T A
Č R

Praha 27. 11. 2017

Nový projekt podpořený TAČR zapojuje veřejnost do boje proti kyberzločinu

- **Přilákat, sledovat a analyzovat činnost hackera – to je cíl nového projektu českých odborníků z oblasti IT. Vytvořili komplexní řešení, včetně aplikace, které zapojuje do boje proti kyberútokům veřejnost a stává se tak účinnější.**
- **Výstupem projektu je webová služba Honeypot as a Service (HaaS), vyvinutá odborníky ze zájmového sdružení CZ.NIC, a poloprovoz veřejného honeypotu, na který bude možné přesměrovat útoky z koncových zařízení. Obě části se spustí nejpozději v květnu příštího roku.**
- **Unikátní inovaci v boji proti kyberzločincům podpořila Technologická agentura ČR (TA ČR) částkou 1,3 milionu korun z programu DELTA.**

Přilákat, zmást a odhalit hackera – to je cíl

Zapojit veřejnost do boje proti kyberútokům je cílem projektu, na kterém nyní intenzivně pracuje webová služba Honeypot v týmu s odborníky ze zájmového sdružení CZ.NIC. Nejpozději do května příštího roku hodlají spustit nejprve poloprovoz veřejného honeypotu, na který bude možné přesměrovat útoky z koncových zařízení, například domácích routerů, a tím zvýšit bezpečnost obyvatel.

„Drtivá většina zkoumání nových typů útoků pomocí honeypotů se zaměřuje na vytvoření honeypotu, který je však pasivní a není schopen obsluhovat větší množství klientů. Sofistikovaní útočníci však mezi sebou sdílejí informace o známých honeypotech a dovedou se jim pak vyhnout. Projekt HaaS zahrnuje vytvoření sítě minimálně pěti set koncových uživatelů a techniky pro přesměrování těchto uživatelů na centrální honeypot. Cílem našeho výzkumu je pak zajistit, aby byl útočník co nejdéle přesvědčen, že útočí na skutečný cíl, tedy na počítač, server nebo router, nikoliv honeypot,“ vysvětlil práci na inovaci Ladislav Lhotka ze sdružení CZ.NIC, které zajišťuje provoz obou částí projektu. Předkládané řešení je podle něj unikátní především v přesměrování útoků vedených na reálné systémy do honeypotu, a dále zaměřením na koncové uživatele. Jak dokládají zkušenosti z jiných projektů, některé útoky, například ransomware SynoLocker, míří právě na koncové uživatele.

Počty kyberútoků enormně narůstají

Na aplikovaný výzkum v oblasti kybernetické bezpečnosti přispěla dotací ve výši 1,3 milionu korun z programu DELTA Technologická agentura ČR. „Analýza chování útočníků z podpořeného projektu bude následně využita pro inovaci mechanismů pro SSH honeypoty, práci českého národního bezpečnostního týmu CERT a zlepšení připravenosti České republiky na kybernetické útoky. Státní podpora takových projektů má proto velký smysl,“ prohlásil předseda TA ČR Petr Očko. Program DELTA slouží k podpoře výzkumné spolupráce s inovačně vyspělými zeměmi – v tomto případě s Tchaj-wanem „Tento program výrazně zvyšuje uplatnitelnost výsledků projektů na globálních trzích,“ upozornil Petr Očko s tím, že další výzvu v něm chystá TA ČR na podporu spolupráce s klíčovými zeměmi na květen příštího roku.

Podrobnosti k technickému řešení

Honeypot (anglicky „hrnec medu“ – pozn. red.) je informační systém, jehož účelem je přitahovat potenciální kybernetické útočníky, zaznamenat jejich činnost a odhalit bezpečnostní zranitelnost systémů. Užívají se především pro včasné detekování malwaru. „Malwary stále mění svoji strategii útoku a různými způsoby se skrývají a vyhýbají nalezení. Z těchto důvodů je nutno malware nějak nalákat a poté analyzovat jeho chování. Takto získané informace se mohou použít pro aktualizování antivirových systémů. Výhoda našeho řešení spočívá v tom, že reálný napadeného systému nemusí být nijak zvlášť připraven ani zabezpečen, pouze se na něm instaluje celkem jednoduchá aplikace, která přesměruje provoz na náš centralizovaný honeypot. Takovýto přístup podle našich dosavadních zkušeností plně vyhovuje pro boj s nejběžnějšími typy malwaru,“ vysvětluje základy projektu Ladislav Lhotka.

Honeypoty detekují činnost neoprávněných zdrojů přicházejících do systému a automaticky sbírají data o činnosti potenciálního útočníka. Detekce buď vyloučí, že se jednalo o agresora, nebo to jen potvrdí. Je to rychlejší a bezpečnější, než kdyby se sbírala data z funkčního napadeného systému. Nárůst útoků v posledních letech lze ilustrovat na honeypotech sdružení CZ.NIC, které v roce 2014 zaznamenaly 11,6 mil. spojení, tj. o 84% více než v roce 2013.

Technologická agentura České republiky
Evropská 1692/37, 160 00 Praha 6
+420 234 611 111
info@tacr.cz, www.tacr.cz

Vzhledem k tomu, že projekt počítá s přesměrováním skutečných útoků ze sítí různých poskytovatelů, vyhnutí se tomuto honeypotu bude nesrovnatelně obtížnější. Na rozdíl od jiných známých projektů se tento zaměřuje primárně na koncové uživatele, kteří zatím zůstávali v pozadí zájmu.

Podle odborných odhadů bezpečnostní divize McAffee kybernetický zločin v zemích EU způsobuje ztrátu ve výši 0,41% HDP ročně. *„V případě České republiky se tak jedná o přibližně 18 až 19 miliard korun ročně. Jedny z největších ztrát jsou způsobeny právě útokem využívajícím slabá místa zabezpečení jednotlivých systémů,“* poznamenal Petr Očko.

Technické řešení projektu Honeypot podpořeného TA ČR je následující: První krok pro úspěšné fungování poloprovozu představuje vytvoření dvou logicky i provozně oddělených aplikací (softwaru). První z těchto webových aplikací bude zajišťovat registraci uživatelů pro přesměrování na veřejný honeypot a druhá pak vytváření vlastních honeypotů v rámci centrálního veřejného honeypotu. V rámci projektu byla také vytvořena aplikace haas-mitmproxy, kterázajišťuje přesměrování útočníka (komunikace) z koncového zařízení uživatele na centrální honeypot.

Zdrojový kód aplikace haas-mitmproxy je dostupný pod licencí GPLv3 na projektovém serveru sdružení CZ.NIC (https://gitlab.labs.nic.cz/haas/proxy), a dále bude uživatelům dostupná v podobě balíčků pro běžné operační systémy (Linux, OS X, Windows). Webové rozhraní je dostupné na adrese https://haas.nic.cz a slouží k registraci uživatelů, získání informací o „svém“ honeypotu a nastavení svého koncového počítače či routeru. V rámci webového rozhraní si uživatel může též stáhnout aplikaci haas-mitmproxy a návod na její instalaci a konfiguraci.

Kontakt: **Ing. Ivana Drábková,** tisková mluvčí TA ČR
Tel: + 420 777 016 525, E-mail: drabkova@tacr.cz

T A

Č R

Technologická agentura České republiky

Evropská 1692/37, 160 00 Praha 6
+420 234 611 111
info@tacr.cz, www.tacr.cz