View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

Záložka: Geolokace

Geolokace a bezpečnost počítačových sítí

Chráníte si své internetové soukromí a myslíte si, že nelze určit vaši skutečnou polohu? Jak se zjišťuje poloha v Internetu a kdo ji potřebuje znát?

Čím lépe je útok připraven, tím je větší šance na jeho úspěch; zejména důležitý je moment překvapení a následně rychlost rozvíjení úspěchu. Takto šroubovaná formulace odpovídá sice spíše vojenským zvyklostem, ale i ty se pro kybernetický prostor dají docela dobře aplikovat. Potenciální útočník potřebuje znát o své oběti co nejvíce informací a to nejen technických, ale i obecných, jako je její geografická poloha. Internet k tomuto nabízí řadu možností s přesností od úrovně regionu až po jednotky metrů.

Co vlastně útočník může zjištěním polohy (geolokací) potenciální oběti konkrétně získat? Především souvislosti. Může snadno odhalit aktivní zařízení v dané lokalitě a to bez ohledu na jejich IP adresy. Takto může utvořit účelové uskupení k realizaci velmi efektivního DDoS útoku. Útoky mohou být velmi kvalitně personalizovány a to zejména ve formě mailů, obsahujících na míru ušité, ovšem podvodné informace viz Box 1.

Jak se bránit? Stejně jako u vojenské činnosti je třeba zámysl útočníka co nejdříve rozpoznat. Útočník samozřejmě nemůže být pasívní, avšak je-li opatrný a připravuje-li se postupně, bude objem jeho provozu ležet pod prahem rozlišitelnosti sledovacích mechanismů a unikne tak jejich pozornosti. Zde může napomoci jiný pohled na provoz, geolokační, využívající například možností NetFlow, viz obrázek 1. Takto lze například odhalit podezřelé zdroje aktivity, ty mohou pocházet i ze států, označovaných jinými státy jako méně slušné.

Obr. 1: Zobrazení polohy a intenzity (zeleně nízká) síťového provozu komunikujících zařízení [2].

Určování polohy

Ke zjišťování polohy zařízení lze použít několik skupin metod, které se od sebe liší například použitými principy a přesností. Velmi často jsou hranice mezi dílčími metodami neostré. Základní dělení geolokace rozeznává metody pasivní a aktivní.

Pasivní metody vyhledávání polohy zařízení

U pasivních metod není nutno se zařízením, jehož poloha je zjišťována, nijak komunikovat. Nejjednodušší metoda z této kategorie je založena na faktu, že IP adresy sítí jsou institucím přidělovány (a registrovány) centrálně prostřednictvím regionálních internetových registrátorů [1]. K údajům těchto registrátorů lze snadno přistupovat například pomocí nástroje *whois a* zjištění IP vlastníka adresy tedy znamená zjištění jeho polohy. Přesnost ani spolehlivost nejsou příliš velké, nicméně pro určení státu či města obvykle postačí. Zejména u institucí s rozsáhlými sítěmi, pokrývajícími území státu, se ovšem může stát, že za polohu všech zařízení v dané síti bude považováno registrované sídlo dané instituce. Existují ale i specializované společnosti, které sbírají údaje o IP adresách z různých zdrojů, příslušné polohy zpřesňují (včetně zeměpisných souřadnic) a poskytují na komerční i (v menším rozsahu) nekomerční bázi [4]. Pro přístup k těmto údajům lze využít speciální aplikační programové rozhraní (API), viz [5], což výrazně usnadňuje tvorbu aplikací, používajících geolokaci. Podpora geolokace je již přímo součástí připravovaného standardu HTML5, který zdaleka není dokončen; definitivně tak tomu má být až v roce 2022 (!).

Komplikaci co do určení skutečného polohy představují tunelovací mechanismy, obvykle kombinované s překladem adres. Za polohu bude považován výstup z tunelu; který se od

1 Těch je na zeměkouli celkem pět: RIPE (pro Evropu a země bývalého Sovětského svazu), ARIN (Severní Amerika), LACNIC (Latinská Amerika), APNIC (Asie, Austrálie a země v Pacifiku), AfriNIC (Afrika).

skutečného stanoviště může významně lišit. Tohoto využívají nejrůznější anonymizační systémy, jejichž cílem je onu reálnou polohu utajit; například projekt Tor [8].

V 90. letech 20. století se objevila myšlenka vložit údaje o poloze zařízení přímo do systému DNS, takže by byly dostupné nástroji typu *nslookup* či *dig*, viz RFC1712 a RFC1876. Vložení by musel provést příslušný administrátor, což by představovalo jeho dodatečnou zátěž. Možná i proto se podpora a využívání této metody příliš nerozšířily a pokud ano, pak obvykle pro popis poloh významných zařízení typu servery nebo směrovače.

Příklad záznamu v DNS Univerzity obrany v Brně pro zařízení `routks.unob.cz` s uvedením jeho IP adresy, zeměpisných souřadnic a nadmořské výšky.

```
routks.unob.cz.      A    160.216.223.1
routks.unob.cz.      LOC  49 12.795 N 16 35.874 E 227m
```

Pasivní metody mohou mít i exaktnější podobu a poměrně vysokou přesnost zjištění polohy, předpokladem ale je využití dodatečných zdrojů informací. Ty nemusí být zdaleka vždy dostupné a navíc jsou vhodné pouze pro určité situace, například pro zařízení využívající bezdrátové připojení (WiFi, GSM). Je-li předmětná stanice v dosahu dostatečného počtu přístupových bodů WiFi nebo základnových stanic GSM, lze její polohu určit obdobou triangulace. Místo měření úhlů se použijí údaje o intenzitě elektromagnetického pole generovaného přístupovým bodem, o časovém zpoždění (době odezvy) apod. Zásadní komplikací této metody je ovšem potřeba přístupu k informacím získaných těmito přístupovými body nebo základnovými stanicemi.

Velcí výrobci jako je Cisco dodávají pro určení polohy zařízení v bezdrátových sítích s centrální správou a postavených na jejich prvcích hotová řešení [1]. Pokud ale centrálně spravovaná síť neexistuje, je prakticky nemožné získat potřebná data, neboť by bylo třeba oslovit všechny jednotlivé vlastníky, občany i firmy. Navíc jednoduché domácí přístupové body ani nemusí potřebné údaje poskytovat. V případě základnových stanic GSM jsou takové údaje chráněny na základě legislativních norem a zpřístupňují se jen např. pro účely vyšetřování trestné činnosti.

Aktivní metody vyhledávání polohy zařízení

Podstatou těchto metod je aktivní spolupráce předmětného zařízení. Extrémní případ představuje přímé sdělení souřadnic jeho polohy, což připadá v úvahu u zařízení vybavených například modulem GPS nebo obdobným systémem. Nemusí se jednat o záměrnou akci uživatele, ba dokonce může být provedena i proti jeho vůli. S nárůstem počtu tabletů a inteligentních telefonů se stále více otevírá pole pro skrytou změnu nastavení nebo instalaci sledovacího programu do těchto zařízení.

Polohu zařízení lze určit i na základě jiných, tomuto zařízení známých údajů. Zařízení například neustále zjišťuje přístupové body (či základnové stanice) ve svém okolí a může informace o nich sdělit geolokačnímu serveru. Samotné zařízení přitom nemusí být k žádnému přístupovému bodu přihlášeno (nějaký komunikační kanál do Internetu samozřejmě potřebuje). Je-li poloha okolních přístupových bodů známá, je dosti přesný odhad polohy hledaného zařízení poměrně snadný; stačí předpokládat, že přístupový bod pokryje kruh o poloměru asi 150 metrů. Tento postup využívá firma Google za spolupráce s databází GoogleMaps. Klíčem k úspěchu je znalost umístění přístupových bodů. Ty (a nejen je) firma Google v minulosti vyhledávala současně se snímkováním okolí prostřednictvím vozidel Google Street View, aniž by toto zveřejnila. Odhalení uvedené praktiky vedlo v roce 2010 k ostrým reakcím některých států (např. Německo, Kanada), navíc se ukázalo, že byla zčásti zachycována i osobní data uživatelů [7]. Firma Google následně tento postup přestala

používat, nicméně i tak je zmíněná databáze přístupových bodů obrovská a je neustále aktualizována. Jak? Nejčastěji samotnými uživateli, jejichž dotazy obsahují, jak bylo uvedeno, údaje o všech přístupových bodech v jejich okolí. Údaje z těchto dotazů jsou shromažďovány a prostřednictvím databázových metod zpracovávány. Tak lze například doplnit nový přístupový bod včetně jeho umístnění, upřesnit polohu již známého nebo vyřadit ten, který se dlouho neozval. Zajímavé důsledky by mohla způsobit migrace známého přístupového bodu, například při přestěhování uživatele – tam by zpočátku byla poskytována mylná informace o poloze, avšak časem by byla opravena.

Box 1

Malware a geolokace

Geolokace je využívána tvůrci malware k cílenému šíření škodlivého kódu a lákání nových obětí. Rovněž majitelé botnetů obvykle sdružují nakažená zařízení podle jejich geologické polohy. Poloha botů dokonce určuje cenu, za kterou jsou prodáni či pronajati k nelegální činnosti. Znalost polohy je využívána např. k zesílení útoku odepření služby, kdy útoku se zúčastní boti v bezprostřední blízkosti cíle. Vybrané příklady malwaru používající geolokaci jsou:

Waledac – botnet se neslavně proslavil šířením nevyžádané pošty v Internetu. K lákání nových obětí botnet mimo jiné využíval podvodné webové stránky, které na základě polohy oběti vhodně měnily svůj obsah. Botnet např. šířil informace o údajném teroristickém útoku v lokalitě oběti, doplněné o odkaz na falešné stránky agentury Reuters.

Zeus (SpyEye, Ice IX) – trojský kůň vytvořený k nelegálnímu získávání přihlašovacích údajů k účtům el. bankovnictví, el. pošty aj. Trojský kůň obsahuje profesionálně připravené jazykové mutace (italština, francouzština, němčina, turečtina a několik dialektů angličtiny) podvodných stránek. Mimo polohy je navíc možné cílit útok na konkrétní službu anebo organizace viz např. útoky proti bankám v Británii. V současnosti čelí tvůrci a provozovatelé botnetu soudnímu obvinění v USA [6].

Reveton – novinka letošního léta, vyděračská varianta trojského koně (angl. ransomware), který uživateli zablokuje počítač a požaduje zaplacení výkupného viz obrázek 2. Uživateli po zapnutí jeho počítače zobrazí údajné policejní oznámení o porušení zákona daného státu, zjištěného prostřednictvím geolokace, o uložení pokuty a o způsobu, jak provést platbu k odblokování počítače [9].

Box 2

Geolokace a Internet

Své využití našla geolokace nejprve v oblasti cílené reklamy a detekci podvodů při elektronických platbách prostřednictvím Internetu. V současnosti je ale uplatňována v řadě dalších oblastí:

GeoDNS – slouží ke směrování uživatelů na geograficky nejbližší servery s jimi požadovanými službami. GeoDNS je využívána zejména globálními poskytovateli obsahu Akamai, Google, Microsoft, Facebook aj. Použití GeoDNS umožňuje dále vyvažovat zátěž a v případě poruchy přesměrovat provoz do jiné lokality.

Cloudové služby – uživatelé cloud prostředí mohou vyžadovat z obchodních anebo legislativních důvodů geografická omezení, tj. rozhodovat, kde budou jejich aplikace provozovány (včetně geografického zálohování). Na základě geografické polohy mohou být optimalizovány výpočetní zdroje cloudu např. pro velké městské aglomerace.

Dostupnost obsahu – data jsou zpřístupňována na základě polohy uživatele. Jedná se např. o internetové vysílání, kdy na základě vysílacích práv je povolen přístup pouze uživatelům sídlícím ve vybraném státě. Může se též jednat o omezení z důvodu hospodářských sankcí nebo vývozních omezení, viz např. politika USA proti některým režimům.

Vícefaktorová autentizace – během přihlašování uživatele je mimo jeho uživatelského jména a hesla ještě zkontrolována i jeho geografická poloha. Pokud se uživatel hlásí z místa, odkud tak běžně nečiní nebo nesmí činit (např. z internetové kavárny), je mu přístup odepřen.

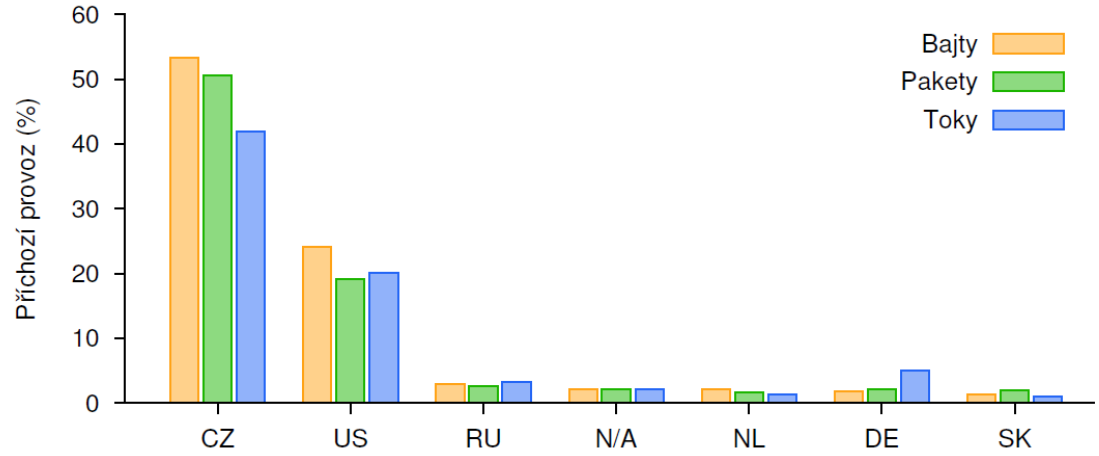
Obr. 2: Personalizovaná výzva, generovaná trojským koněm Reveton, požadující uhrazení pokuty za údajné přechovávání v daném státě (zjištěném geolokací) ilegálního obsahu.

Provoz a sledování sítí

Administrátoři velkých sítí, typicky poskytovatelů připojení (ISP), jsou zvyklí uvažovat nikoliv geograficky, ale na úrovni autonomních systémů (RFC1930). Zabývají se vzájemným propojováním skupin sítí, jejichž skutečná dislokace, o konkrétních IP adresách nehovoříce, pro ně obvykle není důležitá. Při odhalování složitých či neobvyklých problémů tomu ovšem může být jinak. Znalost polohy uživatelů hraje stále významnější roli pro poskytování nových služeb a fungování dnešního Internetu. Více k používání geolokace v Internetu najdete v Boxu 2.

Obrázek 3 ukazuje, ze kterých států pochází provoz tekoucí do sítě Masarykovy univerzity. Nejvyšší podíl má pochopitelně provoz z tuzemska a pak následují USA, kde se nalézají klíčoví poskytovatelé obsahu a služeb. Jim stále více uživatelů svěřuje svá data, která pak končí v datových centrech po celém světě.

Při monitorování síťového provozu pomocí IP toků (NetFlow) je běžná praxe vytvářet profily (náhledy na dění v síti) podle protokolů (TCP, UDP, ICMP atd.) a známých portů (HTTP – 80, DNS – 53 atd.). Tento přístup umožňuje vizuální kontrolu a rozpoznání problému v síťových statistikách, pokud dojde k viditelné anomálii (špička na grafu). Doplněním geoinformací dostávají mnohdy fádní průběhy zobrazovaných dat nový rozměr, který umožňuje snazší orientaci v datech a identifikaci podezřelé komunikace.

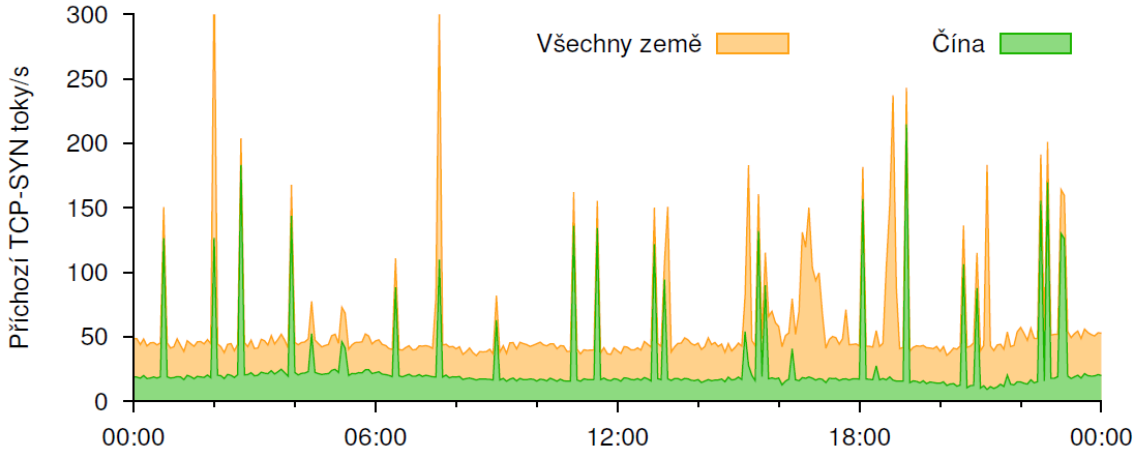


Obr. 3: Rozložení provozu do sítě Masarykovy univerzity podle komunikujících států.

Bezpečnost počítačových sítí

Kybernetický prostor pomíjí klasické pojetí hranic a vzdáleností. Pravidelně tak nastává situace, kdy zdroj bezpečnostního incidentu je mimo vlastní síť. Následně je nutné zjistit o útočníkovi a jeho aktivitách co nejvíce informací. Na základě logů serverů a síťových záznamů lze určit seznam IP adres, kterých se incident dotýká. U nich jsou pak dohledávány údaje typu kontakt na majitele IP adresy, jméno organizace, země původu aj. Jedná se však o pasivní přístup, který se uplatní až poté, co zjistíme, že došlo k incidentu.

Geolokaci pro klasifikaci a profilování sledovaného provozu v reálném čase začínají využívat metody detekce anomálií. Praktický příklad ukazuje obrázek 4, kde jsou zobrazeny neúspěšné pokusy o navázání TCP spojení s počítači v síti Masarykovy univerzity. Neúspěšná spojení jsou typickým příznakem skenování anebo vyhledávání zranitelných či nezabezpečených služeb. Více než 40 % zaznamenaných pokusů pocházelo z Číny. Dedikovaný „čínský“ profil zredukoval množinu zkoumaných NetFlow dat natolik, že bylo možné pozorovat i útoky vyznačující se nízkou intenzitou provozu. V celkovém provozu byly tyto útoky nepozorovatelné, neboť byly upraveny tak, aby je nebylo možné běžnými přístupy detekovat. Jednalo se o soustavné pokusy o proniknutí do připojených počítačů, což by mohlo indikovat např. hrozbu typu APT (Advanced Persistent Threat).



Obr. 4: Neúspěšné pokusy o navázání TCP spojení.

Závěr

Každý počítač (resp. síťové zařízení) v Internetu je identifikován unikátní IP adresou (či adresami), která však sama o sobě nenese informaci o poloze. Metody dovozování polohy původně navržené pro internetovou reklamu si záhy osvojili i tvůrci malware k vytváření stále důmyslnějších útoků. V oblasti počítačových sítí se zejména jedná o používání specializovaných geolokačních databází a personalizaci sdělované informace.

U mobilních zařízení mají geolokační informace důvěrný charakter a ať již způsob jejich získávání nebo následné použití může pro uživatele znamenat řadu bezpečnostních rizik. Mnohdy přehnané snahy některých firem o jejich získání vedly v minulosti k incidentům, kdy uživatelé byli sledováni proti své vůli.

Jednou z hlavních překážek bránících výraznějšímu rozvoji geolokace v Internetu je nejednotný přístup zejména tvůrců obsahu a chybějící standardy. IETF se problematiku snaží řešit pracovní skupinou GEOPRIV [3] (sada obsáhlých a složitých RFC). W3C prosazuje podporu přes HTML5 a Geolocation API [10] (jednodušší, podporováno ze strany Google).

Pavel Čeleda

celeda@ics.muni.cz

Josef Kaderka

josef.kaderka@unob.cz

Použité zdroje

[1] CISCO. Monitoring Wireless Devices. *http://www.cisco.com/en/US/docs/wireless/wcs/7.0MR1/configuration/guide/mon.html.*

[2] HOFSTEDE, R. SURFmap – A Network Monitoring Tool Based on the Google Maps API. *http://surfmap.sf.net/.*

[3] IETF. Geographic Location/Privacy (Active WG). *http://tools.ietf.org/wg/geopriv/.*

[4] MaxMind. Databáze GeoIP. *http://www.maxmind.com/app/ip-location.*

[5] MaxMind. Aplikační rozhraní pro databázi GeoIP. *http://www.maxmind.com/app/developers.*

[6] MICROSOFT et. al. Soudní obvinění proti tvůrcům a provozovatelům botnetu Zeus. *http://www.zeuslegalnotice.com/.*

[7] Office of the Privacy Commissioner of Canada. Complaints under the PIPEDA. *http://www.priv.gc.ca/media/nr-c/2010/let_101019_e.asp.*

[8] Projekt Tor. Anonymizace uživatele při pohybu v Internetu. *https://www.torproject.org/.*

[9] The Swiss Security Blog. Scareware Locks Down Computer Due To Child Porn and Terrorism. *http://www.abuse.ch/?p=3610.*

[10] W3C. Geolocation API Specification. *http://www.w3.org/TR/geolocation-API/.*

Ing. Pavel Čeleda, Ph.D.

Absolvent Univerzity obrany, nyní působí jako odborný pracovník na Ústavu výpočetní techniky Masarykovy univerzity.

Ing. Josef Kaderka, Ph.D.

Absolvent Vojenské akademie v Brně, kde na její následnici, Univerzitě obrany, působí jako vedoucí odborné skupiny na katedře komunikačních a informačních systémů. Je instruktorem síťové akademie Cisco v oblasti počítačových sítí a jejich bezpečnosti.