Retool August 2023 Social Engineering Attack Summary

Incident Name	Retool August 2023 Social Engineering Attack
Date of Incident	August 27th, 2023
Summary	Retool, a popular software company, announced on September 13, 2023, that they had fallen victim to a cyber attack in August 2023. According to their blog post, their employees were targeted in a smishing campaign on August 27, 2023. The employees received smishing texts claiming to be from their IT department regarding an account issue that would impact their healthcare coverage enrollment. Retool had recently transitioned to Okta, and the URL used in these messages appeared to be a legitimate Okta login URL. Unfortunately, one employee fell for this smishing campaign and unknowingly logged in via the malicious URL. Subsequently, the threat actor posing as IT contacted the employee via phone call, using a deepfake of a real employee. It has been reported that the threat actor had access to office floor plans and processes, enhancing their ability to convince the targeted employee and acquire their MFA code. Once in possession of this code, the threat actor added their own device to the employee's Okta account, expanding their access within the environment. Leveraging this access, they logged into an active G Suite session and gained visibility into all authenticator codes synced to that account. In April 2023, Google introduced the option for users to sync these codes to simplify transfers between devices; however, it is crucial to note that this feature can be disabled to prevent automatic syncing. Corporate accounts face challenges in centrally disabling this setting, requiring coordination with Google to mitigate similar incidents at other companies. Armed with the synced MFA codes, the threat actor proceeded to access Retool's VPN and internal admin systems. Exploiting this access, they targeted accounts associated with cryptocurrency customers. As a result, 27 accounts were compromised. Retool promptly informed these affected customers, restored their accounts, and revoked all internal access to authenticated sessions for employees. They also conducted a comprehensive review of access permissions. While the identity of the threat actor has not been officially disclosed, it is noteworthy that phishing campaigns utilizing Okta as a pretext continue to be

	widely employed and successful. Recently, Okta, a provider of identity and authentication services, issued a warning to its customers about an ongoing, sophisticated social engineering attack targeting IT service desk personnel. Multiple Okta customers have reported falling victim to these attacks since August 2023. The attacks exploit vishing techniques to deceive employees.
Key Social Engineering/OSINT Themes	• **Recon** - Retool employee and organizational information was harvested. The threat actor leveraged exposed employee information to conduct a social engineering attack. • **Smishing** - Using a malicious Okta Retool URL , the threat actor socially engineered the employee into clicking the link. • **Vishing -** Once the employee logged in via the malicious URL, they called the employee using a deepfake voice to impersonate an IT helpdesk employee.

Picnic's Recommended Remediations.
 	
For detailed remediations, see the Human Attack Surface Protection Framework (HASP).
	High Risk Employees
	• **HASP Framework 1.1 — Identify high value employee targets**
	  ◦ MITRE Alignment: T1589
	  ◦ NIST CSF Alignment: ID.RA-1
	• **HASP Framework 1.3 — Conduct social engineering risk assessments for high value employee targets**
	  ◦ MITRE Alignment: M1047
	  ◦ NIST CSF Alignment: ID.RA-5
	• **HASP Framework 1.5 — Establish and implement procedures for high value employee targets**
	  ◦ MITRE Alignment: M1056
	  ◦ NIST CSF Alignment: PR.IP-7
	• **HASP Framework 1.7 — Increase detection and monitoring for high value employee targets**
	  ◦ MITRE Alignment: M1040
	  ◦ NIST CSF Alignment: DE.CM-3
	
	Exposed Employee PII
	• **HASP Framework 2.1 — Identify exposed employee PII**
	  ◦ MITRE Alignment: T1589
	  ◦ NIST CSF Alignment: ID.RA-2
	• **HASP Framework 2.2 — Reduce exposed employee PII**
	  ◦ MITRE Alignment: M1056
	  ◦ NIST CSF Alignment: PR.IP-7
	
	Exposed Credentials
	• **HASP Framework 3.7 — Restrict service account access**
	  ◦ MITRE Alignment: M1026
	  ◦ NIST CSF Alignment: PR.AC-4
	• **HASP Framework 3.8 — Monitor for account takeover (including real time alerts on exposed credentials)**
	  ◦ MITRE Alignment: DS0028
	  ◦ NIST CSF Alignment: DE.CM-3
	• **HASP Framework 3.9 — Monitor for MFA configuration changes**

- MITRE Alignment: M1032
- NIST CSF Alignment: DE.CM-3

- **HASP Framework 3.10 — Monitor for new MFA registrations**
  - MITRE Alignment: DS0028
  - NIST CSF Alignment: DE.CM-3

Exposed Remote Services

- **HASP Framework 4.2 — Identify exposed shadow IT**
  - MITRE Alignment: T1133
  - NIST CSF Alignment: ID.AM-4
- **HASP Framework 4.4 — Manage shadow IT / remote access**
  - MITRE Alignment: M1030
  - NIST CSF Alignment: PR.AC-3

Indicators of Attack

- **HASP Framework 7.1 — Monitor for suspicious external accounts**
  - MITRE Alignment: T1585.001
  - NIST CSF Alignment: DE.CM-7
- **HASP Framework 7.2 — Request takedowns for suspicious external accounts**
  - MITRE Alignment: M1056
  - NIST CSF Alignment: PR.IP-7
- **HASP Framework 7.3 — Alert your organization about suspicious external accounts**
  - MITRE Alignment: DS0021
  - NIST CSF Alignment: RS.MI-3
- **HASP Framework 7.4 — Monitor for suspicious domains**
  - MITRE Alignment: T1583.001
  - NIST CSF Alignment: DE.CM-7
- **HASP Framework 7.5 — Block suspicious domains**

  MITRE Alignment: DS0038

  NIST CSF Alignment: PR.AC-4

Cyber Awareness

- **HASP Framework 8.1 — Train employees on social engineering attacks**
  - MITRE Alignment: M1017
  - NIST CSF Alignment: PR.AT-1
- **HASP Framework 8.2 — Provide employees social engineering phishing simulation training**
  - MITRE Alignment: M1017
  - NIST CSF Alignment: PR.AT-1
- **HASP Framework 8.4 — Build and establish social engineering policies, processes, and procedures**

  MITRE Alignment: N/A

	NIST CSF Alignment: PR.IP-1
Industry	Software
Actor	TBC
Motivations	Financial
Related Hacks	Coinbase / CoinsPaid
Breach Notice/Company Notice	When MFA isn't actually MFA
Other Sources	Deepfake and smishing. How hackers compromised the accounts of 27 Retool customers in the crypto industry Retool blames breach on Google Authenticator MFA cloud sync feature