CoinsPaid July 2023 Social Engineering Attack Summary

Incident Name	CoinsPaid Social Engineering Attack
Date of Incident	July 22nd, 2023
Summary	CoinsPaid, one of the world's largest cryptocurrency payment providers, suffered a cyber attack on July 22, 2023, which resulted in the theft of $37.3 million. The company suspects that the North Korean APT Lazurus group, which is known to target crypto firms, is behind this attack. Although it is reported that customer funds were not impacted, CoinsPaid's platform and revenue were affected, and the incident required CoinsPaid to shut down operations temporarily. At the time, the company launched an investigation to track and mark the stolen funds with the help of other crypto companies. CoinsPaid released a detailed report on how the attack unfolded on August 7, 2023. The company found that the hacker group spent six months trying to gain access. This included aggressive phishing attempts on CoinsPaid team members, bribery and fake-hiring campaigns, and DDoS attempts. On July 22, the group was finally able to gain access. CoinsPaid stated that because it was not possible to hack the company's systems externally without gaining access to an employee's computer, the group leveraged its extensive reconnaissance to conduct highly sophisticated social engineering campaigns. During these campaigns, one CoinsPaid employee received a fake job offer from crypto.com and, during the interview process, received a test assignment that required the installation of an application that was malicious. Once this application was installed, profiles and keys were stolen from the employee's computer and the attackers gained access to the infrastructure. Once inside, the group found a vulnerability and exploited this to open a backdoor. The attackers then used knowledge gained from their recon of CoinsPaid to withdraw funds.
Key Social Engineering/OSINT Themes	• **Recon** - CoinsPaid employee and organizational information was harvested. The threat actor leveraged exposed employee information to conduct a social engineering attack. • **Fake Job Posting pretext** - The threat actor targeted the employee with a fake cryptocurrency job advert. • **Phishing** - Using the job offer pretext, the threat actor socially engineered the employee into taking part in an interview assessment where they were prompted to install malicious software, which led to the compromise of CoinsPaid.
Picnic's Recommended Remediations.	**High Risk Employees** • **HASP Framework 1.1 — Identify high value employee targets** ◦ MITRE Alignment: T1589

For detailed remediations, see the Human Attack Surface Protection Framework (HASP).

- 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	Cryptocurrency
Actor	Lazurus
Motivations	Financial
Related Hacks	Coinbase
Breach Notice/Company Notice	CoinsPaid is back to processing after being hit by a hacker attack. Client funds were not affected and are fully available The CoinsPaid Hack Explained: We Know Exactly How Attackers Stole and Laundered $37M USD
Other Sources	Social Engineering Enabled $37 Million Theft From Crypto Firm CoinsPaid CoinsPaid blames Lazarus hackers for theft of $37,300,000 in crypto