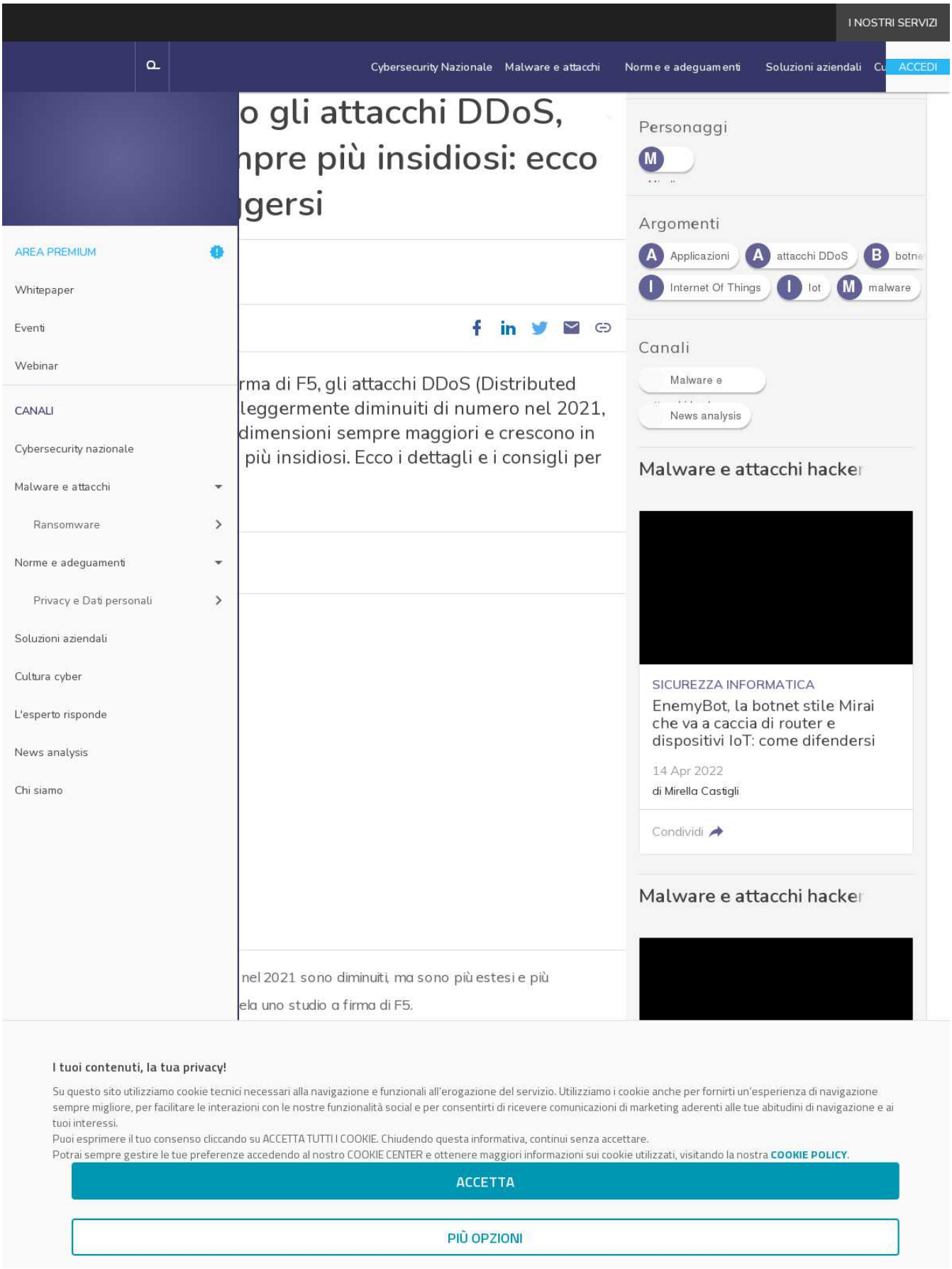

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso

Diminuiscono gli attacchi DDoS, ma sono sempre più insidiosi: ecco come proteggersi

Secondo uno studio a firma di F5, gli attacchi DDoS (Distributed Denial of Service) sono leggermente diminuiti di numero nel 2021, ma stanno acquistando dimensioni sempre maggiori e crescono in complessità diventando più insidiosi. Ecco i dettagli e i consigli per proteggersi Gli attacchi DDoS nel 2021 sono diminuiti, ma sono più estesi e più complessi. Lo rivela uno studio a firma di F5.“Un attacco DDoS (Distributed Denial of Service)”, spiega Rosita Galiandro, Responsabile Osservatorio Cybersecurity Exprivia, “è un tentativo di bloccare il traffico di un server, rete o servizio sopraffacendo la vittima o l’infrastruttura circostante e aumentando a dismisura il traffico Internet al fine di impedire il raggiungimento della destinazione prevista”.“Gli attacchi DDoS sono forse meno ‘spaventosi’ di ransomware o malware devastanti”, commenta Pierguido Iezzi, esperto di cyber security e CEO di Swascan, “ma appartengono comunque al novero delle minacce evergreen nel panorama della cyber”. Ecco perché.Indice degli argomenti Attacchi DDoS sempre più insidiosiAttacchi DDoS quattro volte maggioriI dettagli tecniciCome proteggersi Attacchi DDoS sempre più insidiosi Nel 2021, gli attacchi DDoS in grado di superare la soglia dei 250 Gbps hanno registrato un incremento del 1.300%. Infatti, l’anno scorso è quadruplicata proprio la dimensione media gli attacchi. WHITEPAPER IT: come ridurre i costi operativi del 24%? Una guida completa Datacenter Datacenter Infrastructure Management Scarica il WhitepaperLeggi l'informativa sulla privacyEmail * Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati. Inoltre, supera il 25% la quota di quelli che colpiscono il settore bancario, finanziario e assicurativo (BFSI).“Il fatto che vengano registrati meno attacchi DDoS”, continua Iezzi, “ma spesso più rivolti al mondo del Finance, per esempio, è frutto dell’organica evoluzione del cyber crime”.Infatti “un DDoS lanciato contro un’azienda che espone i propri servizi al pubblico è comunque in grado di impattare significativamente la business continuity e causare quindi ingenti perdite”, mette in evidenza Iezzi.Inoltre, la piattaforma F5 Silverline ha registrato il maggior attacco DDoS della storia: 1,4 Tbps, più di cinque volte superiore rispetto dell’attacco di 253 Gbps (record del 2020) e un attacco da 500 Gbps (febbraio 2021).“D’altro canto, la presenza sempre più diffusa di WAF (Web Application Firewall) e DDoS protection anche su siti ‘minori’ rende meno conveniente per i criminal hacker lanciare attacchi più casuali, ma sprona a creare pattern e attacchi più complessi contro target in grado di fruttare un profitto decisamente maggiore”, continua Iezzi.“Non dobbiamo dimenticare”, conclude l’analista, “che anche se il DDoS sembra aver avuto una leggera flessione, rimane una delle

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso

tecniche più amate dagli hacktivisti". Attacchi DDoS quattro volte maggiori F5 ha archiviato il quarto trimestre del 2021 registrando una dimensione media degli attacchi oltre i 21 Gbps, più di quattro volte maggiore di quelli registrati a inizio 2020.Gli attacchi volumetrici, inoltre, costituiscono il 59% del totale degli attacchi individuati (-66% rispetto all'anno precedente).Aumenta anche la quota degli attacchi DDoS a specifici protocolli e a livello di applicazione (+5% su base annua): il 27% degli attacchi nel 2021 ha usato il protocollo TCP (+17% rispetto all'anno precedente).Gli attacchi alle query DNS sono attualmente più diffusi, in crescita del 3,5% rispetto all'anno precedente e l'uso della frammentazione UDP è diminuito del 6,5%. Gli attacchi di tipo LDAP Reflection hanno registrato una flessione del 4,6%, mentre quelli di DNS Reflection del 3,3%."Insieme ai cambiamenti nella tipologia di attacco, abbiamo continuato a osservare una forte prevalenza di attacchi multivettoriali, tra cui l'episodio da 1,4 Tbps, che utilizzano una combinazione di DNS Reflection e HTTPS GETS", ha spiegato David Warburton, director degli F5 Labs. "Un aspetto particolarmente evidente all'inizio dell'anno, quando gli attacchi multivettoriali hanno superato significativamente quelli a vettore singolo, e che evidenzia uno scenario sempre più impegnativo per la protezione dalle minacce, dove i responsabili della sicurezza dovranno impiegare un numero sempre maggiore di strategie in parallelo per mitigare questi attacchi più sofisticati e prevenire un Denial of Service". I dettagli tecnici "Secondo l'Osservatorio Cybersecurity di Exprivia, nel 2021 i settori più colpiti in Italia da attacchi di tipo DDoS sono stati la Pubblica Amministrazione ed Entertainment", sottolinea Rosita Galiandro: "Attacchi di tipo DDoS sono classificati al sesto posto tra le tecniche di attacco analizzate durante l'intero anno (fonte: Exprivia Threat Intelligence Report 2021)".La Responsabile Osservatorio Cybersecurity Exprivia precisa, quindi, che "gli attacchi DDoS raggiungono l'efficacia sfruttando come fonti di attacco più sistemi informatici compromessi", continua Galiandro: "I dispositivi che vengono presi di mira a tali scopi possono includere computer e risorse di rete come, ad esempio, dispositivi Internet of Things (IoT). Ogni dispositivo infettato (bot) riesce a diffondere il malware, oltre che essere parte di un attacco DDoS. I bot unendosi generano botnet che sfruttando la potenza della propria numerosità amplificano la portata degli attacchi. Dopo aver creato una botnet, un attaccante può inviare indicazioni a ogni bot da remoto, indirizzando un attacco DDoS verso il sistema target".Ancora l'analista fa notare che "nel momento in cui una botnet attacca una rete o un server, l'attaccante permette ai singoli bot di inviare richieste all'indirizzo IP della vittima. Il risultato del sovraccarico di traffico è la negazione di un servizio, impedendo al normale traffico di accedere a siti web, applicazioni, reti o API. La sofisticatezza di attacchi complessi è rappresentata da un mix di attacchi di protocolli, volumetrici e applicativi. Un attaccante esegue vari tipi di attacchi contemporaneamente o alternativamente, rendendo più complesse le operazioni di difesa e di diminuzione del rischio di downtime e interruzioni che possono influenzare le attività aziendali (attacchi multi-vettore). Quasi tutti gli attacchi DDoS causano il sovraccarico di traffico di una rete o dispositivo target, ma gli attacchi possono essere di vario tipo e si possono distinguere in tre tipologie: attacchi volumetrici; attacchi di protocollo; e quelli a livello applicativo, che

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso

spesso vengono mescolati".La Galiandro sottolinea, quindi, che "la tipologia di attacchi volumetrici ha l'obiettivo di creare congestione saturando tutta la banda disponibile tra il sistema target e Internet. Alla vittima vengono inviate grandi quantità di dati utilizzando una forma di amplificazione DNS o altro per creare una grande quantità di traffico, ad esempio le richieste provenienti da una botnet. Tra gli attacchi volumetrici i più utilizzati sono gli UDP Flood e ICMP Flood e riflessione/amplificazione DNS. In UDP e ICMP Flood vengono inviati un gran numero di pacchetti UDP o ICMP (ping) che consumano la banda del ricevente e le sue risorse, quando cerca di elaborare i dati in arrivo. In questo caso il mittente è sempre falsificato, con il risultato che nodi del tutto innocenti ricevono risposte a pacchetti che non hanno inviato".Gli attacchi di protocollo sfruttano caratteristiche dei protocolli IP ed includono SYN Flood, Ping of Death, Smurf DDoS e altro. Il più utilizzato è il SYN Flood, la cui vittima è bersaglio di un gran numero di richieste di apertura di connessioni TCP (SYN -TCP), che non vengono concluse perché il pacchetto di risposta è inviato al mittente falsificato, lasciando così impegnate le risorse del server, fino a bloccarlo completamente. Nel SYN Flood la connessione segue il principio del 'three-way-handshake modificato' in modo da mettere fuori uso i servizi internet destinati agli utenti. Gli attacchi del tipo DDoS applicativo hanno l'obiettivo di esaurire le risorse della vittima al fine di creare una interruzione dei servizi, ad esempio saturando di richieste un server web. Il più utilizzato è Flood HTTP, in cui si cerca di mandare in crash un sito web o un'applicazione inviando un flusso continuo di traffico falso. Infatti, in funzione dell'elevato numero di richieste di accesso al sito, i sistemi non sono più in grado di rispondere correttamente e di conseguenza si bloccano", conclude Rosita Galiandro. Come proteggersi In aumento è il targeting delle infrastrutture IT: per esempio negli ultimi mesi si sono verificati vari attacchi DDoS aventi come obiettivo primario i servizi di autenticazione 3D Secure. Il tutto avviene tramite piccoli volumi di traffico.Questi attacchi, infatti, sfruttano tecniche di spoofing per mascherare i vettori dell'attacco (effettivi indirizzi IP) con indirizzi IP di soggetti legittimati all'accesso a servizi 3D Secure.Lo scopo è quello di far inserire in blacklist gli indirizzi IP legittimi. Ciò provoca disservizi tali da costringere un merchant a rinunciare alla transazione oppure ad autorizzarla, rinunciando alla verifica. Dunque, la vittima potrebbe prestare il fianco a potenziali frodi.Inoltre, "anche se il numero di attacchi è leggermente diminuito nel 2021, il problema DDoS non si sta affatto attenuando. La dimensione e la complessità di questi attacchi crescono, obbligando le aziende ad una risposta più veloce e articolata", sottolinea Warburton. "Anche se è ragionevole mettere in dubbio l'efficacia di attacchi che possono durare solo pochi minuti, gli attori delle minacce sanno che anche una breve interruzione del servizio può avere conseguenze significative e un impatto negativo sul brand e sulla reputazione".Dunque, "per affrontare attacchi DDoS sempre più sofisticati e articolati, le organizzazioni dovranno adottare misure sempre maggiori, come i controlli upstream per ispezionare e limitare il traffico che raggiunge gli endpoint, e affidarsi a managed service provider, in grado di lavorare insieme ai loro team di sicurezza sia per prevenire gli attacchi che per mitigare rapidamente quelli in corso", conclude Warburton.

Riproduzione autorizzata Licenza Promopress ad uso esclusivo del destinatario Vietato qualsiasi altro uso