باسمه تعالی

حملات تقویت ترافیک

(Amplification Attacks)

مقدمه

دسته‌ای از روش‌های مخرب برای انجام حملات DDoS، استفاده از روش تقویت ترافیک می‌باشد. مکانیزم این گونه از حملات بر اساس ارسال یک درخواست به یک سرور با طول کم و دریافت پاسخ با طول زیاد می‌باشد. حمله‌کننده با قرار دادن آدرس IP جعلی فرد قربانی و ارسال درخواست‌های متوالی با طول کم به یک و یا چندین سرور موجب ارسال حجم زیادی ترافیک به سمت قربانی می‌شود. نکته کلیدی، طول پاسخ بازگردانده شده از سوی سرور می‌باشد. هرچه اندازه پاسخ نسبت به درخواست ارسال شده بیشتر باشد، ترافیک نهایی به سمت قربانی نیز بیشتر می‌شود.

به طور کلی انواع حملات انعکاس یا تقویت ترافیک DDoS[1] به حمله‌کننده این امکان را می‌دهند تا بتواند ترافیک تولید شده را چندین برابر کند.

در برخی از پروتکل‌های پر کاربرد اینترنت، ارسال یک درخواست کم حجم مناسب که آدرس IP فرد قربانی به جای آدرس مبداء قرار گرفته است، می‌تواند یک پاسخ خروجی که اندازه آن بسیار بزرگتر از درخواست اولیه می‌باشد را تولید کند. این ترافیک تقویت شده که از نواقص موجود در ذات پروتکل و یا پیاده‌سازی آن سوءاستفاده می‌کند، می‌تواند چندین مرتبه به سمت فرد قربانی ارسال شود. این امر به فرد حمله کننده این اجازه را می‌دهد تا با ارسال حجم کمی داده، حجم زیادی داده توسط فرد قربانی دریافت شود. نسبت حجم ترافیک دریافتی توسط فرد قربانی به ترافیک ارسالی فرد حمله‌کننده به عنوان شاخص تقویت حملات انعکاس DDoS[2] شناخته می‌شود. در بسیاری از این حملات، شاخص مورد نظر بین ۲ تا ۱۰ می‌باشد. البته آسیب‌پذیری کشف شده در پروتکل BitTorrent این امکان را به حمله کننده می‌دهد که عدد شاخص گفته شده به ۱۲۰ برسد.

[1] DDoS reflection/amplification attacks
[2] reflection DDoS attack's amplification factor

در جدول زیر، تعدادی از متداول‌ترین پروتکل‌ها و سرویس‌هایی معرفی شده‌اند که با سوء استفاده از آن‌ها انجام حمله DDoS امکان‌پذیر می‌باشد. همچنین در مورد هر یک، ضریب تقویت، نوع پروتکل و شماره پورت متداول مورد استفاده ذکر شده است.

ردیف	پروتکل	ضریب تقویت پهنای باند	نوع پروتکل و شماره پورت پیش‌فرض
۱	DNS	28 to 54	UDP/53
۲	NTP	556.9	UDP/123
۳	SNMPv2	6.3	UDP/161
۴	NetBIOS	3.8	UDP 137 to 139
۵	SSDP	30.8	UDP/1900
۶	CharGEN	358.8	UDP/19
۷	QOTD	140.3	UDP/17
۸	BitTorrent	3.8	any
۹	Kad	16.3	UDP/6429
۱۰	Quake Network Protocol	63.9	UDP/26000 and UDP/27960
۱۱	Steam Protocol	5.5	Many – UDP/27015
۱۲	Multicast DNS (mDNS)	2 to 10	UDP/5353
۱۳	RIPv1	131.24	UDP/520
۱۴	Portmap (RPCbind)	7 to 28	TCP-UDP/111
۱۵	MS-SQL	22	UDP/1434