Alien, il banking trojan prende di mira social network e app

La società di sicurezza informatica ThreatFabric ha diramato con il suo ultimo rapporto un'alert riguardo a una nuova cyber minaccia che sta prendendo di mira non solo le app bancarie ma anche social network, servizi di messaggistica istantanea e di posta elettronica di diversi Paesi tra cui Italia, Germania, Francia, Regno Unito, Stati Uniti e Australia.

Si chiama Alien, ed è un trojan in grado di carpire dati da centinaia di app.

Il malware "Alieno"

Secondo gli esperti di sicurezza, Alien rilasciato a inizio anno come Malware-as-a-Service nei forum underground, condividerebbe parte del codice sorgente di Cerberus, il noto malware che, dopo aver avuto il maggior successo nei mesi di giugno e di luglio 2020, ad agosto alcuni bug per lungo tempo lasciati irrisolti ne hanno decretato il declino consentendo, nel frattempo, al team Google Play Protect di trovare dei metodi di rilevamento e rimozione.

Le contromisure rivelatesi efficaci per Cerberus tuttavia non sembrano avere effetto contro Alien che s'impone come un trojan bancario mutevole e adattativo di tutto rispetto, tanto da essere definito "Alieno".

Tra le capacità confermate di questo malware figurano quelle di poter accedere facilmente alla lista dei contatti, carpire messaggi SMS, installare/rimuovere applicazioni e monitorare

in generale tutte le attività del dispositivo infetto. Alien è in grado anche di creare con tecniche overlay numerose false interfacce app, nonché di intercettare i codici generati per l'autenticazione a due fattori (2FA).

Pur basandosi sullo stesso codice di Cerberus e condividendo buona parte delle funzionalità, i ricercatori affermano che gli sviluppatori di Alien hanno personalizzato il protocollo di comunicazione C2 e aggiunto due ulteriori componenti, non presenti in nessuna delle versioni di Cerberus, ovvero un controllo remoto basato su TeamViewer (componente RAT) e uno sniffer per le notifiche (componente stealer).

Alien – la componente RAT

La componente RAT (Remote Access Trojan) implementa un set di comandi dedicati e diversi da quelli previsti dal gestore C2 dei comandi principale.

TeamViewer una volta installato non viene subito attivato. Il Trojan attende la ricezione delle credenziali per configurare la connessione al server TeamViewer e utilizza i privilegi di accessibilità per accedere all'applicazione stessa concedendo eventuali altre autorizzazioni aggiuntive. Solo dopo questa fase d'inizializzazione, se TeamViewer supporta il dispositivo target, gli attaccanti possono ottenere il controllo remoto completo dell'interfaccia utente del dispositivo, monitorando in tempo reale anche il comportamento dell'utente. In caso contrario TeamViewer funzionerà solo in modalità streaming video.

Alien – la componente Stealer

La componente stealer abusa dell'autorizzazione "*android.permission.BIND_NOTIFICATION_LISTENER*_SERVICE" per ottenere il contenuto delle notifiche della barra di stato sul dispositivo infetto. Sebbene questa autorizzazione deve essere

concessa dall’utente manualmente, il malware utilizzando i privilegi di accessibilità è in grado di eseguire in autonomia le interazioni necessarie allo scopo. In tal modo dopo aver ottenuto tali autorizzazioni, tutte le notifiche vengono inviate al server di comando e controllo C2.

Conclusioni

L’aver rilasciato gratuitamente sui forum di hacking il codice sorgente del trojan Cerberus v2 (notizia annunciata di recente da Kaspersky Lab), ha certamente dato adito agli sviluppatori malevoli concorrenti di generare nuove famiglie di malware derivate. È, infatti, ragionevole pensare che bisognerà attendersi un’evoluzione di tale evenienza.

Anche il trend in costante crescita dell’interesse dei criminal hacker a voler capitalizzare le informazioni che si riescono a carpire soprattutto dai dispositivi mobili, divenuti oramai una preziosa fucina informativa, non fa di certo ben sperare.

Nell’appendice dell’articolo pubblicato da ThreatFabric vengono riportati gli elenchi dei campioni trovati in natura (12) e dei package compromessi (226). https://www.threatfabric.com/blogs/alien_the_story_of_cerberus_demise.html

Alien, il banking trojan prende di mira social network e app