Smart Working & Cyber Security

BlueIT®

La quiete prima della tempesta

DEVICE ITALIANI VIOLATI IN VENDITA SUL MERCATO NERO

da prima del lockdown allo Smart Working diffuso

Già dapprima dell'emergenza Covid-19, lo Smart Working aveva iniziato a essere un fenomeno in crescita. In questo periodo fatto di uffici chiusi e dipendenti al lavoro da casa, lo Smart Working è diventato, per molte aziende, l'unico modo per continuare a lavorare. Per gestire lavoro e famiglia in attesa della riapertura delle scuole, il fenomeno si è poi diffuso alle connessioni da seconde case e luoghi di villeggiatura (alberghi, bar, ecc.) coperti da Free Wifi, e ha persino preso il nome di south working. Siamo passati da un livello di protezione generalmente più alto in azienda, a livelli di protezione sempre più bassi, passando a connessioni casalinghe a quelle aperte, in luoghi pubblici. Un altro fenomeno in forte crescita durante il lockdown è stata l'esplosione dell'e-commerce, dove la crescita, in pochi mesi, è stata superiore alla intera crescita dell'ultimo decennio. L'utilizzo di "password reuse" per registrarsi ai siti di e-commerce e alle piattaforme social ha visto l'aumento del rischio di compromissione anche delle credenziali aziendali. Il lavoro da remoto ha quindi dato la possibilità a gruppi di (cyber)criminali di approfittare delle scarse o inesistenti misure di sicurezza informatica in ambiente domestico (tanto più dai luoghi di villeggiatura), cercando di veicolare attacchi diretti verso gli utenti connessi da fuori azienda.

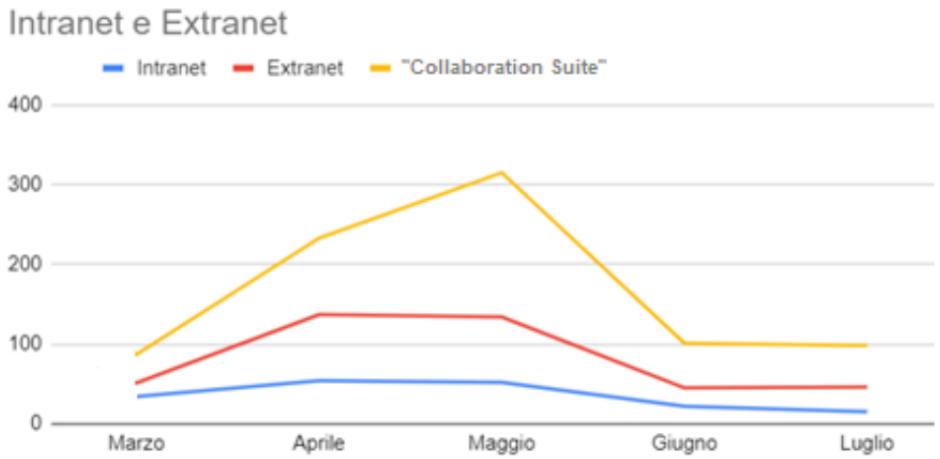
Quando un attacco ha avuto successo e un utente è caduto nella trappola, permettendo l'installazione di software malevolo per il controllo remoto del proprio device (PC, smartphone, tablet), è molto probabile che tale accesso venga messo in vendita sui mercati neri, presenti nella parte sommersa del web. Esiste un mercato criminale emergente che offre informazioni e credenziali in vendita, anche a pochi dollari o euro. Abbiamo quindi provato ad analizzare, mese per mese, l'andamento di questo "black market" (ne esistono molti). Il meccanismo è semplice ed è basato sul conteggio delle informazioni in vendita: come in un mercatino dell'usato, si propone l'articolo in vendita e l'annuncio rimane on-line finché non si perfeziona l'acquisto. L'analisi del mercato ci ha permesso di avere un'idea sullo stato delle infezioni dei device italiani.

Il grafico mostra il numero di nuovi device italiani violati in vendita suddivisi per mese. Abbiamo notato che, nel periodo dall'inizio del lockdown vi è stata un'impennata, passando da meno di duemila device infetti messi in vendita a marzo a quasi quattromila a maggio.

COSA STA SUCCEDENDO ADESSO? Il grafico tende a scendere. Ma è un problema.

È successo che i dati dei device violati sono stati venduti sul mercato nero. L'andamento non lineare ci dà segnali di preoccupazione perché può significare che gli “articoli” vengono effettivamente acquistati e il mercato è florido.

Passiamo adesso ad analizzare un altro tipo di dato che è possibile estrapolare analizzando il mercato nero. Possiamo ad esempio capire quante credenziali di accesso compromesse relative ad accessi di intranet e accessi a una nota collaboration suite sono disponibili sul mercato, dall’inizio dell’emergenza.



Abbiamo quindi analizzato quanti device infetti contengono credenziali di accesso relative ad URL che contengono la parola “intranet”, la parola “extranet” e la parola relativa alla collaboration suite. Anche in questo caso possiamo notare delle curve simili con il picco negativo a marzo. Possiamo quindi dedurre che, ad oggi, il valore più alto, dei device infetti in vendita, è imputabile al raggiungimento del regime della modalità di lavoro in Smart Working causata dal lockdown.

Alessandro Moccia

Cyber Intelligence Analyst BlueIT

COME TUTELARSI?

di Mario Pizzagalli, BU leader BlueIT Shield

Il Covid-19 e il conseguente lockdown hanno cambiato le nostre modalità di lavoro, e estremizzato il concetto di Smart Working. L'emergenza sanitaria non ancora superata fa pensare che le aziende adotteranno sistemi di lavoro da remoto ancora a lungo, facendo proprie best practice e aggiustamenti di quanto sperimentato in corsa da marzo. Visto che non ci rechiamo in ufficio, quindi, il nostro PC - aziendale o personale - non si si collega direttamente alla rete aziendale, ma a quella domestica. Oltre a collegarci ai sistemi informativi dell'azienda (direttamente via Internet per i servizi web, o in vpn ai servizi interni), utilizziamo sistemi di video-conferenza per partecipare a meeting aziendali o con clienti e fornitori. Perché i PC dei dipendenti che accedono ai servizi aziendali utilizzando la rete domestica, sono a rischio compromissione? Perché il più delle volte in casa non hanno una struttura di difesa adeguata. Il PC compromesso contiene credenziali e cookies di sessioni utilizzabili dai (cyber)criminali per accedere alla rete e/o ai servizi aziendali in maniera fraudolenta. Ecco dunque un decalogo di informazioni e comportamenti per ridurre il rischio di compromissione del proprio PC e di intrusioni.

DECALOGO COMPORTAMENTALE

anti cyber-19

1: Mantieni l'antivirus sempre attivato e scarica giornalmente gli aggiornamenti (alcuni antivirus propongono dei servizi da utilizzare quando si utilizzano connessioni gratuite).

2. Se ricevi e-mail da enti coinvolti nella lotta al coronarvirus, ma anche servizi di spedizione, che ti invitano a cliccare su un link velocemente, non farlo, potrebbe essere malevolo o portare ad infettare il tuo PC con un malware/ramsonware.

3. Se ricevi e-mail da un tuo superiore che ti invita/ordina di fornire informazioni o effettuare un'attività in fretta, non agire di impulso. Contatta la persona per telefono e chiedi se ha inviato davvero quel messaggio.

4. Se ricevi una e-mail dal Ministero della Salute, la Protezione Civile o altro ente che ti chiede informazioni relative all'organizzazione della tua azienda o ti chiede codici di accesso o altro, non rispondere.

5. Se ricevi e-mail da enti o aziende che ti propongono test o altro materiale legato alla lotta al Coronarvirus e che ti chiedono informazioni contatta il tuo ufficio acquisti o un tuo superiore.

BLUEIT SPA - WWW.BLUEIT.IT

SETTEMBRE 2020

DECALOGO COMPORTAMENTALE

anti cyber-19

6. Se ricevi una mail da enti coinvolti nella lotta al Coronavirus, che ti chiedono di scaricare un allegato, non farlo. Vai sul sito ufficiale dell'ente e controlla che non sia un metodo per infettare il tuo PC con un malware/ramsonware.

7. Se ricevi una mail che ti propone un vaccino o altra cura contro il Covid-19 non cliccare su nessun link proposto e non scaricare nessun allegato: soprattutto word, excel o pdf.

8. Fai attenzione ai domini web che contengono la parola "corona" o "covid19" e non navigarci con il browser.

9. Se vieni contattato telefonicamente e ti richiedono informazioni personali o relative alla tua azienda presta particolare attenzione.

10. Se vieni invitato a videoconferenze da account non conosciuti non attivare subito la webcam.

BLUEIT SPA - WWW.BLUEIT.IT

SETTEMBRE 2020