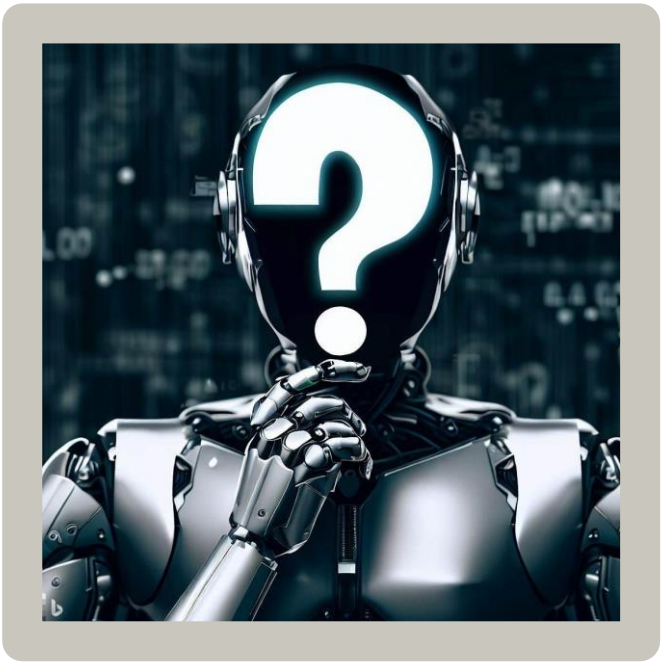
CLASSIFICATION: KC7//CYBER



[French Socksess Story]

Code Name:
Sock Puppet Empire

Affiliation(s):
No clear affiliations identified. Likely independent financially motivated group.

Operating Region(s):
Unknown, but activity suggests coordination across multiple regions via anonymous infrastructure.

Motivation(s):
Financial gain and data theft (extortion).

Summary: The Sock Puppet Empire is a financially motivated group targeting Jus de Chaussette (Socks company). They gained initial access through a malicious upload disguised as a JPEG, which dropped a PowerShell script. The actor used dnscat2 for command and control, and LaZagne to dump credentials. They escalated access by phishing the CEO and CFO, stole confidential data, archived it with WinRAR, and exfiltrated it via bitsadmin. Finally, they attempted extortion by emailing the executives.

Initial Access Vector

The threat actor gained initial access by uploading a malicious file (holesinmysocks.jpeg) through the customer service form on the company's website. Although disguised as an image, the file contained a PowerShell dropper (talking_socks.ps1). When a customer service employee (Mike Oz) opened it, the script executed and provided the attacker with initial access.

Post Exploitation Activity

After gaining initial access through Mike Oz's computer, the attacker executed **LaZagne** to extract credentials from both the customer database and LSASS memory. Using these credentials, they accessed the **customer database of Jus de Chaussette** and internal mailboxes.
The attacker then leveraged **Mike's compromised company email account** (mike_oz@jusdechaussette.fr) to send phishing emails to the CEO (Cho Cetkipu) and CFO (Brooke Entoe). Because the phishing email came from a trusted internal address, both executives opened the malicious attachment, which dropped the same PowerShell script (talking_socks.ps1) on their machines.
With control of the CEO and CFO's accounts, the attacker performed **lateral movement**, accessing **shared folders containing confidential contracts and business documents**. They staged this data locally for exfiltration.

Command and Control

The attacker used **dnscat2** to establish a command-and-control (C2) channel over the DNS protocol. The compromised machines communicated with the attacker-controlled domain thesockwhisperer.com, allowing persistent and stealthy remote access.

Exfiltration and Impact

The attacker copied files from the shared folders using **xcopy**, then archived the stolen data into password-protected files (lies.rar, feetlover.rar) with **WinRAR**. These archives included the **customer database** and **confidential corporate documents**.

For exfiltration, the attacker abused the legitimate Windows tool **bitsadmin** to upload the archives to their controlled domain liarliarsocksonfire.net.

Finally, once they had stolen and exfiltrated the data, the attackers launched an **extortion attempt**, sending threatening emails to company executives and demanding payment in exchange for not leaking the stolen information.

Appendix: Indicators of Compromise

Appendix: Indicators of Compromise

- **Domains**:
  - thesockwhisperer.com
  - liarliarsocksonfire.net
- **IPs**:
  - Three IPs linked to thesockwhisperer.com (used for reconnaissance)
  - 45.134.232.69
  - 8.95.2.97
  - 193.233.125.78
- **Emails**:
  - theempireownsyou@proton.me (attacker)
  - mike_oz@jusdechaussette.fr (compromised employee account)
- **Malicious files**:
  - holesinmysocks.jpeg
  - talking_socks.ps1
  - lies.rar
  - feetlover.rar
- **Tools used**:
  - dnscat2
  - LaZagne
  - xcopy, wmic, bitsadmin

Analyst Notes

The attacker abused legitimate Windows tools (bitsadmin, xcopy, wmic) to blend in with normal system activity.
The initial compromise relied heavily on social engineering and poor security hygiene, as an employee opened an unverified attachment.
Their campaign demonstrated clear knowledge of the company's internal structure, deliberately targeting the CEO and CFO for maximum impact.
The operation was well-structured and persistent, following a clear progression: **initial access → credential theft → internal phishing → data exfiltration → extortion**.