Phishing, +220% di attacchi nel 2020. Il report

Il report Report “Phishing and Fraud 2020”

Gli incidenti di phishing sono aumentati del 220% durante il culmine della pandemia globale, rispetto alla media annuale.

Sono questi i dati evidenziati nel nuovo Report “Phishing and Fraud 2020” degli F5 Labs. Nel 2020 il COVID-19 continua ad essere un fattore significativo nell’aumento dei tentativi di phishing e frode da parte dei criminali informatici.

Sulla base dei dati del Security Operations Center (SOC) degli esperti di sicurezza, il numero degli incidenti di phishing nel 2020 sarebbe ogni anno destinato ad aumentare del 15%. Un risultato ampiamente superato e che potrebbe ulteriormente variare a seguito della seconda ondata della pandemia.

I tre tipi di attacchi principali

I tre obiettivi principali degli attacchi e di phishing tramite email che sfruttano COVID-19 come esca sono stati identificati in

- donazioni fraudolente a falsi enti di beneficenza
- raccolta illecita di credenziali
- diffusione di malware

L’opportunismo degli aggressori che sfruttano disagi e debolezze emotive causate dalla pandemia è stato ulteriormente

dimostrato a seguito dell'analisi dei log di Certificate Transparency (certificati digitali emessi da un'autorità di certificazione ritenuta pubblicamente attendibile).

Il numero di certificati che utilizzano i termini "covid" e "corona" ha raggiunto la cifra record di 14.940 a marzo, con un aumento del 1102% rispetto al mese precedente.

Phishing: Amazon, Apple, PayPal, Netflix i domini più utilizzati

Come già evidenziato nelle edizioni del report degli anni precedenti, la creatività dei truffatori quando si tratta di scegliere nomi e indirizzi dei loro siti di phishing è sempre in crescita.

Da inizio 2020 ad oggi, il 52% dei siti destinati ad azioni di phishing ha utilizzato nomi e identità di brand scelti con cura per i propri indirizzi web. Utilizzando i dati di **Webroot**, gli analisti hanno scoperto che Amazon è stato il brand più sfruttato nella seconda metà del 2020, con **Paypal, Apple, WhatsApp, Microsoft Office, Netflix e Instagram** che comparivano nella lista dei 10 marchi "impersonificati" più diffusi.

Tracciando il furto di credenziali, gli esperti hanno osservato come i criminali tentino di utilizzare le password rubate entro quattro ore dall'attacco di phishing. Alcuni attacchi si verificano addirittura in tempo reale, per finalizzare l'acquisizione di codici di sicurezza di autenticazione a più fattori (MFA). I criminali informatici sono diventati anche più efficienti nelle loro offerte per dirottare URL affidabili, spesso anche gratuitamente. Da soli, i siti WordPress rappresentano il 20% degli URL generici di phishing nel 2020. Nel 2017 la cifra era pari al 4,7%.

I siti fraudolenti utilizzano certificati HTTPS validi

Il 2020 ha visto anche i criminali intensificare i propri sforzi nel dissimulare i siti fraudolenti, facendoli apparire il più autentici e innocui possibile.

Le statistiche hanno rilevato che **la maggior parte dei siti di phishing sfrutta la crittografia**, in particolare il 72% utilizza certificati HTTPS validi per ingannare le vittime.

Quest'anno, il 100% delle drop zone – ovvero le destinazioni dei dati rubati dal malware – ha utilizzato la crittografia TLS (rispetto all'89% del 2019).

Per approfondire

Per scaricare il report "Phishing and Fraud 2020" clicca qui

https://www.key4biz.it/phishing-220-di-attacchi-nel-2020-il-report/336467/