DDoSaaS: DDoS jako služba

Vít Bukač, bukac@mail.muni.cz
Zdeněk Říha, zriha@fi.muni.cz
Vlasta Šťavová, vlasta.stavova@mail.muni.cz
Lukáš Němec, lukas.nemec@mail.muni.cz

V tomto příspěvku se zabýváme analýzou služeb poskytujících za úplatu útoky odepření služby – Denial of Service as Service (DDoSaaS). Tyto služby jsou hrozbou pro slabě až středně výkonné cloudové servery a pro domácí uživatele. Informace, které jsme během našeho výzkumu posbírali, nám umožňují vyslovit názor, že DDoSaaS jsou rizikem pro poskytovatele cloudů i běžné uživatele.

1. Základní charakteristika

Služby DDoSaaSs samy sebe typicky prezentují jako služby stresového testování (stress testing) a často se setkáme s anglickými názvy jako booter nebo stresser. Teoreticky se tedy jedná o servery ochotné k testování odolnosti zvoleného cíle vůči DDoS útokům. Tyto služby jsou přístupné prostřednictvím internetových stránek, které vyžadují předchozí registraci.

Mezi společné rysy internetových stránek DDoSaaS služeb patří:
- Anglický jazyk webových stránek,
- Ceny jsou uváděny v amerických dolarech,
- Jsou snadno dohledatelné pomocí běžných vyhledávačů.

Webové stránky často obsahují Smluvní podmínky, kde se provozovatelé služeb zříkají jakákoli odpovědnosti za škody způsobené uživateli služby. Provozovatelé služeb nicméně nijak nekontrolují, zda zákazník objednává útok na cíl, který má pod svou kontrolou. Nejčastějšími zákazníky služeb DDoSaaS jsou on-line hráči, kteří chtějí získat konkurenční výhodu nad svými oponenty [Kar13].

Tyto služby jsou navrženy s důrazem na uživatelskou přívětivost. Hlavní webová stránka obsahuje přehled zpráv pro zákazníky, jako například nově dostupné typy útoků nebo zvyšující se šířka pásma, a základní statistiky služby. Pro hlášení chyb a problémů zákazníků obvykle bývá k dispozici ticket systém. Mnoho služeb dokonce tvrdí, že poskytují podporu 24 hodin, 7 dnů v týdnu přes kanály instantního messagingu.

Zákazníci jsou převážně lidé bez výraznějších technických znalostí. Pro zaplacení jsou používány běžné a široce rozšířené platební metody (např. Paypal, Bitcoin) a samotné spuštění útoku vyžaduje jen minimální porozumění fungování datových sítí. Základna zákazníků se čas od času rozrůstá díky příležitostným promo akcím, jako například slevy na předplatné slev nebo bezplatných zkoušek. Služby se platí formou předplatného. Po přijetí odpovídající částky je uživateli aktivován jeho účet a uživatel může po dobu předplatného službu prakticky neomezeně využívat. Předplatné se od sebe liší hlavně délkou jednoho

útoku (po uplynutí časového limitu útok skončí, ale uživatel ho může spustit znovu) a maximálním počtem souběžně probíhajících útoků. Ceny začínají okolo 2 USD za měsíc, pro ilustraci uvádíme několik příkladů v Tabulce 1.

DDoSaaS	Cena (USD)	Délka útoku (s)	Souběžně útoků
booter.in	2,5	100	2
connectionstresser.com	5	300	1
hornystress.me	6,99	300	1
lizardstresser.su	10	100	1
networkstresser.net	1,99	300	1
titaniumstresser.net	2,99	100	1

Tabulka 1 Měsíční poplatky za užívání

Současný způsob fungování služeb DDoSaaS poskytuje dobrou úroveň anonymity pro poskytovatele i technicky znalé uživatele. Platby lze zasílat anonymními cryptoměnami, síťový provoz útok používá podvrhnuté zdrojové IP adresy a na webové stránky lze přistupovat prostřednictvím anonymizačních proxy serverů.

2. Kill Chain

Fungování DDoSaaS ukážeme na kill chain metodice, kterou navrhli Hutchinson a spol. v [Hut11]. Kill chain rozděluje útok do sedmi fází, přičemž každá fáze může začít až v okamžiku, kdy úspěšně skončila fáze předchozí. Harris, Konikoff a Petersen použili kill chain na rozbor průběhu DDoS útoku prováděného botnetem v [Har13].

Reconaissance

V této fázi se potenciální útočník snaží o získání IP adresy nebo doménového jména počítače, který se chystá napadnout. V triviálním případě stačí převzít obecně známé doménové jméno serveru nebo použít základní systémové utility.

Avšak DDoSaaS jsou ve značné míře využívány hráči počítačových her. Zjištění IP adresy protivníka v online hře není triviální úkol, neboť hry obvykle využívají klient-server architekturu a přímá komunikace mezi hráči není možná. Používají se tedy tzv. resolvery, které dovolují spojit nickname uživatele vybrané služby (např. Skype) s jeho aktuální používanou IP adresou. Resolvery bývají buď přímo součástí webových stránek stresserů nebo jsou z nich odkazovány.

Weaponization & Delivery

Útočník určuje parametry požadovaného útoku. Vyžadován je především požadovaný typ útoku, délka a cílový port. Další možnosti nastavení vlastností útoku jsou velice omezené. Obvykle není možno specifikovat míru randomizace polí paketu ani vlastností datových toků. Všechny tyto parametry jsou napevno určeny jako neměnné charakteristiky vybraného typu útoku.

Na výběr bývá 5-10 různých typů útoku, založené na protokolech TCP, UDP a HTTP. Výběr požadovaného typu útoku také určuje, jakým způsobem budou pakety doručeny k cíli.

DDoSaaS intenzivně využívají IP spoofing. Zjevnou preferenci mají záplavové útoky založené na protokolu UDP. Tyto útoky využívají amplifikaci špatně konfigurovaných zařízení připojených k síti, jako jsou servery nebo domácí routery.

Exploitation

Jak už bylo uvedeno, útoky generované stressery jsou ve značné míře založeny na hrubém zahlcení cíle pomocí velkého množství dat. Dostupná šířka pásma pro útoky se většinou inzeruje v řádu několika gigabitů za sekundu někdy i více (např. Anonymous Stresser 5 Gbit/s, Quantum Booter 15 Gbit/s). Tato šířka pásma je však pouze teoretická. Reálně je výrazně nižší a navíc je sdílena všemi souběžně probíhajícími útoky.

Jen minimum DDoSaaS podporuje i útoky využívající zranitelnosti v běžně používaných protokolech. Jedná se především o útoky typu Slowloris a R-U-D-Y, které náleží do rodiny tzv. pomalých DDoS (slow DDoS). Jejich smyslem je udržení velkého množství souběžně otevřených spojení, čímž je postupně vyčerpána kapacita serveru pro otevření spojení k legitimním uživatelům.

Installation

Při DDoS útoku nedochází k instalaci malwaru na cílový počítač. Fáze instalace nemá proto žádnou navázanou akci a je přeskočena.

Command and Control (C2)

Útoky prováděné pomocí DDoSaaS mají obvykle délku řádově několik minut. Pokud útočník chce napadat cílový počítač dlouhodobě, může využívat přestávek mezi útoky k úpravě parametrů útoku, aby obránce neměl možnost přizpůsobovat své systémy. Protože, jak už bylo uvedeno, možnosti nastavení útoků jsou omezené, útočník může především měnit použité typy útoků.

I když je útočník informován o úspěšném zahájení útoku, DDoSaaS obvykle nepodporují setrvalý monitoring dostupnosti cíle a to ani pomocí triviálních metod jako například ping. Převážně technicky méně znalí zákazníci proto mohou mylně asociovat spuštění útoku vůči cíli s jeho úspěšným zahlcením.

Actions on objectives

Jakmile útočník dá pokyn k zahájení útoku, je nově vytvořen odpovídající požadavek a zařazen do fronty útoků. DDoSaaS jsou velice flexibilní, neboť k zahájení dochází obvykle během několika sekund. Úspěch útoku závisí na řadě faktorů, především pak na rychlosti připojení cíle, dostupným anti-DDoS systémům v jeho síti i síti jeho ISP a také na kvalitě infrastruktury, kterou DDoSaaS využívá. V případě napadení serveru hostovaného u

světoznámého poskytovatele cloudových služeb je pravděpodobnost doručení paketů útoku méně než 50 %.

3. Datové toky

Obvyklá průměrná bitrate během útoku se pohybuje na úrovni mezi 100 Mbit/s a 500 Mbit/s. Takové útoky mají potenciál nejen kompletně zahltit domácí připojení, ale narušit i fungování slabších serverů.

Služby DDoSaaS využívají malý počet výkonných serverů, které provádí samotný útok. Ve velké míře je využíván IP spoofing, aby byla znesnadněna identifikace zdrojových serverů, což by mohlo vést ke snížení jejich reputace nebo dokonce odstavení. Útočný provoz s podvrženými IP adresami se obvykle následně zesiluje nic netušícími špatně zkonfigurovanými prostředníky [Pax01].

Datové toky generované službami se také vykazují jednoduchostí. Nesetkáváme se s randomizací ani jinými technikami pro znesnadnění detekce. Naopak, útoky jsou obvykle snadno identifikovatelné, neboť cílový počítač přijímá až odpovědi prostředníků, aniž by sám datové toky inicioval. Kombinace jednoduchých až prototypových charakteristik datového provozu a relativně nízkých hodnot bitrate znamená, že útoky by měly být detekovatelné i velmi jednoduchými metodami (např. porovnávání počtu SYN/SYNACK segmentů, podobnostní vyhledávání mezi souběžnými toky či vyhledávání známých délek paketů).

Služby DDoSaaSs také umí rychle využít nově objevené metody útoků. Setkali jsme se například se stránkami nabízejícími útoky násobené pomocí nedávno objevených zranitelností v Joomla, MSSQL a SSDP. Nabídka útoků se zpravidla v čase dynamicky mění, jak operátoři služeb zakupují nové skripty, které generují nejnovější známé útoky.

4. Závěr

Během let vývoje došly DDoSaaS služby dlouhou cestu. Z prostých inzerátů na hackerských fórech se změnily ve vysoce automatizované a snadno přístupné nástroje pro širokou klientelu, které snesou srovnání se soudobými e-shopy. Jsou podporovány moderní platební metody jako Paypal nebo Bitcoin, uživatelé mají prostředky pro řešení stížností a služby samotné neustále aktualizují nabídky podporovaných útoků.

Hlavní hrozba DDoSaaS spočívá právě v jejich velké dostupnosti. Samotné generované útoky nejsou příliš silné, snadno se detekují a nepředstavují hrozbu pro běžně zabezpečené datové sítě.

Na druhou stranu jsme přesvědčeni, že hrozba služeb typu DDoSaaS se v budoucnu bude zvyšovat. To především díky nízké ceně, značné reklamě, dosažitelné anonymitě a business modelu, který činí tyto služby rychle a široce přístupné pro mnoho potenciálních zákazníků. Zároveň očekáváme, že se zvýší počet služeb DDoSaaS, a to především jako důsledek volně přístupných zdrojových kódů a nízkých počátečních nákladů na vstup do odvětví při srovnání s potenciálem zisku.

Literatura

[Har13] Harris, Bryan, Eli Konikoff, and Phillip Petersen. "Breaking the DDoS attack chain." Institute for Software Research (2013).

[Hut11] Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains." Leading Issues in Information Warfare & Security Research 1 (2011).

[Kar13] M. Karami and D. McCoy. "Understanding the Emerging Threat of DDoS-as-a-Service". 6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (2013).

[Pax01] Paxson, Vern. "An analysis of using reflectors for distributed denial-of-service attacks." *ACM SIGCOMM Computer Communication Review* 31.3 (2001).