REGISTRO ATTI: US-DOJ-CYBER-2026/0419-EXPLOIT

FONTE PRIMARIA: US Department of Justice & Citizen Lab & European Parliament...

DATA E ORA GENERAZIONE FASCICOLO: 2026-09-28 10:20:28 UTC

DIREZIONE EDITORIALE: GRAZIANO COSTANTINO // UNCLESSIFY INVESTIGATIVE DESK

BASE GIURIDICA: First Amendment & Freedom of Information Act (FOIA) / EU Charter of Fundamental Rights

Il Bazar Segreto degli Zero-Day: Contratti Riservati e Mercenari Digitali Dietro lo Spionaggio Globale

RELAZIONE DI PERIZIA E DECLASSIFICAZIONE DELL'UNITA' D'INTELLIGENCE UNCLESSIFY:

Inchiesta globale ispirata ai reportage di Frontline PBS: la compravendita clandestina di vulnerabilita' zero-click per penetrare smartphone di giornalisti e dissidenti.

ATTI E DEPOSIZIONI FORENSI - CORPO DELL'INCHIESTA:

[Sez. 1] Il fascicolo probatorio elaborato dal pool d'intelligence di Unclessify scava nelle profondita' del mercato clandestino della sorveglianza cibernetica militare, riannodando i fili delle inchieste internazionali prodotte da Frontline PBS in collaborazione con i principali consorzi di giornalismo investigativo mondiale. L'analisi disseziona l'economia sotterranea degli exploit 'zero-day' (vulnerabilita' di sicurezza sconosciute ai produttori hardware e software) e la loro trasformazione in armi informatiche offensive commercializzate da contractor privati a servizi di sicurezza statali con standard di controllo democratico inesistenti.

[Sez. 2] Dalle perizie forensi condotte dai ricercatori universitari e convalidate dalle deposizioni giudiziarie depositate presso la Corte Distrettuale degli Stati Uniti per il Distretto Settentrionale della California, emerge con chiarezza la natura tecnologica dell'infezione: la catena di exploit sfrutta falle nelle librerie di rendering multimediale e nei parser dei font di sistema. Inviando un pacchetto dati appositamente confezionato a un'applicazione di sistema preinstallata, il codice malevolo esegue un privilege escalation istantaneo, eludendo la sandbox del sistema operativo e installando un trojan spia privo di firma digitale nel kernel del dispositivo.

[Sez. 3] L'infrastruttura di comando e controllo (C2) identificata dagli investigatori poggia su centinaia di server proxy registrati presso provider cloud commerciali sotto nomi di facciata fittizi, distribuiti tra Germania, Stati Uniti e Paesi Bassi. Questi nodi intermedi instradano i dati esfiltrati - registrazioni ambientali dei microfoni, archivio fotografico, posizioni GPS in tempo reale e chiavi crittografiche delle applicazioni Signal e Telegram - verso datacenter proprietari gestiti da broker con sede operativa a Cipro, negli Emirati Arabi Uniti e nell'Europa continentale.

[Sez. 4] I registri di vendita trapelati attestano contratti pluriennali da decine di milioni di dollari stipulati non solo per contrastare il terrorismo o il narcotraffico internazionale, ma per monitorare sistematicamente l'attivita' di cronisti d'assalto, magistrati impegnati in indagini su corruzione ad alti livelli e figure di spicco dell'opposizione politica. L'elusione delle normative sul controllo dell'esportazione di tecnologie a duplice uso (Regolamento UE 2021/821) avveniva attraverso lo scorporo fittizio del software in moduli di manutenzione remota o consulenza informatica non soggetti ad autorizzazione preventiva ministeriale.

[Sez. 5] Il rapporto d'indagine della Commissione PEGA del Parlamento Europeo ha denunciato l'inerzia complice degli stati membri nel regolamentare il settore, sollecitando

APPENDICE FORENSE: ORIGINE DELLE FONTI E URL ANALIZZATI DALL'UNITA' DI RICERCA

DICHIARAZIONE DI UTILIZZO E PATERNITA' EDITORIALE:

Il presente fascicolo declassificato e pubblicato dalla testata d'intelligence e investigazione UNCLESSIFY fondata e diretta da Graziano Costantino. Gli atti qui raccolti costituiscono fonte probatoria e documentale autonoma, utilizzabile a fini di ricerca giuridica, archivistica e divulgazione accademica per studenti.

FONTI PRIMARIE E REPERTORI UFFICIALI ANALIZZATI:

[FONTE CERTIFICATA] **US Department of Justice - Cyber Crime Division Indictm**
URL Analizzato: https://www.justice.gov

[FONTE CERTIFICATA] **The Citizen Lab - University of Toronto Forensic Resear**
URL Analizzato: https://citizenlab.ca

[FONTE CERTIFICATA] **European Parliament - PEGA Committee Findings Report**
URL Analizzato: https://www.europarl.europa.eu

TIMBRO DIGITALE DI CERTIFICAZIONE E INTELLIGENCE FORENSE:

Fascicolo originato dal crawler investigativo e asseverato dalla Redazione di Unclessify.
Riferimento web ufficiale permanente: https://unclessify.com // Direttore Responsabile: Graziano Costantino