Honeypot as a Service

Honeypot as a Service (HaaS) je služba, kterou mohou využít zájemci z celého světa, pokud chtějí sledovat útoky mířící na jejich infrastrukturu; ať se již jedná o domácí router nebo server. Díky řešení, které provozuje Národní bezpečnostní tým CSIRT.CZ, jsou zachycená data (např. malware) využívána pro další analýzu a zlepšení připravenosti na budoucí útoky.

Hlavní myšlenka projektu[1] je spojená s výzkumným projektem Turris, v jehož rámci se zkoumají útoky, jimž čelí běžní uživatelé i firmy. Data o útocích poskytuje tzv. honeypot, který je spuštěný na jednotlivých routerech. Z těch se pak data přenáší do centrály, kde se dále vyhodnocují. Takto získaná data jsou pak dále využívána k upozornění koncových sítí na potenciálně problematické stroje. Získané vzorky malwaru jsou také poskytovány antivirovým společnostem k dalšímu zkoumání.

Právě zkušenosti z projektu Turris vedly k myšlence vytvoření sítě honeypotů, které budou získaná data odesílat na místo, kde budou dále vyhodnocována. Právě v rámci projektu Turris měli uživatelé poprvé možnost zapojit se do společného sběru dat o útocích, které byly dále vyhodnocovány a opět využívány k lepšímu zabezpečení těchto routerů.

V rámci projektu HaaS dochází k vytvoření proxy, která příchozí útoky přesměruje na naše honeypoty, čímž nám umožní jejich snadnější úpravy. Toto řešení má dvě zásadní výhody. Z pohledu útočníků je těžké predikovat, kde by mohli na honeypot narazit a vyhnout se detekci svých pokusů o útoky. S narůstajícím počtem zapojených uživatelů tak bude stále těžší se detekci vyhnout. Řada především domácích uživatelů má dynamicky přidělovanou veřejnou IP adresu, díky čemuž se bude z pohledu útočníků honeypot „stěhovat“ a oni se nebudou moci spolehnout na své seznamy IP adres a rozsahů, kterým se mají jejich nástroje při útocích vyhnout. Druhou výhodu představuje pokrytí mnoha různých sítí a typů koncových uživatelů. Díky tomu bude možné určit, zda se v konkrétním případě jedná o plošný útok, nebo zda se útočník specializuje na určité rozsahy IP adres, např. na IP adresy patřící státní správě, pokud ta se do projektu také aktivně zapojí.

Technické řešení HaaS se skládá ze tří částí. Nejdůležitější je honeypot Cowrie[2] dříve známý jako Kippo, který je provozovaný na dedikovaném serveru. Další důležitou součástí je HaaS Proxy, která běží na straně uživatele. V prvé řadě přesměrovává příchozí útok na honeypot Cowrie a navíc přidává i další informace, např. zdrojovou IP adresu útoku a použité heslo. Poslední částí celého řešení je web[3], kde si uživatel může zobrazit průběh útoků, ale i celkovou statistiku ze všech zařízení zapojených do projektu.

Tímto způsobem uživateli odpadají starosti s provozem vlastního honeypotu. Nemusí se starat o jeho aktualizace a díky proxy, která útok přesměruje, se veškerý škodlivý kód provádí mimo jeho infrastrukturu. Nehrozí, že by útočník využil neznámé zranitelnosti a získal plný přístup k napadenému zařízení, pomocí kterého by mohl provádět další útoky v napadené síti. Dále má uživatel k dispozici přehledné rozhraní pro zobrazení jednotlivých příkazů, k jejichž spuštění mělo dojít. K dispozici má také

[1] Projekt „Honeypot jako služba (HaaS)“ (TF02000057) byly podpořen Technologickou agenturou ČR (TAČR) v rámci 2. výzvy programu Delta.
[2] https://github.com/micheloosterhof/cowrie
[3] https://haas.nic.cz

mapy. Na hlavní stránce je mapa zobrazující státy, ze kterých přicházejí útoky nejčastěji. Pro každé připojené zařízení je navíc k dispozici mapa s útoky mířícími pouze na něj. Na stránkách lze rovněž najít jak celkovou statistiku útoků, tak i detailní data obsahující příkazy ze všech zachycených útoků.

Do projektu se může zaregistrovat kdokoli a služba je poskytována zdarma. Registrace i návody na zprovoznění služby jsou k dispozici na stránkách projektu. V současné době je do projektu zapojeno kolem dvou tisíc zařízení, z nichž denně zaznamenáváme stovky tisíc útoků.

Analýza získaných dat

Útočníci či jejich automatizovaní boti se často pokoušejí na svůj cíl nahrát různé soubory. Typicky to bývá malware (trojan) sloužící ke vzdálenému ovládání napadeného počítače, avšak není to vždy pravidlem. Např. v březnu bylo v HaaS zachyceno celkem 2 240 unikátních souborů o celkové velikosti 4,3 GB dat. Konkrétnější rozdělení souborů je vidět v tabulce 1.

Co se týče cílových architektur, zachycené binární soubory byly velmi rozmanité – od ARM přes MIPS až po x86 včetně nejrůznějších pod-variant. Dva největší soubory měly stejný začátek jako instalační media Debian 9.3 a Linux Mint 18.3, což se dá nejpravděpodobněji vysvětlit snahou útočníků ověřit, kolik si můžou na nově získaný stroj uložit dat. Dalším zajímavým nálezem byl 17 MB textový soubor obsahující přes milion domén, ze kterých se 945 nacházelo v doméně .CZ. Vzhledem k faktu, že se mezi českými doménami nápadně často vyskytovaly domény státní správy, byl tento soubor předán k další analýze Národnímu úřadu pro kybernetickou bezpečnost (NÚKIB).

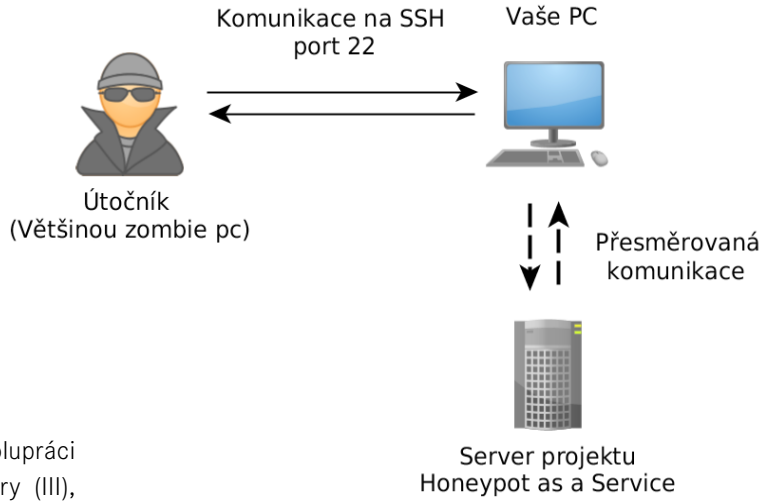
[4] https://fe.nix.cz/
[5] https://ssdeep-project.github.io/ssdeep/index.html
[6] https://www.virustotal.com/

Typ souboru	#
Binární spustitelné soubory	**1 540**
Bourne-Again shell script	358
ASCII text	238
Ostatní	52
Perl script text executable	26
Data	16
HTML dokument	10

Tab. 1: Rozdělení souborů

Další analýza vybraných vzorků probíhala ve spolupráci s tchaj-wanským Institute for Information Industry (III), kterému byly poskytnuty vzorky zachycených souborů. Na základě námi provedené dynamické analýzy pak byly odhaleny snahy o komunikaci s Command and Control serverem, tj. řídícím počítačem pro botnet. Komunikace vypadala typicky tak, že po úvodní inicializaci docházelo pouze k pravidelnému udržování spojení (keep-alive). Další zachycené vzorky se snažily připojit do tzv. těžebního poolu, kde bylo jejich úkolem těžit virtuální měnu. U jiných vzorků byla zaznamenána snaha o DDoS útok, která se později projevila jako snaha o detekci schopnosti napadeného počítače podvrhnout zdrojové IP adresy. Tomu je možné v dnešní době zabránit implementací mezinárodního doporučení BCP 38[1]. Avšak dodržování tohoto opatření není vždy jednoduché a závisí primárně na rozhodnutí společnosti či poskytovatele připojení k Internetu. Doporučení BCP 38 je aplikováno také v rámci bezpečnostního projektu FENIX[4], kde je přímo vyžadováno od členů do projektu zapojených.

Cílem projektu FENIX je dostupnost internetových služeb v případě masivních DDoS útoků mířící na českou infrastrukturu.



Na rozdíl od DDoS útoku se výše zmíněný malware pokusil poslat pouze několik paketů s odlišnou zdrojovou IP adresu na adresu svého C&C serveru. Pokud by se ukázalo, že je toho čerstvě získaný počítač schopný, byl by s největší pravděpodobností zneužit právě k DDoS útokům. Ty dnes patří k velmi častému typu útoků, jejichž cílem je vyčerpání prostředků cíle, který nemá šanci poznat, zda se jedná o legitimní požadavek uživatele zobrazujícího obsah webových stránek, nebo uměle vygenerovaný provoz.

Během analýzy byl využit rovněž nástroj SSDeep[5], který se ukázal jako vynikající řešení pro shlukování příbuzných vzorků malwaru. Z celkem 410 vzorků identifikoval 14 skupin obsahujících příbuzné vzorky. Z celé sady nebylo možné nikam přiřadit pouze 27 vzorků. Ověření některých skupin bylo provedeno porovnáním zachycené komunikace s C&C serverem. Např. v komunikaci trojského koně označovaného na Virustotal[6] jako „ELF:Elknot-AE [Trj]“ se vyskytoval řetězec „-== Love AV ==-“.

Služba Virustotal umožňuje otestování nahraných vzorků antivirovými programy a následně zobrazuje výsledky, kolika antiviry je daný vzorek detekován. U hlavních hráčů se míra detekce vzorků nelišila. Infekce byla navíc potvrzena i u vzorků, které byly na Virustotal nahrané poprvé. Nutno dodat, že zmíněné vzorky byly příbuzné s těmi, které byly na Virustotal nahrány dříve. Virustotal totiž získané vzorky sdílí s antivirovými společnostmi, což zpřesňuje možnosti detekce.

V rámci analýzy získaných dat byly nalezeny spojitosti mezi různými skupinami vzorků. Mezi rodinami označovanými jako „ELF:Aesddos-H [Trj]“ a „ELF:Elknot-AE [Trj]“ byly nalezeny vzorky, které se připojovaly na stejnou IP adresu 118.184.32.55. Díky systému passive DNS bylo navíc objeveno, že zatímco „ELF:Elknot-AE [Trj]“ často využíval poddomény *.f3322.net; jedna z takových poddomén v minulosti odkazovala na IP adresu 222.186.34.102, kam se právě připojovaly některé vzorky ELF:Aesddos-H [Trj].

Systém Passive DNS je v podobných analýzách neocenitelným nástrojem. Uchovává totiž historické záznamy překladů doménových jmen a IP adres, čímž umožňuje právě takové spojení jako v odstavci výše. Záznamy doménových jmen se totiž mohou měnit. Při pozdější analýze by již bez systému Passive DNS nebylo možné zjistit, kam v minulosti či konkrétním čase ukazoval. Např. zadáním hledané domény lze získat všechny IP adresy, na které doména v historii odkazovala, včetně časového období, kdy tomu tak bylo. Pokud se ukáže, že v minulosti doména odkazovala pouze na dvě IP adresy, přičemž jedna je shodná s IP adresou v odděleném případu, naznačuje to možnou souvislost, která by jinak byla přehlédnuta.

Takto získané adresy C&C serverů jsou dále využity např. v projektu Turris, kde slouží k zlepšování ochrany uživatelů.

Testovací prostředí

Pro tuto analýzu byl ve zkušebním provozu využit specificky připravený systém postavený na Raspberry Pi, aby případný malware při snaze detekovat, zda neběží ve virtualizovaném prostředí, byl přesvědčen, že běží na legitimním fyzickém stroji.

V dnešní době, kdy mezi často napadaná zařízení patří routery, IP kamery a obecně zařízení nejrůznějších procesových architektur, již nevadí, že vybraná platforma běží na architektuře ARM. Na rozdíl od běžného fyzického počítače to umožnilo omezit případnou persistenci malwaru pouze na paměťovou kartu, která byla navíc uzamčena pro zápis. Veškeré operace byly tedy prováděny pouze v operační paměti, díky čemuž stačil pro vyčištění celého zařízení pouhý restart.

K podpoře dalších architektur byla přidána podpora QEMU (Quick EMUlator). Nevýhodu tohoto řešení představuje případná detekce emulace procesoru malwarem. Pokud tedy byl malware kompilován pro jinou architekturu a nebránil se spuštění v emulovaném prostředí, bylo jej možné analyzovat i tak.

Z celého provozu byla sledována a zaznamenávána síťová komunikace. Sledování provozu při běhu bylo nutné pro včasné zastavení případných útoků na cizí infrastrukturu. Následnou analýzou získané komunikace bylo možné získat jak IP adresy C&C serverů, tak i některé specifické charakteristiky komunikace (viz DDoS výše).

Testovací prostředí bylo pravidelně kontrolováno, zejména pro ověření, zda nedošlo k trvalé změně – především na SD kartě. Žádná změna však nebyla nalezena.

Následnou automatizací celého procesu se rovněž podařilo zkrátit prostoje mezi jednotlivými vzorky a minimalizovat manuální práci. Nicméně při připojení zařízení do Internetu není možné nechat běžící malware bez dozoru.

Závěr

A jaké jsou další plány? Určitě chceme zkusit zopakovat podobnou analýzu na jiné architektuře. Nabízí se i možnost přidání jiných honeypotů. Rovněž by stálo za pokus udělat ve stávajícím honeypotu takové úpravy, které by případné útočníky lépe přesvědčily, že se se jedná o skutečný stroj. Zvážit by šla i integrace poloautomatických analýz rovnou do projektu Turris, kde by nalezené IP adresy C&C serverů byly automaticky blokovány na firewallu a/nebo reportovány správci sítě. Bylo by však zapotřebí zamezit případnému podvrhnutí IP adresy specificky upraveným spustitelným souborem tak, aby došlo např. k zablokování přístupu na legitimní server.

Martin Kunc
martin.kunc@nic.cz

Martin Kunc

Vystudoval Aplikovanou Informatiku na Jihočeské univerzitě. Před nástupem do CZ.NIC se podílel na vývoji kryptografického hardware. Nyní se jako bezpečnostní analytik věnuje především síťovým hrozbám.

POUŽITÉ ZDROJE

[1] Ferguson, P., Senie, D. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. The Internet Society, 2000, RFC 2827. Dostupné na https://tools.ietf.org/html/bcp38.