HN obsah rozhoduje

KYBERNETICKÁ BEZPEČNOSŤ

PIATOK – NEDEĽA
31. MARCA – 2. APRÍLA 2023

Partneri špeciálnej prílohy:

ALISON

ALITER TECHNOLOGIES

Nepodceňujte to. Brutálne útoky už vedia robiť aj chlapci od susedov

xxxxx

FOTO: DREAMSTIME

DDOS ÚTOKY V ČÍSLACH

79 percent
– o toľko vzrástli vo svete útoky na aplikačnej vrstve v roku 2022 v medziročnom porovnaní

10 až 20 minút
trvala väčšina útokov v poslednom kvartáli 2022.

8 hodín
bolo priemerné trvanie útoku.

4 dni
dlho trval najdlhší útok.

Zdroj: správa CloudFlare, DDoS Threat Landscape Report Q4 2022

TÉMA

DDoS útoky sú ako online bombardovanie. V jednej chvíli príde toľko požiadaviek, že sieť alebo služba „kľakne“. Proste nie je dostupná.

Každý, kto sa spolieha na svoju online prítomnosť a služby, je zraniteľný proti útokom DDoS. Ak je nedostupná webová stránka, je to najmä reputačné riziko. Ak však ide o elektronický obchod, finančné inštitúcie, webové stránky s hrami či hazardnými hrami, mediálne spoločnosti a zdravotnícke organizácie, je to až existenčné riziko.

Ide to hore

Presné počty a typy DDoS útokov na globálnej úrovni je prakticky nemožné zistiť. Súvisí to so stupňom a spôsobom viditeľnosti do DDoS útokov organizácií, ktoré reporty pripravujú. Výsledky však vykazujú regionálne odlišnosti, v prípade Slovenska spojené prevažne s vojnou na Ukrajine.

Profesionáli tak predpokladajú, že nárast DDoS útokov u nás je výrazne vyšší ako globálne. Národné centrum kybernetickej bezpečnosti SK-CERT sleduje tento typ kampaní už od začiatku a v ostatnom čase eviduje viacero vĺn týchto útokov.

Dobrovoľné botnety

V slovenskom kybernetickom priestore sa objavila nová tendencia DDoS útokov. Miesto použitia veľkých botnetov pozostávajúcich z kompromitovaných zariadení sa útočníci čoraz viac uchyľujú k hacktivizmu a spúšťajú útoky z počítačov sympatizantov.

Aj v januári evidovala jednotka CSIRT.SK hlásenia útokov na webové stránky televíznych staníc a bánk a vládnej siete Govnet. K útoku sa prihlásila prorusky orientovaná hacktivistická skupina Anonymous Russia. Trend hacktivizmu v DDoS útokoch rastie a predstavuje významné nebezpečenstvo pre organizácie.

Ako to funguje?

Hacktivisti si zvyčajne stiahnu nástroj, ktorý im umožňuje získať zoznam cieľov a spustiť proti nim útoky. „Pozorujeme aj prípady, keď tento nástroj zahŕňa aj systém odmien v kryptomene, ktorý motivuje účastníkov a robí z toho lukratívne podnikanie,“ delí sa o skúsenosti Milan Pikula z NCKB SK-CERT. Hacktivisti si často neuvedomujú ďalší bezpečnostný rozmer, že tieto nástroje môžu potenciálne obsahovať aj inú skrytú funkcionalitu.

Tým, že útočníci využívajú siete aktivistov, vykonávajú útoky s väčšou ľahkosťou a efektivitou.

> Od úvodného oznamu k začiatku útoku prejde len niekoľko hodín.
>
> **Milan Pikula,**
> Národné centrum kybernetickej bezpečnosti SK-CERT

A tak od úvodného oznamu k začiatku útoku prejde len niekoľko hodín. V čase útoku je už potom neskoro začať myslieť na obranu. Organizácie bez rozdielu veľkosti a zamerania preto musia zaviesť a otestovať pokročilé bezpečnostné opatrenia na ochranu sietí pred týmito novými typmi útokov.

Celkom populárna služba

DDoS útoky sa dajú aj jednoducho „nakúpiť“ na webe, a to už nehovoríme len o dark webe. Komerčné kyberzločinecké stránky sa často maskujú za služby a ponúkajú testovanie bezpečnosti. V skutočnosti si tak zákazník kupuje cielený útok.

„Tu sú v riziku všetky organizácie, keďže konkurencia, nespokojný zákazník, prepustený zamestnanec alebo povedzme aj nespokojný pacient môžu takto zaútočiť a spôsobiť výpadok služieb,“ vysvetľuje manažér kybernetickej bezpečnosti Pavol Vrabec z martinskej univerzitnej nemocnice.

Oči pre plač

Dosah DDoS útoku závisí od toho, či mieri na webové servery alebo na aplikačnú úroveň a ako je od týchto služieb závislý predmet podnikania alebo poslanie organizácie. Úlohu zohráva aj to, či je to automat alebo cielený, na mieru šitý útok. Keďže život a svet sa v mnohých rozmeroch preniesol do internetového a aplikačného prostredia, nedostupnosť akejkoľvek služby prináša diskomfort, problémy a komplikácie. Vedúca úseku bezpečnosti vo Východoslovenskej energetike Diana Legdanová hovorí o tom, že pre útočníkov sú DDoS útoky stále zaujímavé a vyžadujú ostražitosť.

Štatistiky nepustia

K varovaniam sa pripája aj Tomaš Masný, riaditeľ informačnej bezpečnosti Slovak Telekom. „Intenzita a sila DDoS útokov je variabilná a významná. Pohybuje sa od jednotiek až po stovky gigabajtov za sekundu. Naše centrum bezpečnostných operácií, čiže SOC, eviduje a pravidelne reportuje počty týchto útokov.“

Ako veľký operátor ponúkajú štandardne službu DDoS ochrany, ale ešte stále je mnoho prípadov, keď si význam takejto ochrany zákazník uvedomí, až keď je pod útokom a dochádza k škodám.

Pozornosť každú sekundu

Systém DDoS ochrany u operátorov je plne automatický. „Ak je potrebné, vedia zasiahnuť SOC analytici a blokovať útok aj manuálne alebo doladiť ochranu na konkrétne prevádzkové potreby. Zákazník si v rozhraní vie kedykoľvek skontrolovať priebeh útokov a ochrany,“ dopĺňa Henrich Šnajder za Orange Slovensko.

„Zákazníkov máme zo všetkých segmentov, malých, stredných aj veľké korporácie, chránime tiež viacerých poskytovateľov internetu, mediálne domy a obchodné reťazce.“

Útoky idú do práčky

Detekcia útoku je už automatizovaná. Technológia spozornie, ak identifikuje abnormálne správanie siete a pri prekročení stanovených hodnôt detekuje útok. Ak už je jasné, na akú konkrétnu IP adresu smeruje DDoS útok, dátový tok sa presmeruje a eliminuje sa škodlivý. Po skončení je dôležité analyzovať odrazený útok a zdieľať informácie. Zároveň sa vykonávajú konfiguračné opatrenia do budúcnosti.

Dobre kúpená služba

Kľúčovú úlohu pri predchádzaní škodám zohráva toľko spomínané stredisko bezpečnostných operácií (SOC). Keďže vybudovanie a prevádzka sú náročné, služby SOC si organizácie aj v tomto prípade prenajímajú.

Vyladené stredisko SOC odhaľuje útoky, zavádza a vykonáva plány reakcie na incidenty, nasadzuje nástroje a techniky na zmierňovanie útokov. „Najdôležitejšou súčasťou sú však proaktívne opatrenia, čím sa minimalizuje vplyv DDoS útokov,“ zhŕňa skúsený SOC manažér Ján Andraško.

To najhoršie na koniec

Podľa skúseností Júliusa Selecského z Esetu firmy často ignorujú fakt, že na DDoS útoku sa môžu podieľať ich zariadenia. Čokoľvek, čo je pripojené do internetu, môže byť hacknuté a zapojené do útočného botnetu. Ak je zariadenie zraniteľné a nedá sa aktualizovať, aj po reštarte spravidla dochádza k jeho opätovnému infikovaniu.

Zapojenie v botnete má na fungovanie zariadenia minimálny alebo žiadny vplyv, čiže sa náročne identifikuje. Krajná situácia je, „keď vám polícia rozrazí dvere, že váš router útočí na banku“.

V sekcii Kybernetická bezpečnosť v online verzii nájdete odporúčania Národného centra kybernetickej bezpečnosti SK-CERT Ako sa brániť proti útokom na aplikačnej vrstve.

Spoločnosti podieľajúce sa na obsahu špeciálnej prílohy

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti · auditori.it · CHECK POINT · eset · Progress · SOITRON · SK CERT Národné centrum kybernetickej bezpečnosti

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 31. MARCA 2023 – 2. APRÍLA 2023

Prečo sa báť? Odpovede na 30 sekúnd

ANKETA

Profesionálov sme požiadali o takzvanú výťahovú odpoveď. Vžili sa do situácie, keď sa rozprávajú s majiteľom malej alebo strednej firmy a veľmi krátko argumentujú, prečo sa ho týka kybernetická bezpečnosť.

„Kto by na nás útočil? My nie sme pre nikoho zaujímaví. Nás sa kybernetická kriminalita netýka!“

Ivan Makatura
generálny riaditeľ
Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

Milý Vincent, ak tvrdíš, že „nie ste pre nikoho zaujímaví“, vyzerá to, ako keby si si nevážil svoj majetok. Možno si iba neuvedomuješ, aká je hodnota dát, od ktorých je tvoja forma závislá. V prípade ich straty nevieš poskytovať služby a je otázkou času, kedy svoju firmu zatvoríš. Navrhujem, aby si si dal vykonať kvalitnú analýzu rizík. Z reportu zistíš, nakoľko ste pre útočníkov zaujímaví.

Martin Lohnert
riaditeľ centra kybernetickej bezpečnosti Void SOC
Soitron

O vyvrátenie tohto známeho mýtu sa nepretržite starajú operátori botnetov, ransomvérové gangy, teroristické skupiny, hacktivisti, vaši nespokojní súčasní aj bývalí zamestnanci, zlomyseľní konkurenti, autori malvéru, nepriateľskými štátmi sponzorované APT skupiny, nudiace sa script kiddies, nájomní hackeri, alebo aj obyčajné ľudské chyby. Počkáte, kým vás presvedčia?

Jana Puškáčová
manažérka útvaru Informačná bezpečnosť
MOL IT & Digital Slovensko

Kybernetický útok dokáže využiť príležitosť bez ohľadu na veľkosť firmy. Malé a stredné firmy sú náchylnejšie na sociálne inžinierstvo. Dnes už je aj útok hackera komoditou a konkurenčný boj sa veľmi ľahko môže preniesť do kyberpriestoru.

Peter Dufek
manažér kybernetickej bezpečnosti
Procare a Svet zdravia

Myslieť si, že v dnešnej dobe nie je nejaká malá alebo stredná firma pre kyberzločin zaujímavá, je mylné. Aj malé firmy sú závislé od elektronických dát a ich zašifrovanie alebo krádež s následným „výpalným“ môže viesť nielen k úplnej likvidácii firmy, ale aj k strate dobrého mena alebo pokutám od dozorných orgánov.

Ján Grujbár
generálny riaditeľ
Aliter Technologies

Ukazuje sa, že práve malé a stredné firmy ako vy sú zaujímavým terčom pre hackerov. Práve vďaka slabej alebo nulovej ochrane. To prináša veľké zisky pri malom úsilí. Môžete byť vstupnou bránou k veľkým hráčom pri útokoch na dodávateľské reťazce. Pomôže iba prevencia. Riešiť ukradnuté dáta, zablokovaný prístup do systémov alebo zničenú reputáciu a stratu dôvery, až keď sa to stane, je ako utekať do poisťovne so žiadosťou o poistenie bytu, keď vás vytopilo alebo vás vykradli.

Tomáš Valenta
riaditeľ
Check Point Software Technologies na Slovensku

Paradoxne, malé firmy platia často a ochotne, pár stovák alebo tisícov. Zaplatíte raz, dvakrát a potom vám už nebudú stačiť žiadne peniaze. A posmelíte ďalších útočníkov. V sieti sa automaticky hľadajú zraniteľnosti a útočníkom je jedno, či ste malá alebo veľká firma. Na kyberútoku nie je nič osobné. Raz na to doplatíte, teda doplatíme všetci.

Ivan Kopáčik
bezpečnostný expert
Gordias

Dnešné kyberútoky sú vo veľkej miere automatizované. Terčom sú všetky zraniteľné subjekty, bez ohľadu na ich veľkosť a dôležitosť. A vysoká miera automatizácie znamená, že pre kyberzločincov je v hľadáčiku aj vaša firma.

Roman Varga,
manažér kyberbezpečnosti
Dôvera, zdravotná poisťovňa

Máte internet? Kybernetická kriminalita sa týka každého, kto používa internet. Útočníci sa snažia získať citlivé informácie, ako sú heslá, bankové údaje alebo iné osobné údaje. Môžu sa snažiť zneužiť vaše zariadenia na šírenie spamu alebo na útoky na iné zariadenia. Pre vás je bytostne dôležité chrániť sa pred kybernetickými hrozbami.

Roman Čupka
hlavný konzultant
Progress | Flowmon a CEO Synapsa Networks

Ak mi dáte k dispozícii na jednu hodinu vášho IT človeka a budem si môcť zapojiť pasívny senzor do vašej počítačovej siete, ktorý v ničom neovplyvní vaše IT prostredie, na druhý deň vám môžem dokázať opak. Ak nič podozrivé nenájdem, máte u mňa večeru a miesto si vyberte, kde chcete.

David Dvořák
CEO a zakladateľ konzultanti.it

Veľa útokov je vedených za predpokladu, že máte vo firme niečo, na čom vám záleží, a bude vás bolieť, ak vám to zoberú. Otázka teda nie je – prečo by na vás útočili. Pýtam sa vás, či máte niečo cenné, o čo by ste neradi prišli. Ak áno, tak si buďte istí, že hackeri to budú radi skúšať, kým sa im nepodarí dostať sa do vašich systémov. Nejde o to, či na vás niekto zaútočí. Ide iba o to, kedy sa to stane.

Tomáš Zaťko
CEO, etický hacker
Citadelo

Že ste nezaujímaví? Hackeri milujú ľahké ciele! Dáta ukradnuté z vašej firmy sa objavia na Twitteri a zákazníci zúria. Táto nočná mora je skutočná a udrie vtedy, keď to najmenej čakáte. Stáva sa to denne. Nebuďte varovným príkladom!

Marián Klačo
vedúci oddelenia bezpečnosť informácií, Volkswagen Slovakia

Viete, aké informácie sa vo vašej firme spracúvajú a akú hodnotu pre vás majú? Lebo každý, kto pozná hodnotu, dôležitosť a citlivosť informácií, ktoré má „doma“, vie, čím je pre potenciálnych útočníkov zaujímavý. A preto aj vie, že ich musí chrániť.

Jakub Berthoty
advokát, Dagital Legal

Otvorte si svoj SPAM priečinok v e-mailovej schránke a spýtajte sa ešte raz, či sa vás to netýka. Denne dostávate desiatky podvodných e-mailov. Stačí, aby ste vy alebo váš zamestnanec uverili a klikli aspoň na jeden z nich. A to je len tá viditeľná časť kybernetickej kriminality.

Rastislav Janota
riaditeľ
Národné centrum kybernetickej bezpečnosti SK-CERT

Útočníkov zaujíma každý človek aj každé zariadenie. Hodnota osobných údajov každého človeka na čiernom trhu je nezanedbateľná. Vaše zariadenia môžu byť následne použité ako odrazový mostík na ďalšie útoky. Vždy ľuďom hovorím: Predstavte si situáciu, ako vám polícia klope na dvere, že z vášho počítača alebo mobilu niekto zaútočil na jadrovú elektráreň... To asi nechcete.

Martin Oczvirk
riaditeľ odboru informačnej bezpečnosti a certifikácie
Úrad na ochranu osobných údajov

To, že nie som bohatý, neznamená, že sa ku mne nemôže niekto vlámať. Aj malé podniky spracúvajú rovnaké druhy citlivých údajov ako veľké firmy. Malé firmy pracujú pre iné firmy, majú zákazníkov a často vložia do podnikania všetko, čo majú. Kybernetický incident znižuje dôveru v schopnosť firiem chrániť citlivé údaje partnerov. Navyše menšie podniky sú náchylnejšie na útoky, keďže často nemajú zdroje na riadnu kybernetickú ochranu.

Michal Gross
riaditeľ IT bezpečnosti
365.bank

Pre útočníkov sú zaujímavé všetky ciele, ktoré im môžu priniesť akýkoľvek zisk. Limitované zdroje malých firiem znamenajú kompromisné nastavenie bezpečnostných opatrení a nedostatočné vzdelávanie zamestnancov o hrozbách, ako sú ransomvér alebo podvody cieleným phishingom. Na redukciu dosahu útokov odporúčam používať dvojfaktorovú autentifikáciu, včas patchovať, zálohovať a oddeliť súkromnú agendu z firemných zariadení.

Tibor Paulen
manažér informačnej bezpečnosti
Stredoslovenská distribučná

Mama myš často prízvukovala svojim deťom: „Orol sa môže objaviť kedykoľvek, aj keď ho nevidíte. Dávajte si pozor a dodržujte všetky zásady, ktoré dookola omieľam.“ Jedno mláďa rebelovalo: „Nemusím sa schovávať. Som malá sivá myška, orol ma z tej veľkej výšky neuvidí. A keby aj, takých ako ja sú v poli tisíce. A všetky sú tučnejšie a nápadnejšie ako ja.“ Lenže orol tadiaľ lietal často a nebol jediný. Náhoda zafungovala.

Andrej Žucha
generálny riaditeľ
ALISON Slovakia

Viete, kto sa vám pozerá do účtovníctva, na fotky a do mailovej schránky? A ste si istí? Záškodníci môžu byť infiltrovaní v systéme aj týždne a mesiace a čakať, aby vás využili na útok alebo začali vydierať vás a vašich zákazníkov. Môžu si tak hospodáriť s vašou firmou, alebo dokonca so životom. Tieto incidenty sú častejšie, ako by ste predpokladali. Hanba a strach však bránia obetiam o tom hovoriť.

Richard Kiškováč
generálny riaditeľ
Elkan

Predstav si, že prídeš do práce a nedostaneš sa ani do jedného počítača, ktorý máš vo firme. Počítače a všetko v nich bude zašifrované. Stane sa to automaticky, bez väčšej námahy útočníka. Koľko dáš firme, aby ti to celé vyčistila a obnovila? Nezaplatíš radšej útočníkovi polovicu z toho za odšifrovanie? Prečo by to nakoniec neskúsil, jemu sa to môže len podariť.

Timea Tomčová
manažérka kybernetickej bezpečnosti
Poisťovňa Union

Ako sa nemôžeme spoliehať na to, že menší byt sa nestane terčom vykrádačky, tak sa nemôžeme spoliehať, že menšia spoločnosť sa nestane terčom kybernetického útoku. Pozrime sa na to očami útočníka. Veľké spoločnosti investujú nemalé zdroje do bezpečnosti, preto pripraviť úspešný útok na veľkú spoločnosť je pomerne zložité. Z toho dôvodu nie je nič nezvyčajné, ak si útočník za cieľ zvolí menšiu spoločnosť aj za cenu menšieho úlovku.

Ján Adamovský
riaditeľ bezpečnosti
Slovenská sporiteľňa

Apríl je mesiac bláznovstiev. Takže: Snažiť sa ošetriť riziko, ktoré môže doslova v okamihu kompletne zničiť dlhoročne budovaný biznis, predsa nemá zmysel. Namiesto zálohovania dát a ochrany pred ransomvérom zaplatíme výkupné desiatky až stovky tisíc eur. Prípadne ak naši účtovníci naletia na podvodný e-mail a pošlú päťdesiattisíc na falošný účet, taktiež to nikoho nebude vôbec trápiť. Ozaj?

Július Selecký
senior technický špecialista ESET

Ak si myslíte, že nie ste atraktívny cieľ, a podceňujete bezpečnostné opatrenia, ste v skutočnosti ešte atraktívnejší cieľ. Menšie firmy majú často slabšie chránené systémy a absentuje tu povedomie zamestnancov o hrozbách. Útočníci tak majú väčšiu šancu, že uspejú s plošnými kampaňami, ktoré im nezaberú veľa času a prostriedkov. Odporúčam sústrediť sa na obranné mechanizmy proti ransomvéru, phishingu či krádeži citlivých dát.

Jaroslav Oster
predseda správnej rady
Preventista.sk

Odpovede podobného typu sú na dennom programe, a nielen v biznis sektore. Kompetentní si často neuvedomujú, že kriminálne aktivity sa nemusia týkať výsostne ich inštitúcie, ale cielenými sú ich zamestnanci. A už vôbec si nepripúšťajú možnosť, že páchateľom na ich systémoch môže byť ich zamestnanec, a opatrenia, ktoré by mali prijať, majú chrániť aj pred takýmto „skrytým“ rizikom.

Pavol Adamec
výkonný riaditeľ oddelenia Riadenie rizík
KPMG Slovensko

Kopa firiem „ľahne“, lebo jednoducho stáli v ceste. Veď – kto by na nás útočil? Vojak síce cieli granát, ale črepina sa nestará, koho zasiahne cestou na cieľ. Aj počítačový vírus môže mať cieľ, ale nestará sa, koho zasiahne, keď sa snaží k nemu dostať najľahšou cestou. Že ste vedľajšou obeťou v boji? Tvorcu vírusu to netrápi. A vás?

Tomáš Hettych
viceprezident,
ISACA

Vaše informačné aktíva máte uložené na rôznych miestach, prevažne v cloudových úložiskách od renomovaných poskytovateľov služieb. A nemyslím tým len osobné údaje. Denne zdieľate aktivity cez sociálne siete a komunikujete cez rôzne komunikátory. Ak si dnes stále myslíte, že nemáte čo skrývať a nemusíte chrániť svoje súkromie a citlivé informácie, tak robíte fatálnu chybu.

HOSPODÁRSKE NOVINY
PIATOK – NEDEĽA 31. MARCA 2023 – 2. APRÍLA 2023

Tieto DDoS útoky sa stali míľnikmi roku 2022

Január

Ukrajinu zasiahol rozsiahly kybernetický útok, ktorý znefunkčnil vládne a ministerské webové stránky.

Február

Ukrajina čelila sérii cielených DDoS útokov na jej ozbrojené sily, ministerstvo obrany, verejný rozhlas a na webové stránky národnej banky.

Máj

Terčom neustálych útokov proukrajinských hackerov bola Sberbank. Banka zaznamenala najväčší DDoS útok s meranou rýchlosťou **450 gigabajtov za sekundu**.

SBERBANK

Jún

Bol mitigovaný doteraz najväčší zaznamenaný HTTPS DDoS útok so silou **26 miliónov požiadaviek za sekundu**. Cielil proti webovej stránke využívajúcej bezplatný plán od Cloudflare.

CLOUDFLARE

Júl

Nórsko, Taliansko aj Litva boli obeťou rozsiahleho DDoS útoku. Cieľom v Nórsku boli veľké spoločnosti poskytujúce dôležité služby obyvateľom. Predpokladá sa, že útoky vykonali proruské hackerské skupiny s cieľom odradiť od podpory Ukrajiny.

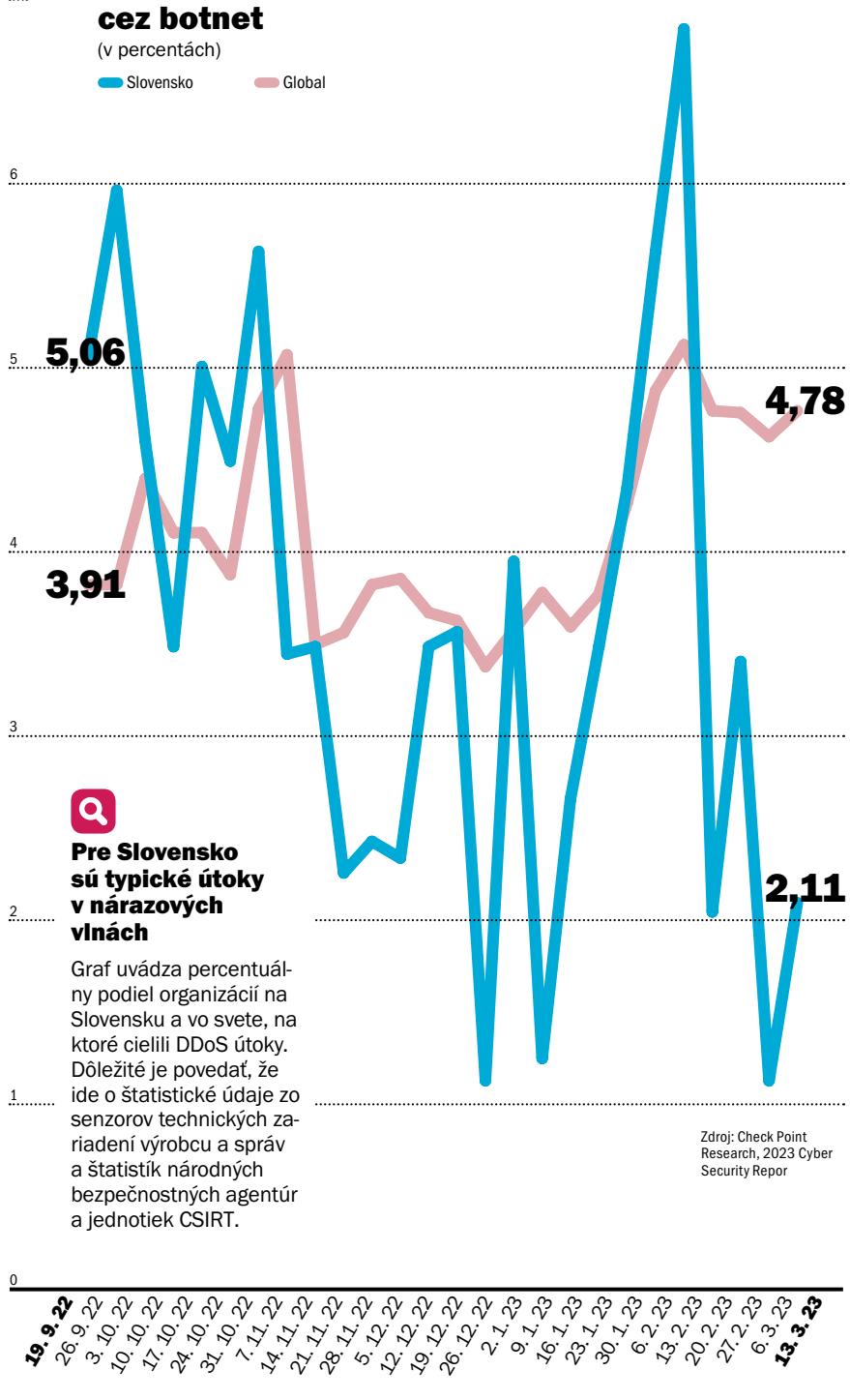
August

Proruská hacktivistická skupina Killnet sa verejne zamerala na výrobcu lietadiel Lockheed Martin a vyzvala ďalšie hackerské skupiny, aby sa k útokom pridali.

Útoky vedené cez botnet

(v percentách)

Slovensko — Global



Pre Slovensko sú typické útoky v nárazových vlnách

Graf uvádza percentuálny podiel organizácií na Slovensku a vo svete, na ktoré cielili DDoS útoky. Dôležité je povedať, že ide o štatistické údaje zo senzorov technických zariadení výrobcu a správ a štatistík národných bezpečnostných agentúr a jednotiek CSIRT.

Zdroj: Check Point Research, 2023 Cyber Security Repor

September

Zaznamenali nový rekordný DDoS útok s vrcholom na úrovni **704,8 milióna paketov za sekundu** (Mpps), čo je asi o 7 percent viac ako pri predchádzajúcom útoku zaznamenanom na rovnakú európsku organizáciu v júli 2021.

Október

Skupina Killnet spustila DDoS útok proti vládnym webovým stránkam v Bulharsku, čo malo za následok ich nedostupnosť. Prihlásila sa aj k zodpovednosti za útoky na vládne weby v USA, pričom zasiahnuté boli webové stránky štátov Colorado, Kentucky, Mississippi a iných.

November

Internetovú stránku Európskeho parlamentu napadli po hlasovaní, ktoré vyhlásilo Rusko za sponzora terorizmu. K zodpovednosti za rozsiahly DDoS útok sa prihlásili skupiny Killnet a Anonymus Russia.

DDoS útoky? Veľa sa už o nich napísalo, ale ešte stále je to málo

TREND

Hackerská skupina Anonymous používa DDoS útoky ako nástroj, pomocou ktorého si vynucuje svoje politické ciele. Aj skupina, aj útoky si získavajú mediálnu pozornosť.

Rôzne hacktivistické a kyberzločinecké skupiny veľmi často používajú DDoS útoky. FOTO: DREAMSTIME

Hacktivistické a kyberzločinecké skupiny používajú DDoS útoky, lebo sú ľahko dostupné a funkčné.

Častou motiváciou útočníkov je diskreditácia organizácie či vyvolanie neurčitých stavov v správaní technických prvkov alebo vo vykonávaní procesov. Tým si útočníci „otvárajú dvierka“ k ďalším typom útokov.

Útočníci menia stratégiu

Na základe samotnej definície Distributed Denial of Service útok spôsobí, že služba sa stane nedostupnou. Ak sú útoky realizované pomocou extrémneho množstva požiadaviek, ide o volumetrické útoky. Tento typ útokov zneužíva fyzické limity sieťových prvkov, akými sú rýchlosť a priepustnosť liniek a sieťových kariet. Limitovaná je aj kapacita centrálneho procesora, čo obmedzuje možnosti spracovávania požiadaviek.
Tu by sa dal robiť vyčerpávajúci zoznam DDoS útokov či už na základe ISO/OSI modelu, cieľového protokolu alebo hardvérového komponentu. Namiesto toho sa však pozrime na trendy.

Nenápadne, ale isto

Ak hovoríme, že volumetrický DDoS útok využíva hrubú silu, na druhej strane tejto pomyselnej stupnice je DDoS útok typu slow loris. Ten, naopak, posiela relatívne málo požiadaviek, no drží extrémne veľa otvorených spojení.

Pre každé spojenie musí cieľová služba alokovať miesto RAM pamäte. Pri dostatočnom počte otvorených spojení sa RAM zaplní a služba sa stáva nedostupnou. Hoci oba prístupy využívajú princípy DDoS, obrana proti nim je diametrálne odlišná.

Keď zariadenia nevládzu

Ak ste sa teda niekedy čudovali, prečo skupina hackerov vie urobiť „na počkanie“ úspešné útoky na kľúčové organizácie a vlády, tak je to práve pre fyzické limity ochrany proti DDoS útokom. Aj to najvýkonnejšie bezpečnostné zariadenie či služba v cloude majú limity.

Tu je namieste uviesť obligátnu bezpečnostnú „poznámku pod čiarou“, že neexistuje 100-percentná ochrana. Práve pri DDoS útokoch má svoje nekompromisné ratio. Existujú však efektívne riešenia, ako eliminovať dosah takéhoto útoku. A to do významnej miery.

Začíname u seba doma

Základná vrstva ochrany sa dá realizovať už správnym škálovaním samotnej služby. Rozložením záťaže pomocou LoadBalancerov medzi viaceré servery či využívaním CDN (content deliver networks) sa záťaž na službu efektívne rozkladá medzi viaceré zdroje.

> Práve sme nastavili optimálnu ochranu proti DDoS útokom, nie 100-percentnú.
>
> **Michal Srnec,**
> CISO Aliter Technologies

K základným prvkom ochrany patrí aj architektúra siete, respektíve publikovanej služby. Služby pre zákazníkov a tie, ktoré konzumuje samotná organizácia, je vhodné rozdeliť medzi rôzne siete. Na aplikačnej úrovni je vhodné použiť metódy ako captcha či rôzne typy presmerovaní. Hoci tieto nastavenia sú často súčasťou dedikovaných zariadení, stále ich vieme realizovať vo vlastnej sieti, a tým zvýšiť úroveň ochrany proti DDoS útokom.

Pridávame hardvér

V druhom kroku zvážme implementáciu zariadení na filtrovanie DDoS útokov. Poskytujú komplexné metódy detekcie, alarmov a možností nastavenia filtrovania škodlivých požiadaviek. Efektivita takýchto zariadení je pri správnom nastavení pomerne vysoká, keďže pre detekciu útokov používajú komplexné heuristické modely a nezriedka aj prvky strojového učenia.

Správna architektúra siete v spojení s hardvérovým vybavením poskytujú bohaté možnosti nastavenia, v oboch prípadoch však počítajte so zriaďovacími a operatívnymi nákladmi.

Služba od poskytovateľa

Väčšina poskytovateľov internetového pripojenia poskytuje službu ochrany pred DDoS útokmi. Nespornou výhodou je, že potenciálny útok sa filtruje ešte pred vstupom do vašej infraštruktúry.

Implementačné náklady bývajú oveľa nižšie. Nevýhodou takéhoto riešenia je práve jeho balíkovosť, čiže absencia možnosti detailného nastavenia.

Služba cloudovej DDoS ochrany posúva útoky ešte ďalej od infraštruktúry. Predstavuje dodatočný element ochrany a vyšší stupeň komfortu z hľadiska možností ochrany, škálovania a nastavenia. Vzhľadom na pomerne jednoduchú implementáciu tejto služby v súčasnosti existuje niekoľko riešení, ku ktorým patria pravidelné reporty a monitorovacie rozhrania.

Nikdy sa to nekončí

Výber riešenia závisí od mnohých faktorov, akými sú možnosti implementácie, akútnosť potreby či v neposlednom rade dostupný rozpočet.

A ani potom nemôžeme spať na vavrínoch – o samotnú DDoS ochranu sa treba pravidelne starať, monitorovať a upravovať jej nastavenia, aby efektívne plnila úlohu vzhľadom na meniace sa požiadavky organizácie a aj povahu útokov.

PORADŇA

Kedy opakovať audit KB?

Audit, konzultácie, servis, implementácia alebo riešenie incidentov? Každá vaša otázka je v kybernetickej bezpečnosti dôležitá.

Či už ste mikropodnik alebo veľká firma, v tejto oblasti stojíte pred mnohými výzvami. Pýtajte sa profesionálov.

Ako lokálny prevádzkovateľ internetu patríme medzi prevádzkovateľov základnej služby. Audit kybernetickej bezpečnosti sme dali urobiť a odovzdali ho v novembri 2021. Zároveň sme si vedomí, že ho treba opakovať. Keďže odvtedy je viacero novelizácií zákona, aké máme povinnosti?

V ostatnom období sa často stretávame s touto otázkou zo samosprávy alebo zdravotníckych zariadení.

Dôležité je povedať, že termín auditu súvisí s tým, či ste robili významné zmeny v parametroch, sieťach a informačných systémoch vašej základnej služby.

Audit kybernetickej bezpečnosti totiž musíte urobiť pri každej významnej zmene. A to najneskôr do dvoch mesiacov, odkedy zmena významne ovplyvnila bezpečnostné opatrenia. Opis, o aké vplyvy ide, nájdete v príslušnej vyhláške NBU.

Ak ste však od posledného auditu významné zmeny neurobili, nový audit musíte začať do dvoch rokov od vydania záverečnej správy o výsledkoch auditu. Vo vašom prípade najneskôr v novembri toho roka.

Na základe informácií z trhu a aj z vlastnej skúsenosti odporúčame začať s výberom audítora, a teda aj s výkonom auditu čo najskôr.

Je totiž veľmi pravdepodobné, že už od septembra nebudú dostupné kapacity na výkon takýchto auditov, keďže väčšina prevádzkovateľov základných služieb mala vykonaný audit k novembru 2021.

Marián Illovský,
certifikovaný audítor
kybernetickej bezpečnosti
auditori.it

Otázky posielajte na adresu: **kyberporadna@mafraslovakia.sk**

RIEŠENIA

Aj v tomto prípade platí, že ak viete, čo sa deje, ste o krok vpred

V kybernetickom svete číha množstvo nástrah. Útoky sú čoraz sofistikovanejšie, útočníci sebavedomejší a pripravení vymýšľať nové metódy pre dosahovanie svojich cieľov.

Aké spôsoby používajú útočníci, aby sa dostali bližšie k vám a vašim dátam? Ako príklady uvádzame niekoľko bežných taktík, ktoré môžu útočníci použiť, aby obišli detekciu a obranu proti útokom DDoS.

Distribuované útoky

Spustenie DDoS útokov z viacerých zdrojov, čo obrancom sťažuje identifikáciu zdroja útoku.

Útoky na aplikačnej vrstve

Zameranie sa na konkrétne aplikácie alebo služby, ich zahltenie prevádzkou a následne ich zlyhanie.

IP spoofing

Na skrytie svojej skutočnej IP adresy sa použije technika spoofingu IP – falšovania zdrojovej adresy, čo obrancom sťažuje blokovanie prevádzky.

Botnety

Pre spustenie útokov DDoS sa použijú botnety, čo sú siete napadnutých počítačov a IoT zariadení, napríklad senzorov alebo dokonca aj domácich zariadení, ako sú IP kamery alebo aj chladničky, ktoré sú pripojené do internetu. Botnety môžu generovať veľké množstvo sieťovej komunikácie z rôznych miest, čo sťažuje sledovanie zdroja útoku.

Amplifikácia útoku

Na zvýšenie objemu útoku sa použije technika efektívneho znásobenia premávky, napríklad využitím špecifických funkcií protokolov DNS alebo NTP. Princíp je jednoduchý: nájsť službu, ktorú viem prinútiť odpovedať väčším množstvom dát, ako útočník posiela, a presmerovať tieto dáta na svoj cieľ

A čo s tým?

Tu je niekoľko krokov, ktoré je nevyhnutné realizovať vo vašej organizácii.

1. Implementujte obrannú stratégiu DDoS. Mali by ste mať zavedenú komplexnú obrannú stratégiu DDoS, ktorá zahŕňa technické riešenia aj procesy. Táto stratégia by sa mala zaoberať všetkými potenciálnymi vektormi útokov DDoS a poskytnúť návod, ako reagovať na útok.

2. Používajte sieť na doručovanie obsahu. CDN sieť môže pomôcť absorbovať DDoS jeho distribúciou v sieti serverov. Môže to pomôcť znížiť vplyv útoku na infraštruktúru organizácie.

3. Implementujte obmedzenia rýchlosti. Zabránite tak útokom na aplikačnú vrstvu obmedzením počtu požiadaviek, ktoré môžu byť odoslané konkrétnej aplikácii alebo službe. Pomáha to zabrániť zahlteniu aplikácie.

4. Používajte systémy prevencie narušenia. Tento systém (IPS) pomôže identifikovať a blokovať pokusy o spoofing IP, ako aj iné typy škodlivej prevádzky.

5. Pravidelne testujte a aktualizujte obrany. Testovanie a aktualizácia podľa potreby zabezpečujú, aby bola DDoS obrana účinná proti najnovším typom týchto útokov.

Pri obrane využite spoluprácu s poskytovateľmi internetových služieb alebo služby tretích strán.

6. Nasaďte služby anti-DDoS. Mnohí poskytovatelia ponúkajú služby, ktoré pomôžu organizáciám brániť sa. Zvyčajne zahŕňajú čistenie prevádzky, obmedzenie sadzieb a ďalšie techniky zmierňovania DDoS.

7. Zdieľajte informácie o hrozbách. Pomôžete tak identifikovať a blokovať škodlivé prenosy.

Obrana proti DDoS útokom je súčasťou kybernetickej odolnosti. FOTO: DREAMSTIME

8. Implementujte aj filtrovania prenosov. Poskytovatelia internetových služieb môžu implementovať filtrovanie prenosu na okraji siete a blokovať tak prenosy zo známych škodlivých zdrojov.

9. Vypracujte si incident plány. V prípade útoku budú definované úlohy a zodpovednosti každej strany.

10. Zúčastňujte sa na celoodvetvových iniciatívach. Cieľom je zlepšiť bezpečnosť a odolnosť smerovacej infraštruktúry internetu.

A jedenásta rada:
Odložte si toto desatoro. Odvetvie kybernetickej kriminality sa stále vyvíja a hľadá agresívnejšie formy. Principiálne pravidlá kybernetickej bezpečnosti sú však oporou.

Stanislav Smolár,
manažér oddelenia
bezpečnosti Soitron