Okta August 2023 Social Engineering Attack Advisory

Incident Name	Okta August 2023 Social Engineering Attack Advisory
Date of Incident	August 2023
Summary	Okta, a provider of identity and authentication services, recently issued a warning to its customers regarding an ongoing, sophisticated social engineering attack that has been targeting Okta customers. Beginning in August of 2023, numerous Okta customers reported being targeted by social engineering attacks that focused on IT service desk employees. The threat actor utilized a technique known as vishing to trick employees into resetting multi-factor authentication (MFA) settings for highly privileged users. If successful, the threat actor leveraged their access to Okta super admins and abused legitimate features to impersonate other users within the organization. Several tactics, techniques, and procedures (TTPs) were identified by Okta during the investigation. One notable finding was that the threat actors seemed to possess passwords for privileged accounts, or were able to manipulate the delegated authentication flow via active directory before contacting IT service desk employees. The threat actors also utilized anonymizing proxy services with IP addresses and devices not previously associated with the compromised user's account. Once the super admin accounts were compromised, the threat actors used these permissions to give higher privileges to other accounts, reset or remove MFA settings for admin accounts, and even configure a second Identity Provider to act as an "impersonation app" to access applications within the compromised organizations on behalf of other users. The identity of the threat actor remains unknown, but the tactics used resemble those previously employed by groups known as "muddled libra," "scattered spider," and "scatter swine," who utilize the 0ktapus phishing kit to create fake auth portals to harvest credentials and MFA tokens. The muddled libra group has previously targeted organizations in the software automation, Business Process Outsourcing (BPO), telecoms, and technology industries, and they are known to conduct recon on organizations to gather employee data such as credentials and phone numbers. They then register lookalike domains and use the 0ktapus phishing kit to trick employees through smishing or vishing campaigns. Similar attacks have been carried out against other companies that use Okta for authentication, such as Twilio and Cloudflare, where smishing campaigns were employed by the threat actor. The 0ktapus group has also been attributed to a smishing campaign against crypto exchange Coinbase in February of 2023, in which an employee was tricked into entering their credentials into a phishing site. These cases illustrate the

	growing popularity of using authentication platforms such as Okta for threat actors, who have been highly successful in compromising target organizations using social engineering tactics and credential harvesting.
Key Social Engineering/OSINT Themes	• **Recon** - Customer of Okta, employee and organizational information was harvested. The threat actor leveraged exposed employee information to conduct a social engineering attack. • **Vishing** - The threat actor targeted IT service personnel with high privileges and tried to convince them to reset MFA on high privileged accounts.
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	Telecommunications, Technology, Professional Services
Actor	Suspected to be 'muddled libra', 'scattered spider' or 'scatter swine'
Motivations	Financial
Related Hacks	Twilio/ Cloudflare/ Coinbase

Breach Notice/Company Notice	Cross-Tenant Impersonation: Prevention and Detection
Other Sources	Okta Warns of Social Engineering Attacks Targeting Super Administrator Privileges Okta: Hackers target IT help desks to gain Super Admin, disable MFA More Okta customers trapped in Scattered Spider's web https://unit42.paloaltonetworks.com/muddled-libra/ 'Muddled Libra' Uses Oktapus-Related Smishing to Target Outsourcing Firms