Kroll August 2023 SIM Swap Attack

Incident Name	Kroll August 2023 SIM Swap Attack
Date of Incident	August 19th, 2023
Summary	Kroll is a global company providing organizations with risk and financial solutions. On August 19th, 2023, they discovered that a T-Mobile account belonging to a Kroll employee had been compromised by a threat actor, and T-Mobile had allowed the threat actor to transfer the employee's phone number to their own device. It is alleged that once the threat actor gained access to the phone number, they were able to bypass multi-factor authentication (MFA) and access the employee's account. As a result, the threat actor was able to access Kroll's cloud-based assets, which included personal information such as names, addresses, emails, and debtor claim details of bankruptcy claimants from companies like BlockFI, FTX, and Genesis. Kroll has notified the affected customers about the breach of their data. FTX and BlockFI, two affected companies, have released statements confirming that user passwords and funds were not impacted by this breach since it was specific to Kroll's systems. Additionally, several individuals have reported receiving phishing emails related to this breach. FTX has shared examples of these emails on social media platforms. The phishing emails aim to deceive customers by impersonating FTX and encouraging them to withdraw their digital assets. The ultimate goal is to steal customers' seeds in order to empty their crypto wallets.
Key Social Engineering/OSINT Themes	• **Recon** - Kroll employee and organizational information was harvested, including employee phone numbers and personal details. The threat actor leveraged exposed employee information to perform a SIM swap attack. • **SIM Swap** - The threat actor used the employee information to contact T-Mobile and swap their number to the threat actors SIM so that they would receive all employee SMS messages and calls. This access was then used to access the employees cloud based account to access the data.
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

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	Financial Services, Professional Services
Actor	Unknown
Motivations	Financial
Related Hacks	Coinbase / CoinsPaid
Breach Notice/Company Notice	Security Incident | Kroll
Other Sources	Kroll data breach exposes info of FTX, BlockFi, Genesis creditors Kroll's Crypto Breach Highlights SIM-Swapping Risk Kroll Employee SIM-Swapped for Crypto Investor Data Kroll Suffers Data Breach: Employee Falls Victim to SIM Swapping Attack