Come difendersi dalle campagne che prendono di mira gli utenti PEC

Nelle ultime settimane si è sentito parlare di diverse “campagne di attacco” a opera di criminali informatici che diffondono malware e virus via web e di tecniche avanzate di phishing per rubare dati agli utenti. Frodi informatiche di questo tipo fanno leva soprattutto sull’attendibilità del mezzo utilizzato per diffondersi.

Ecco perché, oltre alla e-mail tradizionale, anche la Posta Elettronica Certificata è diventata uno dei canali attraverso cui vengono veicolate queste campagne. A lanciare l’allarme è AssoCertificatori, Associazione dei Prestatori Italiani di Servizi Fiduciari Qualificati e dei Gestori Accreditati, che ha pubblicato una nota stampa per denunciare questo tipo di attività criminali.

Per organizzare l’attacco, il criminale informatico si appoggia su una botnet, una rete di computer e dispositivi che sono compromessi da malware. Queste postazioni di utenti, che magari non sanno nemmeno di avere il PC infetto, rappresentano la base dalla quale i criminali avviano i loro attacchi. I dispositivi che fanno parte della botnet diventano quindi – all’insaputa dei loro utilizzatori – veicolo di propagazione degli stessi virus che li hanno infettati e di frodi informatiche diffuse tramite malspam, phishing e social engineering.

Tutte queste tecniche fanno spesso leva sulla fiducia che il destinatario ha nei confronti del mittente e soprattutto cercano di servirsi illecitamente di uno strumento autorevole come la Posta Elettronica Certificata per rendere i messaggi più convincenti e plausibili perché trasmessi su un canale certificato.

Come fare per evitare le frodi? Purtroppo è semplice che la propria postazione entri a fare parte di una botnet, ad esempio è sufficiente inserire nel PC una chiavetta USB compromessa o aprire un file infetto magari scaricato in automatico navigando su un sito internet compromesso. Per questo, ogni utente deve essere consapevole di queste potenziali situazioni e assicurarsi che la propria postazione sia in stato di sicurezza, a partire dal semplice aggiornamento dell’antivirus.

Se il computer non è posto in sicurezza e da esso si accede a una casella di Posta Elettronica Certificata, è probabile che quell’indirizzo PEC venga utilizzato per veicolare i malware, così come è possibile che i criminali abbiano accesso ad aree protette come l’home banking o le aree di pagamento di siti e-commerce, con evidenti probabilità di subire furti economici.

Per evitare che ciò avvenga, esistono una serie di accorgimenti utili da attuare: a **livello comportamentale**, relativi a tutte quelle cautele che è utile prendere per evitare di aprire il messaggio PEC ritenuto sospetto e che costituiscono un primo livello di sicurezza diretto da parte dell’utente, e a **livello tecnico**, utili a evitare il problema dal punto di vista applicativo, come ad esempio tenere aggiornati il sistema antivirus e in generale tutti i software utilizzati ogni giorno.

L’utilizzo del "buon senso", ad ogni modo, è una buona norma da ricordare sempre. Di seguito alcune raccomandazioni per andare in questa direzione:

- avere cura della propria password (non salvare le credenziali di accesso alla casella PEC nei vari form di accesso online; non salvare la propria password all’interno di file mantenuti sui dispositivi; non utilizzare la medesima password per più applicativi; non comunicare la password a terzi);
- non cliccare su link presenti, se non si è sicuri che la URL a cui fanno riferimento sia lecita;
- non scaricare gli allegati di mittenti sconosciuti;

- prima di aprire un allegato non atteso chiedere conferma al mittente;
- effettuare una scansione antivirus della propria postazione e degli allegati che si intende aprire con software aggiornato e proveniente da fonti attendibili;
- non eseguire le macro dei documenti Microsoft Office;
- valutare con attenzione il contenuto dei messaggi: gli istituti di credito, come anche un provider, non chiedono di inserire dati sensibili all'interno di form online.

Nel caso ci sia anche solo il sospetto di aver perso il controllo della propria postazione, è necessario intervenire tempestivamente, attraverso due semplici operazioni:

Mantenere sicuri i dispositivi - Per prima cosa, al fine di evitare successive ulteriori intrusioni, si raccomanda di mettere in sicurezza tutte le postazioni utilizzate, eseguendo tutti i controlli e gli interventi tecnici necessari a ripulire da infezioni dovute a malware e virus.

Modificare le password - Appurata la "pulizia" dei dispositivi, si consiglia di procedere comunque alla variazione delle password di accesso utilizzate per i servizi web in generale (tra cui, ovviamente la PEC). La modifica periodica della password (con cadenza almeno trimestrale) rappresenta in generale una buona norma da rispettare nell'utilizzo delle proprie credenziali.

Ad attirare l'attenzione dei criminali informatici è stata probabilmente l'enorme diffusione della PEC in Italia, con oltre 10 milioni e mezzo di caselle attive e quasi 430 milioni di messaggi scambiati nel bimestre marzo-aprile 2019 (fonte AgID); ma attraverso accorgimenti comportamentali, tecnici e buon senso è possibile continuare a difendere le proprie caselle di Posta Elettronica Certificata e, più in generale, i propri dati.

I Gestori PEC accreditati stanno portando avanti importanti collaborazioni con le Autorità nazionali per continuare l'attività di contrasto al phishing via PEC, si tratta di tavoli di lavoro comuni tramite cui è attivo un costante monitoraggio della situazione attraverso software specializzati nel rilevamento delle frodi. Grazie al tavolo operativo continua inoltre la diffusione di contenuti, guide e materiali di supporto che indicano le buone prassi da adottare: è tramite tutte queste operazioni e una sempre maggiore sensibilizzazione degli utenti alla protezione dei propri dati che si ottiene il più alto livello di sicurezza.

Per maggiori informazioni ecco l'approfondimento per contrastare fenomeni di phishing e malware: http://aru.ba/pecfenomeni

Aruba S.p.A.

Aruba S.p.A., fondata nel 1994, è la prima società in Italia per i servizi di data center, cloud, web hosting, e-mail, PEC e registrazione domini e possiede una grande esperienza nella realizzazione e gestione di data center, disponendo di un network attivo a livello europeo: oltre ai data center proprietari - 3 già attivi in Italia ed uno in arrivo entro il 2020, più un altro in Repubblica Ceca - ulteriori strutture partner sono in Francia, Germania, UK e Polonia. La società gestisce oltre 2,6 milioni di domini, più di 8,6 milioni di caselle e-mail, oltre 6 milioni di caselle PEC, oltre 130.000 server ed un totale di 5 milioni di clienti. E' attiva sui principali mercati europei quali Francia, Inghilterra e Germania e vanta la leadership in Repubblica Ceca e Slovacca ed una presenza consolidata in Polonia e Ungheria. In aggiunta ai servizi di web hosting, fornisce anche servizi di server dedicati, housing e colocation, servizi managed, firma digitale, conservazione sostitutiva e produzione di smart-card. Dal 2011 ha ampliato la sua offerta con servizi Cloud e nel 2014 è diventata Registro ufficiale della prestigiosa estensione ".cloud". I Data Center di Aruba sono in grado di ospitare oltre 200.000 server. Per ulteriori informazioni: https://www.aruba.it

Ufficio Stampa Aruba:

SEIGRADI *Barbara La Malfa / Stefano Turi* Via Eustachi, 31 – 20129 Milano (MI) Tel. +39.02.84560801 Fax +39.02.84560802 Email: aruba@seigradi.com Sito: https://www.seigradi.com/	**ARUBA S.p.A.** Ufficio Stampa Via Orti Oricellari 8/D 50123 Firenze Email: ufficio.stampa@staff.aruba.it Sito: https://www.aruba.it/