Avast – Metody pro extrakci a detekci vzorů v programovém kódu

Stav řešení projektu v roce 2019

Úvod

Rok 2019 byl třetím rokem řešení projektu společnosti Avast Software. V tomto roce bylo navázáno na předchozí výsledky v oblasti získávání tzv. *threat intelligence* z honeypotů. Řešení bylo rozšiřováno společně s výzkumem v dalších oblastech získávání informací o útočnících v kyberprostoru s využitím technologie klamu.

Průběh řešení v roce 2019

V této kapitole jsou shrnuty oblasti, kterým byla v rámci tohoto projektu věnována pozornost. V první polovině roku probíhala práce převážně na vylepšování e-mailového honeypotu ve formě lepší vizualizace získaných znalostí a schopnosti rychlé reakce na detekované anomálie. Dále probíhaly experimenty s open-source honeypoty jako jsou Dionaea[1] a Heralding[2]. V neposlední řadě proběhla také analýza malware aliasů poskytnutých společností Abuse.ch[3] a porovnání s aliasy společnosti Avast Software.

Pokročilá vizualizace

V minulém roce byl zprovozněn dashboard založený na platformě Grafana, který je používán pro monitoring hrozeb zachycených v e-mailovém honeypotu. Ukázalo se však, že je výhodné mít možnost odkazovat se na další systémy společnosti Avast Software a analyzovat chycené vzorky detailněji. Toto platforma Grafana neumožňuje.

Z toho důvodu byla navržena a implementována samostatná threat intelligence platforma, která ve vhodné podobě zobrazuje chycené hrozby ve formě e-mailových kampaní, jejich příloh

[1] https://github.com/DinoTools/dionaea
[2] https://github.com/johnnykv/heralding
[3] https://abuse.ch/

a URL odkazů. Těmto hrozbám jsou s využitím dalších systémů společnosti Avast Software přiřazeny tzv. tagy, které označují o jakou rodinu malware se jedná. Umožňuje také rychlé procházení dalších informací o daném vzorku, jako jsou například výsledky z dynamické analýzy vzorku, apod.

Sledování hrozeb v reálném čase

Abychom dále snížili čas, který musí malware analytici pro zjištění nových znalostí věnovat novému systému, navrhli a implementovali jsme systém zasílání upozornění. S využitím již zmíněného systému pro přidělování tagů a systému dynamické analýzy jsou všechny příchozí vzorky automaticky označovány. Pokud dojde k situaci, že některý z příchozích vzorků není systémy rozpoznán, jsou malware analytici varováni o neznámé hrozbě v řádu několika desítek minut po začátku škodlivé e-mailové kampaně. Výsledkem těchto upozornění je tedy rychlá reakce při počátku šíření neznámé hrozby.

Experimenty s dalšími honeypoty

Po úspěšném nasazení e-mailového honeypotu a všech jeho součástí byly provedeny experimenty a nasazení několika dalších honeypotů. Mezi ty, které jsme se rozhodli využívat i nadále, byly také nástroje Dionaea a Heralding.

Dionaea je nízko-interaktivní honeypot využívající knihovnu libemu pro zachytávání zranitelností a exploitů ve velké škále a to různých služeb. Mezi nejvíce zneužívané patří zranitelnosti ve službě Samba, což je implementace protokolu SMB[4] pro služby přenosu souborů na systémech Windows. Tyto zranitelnosti jsou aktuálně využívány hlavně pro šíření červu WannaCry[5] a různých cryptominerů[6]. Denně jsou naše systémy schopny zachytit několik stovek unikátních vzorků malware a tisíce pokusů o útok, a to na každé samostatné instanci tohoto honeypotu.

Druhým nástrojem honeypot, který využíváme i nadále, je honeypot Heralding. Jedná se o nízko-interaktivní honeypot, který je schopen zachytávat přihlašovací údaje do různých služeb. Získané údaje pak bude možné využít ke zlepšení znalostí o slabých heslech a k varování uživatelů o této skutečnosti a možném nebezpečí.

Experimenty s Canarytokens

Další oblastí, které jsme se v rámci projektu věnovali, byly tzv. honey tokens. V jistém slova smyslu se jedná také o honeypoty, které však mají pouze virtuální formu, jakou jsou například soubory. Naše řešení bylo inspirováno open-source projektem Canarytokens[7], což jsou honey tokeny, které zašlou upozornění při svém otevření.

[4] https://docs.microsoft.com/cs-cz/windows/win32/fileio/microsoft-smb-protocol-and-cifs-protocol-overview
[5] https://www.avast.com/c-wannacry
[6] https://blog.avast.com/topic/cryptomining
[7] https://canarytokens.org/

Po vzoru Canarytokens jsme vyvinuly vlastní systém, který zpracovává zprávy zasílané z otevíraných souborů. Následně jsme provedli úpravu systémů společnosti Avast Software, která nám umožnila distribuovat tyto soubory mezi autory malware. V aktuální době probíhá testovací běh tohoto systému, jehož cílem je sběr informací o těchto entitách a korelace s dalšími systémy společnosti Avast Software.

Analýza malware aliasů

Poněkud odlišnou oblastí, jíž jsme se v rámci tohoto projektu zabývali, bylo vyvinutí skriptů pro automatické porovnání aliasu vzorků malware mezi společnosti Abuse.ch a Avast Software. V budoucnu je však bude možné využít pro porovnání libovolného seznamu dvojic aliasů. Implementované nástroje jsou schopny automaticky porovnat dvojice označení zmíněných vzorků a produkovat report, který může sloužit několika účelům.

1. Zjištění, které vzorky malware nejsou společností Avast Software detekovány.
2. Zjištění, které rodiny malware nejsou společností Avast Software identifikovány.
3. Zjištění, které názvy rodin malware jsou synonymy.

Výstupy řešení

V tomto roce došlo k ostrému nasazení našeho e-mailového honeypotu a jeho obohacení o pokročilou vizualizaci výsledků, napojení na systémy společnosti Avast Software a přidání systému pro upozornění uživatelů o neznámé hrozbě v reálném čase.

Dále došlo k nasazení honeypotů Dionaea a Herlading, jejichž výsledky jsou rovněž v reálném čase zasílány dalším systémům společnosti. Podobně jako vzorky z e-mailového honeypotu jsou také vzorky z nástroje Dionaea napojeny k systému automatických upozornění.

Posledním výstupem byla sada nástrojů pro porovnávání aliasů malware a generování reportu. Ten umožňuje vyhodnocení detekčních schopností společnosti, společně s nalezením synonym aliasů malware rodin.

Plány na další období

V dalším roce budeme pokračovat v práci s honeypoty pro získávání *threat intelligence*. Především se chceme zaměřit na využití honey tokens pro oklamání útočníků a získávání informací o těchto entitách. Kromě analýzy výsledků z aktuálního nasazení inspirovaného systémem Canarytokens chceme provést další experimenty, jejichž podoba bude formována v následujícím roce.