PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4723 di Lunedì 22 giugno 2020

Conoscete la COVID-19 Cyber Defence Alliance?

Tutti conoscono l'attenzione che l'Unione europea pone alla sicurezza informatica. Questa attenzione viene sottolineata da adeguati finanziamenti, erogati ad associazioni che si concentrano su temi specifici di sicurezza informatica.

Si chiama ECHO la rete di centri di sicurezza informatica, che non solo tiene sotto controllo lo scenario criminale informatico, ma ha recentemente prestato specifica attenzione alla criminalità informatica, che si è espansa rapidamente, nell'attuale regime pandemico. Ecco la ragione per la quale tutti i centri che fanno parte di questo gruppo hanno fondato la COVID-19 Cyber Defence Alliance. Il suo obiettivo è quello di supportare tutte le iniziative che proteggono i paesi europei, i servizi primari e le infrastrutture critiche da attacchi informatici.

Il 6 aprile si è tenuto uno dei primi incontri, durante il quale i rappresentanti di 15 Stati membri hanno esaminato, suddivisi in due gruppi, l'atteggiamento degli hackers, che operano su uno scenario pandemico. La conclusione principale ha confermato che questa situazione offre agli attaccanti informatici delle opportunità uniche per utilizzare le più moderne tecniche e procedure di attacco, soprattutto a fronte di un numero crescente di dipendenti che lavorano da casa, giovani che utilizzano il computer per i collegamenti scolastici, così come l'elevato livello di sensibilità emotiva che nasce nelle persone, che vivono in un contesto di pandemia.

Indipendentemente dal motivo dell'attacco informatico, sia per profitto sia per turbamento sociale, il gruppo di lavoro ha concluso che oggi le opportunità offerte ai malviventi sono purtroppo in continua crescita. Il progetto è stato sovvenzionato dalla unione europea nell'ambito del programma Horizon 2020.

È stato pubblicato un documento specifico, che i lettori trovano in allegato, che offre una panoramica di queste tecniche di attacco. In tale documento i lettori troveranno alcune preziose indicazioni sull'atteggiamento mentale degli attaccanti.

La squadra degli esperti ha raccomandato di elaborare periodicamente dei messaggi, da inviare al pubblico in generale, con contenuto facilmente comprensibile, in modo da garantire la diffusione e la comprensibilità di messaggi di sicurezza. Inoltre, dovranno essere sviluppati messaggi specifici per aziende e settori, che potrebbero essere oggetto di attacchi particolari. Di particolare interesse è la individuazione dei tre profili degli attaccanti che sono così classificati:

- l'hacker criminale,
- l'hacktivist, vale a dire un hacker che opera con motivazioni sociali e politiche, ed infine
- i gruppi di hacker supportati da specifici paesi.

È evidente che gli obiettivi di queste tre categorie di attaccanti sono ben diversi e quindi vengono utilizzate tecniche diverse e bisogna mettere a punto difese specifiche.

Le modalità di attacco principali sono:

- invio di messaggi di posta elettronica,
- invio di messaggi WhatsApp,
- accesso ad apparati di utenti utilizzati in un contesto BYOD - Bring your on device,
- attacco di apparati medicali
- attacchi indirizzati ad applicativi mobili per COVID 19, come ad esempio l'applicativo italiano " immuni".

Il documento, in conclusione, raccomanda a tutti i responsabili informatici di accrescere il livello di sensibilizzazione degli operatori, diffondendo periodiche notizie sulle più recenti tecniche di attacco e metodi di difesa.

ECHO WhitePaper Hackers Mindset FINAL (pdf)

Adalberto Biasiotti