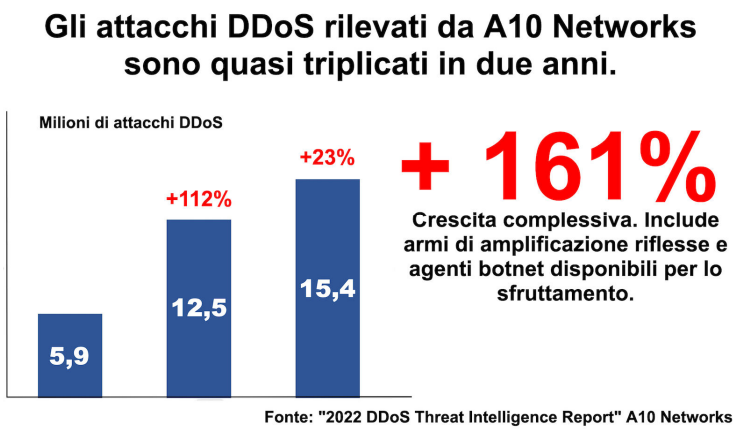
La ricerca di A10 Networks sulle minacce informatiche rileva e traccia le origini degli attacchi DDoS, riportando oltre 15 milioni di armi

Lo rivela il report dell'azienda statunitense. Le aziende impiegano sempre più spesso principi Zero Trust per proteggere l'infrastruttura digitale.

Roma 30 giugno 2022 – È ben noto che la pandemia ha causato un picco di attacchi informatici, tra cui malware, ransomware e attacchi DDoS. Gli autori delle minacce hanno cercato di interrompere non solo i servizi su cui le persone fanno affidamento ogni giorno, come l'assistenza sanitaria, l'istruzione e la finanza, ma anche le infrastrutture critiche come le catene di approvvigionamento alimentare, i servizi pubblici e le agenzie governative. Di conseguenza, c'è stato un drammatico aumento delle armi (computer, server e dispositivi IoT) che possono essere utilizzate per lanciare questi attacchi. Nella seconda metà del 2021, il team di ricerca sulla sicurezza di A10 Networks ha tracciato oltre 15,4 milioni di armi DDoS, quasi triplicate rispetto ai 5,9 del 2019.



Recentemente, l'intelligence di A10 Networks ha dettagliato l'uso di attacchi DDoS per interrompere le infrastrutture e le comunicazioni in Ucraina nel febbraio 2022, proprio quando la Russia ha lanciato il suo attacco di terra.

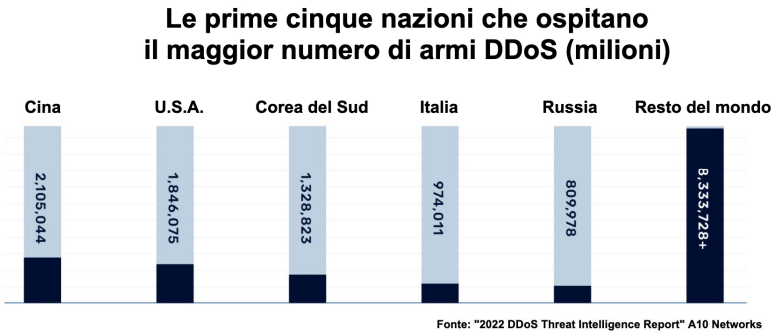
Il team di ricerca dell'intelligence sulle minacce di A10 ha monitorato progressi significativi nella portata e nell'intensità dei crimini informatici:

- Le armi DDoS sono in aumento: il team di ricerca sulla sicurezza di A10 ne ha tracciate 15,4 milioni
- C'è stato un aumento di oltre il 100 per cento, anno dopo anno, di potenziali armi di amplificazione più oscure, tra cui Apple Remote Desktop (ARD), che è stato utilizzato nel conflitto Russia-Ucraina
- Gli aggressori hanno sfruttato l'ormai nota vulnerabilità Log4j: più del 75 per cento ha avuto origine in Russia

Queste e altre tendenze sono incluse nel report DDoS Threat Report 2022 di A10 Networks, che fornisce approfondimenti dettagliati, tra cui le origini dell'attività DDoS;

la crescita delle armi DDoS e delle botnet; il ruolo del malware nella propagazione delle armi e degli attacchi DDoS; i passi che le aziende possono compiere per proteggersi da tali attività.

Le aziende devono agire ora adottando i principi Zero Trust



Dato il conflitto Russia-Ucraina in corso, il 21 marzo 2022 l'amministrazione Biden-Harris ha pubblicato una guida che esorta le organizzazioni statunitensi ad agire rapidamente per proteggersi dagli attacchi informatici e dalla guerra informatica sponsorizzata dagli stati. La guida, pur essendo rivolta a quelle con sede negli Stati Uniti, dettaglia un senso di urgenza per le organizzazioni mondiali affinché rivalutino la loro posizione sulla sicurezza. Impiegare i principi di Zero Trust non solo può proteggere le reti, ma anche garantire che non siano utilizzate per lanciare attacchi. Le soluzioni di sicurezza di A10 per la protezione DDoS, l'ispezione TLS/SSL del traffico crittografato e le funzionalità di sicurezza dell'application delivery possono fornire politiche di Zero Trust basate sull'identità e sul contesto per un accesso controllato.

"I recenti eventi – ha affermato Dhrupad Trivedi, president e CEO di A10 Networks – sottolineano l'impatto spesso devastante che gli attacchi informatici hanno sui governi e sul business in tutto il mondo. A10 Networks traccia l'origine delle armi DDoS, oltre ad altri vettori di attacco, per fornire ai clienti informazioni utili sulle minacce. Questo è un componente critico di un quadro di Zero Trust per aiutare le organizzazioni ad anticipare e mitigare meglio gli attacchi informatici, e anche per garantire che le reti non vengano inavvertitamente utilizzate per attività offensive".

A testimonianza dell'innovazione tecnologica di A10, Frost & Sullivan ha recentemente valutato le soluzioni di protezione DDoS di A10, insieme a diversi altri fornitori, e ha assegnato ad A10 il "2021 Frost & Sullivan Customer Value Leadership award for global DDoS mitigation, for excellence in best practices".

Inoltre, per supportare ulteriormente le esigenze di cybersecurity dei clienti e per contribuire fornire a soluzioni per le minacce informatiche, A10 ha recentemente aderito alla Microsoft Intelligent Security Association (MISA), che è un ecosistema di fornitori di software indipendenti e fornitori di servizi di sicurezza gestiti che hanno integrato le loro soluzioni per difendersi meglio da un mondo di minacce crescenti.

A10 Networks
A10 Networks (NYSE: ATEN) fornisce servizi applicativi sicuri per ambienti on-premises, multi-cloud e edge-cloud su iperscala. La missione è consentire ai service provider e alle imprese di fornire applicazioni business-critical sicure, disponibili ed efficienti per la trasformazione multi-cloud e la preparazione al 5G. Le soluzioni A10 Networks proteggono gli investimenti, supportano nuovi modelli di business e aiutano le infrastrutture a evolvere nel futuro, consentendo ai clienti di fornire l'esperienza digitale più sicura e disponibile. Fondata nel 2004, A10 Networks ha sede a San Jose (California, USA) e serve clienti operanti a livello mondiale. Per maggiori informazioni: www.a10networks.com e @A10Networks.

###

Informazioni per i media:
Attitudo - Giuseppe Turri
tel. 0362.17.87.591 - 335.73.90.945
giuseppe.turri@attitudo.it
www.attitudo.it