



# Avast – Metody pro extrakci a detekci vzorů v programovém kódu

Stav řešení projektu v roce 2020

## Úvod

Rok 2020 značil čtvrtý rok úspěšného řešení projektu společnosti Avast Software. Stejně jako v předchozích letech byl v projektu kladen důraz na získávání tzv. *threat intelligence* a to převážně s využitím technologií pro oklamání útočníka v kyberprostoru.

## Průběh řešení v roce 2020

V této kapitole budou shrnuty oblasti, kterým jsme se v rámci tohoto projektu věnovali v roce 2020. Naše práce získávání informací o aktuálních hrozbách byla významně ovlivněna světovými trendy a nejrozšířenějšími kybernetickými hrozbami.

### Rozšiřování viditelnosti v doméně vzdáleného přístupu

S příchodem pandemie koronaviru byla část populace nucena přejít k práci z domova. Se zvyšující se potřebou využívat vzdáleného přístupu rostl také počet útoků na tuto službu[1]. Cílem naší práce byla příprava vysoce interaktivního honeypotu pro sledování hrozeb protokolu vzdáleného přístupu (RDP). S tím vznikla také platforma pro vizualizaci získávaných dat. Řešení bylo zaměřeno na jednoduchou škálovatelnost systému v budoucnu. Kromě toho byl vytvořen také nízce interaktivní honeypot pro sledování brute-force útoků na tuto službu společně se zachytáváním přihlašovacích údajů využitého protokolu NTLMv2.

Získávané znalosti o útočnících pak přispívají k lepší ochraně uživatelů v rámci produktu *Remote Access Shield* společnosti Avast.

---

[1] https://hotforsecurity.bitdefender.com/blog/spike-in-remote-work-leads-to-40-increase-in-rdp-exposure-to-hackers-22782.html

## Sběr a vizualizace metadat škodlivých vzorků ransomware

Ransomware dnes stále patří mezi nejběžnější hrozby v online prostředí[2]. Kvůli tomu se naše snahy o zjišťování informací o aktérech za těmito škodlivými rodinami malware ubíraly i tímto směrem. Pro oklamání těchto útočníků byl navržen systém tzv. honey tokenů – emailů, které by byly odesílány na emailové adresy útočníků. Pro tento systém jsme však potřebovali zdroj čerstvých emailových adres útočníků.

Proto byl navržen systém, který automaticky sbírá emailové adresy útočníků spolu s dalšími metadaty o daném ransomware útoku. Tyto informace tak slouží nejen k následnému využití výše popsaným systémem, ale agreguje tato metadata na jednom místě. Ta pak mohou sloužit k porovnání nebo identifikaci škodlivých rodin ransomware. Samotná idea klamání útočníků s využitím implementovaného systému je nadále v režimu vývoje.

## Systém pro automatické nasazení a správu honeypotů

Se zvyšujícím se počtem vyvinutých a spravovaných honeypotů roste náročnost jejich údržby a správy. V rámci tohoto projektu byl tedy vyvinut systém postavený na technologii Ansible[3], který tuto činnost automatizuje. Díky vyvinutému systému je možné nasazovat podporované honeypoty jediným příkazem. Společně s honeypoty se pak nasadí i monitoring jak systémových prostředků tak běžících procesů. Pokud následně dojde k chybě či pádu honeypotu, umí náš systém buď sám problém vyřešit (například restartováním procesu), nebo problém nahlásí na odpovídající interní kanál společnosti.

Díky tomuto systému se tak můžeme soustředit na další experimenty a výzkum, bez nutnosti trávit čas sledováním funkčnosti aktuálně nasazených instancí.

# Výstupy řešení

Výsledky naší práce na emailových honeypotech byly prezentovány na mezinárodní konferenci SECRYPT 2020[4]. Ta se kvůli pandemii koronaviru přesunula z plánované Paříže do online prostředí.

Co se týče praktických a experimentálních výstupů, byla úspěšně nasazena platforma pro sledování útoků protokolu RDP. Dále bylo úspěšně otestováno řešení pro automatické nasazení, správu a monitoring různých druhů honeypotů, s důrazem na budoucí rozšiřitelnost tohoto řešení. V neposlední řadě byla nasazena platforma pro získávání a vizualizaci metadat nejnovějších škodlivých vzorků typu ransomware.

# Plán na další období

V dalším období bude kladen důraz převážně na tři oblasti. V první řadě budeme pokračovat v našich současných projektech, které sledují světové trendy v oblasti kybernetické

[2] https://www.infosecurity-magazine.com/news/ransomware-tops-2020-threat/
[3] https://www.ansible.com/
[4] http://www.secrypt.org/?y=2020

bezpečnosti. Díky technologiím založených na oklamání útočníka máme přehled o aktuálních hrozbách v různých oblastech online světa.

Druhým pilířem naší práce je využití těchto technologií v oblasti *Internet of Things* (IoT). Tato oblast se v posledních letech ukázala jako velmi náchylná ke kybernetickým útokům. Její sledování s využitím honeypotů se tak nabízí.

Posledním cílem je vyhodnocení *threat intelligence* dat poskytovaných třetími stranami. Společnosti, jako je Shadowserver Foundation[5], poskytují data o útočnících ze své celosvětové sítě honeypotů. Ty jsou určeny převážně pro národní orgány kybernetické bezpečnosti a pro výzkumné účely. Cílem naší práce by bylo porovnání těchto dat s daty, které jsme schopni shromáždit pomocí našich systémů.

[5] https://www.shadowserver.org/