Pavel Bašta
CZ.NIC, z. s. p. o.; Milešovská 5; 130 00 Praha 3

Budování a implementace českého národního Cyber Threat Intelligence System

Výzkumný projekt PRedikce a Ochrana Před Kybernetickými Incidenty,[1] dále jen PROKI, vznikl na půdě českého národního bezpečnostního týmu CSIRT.CZ[2] jako reakce na rostoucí počet dostupných zdrojů informací o probíhajících i uskutečněných kybernetických incidentech a jejich původcích. Ve svých východiscích projekt reaguje na dva hlavní problémy, které sebou přináší rostoucí tlak na zpracování těchto informačních zdrojů. První z nich je potřeba distribuce informací o incidentech do jednotlivých sítí způsobem, který bude pro správce v koncových sítích srozumitelný a přehledný. V souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti systém zároveň umožní na základě zjištěných hrozeb poskytovat informace pro vydání varování NBÚ dle § 12 výše uvedeného zákona. Druhý problém pak představuje rostoucí potřeba hlubší analýzy jednotlivých incidentů a vztahů mezi nimi.

Zdroje informací o incidentech a problematika jejich zpracování

Pro získávání informací o kybernetických bezpečnostních incidentech v prostředí Internetu je možné využít následující typy zdrojů. První z nich představují tzv. honeypoty. Tato zařízení umožňují detekovat útoky, případně sledovat počínání útočníků po úspěšné kompromitaci systému. Může se jednat o zařízení, která jsou záměrně nakonfigurována tak, aby „podlehla" útočníkovi a provozovatel příslušného honeypotu (např. výzkumná organizace či CSIRT/CERT) si tak ověřil, že se jedná o skutečný záměr. Zároveň tento typ honeypotů umožňuje sledovat další útočníkovo počínání a získávat tak například vzorky nového malware.[3] Jiný typ honeypotu může stavět na využití IP adres, které ještě nikdy nebyly v prostředí Internetu využity k jinému účelu. Proto lze pokusy o komunikaci s těmito IP považovat za podezřelou. Útočníci při hledání zranitelných zařízení na Internetu často skenují například celý IPv4 rozsah, což pak znamená, že při svém skenování narazí i na tyto honeypoty. Protože však neexistuje reálný důvod, aby běžný uživatel Internetu začínal komunikaci s dosud nevyužívaným rozsahem IP adres, je takovéto chování vyhodnoceno honeypoty jako pokus o útok. Nevýhodou tohoto druhu honeypotů je větší náchylnost k false positive, neboť komunikaci může zahájit omylem i uživatel, který nemá žádné útočné úmysly, například díky překlepu při zadávání IP adresy.

---

[1] Projekt „Predikce a ochrana před kybernetickými incidenty (PROKI)" (VI20152020026) je realizován v rámci Programu bezpečnostního výzkumu ČR na léta 2015 – 2020.

[2] Provozovatelem národního CERT dle § 17 a 18 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, je na základě veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem dne 18. prosince 2015 sdružení CZ.NIC, správce národní domény .cz.

[3] Výkladový slovník kybernetické bezpečnosti (ISBN 978-80-7251-397-0) definuje malware jako obecný název pro škodlivé programy. Mezi tyto programy patří především počítačové viry, trojské koně, červy, špionážní software.

Další zdroj informací nabízejí síťová zařízení, jako jsou firewally, různé síťové sondy či Intrusion Detection Systémy (IDS). Ty mohou logovat zachycené pokusy o neoprávněnou komunikaci. Ne každý takovýto pokus však musí být nutně útokem. V tomto ohledu svou kvalitou vyčnívají data z výzkumného projektu Turris,[1] která jsou získávána z firewallů routeru Turris a jsou vyhodnocována speciálními algoritmy. Vzhledem k velkému rozprostření těchto zařízení napříč sítěmi v České republice lze mnohem lépe rozlišit reálný útok od jiné náhodné události. Pokud konkrétní IP adresa otestuje určitý port, či sadu portů napříč sítěmi, je velmi nepravděpodobné, že by se jednalo o náhodnou událost a takovéto počínání lze tedy považovat za podezřelé.

Zvláštní druh dat pak představují informace o klientech botnet sítí.[2] Ty jsou obvykle získávány díky sledování provozu u objevených řídících serverů botnetů (C&C), nad kterými se nějakým způsobem (obvykle v USA na základě rozhodnutí soudu) podařilo převzít kontrolu. Díky sledování IP adres, které se k takovémuto serveru připojují, je pak možné identifikovat nakažené počítače, které byly součástí botnetu.

Dalšími zdroji informací o bezpečnostních incidentech mohou být informace detekované samotnými uživateli (typicky phishingové stránky), nebo informace pocházející především z behaviorální analýzy malware (typicky C&C servery). Informace z behaviorální analýzy poskytuje například známá služba VirusTotal, ale získávají je také ostatní analytici v rámci vlastních analýz zachycených vzorků malware. Velmi dobré informace o chování malware lze získat při použití open source programu ProcDOT. Tento nástroj zobrazí informace o souborech, ke kterým daný proces přistupoval, o klíčích registru Windows, o síťové komunikaci a dalších důležitých parametrech. Takto lze rychle získat komplexní přehled o chování malware a zároveň rozpoznat klíčové části průběhu infekce, například při napadení skrz neošetřenou chybu prohlížeče. Jednotlivé části je možné interaktivně procházet, stejně jako pustit mód animace, který nám pomůže pochopit průběh infekce v čase.[3]

Velká variabilita zdrojů přináší nároky na jejich hromadné zpracování a následné využití. Problém se týká jak variability metod použitých pro doručení (HTTP, SMTP, vlastní API), tak ještě širší variability formátů, ve kterých jsou informace doručovány (csv, xml, json, stix, openioc). Nesené informace jsou také nekonzistentní z pohledu typu útoku (domény a URL hostující malware, IP adresy aktivně útočící na jiné stroje, IP adresy C&C serverů, IP adresy klientů botnetů, či phishingové URL). Shromáždění všech těchto informací do jednoho místa a jejich distribuce a vyhodnocování jsou tedy náplní našeho výzkumného projektu.

Sběr informací o incidentech

Po zvážení různých kritérií, jako jsou množství podporovaných zdrojů, otevřenost projektu, možnost snadné tvorby vlastních konektorů a možnost obohacení dat, byl jako základní kámen systému PROKI vybrán společný open source projekt IntelMQ

[1] Více informací lze nalézt na webových stránkách projektu www.turris.cz
[2] Botnet představuje označení pro síť infikovaných počítačů, které umožňují útočníkovi ovládat výpočetní výkon až mnoha set tisíc strojů současně. Hlavní zneužití botnetů představuje realizaceDDoS útoků nebo infikování počítačů dalším malwarem.
[3] BAŠTA, Pavel. ProcDOT a Density Scout: užitečné nástroje pro analýzu malware. IT Systems. CCB, spol. s r. o., 2016, (1 - 2), 26-27. ISSN 1802-615X.

vyvíjený ve spolupráci Evropské agentury pro informační a síťovou bezpečnost (ENISA) a evropských CSIRT.[1] Tento projekt splňuje požadavky na jednoduchost a modularitu, která nám i v budoucích fázích projektu umožní reagovat na případné změny zdrojů informací o incidentech i jejich snadné rozšiřování. Náš tým se také aktivně zapojil do vývoje tohoto software. Funkcí IntelMQ v rámci projektu PROKI je tedy primárně získávání dat týkajících se bezpečnostních incidentů z různých zdrojů. Tyto data jsou následně sjednocena a obohacena o geolokační informace a společně s daty z IntelMQ předávána dalším dvěma článkům.

Notifikace a distribuce

První z těchto článků představuje vlastními silami naprogramovaná aplikace, která se stará o inteligentní distribuci informací o incidentech do zdrojových sítí. Pokud mají být informace o incidentech skutečně řešeny, je potřeba je do koncových sítí rozesílat v rozumném intervalu a zároveň je členit tak, aby si správce dané sítě mohl sám určit prioritu jejich řešení, případně rozhodnout, které má zájem řešit a které nikoliv. Ze zkušenosti z provozu národního bezpečnostního týmu CSIRT.CZ víme, že to, co může menší společnost vyhodnotit jako incident vyžadující řešení, může být pro velkého poskytovatele připojení minoritní záležitost. Záleží také na zasazení incidentu do reálného prostředí. Z pohledu ISP[2] bude mít zcela jistě jinou prioritu podezření na malware na některém z jeho webových serverů a jinou prioritu podezření na malware na stanici koncového zákazníka. Software určený k rozesílání těchto zpráv do koncových sítí získává potřebné kontaktní informace z veřejně dostupného WHOIS[3] rozhraní. Při rozesílání informací o incidentech jsou preferovány kontakty typu abuse.[4]

Archivace a analýza incidentů

Druhým z článků, do kterých systém IntelMQ předává data je analytická část, která je v našem systému reprezentována systémy Elasticsearch a Kibana. Tyto nástroje se starají o ukládání, indexaci a zobrazování získaných informací o incidentech. Tento software bude dále rozvíjen tak, aby byla data automaticky, či na vyžádání analytika obohacována o informace z dalších zdrojů. Kromě zcela veřejných zdrojů, jakými jsou různé IP reputační servery, či služba VirusTotal, se jedná i o data z databáze PassiveDNS, do které máme jako národní bezpečnostní tým umožněn přístup.

Servery poskytující informace o reputaci jednotlivých IP adres mohou být dalším vodítkem, které může doplnit další informace ke konkrétní IP adrese. Zatím nebylo rozhodnuto, zda a které z těchto systémů budou v rámci projektu PROKI využity.

[1] Více informací viz. https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/incident-handling-automation
[2] Zkratka pocházející z anglického Internet Service Providers (poskytovatelé internetových služeb). Pod ISP se rozumí jak poskytovatelé připojení k Internetu, tak poskytovatelé obsahu.
[3] WHOIS představuje označení pro databázi, která slouží k evidenci údajů o majitelích internetových domén a IP adres. Provozovatelem WHOIS s informacemi o držitelích české národní domény .cz sdružení CZ.NIC. Databázi s informacemi o alokaci IP adresních bloků v regionu Evropy pak spravuje organizace RIPE NCC (www.ripe.net).
[4] Podrobněji se problematice věnuje článek „Kde hledat abuse kontakty?" dostupný na https://blog.nic.cz/2016/04/04/kde-hledat-abuse-kontakty/

Služba VirusTotal umožňuje uživatelům nahrávat vzorky podezřelých souborů, které jsou pak podrobeny analýze několika desítkami antivirových řešení. Uživateli je následně zobrazena informace o tom, která antivirová řešení detekovala jím odeslaný vzorek jako malware. Tato služba však také v rámci testování nahraných vzorků analyzuje jejich chování a sleduje jejich síťovou komunikaci. V databázi takto identifikovaných IP adres lze vyhledávat jak prostřednictvím webového rozhraní, tak i prostřednictvím API. Výstupem pak jsou kompletní informace k dané IP, včetně informací o vzorcích malware, které byly na této IP adresy dostupné, nebo s ní naopak komunikovaly. Tyto informace mohou být užitečné například pro identifikaci nového C&C serveru.

Služba PassiveDNS pak přináší do světa incidentů, který je v pojetí PROKI svázán s IP adresami další rozměr v podobě doménových jmen. Tato služba je založena na sondách, které jsou v různých sítích umístěny za DNS servery (kvůli anonymitě uživatelů) a které sledují dotazy odcházející z těchto DNS serverů. Tyto dotazy a odpovědi na ně jsou pak ukládány do databáze, ve které je možné pomocí rozhraní i pomocí API vyhledávat domény, směřující na konkrétní IP adresu, stejně jako informace o IP adrese, na kterou směruje konkrétní doménové jméno. Jakmile je IP adresa nebo jméno serveru označena jako škodlivá, je díky databázi Passive DNS snadné identifikovat názvy dalších domén, které využívají tuto IP adresu, stejně jako dalších zón využívajících tento name sever a tím odhalit další nebezpečné domény či IP adresy.[1] Důležité je, že takto lze získat i historické údaje a díky tomu je možné hledat spojitosti mezi aktuálně probíhajícími incidenty a těmi historickými.

Analytická část projektu tak přinese možnost zjistit historii informací o incidentech spojených s konkrétní IP adresou, možnost pravidelně vyhodnocovat dění spojené s nejproblematičtějšími IP adresami, nalézt sítě, které jsou největším zdrojem incidentů, což v poměru k jejich velikosti může ukazovat i na zaměření dané společnosti minimálně na tolerování problematických aktivit. Tato část projektu nám také umožní sledovat spojitosti mezi incidenty a díky tomu predikovat další možné cíle či zdroje útoků.

Současný stav projektu

Realizace projektu PROKI byla zahájen v září 2015 a v průběhu loňského roku byla realizována především analýza existujících systémů Cyber Threat Intelligence a zkušenost s jejich nasazením u bezpečnostních týmů CERT/CSIRT v zahraničí a analýza dostupných zdrojů využitelných pro potřeby systému.

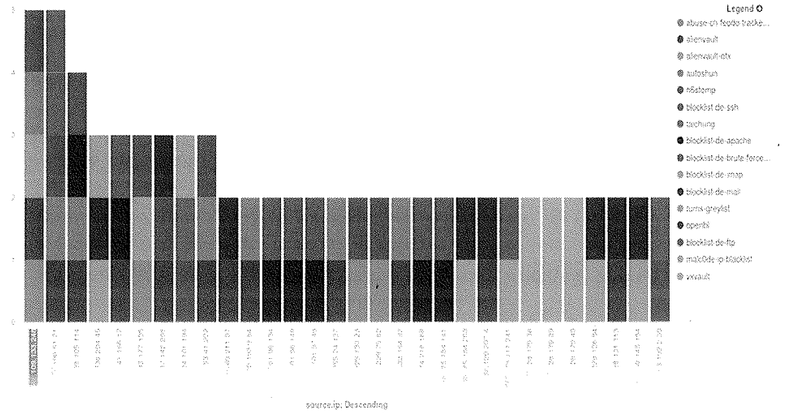
V současné době se projekt nachází v implementační fázi, jejíž nedílnou součást představuje též beta-testování již naimplementovaných funkcionalit. Mezi ně se řadí především rozhraní pro odesílání informací o incidentech, do kterého se zapojilo několik významných ISP a hostingových společností z České republiky. V průběhu letošního roku je plánována analyticky náročná implementace propojení na externí služby.

[1] LIU, Cricket. Strengthen your network security with Passive DNS. *InfoWorld* [online]. 2015. Dostupné z: http://www.infoworld.com/article/2994016/network-security/strengthen-your-network-security-with-passive-dns.html

Přesto, že projekt je teprve na počátku své realizace[1] již nyní se podařilo identifikovat například dva C&C servery umístěné v České republice.

V níže uvedeném náhledu (obrázek č. 1) je jeden z výstupů PROKI, který analytikovi Národního bezpečnostního týmu CSIRT.CZ přehledně v grafické podobě zobrazuje 30 IP adres, které vedou v pomyslném celosvětovém žebříčku IP adres reportovaných z největšího množství zdrojů informujících o kybernetických hrozbách za posledních 10 dnů. Každá barva reprezentuje jeden zdroj informací o podezřelých IP adresách. Úplně nahoře je možné vidět modrou barvou znázorněná data z projektu Turris, respektive IP adresy, vyhodnocené projektem jako podezřelé a z tohoto důvodu zahrnuté do tzv. greylistu. Tato data v podobě podezřelých IP adres se velmi často potkávají s dalšími databázemi zaměřenými na shromažďování informací o problematických IP adresách. Ještě zajímavější je situace, pokud některou z podezřelých IP adres zkusíme vložit do databází jako je PassiveDNS nebo VirusTotal.[2]

Obrázek č. 1: Grafické znázornění nejvíce reportovaných závadných IP adres



Jednotlivé IP adresy na ose X jsou řazeny dle četnosti jejich reportování jako zdrojů ohrožení a zároveň podle množství zdrojů, které je reportovaly. Tyto zdroje jsou reprezentovány jednotlivými barvami.

Zdroj: Výstup z projektu PROKI

V dalším kroku systém umožňuje analytikovi porovnávat IP adresy s informacemi z externích zdrojů. Služba PassiveDNS následně na jednu z takovýchto IP adres vrátí seznam domén, které na tuto IP adresu ukazují.

[1] Celková plánovaná doba realizace projektu je 60 měsíců (5 let).
[2] BAŠTA, Pavel. Vytěžování informací o incidentech a jejich distribuce Aneb co je to PROKI. *Blog zaměstnanců CZ.NIC* [online]. 2016. Dostupné z: http://blog.nic.cz/2016/02/04/vytezovani-informaci-o-incidentech-a-jejich-distribuce-aneb-co-je-to-proki/

Obrázek č. 2: Ukázka výstupu historie konkrétní IP adresy v PassiveDNS

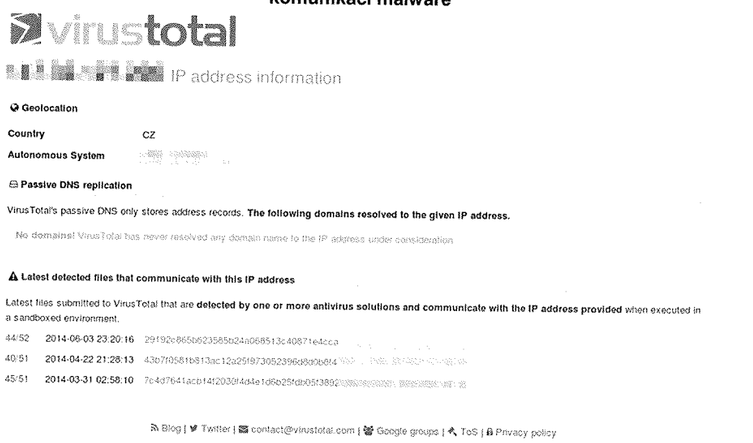
LEFT	RTYPE	RIGHT
aaw5zjuu.info	A	56.64.97
acl4tsgf.info	A	56.64.97
aebmayn.info	A	56.64.97
ahwqxmm.info	A	56.64.97
ajdxzru.info	A	56.64.97
akfbjke.info	A	56.64.97
anpvqug.info	A	56.64.97
antxxit.info	A	56.64.97
aplrcbp.info	A	56.64.97
apm3qjyp.info	A	56.64.97
asbojayg.info	A	56.64.97
ato2voqt.info	A	56.64.97
ayfdzrc.info	A	56.64.97
azo1pinz.info	A	56.64.97
badnnri.info	A	56.64.97
bavwehfm.info	A	56.64.97
bicembyn.info	A	56.64.97
bjewzvj.us	A	56.64.97
bjiwchl.us	A	56.64.97
bndosgs.us	A	56.64.97
bnizxyi.us	A	56.64.97
bnxextd.info	A	56.64.97
boaerbp.info	A	56.64.97
braftam.us	A	56.64.97

V levém sloupci můžeme vidět jednotlivé domény a jejich A záznamy, které všechny ukazují na IP adresu, vyhodnocenou v rámci PROKI jako problematickou. Neobvyklé názvy domén ukazují na možné zneužívání IP adresy, například jako C&C serveru botnetu.

Již samotné názvy domén v tomto případě ukazují na možné zneužití IP adresy, například jako C&C serveru. Analytik tak v rámci své činnosti může dále sledovat historii těchto domén a najít tak další potenciální C&C servery.

Naopak pro jinou IP adresu analytik získá ze služby VirusTotal informace o konkrétních vzorcích malware, který s danou IP adresou komunikoval (obrázek č. 3).

Obrázek č. 3: Ukázka výstupu z VirusTotal zobrazující využití konkrétní IP adresy pro komunikaci malware



V dalším kroku pak získal konkrétní informace ke konkrétnímu malware. Zjistil tak, že malware využívá kromě C&C serveru v České republice také jeden ze Švédska a mohl tak poslat do této sítě konkrétní informaci.

Pokud se nám naopak podaří získat například vzorek malware z napadeného serveru, budeme další analýzou získávat informace o jeho dalším chování. Bude-li však výsledkem takového útoku například instalace malware na napadený server, plánujeme využití nástroje ProcDOT jako jednoho z nástrojů pro rychlou orientaci v chování malware, především pak pro zjištění IP adres, které malware pro svou další komunikaci využívá.[1] Díky tomu budeme schopni rychle detekovat řídící servery botnetů a v roli národního CERT České republiky dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, o nich informovat partnery, kteří proti takovýmto serverům mohou zakročit. Takto získané informace navíc skrz bezpečnostní tým CZ.NIC-CSIRT umožní detekovat rovněž případné napadené počítače uživatelů, kteří jsou zapojeni do výzkumného projektu Turris.

Projekt PROKI představuje unikátní nástroj pro detekci, identifikaci a predikce kybernetických hrozeb a vyhodnocování kybernetických bezpečnostních incidentů (tzv. Cyber Threat Intelligence)., který umožňuje národnímu bezpečnostnímu týmu CSIRT.CZ nebýt odkázán k roli pouhého řešitele reportovaných incidentů, ale umožňuje mu se proaktivně zapojit do boje proti narůstající kybernetické kriminalitě.

[1] BAŠTA, Pavel. ProcDOT a Density Scout: užitečné nástroje pro analýzu malware. IT Systems. CCB, spol. s r. o., 2016, (1 - 2), 26 - 27. ISSN 1802-615X.