



بخشی از ترجمه مقاله

عنوان فارسی مقاله :

راه حل هایی برای حملات DdoS روی ابر

عنوان انگلیسی مقاله :

solution for ddos attacks on Cloud



توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، [اینجا](#) کلیک نمایید.



بخشی از ترجمه مقاله

IV. Conclusion

As the Cloud Computing technology adopts and advances towards embracing Cloud services, DDoS attacks have only increased in the past few years and show no signs of abating in volume, complexity or magnitude. The traditional IT defense systems on premise DDoS solutions or taken from ISPs can hardly be expected to take on the wide range of new types of dynamic attacks.

DDOS attacks are becoming large enough to overwhelm Cloud provider's ability to absorb Server based attacks harness data center computational and networking resources to stage DDOS attacks of unprecedented volumes. Due to the increased attack volume, collateral damage is becoming a major cause of concern – packet loss, delays, high latency for internet traffic of those whose network traffic simply happens to traverse the WAN saturated by a DDOS attack. DDOS attacks are not only being used to disrupt services, but also to distract security resources while other types of attacks are attempted like fraudulent transactions. Adaptive DDOS attacks are prevalent – attackers attack traffic on the fly to avoid identification and confuse mitigation plans. Reflective and Amplification attacks are most common – leveraging misconfigured DNS, NTP and other network resources by spoofing source IP addresses

4. نتیجه گیری

از آنجایی که تکنولوژی رایانش ابری پذیرفته شده و در راستای بهره گیری از سرویس های ابری گسترش می یابد، در نتیجه حملات DDoS تنها در چند سال گذشته افزایش یافته و هیچ نشانه ای از کاهش حجم، پیچیدگی یا دامنه نشان نمی دهند. راه حل های DDoS بر فرض سیستم های تدافعی IT سنتی یا بدست آمده از ISP به سختی در طیف گسترده انواع جدید حملات پویا به کار گرفته می شوند.

حملات DDoS برای درهم شکستن توانایی تامین کننده ابر در جهت جذب حملات مبتنی بر سرور، و مهار و کنترل منابع شبکه سازی و محاسباتی مرکز داده به منظور طبقه بندی حملات DDOS با حجم های غیر منتظره به اندازه کافی بزرگ می شوند. به خاطر افزایش حجم حمله، آسیب پهلو به پهلو به یک دلیل اصلی نگرانی تبدیل می شود- تلفات بسته، تاخیرها، تاخیر بالا برای ترافیک اینترنتی آنهایی که ترافیک شبکه برای پیمایش WAN اشباع شده با حمله DDOS به وقوع می پیوندد. از حملات DDOS نه تنها برای مختل نمودن و وقفه در سرویس ها، بلکه همچنین برای منحرف نمودن منابع امنیتی استفاده می شود درحالیکه انواع دیگر حملات مثل تراکنش های کلاهبردانه و متقلبانه شروع می شوند. حملات DDOS تطبیقی رایج هستند- مهاجمین به ترافیک در حین پرواز حمله می کنند تا بدین طریق از شناسایی اجتناب کرده و برنامه های کاهش حمله را مغشوش نمایند. حملات انعکاسی (بازتابی) و تقویت کننده معمول ترین حملات می باشند که با اسپوفینگ یا اسپوف کردن آدرس های IP مبداء، DNS، NTP و سایر منابع شبکه درست پیکره بندی نشده را اهرم می نمایند.



توجه!

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، [اینجا](#) کلیک نمایید.

برای جستجوی جدیدترین مقالات ترجمه شده، [اینجا](#) کلیک نمایید.