PICNIC™

TARGET INTELLIGENCE REPORT | ISSUE NO.3

Mailchimp

LESSONS LEARNED

Prepared by:
MANIT SAHIB & FELISHA MOUCHOUS
Office of Global Threat Intelligence, Picnic Corporation

getpicnic.com

TABLE OF CONTENTS

INTRODUCTION

Social engineers collect intelligence on human targets to develop paths for attack and compromise. Picnic's platform emulates this external, human attack surface reconnaissance to expose **TARGET INTELLIGENCE** about an organization. Picnic pairs this unique perspective of threat actors with automated actions that reduce risk for its customers.

Picnic offers Target Intelligence Reports to help security teams better understand how attackers use open-source intelligence and established infrastructure to launch attacks. By reducing their human attack surface, organizations can disrupt attacker reconnaissance and resource development, which in turn reduces the risk of attacks.

EXECUTIVE SUMMARY

In this report (Issue #3), we analyze three **Mailchimp breaches that occurred between March 2022 and January 2023** to understand how the attacker leveraged open-source information and used social engineering to target Mailchimp employees. The report includes proactive remediation steps for organizations to take to help lower the risk of attackers being successful in the future.

We used Picnic's platform to expose threat actor reconnaissance and resource development.

We also analyzed public reporting about the attack to provide a more complete picture of the attack and remediation actions taken by victims.

Overall, these breaches highlight how important it is for companies to proactively understand, limit, and continuously monitor employee and organizational exposure, and to preemptively identify and block attacker infrastructure. Combining these capabilities can mitigate the threat of attackers launching successful social engineering attacks against organizations.

The data in this report is valid through March 2023.

MAILCHIMP INCIDENT SUMMARY

JANUARY 2023

Mailchimp is a popular email marketing service. On January 11th, 2023, Mailchimp noticed unauthorised activity on its system and found that 133 customer accounts had been breached.

An unauthorized actor had gained access to these accounts after targeting Mailchimp employees and contractors with a social engineering attack and then using harvested credentials from the attack to access internal Mailchimp systems. These systems included customer support and account administration.

In response to this breach, Mailchimp suspended the affected accounts and worked with customers to help them reinstate their accounts and provide additional support.

One of Mailchimp's customers, WooCommerce, informed its own customers that their data (names, addresses, emails, URLs) had been compromised in this breach and that they were now at higher risk of being targeted with phishing campaigns. FanDual, another Mailchimp customer, also warned its customers to be on guard against phishing campaigns after their details were compromised too as a result of the breach.

https://mailchimp.com/en-gb/january-2023-security-incident/

This is not the first time Mailchimp has suffered a data breach, as the company was breached twice in 2022 under similar circumstances.

AUGUST 2022

In August 2022, dozens of companies including Twilio and Mailchimp were targeted in an Okta style SMS phishing attack (0ktapus). As a result, 214 Mailchimp accounts related to the crypto and financial industry were compromised when attackers gained access to internal tooling using compromised employee credentials. Following the attack, Mailchimp suspended accounts related to cryptocurrency while the company investigated the breach and contacted customers regarding how to secure their accounts.

Mailchimp's customer DigitalOcean was also caught up in this attack and its Mailchimp account and some of its customer email addresses were compromised. The company noticed on August 8th that its Mailchimp account had been suspended with no access or additional information provided. DigitalOcean was subsequently informed by Mailchimp that this was due to a terms of service violation. At the same time, a customer informed DigitalOcean that their password had been reset without them having performed this action. This led to an investigation by DigitalOcean's security team.

MAILCHIMP INCIDENT SUMMARY CONT.

After contacting Mailchimp, DigitalOcean subsequently received a formal notification on August 10th of unauthorized access to its and other accounts by an attacker who had compromised Mailchimp's internal tooling. The attacker had initiated password resets using a limited set of DigitalOcean accounts obtained via the Mailchimp breach. One reset was successful but the customer had a second factor of authentication so the attacker could go no further. DigitalOcean also found evidence of other password resets that were unsuccessful.

Once the company became aware of this compromise, DigitalOcean migrated its services away from Mailchimp to another email services provider. DigitalOcean also reached out to its customers that may have been affected in the breach and advised them to look out for phishing attempts and to enable two-factor authentication on their accounts.

MARCH 2022

In March 2022, a similar breach occurred when an attacker gained access to Mailchimp customer and account management tools after socially engineering employees for their credentials.

319 Mailchimp accounts, along with audience data and API keys for some of Mailchimp's customers, were exposed in this attack. Accounts that were in the financial and cryptocurrency industry were specifically targeted. Although Mailchimp has not stated how the employees were socially engineered, it is likely that they fell for a phishing campaign through which their credentials were harvested and used to gain access. This breach put Mailchimp's customers at risk, as attackers could conduct phishing campaigns against them with this information.

Mailchimp reported that on April 2nd the attacker used the information gained in the breach to launch a phishing campaign against a Mailchimp user's contacts. The company took steps to inform the account owner and block their access from the platform. The attacker, however, was able to use the information to launch the campaign without using Mailchimp's platform.

Mailchimp stated at the time that it had informed the affected customers, consulted a forensic company to investigate the breach, and limited employee access to internal systems. The company also said it is putting additional security measures in place while the breach is being investigated.

https://www.digitalocean.com/blog/digitalocean-response-to-mailchimp-security-incident
https://mailchimp.com/en-gb/august-2022-security-incident/
https://mailchimp.com/en-gb/march-2022-security-incident/

MAILCHIMP INCIDENT SUMMARY CONT.

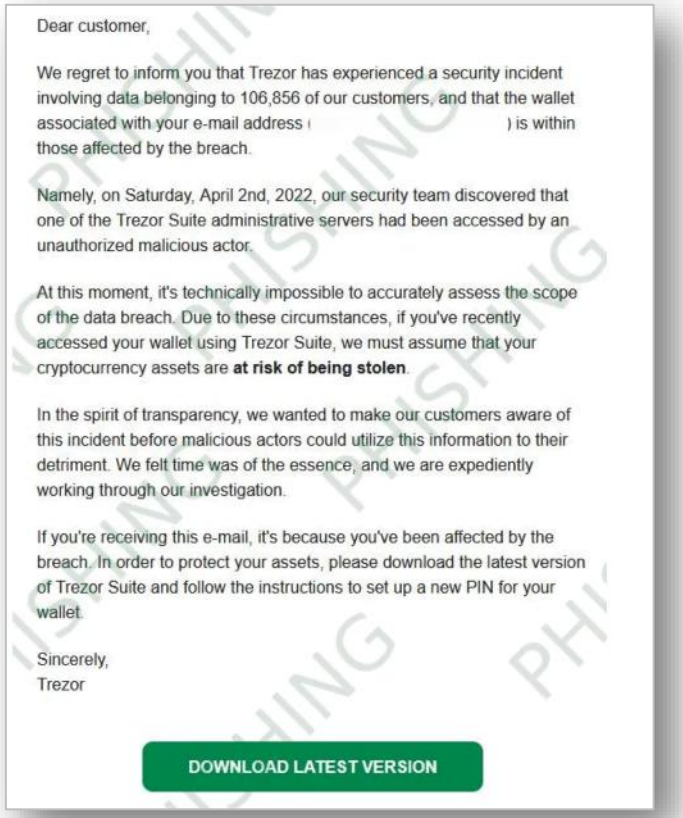
Trezor customer impact

APRIL 2022

In April 2022, Mailchimp cryptocurrency customer Trezor announced that attackers were leveraging their access from the Mailchimp breach to conduct a phishing campaign against Trezor customers. The phishing email to customers informed them of a security breach and included an update download that users were prompted to click on. Once the user clicked on and downloaded the seemingly legitimate but malicious software, they were prompted to connect to their crypto wallet and enter their seed, or risk their cryptocurrency being stolen. Trezor informed its customers of this issue and provided steps they could take to secure themselves. The company also advised customers to not open any emails from Trezor until the issue was resolved and the phishing domains were taken down.

A class action lawsuit was filed against Mailchimp and its parent company Intuit by plaintiff Alan Levinson, claiming millions of dollars in stolen cryptocurrency as a result of Intuit and Mailchimp failing to prevent the data breach and disclose it in a timely manner.

In February 2023, Trezor announced that it had been targeted by another phishing campaign in which attackers were targeting its customers via SMS and email to inform them that Trezor had



Dear customer,

We regret to inform you that Trezor has experienced a security incident involving data belonging to 106,856 of our customers, and that the wallet associated with your e-mail address ( ) is within those affected by the breach.

Namely, on Saturday, April 2nd, 2022, our security team discovered that one of the Trezor Suite administrative servers had been accessed by an unauthorized malicious actor.

At this moment, it's technically impossible to accurately assess the scope of the data breach. Due to these circumstances, if you've recently accessed your wallet using Trezor Suite, we must assume that your cryptocurrency assets are **at risk of being stolen**.

In the spirit of transparency, we wanted to make our customers aware of this incident before malicious actors could utilize this information to their detriment. We felt time was of the essence, and we are expediently working through our investigation.

If you're receiving this e-mail, it's because you've been affected by the breach. In order to protect your assets, please download the latest version of Trezor Suite and follow the instructions to set up a new PIN for your wallet.

Sincerely,
Trezor

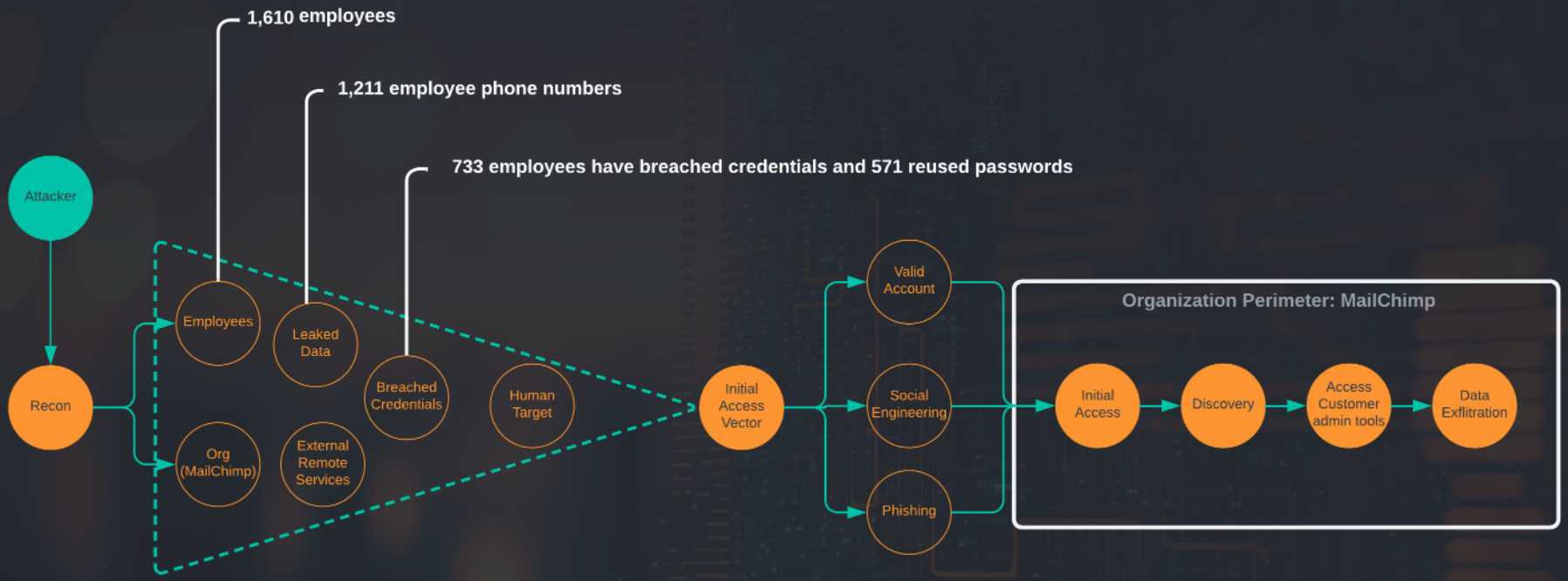
DOWNLOAD LATEST VERSION

suffered a data breach. The campaign prompted customers to go to a phishing site to 'secure' their assets at which point they were asked to enter their recovery seed. The campaign prompted customers to go to a phishing site to 'secure' their assets at which point they were asked to enter their recovery seed. Doing so would allow the attacker to compromise their crypto wallets. Trezor stated that the company had not in fact been involved in a data breach and advised customers not to click on these links. The information the attackers used in this attack is likely to have come from Mailchimp's previous breach in 2022, when Trezor customer information was compromised.

https://blog.trezor.io/ongoing-phishing-attacks-on-trezor-users-edd840b17304

MAILCHIMP INCIDENT SUMMARY CONT.

Mailchimp Breach Compromise Path



THREAT ACTOR

0ktapus / Scatter Swine

AUGUST 2022

It has been reported by the cybersecurity company Group-IB that the August 2022 attack on Twilio and Cloudflare was part of a larger campaign that targeted and compromised over 130 organizations in and around the same time frame. Mailchimp was one of the organizations targeted.

The threat actor responsible has been named as '0ktapus' or 'Scatter Swine' and is known for persistent phishing campaigns and for targeting organizations that use Okta for authentication. This actor potentially gathered 10,000 employee credentials during its campaigns.

Okta itself has been targeted by this actor on numerous occasions and has also collected TTPs used by the actor to help organizations protect themselves.

Tools And Techniques Used By This Actor

DATA BROKERS & PREVIOUS BREACHES

To find data about employees and link them with phone numbers.

SMISHING

This threat actor conducts bulk phishing campaigns via SMS to trick employees into clicking on links that look legitimate.

CREDENTIAL HARVESTING

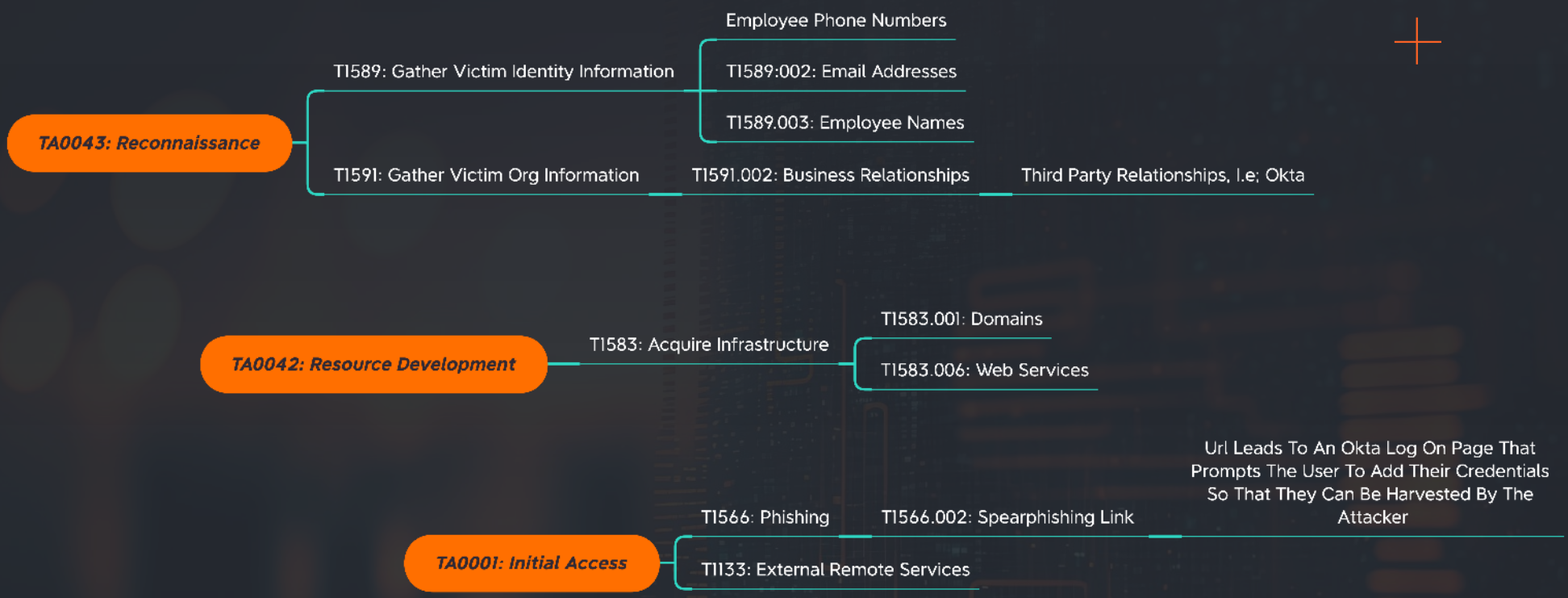
Phishing kits that capture employee credentials and OTP codes. In some cases, this triggers push notifications to try and get users to accept it.

MFA fatigue is a technique in which the attacker bombards a user with many push notifications until they intentionally or unintentionally accept the prompt.

Source: https://sec.okta.com/scatterswine

MITRE ATT&CK TTPs

Oktapus



PICNIC'S INCIDENT ANALYSIS

For the attackers to be successful in these breaches, they needed to find real phone numbers and employee information. They also had to register lookalike domains and host phishing pages to trick the employees and harvest their credentials.

Picnic emulated threat actor reconnaissance to demonstrate how data on Mailchimp employees was gathered for the attacks.

Using Picnic's technology platform, we were able to gather and analyze data from a sample of 1,610 Mailchimp employees with different seniority levels throughout the organization. We also identified indicators of attack that point to threat actors acquiring infrastructure to launch a phishing campaign.

- **1,211 Mailchimp employees have one or more phone numbers** that are readily available online and can be leveraged in a smishing attack.
- Of the 1,610 employees sampled, **733 employees have been in data breaches. 571 of these employees have shown evidence of password reuse** where the same password has appeared in more than one password breach.
- Picnic found **79 suspicious Mailchimp lookalike domains**. Using our platform, we can visualize this risk and drill down into each domain to find out more information.

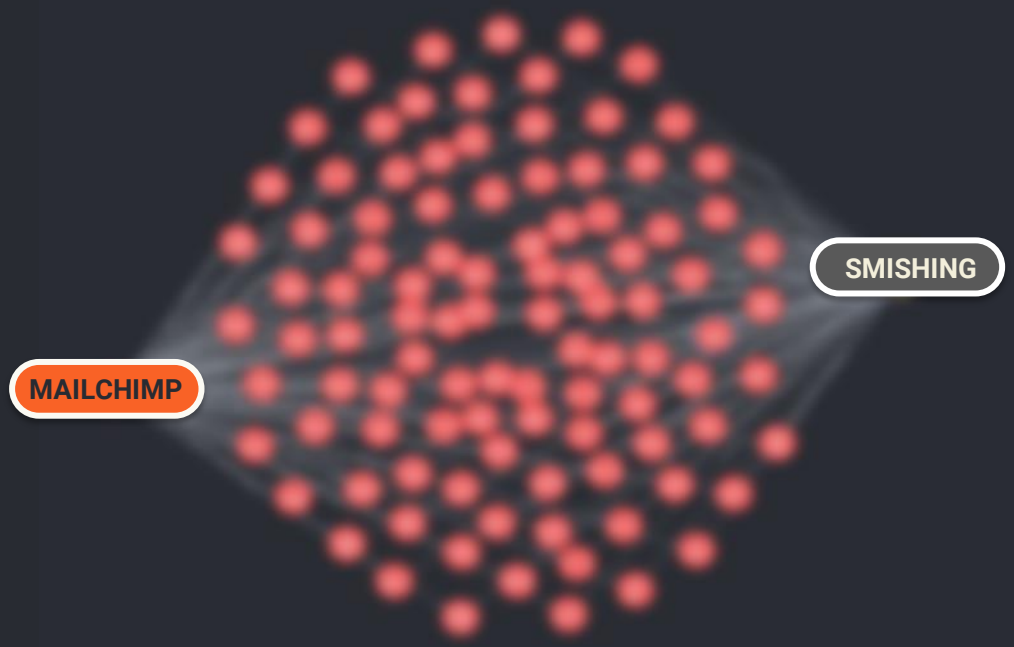
PICNIC HUNTING FOR RECON

Smishing Risk View: 1,211 employees

Of the 1,610 Mailchimp employees whose details we have found, 1,211 of these employees have one or more phone numbers exposed on the internet.

The 0ktapus threat actor in August 2022 was able to leverage these exposed numbers to target employees. One such example was the Twilio Inc. breach.

Mailchimp employees that can be targeted in a smishing attack



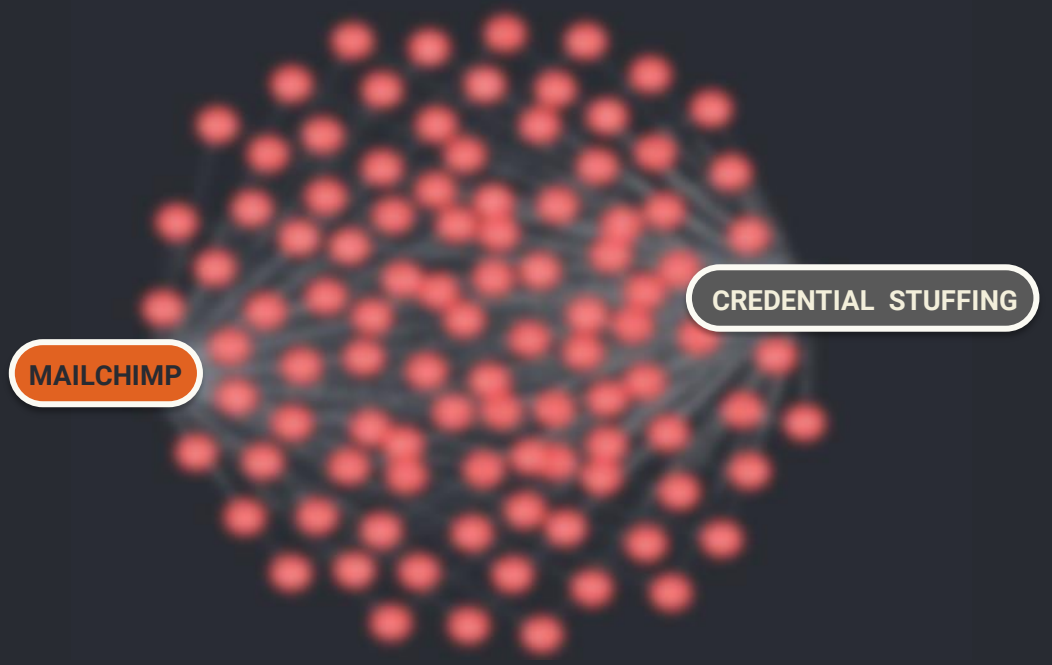
Credential Stuffing Risk View: 733 employees

Of the 1,610 Mailchimp employee details we analyzed, 733 of these employees have breached credentials that have been exposed in one or more breaches.

571 of these employees have evidence of password reuse since the same password was found in separate breach databases.

Threat Type Employee Company

Mailchimp employees (names redacted for security) that can be targeted in a credential stuffing attack



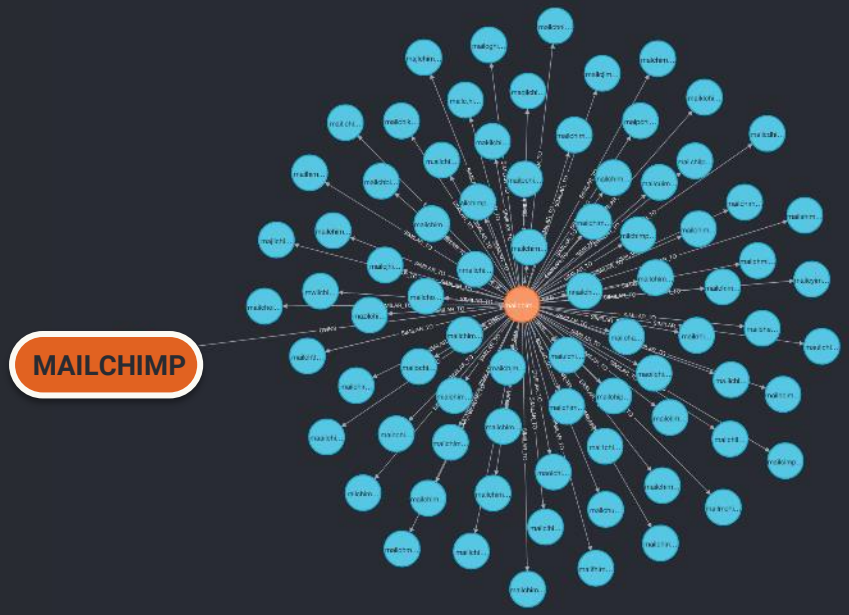
PICNIC IoATTACK

Suspicious Domains View: 79

There are 79 registered suspicious Mailchimp lookalike domains that could be used to target the company. To determine if a domain is suspicious, we look at the WHOIS record to see who registered the domain, when it was registered, and the reputation.

If an attacker is preparing to launch an attack it is highly likely that new lookalike domains will be registered together. It is important to identify these as soon as possible so that organizations can take action to block domains before they can be used.

Company Company Domain Suspicious Domain



1. mailchemp.com
2. mailchmip.com
3. mailchipm.com
4. mialchimp.com
5. mailhcimp.com
6. ma.ilchimp.com
7. mail.chimp.com
8. mailc.himp.com
9. m.ailchimp.com
10. maildhimp.com
11. mailchump.com
12. maipchimp.com
13. maolchimp.com
14. mailchimo.com
15. mailchomp.com
16. mailfhimp.com
17. majlchimp.com
18. mailch9mp.com
19. mwilchimp.com
20. mailcuimp.com
21. mailcyimp.com
22. mailchjmp.com
23. maiilchimp.com
24. maailchimp.com
25. mailchim.com
26. malchimp.com
27. mailchmp.com
28. mailcimp.com
29. mailhimp.com
30. ailchimp.com
31. milchimp.com
32. mazilchimp.com
33. makilchimp.com
34. mailchikmp.com
35. mailchnimp.com
36. mailcdhimp.com
37. mailcghimp.com
38. mailpchimp.com
39. mailchbimp.com
40. maoilchimp.com
41. majilchimp.com
42. mailcjhimp.com
43. mailmchimp.com
44. mailchoimp.com
45. maiklchimp.com
46. maqilchimp.com
47. mauilchimp.com
48. maiulchimp.com
49. mailochimp.com
50. mailchilmp.com
51. mailchirp.com
52. mallchimp.com
53. mailchinmp.com
54. nailchimp.com
55. railchimp.com
56. mai1chimp.com
57. nnailchimp.com
58. nmailchimp.com
59. mailclhimp.com
60. mailchimmp.com
61. mainchimp.com
62. mailclimp.com
63. mailchamp.com
64. mailchimpy.com
65. mailchimpg.com
66. mailchimpi.com
67. mailchimpm.com
68. mailchimpn.com
69. mailchimpv.com
70. mailchimpk.com
71. mailchimpl.com
72. mailchimpr.com
73. mailchimps.com
74. mailchimpz.com
75. mailchimpe.com
76. mailchimpt.com
77. mailcjimp.com
78. mailchilp.com
79. mailshimp.com

MITIGATIONS

For Existing Picnic Customers

REDUCE EMPLOYEE ATTACK SURFACE

- Enroll employees in CheckUp to continually reduce exposed PII, neutralize exposed credentials, and ensure social media operational security.
- Enable MFA on all accounts.

MITRE Ref: T1589; T1593
MITRE Mitigation: M1056 [Pre-Compromise]

REDUCE ORGANIZATIONAL ATTACK SURFACE

- Review suspicious domains identified by Picnic and block newly registered domains similar to your organization's.
- Review Picnic's risk assessment of any external facing components and take any recommended remedial actions.
- Review improper DNS DMARC settings identified by Picnic and ensure the correct settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party.
- Securely configure MFA on all accounts, using physical FIDO2 compliant tokens as another factor of authentication where possible.
- Regularly audit employee access to one of least privilege (including offboarding), especially for at-risk users identified by Picnic.
- Regularly audit 3rd party access to one of least privilege, especially for at-risk users identified by Picnic.
- Monitor and neutralize sensitive information disclosure identified by Picnic, such as exposed passwords associated with personal and company accounts.

MITRE Ref: T1592; T1589: T1590; T1591; T1596
MITRE Mitigation: M1056 [Pre-Compromise]

MITIGATIONS

For Non-Picnic Customers (Recon)

REDUCE EMPLOYEE ATTACK SURFACE

- Ensure any breached credentials are remediated to stop password reuse.
- Review online exposure and ensure personal details are removed.
    - These can be leveraged to build trust.
    - For info that can't be removed, e.g., conference presentations, be aware of how these can be leveraged.
- Enable MFA on all personal accounts to prevent account compromise.
- Use different emails and photos for different online activity.
    - Disrupts data aggregation, including reverse image lookup.
- User awareness: If it's too good to be true, it's probably phishing.

MITRE Ref: T1589; T1593
MITRE Mitigation: M1056 [Pre-Compromise]

REDUCE ORGANIZATIONAL ATTACK SURFACE

- Regularly review any external facing components to understand exposure. Allow those that are trusted, remove those that are not, and ensure MFA is enabled for all accounts.
- Ensure DNS DMARC settings are enforced to mitigate against impersonation attacks either on yourself or against a trusted 3rd party.
- Regularly audit employee access to one of least privilege (including offboarding).
- Regularly audit 3rd party access to one of least privilege.
- Monitor and remove sensitive information disclosure.

MITRE Ref: T1592; T1589: T1590; T1591; T1596
MITRE Mitigation: M1056 [Pre-Compromise]

For Non-Picnic Customers (IoAttack)

REDUCE EMPLOYEE ATTACK SURFACE

- Identify and block newly registered domains similar to your organization's.
    - This way if used in an attack (e.g., user clicking), the request to domain is blocked.
- Monitor for expiring domains which could be leveraged for the above.
- Expand monitoring to include trusted 3rd parties.
    - This ensures your ecosystem is pro-actively monitored and protected.
    - This can also prevent C2 comms, credential harvesting
- Use Time-Stamp Pivoting to determine domains registered together.

MITRE Ref: T1583.001
MITRE Detection: DS0038

REDUCE ORGANIZATIONAL ATTACK SURFACE

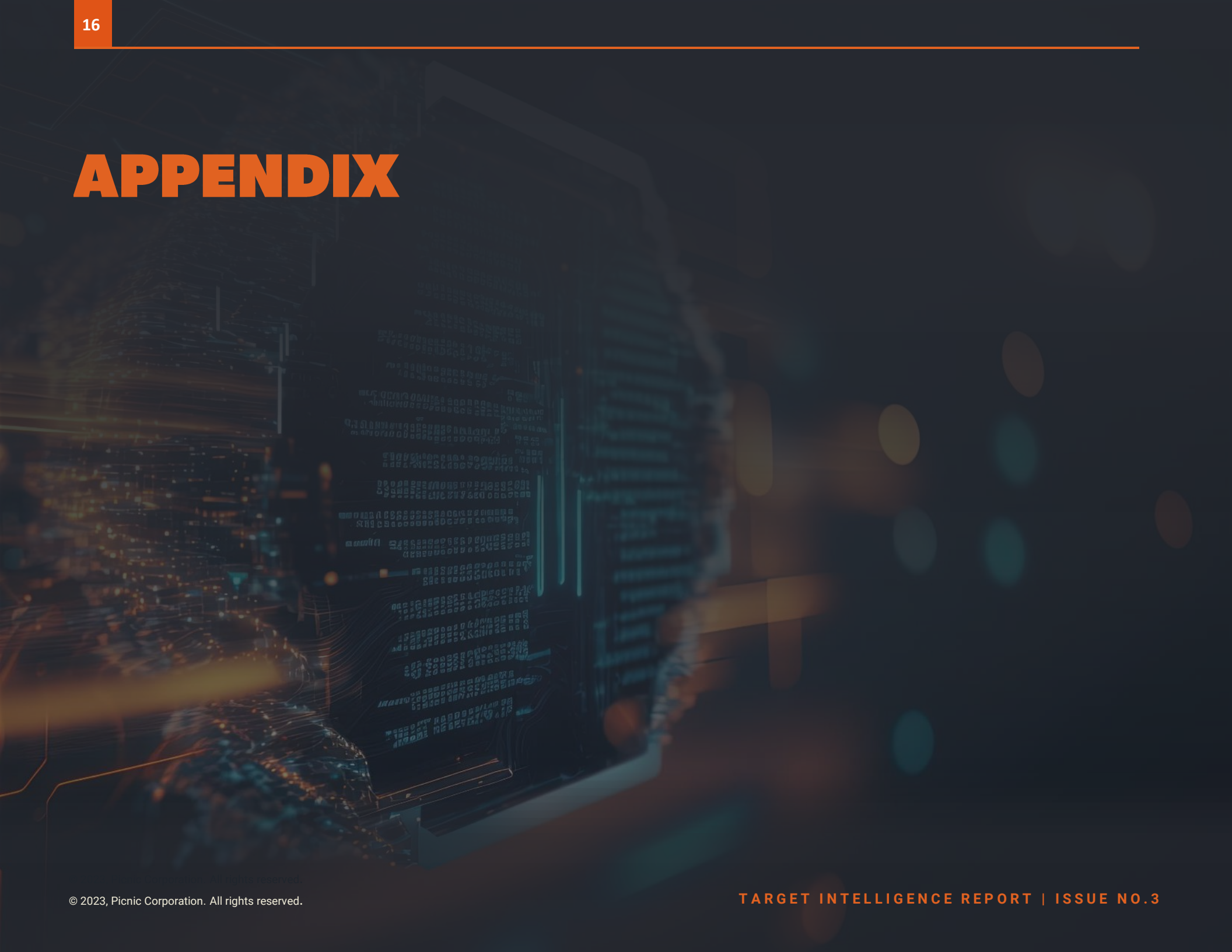
- Identify and block suspicious accounts:
    - Tied to your organization pages
    - Claiming to work for you
    - Befriending employees
    - Detections:
        - Profile creation date
        - Multiple new connections
        - Organizations side, multiple connection request
        - Profile picture, eyes not legitimate / reverse image search

MITRE Ref: T1585.001
MITRE Detection: DS0021

CITATIONS

- https://mailchimp.com/en-gb/january-2023-security-incident/
- https://techcrunch.com/2023/01/18/mailchimp-hacked/
- https://www.bleepingcomputer.com/news/security/mailchimp-discloses-new-breach-after-employees-got-hacked/
- https://thehackernews.com/2023/01/mailchimp-suffers-another-security.html
- https://www.itpro.co.uk/security/data-breaches/369910/mailchimp-data-breach-impact-unravels-second-customer-damage
- https://mailchimp.com/en-gb/august-2022-security-incident/
- https://www.theregister.com/2022/08/16/digital_ocean_dumps_mailchimp/
- https://techcrunch.com/2023/01/18/mailchimp-hacked/
- https://thehackernews.com/2023/01/mailchimp-suffers-another-security.html
- https://www.techtarget.com/searchsecurity/news/252523911/Mailchimp-suffers-second-breach-in-4-months
- https://www.digitalocean.com/blog/digitalocean-response-to-mailchimp-security-incident
- https://www.bleepingcomputer.com/news/security/twilio-hackers-hit-over-130-orgs-in-massive-okta-phishing-attack/
- https://mailchimp.com/en-gb/march-2022-security-incident/
- https://techcrunch.com/2022/04/04/mailchimp-internal-tool-breach/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAACjB0fHNVqDK2EbCrTQdIF9QFDHKAOCRDjUIkNgH4mHjC7LZFdZGXa3FjTE-sgoO97OOaxIM5ul0uNUQDN1U1bhHj-vFkoklpo8szHpGxyyW948ZBV4vaO1bPIXDu0kGN6a-SMGS_iAi_PxRsYqVvulSZ9GTL67vBD2JGxUnWjKV
- https://www.bleepingcomputer.com/news/security/hackers-breach-mailchimps-internal-tools-to-target-crypto-customers/
- https://thehackernews.com/2022/04/hackers-breach-mailchimp-email.html
- https://www.bloomberg.com/news/articles/2022-04-04/mailchimp-says-it-was-breached-and-user-accounts-accessed
- https://www.securemac.com/news/lessons-learned-from-the-mailchimp-breach
- https://blog.trezor.io/ongoing-phishing-attacks-on-trezor-users-edd840b17304
- https://twitter.com/Trezor/status/1510558771944333312?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1510558771944333312%7Ctwgr%5Ed5ce415c383328077c6fc141ac55f99eb8749b62%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcdn.embedly.com%2Fwidgets%2Fmedia.html%3Ftype%3Dtext2Fhtmlkey%3Da19fcc184b9711e1b4764040d3dc5c07schema%3Dtwitterurl%3Dhttps3A%2F%2Ftwitter.com%2Ftrezor%2Fstatus%2F1510558771944333312image%3Dhttps3A%2F%2Fi.embed.ly%2F1%2Fimage3Furl3Dhttps253A252F252Fabs.twimg.com252Ferrors252Flogo46x38.png26key3Da19fcc184b9711e1b4764040d3dc5c07
- https://topclassactions.com/lawsuit-settlements/privacy/data-breach/mailchimp-data-breach-led-to-stolen-crypto-class-action-says/
- https://heimdalsecurity.com/blog/crypto-customers-targeted-in-mailchimp-data-breach/
- https://portswigger.net/daily-swig/trezor-cryptocurrency-wallets-targeted-with-phishing-attacks-following-mailchimp-compromise
- https://www.bleepingcomputer.com/news/security/trezor-warns-of-massive-crypto-wallet-phishing-campaign/
- https://sec.okta.com/scatterswine

APPENDIX



HUMAN ATTACK SURFACE MANAGEMENT PLATFORM

Automated risk detection, prioritization, and mitigation

Social engineering remains the top technique used by threat actors that leads to cybersecurity breaches worldwide, resulting in successful ransomware attacks, sabotage, compromised data, reputational damage, and financial losses.

If 92% of cyberattacks are specifically crafted from data tied to the human element, imagine the impact of knowing, managing, and reducing your human attack surface.

Picnic offers a frictionless cybersecurity solution that mitigates the threat of social engineering by proactively disrupting attacker reconnaissance and resource exploitation, effectively reducing the human attack surface at an enterprise-wide scale.

Why Picnic?

RISK VISIBILITY
Identify the resources most at risk and see the human attack surface through the lens of the social engineer to identify high-value targets and pathways to compromise.

RISK REDUCTION
Manage risk effectively by taking control of your organization's OSINT exposure and empowering HVTs, employees, and supply chain contractors to do the same with their exposure.

PREDICTION & PREVENTION
Eliminate target opportunities and attacker motives. Defend forward by preventing the compromise of users with Privileged Technical Access, wire fraud, credential stuffing, and identity theft, among other threats.

PERFORMANCE
Improve prediction and prevention by automating continuous risk detection for fewer active threats to detect and respond to.

EMPLOYEE PRIVACY & AWARENESS
Enable learning and aha moments through private and personalized risk assessments and recommendations via Picnic's employee facing portal.

SAVINGS
Reduce the operating costs of the cybersecurity program downstream by denying attackers the most attractive ingress vector to corporate and personal data and devices.

READY TO GET STARTED?
Schedule a short demo.
getpicnic.com/schedule-demo

METHODOLOGY

We Use Picnic's Methodology To Gather And Analyze Data About Organizations And Their Employees

1. HUNTING FOR RECON (ORG EXPOSURE)

(a) Employee footprint

(b) Organizational footprint

(c) 3rd Party footprint

2. HUNTING FOR IoATTACK (ATTACKER EXPOSURE)

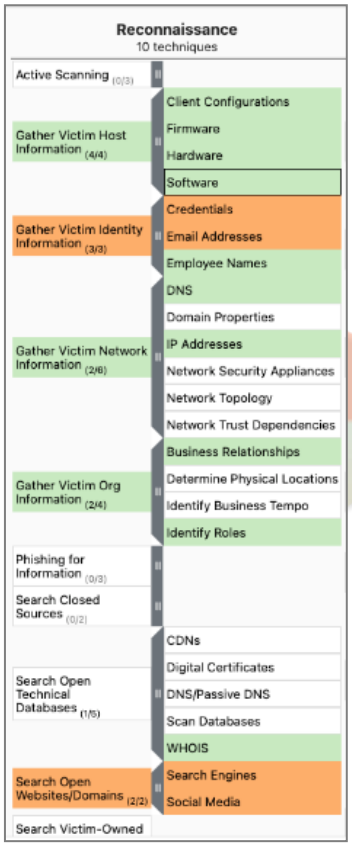
(a) Acquired Infrastructure Domains

(b) Established Accounts

PICNIC'S HUNTING FOR RECON

Org Exposure

1.



EMPLOYEE EXPOSURE

- Name
- Email
- Role [access & value]
- Breached Data [password reuse]
- Interests [emotional ties]
- Associates [trust relationships]

T1589; T1593

ORG EXPOSURE

- External Remote Services [potential entry points]
- Impersonation Ability
- 3rd Party Suppliers / Trusted Relationships
- Technology Stack

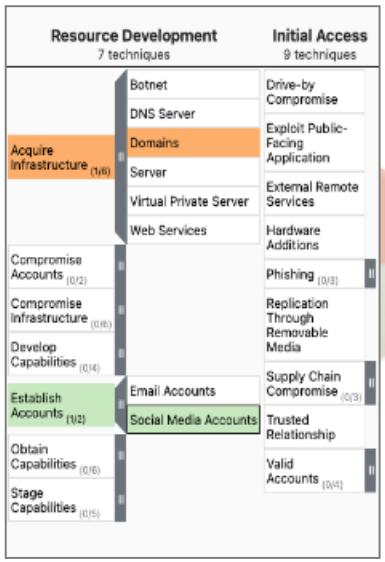
T1592; T1589: T1590; T1591; T1596

WEAPONIZATION

PICNIC'S HUNTING FOR IoATTACK

Attacker Exposure

2.



ACQUIRED INFRASTRUCTURE: DOMAINS

Monitor for newly registered domains similar to the org's & known 3rd parties.

- Registering a domain similar to the target is one of the first steps an attacker takes.
- This is done to disguise inbound/outbound traffic from the target.
- This also could be used for credential harvesting. By identifying the domain earlier, we can anticipate from where the attacks would generate.

T1583

ESTABLISHED ACCOUNTS: SOCIAL MEDIA

- Identify and block suspicious accounts, a.k.a. sock puppets or honey traps.
- These are used to build trust and socially engineer the target into performing an action (e.g., clicking a link).
- This is a common technique used to engage the target outside of the org's traditional security controls (e.g., social media / LinkedIn).

T1585.001 & T1566.003

INITIAL ACCESS

PICNIC'S ATTACK PREDICTION AND MITIGATION FRAMEWORK

DATA COLLECTION

Hunting for Recon

- OSINT on Employees
- OSINT on Target Org
- OSINT on Supply Chain

DATA ANALYSIS

- High Value Targets
- Data Aggregation
- Hunting for IoAttack
- Threat Intelligence

IDENTITY ATTACK SURFACE RISK

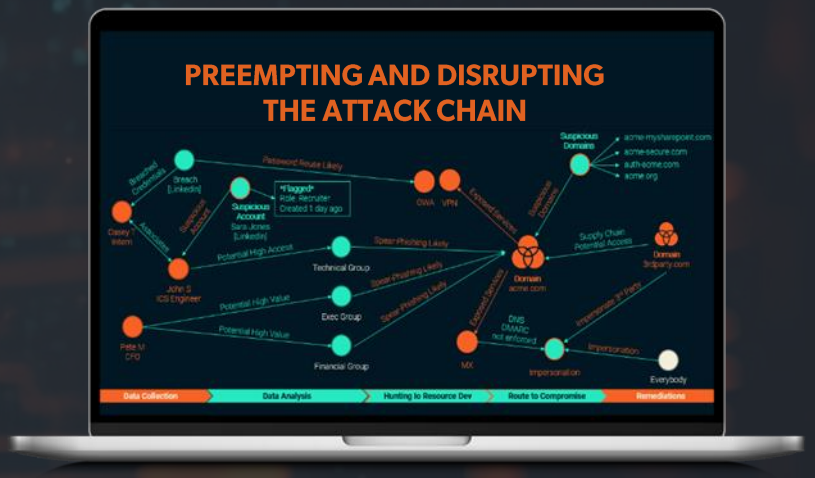
- Expose Paths to Compromise
- Prioritize Paths to Compromise

MITIGATIONS

Prioritized mitigation to reduce mean time to mitigate and reduce attack surface

- User Awareness
- User Reduced Attack Surface
- Security Team Awareness
- Org Reduced Attack Surface
- Supply Chain Awareness
- Supply Chain Reduced Attack Surface

PICNIC'S VISUALIZATION OF ATTACK AND MITIGATION FRAMEWORK



PICNIC™

TARGET INTEL REPORT LIBRARY

MANIT SAHIB
Director of Global Threat Intelligence at Picnic Corporation

Manit is a Certified Red Teamer and Expert Social Engineer. Formerly Head of Red Teaming for the UK's central bank, Manit now leads Picnic's Global Threat Intelligence function, building the attacker mindset and techniques into the Picnic product line.

FELISHA MOUCHOUS
Principal Security Consultant at Picnic Corporation

Felisha is an Ethical Hacker who previously led the Penetration Testing Team for the UK's Central Bank. Felisha now works in Picnic's Global Threat Intelligence function, where she monitors and analyzes threat actor TTPs (tactics, techniques, and procedures) to enhance Picnic's product offering. She also hosts Picnic's Human Hacking 101 series.