ALISON

Kto roznáša infekciu v kybernetickej pandémii a ako sa na tom zarába

Ešte nedávno bol na čele rebríčka ransomvérových útokov ten na Colonial Pipeline, ktorý zastavil transport surovín a vyšiel obeť na vyše štyri milióny dolárov. Stačí kúpiť na zabehnutom trhu ransomvér a mať kŕdeľ botov.

Ostatný masívny útok? Predvčerom

Najnovšou obeťou sa koncom mája stal najväčší svetový dodávateľ mäsa, čo predstavuje novú hrozbu pre **globálnu potravinovú bezpečnosť**, už aj tak postihnutú pandémiou. Spoločnosť JBS SA má zablokované severoamerické a austrálske počítačové siete. Oznámila to e-mailom bez komentára a uviedla, že „incident môže oddialiť určité transakcie so zákazníkmi a s dodávateľmi“.

Rastúce odvetvie

Na úspechu ransomvérových útokov sa podieľa aj fakt, že ich uskutočnenie si nevyžaduje špeciálnu technickú dômyselnosť. Obchodný model ransomvér ako služba (RaaS) poskytuje služby potenciálnym útočníkom podobne ako v bežnom softvérovom a infraštruktúrnom priemysle. Softvér ako služba (SaaS) zaznamenal úspech už dávno a teraz ho zlepšujú zločinecké organizácie.

Zákazník sa jednoducho prihlási na portál RaaS, vytvorí si účet, zaplatí bitcoinom, zadá podrobnosti o type škodlivého softvéru, ktorý si želá vytvoriť, a klikne na tlačidlo odoslať. Predplatitelia si môžu objednať zákaznícku podporu, spojiť sa s komunitou, majú na portáli dokumentáciu, aktualizáciu funkcií a ďalšie výhody identické s legitímnymi produktmi SaaS.

Korporátne zručnosti

Špecialisti, ktorí ponúkajú balíky exploitov a vytvárajú RaaS ponuky, sú profesionálni programátori, často predtým zamestnaní v korporáciách a vo veľkých firmách. Teraz pracujú ako sólisti a **kvalita ich ponúk sa líši**. Zatiaľ čo tie sofistikovanejšie predstavujú zákaznícke konzoly, ktoré zobrazujú štatistiku infekcie, šifrované súbory a platby výkupného, na trhu sú v ponuke aj jednoduché softvéry.

Platba je za používanie licencie, mesačný paušál, podiel na výkupnom alebo motivačný systém „no ransom no fee“, čiže platba za službu iba v prípade **úspešného výkupného**. Napríklad paušálne platby sa pohybujú od 500 dolárov mesačne po 200 dolárov týždenne.

A či je model ziskový?

O tom niet pochýb. Celkové výnosy RaaS modelu sa v roku 2020 pohybovali na úrovni **20 miliárd** amerických dolárov. Rok predtým to bolo „iba“ 11,5 miliardy amerických dolárov. V celosvetovom prieskume piatich tisícok IT manažérov sa potvrdilo, že až 51 percent z nich zasiahol v roku 2020 ransomvérový útok a 27 percent z nich sa rozhodlo zaplatiť výkupné.

ALISON

Na čele útoku idú boty

Niekde sa to musí začať. Internetový bot (skratka pre „robot“) je softvérová aplikácia, ktorá spúšťa **automatizované úlohy** cez internet. Pre svojho majiteľa vykonáva určitú rutinnú činnosť na internete, najčastejšie zbiera dáta, odosiela a spracováva požiadavky na služby vzdialených serverov. Úlohy vykonávané botmi sú zvyčajne jednoduché a vykonávajú sa omnoho rýchlejšie v porovnaní s ľudskou aktivitou na internete.

Tí zlí

Spider Bots, Scraper Bots, Spam Bots, Social Media Bots, Ticketing Bots sú škodlivé boty, používané na automatické skenovanie zraniteľností webových stránok a na jednoduché útoky. Slúžia na konkurenčný zber dát, krádež osobných a finančných údajov, neoprávnené prihlasovanie, podvody s digitálnou reklamou a na transakčné podvody.

„Zlé“ boty (bad bots) vykonávajú škodlivé úlohy, ktoré umožňujú útočníkovi **vzdialene prevziať kontrolu** nad napadnutým počítačom. Po infikovaní sa tieto stroje označujú aj ako zombie. Kybernetický zločin tak môže prenajať botnety ďalej na zasielanie spamov, podvody, phishing, odcudzenie totožnosti a útoky na legitímne webové stránky a siete.

Boty v sieťach sociálnych médií sa používajú na automatické generovanie správ, podporu kampaní, sledujú používateľov, generujú lajky alebo sú to falošné účty. Odhaduje sa, že **9 – 15 percent účtov** na Twitteri sú sociálne roboty. Používajú sa na infiltráciu do skupín ľudí a na propagáciu konkrétnych myšlienok. Aj keď sociálne siete prijímajú regulácie, sociálne boty tu zohrávajú v online verejnej mienke významnú úlohu. Keďže vykazujú podobné správanie ako skutoční používatelia, je ťažké ich identifikovať.

Činnosť botov rastie

Škodlivé boty predstavovali v minulom roku 25,6 % z celkového objemu sieťovej prevádzky na webových stránkach. V porovnaní s rokom 2019 ide o **nárast 6,2 percenta**.

Podiel „dobrých“ botov (good bots) predstavuje 15,2 percenta sieťovej prevádzky. Na internete sa totiž pohybuje veľa druhov botov, legitímnych aj škodlivých. Medzi tie legitímne sa radí napríklad Googlebot, aplikácia, ktorú používa Google na prehľadávanie internetu a indexovanie na účely vyhľadávania.

Ľudia a ich návštevnosť webových stránok tvorili 59,2 objemu prevádzky, čo znamená za rok 2020 medziročný pokles. V každom prípade sa tak **frekvencia** softvérovej „premávky“, či už dobrej alebo zlej, v porovnaní s ľudskou zvyšuje. A to aj napriek tomu, že hovoríme o pandemickom roku, keď sa používanie počítačov a mobilných zariadení dramaticky zvýšilo.

Zdroj: Bad Bot Report 2021

Zlé boty zasahujú všetky odvetvia

Medzi odvetvia s najvyššou prevádzkou zlých botov patria telekomunikácie a poskytovatelia internetových služieb. Aktivita zlých botov tvorila v telekomunikáciách a ISP až **45,7 percenta z celkovej sieťovej prevádzky**, nasleduje odvetvie počítače & IT (41,1 %), šport (33,7 %), spravodajstvo (33 %) a podnikové služby (29,7 %)

Sú rafinované

Väčšinu prevádzky škodlivých botov tvoria tzv. pokročilé trvalé boty (Advanced Persistent Bots – APB) dosahujúce 57,1 percenta. Ide o kombináciu miernych a pokročilých botov, ktorých odhalenie a **oslabenie je náročnejšie**. Cyklujú náhodnými adresami IP, vstupujú cez anonymné proxy, menia svoju identitu a napodobňujú ľudské správanie.

Sú domácej výroby

Zlé boty často pochádzajú z tej istej krajiny, na ktorú cielia. USA, Čína a Spojené kráľovstvo sú v prvej trojke krajín, z ktorých pochádza najviac prevádzok zlých botov. Rovnako sa nachádzajú aj v rebríčku krajín, ktoré sú najčastejšie vystavené útokom.

Meat Is Latest Cyber Victim as Hackers Hit Top Supplier JBS, Bloomberg 31. 5. 2021

Combating the Rise of Ransomware-as-a-service, apríl 2021

Bad Bot Report 2021

Bots