Threat Intelligence Snapshot

Malware Incident – Oski Loader

Laura Salguero[a]

[a]*Cybersecurity Analysis Practice*

February 20, 2026

Abstract—A phishing email titled “Nuevo pedido urgente” delivered a malicious PowerPoint file to an accounting employee. Execution triggered payload download, credential harvesting behavior, outbound C2 communication, and self-deletion activity. The sample is widely classified as a Trojan.

INCIDENT OVERVIEW

Initial Vector	Phishing ("Nuevo pedido urgente")
Payload	VPN.exe (Loader + Stealer)
MD5	12c1842c3ccafe7408c23ebf292ee3d9
Detection Ratio	61 / 72 (VirusTotal)
Popular Label	trojan.mint/zitirez
Malware Family	Stealc / Oski Stealer
C2 Server	171.22.28.221

CYBER KILL CHAIN

Attack Flow

Phishing Email
↓
User Execution (Malicious PPT)
↓
VPN.exe Loader Execution
↓
HTTP C2 Communication
↓
Download of Additional DLL Modules
↓
Credential Harvesting (Stealc)
↓
Data Exfiltration (HTTP POST)
↓
Self-Deletion via cmd + timeout

PROCESS TREE OBSERVED

```
powerpnt.exe
   -> VPN.exe
        -> cmd.exe
             -> timeout.exe /t 5
        -> DLL modules (sqlite3.dll, nss3.dll, ...)
```

DEFENSE EVASION MECHANISM

```
cmd.exe /c timeout /t 5
 -> del /f /q "VPN.exe"
 -> del "C:\ProgramData\*.dll"
```

Execution is delayed for 5 seconds and then removes its own binary and dropped DLL artifacts.

BEHAVIORAL ANALYSIS

Category	Observation
Execution	VPN.exe (311 KB PE)
Persistence	None observed
Credential Access	Browser credential harvesting
Crypto	RC4 decryption routine
Defense Evasion	Self-delete after 5s
Environment Checks	CPU name check, debug detection
Exploit Ref	CVE-2016-0101 behavior tag

C2 COMMUNICATION

Primary C2 IP: 171.22.28.221
POST endpoint: 171[.]22[.]28[.]221/5c06c05b7b34e8e6.php
DLL download path: 171[.]22[.]28[.]221/9e226a84ec50246d/

Downloaded modules:

- sqlite3.dll
- freebl3.dll
- mozglue.dll
- msvcp140.dll
- nss3.dll
- softokn3.dll
- vcruntime140.dll

Repeated HTTP POST exfiltration observed (200 OK responses).

MITRE ATT&CK MAPPING

Tactic	Technique
Initial Access	T1566 – Phishing
Execution	T1204 – User Execution
Credential Access	T1555 – Credentials from Stores
Command & Control	T1071 – Application Layer Protocol
Defense Evasion	T1070 – Indicator Removal
Discovery	T1082 – System Information Discovery

INDICATORS OF COMPROMISE

MD5	12c1842c3ccafe7408c23ebf292ee3d9
C2 IP	171.22.28.221
POST URI	/5c06c05b7b34e8e6.php
DLL Path	/9e226a84ec50246d/
Process	VPN.exe
Threat Label	trojan.mint/zitirez

THREAT INTELLIGENCE SOURCES

- Any Run Analysis Report
- Any Run Task
- VirusTotal Report