ProcDOT a Density Scout

Užitečné nástroje pro analýzu malware

Pavel Bašta

Začátkem října proběhlo v rámci mezinárodního projektu „Cyber Security in Danube Region“ podpořeného Evropskou unií školení bezpečnostních týmů fungujících v rámci podunajského regionu. Protože sdílení informací a poznatků je v oblasti bezpečnosti zcela klíčové, rozhodl jsem se sepsat příspěvek, kterým bych chtěl bezpečnostní komunitu v České republice upozornit na dva velice zajímavé, bezplatné nástroje, které byly v rámci uvedeného školení prezentovány. V rámci školení zaměřeného na analýzu malware prezentoval kolega Christian Wojner z Rakouského bezpečnostního týmu CERT.at jeho vlastní nástroje ProcDOT a DensityScout.

ProcDOT

ProcDOT je nástroj, který je velmi užitečný při takzvané behaviorální analýze. Pravděpodobně každý, kdo někdy analyzoval nějaký malware pro operační systémy z dílny Microsoftu nebo pracoval jako správce těchto systémů, se již setkal s nástroji z rodiny Sysinternals. O operačních systémech Windows umí tyto nástroje prozradit spoustu věcí, od podrobností o běžících procesech, přes informace o síťové komunikaci či změnách v registru, až po informace o všech procesech automaticky spouštěných se startem systému. Právě výstup z jednoho z těchto nástrojů, konkrétně z programu Process Monitor, využívá nástroj ProcDOT. Dalším vstupem jsou pak PCAP soubory z programů jako jsou WinDump či Wireshark.

Process Monitor umožňuje sledovat aktivitu týkající se registrů, souborového systému, procesů, knihoven a síťové aktivity. Wireshark a WinDump pak dokáží zachytávat kompletní síťový provoz. ProcDOT následně dokáže na základě souboru s informacemi zachycenými nástrojem Process Monitor a na základě PCAP souborů se síťovým provozem vykreslit velmi přehledný graf znázorňující chování a komunikaci určitého programu.

Pokud si budete chtít program ProcDOT vyzkoušet, budete potřebovat kromě samotného programu také některé další komponenty. ProcDOT je možné používat jak ve Windows, tak v Linuxových operačních systémech. Pokud však budete testovat malware pro Windows, stejně budete potřebovat aspoň jednu licenci Windows, aby jste mohli pomocí nástrojů Process Monitor, Wireshark či WinDump získat informace, které si následně necháte v ProcDOTu přehledně znázornit. Důležité je, že výstupy z programu Process Monitor je potřeba ukládat ve formátu CSV.

Na stroji, kde budete používat samotný program ProcDOT je potřeba nainstalovat ještě komponenty tcpdump a Graphviz. Po spuštění programu pak budete vyzváni k zadání cesty k těmto komponentám.

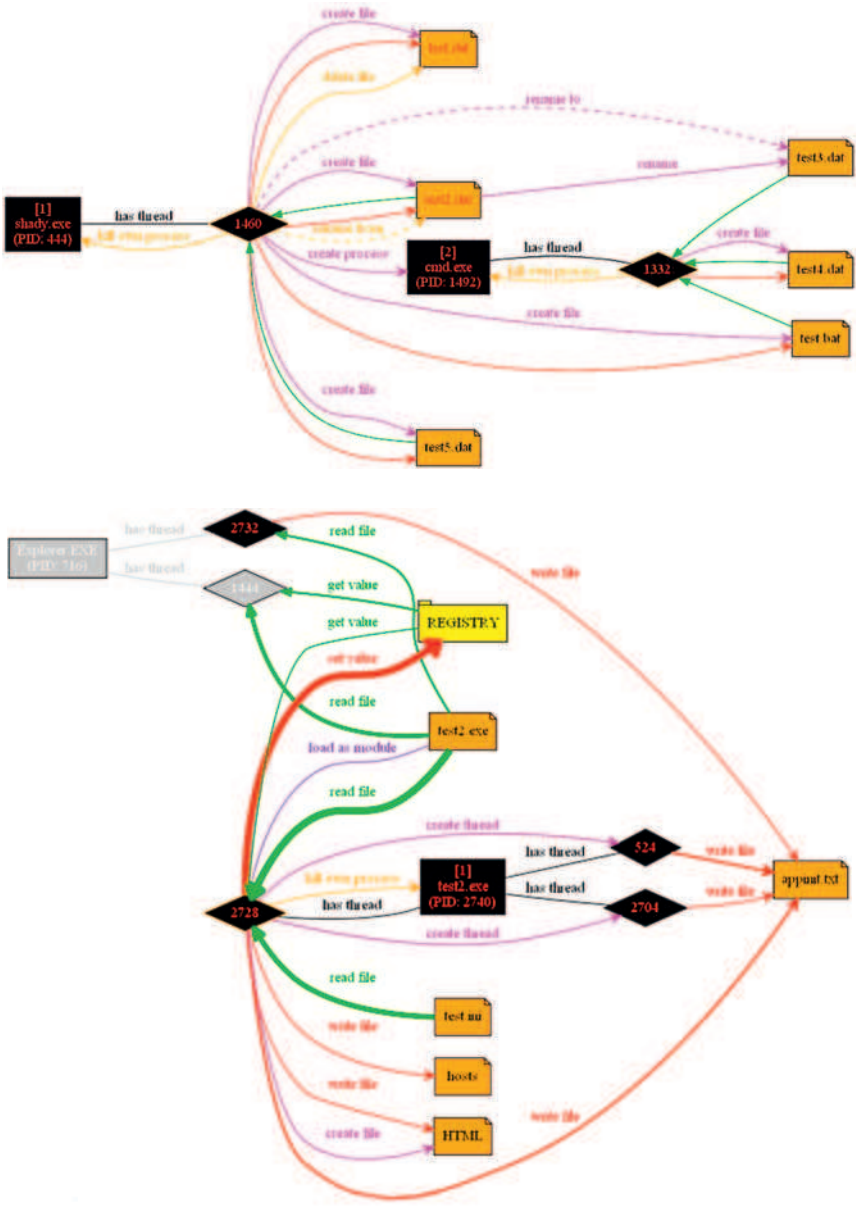
Okno programu nemusí na první pohled působit úplně přehledným dojmem, nicméně na ovládání programu si rychle zvyknete. V položkách Procmon-CSV a Windump-File zadáme programu cestu k informacím získaným při spuštění malware. Důležitá je položka Launcher, která nám umožňuje vybrat proces, od kterého se má začít vykreslovat graf. Pokud jsme tedy testovali webové stránky, které přes nějakou zranitelnost prohlížeče instalují na systém malware, pak zvolíme jako výchozí proces prohlížeč. Pokud jsme testovali vlastní binárku malware, pak jako výchozí proces zvolíme tuto binárku.

Položky no paths, compressed a dumb pak definují zda se budou cesty k souborům a klíčům registru vypisovat celé, zda se informace o přístupech do registru zkomprimují na informace typu klíče umožňující automatický start a ostatní. Třetí z voleb říká, zda se uplatní speciální smart following algoritmy, které by měly znázornit pouze relevantní události. Kliknutím na tlačítko refresh pak spustíme generování samotného grafu (viz. Obr. 1).

ProcDOT nám 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. V grafu lze také vyhledávat textové řetězce, což opět může pomoci nalézt například komunikaci s konkrétní doménou. To vše dělá z ProcDOTu velmi silný nástroj pro behaviorální analýzu malware.

Density Scout

Druhý z nástrojů, Density Scout, může být užitečným pomocníkem v případě, že před sebou máte počítač s podezřením na napadení malware, u kterého klasické metody detekce selhávají. Tento nástroj skenuje všechny soubory v nastaveném adresáři a počítá pro tyto soubory jejich entropii. Těží přitom z typického chování autorů malware, kteří své



Obr. 1: Ukázka grafu vytvořeného v ProcDOT, který znázorňuje chování a komunikaci určitého programu.

produkty různými způsoby maskují. Použití nástrojů pro obfuskaci kódu však zvyšuje entropii vzniklých souborů. Na druhou stranu, většina běžných spustitelných souborů pro Windows tyto metody nepoužívá. Proto bude potenciální malware vynikat svou entropií oproti běžným souborům. Není to stoprocentní metoda, ale v případě hledání možné infekce na počítači nám může pomoci vytipovat vhodné adepty pro další analýzu. Všechny informace o tomto programu, včetně možnosti jeho stažení, najdete na adrese http://www.procdot.com. Důležité také je, že program je zcela zdarma.

Obr. 2: Ukázka výsledku analýzy provedené pomocí nástroje Density scout.

```
C:\density_scout>densityscout.exe -pe -p 1 -o results.txt C:\WINDOWS

DensityScout (Build 43)

by Christian Wojner

Calculating density for file ...
(0.78650) | C:\WINDOWS\explorer.exe
(0.99505) | C:\WINDOWS\notepad.exe
(0.55320) | C:\WINDOWS\setup.exe
(0.98315) | C:\WINDOWS\twain.dll
(Density) | Filename
-------------------------------------------------------------

C:\density_scout>
```

Na obrázku 2 můžeme vidět výsledek analýzy provedené pomocí nástroje Density scout. Parametr -pe určuje, že se budou kontrolovat pouze PE soubory, navíc identifikované na základě magic numbers. Díky tomu budou detekovány i spustitelné soubory i s jinými příponami, než jaké mají běžně spustitelné soubory. Parametr -p 1 říká programu, aby nám zobrazil pouze soubory, které budou mít „hustotu“ nižší než dané číslo. Parametr -o pak ukládá kompletní výsledky také do souboru results.txt. Posledním parametrem je pak cesta k adresáři, který chceme testovat.

Na výstupu z našeho testování můžeme vidět, že nejnižší „hustotu“ mají soubory exploror.exe, notepad.exe, setup.exe a twain.dll. Soubor setup.exe je přitom skutečně soubor, který obsahuje bankovního trojského koně a který byl již více než před rokem servírován uživatelům jako údajný update Flash Playeru na falešných stránkách Seznam.cz a Google.com. Program DensityScout je také zdarma a můžete si jej stáhnout na stránkách rakouského národního bezpečnostního týmu https://cert.at.

Využití v praxi – projekty PROKI a Turris

Doufám, že vám představené nástroje pomohou v běžné praxi. My je v našem týmu plánujeme využít při analýzách útoků identifikovaných v projektu PROKI (Predikce a Ochrana před Kybernetickými Incidenty) realizovaného v rámci bezpečnostního výzkumu v České republice. V něm se chceme zaměřit především na sledování síťových útoků.

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. Díky tomu budeme schopni rychle detekovat řídící servery botnetů a v roli národního CSIRT České republiky o nich informovat partnery, kteří proti takovýmto serverům mohou zakročit. Takto získané informace navíc skrz bezpečnostní tým CZ.NIC-CSIRT umožní detekovat také případné napadené počítače uživatelů, kteří jsou zapojeni do výzkumného projektu Turris. ■

Pavel Bašta

Autor článku je bezpečnostní analytik sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ