POLIZIA DI STATO
COMPARTIMENTO POLIZIA POSTALE E DELLE COMUNICAZIONI "SICILIA ORIENTALE"

SEGNALAZIONI LUGLIO 2019			
Rif. Prot.	**CTPH11/2q/II/2/2018/01929**	**Data**	**22/07/2019**

Destinatari	**Enti destinatari delle informazioni riservate**

Oggetto	**sLoad: è in corso una campagna basata su messaggi PEC** **TrickBot: distribuita la minaccia tramite falsi update di Chrome e Firefox**
Data Eventi	In corso
Descrizione Evento	Nell'ambito della propria attività istituzionale, questo Ufficio è venuto a conoscenza che è in corso di tracciamento una nuova campagna di distribuzione del trojan sLoad attraverso email PEC . I criminali stanno inviando messaggi il cui testo invita a consultare il sito dell'Agenzia per l'Italia Digitale per verificare la firma digitale. In allegato alla P.E.C. si trova un archivio ZIP contenente un PDF e un VBS entrambi con filename "comunicazione clientela"; all'apertura del primo si verifica un errore che induce i target ad aprire il secondo. Il VBS esegue un PowerShell che scarica sLoad il quale resta in attesa di comandi. Questo attacco presenta alcune somiglianze con quello che ha colpito l'Ordine degli Ingegneri di Roma. **TrickBot:** Questo Ufficio è venuto a conoscenza, altresì, che attori non identificati hanno creato un falso sito Office 365 che sta distribuendo il trojan e stealer TrickBot camuffato da update per i browser Chrome e Firefox. La pagina fake è molto ben architettata e tutti i link presenti su di essa puntano a pagine ospitate su domini di Microsoft. Dopo alcuni secondi, alla vittima viene mostrato un alert che la invita ad aggiornare il browser in uso. Cliccando sul bottone Update, verrà scaricato un eseguibile chiamato upd365_58v01.exe in grado di installare TrickBot sul PC target iniettandolo in un processo svchost.exe per mascherarne la presenza il più a lungo possibile
Suggerimenti	Sensibilizzare il personale ed i professionisti al fine di non aprire mail inattese o comunque di provenienza incerta, evitando nel modo più assoluto di aprire allegati di cui non si conosce la natura e l'origine.

IL DIRIGENTE DEL COMPARTIMENTO p.t.
PIAZZA