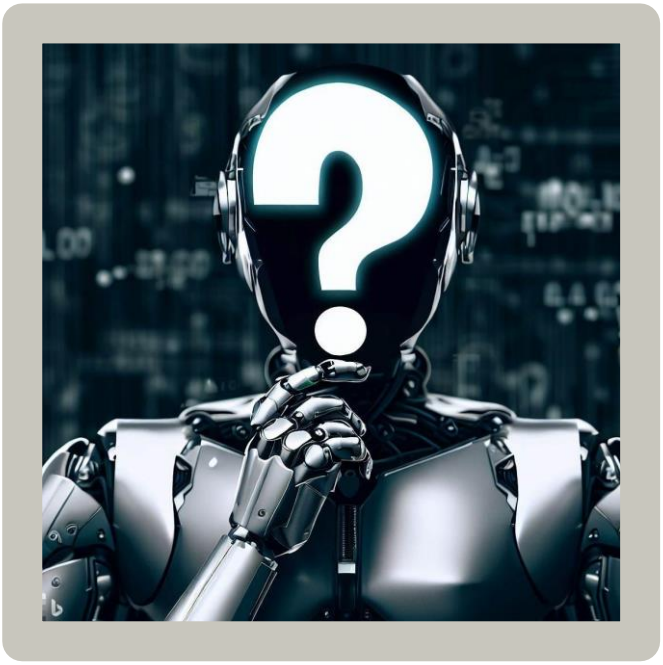
CLASSIFICATION: KC7//CYBER



[Actor Preview]

Code Name:
EnvolveLabs

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

Operating Region(s):
External, leveraging phishing and malicious file delivery.

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

Summary: The EnvolveLabs attack was a phishing-driven cyberattack that began when Terry Simpson, an employee using host DLY5-DESKTOP, received an email with subject 'Research opportunities! Apply today' from john-n-johnmoderno@yahoo.com. The email contained a link to disarm-remarkable.science, which delivered a malicious ZIP file named ResearchBibliographyGenerator.zip. Upon execution, the ZIP dropped updater.dll, which was observed on VirusTotal as S4ZD8JVW.dat. The malware executed reconnaissance commands such as 'whoami' and established persistence by beaconing to 199.57.49.250:8888. Further malicious domains included deprived.tech, illness.med, and vaccine.science. Subsequent phishing waves included emails from vaccinejournal@yahoo.com and pfizar.fda@hotmail.com with interview and FDA-themed lures. The operation resulted in data exfiltration using curl to send compressed files to pastebin.com.

Initial Access Vector

The initial compromise occurred when Terry Simpson opened ResearchBibliographyGenerator.zip, downloaded from disarm-remarkable.science via a phishing email. The email came from john-n-johnmoderno@yahoo.com with the subject 'Research opportunities! Apply today'.

Post Exploitation Activity

Following execution, updater.dll was dropped and loaded. The malware executed reconnaissance commands such as 'whoami' and initiated connections to attacker infrastructure. Additional malicious emails with subjects like 'Interview Request - Recent research article' were used for persistence and lateral movement. Actor-controlled infrastructure included illness.med and vaccine.science.

Command and Control

Persistence and communication were maintained through updater.dll beaconing to 199.57.49.250:8888. The malware used command line executions with parameters such as '-p' for establishing C2.

Exfiltration and Impact

The threat actor used Mimikatz to dump credentials and exfiltrated data to F:\exfil\Users. The stolen files were compressed and exfiltrated using curl to pastebin.com. The campaign also targeted users with clan.io-themed phishing, resulting in the compromise of Erica Wilson's account. Actor IP 223.80.243.56 was used to compromise 8 accounts, and related malicious infrastructure included arbiters-tail.info and activists.tk.

Appendix: Indicators of Compromise

Domains:
- - disarm-remarkable.science
- deprived.tech
- illness.med
- vaccine.science
- clan.io
- arbiters-tail.info
- activists.tk

Threat IPs:
- 199.57.49.250
- 223.80.243.56

Malicious Files:
- ResearchBibliographyGenerator.zip
- updater.dll (S4ZD8JVW.dat)
- ftp.txt

Emails:
- From: john-n-johnmoderno@yahoo.com | Subject: Research opportunities! Apply today
- From: vaccinejournal@yahoo.com | Subject: Interview Request - Recent research article
- From: pfizar.fda@hotmail.com | Subject: Interview Request - Recent research article
- From: gaara@qq.com | Subject: 50% discount on Naruto anime this weekend

Analyst Notes

The Research Heist Operation demonstrates how phishing and malicious attachments can lead to full system compromise, data theft, and persistence via DLL implants. Terry Simpson was the initial victim, and subsequent phishing waves expanded the actor's access, compromising multiple accounts. Multi-factor authentication, attachment sandboxing, and better phishing awareness training could have reduced the impact.