

COMUNICATO STAMPA

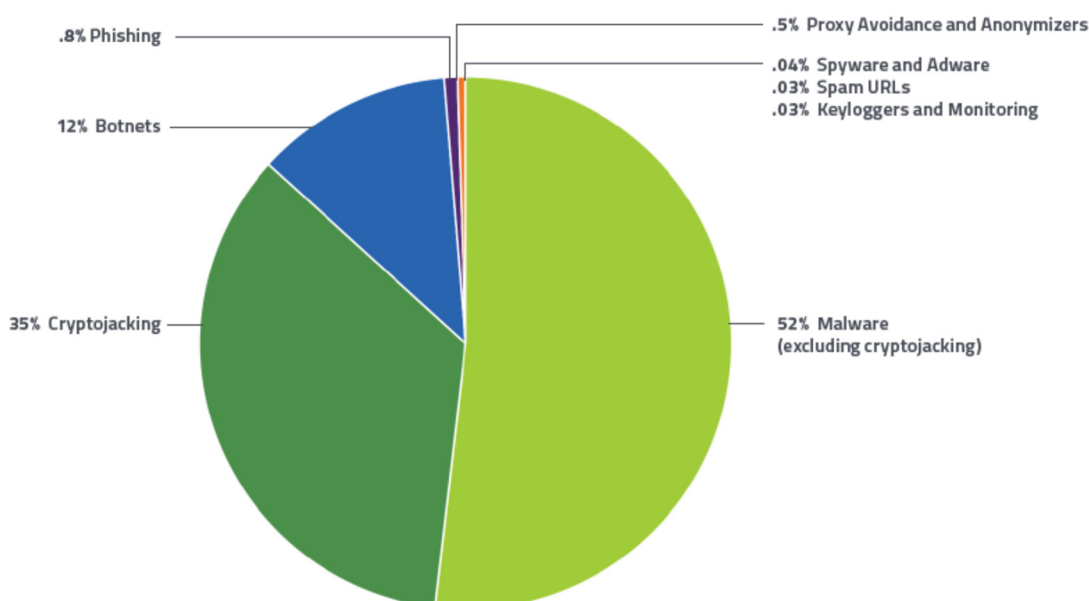
Malware, ransomware e phishing: i dati del 2018 secondo Webroot

Il team di Webroot ha analizzato i dati di milioni di clienti raccolti da inizio anno creando un report che fotografa la cybersecurity mondiale. Achab ha organizzato a Milano il prossimo 13 novembre il Webroot Day per illustrare le potenzialità di questo antivirus

MILANO – Webroot, prima azienda ad avvalersi del cloud e dell'intelligenza artificiale per arrestare le minacce zero-day in tempo reale e creatrice dell'antivirus omonimo in grado di proteggere le aziende e gli utenti di tutto il mondo con l'intelligence delle minacce e la sicurezza per endpoint e reti, ha reso pubblico alcuni giorni fa il report che analizza i dati di milioni di clienti dall'inizio del 2018. Il documento mette in luce alcune tendenze nel mondo della cybersecurity.

Uno degli aspetti più importanti sulla sicurezza in Rete emerso nel report è che non possiamo mai considerare i nostri sistemi informatici perfettamente sicuri. In secondo luogo, l'hardware (inteso come firewall) può essere altrettanto suscettibile a difetti sfruttabili da parte di chi ha cattive intenzioni così come accade per i software. Due nuove vulnerabilità, Meltdown e Spectre, hanno interessato quasi tutti i dispositivi con una CPU: si tratta forse del peggiore primo semestre di sempre in termini di sicurezza informatica rilevato ad oggi. Fino a quando non sono stati corretti, questi due bug hanno aperto le porte a cattivi attori che hanno potuto accedere a dati privati, come ad esempio le credenziali di accesso. Inoltre, Meltdown e Spectre sono esistiti per due decenni prima di essere scoperti, e ciò significa che ci sono sicuramente molti altri bug in agguato.

Ecco il panorama degli attacchi informatici da inizio 2018 secondo Webroot:



Malware, ransomware, cryptojacking e botnet continuano a dominare il panorama delle minacce. Da gennaio a giugno, l'87% delle minacce era costituito da malware (incluso il ransomware) e cryptojacking, seguito dal 12% di botnet.

L'anno scorso il **ransomware** ha seminato il panico. Molte aziende si sono trovate spesso a soccombere alle richieste di riscatto sempre più costose tramite criptovalute.

Tuttavia, oggi, un uso crescente di buoni backup, compresi i backup su cloud in grado di preservare le vecchie versioni dei file dagli attacchi dei ransomware, ha depotenziato questa categoria di minacce. La minaccia del ransomware si è ulteriormente ridotta a mano a mano che gli utenti hanno adottato Windows 10. A metà anno, Webroot ha visto il 75% dei consumatori e il 40% delle imprese migrare a questo sistema operativo, più sicuro dei suoi predecessori. Ma il ransomware non è scomparso: si è evoluto, invece, in un modello di business più mirato per i criminali che cercano connessioni RDP (Remote Desktop Protocol) non protette come vettore di attacco.

Mentre anche la percentuale di attacchi **malware** è in calo (dell'1% rispetto all'anno precedente), il phishing è in ascesa. Il phishing e gli attacchi di social engineering mirati sono in aumento: i dati di Webroot segnalano addirittura un aumento di oltre il 60% da gennaio di quest'anno. Il phishing, infatti, continua a essere un metodo efficace per entrare nelle reti aziendali: basta solo che una persona si lasci ingannare per ottenere le credenziali di accesso. E mentre Google è stato un obiettivo primario negli ultimi tre anni, Dropbox (con il 17% degli attacchi) ha superato Google (al 15%) in questo 2018. Quando un malintenzionato entra nell'account Gmail di qualcuno, la ricompensa potenziale in genere è limitata ai dati di quella sola persona. Con Dropbox, invece, la ricompensa può essere molto più grande: i consumatori e gli utenti aziendali su Dropbox accumulano documenti riguardanti sia le informazioni personali che quelle aziendali. Ottenere l'accesso a un account Dropbox aziendale, dunque, può sbloccare una quantità enorme di dati altamente sensibili.

Nelle conclusioni del rapporto firmato Webroot si legge: "Il 2018 probabilmente vedrà molte più istanze di cryptojacking. La cybersecurity non è perfetta e i creatori di minacce non stanno fermi. Il modo migliore e unico per resistere alle minacce in evoluzione è quello di impiegare un approccio a più livelli: dotarsi di una comprovata tecnologia di sicurezza che copra tutti i possibili vettori di minacce e che sia costantemente aggiornata, abbinata ad un addestramento consapevole e costante dell'utente finale".

Per discutere di tutto questo, **Achab** - azienda specializzata nella distribuzione di soluzioni software a valore agli operatori del mondo ICT – ha organizzato il **Webroot Day** il prossimo **13 novembre** a Milano. Durante la giornata di formazione gratuita rivolta agli MSP (Managed Service Provider), Achab illustrerà le potenzialità di **Webroot**, l'antivirus di nuova generazione che protegge in tempo reale gli endpoint da virus, malware e attacchi zero-day senza aggiornamento delle firme.

Sia al mattino che nel pomeriggio, sono stati organizzati dei laboratori tecnici in cui i partecipanti potranno toccare con mano la soluzione proposta, dalla configurazione fino all'analisi dei log.

Chi volesse partecipare alla giornata può iscriversi gratuitamente [qui](#).

Ufficio stampa Achab
Silvana Salvadori
Tel. 3477637646
Ufficiostampa@kore-events.com

Achab

Achab è specializzata nella distribuzione agli operatori del mondo ICT (VAR, ISV, MSP) di soluzioni software a valore. Nel corso degli anni, l'azienda è diventata un punto di riferimento unico per l'intera infrastruttura ICT delle piccole e medie imprese, grazie a soluzioni che garantiscono ai clienti la possibilità di perseguire gli obiettivi di business in maniera efficiente ed efficace.

Sul mercato italiano, la società collabora con una rete di oltre 1600 rivenditori qualificati, in grado di rispondere a ogni esigenza degli utilizzatori finali, dalla consulenza di prevendita fino alla consegna della soluzione chiavi in mano, dalla formazione alla manutenzione. Fondata nel 1994, Achab ha sede unica a Milano. Attualmente, sono oltre 25.000 le piccole e medie aziende italiane che utilizzano i prodotti distribuiti da Achab.

Webroot

Fondata nel 1997, Webroot fornisce soluzioni di sicurezza finalizzate a proteggere le informazioni personali e le attività aziendali da minacce in seguito alla navigazione in Internet. Con sede a Broomfield, Colorado, l'azienda è privata ed è sostenuta da alcune delle più importanti società di venture capital del settore, tra cui Technology Crossover Ventures, Accel Partners e Mayfield. Webroot ha attualmente circa 400 dipendenti nel mondo. Prodotti di Webroot distribuiti da Achab: Webroot e Webroot DNS Protection.