Covid, boom di minacce informatiche a tema

Redazione | 22/11/2020 | Sicurezza digitale

Secondo Clusit**,** l'associazione degli esperti di sicurezza informatica, durante la pandemia il 14% delle minacce informatiche registrate hanno riguardato il tema del Coronavirus: 119 attacchi gravi, di cui il 20% tramite le tecniche di ***phishing*** e ***social engineering*** con oggetto Covid-19.

Secondo gli esperti, il primo semestre 2020 è maglia nera della *cybersecurity*: 850 attacchi noti utilizzati (+7% rispetto all'anno precedente), di cui attacchi alle infrastrutture critiche (+85%) e al settore della ricerca (+63%).

Attacchi tramite ***malware*** e tecniche multiple/Apt (*Advanced persistent threat*) basate comunque su *malware* sono stati il 45%; quelli tramite *phishing* e *social engineering* (+26% rispetto all'anno precedente) il 20%. Di questi ultimi, il 40%, ha sfruttato il tema Covid-19 e le relative incertezza e sensibilità sul tema.

Secondo Clusit, tecniche di attacco meno sofisticate (**SQLi, DDoS**, vulnerabilità note, *account cracking, phishing* e *malware* semplice) sono il 76% del totale. La conclusione è che possono ancora essere realizzati attacchi gravi di successo a costi molto bassi e con relativa semplicità.

Le minacce informatiche a tema

Tornando al coronavirus e relativa pandemia, il Covid-19 è stato utilizzato come tema di crimini informatici, nel 72%dei casi per estorcere denaro; nel 28% per spionaggio e di guerra dell'informazione (o *information warfare*), ossia per assicurarsi vantaggi militari attraverso utilizzo di gestione e utilizzo dell'informazione.

Il 12% degli attacchi a tema Covid-19 (soprattutto con natura di spionaggio) ha avuto come obiettivo il settore governativo, militare e l'*intelligence*. Tra questi alcuni casi gravi di **BEC scam** (Business email compromise), compiuti nelle prime fasi concitate di approvvigionamento dei presidi di sicurezza (in particolare le mascherine), generando notevoli danni.

Come danni collaterali e aggiuntivi, oltre quelli diretti da attacchi di vario genere, Clusit sottolinea, inoltre, la diffusione di *fake news*, alimentando la confusione sulla pandemia.
Secondo Clusit**,** l'associazione degli esperti di sicurezza informatica, durante la pandemia il 14% delle minacce informatiche registrate hanno riguardato il tema del Coronavirus: 119 attacchi gravi, di cui il 20% tramite le tecniche di ***phishing*** e ***social engineering*** con oggetto Covid-19.

Secondo gli esperti, il primo semestre 2020 è maglia nera della *cybersecurity*: 850 attacchi noti utilizzati (+7% rispetto all'anno precedente), di cui attacchi alle infrastrutture critiche (+85%) e al settore della ricerca (+63%).

Attacchi tramite ***malware*** e tecniche multiple/Apt (*Advanced persistent threat*) basate comunque su *malware* sono stati il 45%; quelli tramite *phishing* e *social engineering* (+26% rispetto all'anno precedente) il 20%. Di questi ultimi, il 40%, ha sfruttato il tema Covid-19 e le relative incertezza e sensibilità sul tema.

Secondo Clusit, tecniche di attacco meno sofisticate (**SQLi, DDoS**, vulnerabilità note, *account*

cracking, phishing e *malware* semplice) sono il 76% del totale. La conclusione è che possono ancora essere realizzati attacchi gravi di successo a costi molto bassi e con relativa semplicità.

Le minacce informatiche a tema

Tornando al coronavirus e relativa pandemia, il Covid-19 è stato utilizzato come tema di crimini informatici, nel 72%dei casi per estorcere denaro; nel 28% per spionaggio e di guerra dell'informazione (o *information warfare*), ossia per assicurarsi vantaggi militari attraverso utilizzo di gestione e utilizzo dell'informazione.

Il 12% degli attacchi a tema Covid-19 (soprattutto con natura di spionaggio) ha avuto come obiettivo il settore governativo, militare e l'*intelligence*. Tra questi alcuni casi gravi di **BEC scam** (Business email compromise), compiuti nelle prime fasi concitate di approvvigionamento dei presidi di sicurezza (in particolare le mascherine), generando notevoli danni.

Come danni collaterali e aggiuntivi, oltre quelli diretti da attacchi di vario genere, Clusit sottolinea, inoltre, la diffusione di *fake news*, alimentando la confusione sulla pandemia.