MINISTERO DELL'INTERNO

Polizia di Stato

Polizia delle Comunicazioni

COMUNICATO STAMPA

"**Operazione *Neuland*"**

Nel mese in corso, nell'ambito di una lunga ed articolata attività di indagine di livello internazionale, che ha visto coinvolte le Forze di Polizia di diversi Paesi europei, e condotta in Italia dagli investigatori del **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – CNAIPIC del Servizio Polizia Postale e delle Comunicazioni ed il supporto dei Compartimenti Polizia Postale e delle Comunicazioni di Firenze e Reggio Calabria**, è stata data esecuzione, alle perquisizioni locali ed informatiche, disposte **dalla Procura della Repubblica di Roma,** nei confronti di 2 giovani hacker italiani: **F.E.** (di anni 20) residente nel mantovano e **S.A.**(di anni 19) residente in provincia di Catanzaro, responsabili di una complessa attività criminale finalizzata alla creazione ed alla vendita nel *Dark Web* di virus informatici per la successiva diffusione.

Le attività di indagine di livello internazionale hanno riguardato in prima battuta il servizio *CAV* (Contro-Anti -Virus) denominato ***Razorscanner***[1] ed il software di *crypting* noto come ***Razorcrypter***, distribuito tramite una piattaforma nel *Dark Web*.

Gli amministratori della piattaforma infatti, oltre alla possibilità di testare i virus autoprodotti accertandone la riconoscibilità da parte degli antivirus, offrivano un servizio di crypting, consistente in un software progettato per poter nascondere i malware all'interno di programmi leciti ed agevolarne quindi la diffusione.

In particolare gli utilizzatori di *Razorcrypter* potevano quindi caricare il file crittografato su *Razorscanner* e testarne oltre la capacità di occultamento (stealth) del codice appena generato, la possibilità di aggirare i controlli antivirus.

L'operazione, chiamata in codice NEULAND, è stata coordinata dal Centro Europeo per la lotta contro la Cybercriminalità di Europol (EC3) e dalla Joint Cybercrime Action Taskforce (J-CAT), un gruppo specializzato di cyber investigatori di Europol, ed ha visto la contemporanea coordinata esecuzione di ulteriori 43 provvedimenti di perquisizione, che hanno portato in tutta Europa all'arresto di 4 cybercriminali ed al deferimento di ulteriori 5 hacker denunciati in stato di libertà.

---

[1] Il CAV *Razorscanner* costituisce di fatto un servizio che aiuta a testare la copertura e la capacità di occultamento dei file malevoli.

L'operazione si è, successivamente alla individuazione dei fornitori del suddetto servizio, concentrata sugli utilizzatori che si celavano dietro la stessa piattaforma contro-antivirus ed il servizio di *crypting*.
Tra gli utilizzatori di tale servizio **F.E.** ed **S.A.**, operanti sul territorio nazionale. Entrambi, già noti nel *Dark Web* ed agli specialisti della Polizia Postale, sono abili *Malware-writer*, esperti nella programmazione di virus informatici, che successivamente mettevano a disposizione di altri cybercriminali all'interno del *Dark Web*[2].
Le attività di perquisizione locale e personale hanno portato al sequestro di una notevole mole di strumenti informatici utilizzati dagli hacker per l'ideazione e la produzione dei malware e quindi alla denuncia dei due cybercriminali per il reato di diffusione di virus previsto dall'art. 615 quinquies del Codice Penale.
L'EC3 di Europol ha fornito un ampio sostegno alle indagini garantendo lo scambio delle informazioni e l'analisi approfondita dei malware che avevano sfruttato la piattaforma *CAV Razoscanner* .
Sono state pianificate diverse riunioni di coordinamento e conferenze telefoniche al fine di agevolare il coordinamento operativo ed evitare possibili conflitti organizzativi. Questo caso è un eccellente esempio di come una forza di polizia locale possa trarre beneficio dalla collaborazione con Europol per l'esecuzione di importanti azioni a livello nazionale e internazionale contro i criminali informatici.
Non si escludono ulteriori sviluppi in ragione dell'analisi del materiale sequestrato e dei movimenti bancari dai quali potranno emergere gli acquirenti di tali particolari malware, spesso utilizzati per spiare le vittime o per la sottrazione di dati sensibili ovvero dati di accesso ai sistemi di home banking.

Il CNAIPIC

Nel quadro delle strategie di protezione delle infrastrutture critiche informatizzate, l'istituzione, all'interno del **Servizio Polizia Postale e delle Comunicazioni**, del **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC)** si propone come modello operativo di assoluto carattere innovativo, anche in relazione al contesto internazionale.

---

[2] E' stato accertato come entrambi gli indagati fossero gli autori del malware denominato "*uWarrior*" e del vettore di trasmissione denominato "*Inferno W0rm*"

Ai sensi dell'**art. 7 bis della legge 31 luglio 2005 n. 155** (che ha convertito con modificazioni il decreto legge 27 luglio 2005 n. 144, recante "*Misure urgenti per il contrasto del terrorismo internazionale*") il **CNAIPIC** è incaricato, in via esclusiva, dello svolgimento di attività di prevenzione e contrasto dei crimini informatici, di matrice criminale comune, organizzata o terroristica, che hanno per obiettivo i sistemi informatici o le reti telematiche a supporto delle funzioni delle istituzioni e delle aziende che erogano o gestiscono servizi o processi vitali per il *Sistema Paese*, convenzionalmente definite *infrastrutture critiche informatizzate* e che, sempre ai sensi della citata norma di legge, sono state individuate come tali con il **decreto del Ministro dell'Interno del 09 gennaio 2008.**

Il **CNAIPIC** interviene, quindi, in favore della sicurezza di una gamma di infrastrutture connotate da una criticità intersettoriale (in virtù dei sempre più stretti vincoli di *interconnessione ed interdipendenza* tra i differenti settori infrastrutturali) e su una tipologia di *minaccia* che può avere tanto un'origine extraterritoriale quanto una proiezione ad "*effetto domino*" e transnazionale delle sue conseguenze.

Il modello operativo si fonda, inoltre, sul principio delle *partnership "pubblico-privato"*: il **CNAIPIC**, infatti, assume (mediante un *Sala operativa* disponibile h24 e 7 giorni su 7) una collocazione centrale all'interno di un *network* di realtà infrastrutturali critiche (istituzionali ed aziendali), ed opera in stretto collegamento con organismi di varia natura (nazionali ed esteri), impegnati tanto nello specifico settore quanto sul tema della sicurezza informatica, con i quali intrattiene costanti rapporti di interscambio informativo e provvede (attraverso Unità di *intelligence* e di *analisi*) alla raccolta ed all'elaborazione dei dati utili ai fini di prevenzione e contrasto della *minaccia*.

Il suddetto rapporto di partenariato trova il proprio momento di formalizzazione nella stipula di specifiche convenzioni; dal 2008 ad oggi sono state stipulate convenzioni, tra le altre, con i seguenti enti ed aziende: ENAV, TERNA, ACI, TELECOM, VODAFONE, FFSS, UNICREDIT, RAI, CONSOB, ANSA, ATM – AZIENDA TRASPORTI MILANESI, ABI, BANCA D'ITALIA, SIA SSB, INTESA SANPAOLO, ENEL, FINMECCANICA, H3G, ATAC, EXPO 2015.