Eat’n Park OSINT

Eric J. Miller and Zarek Rush

Robert Morris University

Emerging Topics in Cybersecurity (CYBS-4360-A)

Professor Hopkins

4/17/2025

Introduction

Open Source Intelligence (OSINT) is labeled as the gathering of publicly available information and data for any kind of intelligence purpose. In the field of cybersecurity, this can be an invaluable tool to understand an organization's security landscape better, how it handles risks, and defend against attacks. On the opposite side of the spectrum, attackers can use OSINT to understand their target, possible threat vectors, targets, and more. Our group, consisting of Eric Miller and Zarek Rush, has decided to conduct an OSINT assessment against Eat’n Park. This assessment will include information gathered from online tools and websites, as well as information gathered in person, to gather as much information as possible from every angle.

Rationale

Eat’n Park was chosen for multiple reasons. It is a local family-owned chain of restaurants branching out from Homestead, PA, with locations open in other states, including Ohio and West Virginia, with over 8,000 employees. Local companies are known to not have as good security standards as nationwide or global organizations, as they do not see as much traffic as these companies, nor have the money or knowledge of what cybersecurity standards are needed to protect their organization. This makes them easy targets to conduct an OSINT assessment on, as they likely have open attack surfaces that bigger companies would have.

Eat’n Park has a large number of locations for a local company. This means that the company has a bigger surface of attack than most other local organizations. A bigger attack surface means that more potential entry points are opened up, more ways to attack the company are available, and the chances of attacks such as phishing emails being successful go up.

The third reason why Eat’n Park was chosen was because of the availability. Because an Eat’n Park location was close to Robert Morris University, the group could conduct OSINT gathering at a physical location, which could provide the opportunity to gather valuable information for the overall assessment.

Methodology

The methodology of the assessment came from two different sides, a physical and digital one. The physical methodology is to sit down and eat like a regular customer while using OSINT tools such as Bluetooth scanners, Wi-Fi scanners, taking notes of physical security, and taking photos of this information to reference in the group's report. This methodology is simple, but effective, as no attacks are involved in an OSINT operation, so no network scans or anything that can be perceived as a threat will be done.

For the digital methodology, numerous known OSINT websites and tools will be used to gather as much information as possible. These will include Hunter.io, URLScan, Nikto, and Hudson Rock. Using all of these sources will allow the team to see already available information about the organization and form a complete assessment of their digital security landscape.

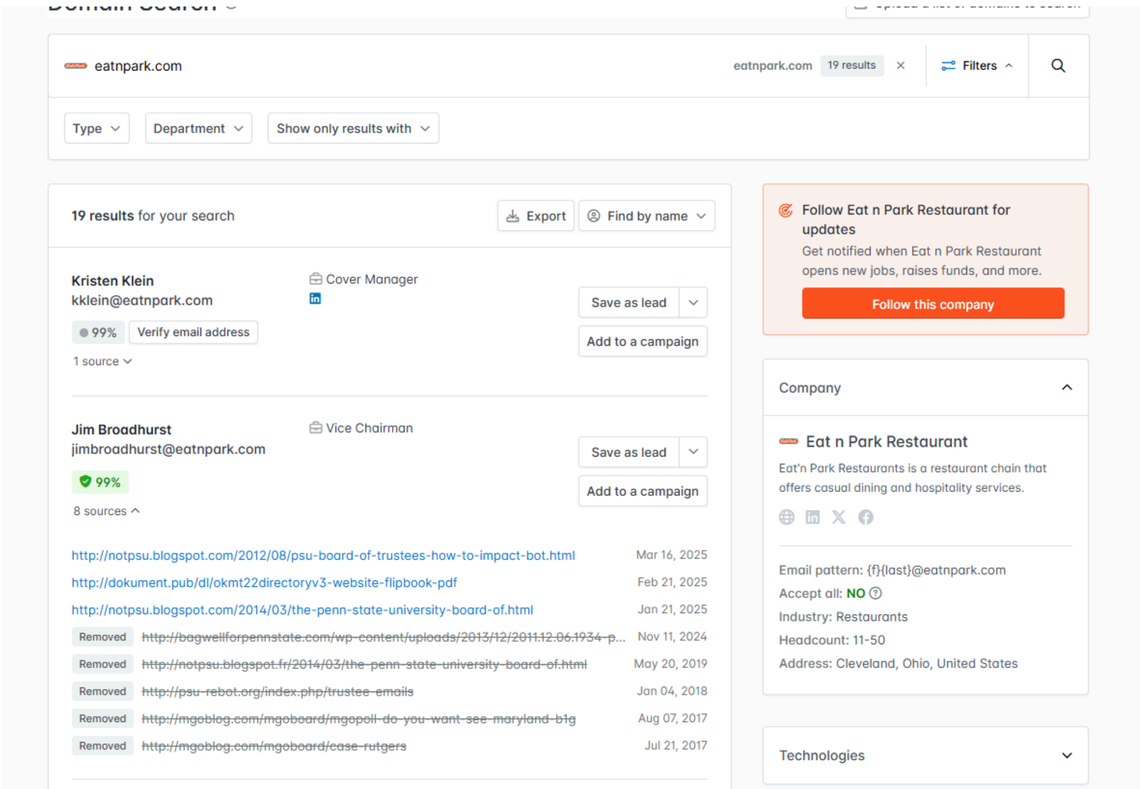
Targets

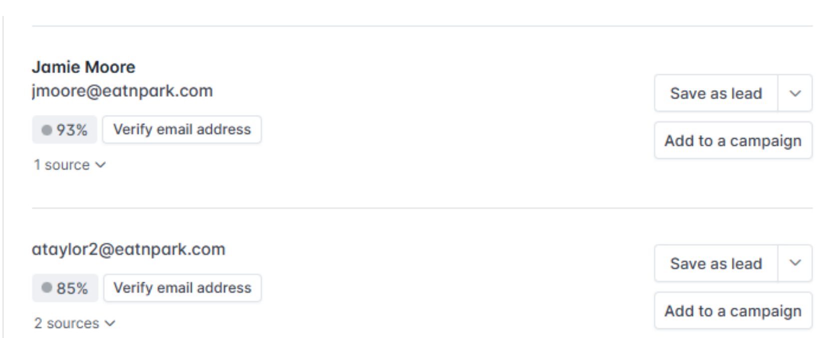
The main targets we are looking for are known problems with Eat'n Park's security, employee email addresses, weaknesses in their Wi-Fi network or Bluetooth devices, and any known systems that the organization uses. Known problems in the organization's security will let the team know what weaknesses may still be active in their online security. Email addresses can be used as a target for social engineering attacks and to see if any of the addresses have been involved in data breaches before. Weaknesses in their Wi-Fi network or Bluetooth devices will allow the team to know what exploits can be conducted against the organization. Known systems that the organization uses will allow for a lookup of those systems and to see if any exploits can be conducted against them.

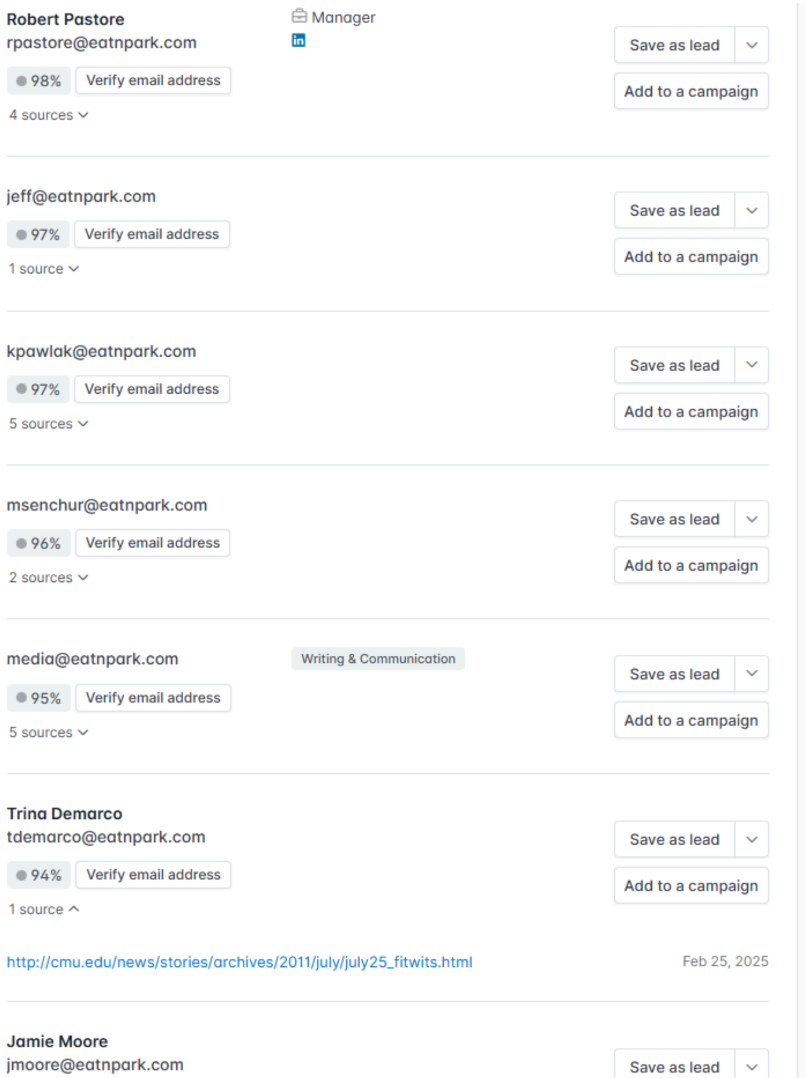
Information Gathered

The following information is what was gathered during the group's OSINT gathering. The name of the tools used will be stated, along with a brief description of what was found. A deeper analysis and understanding of what was found will be located under the "**Analysis**" section of this report. The information will be provided in the order they were obtained. The information gathered is as follows:

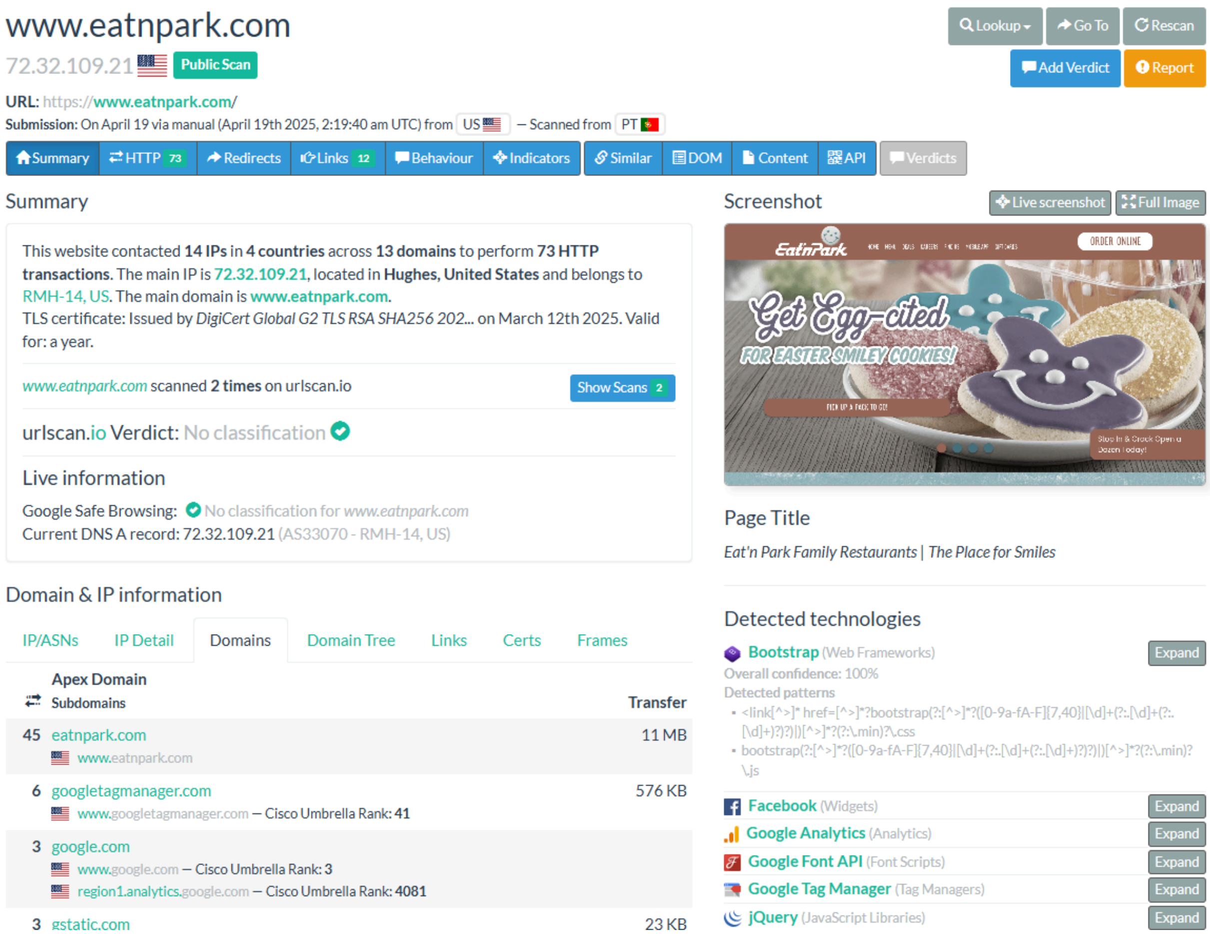
Discovered email addresses via Hunter.io:






Robert Pastore
rpastore@eatnpark.com
Manager
98%
Verify email address
4 sources
Save as lead
Add to a campaign
jeff@eatnpark.com
97%
Verify email address
1 source
Save as lead
Add to a campaign
kpawlak@eatnpark.com
97%
Verify email address
5 sources
Save as lead
Add to a campaign
msenchur@eatnpark.com
96%
Verify email address
2 sources
Save as lead
Add to a campaign
media@eatnpark.com
Writing & Communication
95%
Verify email address
5 sources
Save as lead
Add to a campaign
Trina Demarco
tdemarco@eatnpark.com
94%
Verify email address
1 source
Save as lead
Add to a campaign
http://cmu.edu/news/stories/archives/2011/july/july25_fitwits.html
Feb 25, 2025
Jamie Moore
jmoore@eatnpark.com
Save as lead

Info Gained from URLscan.io:



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

The Eat'n Park location used for in-person OSINT gathering is located at 7370 McKnight Rd. Pittsburgh PA. Nothing of value was gained as using the LighBlue Bluetooth scanner and the McKnight location had no public or private Wi-Fi besides the IoT network. Using inSSIDer, the following information was gathered about the IoT network and devices connected to it:

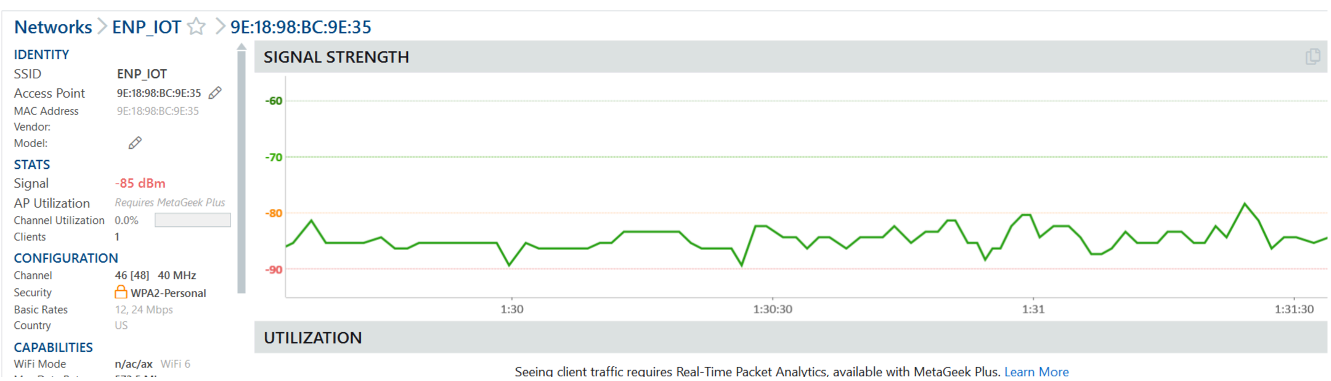
Networks found:

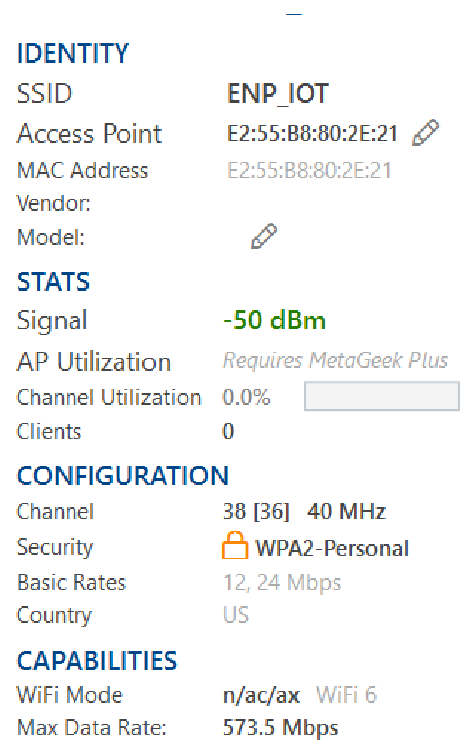
myChevrolet3887	-25 dBm	1	-	1		b/g/n	72.2	now
[HIDDEN] on ENP_IOT	-35 dBm	4	-	11, 38 [36], 46 [48], 155 [149]		a/b/g/n/ac/ax	866.7	now
ENP_IOT	-36 dBm	6	1	1, 6, 11, 38 [36], 46 [48], 155 [149]		a/g/n/ac/ax	866.7	now
[HIDDEN] on C6:9E:28:70:BC:05	-50 dBm	1	-	6		b/g/n	144.4	now
CBCI-7990	-64 dBm	2	-	1, 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

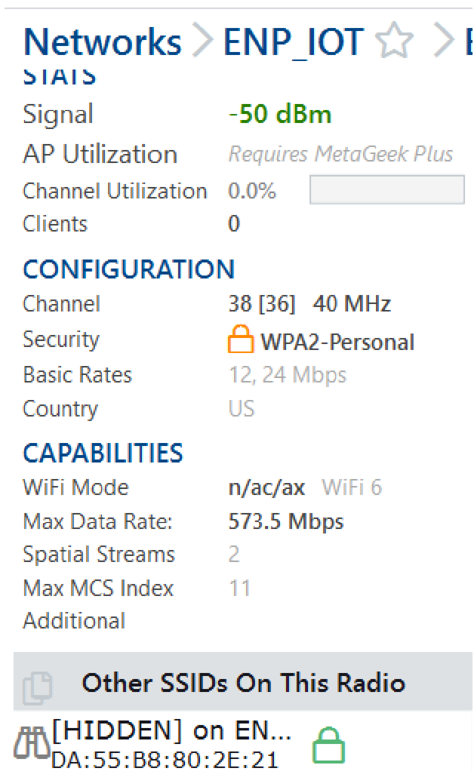
Devices listed connected to the IOT network:

Radio	Signal	Clients	Channel	Width	Security	Mode	Basic Rates	Max Rate	Last Seen
FE:9E:38:70:BC:05	**-59 dBm**	-	155 [149]	80 MHz		a/n/ac	12, 24	866.7	now
E2:55:A8:80:2E:21	**-36 dBm**	-	11	20 MHz		g/n/ax	12, 24	286.8	now
E2:55:B8:80:2E:21	**-49 dBm**	-	38 [36]	40 MHz		n/ac/ax	12, 24	573.5	now
9E:18:88:BC:9E:35	**-67 dBm**	-	1	20 MHz		g/n/ax	12, 24	286.8	now
FE:9E:28:70:BC:05	**-53 dBm**	-	6	20 MHz		g/n	12, 24	144.4	now
9E:18:98:BC:9E:35	**-88 dBm**	1	46 [48]	40 MHz		n/ac/ax	12, 24	573.5	now

About the devices on the network:




IDENTITY
SSID ENP_IOT
Access Point E2:55:B8:80:2E:21
MAC Address E2:55:B8:80:2E:21
Vendor:
Model:
STATS
Signal -50 dBm
AP Utilization Requires MetaGeek Plus
Channel Utilization 0.0%
Clients 0
CONFIGURATION
Channel 38 [36] 40 MHz
Security WPA2-Personal
Basic Rates 12, 24 Mbps
Country US
CAPABILITIES
WiFi Mode n/ac/ax WiFi 6
Max Data Rate: 573.5 Mbps


Networks > ENP_IOT >
Signal -50 dBm
AP Utilization Requires MetaGeek Plus
Channel Utilization 0.0%
Clients 0
CONFIGURATION
Channel 38 [36] 40 MHz
Security WPA2-Personal
Basic Rates 12, 24 Mbps
Country US
CAPABILITIES
WiFi Mode n/ac/ax WiFi 6
Max Data Rate: 573.5 Mbps
Spatial Streams 2
Max MCS Index 11
Additional
Other SSIDs On This Radio
[HIDDEN] on EN...
DA:55:B8:80:2E:21

Network Scan on eatnpark.com done by Nikto:

- Nikto

+ Target IP: 72.32.109.21

+ Target Hostname: eatnpark.com

+ Target Port: 80

+ Start Time: 2025-04-19 23:12:53 (GMT-7)

+ Server: Microsoft-IIS/10.0

+ /: Retrieved x-aspnet-version header: 4.0.30319.

+ /: Retrieved x-powered-by header: ASP.NET.

+ Root page / redirects to: https://www.eatnpark.com

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

+ /aspnet_client: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "172.24.32.21". See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649

+ OPTIONS: Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .

+ OPTIONS: Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST .

+ Scan terminated: 0 error(s) and 6 item(s) reported on remote host

+ End Time: 2025-04-19 23:13:54 (GMT-7) (61 seconds)

+ 1 host(s) tested

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 gained from Hudson Rock:

Compromised Individuals

- 5 Employees compromised
- 23 Users compromised
- Last employee compromise: June 16, 2021
- Most recent user compromise: February 15, 2025

Infostealer Malware Used

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

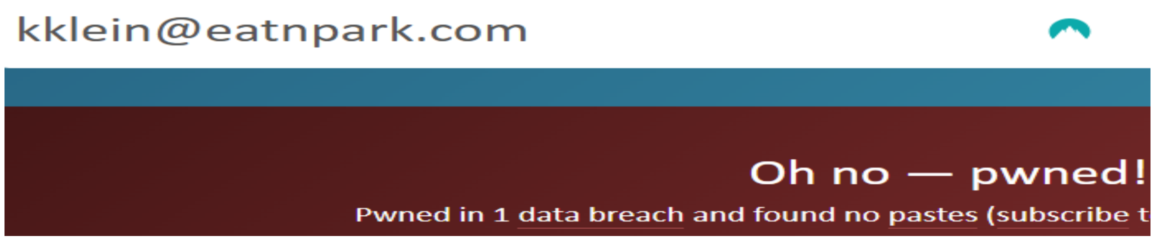
- RedLine – 36 infections
- Lumma – 10 infections
- StealC – 2 infections

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 gained from Have I been Pwned? :

Using the emails we found from hunter.io, I input them into this site to see if these emails have been involved in any data breaches. Here is what I found out:



Compromised data: Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses, Social media profiles

Compromised data: Dates of birth, Email addresses, IP addresses, Names, Partial credit card data, Phone numbers, Physical addresses, Purchases, Employers, Job Titles, Social Media Profiles

Compromised Data: Email Addresses, Passwords, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles, Physical Addresses, Education Levels (Passwords were discovered in half of the breaches it was involved in)

Compromised data: Email addresses, Employers, Geographic locations, Physical Addresses, Job titles, Names, Phone numbers, Social media profiles

Compromised Data: Dates of birth, Email addresses, Genders, Names, Passwords, Phone numbers, Physical addresses, Geographic locations, Job titles, Salutations, Social media profiles, IP Addresses, Purchases, Partial Credit Card Info, Purchases (Passwords were discovered in 12 of the breaches)

Compromised data: Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages, Geographic Locations, Job Titles, Education Levels, Social Media Profiles (Password were discovered in 6 of these breaches)

Analysis

The first website used was Hunter.io, an email outreach platform that allows users to find companies' known email addresses. Plugging in Eat'n Park, multiple high-level and low-level employee emails were found, such as the vice chairman's and managers'. These emails could be used as targets for spear phishing attacks and whaling attacks.

URLscan.io revealed the IP address used to host Eat'n Park's website and the detected technologies used in the website. These include Bootstrap, jQuery, and Google Analytics. Bootstrap is a web framework that has had known issues with cross-site scripting exploits in the past across multiple versions. If the organization is using an older version of this framework, the website could be vulnerable to this attack.

The on-location OSINT gathering did not provide as much information as hoped. The LightBlue Bluetooth scanner did not provide adequate results, and the location did not have any public Wi-Fi to connect to. They did have an IoT network, and using the inSSIDer tool, it was possible to see devices connected to the network. Looking up these Mac addresses, we see that Samsung and Cisco devices are connected, but the exact devices are unknown. InSSIDer also shows hidden networks that are picked up, and one of these, titled "C6:9E:28:70:BC:05," was very close to the physical location of the group when using the tool. It is speculated that this is a hidden network used by managers and staff. Default passwords were used to attempt to gain access to the IoT network, but were unsuccessful.

Using Nikto to conduct a network scan revealed an array of vulnerabilities on the company's website. The first vulnerability found was that the TRACE method was enabled, which can lead to cross-site tracing attacks, allowing attackers to steal authentication cookies or headers that are not normally accessible via JavaScript due to browser security restrictions. The next vulnerability is that they left the server header and version wide open for anyone to see, which can allow attackers to use version-based exploits or targeted CVEs on the network. They also lack security headers, allowing for MIME-sniffing, clickjacking, XSS, inline JS, and data injection. Internal IP leakage was also discovered, which could allow an attacker to learn the internal IP structure and pivot through the network in Server-side request forgery or internal recon. Lastly, it was found that they have unrestricted HTTP methods, which could provide recon data or potential method override attacks for bad threat actors.

Hudson Rock revealed that 5 employees and 23 users were compromised using infostealer malware, with a total of 56 known infections. The types of malware found were RedLine, with a total of 36 infections. (This malware is designed to harvest credentials, cookies, autofill data, crypto wallets, etc. This is widely sold on cybercrime markets as a Malware-as-a-Service (MaaS). It can be delivered via malicious email attachments, fake software cracks, Discord spam, or YouTube tutorials.) Lumma with 10 infections, (Is a newer and increasingly popular infostealer that includes modern evasion features and harvests the same data as RedLine, but often evades antivirus software due to frequent repackaging. It is active on Telegram-based groups), and StealC with 2 infections (Used in more targeted campaigns rather than mass credential harvesting like RedLine or Lumma. So, that may be why there are fewer infections. They are known for targeting password managers, clipboard data, and other custom configuration thefts). The stolen credentials from the users' compromised accounts could lead to internal network access, privilege escalation, and lateral movement in the environment. As for the users, it could lead to account takeover, fraud, or payment abuse.

The last website I used to gather OSINT information was have i been pwned? This website was used to find out if any of the emails we discovered have been involved in any data breaches and what data was compromised in them. So, out of the 10 emails, we discovered that 6 of them were involved in numerous data breaches, with half of them having their passwords compromised. All the emails involved in these breaches were from employees ranging from the vice chairman to managers and the director of Corporate Communications & Community Partnerships. This information allows for bad threat actors to either gain access to these accounts and the network, and allow them to escalate their privileges through the network, or do whatever they want, depending on the level of access that account has. They also become key targets for phishing attacks because of the amount of data threat actors have gathered on them. The compromised data involved were Credit status information, Dates of birth, Education levels, Email addresses, Ethnicities, Family structure, Financial investments, Genders, Home ownership statuses, Income levels, IP addresses, Marital statuses, Names, Net worths, Occupations, Personal interests, Phone numbers, Physical addresses, Religions, Spoken languages, Geographic Locations, Job Titles, Education Levels, Social Media Profiles. So, as you can see, this allows for threat actors to make extremely personal phishing attacks, making them more believable and increasing the chances of that employee falling for it.

Threat Analysis

With the information found while conducting our investigation, Eat'n Park's assets are very vulnerable. Though they are vulnerable to errors in network setups or systems. They are most vulnerable due to errors made by their employees. Doing the physical OSINT on the Eat'n Park locations did not give the team much information at all, as they had no public Wi-Fi, and their IoT network was secure. They did not even have Bluetooth devices that the team could connect to. What was found, however, was a multitude of emails, addresses, names, numbers, and social media profiles due to malware, data breaches, and other cyber attacks. While Nikto did a scan on the Eat'n Parks website and found multiple vulnerabilities there as well, the best way to gain access to or attack the company's assets is through its employees.

Social engineering attacks, malware, and data breaches are seen to regularly affect and steal information about Eat'n Park employees at a high level. Using this information, it would be possible to gain access to their company tax forms, such as a W-2, their bank accounts, their employee number, possible work-related account information, and possible passwords from their social media accounts. It is through attacking not the organization but its employees that Eat'n Parks' assets are the most vulnerable and where bad threat actors can gain internal access to their network.

Conclusions

To summarize the group's findings, Eat’n Park is a vulnerable company not through how insecure its website or Wi-Fi is, but due to its employees. Numerous forms of attacks are seen to be highly successful against the organization's workers, as malware, social engineering attacks, and data breaches reveal critical personal information. This opens up a multitude of pathways to possibly attack the company's assets. These can range from phishing attacks and spear phishing attacks, fake websites, and even possibly leaving around malicious USB drives, as “In the first half of 2023, Mandiant Managed Defense saw a threefold increase in the number of attacks using infected USB drives” (Firch, 2024). While these attacks are basic, they have proven to work against the organization in the past and will likely continue to work unless drastic improvements are made to the organization's security landscape.

The security measures the group suggests Eat’n Park take to prevent these attacks from occurring are training programs, establishing company-wide policies and procedures, and MFA. While it is impossible to enforce a strategy that prevents employees from falling victim to social engineering attacks at home through their own personal systems, teaching employees what they look like and how to look out for them through training programs could help prevent this. According to CISA, or the Cybersecurity & Infrastructure Security Agency, common indicators of social engineering attacks are suspicious sender addresses, generic greetings and signatures, suspicious attachments, and suspicious links. In the organization’s potential training program, these are the topics that should be included, and staff should be able to spot malicious emails, messages, and calls by the end.

Establishing company-wide policies and procedures could greatly benefit the organization. As seen in the "**Information Gathering**" section, company emails were used for a multitude of purposes besides work. A policy stating that company emails are not to be used for personal purposes should be instated to stop the possibility of any personal information being taken from these emails. If this action had been taken beforehand, the "tdemarco@eatnpark.com" email would likely not have had its marital status and religious status leaked. Procedures such as forcing each Eat'n Park location to follow compliance standards set by the company would ensure that all security policies are followed.

If MFA or Multi-Factor Authentication is not in place at Eat'n Park, the organization must put it into place as soon as possible. Due to the amount of information stolen that can be used to access potential organizational systems, employee data, and more, a system such as MFA could help prevent unauthorized access even with data breaches occurring. MFA requires something the user is, knows, or has, an example of this being something you know, such as a password, and something you have, such as a code texted to a specific phone number. This means that even with the passwords leaked due to data breaches, attackers could still not access user accounts as they do not have the aspect of something the user has, such as a phone number-specific code.

While Eat'n Park was discovered to be vulnerable to numerous attack vectors, such as malware and social engineering, leading to data breaches, the company can implement ways to prevent this in the future. This can be done utilizing tools such as training programs, policies and procedures, and MFA. If the organization takes these issues seriously and does its due diligence to protect its employees, these cybersecurity issues can be prevented.

References

bootstrap vulnerabilities | Snyk. (2024). Find Detailed Information and Remediation Guidance for Vulnerabilities and Misconfigurations. https://security.snyk.io/package/npm/bootstrap

CISA. (2021, February 1). *Avoiding Social Engineering and Phishing Attacks*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Firch, J. (2024, May 19). *How Ransomware Spreads In 2024: 5 Common Methods*. PurpleSec. https://purplesec.us/learn/common-ways-ransomware-spreads/

Have I been pwned: Check if your email has been compromised in a data breach. Have I Been Pwned. (n.d.). https://haveibeenpwned.com/?__cf_chl_tk=b56PHeUaxf4hKikN6Pi1cmEHQBm3DXp52WJIM1aQzJ4-1745896342-1.0.1.1-uRoSwvJQickpoESx28j_vQoohP3EkXXTytDexY7iycg

Hudson Rock - Infostealer Intelligence Solutions. (n.d.). https://www.hudsonrock.com/

Hunter. (2019). Hunter. https://hunter.io/

OSINT framework. OSINT Framework. (n.d.). https://osintframework.com/

URL and website scanner - urlscan.io. (n.d.). Urlscan.io. https://urlscan.io/