REGISTRO ATTI: US-DOJ-FBI-2026/0771-RANSOM
FONTE PRIMARIA: Federal Bureau of Investigation (FBI) & US Department of Jus...
DATA E ORA GENERAZIONE FASCICOLO: 2026-09-28 10:20:29 UTC
DIREZIONE EDITORIALE: GRAZIANO COSTANTINO // UNCLESSIFY INVESTIGATIVE DESK
BASE GIURIDICA: Diritto di Cronaca Giudiziaria / Trasparenza Atti Pubblici

Briefing Operativo FBI Cyber Division: Smantellamento delle Infrastrutture dei Cartelli Ransomware

RELAZIONE DI PERIZIA E DECLASSIFICAZIONE DELL'UNITA' D'INTELLIGENCE UNCLESSIFY:
Conferenza stampa e rilievi dell'operazione congiunta FBI-Europol: il sequestro dei server di comando, delle chiavi di decifratura e dei wallet bitcoin dei cartelli del cyber-crime.

ATTI E DEPOSIZIONI FORENSI - CORPO DELL'INCHIESTA:

[Sez. 1] Il briefing ufficiale dei vertici della Cyber Division dell'FBI documenta i dettagli investigativi e tecnici della piu' vasta operazione internazionale di contrasto ai cartelli transnazionali del ransomware. L'intervento coordinato tra il Dipartimento di Giustizia statunitense, Europol e le forze di polizia di quattordici Paesi ha portato alla neutralizzazione dell'infrastruttura tecnologica dei gruppi criminali noti come LockBit, BlackCat e Hive, responsabili di migliaia di attacchi informatici a catena contro infrastrutture critiche, aziende sanitarie e reti governative.

[Sez. 2] L'operazione ha visto l'infiltrazione diretta dei sistemi informatici degli hacker da parte degli specialisti governativi: per oltre sette mesi gli agenti sotto copertura hanno monitorato i canali di comunicazione interna dei cartelli, accedendo ai pannelli di controllo del modello 'Ransomware-as-a-Service' (RaaS) in cui i programmatori fornivano il malware agli affiliati in cambio di una percentuale variabile tra il venti e il trenta per cento sui riscatti riscossi in criptovalute.

[Sez. 3] Il colpo piu' significativo sul piano operativo e' stato il recupero preventivo delle chiavi maestre di decifratura: gli investigatori hanno potuto consegnare a oltre tremila aziende e ospedali i software di sblocco prima che questi cedessero al ricatto milionario, impedendo la distrazione di oltre duecento milioni di dollari verso i portafogli virtuali della criminalita' organizzata.

[Sez. 4] Il tracciamento finanziario condotto sui registri pubblici della blockchain ha consentito di mappare i flussi di conversione del denaro sporco attraverso 'mixer' decentralizzati e intermediari situati in giurisdizioni prive di cooperazione giudiziaria internazionale. Unclessify include nel proprio archivio gli atti d'indagine declassificati e le schede tecniche degli indicatori di compromissione (IoC), fornendo una risorsa forense strategica per i professionisti della sicurezza digitale.

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] **Federal Bureau of Investigation (FBI) & US Department o**
URL Analizzato: https://www.fbi.gov

[FONTE CERTIFICATA] **Player Video Forense Unclessify**
URL Analizzato: https://unclessify.com/it/video/video-fbi-cyber-division-briefing-ransomwar

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