NEWS

Attacchi malware, è boom di domini collegati al Coronavirus (+600%)

Strutture ospedaliere e aziende in smart working: il cybercrimine cavalca l'onda del Covid-19

9 APRILE 2020  DI MARCO SCOTTI

NEWS

L'emergenza sanitaria ha aperto un nuovo fronte di attacco per hacker e cybercriminali: è quanto emerge dall'analisi effettuata da Yarix, divisione Digital Security di Var Group. Attraverso il proprio team specializzato in Cyber Threat Intelligence, Yarix ha preso in esame i 100.000 domini che in media vengono registrati ogni giorno nel mondo, per un lasso di tempo che va dal 23 febbraio alla metà di marzo.

Con un trend di incremento non dissimile dalla curva crescente dell'attenzione pubblica sul tema, sono aumentate del 600% le registrazioni di nuovi domini contenenti parole chiave come 'Covid' e 'Coronavirus', in associazione ad altri termini generalmente utilizzati per attività di malware, phishing e scam (es. login, recovery, access, password, account...).

"Facendo leva sulla preoccupazione e i timori legittimamente diffusi a livello di opinione pubblica, il cybercrime sta dando prova di rapidità e aggressività nel dispiegare attacchi contro imprese, istituzioni, strutture sanitarie ed utenti finali. Ricorrendo in particolare a tecniche di phishing, gli hacker stanno inviando mail 'malevole' inserendo come finto mittente il richiamo a ospedali o istituzioni sanitarie. Altrettanto diffusi, nei dati che stiamo rilevando, i tentativi di truffa, contenenti minacce di diffusione di dati personali e di contagio Covid19 ai danni di quanti rifiutino di pagare un riscatto, in bitcoin", commenta Mirko Gatto, Head of Digital Security Division Var Group.

Le tipologie di attacco – focus Covid19

Il boom di registrazioni – evidenziato dagli analisti di Yarix – è il segnale di un parallelo incremento di attività criminali quali:

- Phishing: tramite link inviati via mail, gli utenti vengono dirottati su pagine web create ad-hoc – simili in tutto a pagine ufficiali di Microsoft, Webmail e altri servizi online –, per carpire le credenziali di accesso delle vittime. Come ulteriore leva di inganno, ricorrono in questo periodo diciture come "Si prega di accedere ad Office Online per visualizzare un importante documento sulla situazione mondiale del Coronavirus";

- Estorsione via mail: alla vittima viene notificato che tutte le sue passwords sono in possesso degli attaccanti e che i propri familiari saranno infettati da Coronavirus, salvo pagamento di un riscatto in bitcoin;

- Diffusione di Malware: autorevoli – ed evidentemente fasulli – esponenti di istituzioni sanitarie diramano via mail comunicazioni, linee guida e mappe interattive del contagio. Cliccando sull'allegato indicato, si liberano malware come TrickBot e Emotet;

- Campagne di lucro: su alcuni forum underground (dark web), gli hacker si scambiano opinioni su "come fare soldi" con il Covid19 e si può accedere a vendite promozionali di articoli illegali sempre legati al Coronavirus.

Come riconoscere una mail malevola – i consigli di Yarix

A livello internazionale, ospedali e istituzioni sanitarie internazionali stanno lottando contro il contagio da Coronavirus, ma anche contro il cybercrime: nelle ultime settimane si moltiplicano gli attacchi ransomware e DDos, come nei casi recenti del Dipartimento per la Salute USA o dell'Ospedale di Brno in Repubblica Ceca. È, dunque, fondamentale che gli utenti in rete siano consapevoli della situazione e sappiano riconoscere i tentativi di attacco dei cybercriminali 'camuffati' da operatori della sanità.

Secondo gli esperti Yarix, una mail è dubbia quando:

1. Ha un tono allarmistico e fa leva su paura e urgenza;

2. Chiede informazioni di carattere finanziario o dati personali;

3. Utilizza modalità di saluto desuete o inusuali (es. Signore/Signora);

4. Proviene da indirizzi poco credibili o ignoti (es. aol.com);

5. Contiene macroscopici errori di grammatica o di ortografia (es: Il virus si sta difondendo come mai e minacia la salute del mundo; la WHO è facendo tutto il possibile per contenere il situazione di ora).

Smart Working – i rischi da gestire

La diffusione repentina del 'lavoro intelligente' rappresenta, nella congiuntura attuale, una grande risorsa. Ma implica importanti criticità sul piano della sicurezza digitale, che è fondamentale riconoscere e gestire in maniera professionale.

Sembrano esserne consapevoli le imprese che, dalla metà di marzo, hanno sollecitato il supporto operativo e consulenziale di Var Group con un incremento del 60% e una prospettiva stimata di ulteriore aumento pari al +200%, per le prossime settimane.

1. Ecco nel seguito un vademecum cui attenersi:

1. Dispositivo: assicurarsi che siano installati antivirus e aggiornamenti di sicurezza;

2. Password: non memorizzarle, né lasciarle in evidenza su note scritte in prossimità del PC;

3. Informazioni aziendali: bloccare la postazione quando non è in uso e non archiviarle su chiavette USB o Flash Drive;

4. Privacy: non usare reti wi-fi pubbliche e considerare la possibilità che il display possa essere accessibile a terzi non autorizzati;

5. Phishing, Virus, Malware: essere consapevoli degli attacchi in corso in tema di Covid19.

ATTACCHI MALWARE, È BOOM DI DOMINI COLLEGATI AL CORONAVIRUS (600%)

TAGS MALWARE, CORONAVIRUS, YARIX