Okta October 2023 Breach

Incident Name	Okta October 2023 Breach
Date of Incident	2nd - 18th October 2023
Summary	Okta, a well-known identity and authentication provider based in the US, suffered a data breach in October 2023. On October 20, 2023, Okta released details stating that the threat actor gained access to a support case management system and not their main production system. The threat actor used stolen credentials, likely obtained by socially engineering an Okta employee, to gain access to the compromised system. Once the threat actor gained access, they were able to view support files uploaded by Okta customers. These files include HTTP Archive (HAR) files, which Okta uses for troubleshooting issues by replicating customer browsing activity. These files contain sensitive data such as session tokens and cookies, which allowed the threat actor to impersonate valid users. Okta has informed impacted customers and asked them to revoke session tokens while recommending that HAR files be sanitized before being shared. They have also released a number of indicators for the threat actor, such as IPs, so that they can be blocked by their customers. On October 2nd, 2023, BeyondTrust, a customer of Okta, detected suspicious activity on an internal Okta admin account. They immediately contained the activity so that there was no impact on customers. On October 20th, 2023, BeyondTrust released a detailed write-up of this incident and timeline. They state that the threat actor was using a valid session cookie stolen from Okta's support system. Once the activity was contained, they informed Okta about the potential breach. BeyondTrust did not receive official confirmation of this breach until October 19th, 2023 after providing evidence to Okta. Another customer of Okta, Cloudflare, had also reported a similar breach. Cloudflare released a detailed write-up on this incident. They noticed suspicious activity on their system on October 18th, 2023. They traced this attack back to Okta, where the threat actor leveraged an authentication token to gain access to Cloudflare's Okta instance. Cloudflare's Security Incident Response Team contained the incident to minimize the impact. They stated that none of their customers' information or systems were affected. They also stated that they contacted Okta before it was reported to them and said that the threat actor leveraged a token from an Okta support ticket opened by a Cloudflare employee. The actor was able to access two Cloudflare employee accounts. This is not the first time Cloudflare has dealt with an Okta-based attack. In January 2022, Okta was compromised by threat actor LAPSUS$ where they gained access to a third-party Okta support

	engineer account (SITEL) with superuser access. Many customer tenants were accessed this way, and Cloudflare reset passwords as a precautionary measure. Okta had previously 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** - Okta employee and organizational information was harvested. The threat actor is likely to have leveraged exposed employee information to conduct a social engineering attack to steal employee credentials. • **Credential Harvesting -** The threat actor is likely to have used social engineering tactics such as phishing to trick an Okta employee into handing over their credentials. Note: Okta has stated that stolen credentials were used in this attack but, at the moment, has not released any details on how they were stolen.

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 3.1 — Identify exposed work credentials**
	  ◦ MITRE Alignment: T1589.001
	  ◦ NIST CSF Alignment: ID.RA-2
	• **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	Technology
Actor	TBD
Motivations	Financial
Related Hacks	Cloudflare, BeyondTrust, Twilio
Breach Notice/Company Notice	Tracking Unauthorized Access to Okta's Support System
Other Sources	How Cloudflare mitigated yet another Okta compromise BeyondTrust Discovers Breach of Okta Support Unit | BeyondTrust Cloudflare's investigation of the January 2022 Okta compromise Okta's Investigation of the January 2022 Compromise Threat actors breached Okta support system and stole customers' data Okta says its support system was breached using stolen credentials