[Actor Preview]

Code Name:
Celestial Cowboy Heist

Affiliation(s):
No known affiliations. Likely independent financially motivated cybercriminals.

Operating Region(s):
Likely external, using phishing infrastructure and compromised accounts.

Motivation(s): Financial gain through theft and resale of intellectual property (exclusive fashion designs).

Summary: The Celestial Cowboy Heist was a phishing-driven cyberattack against Celestial Cowboy Couture, a luxury fashion brand in Deadwood, South Dakota. The campaign began when CEO Jane Hartley clicked on a malicious link, leading to the compromise of her account. The attackers then used Jane's trusted identity to send phishing emails to lead fashion designer Megan Lucia. Megan executed a malicious payload that gave the attackers deeper access. Using this foothold, the attackers discovered and exfiltrated sensitive fashion designs, which were later sold on OutlawBuy.com, damaging the brand's reputation.

Initial Access Vector

The initial compromise occurred when CEO **Jane Hartley** clicked on a phishing link that resulted in her account being taken over. From her compromised account, the attackers sent internal phishing emails to **Megan Lucia (Lead Fashion Designer)**. The phishing email had the subject line: "URGENT: From your CEO - Immediate Action Required: You are getting promoted Cowboy!!!!" Believing it to be legitimate, Megan opened the attachment and executed the malicious payload.

Post Exploitation Activity

After compromising **Megan Lucia's** account and workstation, the attackers discovered a folder named "designs_to_steal" containing four suspicious ZIP files. They also deployed a malicious executable **advanced-uploader.exe**. Obfuscated PowerShell commands were executed to connect to attacker domains, including **im-your-huckleberry.com**. Using these tools, the attackers staged fashion design files for exfiltration. Soon after, knock-off designs appeared on **OutlawBuy.com**, confirming the theft and monetization of Celestial Cowboy Couture's intellectual property.

Command and Control

Persistence and communication with attacker infrastructure were maintained through obfuscated PowerShell commands running via **C:\Windows\System32\powershell.exe**. The commands were encoded in Base64 and reversed before decoding, leading to URLs hosted at **im-your-huckleberry.com**. Suspicious logins originated from IP **192.124.249.15**, which was observed accessing both Megan Lucia's and Jane Hartley's accounts. Additional activity was tied to IP **142.250.191.78**.

Exfiltration and Impact

The attackers used **advanced-uploader.exe** to package and upload stolen designs to external servers. The stolen files were later leaked and sold on **OutlawBuy.com**. Threat domains used in this campaign included **secure-celestial.com**, **celestialcowboy-support.com**, and **cccouture-hr-update.com**. The breach severely harmed Celestial Cowboy Couture's reputation and financial prospects, as their flagship collection was compromised before launch.

Appendix: Indicators of Compromise

Domains:
- im-your-huckleberry.com
- secure-celestial.com
- celestialcowboy-support.com
- cccouture-hr-update.com

Threat IPs:
- 192.124.249.15
- 142.250.191.78

Malicious Files:
- advanced-uploader.exe
- designs_to_steal/*.zip

Emails:
- From: jane_hartley@celestialcowboy.com (compromised CEO)
- To: megan.lucia@celestialcowboy.com (Lead Fashion Designer)
- Subject: URGENT: From your CEO - Immediate Action Required: You are getting promoted Cowboy!!!!

Analyst Notes

The Celestial Cowboy Heist highlights how cybercriminals exploited the trust between executives and staff. **Jane Hartley (CEO)** was the initial victim, enabling attackers to pivot internally and compromise **Megan Lucia (Lead Fashion Designer)**. From there, they exfiltrated high-value intellectual property. The attack also exploited Megan's online footprint, as her public LinkedIn frustration post may have marked her as an easy target. Enhanced phishing awareness training, multi-factor authentication, and continuous monitoring of login anomalies could have prevented or minimized this incident.