PICNIC™

TARGET INTELLIGENCE REPORT

ISSUE NO.1

# TWILIO

## LESSONS LEARNED

PREPARED BY:
MANIT SAHIB & FELISHA MOUCHOUS
Office of Global Threat Intelligence, Picnic Corporation

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

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

Picnic's Target Intelligence Reports help security teams understand how attackers leveraged open-source intelligence (OSINT) exposure and established infrastructure in an attack so organizations can preemptively remediate risk to their organization by reducing their human attack surface to disrupt attacker reconnaissance and resource development.

In this report, we have analyzed the September 2022 Twilio data breach to understand how attackers leveraged OSINT to fuel social engineering against Twilio employees.

Picnic used our technology 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, the Twilio breach highlights 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 October 2022.

# INCIDENT SUMMARY

## Twilio

Twilio is a US-based company that provides communication services for voice calls and SMS messaging for 3rd party companies.

On August 4th, 2022, current and previous employees reported getting SMS messages, pretending to be from IT, asking them to change their expired passwords, and prompting them to log in with their credentials.


The URLs used in this attack looked like legitimate domains since the attacker registered domains with base words such as twillio/okta/sso. When several employees went to log in to the seemingly legitimate sites, the attacker successfully harvested their credentials and used them to gain access to Twilio's internal systems, leading to data compromise for some of their customers. The nature of the attack was such that most organizations would likely have been breached.

Overall, 209 Twilio customers were impacted by this breach, through which some of their data was exposed. One high-profile customer was 'Signal', a privacy-focused messaging service. It is reported that the phone numbers and SMS verification codes for about 1,900 users were breached. 93 Authy users were also found to have been affected. Authy is Twilio's two-factor authentication service. The attacker was able to register additional devices to the Authy accounts as part of this compromise. Okta, a cloud authentication provider, also announced that some of their customers' mobile numbers and SMS OTP (one-time password) codes were also available to the attacker, highlighting growing exposure of supply chain compromises.

# INCIDENT SUMMARY: PRE-ATTACK

## How Threat Actors Leveraged OSINT To Compromise Twilio

**STEP 1**

To expose what happened before the attack, Picnic emulated threat actors by cross referencing employees' public data from Twilio's LinkedIn roster (the starting point of most attacks) against existing exposed 3rd party breach data sets (e.g., haveibeenpwnd.com) and data brokers (e.g., white pages).

The results of these operations, which took less than a few hours in total, was a clean, fully-populated list of personal information such as employees':

- Full Name
- Home Address
- Mobile Number
- Work Email
- Personal Email
- Mobile Number
- Cleartext Passwords

With this information, threat actors were able to move onto the next step of the attack.

**STEP 2**

Attackers created fake domains and login pages that looked like Twilio's—for example: twilio-sso.com or twilio-okta.com (these were alleged to have been used in the attack specifically).

**STEP 3**

Attackers used automated SMS services (such as Twilio's own service or SendGrid) to send mass SMS messages to employees of Twilio. The personal data collected in Step 1 (name, phone, etc.) is the raw material that powers the SMS messages to the intended victims.

**STEP 4**

Attackers then waited for Twilio employees to come to the fake landing page (from Step 2) and enter their valid credentials (also known as a watering hole or credential harvesting attack).

**STEP 5**

Attackers harvested valid credentials provided in Step 4 and reused illicitly in Twilio systems.

# INCIDENT SUMMARY: POST-ATTACK

## Twilio Responded To This Attack By:

- Resetting credentials of the compromised Twilio employee user accounts.
- Revoking all active sessions associated with the compromise of Okta-integrated apps.
- Blocking all indicators of compromise associated with the attack.
- Initiating takedown requests of the fake Twilio domains.
- Implementing stronger two factor precautions and distributing FIDO2 tokens to all employees.
- Implementing additional layers of control within their VPN.
- Removing and limiting certain functionality within specific administrative tooling.
- Increasing the refresh frequency of tokens for Okta-integrated applications.
- Conducting supplemental mandatory security training for all employees regarding attacks based on social engineering.

https://www.twilio.com/blog/august-2022-social-engineering-attack

# THREAT ACTOR

## 0ktapus / Scatter Swine

It has been reported by the cybersecurity company Group-IB that the Twilio hack was part of a larger campaign that targeted and compromised over 130 organizations in and around the same time frame, including Cloudflare, with is also covered in this report (See Page 8). The threat actor responsible has been named as '0ktapus' or 'Scatter Swine' and they are known for persistent phishing campaigns and for targeting organizations that use Okta for authentication. It is reported that they have potentially gathered 10,000 employee credentials during their 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

# RELATED ATTACK

## Cloudflare

Around the same time Twilio was targeted, Cloudflare reported a similar attack and published details on their blog about the nature of the attack and how they were able to stop the attacker from breaching their network.

On July 20, 2022, Cloudflare employees received smishing text messages that contained URLs that directed them to a lookalike Cloudflare Okta (login) page. 76 employees were reported to have received text messages on personal and work phones. Family members of employees are also reported to have received messages. As with the Twilio attack, the threat actor was able to match employee records with phone numbers that are likely to have come from previous external breaches. Cloudflare did not find any evidence in their logs that they were compromised for these details.

Out of those targeted, Cloudflare reported that 3 employees fell for the smishing attack and entered their credentials on the attacker's phishing page (that looked like the Cloudflare Okta login page). The attacker attempted to use these credentials to access the real Cloudflare login page but, since Cloudflare requires a FIDO2-compliant token as their second type of authentication, the attacker could not access their accounts.

## Cloudflare Responded To This Attack By:

- Blocking the phishing domain used in the attack with their Cloudflare gateway
- Resetting compomised employee credentials
- Taking down the attacker infrastructure (domain and digital ocean site)
- Auditing logs and updating monitoring

Source: https://blog.cloudflare.com/2022-07-sms-phishing-attacks/

# PICNIC'S INCIDENT ANALYSIS

For the attacker to be successful, 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 Twilio employees was gathered for the attack.

## Key Findings

**SMISHING**

We identified 1,160 Twilio employees who have one or more phone numbers that are readily available online which could be used in future smishing attacks.

**DATA BROKERS & PREVIOUS BREACHES**

Of the 5,752 Twilio employees whose details we were able to find, 2,328 employees have been in data breaches.

**SUSPICIOUS DOMAINS**

We identified 52 suspicious domains that could be used against Twilio. Using our platform, we can visualize this risk and drilldown into each domain to find out more information.

# TWILIO INCIDENT

## MITRE ATT&CK TTPs

**TA0043**: RECONNAISSANCE

- **T1589**: Gather Victim Identity Information
  - Employee Phone Numbers
  - **T1589.002**: Email Addresses
  - **T1589.003**: Employee Names
- **T1591**: Gather Victim Org Information
  - **T1591.002**: Business Relationships
    - Third Party Relationships, i.e.: 0kta

**TA0042**: RESOURCE DEVELOPMENT

- **T1583**: Acquire Infrastructure
  - **T1583.001**: Domains
  - **T1583.006**: Web Services

**TA0001**: INITIAL ACCESS

- **T1566**: Phishing
  - **T1566.002**: Spear Phishing Link
    - URL Leads To An Okta Log On Page From Which The Attacker Can Harvest The User's Credentials
- **T1133**: External Remote Services
  - Using Harvested Credentials To Access Twilio Resources

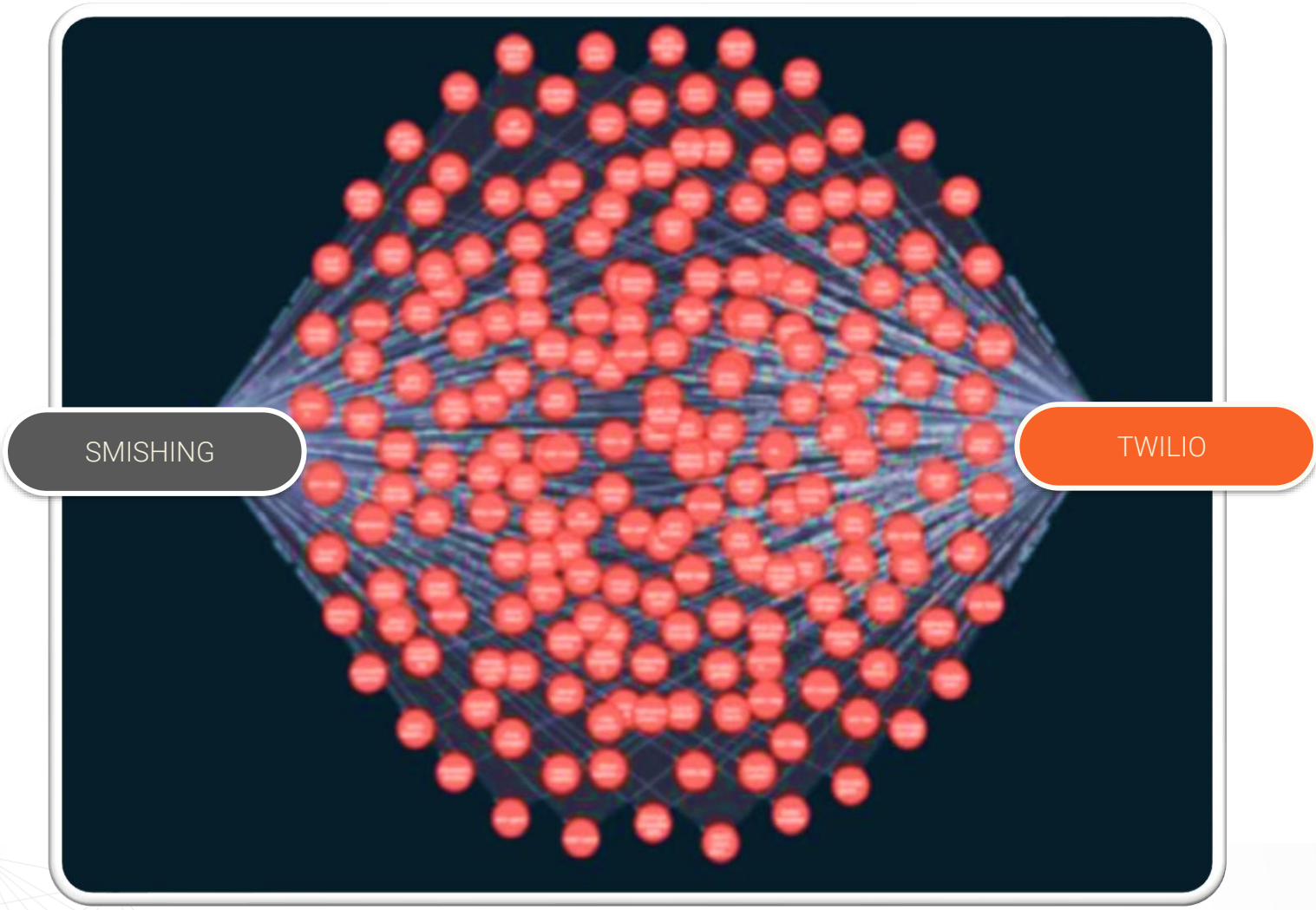
# PICNIC HUNTING FOR RECON

## Smishing Risk View

Out of the 5,752 Twilio employees whose details we have found, 1,160 of these have one or more phone numbers exposed on the internet.

The attacker in the Twilio breach was able to leverage these exposed numbers to launch a phishing campaign against the employees.

**Twilio employees that can be targeted in a Smishing attack.**




Threat Type  Employee  Company

# PICNIC HUNTING FOR RECON

## Credential Stuffing Risk View

Our platform identified 2,328 Twilio employees who have been involved in data breaches where their personal and/or work passwords were exposed.

**Twilio employees that can be targeted in a Credential Stuffing attack.**

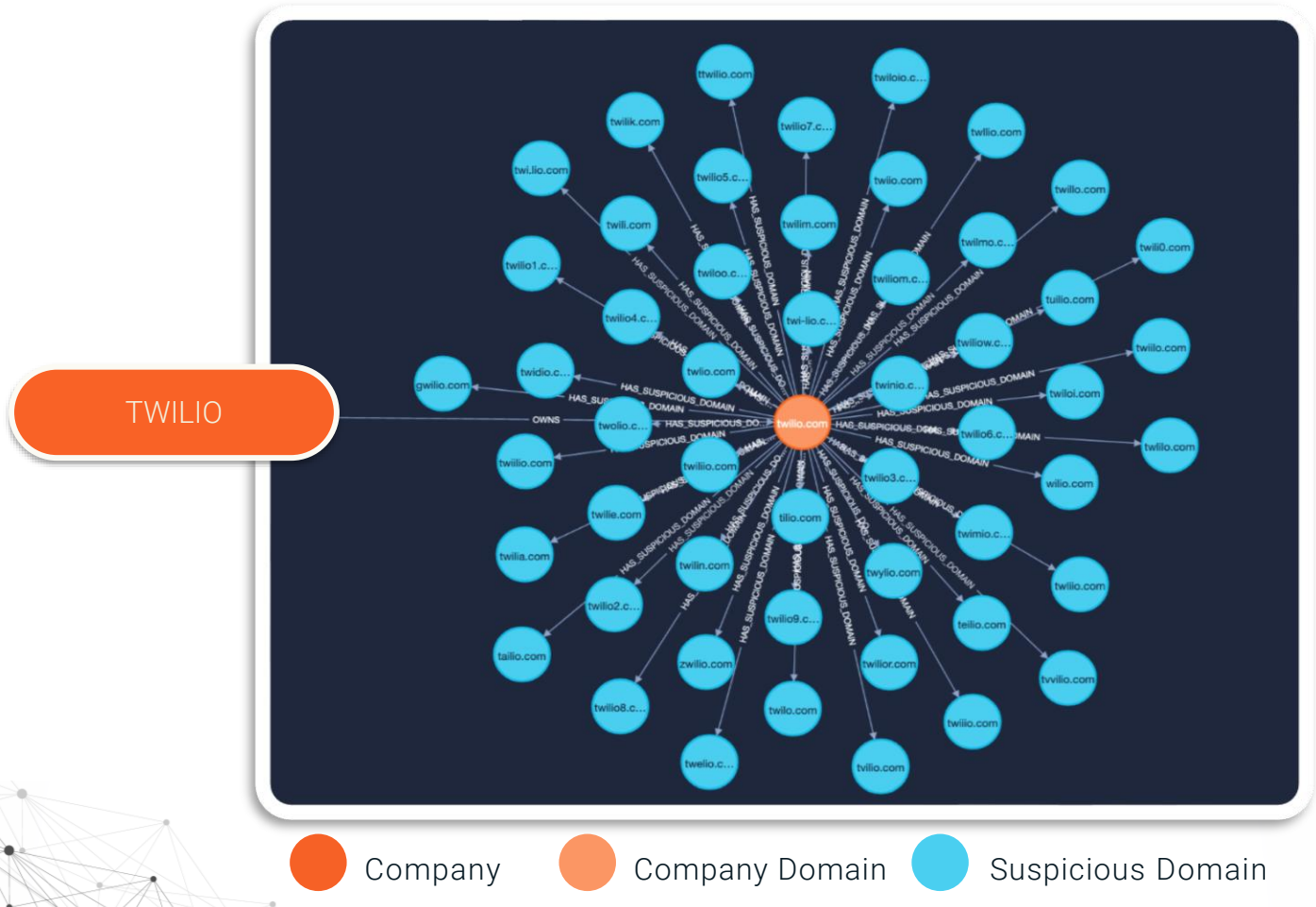
# PICNIC IoATTACK

## Suspicious Domains View

Picnic's platform identified 52 registered suspicious domains that could be used to target Twilio.

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 domain's 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 them before they can be used.



# THREAT ACTOR: SCATTER SWINE

## Suspicious Domains View

### 52 REGISTERED SUSPICIOUS DOMAINS

1. ttwilio.com
2. twilie.com
3. twilia.com
4. twelio.com
5. twiloi.com
6. twi.lio.com
7. zwilio.com
8. twolio.com
9. twiloo.com
10. teilio.com
11. tailio.com
12. gwilio.com
13. twiliio.com
14. twiilio.com
15. twilio1.com
16. twilio2.com
17. twilio3.com
18. twilio4.com
19. twilio5.com
20. twilio6.com
21. twilio7.com
22. twilio8.com
23. twilio9.com
24. twiliom.com
25. twilior.com
26. twiliow.com
27. tuilio.com
28. tvilio.com
29. twidio.com
30. twilik.com
31. twilim.com
32. twilin.com
33. twilmo.com
34. twimio.com
35. twinio.com
36. twylio.com
37. tvvilio.com
38. twiiio.com
39. twiilo.com
40. twili0.com
41. twillo.com
42. twliio.com
43. twlilo.com
44. twllio.com
45. twi-lio.com
46. twiloio.com
47. tilio.com
48. twiio.com
49. twili.com
50. twilo.com
51. twlio.com
52. wilio.com

### THIS THREAT ACTOR IS ALSO KNOWN TO USE THE BELOW DOMAINS

- {targeted organization}-corp.net
- {targeted organization}-help.com
- {targeted organization}-help.net
- {targeted organization}-helpdesk.com
- {targeted organization}-login.co
- {targeted organization}-mfa.com
- {targeted organization}-okta.co
- {targeted organization}-okta.com
- {targeted organization}-okta.net
- {targeted organization}-okta.org
- {targeted organization}-okta.us
- {targeted organization}-onelogin.com
- {targeted organization}-sso.com
- {targeted organization}-sso.net
- {targeted organization}-vpn.com
- {targeted organization}-vpn.net
- {targeted organization}-vpn.org
- okta-{targeted organization}.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 org'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 remove sensitive information disclosure identified by Picnic, such as exposed passwords associated with personal and org breached credentials.

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]

# MITIGATIONS

## For Non-Picnic Customers (IoAttack)

### REDUCE EMPLOYEE ATTACK SURFACE

- Identify and block newly registered domains similar to your org'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, cred 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
        - Org side, multiple connection request
        - Profile picture, eyes not legitimate / reverse image search

Mitre Ref: T1585.001
Mitre Detection: DS0021

# CITATIONS

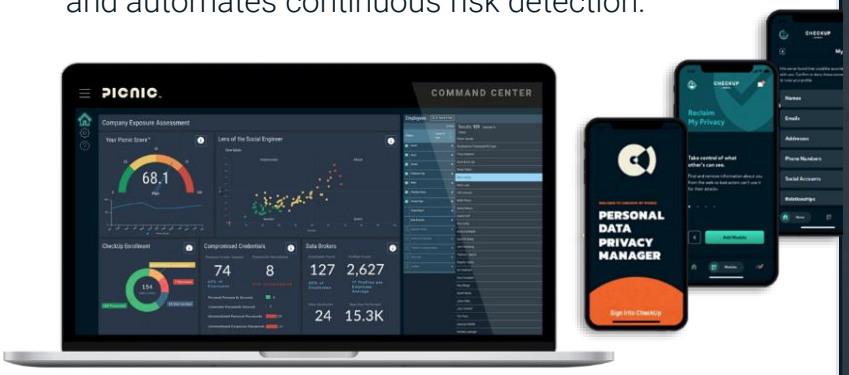

- https://www.twilio.com/blog/august-2022-social-engineering-attack
- https://support.signal.org/hc/en-us/articles/4850133017242
- https://techcrunch.com/2022/08/15/signal-phone-number-exposed-twilio
- https://www.twilio.com/blog/august-2022-social-engineering-attack
- https://www.bleepingcomputer.com/news/security/okta-one-time-mfa-passcodes-ex-posed-in-twilio-cyberattack/
- https://sec.okta.com/scatterswine
- https://www.malwarebytes.com/blog/news/2022/08/twilio-data-breach-turns-out-to-be-more-elaborate-than-suspected
- https://techcrunch.com/2022/08/25/twilio-hackers-group-ib/
- https://sec.okta.com/scatterswine
- https://www.theregister.com/2022/08/25/twilio_cloudflare_oktapus_phishing
- https://blog.cloudflare.com/2022-07-sms-phishing-attacks

# APPENDIX

# ABOUT PICNIC

## Enterprise-wide Social Engineering Detection, Protection, And Prevention

Picnic's platform is a holistic social engineering risk management solution for enterprises. Our technology emulates attacker reconnaissance on the public data footprint of your organization and its people, automatically exposes the pathways to compromise and likely human targets revealed by your data, streamlines remediation, and automates continuous risk detection.




- Continuously monitor and reduce company and employee OSINT exposure, commonly leveraged for pretexting and initial access.
- Preemptively identify and block threat actor established infrastructure and accounts before they can be used for weaponization and delivery.
- Utilize a dual-pronged approach to preempt and disrupt attacker reconnaissance and resource development, mitigate risks, and prevent compromise.

We Proactively See And Remediate Human Risk Beyond The Corporate Perimeter

### RECON

Leverage full visibility of external company and employee data to hunt threats, eliminate risk, and safeguard users

### ANALYZE

Automatically expose social engineering attack and compromise paths before they happen

### REMEDIATE

Neutralize vulnerabilities, reduce attack surface, and prevent attacks

LEARN MORE

# 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

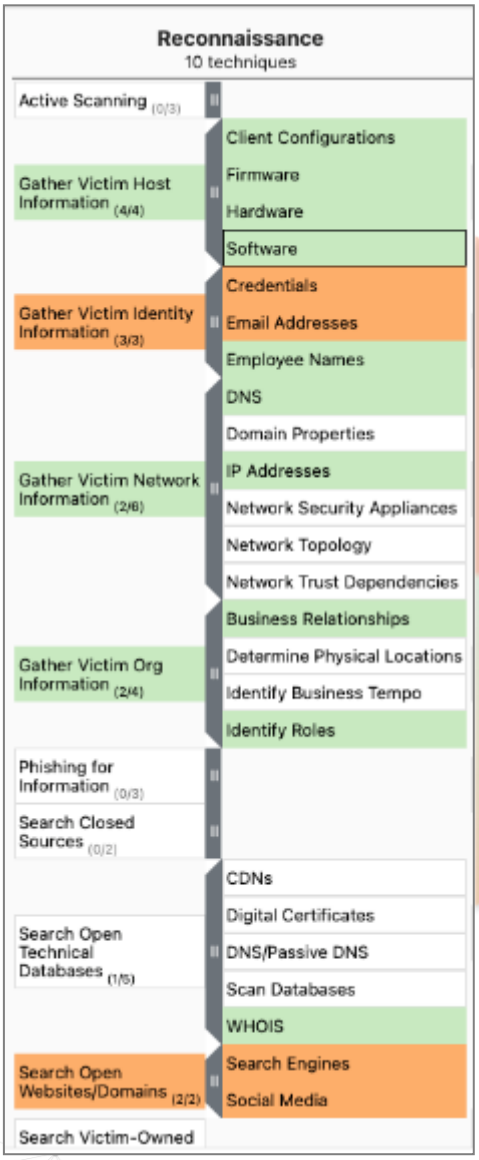
(c) 3rd Party footprint

### 2. HUNTING FOR IoATTACK (ATTACKER EXPOSURE)

(a) Acquired Infrastructure Domains

(b) Established Accounts

# PICNIC'S HUNTING FOR RECON (ORG EXPOSURE)




## EMPLOYEE EXPOSURE

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

T1589; T1593

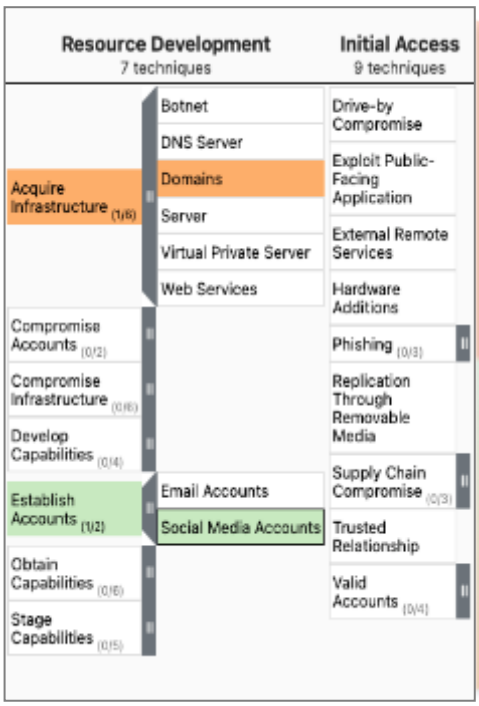
## ORG EXPOSURE

- 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)




## 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

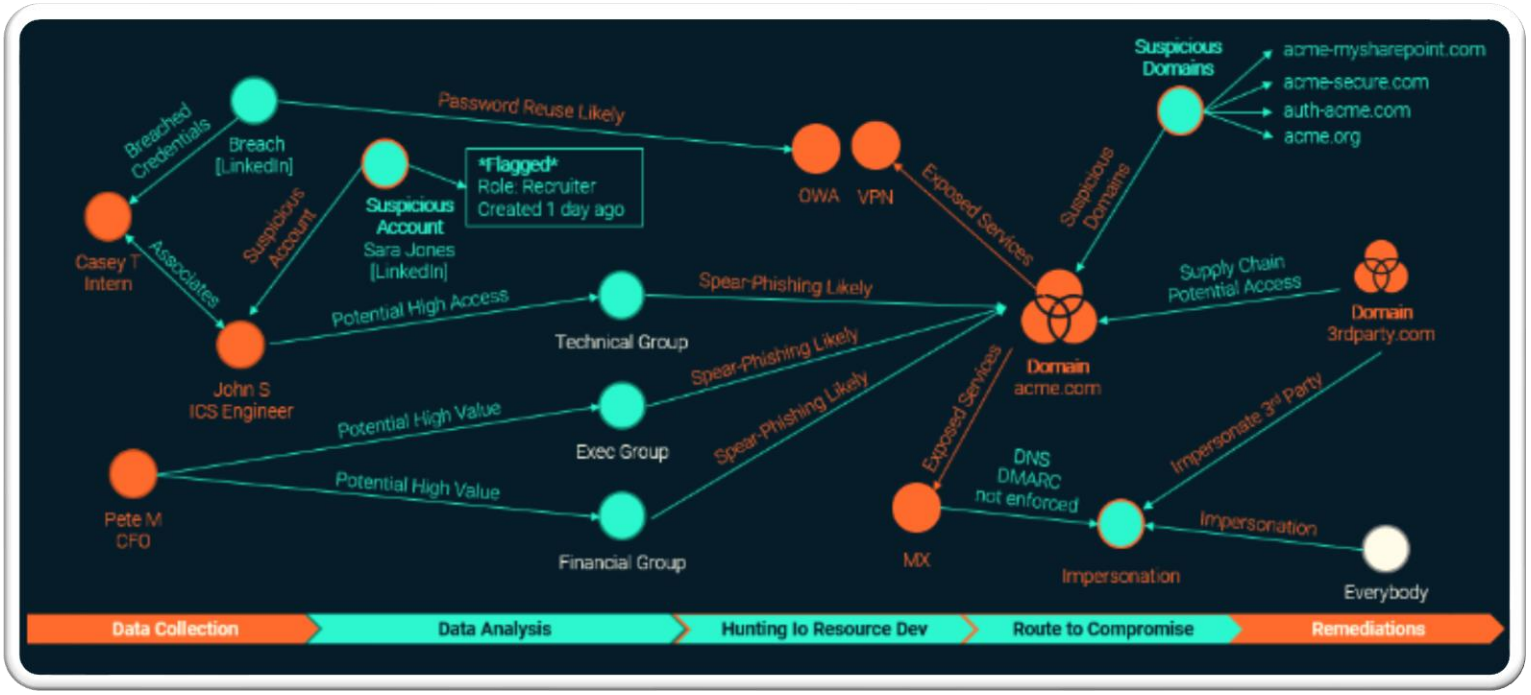
- Expose Paths to Compromise
- Prioritize Paths to Compromise

## 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

## Preempting And Disrupting The Attack Chain

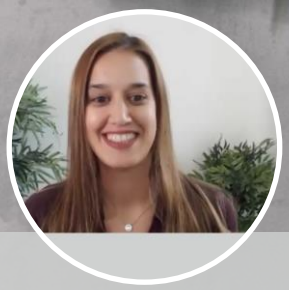


PICNIC™

## 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.