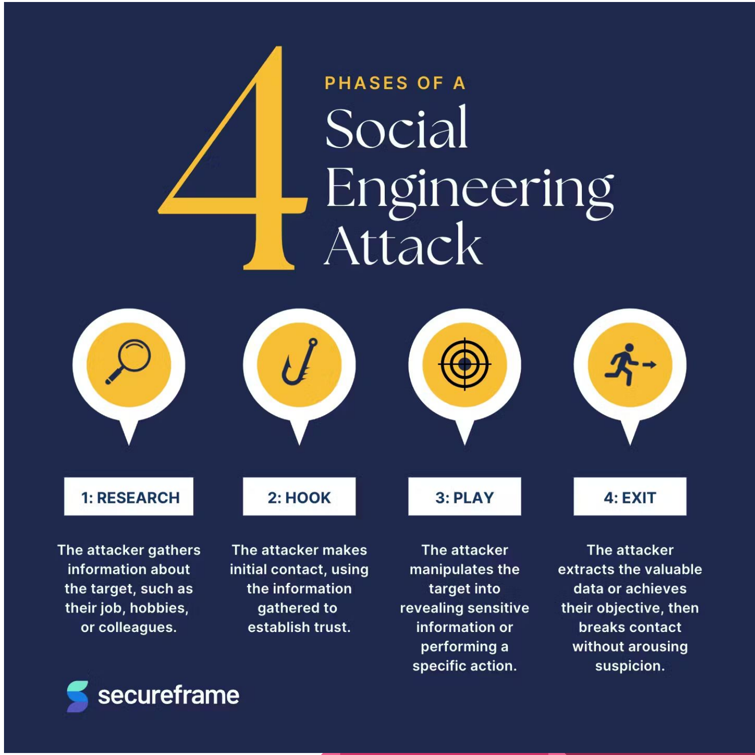
- Trace Enabled
  - cross-site tracing attacks, allowing attackers to steal authentication cookies or headers that are not nor accessible via JavaScript due to browser security restrictions
- Server/Version Disclosure
  - version-based exploits or targeted CVEs on the network
- Missing security headers
  - MIME-sniffing, clickjacking, XSS, inline JS, and data injection
- Internal IP leakage
  - an attacker could learn the internal IP structure and pivot through the network in Server-side request forgery or internal recon
- Unrestricted HTTP methods
  - potential method override attacks for bad threat actors

Analysis

- Hudson Rock
  - Revealed the company’s attack surfaces and all known employees and users accounts and machines that were affected
- Haveibeenpwnded?
  - Showed all the emails that were compromised and what data was leaked

Threat Analysis

- Vulnerable assets found.
  - Email addresses
  - Home addresses
  - Employee names
  - Phone numbers
- Good on-location security.
- Known to be vulnerable to malware.
- Overall, best to attack its employees through social engineering attacks and malware as it is known to work.



4 PHASES OF A Social Engineering Attack

1: RESEARCH

The attacker gathers information about the target, such as their job, hobbies, or colleagues.

2: HOOK

The attacker makes initial contact, using the information gathered to establish trust.

3: PLAY

The attacker manipulates the target into revealing sensitive information or performing a specific action.

4: EXIT

The attacker extracts the valuable data or achieves their objective, then breaks contact without arousing suspicion.

secureframe

Conclusion

- Main weakness is employees.
    - Involved in numerous data breaches
    - Very vulnerable to malware attacks
- Suggest social engineering attacks as an entrance.
    - Spear phishing
    - Whaling
    - Leaving around malicious USBs
        - Number of attacks using this method have multiplied in recent years
- Common form of attacking, but proven to work and the information to do so is available.

Conclusions - Defensive Measures

- Difficult to defend against knowledgeable or uncaring employees.
  - We suggest a training program to enforce learning
- Instate company policies.
  - Do not use company emails for outside work purposes
- MFA.
  - Basic security measure
  - Ensures that even with credential leaks, attackers cannot gain access to accounts