Multi-Stage In-Memory Agent Tesla Campaign Targets LATAM

Archived: 2026-04-05 17:39:29 UTC

Symantec has identified a new Agent Tesla campaign leveraging business-themed social engineering to target organizations across Latin America, Spain, and other international sectors. The actor impersonates a company that advertises outsourced management, consulting, and facility services.

The email (Subject: “Solicito su apoyo para procesar y confirmar Orden de Compra adjunta”) requests support to process and confirm an attached purchase order (Orden de compra_N202501023.PDF.001)

The message instructs the recipient to urgently confirm delivery dates and pricing, suggesting that failure to respond within 48 hours implies acceptance — a technique designed to push rapid user action. The attached file masquerades as a PDF invoice but is instead a compressed archive used to launch malware.

Attack chain: Email > RAR attachment > JScript loader (.jse) > PowerShell (downloaded) > PowerShell (in-memory execution) > .NET loader (in-memory) > .NET Agent Tesla payload (in-memory)

The PowerShell downloader retrieves its second stage from hxxp://172[.]245[.]246[.]93/jojoServer_Encrypted.jpg — a common steganographic-style trick, though the payload is not an image.

Once executed, the staged loaders transition fully in-memory to hinder detection and avoid leaving artifacts on disk. The malware leverages obfuscation, masquerading, and AMSI bypass techniques to remain stealthy, before harvesting credentials and system information for exfiltration over encrypted channels.

Observed techniques include:

- **Execution:** Native API (T1106)
- **Persistence & PrivEsc:** Registry modification / system process tampering (T1112, T1543, T1055)
- **Defense Evasion:** Obfuscation, masquerading, AMSI bypass, encrypted C2 (T1027, T1036, T1562, T1573)
- **Credential Access:** Credential dumping, email credential harvesting (T1003, T1552, T1114)
- **Discovery & Collection:** System discovery and data harvesting (T1057, T1082, T1005)
- **C2:** HTTP(S) encrypted communications (T1071, T1573)

This campaign shows broad, opportunistic targeting across Latin America and select international regions. Primary targeting includes Mexico, Peru, Colombia, Dominican Republic, Ecuador, Costa Rica, Brazil, Chile, and Spain.

Impacted sectors span:

- Finance & Banking / Insurance
- Government (Health, Finance, Environment)
- Retail / E-commerce
- Automotive & Heavy Machinery

- Energy / Utilities / Mining
- Manufacturing (Paper, Packaging, Defense Components)
- Telecommunications, Logistics & Maritime
- Healthcare / Diagnostics
- Agriculture & Food Supply Chain
- NGOs and Research Organizations

Symantec protects you from this threat, identified by the following:

Behavior-based

- SONAR.Stealer!gen1

Carbon Black-based

- Associated malicious indicators are blocked and detected by existing policies within Carbon Black products. The recommended policy at a minimum is to block all types of malware from executing (Known, Suspect, and PUP) as well as delay execution for cloud scan to get maximum benefit from Carbon Black Cloud reputation service.

EDR-based

- Both Symantec and Carbon Black EDR are capable of monitoring and flagging this threat actor's tactics, techniques and procedures.

Email-based

- Coverage is in place for Symantec's email security products and Email Threat Isolation (ETI) technology provides an extra layer of protection for our customers.

File-based

- ISB.Downloader!gen348
- Trojan.Gen.MBT
- XSNet.Js!gen2
- XSNet.Ps1!gen2

Machine Learning-based

- Heur.AdvML.B

Web-based

- Observed domains/IPs are covered under security categories in all WebPulse enabled products

---