AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

# ***Tecnologia -*** *Cyberwar: email militari ucraine private compromesse per colpire i governi europei e la gestione dei rifugiati*

**Roma** - 02 mar 2022 (Prima Pagina News) **I ricercatori Proofpoint hanno identificato un attore che sfrutta messaggi compromessi per colpire l'Europa. Incluso un allegato macro pericoloso che tentava di scaricare un malware basato su Lua, soprannominato SunSeed.**

I ricercatori Proofpoint hanno identificato una campagna di phishing proveniente da un indirizzo email (ukr[.]net) che sembra appartenere a un membro compromesso del servizio armato ucraino. Questa scoperta arriva sulla scia degli avvisi del Computer Emergency Response Team ucraino (CERT-UA) e del Servizio Statale di Comunicazioni Speciali e Protezione delle Informazioni dell'Ucraina relativi alle diffuse campagne phishing rivolte agli account di posta elettronica privati dei membri del servizio armato ucraino da parte di 'UNC1151', che Proofpoint traccia come parte di TA445. L'email rilevata da Proofpoint può rappresentare la fase successiva di questi attacchi e includeva un allegato macro dannoso che utilizzava temi di ingegneria sociale relativi alla riunione di emergenza del Consiglio di sicurezza della NATO tenutasi il 23 febbraio 2022. Il messaggio conteneva anche un allegato pericoloso che ha tentato di scaricare un malware Lua, denominato SunSeed, e ha preso di mira il personale del governo europeo incaricato di gestire il trasporto e il trasferimento della popolazione in Europa. Proofpoint non ha attribuito definitivamente questa campagna all'attore di minacce TA445, ma i ricercatori riconoscono che tempistica, utilizzo di indirizzi di mittenti compromessi allineati ai report del governo ucraino e vittime della campagna si allineano con le tattiche di TA445 per includere il target e la raccolta intorno al movimento dei rifugiati in Europa. Proofpoint valuta che, alla luce della guerra Russia-Ucraina in corso, le azioni di attori proxy come TA445 continueranno a prendere di mira i governi europei per raccogliere informazioni sul flusso dei rifugiati dall'Ucraina e su questioni di rilievo per il governo russo. In particolare, TA445, che sembra operare dalla Bielorussia, ha un impegno storico dedicato a massicce operazioni di disinformazione volte a manipolare l'atteggiamento europeo rispetto al flusso dei rifugiati all'interno dei paesi della NATO. Queste narrazioni controllate possono avere l'obiettivo di influenzare l'atteggiamento anti-rifugiati all'interno dei paesi europei e amplificare le tensioni tra i membri della NATO, riducendo il sostegno occidentale per le entità ucraine coinvolte nel conflitto armato. Questo approccio è un fattore noto all'interno del modello di guerra ibrida impiegato dall'esercito russo e per estensione da quello della Bielorussia. Con i dati a disposizione di Proofpoint riguardo questa campagna, si possono trarre conclusioni al momento circoscritte riguardo al target. I messaggi email osservati da Proofpoint erano limitati a enti governativi europei e le persone prese di mira possedevano una gamma di competenze e responsabilità professionali. Tuttavia, c'era una chiara preferenza nel colpire individui con responsabilità relative a trasporti,

allocazione finanziaria e di budget, amministrative e di trasferimento della popolazione in Europa. Questa campagna può rappresentare un tentativo di ottenere informazioni sulla logistica che circonda il movimento di fondi, forniture e persone nei paesi membri della NATO.

*(Prima Pagina News) Mercoledì 02 Marzo 2022*

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it