



Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA
CENTRO OPERATIVO PER LA SICUREZZA CIBERNETICA
UMBRIA

**“Materiale da non divulgare”
SOLO USO INTERNO**

PROTOCOLLO	SEGN_2026_11	DATA	16/01/2026
-------------------	--------------	-------------	------------

OGGETTO	c-ares campagna sfrutta il DLL Side-Loading per distribuire malware
----------------	--

DESTINATARI	Enti destinatari delle informazioni riservate.
--------------------	--

DESCRIZIONE	Nell'ambito della propria attività istituzionale questo Centro è venuto a conoscenza che Ricercatori di sicurezza hanno identificato una campagna malware attiva che sfrutta una vulnerabilità di DLL Side-Loading nell'utility legittima ahost.exe, componente della libreria open-source c-ares utilizzata per lookup DNS asincroni. Questa utility viene comunemente distribuita con Git for Windows e strumenti di sviluppo come GitKraken e GitHub Desktop. Gli attaccanti abbinano una DLL malevola denominata libcares-2.dll a versioni firmate di ahost.exe, spesso rinominato, per eseguire codice malevolo aggirando le difese legacy basate su firme digitali. La campagna distribuisce malware commodity tra cui infostealer come Agent Tesla, FormBook, Lumma Stealer, Nocturnal Stealer e CryptBot, insieme a RAT quali Remcos, QuasarRAT, Dark Crystal RAT e XWorm, mascherati da documenti aziendali. I target principali sono dipendenti con ruoli in ambito finanza, approvvigionamenti, supply chain e amministrazione, all'interno di settori commerciali e industriali quali Oil & Gas e Import/Export. Gli attaccanti utilizzano nomi di file localizzati in più lingue, tra cui arabo, spagnolo, portoghese, farsi e inglese, indicando un approccio globale e mirato. Il meccanismo sfrutta la modalità di caricamento delle DLL di Windows: quando ahost.exe viene eseguito, cerca libcares-2.dll nella propria directory prima di altre posizioni, permettendo il caricamento della versione malevola. Il file ahost.exe firmato da GitKraken è stato segnalato più volte e associato a più campagne, indicando una distribuzione massiva. Gli attaccanti usano nomi ingannevoli come order.exe, protect.exe o ESTADO DE CUENTA per mascherare i file eseguibili. In un caso analizzato, Dark Crystal RAT inietta se stesso in Addinprocess32.exe per persistere anche dopo la chiusura del processo iniziale, stabilendo connessioni DNS verso server di C2. La tecnica impiegata rappresenta una minaccia significativa poiché sfrutta la fiducia degli utenti nelle applicazioni firmate, rendendo il rilevamento particolarmente difficile per soluzioni di sicurezza legacy. <i>Si allega alla presente un archivio zip cifrato con password “cnaipic”, contenente gli indicatori di compromissione afferenti alla presente comunicazione.</i> Si raccomanda inoltre, come sempre, di esercitare estrema cautela nel trattare email di provenienza sospetta e, soprattutto, di non cliccare mai su link presenti all'interno delle segnalazioni.
--------------------	--

NOTE	Si prega di fornire riscontro a questa nota, facendo riferimento al nostro numero di protocollo, solo in caso di effettiva compromissione dei sistemi informatici. Si prega inoltre di garantire la riservatezza delle informazioni fornite, limitando la divulgazione delle stesse alla sola Constituency.
-------------	---

LuC

Centro Operativo per la Sicurezza Cibernetica
Tel. +39-075-9115311

poltel.pg@poliziadistato.it – dipps509.000p@pecps.poliziadistato.it

TPL-CLEAR