VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INFORMAČNÍCH SYSTÉMŮ
DEPARTMENT OF INFORMATION SYSTEMS

ANALÝZA SÍŤOVÉ KOMUNIKACE RANSOMWARE

RANSOMWARE TRAFFIC ANALYSIS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. MICHAL ŠRUBAŘ**
AUTHOR

VEDOUCÍ PRÁCE — **Doc. Ing. ONDŘEJ RYŠAVÝ, Ph.D.**
SUPERVISOR

BRNO 2017

Zadání diplomové práce/20204/2016/xsruba03

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav informačních systémů Akademický rok 2016/2017

Zadání diplomové práce

Řešitel: **Šrubař Michal, Bc.**
Obor: Bezpečnost informačních technologií
Téma: **Analýza síťové komunikace Ransomware**
Ransomware Traffic Analysis
Kategorie: Bezpečnost

Pokyny:

1. Seznamte se s problematikou Ransomware.
2. Za použití existujících nástrojů vytvořte prostředí, ve kterém bude možné sledovat síťovou komunikaci infikovaných uzlů tímto typem malware.
3. Proveďte analýzu síťové komunikace vybraných typů Ransomware.
4. Na základě této analýzy vytvořte behaviorální signatury tohoto typu malware.
5. Vytvořené signatury se pokuste začlenit do existujícího systému Mendel od společnosti GreyCortex.
6. Proveďte zhodnocení dosažených výsledků a navrhněte možná rozšíření.

Literatura:

- G. Zhao, K. Xu, L. Xu and B. Wu, "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis," in *IEEE Access*, vol. 3, no. , pp. 1132-1142, 2015.
- H. Lim, Y. Yamaguchi, H. Shimada and H. Takakura, "Malware classification method based on sequence of traffic flow," *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, Angers, France, 2015, pp. 1-8.
- Nolen Scaife; Henry Carter; Patrick Traynor; Kevin R. B. Butler: CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data. IEEE 36th International Conference on Distributed Computing Systems (ICDCS), 2016.
- S. Grzonkowski, A. Mosquera, L. Aouad and D. Morss, "Smartphone Security: An overview of emerging threats.," in *IEEE Consumer Electronics Magazine*, vol. 3, no. 4, pp. 40-44, Oct. 2014.
- Charles Nicholas and Robert Brandon. 2016. Document Engineering Issues in Malware Analysis. In Proceedings of the 2016 ACM Symposium on Document Engineering (DocEng '16). ACM, New York, NY, USA, 3-3.

Při obhajobě semestrální části projektu je požadováno:

- Dokončení bodů 1 až 3 zadání.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci dřívějších projektů (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Ryšavý Ondřej, doc. Ing., Ph.D.**, UIFS FIT VUT
Datum zadání: 1. listopadu 2016
Datum odevzdání: 24. května 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav informačních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Dr. Ing. Dušan Kolář
vedoucí ústavu

Abstrakt

Cílem této práce je přiblížení problematiky malware typu ransomware a následně analýza síťové komunikace crypto-ransomware a možné detekce tohoto typu malware. Práce popisuje v jakém prostředí zkoumání této síťové komunikace bylo provedeno a jaká byla zvolena metodologie. První část práce se zabývá samotnou analýzou síťového provozu tohoto typu malware se zaměřením na HTTP a DNS komunikaci. Dále se zabývá anomáliemi, které je možné během komunikace tohoto malware pozorovat na síti. Soustředí se také na chování uživatele, jehož zařízení ransomware infikuje. Výsledkem práce je popis čtyřech detekčních metod, které jsou schopny rozpoznat ransomware ze síťové komunikace za použití HTTP protokolu. Práce dále přináší popis několika signatur, které mohou být použity jako ukazatel možné infekce ransomware.

Abstract

The focus of this work is crypto-ransomware; a variant of malware, an analysis of this malware's network communication, and the identification of means by which it may be detected in the network. The thesis describes the methodology and environment in which the malware's network communications were studied. The first part of the thesis provides a network traffic analysis of this type of malware with a focus on HTTP and DNS communication, including anomalies that can be observed in the network during this malware's activity. The thesis also includes a discussion of the user behavior of devices infected by this type of malware. The resulting data was used to identify and describe four detection methods that are able to recognize the malware from its network communication using the HTTP protocol. Finally, a description of several signatures that can be used as indicators of a possible infection by this malware are provided.

Klíčová slova

Škodlivý software, Malware, Ransomware, Crypto-malware, HTTP POST Check-in, DNS, WannaCry, Malware lab, TOR.

Keywords

Malware, Ransomware, Crypto-ransomware, Crypto-malware, HTTP POST Check-in, DNS, WannaCry, Malware lab, TOR.

Citace

ŠRUBAŘ, Michal. *Analýza síťové komunikace Ransomware*. Brno, 2017. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ryšavý Ondřej.

Analýza síťové komunikace Ransomware

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana docenta Ondřeje Rýšavého. Další informace mi poskytli zaměstnanci společnosti GreyCortex, s.r.o. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Michal Šrubař
23. května 2017

Poděkování

V první řadě děkuji společnosti GreyCortex za zapůjčení senzoru MENDEL a poskytnutí fyzických prostředků pro vytvoření testovacího prostředí bez kterého by nebylo možné na této diplomové práci pracovat. Dále děkuji mému vedoucímu docentovi Ing. Ondřeji Ryšavému, Ph.D. a mým kolegům Mgr. Michalu Mertovi a Bc. Martinu Korci.

Obsah

Kapitola 1

Úvod

Smyslem této diplomové práce je seznámit čtenáře s problematikou malware typu crypto-ransomware se zaměřením na analýzu síťové komunikace a následně detekci ransowmare na základě odpozorovaných vzorů v této komunikaci.

Obecné problematice ransomwre je věnována kapitola č. 2, ve které se čtenář seznámí s tím, co to vlastně ransomware je a z čeho se ransomware vyvinul. Kapitola dále pojednává o způsobech, kterými může dojít k infekci zařízení tímto typem malware. V dalších sekcích se čtenář dozví, jaké typy kryptografických algoritmů ransomware používá a jakým způsobem je využívá ve svůj prospěch. Poslední sekce poté popisují, jakým způsobem autoři tohoto typu malware na této činnosti vydělávají peníze, na kolik je tato činnost výnosná, jaká je aktuální situace okolo crypto-ransomware a jaké jsou predikce do budoucnosti.

Kapitola č. 3 se zabývá samotnou analýzou síťové komunikace tohoto typu malware. Popisuje jakým způsobem a z kterých komponenet je sestaveno testovací prostředí, které bylo pro tuto analýzu vytvořeno a dále popisuje metodologii, která byla při analýze použita. Dále se zabývá analýzou obecných vzorů v síťové komunikaci crypto-ransomware a blíže se zaměřuje na 4 vzorky, které byly v síťové komunikaci tohoto typu malware odpozorovány. Zejmena se jedná o zaměření na komunikaci pomocí protokolů HTTP a DNS. Poslední sekce této kapitoly přináší analýzu ransomware WannaCrypt, který udeřil zrovna v době dokončování této diplomové práce a je považován za ransomware, který způsobil nejvíce škody v historii tohoto typu malware. Část této analýzy byla také publikována na některých českých a zahraničních serverech zabývajících se internetem nebo bezpečnostní.

Poznatky z analýzy síťové komunikace byly využity pro vytvoření několika detekčních metod, které jsou blíže popsané v kapitole č. 4. Tyto detektory byly experimentálně implementovány do systému MENDEL od společnosti GreyCortex a poté otestovány v reálném prostředí. Kapitola dále popisuje výsledky tohoto testování a zamýšlí se nad užitečností jednotlivých detekčních metod. Poslední sekce se poté zamýšlí nad zhodnocením těchto experimentů.

Kapitola 2

Ransomware

Tato kapitola shrnuje základní informace o tom, co to vlastně ransomware je, z čeho se vyvinul, jaká je aktuální situace kolem tohoto typu malware a jaké jsou predikce do budoucnosti. Tato kapitola také dále popisuje jaké kryptografické algoritmy dnes ransomware používají a jakým způsobem je využívají ve svůj prospěch.

2.1 Co je vlastně ransomware?

Za ransomware se dá obecně označit jakýkoliv škodlivý software[1], který útočníkům umožňuje zamezit přístup k informacím, datům nebo hardware jednotlivce nebo společnosti a poté vyžadovat výkupné[2] za znovu zpřístupnění těchto zdrojů [14] [3]. Dnes by se dal ransomware rozdělit na dva typy škodlivého software:

- Locker-ransomware a
- Crypto-ransomware.

Prvním z nich je tzv. locker-ransomware, který je navržen tak, aby pouze zamezil přístup k infikovanému zařízení. Většinou toho zamezení provede uzamčením uživatelského rozhraní tak, aby napadený uživatel mohl využívat pouze například numerickou klávesnici pro zadání kódu, který potvrdí platbu finančního poplatku, který je po uživateli požadován, jestliže chce opět získat přistup ke svému zařízení. Tento typ škodlivého software ponechává uživatelská data nezměněná a ve velké většině případů je možné ho odstranit navrácením systému do nějakého předchozího stavu. To je možné účinit použitím specializovaného software ovšem pouze za předpokladu, že má uživatel plný přístup k danému systému a proto tento typ ransomware není tak finančně výnosný jako jeho druhá varianta.

Druhý typ ransomware označovaný jako tzv. crypto-ransomware, potichu hledá v systému nebo na síti cenná data, které s pomocí moderní kryptografie zašifruje a tímto způsobem je danému uživateli znepřístupní. Většinou necílí na to znepřístupnit uživateli systém jako takový a systém je tedy možné dále používat. Stejně jako v prvním případě, ransomware poté po uživateli požaduje zaplacení výkupného při jehož zaplacení poté uživatel obdrží dešifrovací klíč. Pomocí tohoto klíče může svá data opět dešifrovat a to vše do určitého časového limitu. Tento typ ransomware většinou nijak neomezuje napadený počítač, díky čemuž může daný uživatel provést on-line platbu [14][3].

[1] v angličtině označovaný jako malware

[2] v angličtině ransom, odtud pochází spojení ransomware

Nutno podotknout, že ne všechny ransomware jsou škodlivé, existují i takové typy ransomware, které si kladou za cíl dát uživatelům lekci a šířit informace o rostoucí hrozbě tohoto typu škodlivého software. Jedním takovým příkladem je např. EduCrypt, který zašifruje uživatelská data ve složkách Plocha, Stažené, Dokumenty, Obrázky, Hudba, Video a zanechá uživateli upozornění v podobě textového souboru obsahujícího instrukce, které je možné vidět na obrázku č. 2.1, pro dešifrování souborů. Žádné výkupné není po uživateli požadováno ani zde neprobíhá žádná komunikace s C&C[3] servery.

> *Well hello there, seems you have a virus! Well you are going to get the decrytor which is here "http://www.filedropper.com/decrypter_1" Don't download random shit on the iternet a hidden.txt file has been created with the decrypt password! Find it!*

Obrázek 2.1: Instrukce crypto-ransomware EduCrypt.

2.2 Způsoby infekce

Existuje mnoho způsobů, kterými je možné se stát objetí ransomware. Mezi nejčastější dnes patří [3][14][10]:

- nevyžádaná pošta,
- drive-by download,
- škodlivá reklama,
- sociální inženýrství,
- downloaders, botnety a další.

2.2.1 E-mailové přílohy

Ransomware se může šířit pomocí podvodných nebo nevyžádaných e-mailů[4], které mohou obsahovat odkazy na infikované webové stránky obsahující Exploit Kit nebo škodlivé soubory jako přílohu, které poté využijí nějaké zranitelnosti aplikace pro stažení ransomware.

2.2.2 Drive-by download

Termínem Drive-by download je označována technika, při které dojde ke stažení a nainstalování škodlivého software zcela bez vědomí uživatele pouhým otevřením infikované webové stránky ve webovém prohlížeči. Často se zde využívá tzv. Exploit Kit, což je softwarový balík, který běží na webovém serveru a jehož cílem je identifikovat softwarové zranitelnosti uživatelského systému, který se na daný webový server připojí skrze webový prohlížeč. Nalezená zranitelnost je poté využita ke spuštění škodlivého kódu na uživatelově systému. Tato technika napadení většinou probíhá v následujících pěti krocích:

1. Uživatel prochází své oblíbené webové stránky (nejčastěji s pornografickým obsahem). Jakmile se dostane na stránku, která byla infikovaná a obsahuje skrytý HTML element `iFrame`, který způsobí, že je uživatel přesměrován na tzv. Landing page, která obsahuje nějaký Exploit Kit.

[3] Command-and-Control
[4] phising e-mails nebo SPAM

2. Exploit kit se nejprve pokusí zjistit zda se nejedná o virtualizované prostředí[5] a zda není Exploit kit analyzován. V tomto kroku se využívá například XMLDOM funkcionality prohlížeče Internet Explorer, pomocí které je možné zjišťovat informace o souborech na lokálním systému. Díky tomu může detekovat například přítomnost bezpečnostního software jako jsou antivirové programy nebo zda není daný prohlížeč spuštěn na virtuálním počítači.

3. Poté se pokusí zjistit verze uživatelova software pro doručení exploitu[6] využívajícího konkrétní zranitelnost.

4. Jakmile Exploit Kit nalezne vyhovující zranitelnost, aplikuje daný Exploit a tím umožní stažení škodlivého software na uživatelský systém.

5. Poté následuje spuštění samotného škodlivého software což může vést ke stažení jiného škodlivého software, například některé varianty ransomware, který po spuštění provede zašifrování všech uživatelských dat.

Dle zpráv od výzkumných skupin *Talos* [4] a *Cisco* [2] byl nejrozšířenějším a nejpokročilejším Exploit Kitem v roce 2016 *Angler Exploit Kit*, který v 62% doručil napadenému systému nějakou variantu ransomware. Ve většině případů se jednalo o *Cryptowall 3.0* nebo *TeslaCrypt 2.0*, které dále využívaly napadnuté redakční systémy Wordpress.

Obrázek č. 2.2 znázorňuje, že skoro 75% exploitů využívalo zranitelnosti v aplikaci Adobe Flash. Zhruba 24% exploitů využilo zranitelnosti v prohlížeči Internet Explorer a zbývající poté webového doplňku Microsoft Silverlight.

2.2.3 Škodlivá reklama

Ransomware může být doručen také pomocí škodlivé reklamy označované jako tzv. Malvertisments, která může být vložena na legitimní stránku. Tato reklama poté uživatele přesměruje na kompromitovaný web obsahující exploit kit.

2.2.4 Downloaders a botnet

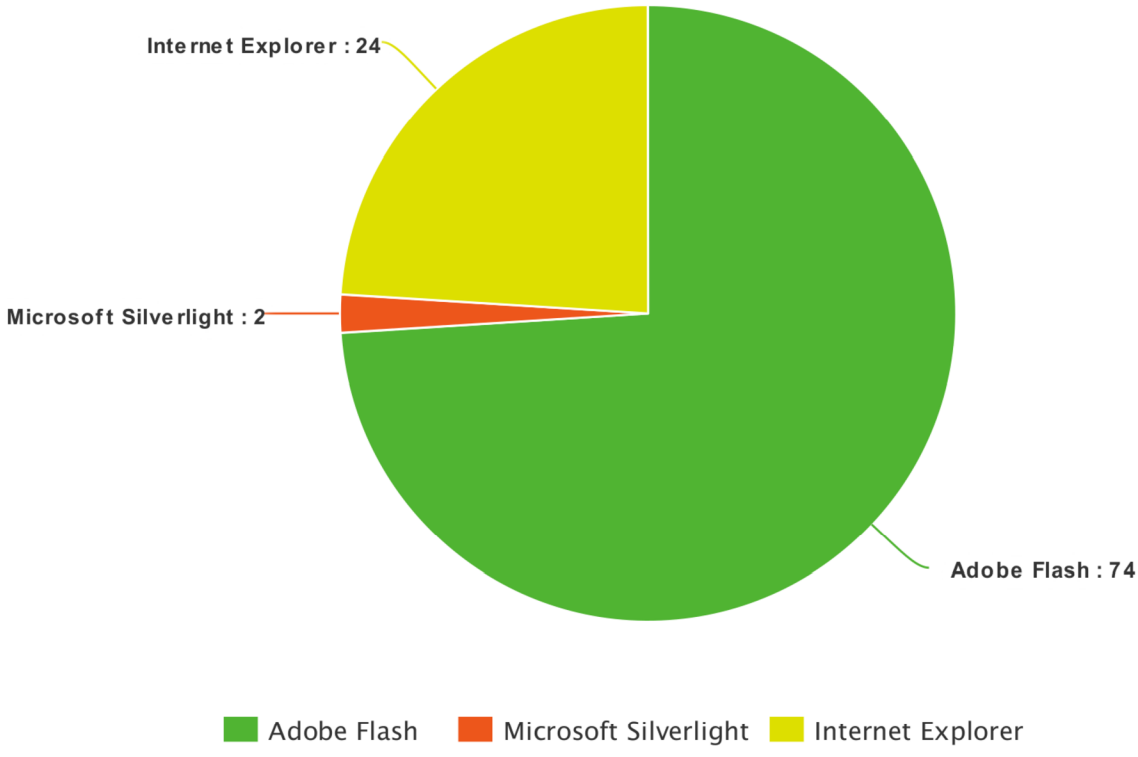
Tato metoda dovoluje distribuovat ransomware pomocí tzv. Downloaders, což mohou být zcela legitimní instalační programy ovšem obohacené o skrytou funkcionalitu. Hlavním smyslem této skryté funkcionality je poté stáhnout a nainstalovat škodlivý software bez povšimnutí uživatele.

2.2.5 Sociální inženýrství

Tato technika se snaží využívat praktiky sociálního inženýrství k tomu, aby klamavě přesvědčila uživatele k instalaci falešného antivirového programu. Většinou tak nastave v okamžiku, kdy uživateli nějaká webová stránka provede falešné oskenování zařízení a detekuje přítomnost škodlivého software nebo uživateli vyhrožuje, že zveřejní jeho soukromé fotografie na internetu pokud uživatel výkupné nezaplatí [9].

[5] pomocí tzv. anti-sandbox checks

[6] software využívající konkrétní zranitelnosti jiného software za účelem získání kontroly nad systémem nebo eskalaci oprávnění



Obrázek 2.2: Procentuální využití zranitelností Exploit Kitem Angler.

2.2.6 Ostatní

Ransomware se může šířit také jinými způsoby jako jsou například webové aplikace, které umožňují posílat zprávy tzv. *Instant Messaging*. Příkladem může být *Facebook* a jeho aplikace *messenger*[7].

2.3 Metody šifrování dat

Většina crypto-ransomware dnes pro samotné šifrování souborů využívá symetrický algoritmus *AES*[8] v kombinaci s RSA. Existují ovšem i varianty, které používají jednoduché metody šifrovaní jako například šifru *XOR*, kterou používají crypto-ransomware *Pclock*, *ODCODC*, *Nemucod* nebo *Marlboro*. Ostatní poté používají například *Base64*, *TripleDES*, algoritmus *RC*[9] ve verzích 2, 4 nebo 6, *Blowfish*, blokovou šifru *GOST*[10], streamovou šifru *Salsa20*[11], eliptické křivky nebo techniku přesouvání bajtů.

[7] https://www.messenger.com/
[8] The Advanced Encryption Standard
[9] Rivest Cipher
[10] https://en.wikipedia.org/wiki/GOST_(block_cipher)
[11] https://en.wikipedia.org/wiki/Salsa20

Většina pokročilejších crypto-ransomware poté kombinuje jak symetrické, tak asymetrické algoritmy. Podle použitých šifrovacích algoritmů je dnes crypto-ransomware možné rozdělit do třech následující skupin:

- jedno-úrovňové,
- dvou-úrovňové a
- tří-úrovňové.

Následující odstavce popisují tyto jednotlivé úrovně a způsoby jakými je využívají konkrétní rodiny crypto-ransomware. Nejedná se o úplný výčet všech crypto-ransomware a popisu šifrovacích metod, které používají, jelikož různých typů tohoto malware je dnes několik stovek. Například projekt *ID Ransomware*[12] je k datu 23. května 2017 schopný detekovat více než 350 různých rodin crypto-ransomware. Každá z těchto rodin poté může mít několik verzí ve kterých se mohou metody a algoritmy navzájem lišit.

2.3.1 Jedno-úrovňové

Příkladem crypto-ransomware, který používá jednostupňové šifrování je například *Jigsaw*, který je dnes považován za prolomený. Oběti, jejichž data byla tímto crypto-ransomware napadena tedy mohou použít již existující nástroje pro dešifrování svých dat. Tento ransomware používá pro šifrování standardní algoritmus AES, přičemž Inicializační Vektor (IV) a klíč je uložen přímo v samotném vzorku malware. Se znalostí IV a klíče je tedy možné zpětně data dešifrovat.

2.3.2 Dvou-úrovňové

Mezi crypto-ransomware, kterou používají dvou-úrovňové šifrování patří např. ransomware *Locky* nebo *CryptoWall*. Činnost crypto-ransomware Locky začíná tím, že skrze šifrovaný kanál z C&C serveru stáhne 2048-bitový veřejný RSA klíč. Poté si vytvoří seznam souborů, které bude šifrovat a pro každý z těchto souborů vygeneruje jedinečný AES klíč. Tento klíč je poté zašifrován pomocí staženého RSA klíče. Locky využívá standardních algoritmu z knihovny *CryptoAPI*[13], které je součástí operačních systémů Microsoft Windows. Během samotného šifrovacího procesu se vytvářejí statistiky říkající, kolik souborů bylo zašifrováno, ve kterých složkách, jaký byla jejich velikost atd. Tyto statistiky jsou poté odeslány na C&C server a na základě těchto statistik je poté pravděpodobně určena velikost výkupného. Většina crypto-ransomware zobrazí dešifrovací instrukce a informace o výkupném jako HTML stránku. Locky tyto informace ovšem vygeneruje jako obrázek, který nastaví na daném zařízení jako tzv. *Wallpaper*. V těchto instrukcích se nachází odkaz na webovou stránku, která je unikátní pro každé napadené zařízení a je přístupná v síti TOR. Tato stránka taktéž obsahuje obecné informace a také poskytuje podporu pro provedení platby výkupného. Jazyk, ve kterém se vygenerují instrukce pro zmíněný wallpaper, se zjistí z nastavení systému pomocí funkce *GetUserDefaultUILanguage*.[14]

Crypto-ransomware *CryptoWall*, který se vyvinul z ransomware *CryptoLocker* používá pro šifrování souborů algoritmy RSA a AES. Předtím, než začne malware provádět šifrování dat, stáhne si veřejný RSA klíč od svého C&C serveru. Tento veřejný klíč je jedinečný pro

[12] https://malwarehunterteam.com/
[13] https://en.wikipedia.org/wiki/Microsoft_CryptoAPI
[14] https://msdn.microsoft.com/en-us/library/windows/desktop/dd318137%28v=vs.85%29.aspx

každé infikované zařízení. Jestliže není infikované zařízení připojené k internetu nebo se není možné spojit s C&C serverem, tak k zašifrování dat nedojde. Skutečné C&C servery se u této varianty nacházejí za proxy servery což je dělá velice těžko vystopovatelné. Starší varianty toho typu ransomware používaly pro komunikaci s C&C serverů pevně dané doménové jména, ovšem novější už implementují DGA[15] algoritmy pro generování náhodných doménových jmen.

Pro šifrování samotných souborů na infikovaném zařízení je použit náhodně vygenerovaný klíč, který je použit v algoritmu AES. Tento klíč je poté zašifrován staženým RSA klíčem a uložen na infikovaném zařízení. Pro dešifrování souborů tedy uživatel musí obdržet privátní RSA klíč z C&C serveru, tím je poté dešifrován klíč, který byl použit pro zašifrování souborů. Pomocí tohoto klíče a algoritmu AES jsou poté dané soubory dešifrovány. Jelikož se privátní klíč, který je potřebný pro dešifrování AES klíče, nachází pouze na C&C serveru a nepřenáší se po síti dokud není zaplaceno výkupné, je prakticky nemožné takto zašifrované soubory bez toho klíče dešifrovat.[12]

2.3.3 Tří-úrovňové

Mezi crypto-ransomware, používající tří-urovňové šifrování je možné zařadit například *CTB-Locker* nebo *Cerber*. První tři písmena v názvu ransomware CTB-Locker jsou zkratky pro anglická slova *Curve*, *TOR* a *Bitcoin*. První část, tj. slovo Curve reprezentuje použítý kryptografický algoritmus, kterým jsou Eliptické křivky neboli ECC[16] (Elliptic Curve Cryptography). Jedná se o jeden z asymetrických kryptografických algoritmů, který se zabývá problémem diskrétního logaritmu nad eliptickými křivkami. Výhodou tohoto algoritmu, oproti RSA, je jeho efektivnost a rychlost za použití kratších šifrovacích klíčů. Například 256-bitový ECC klíč přináší shodnou úroveň bezpečnosti jako 3072-bitový RSA klíč.

Tento crypto-ransomware tedy kombinuje jak symetrickou, tak asymetrickou kryptografii. Jako asymetrickou algoritmus jsou použity výše zmíněné asymetrické křivky a jako symetrický poté AES. CTB-Locker používá podobný princip jako CryptoWall, kdy samotné soubory jsou šifrovaný pomocí algoritmu AES. Samotný klíč, který byl při tomto šifrování použit je poté zašifrován pomocí veřejného klíče ECC. Opět pouze autoři, jakožto držitelé privátního ECC, jsou schopni daná data dešifrovat.

Druhé slovo Tor reprezentuje použití sítě TOR, přes kterou je poslána většina síťové komunikace. Tato komunikace většinou prochází skrze proxy servery, které slouží jako uzly[17] pro skryté služby, na kterých se nacházejí C&C servery. Třetí slovo Bitcoin poté reprezentuje měnu, kterou si autoři nechávají platit za dešifrování dat.[13]

Ransomware *Cerber* používá pro šifrování standardní algoritmy RSA a RC4. Ransomware nejprve na infikovaném zařízení vygeneruje 2048-bitové RSA klíče. Pro samotné šifrování souborů se ovšem použije jiný algoritmus a tím je RC4. Varianta crypto-ransomware Cerber 3 používá 128-bitové RC4 klíče, kde se pro každý soubor vygeneruje jedinečný klíč, kterým je poté soubor zašifrován. Všechny takto vygenerované klíče jsou poté zašifrovány pomocí vygenerovaného RSA klíče. Jestliže tedy Cerber bude šifrovat 150 souborů, vygeneruje 150 jedinečných RC4 klíčů, kde každý z nich poté zašifruje RSA klíčem. Výhodou toho přístupu je poté skutečnost, že získání byť jediného RC4 klíče je možné dešifrovat pouze jeden zašifrovaný soubor. Použití proudové šifry RC4 je zcela záměrné, jelikož je tento algo-

[15] Domain generation algorithm
[16] https://en.wikipedia.org/wiki/Elliptic_curve_cryptography
[17] TOR Relay

ritmus velice rychlý. RSA klíč, který je poté možné použít pro dešifrování souborů, je buď uložen na napadeném zařízení nebo odeslán C&C serveru.

Většina crypto-ransomware začne šifrovat data hned po svém spuštění a uživatel tedy v rozmezí desítek sekund pozná, že byly jeho data zašifrovány. Například crypto-ransomware Chimera je schopný zašifrovat jeden gigabajt dat za zhruba 5 minut. Jeden terabajt dat poté za 75 hodin.

Seznam více než čtyř set rodin crypto-ransomware a kryptografické algoritmy, které používají je možné nalézt v příloze D nebo na datovém médiu ve složce `data/`, viz. příloha A. Aktualizovaný seznam je možné najít na URL adrese http://preview.tinyurl.com/hhc6csy.

2.4 Platba výkupného

V průběhu let se měnily možné způsoby platby výkupného, jak se postupem času stávaly dostupné nové a nové služby plateb. Platby výkupného prošly od posílání šeků na poštovní adresu, prémiově placených SMS zpráv, platebních virtuálních peněženek jako Paysafecard, MoneyPak, UKash, CashU, a MoneXy přes platby kreditní kartou až po virtuální krypto měnu Bitcoin. Při použití Bicoin je poté platba provedena přes servery spravované v darknetu[18] přístupné přes sít TOR.

Preferovanou měnou crypto-ransomware se dnes stává převážně krypto měna Bitcoin[19], která je anonymní a nevystopovatelná, zatímco locker-ransomware využívají převážně systém platebních poukazů. Možným vysvětlením může být právě rozdílný způsob, kterým oba typy malware pracují. Jak bylo zmíněno v sekci 2.1, locker-ransomware zanechají napadené zařízení nepoužitelné a proto by nebylo možné z tohoto zařízení provést zaplacení výkupného on-line [14].

Naopak finanční poukazy je možné vyměnit za peníze například v on-line herních systémech a on-line kasínech. Většinou jsou použity takové, které se nacházejí na rozdílných geografických lokacích a s jinými zákony a proto je těžké je vystopovat. Takto vyprané peníze jsou poté poslány na podvodně připravené debetní karty, ze kterých je poté možné vybrat peníze z libovolného bankomatu.

Dle zprávy [10] v roce 2012 ransomware vydělal svým autorům mezi 750 000 – 1 500 000 euro. Dle zprávy [17] společnosti Symantec si jen crypto-ransomware Trojan.Cryptowall vydělal v květnu 2014 nejméně 34000 amerických dolarů a koncem srpna 2014 to byl už více než jeden milion dolarů. Data[20] z centra IC3[21] úřadu FBI[22] uvádí, že mezi dubnem 2014 a červnem 2015 obdrželi více než 992 stížností ohledně crypto-ransomware CryptoWall od koncových uživatelů a společností a celkové zráty z těchto stížností byly vyčísleny na více než 18 milionů dolarů. Zpráva skupiny Cyber Threat Alliance uvádí, že CryptoWall ransomware verze 3 vydělal svým autorům zhruba 325 milionů dolarů pouze ve Spojených Státech Amerických [1].

Dle zpráv od US-CERT[23] a společnosti Symantec byla začátkem roku 2016 průměrná výše výkupného 200-400 dolarů a preferovanou metodou platby je použití virtuální měny Bitcoin [5]. U některých institucí se mohou hodnoty výkupného pohybovat i kolem desítek

[18] https://en.wikipedia.org/wiki/Darknet
[19] https://www.bitcoin.com/
[20] https://www.ic3.gov/media/2015/150623.aspx
[21] Internet Crime Complaint Center
[22] https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation
[23] United States Computer Emergency Readiness Team

tisíc dolarů [14]. Podle společnosti malwarebytes se 58% společností ve Velké Británii stalo obětmi ransmoware a něco málo pod 40% celosvětově. V nejvíce případech byly zasaženy zdravotní a finanční instituce.

2.5 Aktuální situace

Skupiny stojící za vývojem ransomware stále inovují a proto můžeme v budoucnu očekávat, že se ransomware začně objevovat na zařízeních, na kterých jsme jej doposud neviděli. Dnes jsou velice rozšířené zařízení, které se nosí na těle, tzv. wearable devices a zařízení, které tvoří tzv. Internet of Things (IoT) pod které spadají například routery, ledničky, televize, mobilní telefony, tablety nebo set-top boxy. Právě tyto zařízení dle zprávy [14] mohou mít v budoucnu velký potenciál stát se obětí locker-ransonware i když je dnes ransomware nejvíce cílen na osobní počítače, servery a mobilní zařízení. Nejvíce napadány jsou zařízení s operačním systémem Windows, což není překvapující, jelikož systémy s Windows tvoří 89%[24] podílu operačních systémů na trhu a cílí hlavně na domácí uživatele, podniky, veřejné právní a vzdělávací instituce. Ransomware se dnes také dostává do podvědomí obecné veřejnosti díky případům, kdy byly ransomware infikovány státní instituce [7][6] jako například policejní oddělení ve městě Durham ve státe Severní Karolína nebo několik nemocnic, které byly zveřejněny v médiích.

Ransomware útoky samotné se dnes nabízejí i jako služba[25], u které vůbec není nutné mít potřebné technické znalosti pro vytvoření ransomware ani jak jej rozšířit. Samotné šíření ransmoware je poté zcela na třetí osobě a samotní autoři takové služby se poté mohou pouze soustředit na vývoj samotného ransomware a ne jeho rozšíření. Autoři ransomware si poté sami nechají 30% z výdělku.

Ve státě Kalifornie v USA je použití ransomware bráno jako trestný čin vydírání, které je trestáno až čtyřmi roky odnětí svobody[26].

Ransomware dnes také velice nahrává lenost uživatelů a administrátorů, kteří neprovádějí pravidelné zálohy dat a také neuvědomění si hodnoty digitálních informací, dokud o ně sami nepřijdou [3]. Zpráva Symantec Backup Survey[27] ukazuje, že 25% domacích uživatelů svá data vůbec nezálohuje. Ovšem ani pravidelná záloha tento problém nemusí vyřešit, protože některé varianty ransomware jsou schopné zalohu najít a smazat popř. zašifrovat zálohy provedené na externí disky, které jsou k počítači připojené, což ve výsledku může znamenat, že ransomware může ovlivnit více než jednoho uživatele.

Technologický pokrok pomohl ransomware k hojnému rozšíření. Díky virtuální krypto měně je možné provádět nevystopovatelné převody pěněz. Síť TOR dovoluje útočníkům skrývat své servery na kterých mají uložené privatní klíče. K tomu, aby se uživatel stal objetí ransomware dnes může stačit pouhé jedno kliknutí na webové stránce nebo otevření přílohy v emailu a podle výzkumné skupiny Talos [11] se ransomware dnes stává jedním z nejvíce obávaných a nejvýdělečnějších typů škodlivého software [2]. Jen v roce 2012 bylo identifikováno 16 rodin ransomware [10]. Mezi lety 2013 a 2014 byl zaznamenán 250% nárůst v nových rodinách crypto-ransomware.

V roce 2015 bylo bezpečnostními speciality identifkováno více než čtyři miliony vzorků ransomware [15]. V následujícím roce bylo 64% zaznamenaných ransomware typu crypto-

[24] https://en.wikipedia.org/wiki/Usage_share_of_operating_systems

[25] ransomware-as-a-service (RaaS)

[26] Zákon vstoupil v platnost 1. ledna 2017

[27] http://www.symantec.com/content/de/de/about/downloads/PressCenter/Symantec_Backup_Survey.pdf

ransomware, zbylých 36% byly typu locker-ransomware a dle US-CERT byly nejrozšířenějšími variantami Locky a Samas. Za nejpokročilejší crypto-ransomware je dnes považován CTB-Locker[3].

Ransomware se stává velice výdělečný a sofistikovaný typ malware proti kterému se dnes spojují společnosti zaměřené na IT bezpečnost jako jsou Kaspersky Lab[28] nebo F-security[29], které založily webovou stránku www.nomoreransomware.org, která poskytuje nástroje a dešifrovací klíče, které byly prolomeny bezpečnostními speciality [16].

2.6 Budoucnost ranswomare

Bezpečnostní zpráva pro první polovinu roku 2016 od společnosti Cisco předpovídá, že se u další generace ransowmare začne používat modulární architektůra, která autorům dovolí:

1. rychle specifikovat, které typy souborů a adresářů bude možné zašifrovat,
2. měnit instrukce pro zaplacení výkupného,
3. měnit velikost výkupného a specifikovat data, do kdy je nutné výkupné zaplatit.

Architektura bude dále podporovat různé moduly, které dovolí autorům použít ransomware v různých prostředích a využívat různé metody šíření. Mezi příklady takových modulů patří:

- Modul pro masové šíření ransowamre - tento modul by umožňoval hledat lokální a síťové disky na které by se poté zkopíroval a nastavil své atributy tak, aby bylo obtížné jej objevit nebo smazat. Poté by na tento disk zapsali soubor autorun.inf, který by je automaticky spustil v okamžiku, kdy by byl disk připojen.
- Modul pro využití autentizačních exploitů - tento modul by využíval známých chyb v autentizačních metodách v korporátních sítích, díky kterým by se ransomware mohl šířit na další systémy.
- Modul pro hlášení úspěšného napadení - aby ransomware snížil riziko odhalení, pak by mohl pro komunikaci se vzdáleným serverem a přenos dat používat běžné protokoly jako HTTP[30], HTTPS[31] nebo DNS[32].
- Modul pro napadení počítačů pouze v privátní síti - tento modul by umožňoval napadnout pouze takové uzly v síti, které mají privání IP adresu definovanou podle RFC č. 1918[33].

[28] https://www.kaspersky.com/
[29] https://www.f-secure.com/
[30] Hypertext Transfer Protocol
[31] Hypertext Transfer Protocol Secure
[32] Domain Name System
[33] https://tools.ietf.org/html/rfc1918

Kapitola 3

Analýza síťové komunikace

Tato kapitola se nejprve zabývá popisem vytvořeného testovacího prostředí, které slouží pro zachycení a analýzu síťové komunikace crypto-ransomware. Dále také popisuje metodologie, která byla při samotné analýze zvolena. Další sekce se poté zabývají samotným rozborem pozorovaných vzorů v síťové komunikaci tohoto typu malware. Samotnou detekcí některých pozorovaných vzorů se poté zabývá další kapitola.

3.1 Testovací prostředí

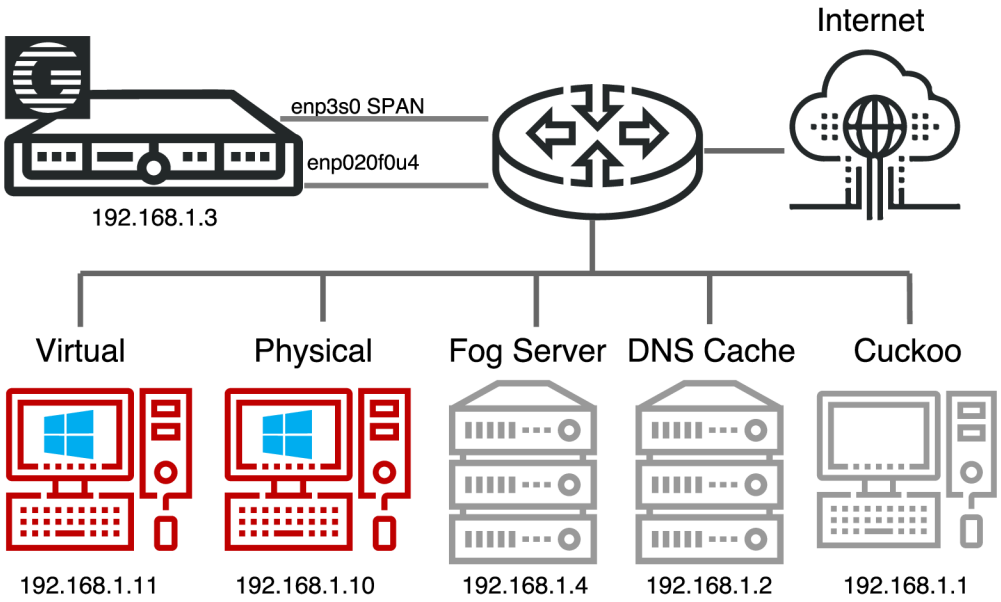
Pro analýzu síťového komunikace crypto-ransomware bylo vytvořeno testovací prostředí jehož schéma je zobrazeno na obrázku č. 3.1. Celá síť se skládá z jednoho routeru MikroTik, který plní úlohu switche, výchozí brány do internetu pro lokální síť a také zajišťuje překlad adres neboli NAT[1]. V prostředí byla dále zapojena DNS Cache, Fog server[2] a dva počítače s referenčním operačním systémem *Windows 7 SP1*, na kterých probíhala analýza jednotlivých vzorků malware. Pro zachycení a analýzu sítové komunikace byl využil open-source sandbox systém *Cuckoo*[3] a senzor *MENDEL*[4] od společnosti *GreyCortex*[5], který analyzoval veškerou komunikaci v sestaveném testovacím prostředí pomocí techniky zrcadlení síťové komunikace označované jako tzv. *Port Mirroring* nebo *SPAN*[6]. Sestavení, zajištění hardware a kompletní zprovoznění včetně konfigurace všech systémů zabralo zhruba 4 měsíce práce.

Samotný sandbox Cuckoo se skládá ze dvou hlavních komponent, kterými jsou webové rozhraní a samotný analyzátor. Předtím, než je možné jednotlivé vzorky analyzovat je potřeba spustit analyzátor, který se nachází ve složce `~/cuckoo/` na počítači s IP adresou 192.168.1.1. Samotné spuštění je možné provést pomocí následujícího příkazu:

```
~/cuckoo/cuckoo.py --debug
```

Volba `--debug` zajistí výpis ladících informací jako jsou například informace o tom, který počítač se pro analýzu použije, v jakém stavu se analýza aktuálně nachází nebo který modul se sandboxu daný vzorek aktuálně zpracovává. Po počáteční inicializaci sandbox

[1] Network address translation
[2] https://fogproject.org/
[3] https://cuckoosandbox.org/
[4] http://www.greycortex.com/mendel-analyst
[5] https://www.greycortex.com/
[6] Switched Port Analyzer



Obrázek 3.1: Schéma testovacího prostředí.

vypíše informaci o tom na které IP adrese je spuštěn, zda se pro analýzu budou používat fyzické nebo virtuální počítače, kolik je takových počítačů k dispozici a pak už jenom uživateli sdělí, že očekává úlohy. Příklad konce výpisu po spuštění sandboxu může vypadat například následovně:

```
[cuckoo.core.resultserver] DEBUG: ResultServer running on 192.168.1.1:2042.
[cuckoo.core.scheduler] INFO: Using "virtualbox"as machine manager
[cuckoo.core.scheduler] INFO: Loaded 3 machine/s
[cuckoo.core.scheduler] INFO: Waiting for analysis tasks.
```

Jakmile je samotný sandbox připravený, očekává vytvoření úlohy, která specifikuje jaký vzorek malware má být analyzován a s jakými parametry. Samotné vytvoření úlohy je možné provést dvěma způsoby:

1. použít webové rozhraní nebo
2. použít skript *submit.py*.

Pro použití webové rozhraní je nutné nejprve spustit webový server na zvoleném portu. Sandbox Cuckoo pro tuto potřebu využívá webový framework *Django*[7], který je možné spustit pomocí příkazu:

```
~/cuckoo/web/manage.py runserver 0.0.0.0:8000
```

Druhou možností je vytvořit úlohu pomocí skriptu `submit.py`, který se nachází ve složce `~/cuckoo/cuckoo/utils/submit.py`. Vytváření úloh pomocí skriptu je vhodné při skriptování, kdy je potřeba najednou vytvořit např. 1000 úloh pro analýzu tisíce vzorků malware,

[7] https://www.djangoproject.com/

zatímco webové rozhraní je velice intuitivní a je tedy vhodnější v případě individuální analýzy.

U obou variant vytvoření úlohy je dále možné specifikovat mnoho doplňujících parametrů, mezi které patří zejména:

- Specifikace tzv. **TIMEOUT** parametru. Analýza jednoho vzorku běží standardně tak dlouho, dokud běží procesy daného malware. Jestliže proces malware skončí dříve než je za počet sekund specifikovaných parametrem TIMEOUT, pak se analýza ukončí až po TIMEOUT sekundách. Jestliže proces běží déle než TIMEOUT sekund, pak přichází do hry tzv. **CRITICAL_TIMEOUT** parametr po kterém je analýza ukončena vždy. Oba parametry jsou udávány v sekundách a jejich výchozí hodnoty jsou nastaveny na 120s pro TIMEOUT a 60s pro CRITICAL_TIMEOUT. Vynucení zadané hodnoty TIMEOUT je možné pomocí volby **Enforce Timeout**.
- Pomocí volby **Machine** je možné zvolit počítač na kterém bude daný vzorek malware analyzován.
- Pomocí volby **Priority** je možné vytvořit úlohu s jinou prioritou než je výchozí. Tato volba je vhodná zejména v případě, kdy běží nějaká dlouhodobá analýza s více vzorky, kterou uživatel nechce přerušit, ale potřebuje v daný moment nárazově zanalyzovat jiný vzorek. Výchozí priorita je nastavena na hodnotu **Medium**.
- Pomocí volby **Machine** je možné vybrat konkrétní operační systém na kterém bude vzorek analyzován. Nebo vybrat, zda má být použit virtuální nebo fyzický počítač nebo, zda se má analýza spustit na všech dostupných počítačích.
- Mnoho dalších, které je možné nalézt v oficiální dokumentaci[8].

Webové rozhraní poté umožňuje nejenom vytváření nových úloh, ale také prohlížení a zkoumání výsledků analýzy. Pro účely této diplomové práce mě zajímala hlavně možnost analýzy síťové komunikace a také možnost stažení této komunikace v souboru ve formátu pcap[9].

V testovacím prostředí byla zapojen také senzor MENDEL, který prováděl monitorování a analýzu veškeré síťové komunikace, která se v testovacím prostředí vyskytla. Tento senzor jako vstup dat zpracovává veškerá data která dostává z ethernetového portu 24, kde je nastaven tzv. *port mirroring*. Všechny ostatní porty routeru Mikrotik byly nastaveny tak, aby posílali veškerou příchozí a odchozí komunikaci právě na tento port číslo 24i,což znamená, že se k senzoru dostane každý paket který testovacím prostředím projde.

Senzor MENDEL poté z těchto síťových dat vytváří vlastní metadata a uchovává všechny potřebná data, která jsou nutná pro IDS[10], behaviorální analýzu a dále výkonnostní analýzu. Jaká data jsou ze síťového provozu extrahována popisuje protokol *ASNM: Advanced Security Network Metrics*[11] [12], jehož popis ovšem překračuje rámec této diplomové práce.

Tento senzor kombinuje jak detekování známého malware na základě IDS signatur, tak detekci neznámých vzorků malware pomocí behaviorální analýzy a dále detekci výkonnostních problémů ve vytvořeném testovacím prostředí.

[8] http://docs.cuckoosandbox.org/en/latest/usage/submit/
[9] tcpdump capture file
[10] Intrusion Detection System
[11] http://www.greycortex.com/advanced-security-network-metrics
[12] http://www.fit.vutbr.cz/~ihomoliak/pubs.php?id=10248

Pomocí tohoto senzoru byla rovněž prováděna analýza vybraných typů crypto-ransomware a implementace detekčních metod, která je dále popsaná v kapitole č. 4 a byla v některých případech cílena a otestována právě na tomto systému.

3.2 Průběh analýzy

Analýza jednoho vzorku crypto-ransomware poté probíhá v následujících krocích:

1. Předání crypto-ransomware vzorku sandboxu Cuckoo pomocí webové rozhraní nebo pomocí skriptu *submit.py*. Webové rohraní sandboxu se nachází na IP adrese `192.168.1.1` na portu 8000. Lze také použít doménové jméno `cuckoo`, tj je možné použít URI `http://cuckoo:8000/`. Sandbox poté vytvoří novou úlohu a nahraje daný vzorek na vybraný systém. V našem případě např. na počítač s IP adresou 192.168.1.11 nebo 192.168.1.10 z obrázku č. 3.1, popřípadě uživatel může zvolit, který systém se má použít.

2. Spuštění daného vzorku a provedení automatické statické i dynamické analýzy. Během této analýzy je zaznamenáváno, která systémová volání ransomware používá, obsah paměti, veškerá síťová komunikace, obrázky z plochy daného systému a celkové chování daného vzorku malware.

3. Po dokončení analýzy jsou veškerá zaznamená data odeslána na Cuckoo server, který provede vyhodnocení a uživatel si je poté může prohlédnou ve zmíněném webovém rozhraní.

4. Posledním krokem je navrácení infikovaného systému do původního stavu, což u fyzického počítače provede Fog server restartováním infikovaného systému a obnovením předchozí zaznamenaného stavu (překopírování naklonovaného obsahu disku). U virtuálního počítače je poté nutné obnovit daný virtuální počítač z tzv. *snapshotu*[13].

Prvotní myšlenka byla provádět veškerou analýzu všech vzorků malware na reálném fyzickém počítači. Minutová analýza jednoho vzorku malware ovšem zabrala zhruba 15 minut, jelikož samotné klonování disku při obnově systému do původního stavu zabrala zhruba 10 minut za použití SSD disků. Další čtyři minuty vzala režie potřebná pro samotnou analýzu (restartování počítače, kopírování dat, získávání výsledků pro analýzu apod).

Pro analýzu bylo k dispozici více než třicet tisíc vzorků crypto-ransomware získaných ze serveru **virusshare**[14] nebo od antivirových společností ***ESET***[15] a ***Avast***[16]. Jestliže bych provedl pouze minutovou analýzu všech vzorků na fyzickém hardware, pak by samotná analýza zabrala více než 300 dnů. Nehledě na možné hardwarové nebo softwarové problémy. Často se stávalo, že se během analýzy použitý sandbox přestal pracovat a bylo potřeba jej restartovat nebo se objevily jiné komplikace.

Na základě této zkušenosti bylo účiněno rozhodnutí přejít od analýzy na fyzickém počítači k analýze vzorků na virtuálním počítači za použití virtualizační technologie **VirtualBox**[17] od společnosti Oracle[18] se kterou trvalo obnovení počítače do výchozího stavu kratší

[13] https://www.virtualbox.org/manual/ch01.html#snapshots
[14] https://virusshare.com/
[15] https://www.eset.com/
[16] https://www.avast.com/
[17] https://www.virtualbox.org/
[18] https://www.oracle.com

dobu než v případě klonování disků na fyzickém počítači. I tak analýza jednoho vzorku zabrala zhruba 10 min, pokud se neobjevily žádné komplikace. Mezi neočekávané komplikace patřilo například neočekávané zastavení provádění analýzy, zaseknutí sandboxu Cuckoo, nefunkční port mirroring a další. Samotná analýza poté běžela zhruba dva měsíce a během tohoto období se mi podařilo zanalyzovat a nasbírat sítovou komunikaci z více než sedmi tisíc vzorku. Takový byl stav ke dnu 21.03.2017, ovšem analýza stále pokračuje.

Provádění analýzy na virtuálním počítači rovněž nebylo jednoduché. Většina dnešního malware se nějakým způsobem snaží detekovat, zda běží na fyzickém nebo virtuálním počítači [8]. Abych snížil pravděpodobnost, že ransomware detekuje, že je spuštěn uvnitř virtuálního počítače, provedl jsem následující kroky, které nastavili virtuální počítač tak, aby co nejvíce odpovídal stavu fyzického počítače. Při vytváření virtuálního počítače jsem nastavil následující parametry tak, aby co nejvíce odpovídaly hostujícímu hardware. Zejména se jednalo o následující parametry:

- BIOS,
- systém,
- základní deska,
- parametry šasi
- a firmware.

Dále jsem použil síťovou kartu `Intel PRO/1000MT Desktop (82540EM)`, které více odpovídá reálné kartě než *virtio-net* a upravil jsem MAC adresu, kde jsem změnil poslední tři bajty oproti MAC adrese hostujícího počítače, aby byl zachován výrobce. Pro vytvoření a nakonfigurování virtuálního počítače jsem použil upravené skripty Michaela Bomana[19], které je možné najít v příloze A. Po instalaci operačního systému na virtuální počítač pak bylo potřeba ještě provést následující kroky:

- neinstalovat Guest Additions,
- nenastavovat sdílené adresáře a
- odstranit z registrů klíče, přidané samotným VirtualBoxem (`vbox-reg.bat`, viz. příloha A).

Po nastavení virtuálního počítače, operačního systému a instalace dalšího software[20] jsem dále postupoval v nastavení sandboxu Cuckoo podle pokynů oficiální dokumentace[21].

Testovací prostředí mimo jiné nabízí další možnosti, mezi které patří dynamická analýza malware nebo analýza webových stránek. Toto prostředí je možné použít nejenom pro analýzu ransomware, ale obecně libovolného typu malware.

[19] http://blog.michaelboman.org/2014/01/making-virtualbox-nearly-undetectable.html
[20] Adobe Reader, Adobe Flash Player, Microsoft Office 2007, Microsoft Silverlight
[21] http://docs.cuckoosandbox.org/en/latest/installation/guest/

3.3 Obecné vzory v síťové komunikaci

V testovacím prostředí, popsaném v sekci 3.1, bylo analyzováno více než sedm tisíc vzorků crypto-ransomware. Během této analýzy bylo pozorováno několik následujících vzorů chování, které ransomware provádí:

- ověřování připojení k internetu,
- komunikace s blacklistovanými IP adresami a C&C servery,
- zjišťování veřejné IP adresy,
- stahování dodatečný souborů,
- komunikace do sítě TOR,
- posílání HTTP POST check-inů,
- anomálie z pohledu počtu cílových portů,
- skenování portů,
- anomální hodnoty HTTP atributu `User-agent`,
- anomálně vysoký počet komunikačních partnerů,
- anomální počet kontaktovaných zemí,
- anomální počet DNS dotazů,
- periodická odchozí komunikace,
- DNS dotazy na externí servery,
- DNS dotazy na škodlivé servery nebo
- komunikace skrze DNS tunel.

3.3.1 Komunikace s blacklistovanými IP adresami a C&C servery

U mnoha analyzovaných vzorků crypto-ransomware byla detekována komunikace s IP adresami, které se nachází na blacklistech jako jsou:

- ZeuS Tracker, https://zeustracker.abuse.ch/,
- BLOCKLIST.DE, http://www.blocklist.de,
- Spamhaus DROP List, https://www.spamhaus.org/drop/,
- JustSpam.org, http://www.justspam.org/ a další.

Tabulka 3.1: Použitý port během komunikace s C&C serverem.

Cílový port	**Počet ransomware [%]**
80	92,53
110	0,16
443	5,91
7001	0,49
7004	0,16
7008	0,16
8080	0,49
23456	0,08

Tuto komunikaci je možné jednoduše detekovat, jestliže máme k dispozici seznam IP adres, které jsou označeny jako škodlivé. Nevýhodou zůstává, že se na tento blacklist dané IP adresy dostanou až po provedení dynamické analýzy crypto-ransomware a malware je tedy vždy jeden krok napřed. Ve většině případů se jedná o komunikaci s C&C serverem. Jak je možné vidět v tabulce 3.1, drtivá většina této komunikace probíhala přes port `80/tcp`. V některých případech je použit protokol HTTP, ovšem objevily se i crypto-ransomware, které použily jiné protokoly jako například HTTPS V některých případech byl sice použit cílový port č. `80/tcp`, ale nebyl použit protokol HTTP. Ve zhruba šesti procentech případů byl použit protokol HTTPS.

3.3.2 Anomálie z pohledu počtu cílových portů

Během analýzy byl detekován také crypto-ransomware využívající trojský kůň *ZeroAccess*, který používá pro komunikaci s C&C serverem peer-to-peer protokol, který komunikuje skrze port `16464/udp`. Ze síťové komunikace je možné vidět, že se malware snaží komunikovat na tomto portu se zařízeními z celého světa. Velice podobně se choval i dále popsaný malware `WannaCrypt`, který provádí skenování všech veřejně dostupných zařízení v síti Internet na dostupnost otevřeného portu `445/tcp`.

3.3.3 Ověření připojení k internetu

Některé crypto-ransomware provádějí tzv. *connectivity check*, pomocí kterého se snaží zjistit, zda je dané infikované zařízení připojeno k síti Internet. Většina analyzovaných malware tuto kontrolu provádí pomocí zaslaní HTTP dotazů na veřejně známy server u kterého je velice pravděpodobné, že bude vždy dostupný. Některé z analyzovaných crypto-ransomware ovšem provádějí tuto kontrolu i na méně známé servery. V atributu `Host` takových HTTP dotazů se pak většinou nachází:

- google.com,
- www.bing.com,
- www.msn.com,
- www.update.microsoft.com.nsatc.net,
- www.expectr.com,

- survey-winner.net,
- survey-winner.com a další.

Toto chování je velice těžko detekovatelné, pokud nějakým způsobem není abnormální. Příkladem crypto-ransomware, který provádí anomálního ověření připojení k internetu může být například *WannaCrypt*, jehož analýza je blíže popsána v sekci 3.8.

3.3.4 Stahování dodatečný souborů

Některé crypto-ransomware si ze sítě Internet stahují software potřebný pro komunikaci se sítí TOR nebo samotný binární soubor, který provede zašifrování dat. Díky tomu je možné na napadené zařízení dopravit crypto-ransomware na míru. Některé crypto-ransomware například na napadené zařízení stáhnou dokument pro aplikaci Microsoft Word nebo PDF soubor, který poté na infikovaném zařízení spustí, čímž využijí konkrétní zranitelnosti dané aplikace jako je například *Microsoft Word* nebo *Adobe Reader*.

3.3.5 Anomální hodnoty HTTP atributu `User-agent`

Za pomoci IDS systému a existujících signatur bylo jednoduché detekovat crypto-ransomware, které během HTTP komunikace používají nestandardní hodnoty v atributu `User-agent`. Tento atribut většinou identifikuje typ komunikující aplikace, verzi této aplikace případně verzi operačního systému nebo výrobce dané aplikace. Například webový prohlížeč *Chrome*[22] ve verzi 51 používá v tomto atributu následující řetězec:

```
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/51.0.2704.103 Safari/537.36
```

Z tohoto řetězce je možné usoudit, že se jedná o webový prohlížeč spuštěný na operačním systému, který používá 64-bitové linuxové jádro.

Pro command-line aplikaci wget[23] je typicky použit řetězec, který vypadá následovně:

```
Wget/1.14 (linux-gnu)
```

Pokud se malware snaží komunikovat za pomoci HTTP protokolu, pak musí hodnotu tohoto atributu vyplnit. Pro malware je ovšem velice problematické tuto hodnotu aktualizovat, aby se v době síťové komunikace úspěšně maskoval za aplikaci, která je na daném zařízení opravdu nainstalována. Tato činnost je proto dobře detekovatelná pomocí signatur protože, například u webových prohlížečů se tento řetězec s každou novou verzí aktualizuje. Většina malware, a především ty starší, pak v tomto atributu použije podezřelé hodnoty jako je například:

```
Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20130405 Firefox/22.0
```

kde je velice nepravděpodobné, že dané zařízení v roce 2017 používá webový prohlížeč *Firefox*[24] ve verzi 22, která byla vydána v roce 2013. Seznam některých pozorovaných hodnot atributu `User-agent` je možné nalézt v tabulce v příloze F nebo úplný seznam ve složce `data` na datovém médiu.

[22] https://www.google.com/chrome/
[23] https://www.gnu.org/software/wget/
[24] https://www.mozilla.org/en-US/firefox/

3.4 Zjištění veřejné IP adresy

Jeden z prvních kroků, které ransomware dělají, je zjištění veřejné IP adresy napadeného zařízení, pomocí které je poté možné určit přibližnou lokalitu a poskytovatele internetu pro dané zařízení. Lokalita může být použita k zacílení ransomware na konkrétní skupinu uživatelů popřípadě k doručení dešifrovacích instrukcí ve správném jazyce.

Existují varianty crypto-ransomware, které se v některých lokalitách vůbec nespustí. Například crypto-ransomware *Cerber* po spuštění kontroluje, jestli se nenachází v zemích Arménie, Ázerbájdžán, Bělorusko, Georgie, Kyrgystán, Kazachstán, Moldávie, Rusko, Turkmenistán, Tádžikistán, Ukrajina nebo Uzbekistán. Jestliže ano, pak se ihned ukončí.

Některé ransomware jazykovou lokalizaci obcházejí tím, že uživatele odkáží na webovou stránku, která poskytuje aktuální dešifrovací instrukce v několika jazycích, čímž mohou redukovat síťovou komunikaci. Nejčastěji používané služby pro zjištění lokality a veřejné IP adresy jsou ve většině případů on-line dostupné webové služby, které jsou určeny přesně pro tento účel. Mezi tuto služby patří například:

- http://icanhazip.com/,
- http://ip-addr.es/,
- http://icanhazip.com/,
- http://myexternalip.com/raw/,
- http://ipinfo.io/ip/,
- http://whatismyipaddress.com/,
- http://api.wipmania.com/,
- http://whatismyip.akamai.com/,
- http://checkip.dyndns.org/,
- http://ip.3322.net/,
- a další.

Během analýzy se objevily také vzorky, které se snažili tuto očividnou aktivitu skrýt tím způsobem, že si zjišťovali danou IP adresu pomocí webových služeb, které nejsou pro tento účel vytvořeny, ale přesto je pomocí nich možné IP adresu získat. Příkladem může být webové stránka *http://rogers.com/*, což jsou webové stránky kanadské společnosti poskytující bezdrátové kabelové a internetové připojení. Tyto stránky vás podle vaší lokality přesměrují na vybrané stránky podle vašeho umístění a proto si zjišťují vaši veřejnou IP adresu.

Následující příkaz byl spuštěn na počítači, jehož veřejná IP adresa je `46.135.160.254`. Jak je možné z příkladu vidět, po stažení objektu ze stránky `http://rogers.com/`, objekt tuto IP adresu obsahuje.

```
> wget http://rogers.com/ -O - | grep 46.135.160.254
[True-Client-IP] = [46.135.160.254]
[Proxy-Client-IP] = [46.135.160.254, 104.103.73.69]
[X-Forwarded-For] = [46.135.160.254, 104.103.73.69]
```

Automatizovanou analýzou jsem rozpoznal zhruba šest desítek služeb jejichž seznam je možné nalézt v příloze B nebo v souboru `ip-services.list` na datovém médiu, včetně skriptu, který ze zaznamenané síťové komunikace, získá seznam služeb, které mohou být použity pro získání veřejné IP adresy.

Tuto aktivitu je možné dobře popsat pomocí signatur, za předpokladu, že máme seznam služeb, které pro tento účel crypto-ransomware využívají. Nevýhodou tohoto přístupu je skutečnost, že takový seznam je potřeba neustále aktualizovat a je tak vždy jeden krok za autory malware. Jiný způsob detekce této aktivity, včetně jeho nasazení v reálném systému a výsledky z následného experimentování je možné nalézt v sekci 4.1 v kapitole 4.

3.5 Check-in v HTTP metodě POST

Během analýzy bylo pozorováno mnoho vzorků crypto-ransomware, které periodicky zasílají data pomocí HTTP protokolu za použití metody POST. Tyto HTTP dotazy jsou odeslány několikrát během krátkého časového okamžiku a je u nich možné sledovat stejné charakteristické vlastnosti. V rámci analýzy jsem ze všech vzorků, které obsahovaly HTTP dotazy s metodou POST, vyextrahoval následující rysy:

1. cílový port,
2. verze HTTP protokolu,
3. HTTP atribut `Host`,
4. HTTP atribut `URI`,
5. HTTP atribut `Content-type`,
6. HTTP atribut `Method`,
7. HTTP atribut `Content-Length` a
8. HTTP atribut `User-agent`.

Tyto vyextrahovaná data je možné nalézt na datovém médiu ve složce `data/`, viz. příloha A. Tabulka č. 3.2 uvádí vyextrahovaná data jednoho z analyzovaných vzorků.

Vybraný vzorek crypto-ransomware byl spuštěn na virtuálním počítači s IP adresou `192.168.1.11` v čase 19:52:55. Jak je z příkladu možné vidět, malware během pár sekund komunikuje s **pěti** rozdílnými IP adresami za použití protokolu **HTTP** na standardní cílový port číslo `80/tcp`. Všechny HTTP zprávy u tohoto vzorku používají stejnou metodu **POST**. Malware pro komunikaci používá doménové jména namísto IP adres, kde všechny kontaktované domény byly dne 14.4.2017 bezpečnostními společnostmi[25] vyhodnoceny jako nedůvěryhodné. Z tabulky je dále patrné, že u všech dotazů je použita stejná hodnota HTTP atributů `Uri`, `Content-type` a `User-agent`. Různé crypto-ransomware používají v atributu `User-agent` různé hodnoty, a je možné pozorovat vzor, kdy vybraný malware používá stejnou hodnotu u všech HTTP zpráv.Všechny dotazy mají stejnou velikost dat i když data mají rozdílný obsah. V rámci časové osy je možné pozorovat, že všechny dotazy jsou odeslány v rámci několika málo sekund.

[25] mezi tyto společnosti patří např.: Fortinet, AlienVault, BitDefender, ESET, Google Safebrowsing a další

Čas	19:52:55.53	19:52:56.26	19:52:57.67	19:52:58.67
Zdrojová IP	192.168.1.11			
Cílová IP	160.153.49.102	208.100.26.234	50.31.14.17	199.79.63.153
Cílový port	80			
Verze protokolu	HTTP/1.1			
Metoda	POST			
Host	toolaria.com	diwali2k15.in	samuday.org	maxmpl.com
URI	/sysstr.php			
Content-type	application/x-www-form-urlencoded			
Content-length	645			
User-agent	Mozilla/5.0 (Windows NT 6.3 rv:11.0) like Gecko			

Tabulka 3.2: Čtyři POST dotazy crypto-ransomware

V rámci analýzy vyextrahovaných dat bylo dále zjištěno, že některé vzorky pro kontaktování vzdáleného serveru používají pouze IP adresu, tj. IP adresa je uvedena v HTTP atributu `Host`. V takovém případě se pak většinou u všech POST HTTP dotazů v atributu `URI` objeviví stejné hodnota.

U některých POST dotazů je možné pozorovat použití stejné hodnoty atributu `URI` ovšem jiných hodnot atributu `Host`. Příkladem tohoto chování je také příklad z tabulky č. 3.2.

Některé crypto-ransomware používají hodnoty atributu `URI`, ve kterých je možné pozorovat vzorky, které je možné dobře zachytit pomocí IDS signatur. Příkladem dotazů používající `URI` obsahující vzor zobrazuje následující příklad:

```
/img3.php?b=gndwsifrqy60ox
/img3.php?r=gndwsifrqy60ox
/img2.php?m=gndwsifrqy60ox
```

Zachycení této `Uri` je možné např. pomocí následující pseudo-signatury:

```
/img[0-9].php?[a-z]=gndwsifrqy60ox
```

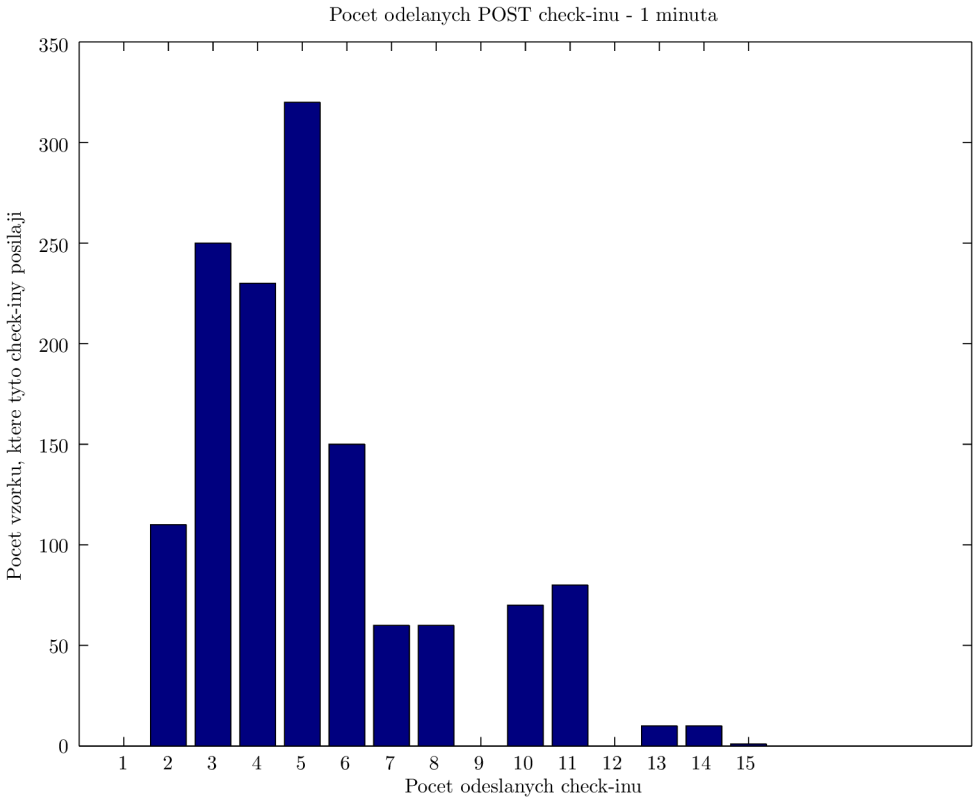
Jiným příkladem může být crypto-ransomware obsahující vzor v atributech `Host` a `Uri`, který je možné vidět v následujícím výčtu.

```
Host: bolexserv10.com Uri: /topem7/image.php
Host: bolexserv20.com Uri: /topem7/image.php
Host: bolexserv30.com Uri: /topem7/image.php
Host: bolexserv40.com Uri: /topem7/image.php
Host: bolexserv50.com Uri: /topem7/image.php
Host: bolexserv60.com Uri: /topem7/image.php
Host: bolexserv10.com Uri: /topem7/image.php
```

Pro výše uvedené příklady je opět typické, že všechny POST dotazy jsou cíleny na stejný vzdálený port a používají stejné hodnoty atributů `Content-Type`, `Content-Length` a `User-Agent`.

Jako cílový port je ve většině případů použit standardní port číslo `80/tcp` ovšem našly se i vzorky, které používají port `8080/tcp` nebo tunelují HTTP komunikaci skrze port `443/tcp`. Co se týče verze HTTP protokolu, bylo pozorováno rovnoměrné použití jak verze 1.0, tak 1.1.

Na obrázku č. 3.2 je zachycen počet HTTP check-inů, které crypto-ransomware posílají v čase. Osa x reprezentuje počet HTTP POST check-inů, které ransomware odeslal v první minutě své síťové komunikace. Osa `y` poté reprezentuje počet vzorků, které odesílají stejný počet těchto check-inů. Z obrázku je patrné, že ransomwary posílají v první minutě od dvou do patnácti těchto check-inů, kde nevíce vzorků jich nejčastěji stihne poslat právě pět. Během experimentování s detektory tohoto chování se nejvíce osvědčilo použít hodnotu 3, tj. detekovat toto chování pokud se v komunikaci vyskytnou nejméně 3 a více HTTP POST zpráv.



Obrázek 3.2: Počet HTTP POST zpráv.

Na základě znalostí získané z této analýzy jsem dále implementoval pomocné skripty, hledající toto chování v reálném síťovém provozu. Výsledky těchto experimentů, popis a návrh detektorů tohoto typu chování se dále zaobírá sekce 4.2 v kapitole 4.

3.6 Analýza DNS dotazů

Některé crypto-ransomware používají pro komunikaci s C&C serverem DNS tunel, tj. komunikují na cílový port č. `53/udp`, ovšem bez použití DNS protokolu. Tuto komunikaci je

dnes možné velice dobře detekovat pomocí IDS signatur nebo znalostí IP adres lokálních serverů v monitorované síti.

3.6.1 DNS dotazy na externí servery

Během analýzy DNS dotazů se ukázalo, že některé crypt-ransomware posílají DNS dotazy na DNS servery, které nejsou nastaveny na infikovaném zařízení. Většinou jsou použity veřejně dostupné DNS servery společnosti *Google*, tj. servery na IP adresách `8.8.8.8` nebo `8.8.4.4`. Dále se také objevují DNS dotazy, které jsou směřovány na servery na IP adresách `194.165.17.3`, `22.71.154.156` nebo `194.165.17.4`. Tyto IP adresy nebyly ke dni 16. dubna 2017 žádnou z bezpečnostních společností označeny jako škodlivé. Toto chování se také objevuje ve spojitosti s posíláním dat skrze DNS tunel. Tímto způsobem je také možné obejít detekci DNS dotazů na infikované servery, jestliže je v monitorované podsíti nasazeno nějaké bezpečnostní řešení, které je schopno detekovat pokus o přeložení podezřelé domény.

3.6.2 Náhodně vygenerované doménové jména

Analýza ukázala, že některé crypto-ransomware používají pro komunikaci s C&C serverem přímo IP adresu, jiné používají náhodně vygenerované doménové jméno a techniku zvanou *Domain Fluxing*. Předpokládejme, že DGA[26] algoritmus, který je v crypto-ransomware použit, je schopen vygenerovat 50 000 různých doménových jmen. Autorovi malware poté stačí každý den zaregistrovat pouze jedno z těchto doménových jmen. Malware poté postupně generuje náhodné domény a snaží se je pomocí DNS protokolu přeložit. V případě úspěšného překladu může začít s daným serverem komunikovat.

Pomocí statické analýzy konkrétního vzorku crypto-ransomware je možné zanalyzovat použitý algoritmus pro generování náhodných domén. Díky této analýze je poté možné vytvořit seznam doménových jmen, které je daný vzorek schopen vygenerovat. Na základě tohoto seznamu poté může vzniknout signatura, která může zachytit doménu, kterou daný vzorek vygeneroval a pokusil se přeložit na IP adresu.

3.7 Interakce uživatele

V okamžiku kdy crypto-ransomware dokončí svojí činnost, tj. úspěšně zašifruje uživatelská data, pak je po uživateli vyžadováno výkupné. Jak bylo zmíněno v sekci 2.4, toto výkupné je ve většině případů vyžadováno formou virtuální kryptoměny Bitcoin. Uživateli jsou většinou poskytnuty velice detailní instrukce o tom, jak platbu provést a to v i několika světových jazycích. Některé typy crypto-ransomware také poskytují odkazy na informace o kryptografických algoritmech, které byly použity pro zašifrování dat.

V některých případech je postižený uživatel odkázán na skrytou službu, tzv. *Onion Service*, přístupnou pouze v síti TOR. URL adresa takové služby je charakteristická svojí doménou nejvyšší úrovně `.onion`. Uživatelům napadených systémů je poté sděleno, že k takové službě mohou přistoupit dvěma způsoby:

1. využít proxy službu *Tor2web*[27] nebo
2. použít *Tor Browser*[28].

[26] Domain generation algorithm
[27] https://tor2web.org/
[28] https://www.torproject.org

3.7.1 Tor2web

On-line služba Tor2web slouží jako webová proxy do sítě TOR, pomocí které je možné přistoupit ke skrytým službám v síti TOR bez instalace dalšího software. Tuto službu crypto-ransomware jednak nabízejí jako jednu z možností jak přistoupit do sítě TOR. Některé crypto-ransomware tuto službu zároveň používají ke komunikaci se svými C&C servery. Tor2web je tedy možné chápat jako prostředníka mezi skrytými službami v síti TOR a uživateli v síti Internet. Jelikož tato služba poskytuje jednostrannou anonymitu[29] a nevyžaduje instalaci žádného dodatečného software, je přirozenou volbou pro tento typ malware.

3.7.2 Tor Browser

Jako druhou možnost crypto-ransomware instruují uživatele ke stažení prohlížeče Tor Browser. Tento prohlížeč umožňuje automaticky směrovat veškerý síťový provoz skrze síť TOR. Uživatel je ve většině případů instruován tento prohlížeč stáhnout z oficiálních webových stránek projektu TOR.

Na skryté službě se poté většinou nachází webová stránka na které si uživatel může zaplatit za tzv. *dekryptor*, který následně může použít pro rozšifrování svých dat. Uživatel je většinou vyzván k vytvoření Bitcoin peněženky, převedení dostatečného množství peněz na tuto peněženku a následné zaslání určitého množství Bitcoinů na uvedenou Bitcoin adresu.

Ransomware také často nabízí seznam možných služeb, kde je možné si bezplatně Bitcoin peněženku vytvořit, přesouvat Bitcoiny z jedno účtu na jiný nebo jednoduše převést jinou měnu na Bitcoin. Mezi doporučované služby většinou patří:

- https://coincafe.com,
- https://bitquick.co,
- https://btcdirect.eu,
- a další

Sekce 4.3 v kapitole 4 se poté zabývá možnými způsoby detekce uživatelského chování při snaze o zaplacení výkupného.

3.8 WannaCrypt

Crypto-ransomware *WannaCrypt* masivně zaútočil dne 12. května 2017. Tento nový malware využívá zranitelnosti *SMBv1*[30] protokolu. I když pro tuto zranitelnost byla dne 14. Března 2017 vydána bezpečnostní záplata, stále bylo ke dni 12. května k sítí Internet připojeno mnoho zařízení, které tuto zranitelnost obsahují. Tento crypto-ransomware je také označován pod názvy *WannaCry, WanaCrypt0r, WCrypt nebo WCRY*. Jelikož se jednalo o aktuální hrozbu v době dokončování této diplomové práce, rozhodl jsem se přidat jednu sekci o detailnější analýze tohoto crypto-ransomware.

Po spuštění binárního souboru se malware nejprve snaží kontaktovat následující doménu

`www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com`

[29] je zaručena pouze anonymita služby, na kterou uživatel přistupuje
[30] Server Message Block, https://en.wikipedia.org/wiki/Server_Message_Block

na portu č. `80/tcp`. Jestliže se mu tuto doménu kontaktovat podaří, pak okamžitě ukončí svojí činnost a nedojde k žádné další síťové komunikaci ani samotnému šifrování souborů na infikovaném zařízení. Tato doména byla identifikována jedním z bezpečnostních analytiků a později označena jako tzv. *kill switch*. Doména byla také v brzké době zaregistrována a díky tomu bylo zabráněno masivnějšímu rozšíření toho crypto-ransomware. Dne 15. května se již internetem šířila modifikovaná varianta tohoto crypto-ransomware, který tento kill switch neobsahovala.

Při prvním spuštění analyzovaného vzorku je možné vidět, že se výše zmíněné doménové jméno přeložilo na Kanadskou IP adresu `144.217.254.3`. Zablokování této konkrétní IP adresy na firewallu ovšem nevedlo k další úspěšné analýze, jelikož už je dnes tato doména přeložitelná na více IP adres. Ve vytvořeném testovacím prostředí, které je blíže popsáno v sekci 3.1, se nachází DNS cache a je tedy možné ovlivňovat DNS dotazy a odpovědi. Při analýze tedy stačí do DNS cache přidat DNS záznam, který pro výše uvedené doménové jméno vrátí neexistující IP adresu v lokální síti, tímto nikdy nedojde k navázání HTTP spojení na vrácenou IP adresu a malware tak pokračuje ve své činnosti.

Mezi další kroky, které WannaCrypt vykoná, je ověření přípojení k internetu. Tuto kontrolu provedl zajímavým způsobem, kdy se pokouší přistoupit k serveru `www.youtube.com`. Tento video sdílející server je dnes velmi populární a proto připojení k tomu serveru za normálních okolností nevzbudí žádné podezření. I když tento server již nějakou dobu neběží na portu č. `80/tcp`, malware přesto tento port použije. Pravděpodobně proto, aby dané chování odpovídalo chování uživatele, který běžně do vyhledávacího pole prohlížeče napíše pouze řetězec `youtube.com`. V takovém případě dojde k automatickému přesměrování na port č. `443/tcp`. V síťové komunikaci ransomware WannaCrypt ovšem k žádnému takovému přesměrování nedojde. Malware zahájí komunikaci na daný server posláním prního SYN paketu a po vrácení prvního ACK[31] paketu od vzdáleného serveru WannaCrypt ukončí komunikaci FIN[32] paketem a dále se vzdáleným serverem nekomunikuje.

Následně malware začne skenovat interní síť ve které se nachází. Konkrétně hledá otevřený port č. `445/tcp`, který bývá ve výchozím nastavení na některých systémech Windows otevřený. Jestliže na síti najde zařízení, která tento port mají otevřený, pokusí se zneužít zranitelnosti CVE-2017-0145[33], která umožňuje vzdálené spuštění kódu. WannaCrypt je díky této zranitelnosti schopný se na tyto systémy rozšířit a následně sám sebe znovu spustit a šířit se tedy na další zranitelné systémy.

Jakmile WannaCrypt provede skenování portu č. `445/tcp` v interní síti, začne provádět stejnou aktivitu ovšem nyní globálně. Malware začne skenovat všechny veřejně dostupná zařízení v síti Internet na otevřený port č. `445/tcp`. Během pěti minut infikované zařízení kontaktovalo více než čtyři tisíce zařízení ve 175 zemích včetně České Republiky. Malware je schopen se tedy šířit nejen lokální sítí ale také globálně na libovolné zařízení, kde by mohl zranitelnosti protokolu Samba využít. V testovacím prostředí, které je blíže popsané v sekci 3.1, byly dále zapojeny zařízení s operačními systémy *Windows XP* a *Windows 7*. Oba z těchto systému byly napadeny a dále se pokoušely daný malware šířit. Na obrázku 3.3 je možné vidět, jak malware začal postupně komunikovat se zařízeními po celém světě. Obrázek zobrazuje prvních sto komunikačních partnerů, kdy infikované zařízení je možné vidět nahoře s IP adresou `192.168.1.13`. U každého vzdáleného zařízení provádělo infikovaného zařízení pouze skenování portu č. `445/tcp`, takže datové přenosy se pohybovaly v rámci několika kilobajtů.

[31] https://www.ietf.org/rfc/rfc793.txt
[32] https://www.ietf.org/rfc/rfc793.txt
[33] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0145

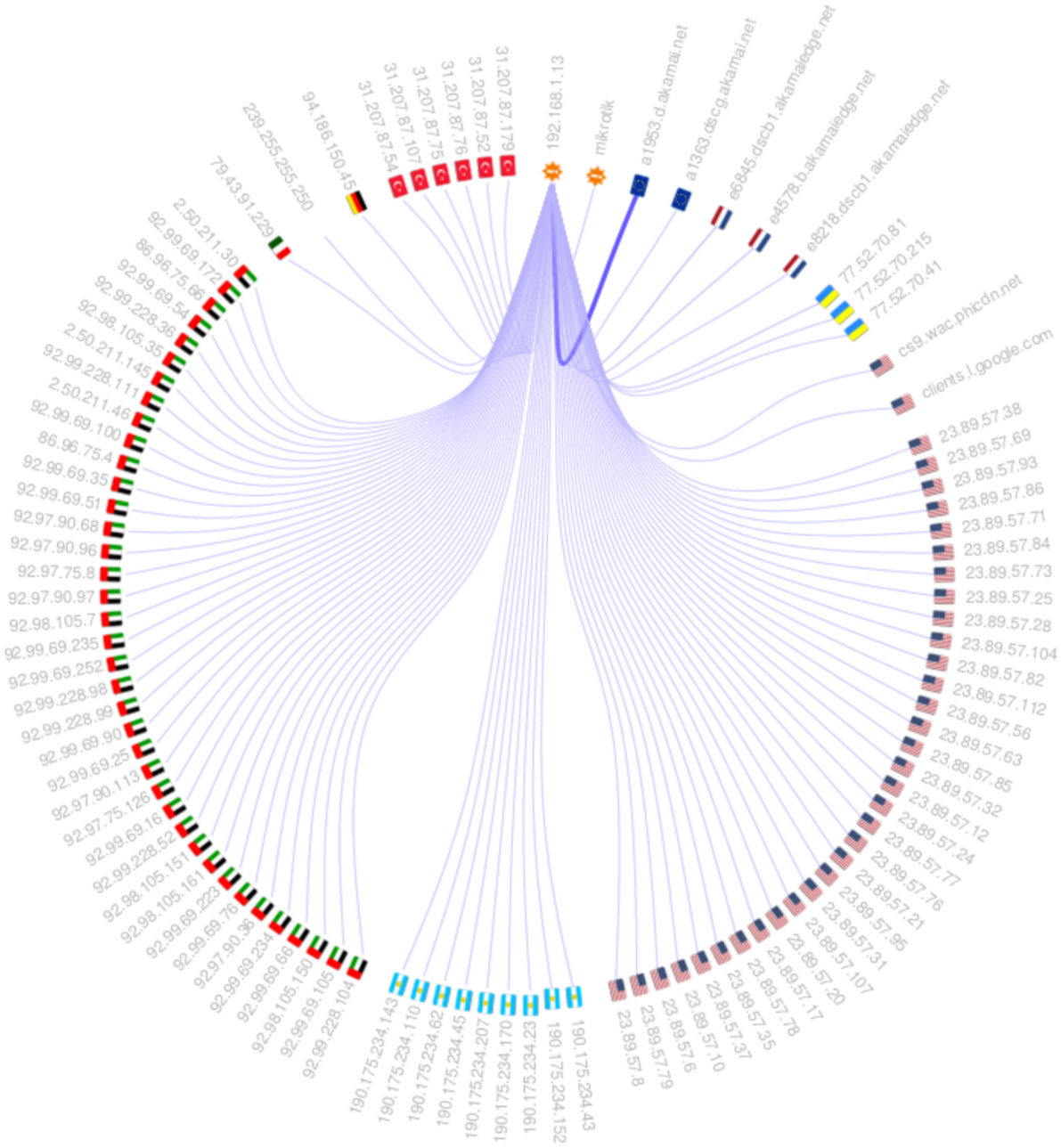
Samotný proces šifrování dat započne v rámci několika málo sekund. Pro uživatele je poté na pracovní ploše zanechán spustitelný soubor *—HOW_TO_DECRYPT—*, který uživateli poskytne potřebné informace o velikosti požadovaného výkupného, adresu Bitcon peněženky, použitý šifrovací algoritmus a čas, do kterého je potřebné dané výkupné zaplatit.

Během pozorování síťové komunikace byla také zachycena komunikace se serverem www.torproject.org, konkrétně s hostem dist.torproject.org. Zde je možné stáhnout software potřebný pro komunikaci se sítí TOR, který poté WannaCrypt zřejmě použije pro kontaktování C&C serveru v síti TOR. Tento malware je schopen zašifrovat nejen lokální soubory, ale také veškeré síťové disky, které jsou k infikovanému zařízení připojeny.

Část této analýzy byla publikována na českém webu http://www.zive.cz[34] a dále byla otištěna v magazínu *Cyber Defense Magazine*[35].

[34] http://www.zive.cz/bleskovky/experti-z-brnenskeho-greycortexu-wannacry-nas-prekvapil-svou-agresivitou-v-siti/sc-4-a-187674/default.aspx

[35] http://www.cyberdefensemagazine.com/detection-of-wannacry-ransomware-based-on-network-behavior/



Obrázek 3.3: Skenování zařízení po celém světě

Kapitola 4

Implementace a experimentování

Tato kapitola se zabývá návrhem a popisem implementace detektorů, které detekují některé vybrané vzorky chování, jejichž analýza a popis se nachází v předchozí kapitole. Tyto detektory experimentálně implementovány v systému MENDEL od společnosti Greycortex. Poté byly poté otestovány v reálném prostředí kde se síťový provoz pohyboval v průměru kolem 480Mb/s. Prostředí obsahovalo zhruba 380 různých síťových zařízení mezi které spadaly servery, osobní počítače, notebooky, chytré telefony, tablety a další.

4.1 Detekce zjištění veřejné IP adresy

V kapitole 3 v sekci 3.4 bylo popsáno, proč a jakým způsobem si crypto-ransomware zjišťují veřejnou IP adresu a jakým způsobem je možné tuto aktivitu odhalit pomocí IDS signatury obsahující řetězce reprezentující použitou službu.

Jiným řešením se může nabízet využít znalosti veřejných IP rozsahů adres sítě, ve které chceme tuto aktivitu detekovat. Předpokládejme systém, který má k dispozici veškerou síťovou komunikaci v prostředí ve kterém je nasazen a má znalost veřejných IP rozsahů, které toto prostředí využívá. S touto znalostí poté může vytvořit dynamická pravidla pro detekční systém, který může tyto informace v obsahu paketů vyhledávat, čímž je možné se vyhnout spravování webových služeb, které informaci o veřejné IP adrese poskytují. Předpokládejme, že máme síť, která má veřejnou IP adresu `51.30.202.192`. Pak následující dynamická signatura zobrazuje pravidlo v jazyce Snort[1], pomocí kterého je možné detekovat aktivitu zjištění této veřejné IP adresy:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET any ( msg:"policy: Internal
Host Retrieving External IP 51.30.202.192 in the payload - Possible
Infection"; flow:established,from_server; content:"|35 31 2e 33 30
2e 32 30 32 2e 31 39 32|"; fast_pattern; priority:2;
classtype:attempted-recon; sid:1900000002; rev:1;}
```

Implementovanou signaturu jsem sledoval po dobu jednoho týdne, během kterého zaznamenala více než dva tisíce událostí. Z těchto dvou tisíc událostí bylo objeveno jedno infikované zařízení, které zjišťovalo svoji veřejnou IP adresu z domény *dbctr.gq* s cílovou IP adresou `212.61.180.100`, která se v té době nacházela na blacklistu *Emerging Threats: Trojan*.

[1] http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

Analýza nalezených událostí ukázala, že zjišťování veřejné IP adresy provádí mnoho aplikací, které v drtivé většině případů používaly protokol `80/http`, v ojedinělých případech poté `25/smtp`, nebo `5222/xmpp`. Mezi příklady těchto služeb patří například následující:

- Služba *gmail-smtp-relay.l.google.com*, kterou používají např. tiketovací systémy[2] pro rozesílaní změn v daných tiketech skrze e-mailové účty společnosti Google.
- Antivirus *Avast* zjišťuje tuto informaci pomocí služby *ip-info.ff.avast.com*. Tato služba vrátí nejenom vaši veřenou IP adresu, ale také název poskytovale vašeho internetového připojení včetně přibližné polohy. Nálsledující text ukazuje informace, které je možné z tého služby ve formátu json získat. Veřejná IP adresa byla převedena na privátní IP adresu `10.0.0.1`, kvůli anonymitě sítě, kde byly navržené detektory testovány.

```
{
"ip":"10.0.0.1",
"continent":"Europe",
"country":"CZ",
"subdivisions":[
 "64",
 "642"
],
"city ":"Brno",
"timezone":"Europe/Prague",
"latitude":49.2,
"longitude":16.6333,
"isp":"CESNET z.s.p.o.",
"asnNumber":2852,
"asnOrganizatio n":"CESNET z.s.p.o.",
"organizati on":"CESNET z.s.p.o."
}
```

- Služba *geoip.ubuntu.com*, kterou používají Linuxové distibuce Ubuntu je schopná získat obdobné informace jako antivirus Avast.
- Google updater v prohlížečích *Chrome* při použití služby *redirector.gvt1.com*.
- VPN software nebo VPN doplňky do webových prohlížečů sloužících pro anonymizaci uživatele. Příkladem může být například doplněk *Hola VPN*[3] pro prohlížeč Chrome.
- Mnoho dalších služeb jejichž seznam je možné nalézt v příloze C a úplný seznam v souboru `public-ip.list` na datovém médiu.

Zjišťování své veřejné IP adresy také často provádí mobilní telefony, kde některé přenáší tuto informaci nešifrovaně skrze port č. `443/tcp`. Následující úryvek XML kódu uvádí část paketu obdrženého z domény *app02.nodes.gslb.mi-idc.com*. telefonem Xiaomi. Veřejná IP adresa byla opět zanonymizována na privátní IP adresu `10.0.0.1`.:

[2] příkladem může být např. *JIRA Software* od společnosti *Atlassian*

[3] https://chrome.google.com/webstore/detail/unlimited-free-vpn-hola/gkojfkhlekighikafcpjkiklfbnlmeio?hl=en

```
<?xml version='1.0'?>
 <stream:stream xmlns='xm' xmlns:stream='xm'from='xiaomi.com'
 challenge='3305390891' ip='10.0.0.1' host='52a6' ps=" ...
```

Z výsledků implementované detekční metody je patrné, že zjištění veřejné IP adresy nebo lokality je velmi jednoduché zamaskovat např. pod antivirový software, linuxovou distribuci nebo webové doplněk a může být tedy velmi obtížně detekovatelné, zda se jedná o legitimní aktivitu či nikoliv.

Tato detekční metoda se sama o sobě v praxi neukázala jako velice použitelná, pokud stavíme detekci pouze na síťové komunikaci. Pokud ovšem tuto metodu použijeme s dalšími detekčními metodami, pak nese hodnotnou informaci.

4.2 Detekce HTTP POST check-inů

Z analýzy HTTP zpráv popsané v sekci 3.5 vyplynulo, že crypto-ransomware, které posílají check-in v HTTP zprávě mění pouze tři proměnné. Tyto proměnné jsou **cílová adresa** a HTTP atributy jako jsou `Host` a `Uri`. Ostatní HTTP atributy atributy `Version`, `Method`, `Content-type`, `Content-length` nebo `User-agent` jsou vždy u všech dotazů stejné. Z této analýzy také vyplynulo, že průměrný vzorek crypto-ransomware, který disponuje tímto chování, pošle 3 takové HTTP zprávy v rámci jedné minuty. Na tyto tři proměnné je možné se podívat jako na domény. Tyto domény jsou reprezentovány množinami D, H a U následovně:

$D = \{stejneIP, ruzneIP\}$
$H = \{stejneIP, stejneDomeny, kombinaceIPdomena, ruzneIP, ruzneDomeny\}$
$U = \{stejneUri, ruzneUri\}$

Doména D představuje možné hodnoty cílové IP adresy pro HTTP zprávy, kde:

- $stejneIP$ - reprezentuje situaci, kdy všechny HTTP zprávy obsahují stejnou jednu IP adresu,
- $ruzneIP$ - reprezentuje situaci, kdy HTTP zprávy obsahují různé IP adresy.

Doména H představuje možné hodnoty HTTP atributu `Host` pro HTTP zprávy, kde:

- $stejneIP$ - reprezentuje situaci, kdy všechny HTTP zprávy obsahují stejnou jednu IP adresu,
- $stejneDomeny$ - reprezentuje situaci, kdy HTTP zprávy obsahují stejné jedno doménové jméno,
- $kombinaceIPdomena$ - reprezentuje situaci, kdy HTTP zprávy obsahují kombinaci IP adresy a doménového jmena,
- $ruzneIP$ - reprezentuje situaci, kdy HTTP zprávy obsahují různé IP adresy,
- $ruzneDomeny$ - reprezentuje situaci, kdy HTTP zprávy obsahují různé doménové jména.

Poslední doména, která je označena písmenem U, reprezentuje množinu charakterizující HTTP atribut `Uri`. Tato atribut může nabýt pouze dvou hodnot:

- *stejneUri* - reprezentuje situaci, kdy všechny HTTP zprávy obsahují v atributu `Uri` stejnou jednu hodnotu,
- *ruzneUri* - reprezentuje situaci, kdy HTTP zprávy obsahují v atributu `Uri` různé hodnoty.

Jestliže nad danými množinami provedeme kartézský součin[4], který definujeme vztahem 4.1, pak získáme uspořádané trojice.

$$D \times H \times U = \{(d, h, u) : d \in D \wedge h \in H \wedge u \in U\} \tag{4.1}$$

Tyto uspořádané trojice poté reprezentuje tabulka č. 4.1, která definuje 20 různých vzorů. Pro klasifikaci se pak sledují kombinace v podobě kartézského součinu a klasifikátor pro tyto hodnoty určuje třídu do které crypto-ransomware patří. U ostatních sledovaných HTTP atributů jako jsou `Host`, `Uri`, `Content-type`, `Content-length` nebo `User-agent` se očekává stejná hodnota v rámci všech odeslaných HTTP zpráv. Dále se předpokládá, že všechny zprávy jsou odesílány na stejný cílový port. Řádek 1 z tabulky 4.1 například reprezentuje detektor, který hledá HTTP zprávy, kde všechny zprávy mají:

- stejnou zdrojovou IP adresu,
- stejnou cílovou IP adresu,
- v atributu `Host` uvedeno stejné doménové jméno a
- v atributu `Uri` uvedenou stejnou hodnotu.

Tabulku č. 4.1 je možné dále minimalizoval. Řádek 1 a řádek 4 z tabulky č. 4.1 reprezentují check-in, které mají v atributu `Host` u všech zpráv buď stejné IP adresy nebo stejné doménové jména. Zda crypto-ransomware použije v tomto atributu IP adresu nebo doménové jméno není z pohledu detekce podstatné. Důležitou informací je, že malware u vše check-inů v tomto atributu použije stejnou hodnotu. I když použití IP adresy je z pohledu běžného uživatele samo o sobě podezřelé, jelikož většina běžných uživatelů nebo ostatních služeb použije k přístupu na webový server doménové jméno. Podobný předpoklad můžeme aplikovat také na různé IP adresy nebo různé doménové jména. Pod tento předpoklad je možné také zahrnout variantu, kdy se v atributu `Host` objeví kombinace jak doménového jména, tak IP adresy.

Na základě tohoto předpokladu jsem tedy sjednotil zmíněné řádky z tabulky č. 4.1 do nové tabulky č. 4.2, která definuje 8 tříd **A-H**, kdy klasifikátor poté určuje, do které třídy daný crypto-ransomware patří. Jestliže tedy klasifikátor vyhodnotí, že se jedná o crypo-ransomware třídy G, pak malware posílá HTTP POST check-in na různé IP adresy, v HTTP atributu `Host` se vyskytují různé hodnoty ovšem v atributu `Uri` se vyskytují stejné hodnoty. Další sekce poté popisuje, které z těchto tříd chování se vyskytují v síťové komunikaci crypto-ransomware a které je možné zachytit v běžné síťové komunikaci.

4.2.1 Experimentování nad crypto-ransomwary

Na základě analýzy a úvahy provedené v sekci 3.5 jsem vytvořil skript napsaný v jazyce Python[5], který hledá v pcap souboru právě taková chování, která popisují třídy A-H z

[4] https://cs.wikipedia.org/wiki/Kart%C3%A9zsk%C3%BD_sou%C4%8Din
[5] https://www.python.org/

Tabulka 4.1: Trojice kartézského součinu množin D, H a U

Řádek	Cíl. IP	Host	Uri
1	stejneIP	stejneIP	stejneUri
2	stejneIP	stejneIP	ruzneUri
3	stejneIP	stejneDomeny	stejneUri
4	stejneIP	stejneDomeny	ruzneUri
5	stejneIP	kombinaceIPdomena	stejneUri
6	stejneIP	kombinaceIPdomena	ruzneUri
7	stejneIP	ruzneIP	stejneUri
8	stejneIP	ruzneIP	ruzneUri
9	stejneIP	ruzneDomeny	stejneUri
10	stejneIP	ruzneDomeny	ruzneUri
11	ruzneIP	stejneIP	stejneUri
12	ruzneIP	stejneIP	ruzneUri
13	ruzneIP	stejneDomeny	stejneUri
14	ruzneIP	stejneDomeny	ruzneUri
15	ruzneIP	kombinaceIPdomena	stejneUri
16	ruzneIP	kombinaceIPdomena	ruzneUri
17	ruzneIP	ruzneIP	stejneUri
18	ruzneIP	ruzneIP	ruzneUri
19	ruzneIP	ruzneDomeny	stejneUri
20	ruzneIP	ruzneDomeny	ruzneUri

Tabulka 4.2: Minimalizovaná trojice kartézského součinu

	Cíl. IP	Host	Uri	Třída	Cíl. IP	Host	Uri
1	stejneIP	stejneIP	stejneUri	**A**	stejneIP	stejnaHodnota	stejneUri
3	stejneIP	stejneDomeny	stejneUri				
2	stejneIP	stejneIP	ruzneUri	**B**	stejneIP	stejnaHodnota	ruzneUri
4	stejneIP	stejneDomeny	ruzneUri				
11	ruzneIP	stejneIP	stejneUri	**C**	ruzneIP	stejnaHodnota	stejneUri
13	ruzneIP	stejneDomeny	stejneUri				
12	ruzneIP	stejneIP	ruzneUri	**D**	ruzneIP	stejnaHodnota	ruzneUri
14	ruzneIP	stejneDomeny	ruzneUri				
5	stejneIP	kombIPdomena	stejneUri	**E**	stejneIP	ruzneHodnoty	stejneUri
7	stejneIP	ruzneIP	stejneUri				
9	stejneIP	ruzneDomeny	stejneUri				
6	stejneIP	kombIPdomena	ruzneUri	**F**	stejneIP	ruzneHodnoty	ruzneUri
8	stejneIP	ruzneIP	ruzneUri				
10	stejneIP	ruzneDomeny	ruzneUri				
15	ruzneIP	kombIPdomena	stejneUri	**G**	ruzneIP	ruzneHodnoty	stejneUri
17	ruzneIP	ruzneIP	stejneUri				
19	ruzneIP	ruzneDomeny	stejneUri				
16	ruzneIP	kombIPdomena	ruzneUri	**H**	ruzneIP	ruzneHodnoty	ruzneUri
18	ruzneIP	ruzneIP	ruzneUri				
20	ruzneIP	ruzneDomeny	ruzneUri				

Tabulka 4.3: Procentuální počet výskytů konkrétních chování

Cíl. IP	Host	Uri	Třídy	Počet výskytů [%]
stejné-IP	stejná hodnota	stejné-URI	A	23,728813559322
stejné-IP	stejná hodnota	různé-URI	B	0
různé-IP	stejná hodnota	stejné-URI	C	1,69491525423729
různé-IP	stejná hodnota	různé-URI	D	0
stejné-IP	různé hodnoty	stejné-URI	E	0
stejné-IP	různé hodnoty	různé-URI	F	0
různé-IP	různé hodnoty	stejné-URI	G	49,1525423728814
různé-IP	různé hodnoty	různé-URI	H	25,4237288135593

tabulky č. 4.2. Při implementaci jsem zvolil Python modul dpkt[6], který poskytuje rychlé zpracování paketů s průběžným uvolňováním paměti, což umožňuje zpracovávat i pcap soubory o velikost několika terabajtů. Zmíněný skript implementuje detektory hledající jednotlivé třídy chování A-H. Vstupem tohoto skriptu je soubor se zaznamenanou síťovou komunikací a jednopísmenná třída chování, které se má v daném souboru hledat.

Implementované detektory byly nejprve otestovány na síťové komunikaci vzorků crypto-ransomware, které byly analyzovány v prostředí popsaném v sekci 3.1. Díky této analýze bylo možné zjistit, jaké chování se u analyzovaných vzorků nejčastěji vyskytuje. Výsledky tohoto experimentu blíže popisuje tabulka č. 4.3.

Jak je možné z této tabulky vidět, nejvíce crypto-ransomware spadá do třídy G. Ransomware spadající do této třídy posílají HTTP POST check-in na různé cílové IP adresy, s použitím různých hodnot v HTTP atributu `Host` a se stejnou hodnotou v atributu `Uri`. Toto chování bylo detekováno u 49% vzorků, které posílaly check-in pomocí HTTP zpráv za použití metody POST. Konkrétní případ těchto zpráv jednoho ze vzorků crypto-ransomware je zachycen v tabulce 4.4. Z této tabulky je patrné, že vzorek odesílá v první minutě své komunikace pět HTTP POST check-inů na různé cílové IP adresy a stejný standardní cílový port č. **80**. U všech check-inů byla použita stejná hodnota atributu `Uri`, tj. `/userinfo.php`. Ostatní sledované HTTP atributy měly u všech pěti zpráv stejné následující hodnoty:

- `Version: HTTP/1.0`,
- `Content-length: 388`,
- `Content-type: application/x-www-form-urlencoded`,
- `User-agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.2)`.

Druhým nejčastějším chováním, které se v crypto-ransmoware vyskytuje zhruba ve 26% případů je chování třídy H popsané v tabulce č. 4.3. U tohoto typu chování se check-in posílají na různé cílové IP adresy za použití různých hodnot v HTTP atributech `Host` a `Uri`. Konkrétní případ těchto zpráv jednoho ze vzorků crypto-ransomware je zachycen v tabulce 4.5.

Z této tabulky je možné vidět, že vzorek v první minutě komunikace odesílá tři HTTP POST check-in na různé cílové IP adresy a stejný standardní cílový port č. `80`. U všech

[6] https://dpkt.readthedocs.io/en/latest/

Tabulka 4.4: Příklad ransomware s chováním třídy G

Cíl. IP	Host	Uri
217.12.199.151	217.12.199.151	/userinfo.php
149.202.109.202	149.202.109.202	/userinfo.php
208.100.26.234	tkunqwsyg.pw	/userinfo.php
217.12.199.151	217.12.199.151	/userinfo.php
149.202.109.202	149.202.109.202	/userinfo.php

Tabulka 4.5: Příklad ransomware s chováním třídy H

Cíl. IP	Host	Uri
23.253.126.58	camelinsuration2.com	/v1.0.1/?v=2.0&c=1194028296
146.185.155.126	146.185.155.126	/v1.0.1/?v=2.0&c=1194023296
87.106.18.112	hamburdtversignablouonee.com	/v1.0.1/?v=2.0&c=1194086796

check-inů byla použita různá hodnota atributu `Host`, kde se objevilo jak použití doménového jména, tak použití IP adresy. Ve sloupci `Uri` je možné vidět řetězce, které na první pohled vypadají stejně, ale při bližším pohledu je možné si všimnout, že se liší. Ostatní sledované HTTP atributy měly u všech tří zpráv stejné následující hodnoty:

- `Version: HTTP/1.1`,
- `Content-length: 202`,
- `Content-type: application/octet-stream`,
- `User-agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)`.

Třetím nejčastěji pozorovaným chováním bylo chování třídy A z tabulky č. 4.3, které se objevilo ve 23% procentech případů. V tomto případě se HTTP POST check-in zasílají na stejné cílové IP adresy za použití stejných hodnot v HTTP atributech `Host` a `Uri`. Příklad takových check-inů je zobrazen v tabulce 4.6.

Z této tabulky je patrné, že malware posílá check-in na stejnou cílovou IP adresu `188.120.246.180` za použití stejné hodnoty v HTTP atributu `Host`. V atributu `Uri` se poté nachází vždy stejná hodnota, tj. `/y.php`, a ostatní sledované HTTP atributy mají opět u všech HTTP zpráv stejné následující hodnoty:

- `Version: HTTP/1.0`,
- `Content-length: 34`,

Tabulka 4.6: Příklad malware s chováním č. 1

Cíl. IP	Host	Uri
188.120.246.180	188.120.246.180	/y.php
188.120.246.180	188.120.246.180	/y.php
188.120.246.180	188.120.246.180	/y.php
188.120.246.180	188.120.246.180	/y.php

Tabulka 4.7: Příklad malware s chováním č. 2

Cíl. IP	Host	Uri
104.239.157.210	truth-about-bakhmatuk.com	/webstat/
208.100.26.234	truth-about-bakhmatuk.com	/
199.2.137.20	truth-about-bakhmatuk.com	/admin/

- `Content-type: application/x-www-form-urlencoded`,
- `User-agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US)`.

V tomto případě se jednalo o napadené webové stránky ruské stavební společnosti www.tvd.ua na kterých se nacházela podvržená webová stránka `y.php` obsahující exploit kit. Samotné doménové jméno bylo zaregistrováno v roce 2010[7].

Posledním a nejméně spatřeným typem chování bylo chování třídy C z tabulky č. 4.3. Toto ojedinělé chování se objevilo pouze u 2% vzorků. Příklad této komunikace je zaznamenán v tabulce číslo 4.7. Vzorek crypto-malware odesílá tři HTTP POST zprávy na různé cílové IP adresy, které obsahují v HTTP atributu `Uri` různé hodnoty u všech třech zpráv. Všechny tyto zprávy jsou odesílány na cílový port 8080 a dále sledované HTTP atributy u všech zpráv obsahovaly stejné následující hodnoty:

- `Version: HTTP/1.0`,
- `Content-length: 35`
- `Content-type: application/x-www-form-urlencoded`,
- `User-agent: Mozilla/4.0`.

4.2.2 Experimentování nad reálným provozem

V dalším kroku byly provedeny experimenty detektorů třídy A, G a H na reálném síťovém provozu zaznamenaném v pcap souborech. Testovací množina sestávala ze zhruba 5 tera bajtů dat získaných od společnosti GreyCortex. Účelem těchto experimentů bylo odhalit další zpřesňující podmínky pro vybrané detektory a dále odhalit legitimní síťový provoz, který může být označen jako tzv. *false positives*[8].

Během experimentování v reálném provozu byl odhalen další prvek do množiny U popsané v sekci 4.2. Tento prvek pracuje pouze s názvem souboru. Jestliže tedy máme `Uri` například:

`/wp-content/plugins/binary.php`,

pak název souboru je řetězec `binary.php`.

Toto chování bylo nejprve zachyceno detektorem implementujícím třídu chování H z tabulky 4.3. Zachycené HTTP zprávy zobrazuje tabulka č. 4.8. Tato tabulka zobrazuje chování vzorku crypto-ransomware, který posílá v rámci jedné minuty pět HTTP zpráv. Všechny zprávy odcházejí na různé cílové IP adresy za použití různých hodnot v atributech

[7] http://network-tools.com/default.asp?prog=whois&host=tvd.ua
[8] typ provozu, který detektor vyhodnotí jako škodlivý i když se jedná o legitimní komunikaci

Tabulka 4.8: Příklad malware s novým chováním

Cíl. IP	Host	Uri
198.58.94.90	serbiotecnicos.com	/media/editors/wstr.php
23.236.62.147	fisioactivo.com	/wstr.php
107.180.39.236	iqinternal.com	/pmtsys/fonts/wstr.php
185.22.184.198	goktugyeli.com	/wstr.php
72.52.4.119	saludaonline.com	/wstr.php

`Host` a `Uri`. V atributu `Uri` se ovšem vždy jako název souboru vyskytuje soubor `wstr.php`. Všechny zprávy jsou odeslány na cílový port č. `80/tcp` a dále sledované HTTP atributy u všech zpráv obsahují stejné následující hodnoty:

- `Version: HTTP/1.1`,
- `Content-length: 645`,
- `Content-type: application/x-www-form-urlencoded`,
- `User-agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch) like Gecko`.

Tato komunikace byla zachycena detektorem implementujícím chování třídy H, protože obsahuje právě tři zprávy, kde se nachází různé hodnoty cílových IP adres, atributu HTTP `Host`, ale stejné hodnoty v HTTP atributu `Uri`.

Experimenty nad reálným provozem dále poodkryly další podmínku, která může výše popsané detektory zpřesnit. Doplňující podmínkou může být, že se nesmí vyskytovat prázdné hodnoty u sledovaných HTTP atributů. Tato doplňující podmínka vyplývá z analýzy nad crypto-ransomware vzorky, kde u všech HTTP zpráv, které vzorky posílají, jsou vždy kompletní HTTP atributy, tj. atributy popsané ve výčtu na začátku sekce 3.5 nikdy neobsahovaly prázdnou hodnotu. Během experimentování a testování vytvořených detekčních metod na reálném provozu a velkých[9] pcap souborech se objevilo mnoho HTTP zpráv, kde některé z těchto atributu neobsahovaly žádná data. Z tohoto faktu tedy vyplývá, že detektory je možné zpřesnit tím, že budou zpracovávat pouze HTTP zprávy, u kterých všechny sledované HTTP atributy obsahují data. Takové zprávy, kde některé HTTP atributy data neobsahují, můžeme z klasifikace automaticky vyloučit.

Na základě analýzy a provedených experimentů byly do systému MENDEL implementovány 3 detektory. Tyto detektory hledají v síťové komunikaci chování třídy A, G a H popsané v tabulce 4.3 v sekci 4.2.1 a dále čtvrtý detektor, který byl objeven během experimentování a je popsan na začátku této podsekce.

4.2.3 False positives

Během experimentů detektory odhalily několik typů komunikace, které mohou být použity pro seznam false positives. Tuto komunikaci generovaly například následující aplikace:

- antivirové programy jako *F-secure*[10] nebo *ESET*[11],

[9] pcap soubory o velikosti v řádech tera bajtů
[10] https://www.f-secure.com/en/welcome
[11] https://www.eset.com

- software *Heroku*[12], který poskytuje Cloudovou platformu jako službu,
- virtualizační plugin *VirtualvCP*[13],
- systémy pro podporu vývoje software od společnosti *Atlassian*[14] jako jsou například *Jira*, *Bamboo*, *Confluence*, *Trello* a další,
- komunikace operačního systému nebo webových prohlížečů s certifikačními autoritami jako je např. *DigiCert*[15],
- verifikace certifikátů pomocí protokolu OCSP[16] do podsítě společnosti *Google* nebo Microsoft,
- komunikace aplikace Microsoft Visual Studio s cloudem Azure,
- online live chat Smartsupp[17],
- produkty společnosti Ooyala[18] pro online streamování videa,
- update software PDF Architect[19] nebo
- aplikace pro online radio Paradise[20].

Ve velké většině případů se ovšem jednalo o aplikace nebo webové služby, které jsou běžně společnostmi využívány. Tyto služby a další komunikaci na interní nebo externí servery tedy můžeme označit jako false positivy. Seznam některých detekovaných služeb, které mohou být označeny jako false positivy je možné nalézt v příloze E nebo úplný seznam poté na datovém médiu v souboru `http-posts-default-fps.list`. Některé citlivé informace jako zdrojové IP adresy nebo časová razítka byla z dat v uvedném souboru záměrně odstraněna z důvodu zachování anonymity sítě, ve které byly experimenty prováděny.

4.3 Detekce uživatelského chování

Pokusy o přístup k doménovým jménům s doménou nejvyšší úrovně `.onion` jsou v síti Internet velice podezřelé, jelikož tuto doménu není možné najít v kořenových DNS záznamech. Pomocí služby Tor2web, popsané v sekci 3.7, je možné libovolnou skrytou službu v síti TOR zpřístupnit pomocí nahrazení TLD[21] `.onion` za jinou doménu, která je poskytována dobrovolnými Tor2web operátory[22]. Mezi nejpoužívanější patří zejména:

- .onion.to,
- .onion.city,

[12] https://www.heroku.com
[13] https://www.virtualvcp.com
[14] https://www.atlassian.com
[15] https://www.digicert.com/
[16] Online Certificate Status Protocol
[17] https://www.smartsupp.com/cs/
[18] www.ooyala.com
[19] http://www.pdfforge.org/pdfarchitect
[20] radioparadise.com
[21] Top-Level Domain
[22] někdy také označované jako tzv. clearnet proxies

- .onion.cab,
- .onion.direct,
- .onion.it,
- .onion.gq
- a další.

Pokus o přístup ke skryté službě v síti TOR je možné detekovat z obsahu DNS dotazů. Doménová jména tzv. `onion` služeb se skládají z šestnácti znaků, které jsou automaticky vygenerovány na základě veřejného klíče a díky tomu jsou také dobře odlišitelná od běžných doménových jmen. Příkladem může být například doména:

$$dpaqjri6tinnqleh.onion.gq. \tag{4.2}$$

Dotazy na skryté služby je možné detekovat pomocí IDS signatury. Dále popsaná signatura je dle syntaxe jazyka snort[23] rozdělena na dva logické celky kterými jsou tzv. hlavička[24] a volby[25].

```
alert udp $HOME_NET any -> any 53 ( content:"|01 00 00 01 00 00 00 00 00 00|";
depth:10; offset:2; content:"|onion|00|"; fast_pattern; )
```

Hlavička této signatury vyjadřuje akci typu `Alert`. Dále specifikuje, že se signatura má aplikovat pouze na pakety přenášené protokolem UDP, který se standardně používá pro komunikaci s DNS servery. Proměnná `$HOME_NET` reprezentuje monitorovanou podsíť ve které se nachází potencionálně infikované zařízení. Zdrojový port může být libovolný, jelikož je u většiny implementací vybrán operačním systémem. Cílová IP adresa může být rovněž libovolná, jelikož dopředu nevíme na který DNS server bude dotaz směrován. Fakt, že má infikované zařízení nastaveno v síťovém nastavení interní DNS server ještě neznamená, že malware tento server opravdu využije. Nic mu nebrání použít jiný veřejně dostupný DNS server[26] na který se bude infikované zařízení dotazovat. Cílový port je standardně `53/udp`.

Volby poté specifikují, že se v binárním obsahu paketu má hledat posloupnost bajtů `01 00 00 01 00 00 00 00 00 00`, kde jednotlivé bajty zleva reprezentují:

- `01 00` – standardní dotaz (flags),
- `00 01` – počet dotazů v paketu (standardně jeden),
- `00 00` – počet odpovědí (u DNS dotazů vždy nulové),
- `00 00 00 00` – počet položek v tzv. *Authority* a *Additional* sekcích, které u DNS dotazů budou nulové.

První dva bajty DNS paketu, které reprezentují ID transakce[27], nejsou v signatuře zahrnuty, protože se používají k párování DNS dotazů a následných odpovědí.

[23] http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node28.html
[24] Rule Header
[25] Rule Options
[26] Například veřejné DNS servery společnosti Google.
[27] Transaction ID nebo také TXID

Za těmito prvními dvanácti bajty DNS dotazu následuje samotná část DNS dotazu specifikující doménové jméno, typ DNS dotazu a třídu. Klíčové slovo `offset` specifikuje, že se výše zmíněných deset bajtů má začít hledat až od třetího bajtu paketu a klíčové slovo `depth` říká, že se má těchto deset bajtů hledat pouze v prvních deseti bajtech paketu. Dále nás zajímá, zda paket obsahuje řetězec `onion` za kterým následuje tzv. *null bajt*[28] ukončující hledané doménové jméno. Klíčové slovo `fast_patter` je použito pro zrychlení vyhledávání.

Díky této signatuře je možné detekovat pokusy o přístup na skryté služby v síti TOR. Signatura by mohla být dále rozšířena pro detekci jednotlivých operátorů úpravou druhého hledaného obsahu. Například pro detekci přístupu k doméně 4.2 by stačilo nahradit druhé klíčové slovo `content` následovně:

```
content:"|onion|00|"; -> content:"|onion|02|gq|00|";
```

V takovém případě by ovšem bylo nutné tyto signatury průběžně aktualizovat v závislosti na aktuálním seznamů operátorů.

Během experimentování tyto signatury samozřejmě detekovaly také uživatele, kteří vědomě přistupují do sítě TOR. Signatura samotná tedy ještě není příznakem infekce crypto-ransomware. Pokud se ovšem spojí s ostatními detekčními metodami, pak může, stejně jako signatura popsaná v sekci 4.1, reprezentovat jeden z ukazatelů infekce tímto typem malware.

4.4 Detekce anomálií nad DNS dotazy

Tato sekce se zabývá detekováním vybraných anomálií v DNS provozu pozorovaného v síťové komunikaci crypto-ransomware.

4.4.1 DNS dotazy na externí servery

Jestliže systém, který monitoruje danou podsíť má znalost interních DNS serverů, pak můžeme ze síťového provozu jednoduše určit, které DNS dotazy odchází na očekávané DNS servery a které na externí DNS servery. Předpokladem samozřejmě zůstává, že každé zařízení v monitorované síti má interní DNS server správně nastaven, což je možné zajistit například pomocí DHCP protokolu. Během experimentování s touto funkcionalitou na reálném provozu se ukázalo, že mezi false positivy mohou patřit například antivirové programy jako jsou *Bitdefender*[29] nebo *Avast*[30], které posílají DNS dotazy na své vlastní DNS servery. Dalším příkladem mohou být některé mobilní aplikace, které nepoužívají DNS server získaný od DHCP serveru. Z této detekce je také nutné vyloučit interní DNS servery, které posílají DNS dotazy na ostatní DNS servery.

4.4.2 Náhodně vygenerované doménové jména

Jestliže malware používá pro komunikaci s C&C serverem IP adresu namísto doménového jména, pak je detekce se znalostí této adresy jednoduchá a dá se postavit na blacklistech. Problém nastane v okamžiku kdy malware použije náhodně vygenerovanou doménu. V takovém případě začne infikované zařízení generovat velké množství DNS dotazů, které není možné přeložit, protože daná doména neexistuje. Během experimentování jsem se zabýval

[28] 00

[29] https://www.bitdefender.com/

[30] https://www.avast.com

Tabulka 4.9: Zhodnocení přesnosti detektorů na reálné provozu

Cíl. IP	Host	Uri	Třída	Počet výskytů [%]	
				Ransomware	Běžná kom.
stejné IP	**stejná hodnota**	**stejné URI**	**A**	**23,72**	**82,75**
stejné IP	stejná hodnota	různé URI	B	0	15,51
různé IP	**stejná hodnota**	**stejné URI**	**C**	**1,69**	**0**
různé IP	stejná hodnota	různé URI	D	0	0
stejné IP	různé hodnoty	stejné URI	E	0	1,72
stejné IP	různé hodnoty	různé URI	F	0	0
různé IP	**různé hodnoty**	**stejné URI**	**G**	**49,15**	**0**
různé IP	**různé hodnoty**	**různé URI**	**H**	**25,42**	**0**

detekcí tohoto chování založeném na poměru počtu nepřeložitelných DNS dotazů oproti počtu přeložitelných DNS dotazů na minutových intervalech. Předpokladem byla hypotéza, že na infikovaném zařízení dojde k nárustu tohoto poměru v okamžiku kdy se začne dotazovat na domény, které neexistují. Tato detekce se ovšem neukázala jako moc přesná, například kvůli špatné konfiguraci DNS serverů nebo routerů. Příkladem mohou například chybějící zpětné[31] DNS záznamy.

4.4.3 Komunikace skrze DNS tunel

Během experimentování se ukázalo, že DNS tunel používá například antivirus Avast pro svoji funkci *Secure DNS*[32]. Avast tuto funkci používá pro ověření doménových jmen oproti vlastnímu DNS serveru, aby zajistil, že IP adresa vrácená od nastaveného DNS serveru je opravdu legitimní. Dalším příkladem může být používání peer-to-peer sítí skrze port `53/udp`.

4.5 Korelace událostí a zhodnocení výsledků

Žádný z navržených detektorů nebo napsaných signatur samozřejmě nedetekovala všechny zkoumané vzorky crypto-ransomware a proto je nutné, aby detekované události systémem MENDEL analyzoval bezpečnostní analytik. Navržené detektory a napsané signatury, včetně znalostí z analýzy popsané v kapitole 3 mohou ovšem sloužit jako cenné indicie, které mohou pomoci při vyšetřovaní bezpečnostních incidentů a rozhodování, zde je daný uzel infikován či nikoliv.

Detektory, které klasifikují crypto-ransomware na základě jejich komunikace za použití HTTP komunikace byl testován v reálném provozu a jeho výsledky popisuje tabulka č. 4.9. V této tabulce je možné vidět jednotlivé třídy chování, které detektory detekují. Sloupec s názvem Ransomware vyjadřuje kolik procent vzorků detektor dané třídy zachytil. V tomto případě se jednalo o test pouze na testovacích datech.

Poté byly stejné detektory spuštěny na běžnou komunikaci po dobu jednoho týdne. Smyslem tohoto testu bylo zjistit, které třídy chování se v běžné komunikaci vyskytují. Testy ukázaly, že v běžné komunikaci se v 82% procentech vyskytuje chování třídy A. V 15%

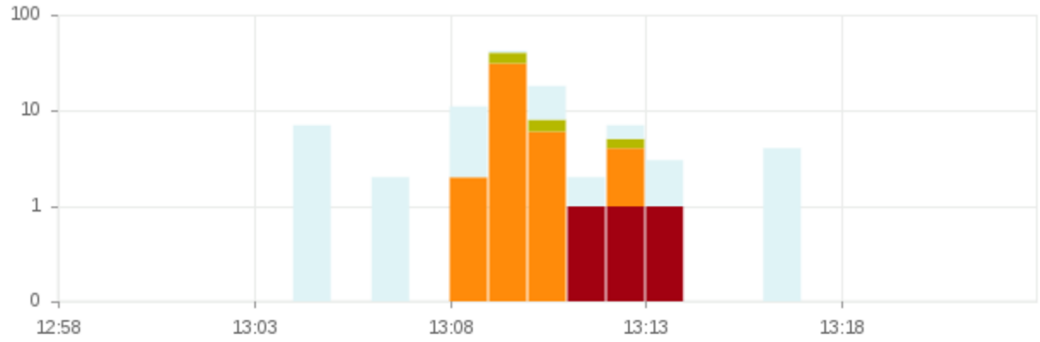
[31] DNS záznamy typu PTR

[32] https://www.avast.com/en-eu/f-secure-dns

se vyskytlo chování třídy B, přičemž takové chování se v komunikaci crypto-ransomware nevyskytlo vůbec. Detektor, který detekuje chování třídy B je pro detekci crypto-ransomware nepoužitelný. Dále se v běžné komunikaci vyskytlo chování třídy E, které se ovšem opět v síťové komunikaci crypto-ransomware nevyskytuje.

Z toho vyplývá, že jakmile klasifikátor detekuje chování ze třídy C, G nebo H, pak se téměř se sto procentní pravděpodobností jedna síťovou komunikaci crypto-ransomware. Jestliže bylo v síťové komunikaci detekováno chování třídy A, pak je potřeba danou událost blíže vyšetřit a na základě znalostí rozhodnout zda se jedná o legitimní komunikaci či nikoliv.

Na obrázku č. 4.1 je možné vidět příklad detekovaného vzorku crypto-ransomware, který spadá do třídy A. Malware byl spuštěn dne 9. Dubna ve 13:08. Na obrázku je možné vidět několik událostí, které byly na daném zařízení detekovány. První událost *Ransomware: HTTP POST Check-in Class A* detekovala posílaní HTTP POST check-in pomocí protokolu HTTP, které odpovídá třídě A z tabulky č. 4.9. Jelikož se jednalo již o známý ransomware, tak byly systémem IDS dále detekovány některé IDS události jako například použití řetězců *MSIE5* a *Windows 95* v atributu `User-agent` i když byl na infikovaném zařízení nainstalován operační systém Windows 7.

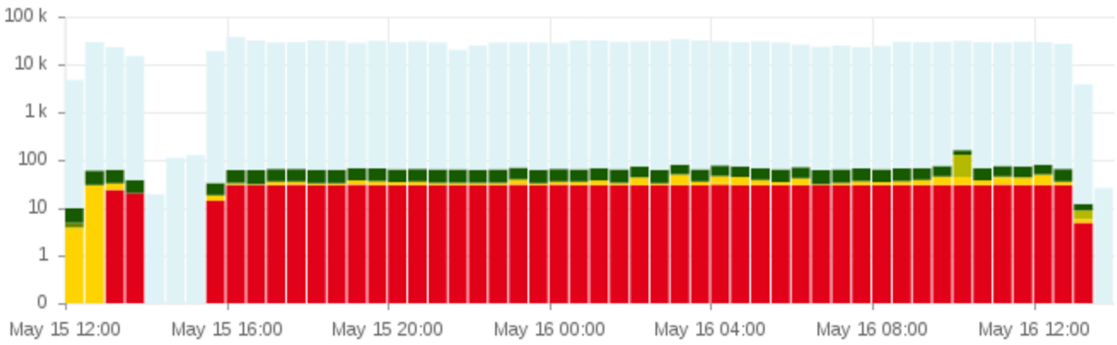


	Name	Service	Date
9	Ransomware: HTTP POST Check-in Class A	HTTP (80)	Apr-09 13:10 – 13:13
7	trojan: Fareit/Pony Downloader Checkin 3	HTTP (80)	Apr-09 13:09
7	trojan: Fareit/Pony Downloader Checkin 2	HTTP (80)	Apr-09 13:08 – 13:09
7	trojan: Pony Downloader HTTP Library MSIE 5 Win98	HTTP (80)	Apr-09 13:08 – 13:09
7	trojan: Trojan Generic - POST To gate.php with no referer	HTTP (80)	Apr-09 13:08 – 13:09
7	trojan: Likely Zbot Generic Post to gate.php Dotted-Quad	HTTP (80)	Apr-09 13:08 – 13:09
5	policy: Windows 98 User-Agent Detected - Possible Malware or Non-Updated System	HTTP (80)	Apr-09 13:08 – 13:09
5	policy: Unsupported/Fake Internet Explorer Version MSIE 5.	HTTP (80)	Apr-09 13:08

Obrázek 4.1: Detekce ransomware spadajícího do třídy A.

Obrázek č. 4.2 ukazuje, jak může v systému MENDEL vypadat seznam událostí, které byly detekovány na zařízení, které bylo infikováno ransomware wannacrypt. Jednalo se o úmyslné infikování jednoho z počítačů v sestaveném testovacím prostředí. V grafu je zobrazen počet toků, které byly na infikovaném zařízení analyzovány a tabulka následně ukazuje bezpečnostní události, které byly během infekce detekovány. První událost *Scan: SMB Port Sweep (445)* detekovala incident typu *port sweep* na port `445/smb`. Tento incident reprezentoval chování při kterém ransomware začal skenovat síť Internet na přítomnost zařízení, které mají otevřen daný port. Dále byly na zařízení detekovány události typu *blacklist*, které

reprezentují komunikaci s blacklistovanými IP adresami. Jelikož byl malware ponechán aktivní více než 24 hodin, tak bylo zaznamenána i periodická komunikace, reprezentovaná události *Periodic: Repetitive Connections (every 30 minutes in 6 hours)*. Tento incident byl detekován, jelikož infikované zařízení stihlo oskenovat síť Internet několikrát a proto se k některým veřejným IP adresám připojovalo periodicky. Na infikovaném zařízení bylo také detekováno použití expoitu na zařízení v lokální síti.



	Name	Dst Hosts	Service	Events	Date
8	Scan: SMB Port Sweep (445)	1	SMB2 (445)	1.3 k	Mon 13:05 – Tue 13:03
7	blacklist: Spamhaus DROP blacklist	8	SMB2 (445)	8	Mon 13:21 – Tue 11:04
6	Scan: Port Sweep-like Behavior (horizontal port scan)	1	SMB2 (445)	41	Mon 12:25 – 13:05
6	exploit: Possible DOUBLEPULSAR Beacon Response	1	MS-DS (445)	4	Mon 15:45
6	blacklist: Openbl.org blacklist	9	SMB2 (445)	24	Mon 17:31 – Tue 12:45
6	blacklist: Blocklist.de blacklist	108	SMB2 (445)	230	Mon 13:18 – Tue 13:00
6	blacklist: Tor blacklist	8	SMB2 (445)	12	Tue 02:26 – 12:52
6	blacklist: Compromised or Hostile Host Traffic	2	SMB2 (445)	2	Mon 18:14 – 22:37
6	blacklist: BotCC blacklist	2	SMB2 (445)	2	Tue 04:14 – 11:43
6	blacklist: General blacklist	6	SMB2 (445)	10	Mon 18:55 – Tue 09:52
5	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	88	SMB2 (445)	94	Mon 16:27 – Tue 12:58
5	scan: Behavioral Unusual Port 445 traffic, Potential Scan or Infection	2	SMB2 (445)	2	Mon 16:21 – 16:24
4	outlier: Data at Subnet Services	1	HTTP (80)	1	Mon 12:28 – 12:29
4	scan: Behavioral Unusual Port 445 traffic, Potential Scan or Infection	1	SMB2 (445)	1	Tue 00:44
3	scan: Behavioral Unusual Port 445 traffic, Potential Scan or Infection	1355	SMB2 (445)	1.4 k	Mon 12:25 – Tue 13:02

Obrázek 4.2: Události detekované systémem MENDEL po infekci ransomware WannaCry.

Kapitola 5

Závěr

Zadání této diplomové práce jsem sám navrhnul, abych se blíže seznámil s problematikou ransomware a systémem MENDEL. Práce splnila mé osobní očekávání, jelikož jsem rozšířil své znalosti v oblasti malware, jejich analýzy a nástrojů pro analýzu určené. Práce mi dále také umožňila nabýt nové znalosti v oblasti identifikace malware na základě dat ze síťové komunikace.

Pro tuto práci bylo nutné vytvořit testovací prostředí, které bylo vytvořeno ve společnosti GreyCortex a je dodnes jeho zaměstnanci využíváno pro analýzu malware a testování systému MENDEL. Toto prostředí bude v budoucnu otevřeno veřejnosti a představuje tedy přínos nejenom pro společsnot GreyCortex, ale také pro ostatní bezpečnostní specialisty v oblasti škodlivého software.

Hlavním přínosem této práce je komplexnější analýza síťového provozu malware typu crypto-ransomware. Na základě této analýzy byly potom navrhnuty a experimentálně ověřeny detekční metody, které se snaží o rozpoznání ransomware čistě na základě jeho síťové komunikace. Konkrétně se jedná o 4 detekční metody, které jsou schopné rozpoznat ransomware z HTTP komunikace. Tři z těchto metod jsou schopny detekovat ransomware téměř se sto procentní jistotou. Ve čtvrtém případě je potřeba detekovanou událost blíže vyšetřit, jelikož se stejný charakter HTTP komunikace objevuje i v běžné síťové komunikaci. Dalším přínosem této práce je několik signatur, které mohou být použity v IDS systému. Tyto signatury poté mohou sloužit jako ukazatele možné infekce. Tyto detektory a signatury byly implementovány v systému MENDEL a díky tomu mohly být otestovány v reálném prostředí.

Práce dále také přináší analýzu síťové komunikace nejaktuálnějšího crypto-ransomware WannaCrypt, kde část této analýzy byla publikována některými českými i zahraničními servery.

Jednou z dalších oblastí, kterou jsem se v rámci této práce zabýval byla klasifikace pomocí algoritmu *Support Vector Machine*. I když se mi pomocí této metody podařilo ransomware klasifikovat (např. podle rysů jako jsou počty paketů, počty toků, počty komunikačních partnerů a další), navržený klasifikátor se při praktickém nasazení ukázal jako nepoužitelný, jelikož extrahované vzory nebyly nikdy dostatečně unikátní, aby podle nich bylo možné s velkou pravděpodobností odlišit legitimní síťovou komunikaci od komunikace crypto-ransomware. Osobně jsem přesvědčen, že výzkum v této oblasti samotné, s počtem vzorků, které jsem měl k dispozici, by vystačil na celou diplomovou práci, což může být také námět na rozšíření této práce.

Literatura

[1] *Cyber Threat Alliance. Lucrative ransomware attacks: Analysis of the cryptowall version 3 threat.* 2015.
URL ttp://cyberthreatalliance.org/cryptowallreport.pdf

[2] *Cisco 2016 Midyear Cybersecurity Report* . July 2016.

[3] Alzaylaee, M. K.; Yerima, S. Y.; Sezer, S.: *Automated Dynamic Analysis of Ransomware: Benefits, Limitations and use for Detection.* June 2006, [Online].

[4] Biasini, N.: *Threat spotlight: Cisco talos thwarts access to massive international exploit kit generating 60m dolars annually from ransomware alone.* 2015, [Online; navštíveno 30.06.2016].
URL http://talosintel.com/angler-exposed/

[5] Brewer, R.: Ransomware attacks: detection, prevention and cure. *Network Security*, ročník 2016, č. 9, 2016: s. 5 – 9, ISSN 1353-4858, doi:http://dx.doi.org/10.1016/S1353-4858(16)30086-1.
URL http://www.sciencedirect.com/science/article/pii/S1353485816300861

[6] Conn, J.: *Ransomware Scare: Will Hospitals Pay For Protection?* 2016.

[7] Dandurant, K.: *Cryptowall attacks durham police files.* 2014.
URL http://www.seacoastonline.com/article/20140607/NEWS/406070322

[8] Ferrand, O.: How to detect the Cuckoo Sandbox and to Strengthen it? *Journal of Computer Virology and Hacking Techniques*, ročník 11, č. 1, 2015: s. 51–58, ISSN 2263-8733, doi:10.1007/s11416-014-0224-9.
URL http://dx.doi.org/10.1007/s11416-014-0224-9

[9] Goodin, D.: *Booming crypto ransomware industry employs new tricks to befuddle victims.* 2015.
URL http://arstechnica.com/security/2015/11/booming-crypto-ransomware-industry-employs-new-tricks-to-befuddle-victims/

[10] Gorman, G. O.; McDonald, G.: *Ransomware: A growing menace.* 2012, [Online; navštíveno 1.01.2017].
URL http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

[11] Group, T.: *Teslacrypt - decrypt it yourself.* 2015, [Online; navštíveno 15.10.2016].
URL http://blogs.cisco.com/security/talos/teslacrypt

[12] Kanurat, A.: *The current state of ransomware: CryptoWall*. 2016.
URL https://blogs.sophos.com/2015/12/17/the-current-state-of-ransomware-cryptowall

[13] Kanurat, A.: *The current state of ransomware: TCB-Locker*. 2016.
URL https://blogs.sophos.com/2015/12/31/the-current-state-of-ransomware-ctb-locker

[14] Savage, K.; Coogan, P.; Lau, H.: *The evolution of ransomware*. Mar 2016, [Online; navštíveno 12.12.2016].
URL http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[15] Squires, K.: *IT Matters: Security in 2016*. 2016.
URL http://www.mmdonline.com/opinions/matters-security-2016/

[16] Ransomware menace grows as new threats emerge. *Network Security*, ročník 2016, č. 8, 2016: s. 1 – 2, ISSN 1353-4858,
doi:http://dx.doi.org/10.1016/S1353-4858(16)30072-1.
URL http://www.sciencedirect.com/science/article/pii/S1353485816300721

[17] Wood, P.; aj.: *Symantec. 2016 Internet Security Threat Report*. 2016.
URL https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Přílohy

Seznam příloh

Příloha A

Obsah přiloženého paměťového média

`code/virtualbox/createVBoxVM.py`
- skript pro vytvoření virtuálního počítače ve Virtual Boxu
`code/virtualbox/vboxConfBios.py`
- skript pro nastavení vytvořeného virtuálního počítače
`data/public-ip.list`
- úplný seznam identifikovaných služeb vracejících veřejnou IP adresu dotazovatele
`data/Ransomware_Overview.ods`
- seznam známých crypto-ransomware a kryptografických algoritmů, které používají
`data/http-post-check-ins.ods`
- data z HTTP POST komunikace
`data/http-posts-default-fps.list.csv`
- HTTP POST dotazy, které je možné použít jako výchozí false positivy
`data/user-agents.list`
- odpozorované hodnoty atributu `User-agent`

Příloha B

Služby zjišťující veřejnou IP adresu

Doménové jméno	
ip-adress.com	trackip.net
meuip.net.br	myip.kz
localize.pdfforge.org	showip.net
whoer.net	myip.dnsomatic.com
www.ip.cn	checkip.amazonaws.com
ip.taobao.com	software77.net
iplocation.com	pijoto.net
ip2city.asp	ipinfo.io
ip-api.com	ip.tyk.nu
speedtest.net	showmyip.com
wtfismyip	geolocation.com
www.ip-tracker.org	cmyip.com
sina.com.cn	myip.ozymo.com
checkip.dyndns.org	dawhois.com
ipecho.net	ip-address.ru
geoplugin.net	pr-cy.ru
ip.webmasterhome.cn	ip.42.pl
www.whatsmyip.us	speed-tester.info
ip2nation.com	freehostedscripts.net
ipchicken.com	whoer.net
ip-api.com	whatismyip.com
myip.ch	whereisip.net
b4secure.com	youip. net
iplocation.net	api.ipify.org
ipmonkey.com	whatismyip.com
icanhazip.com	ip2location.com
useragent.cc	iplogger.ru
tinytools.nu	ip-score.com
whatismyipaddress.com	ipinfo.io

Tabulka B.1: Seznam některých služeb zjištujících veřejnou IP adresu

Příloha C

Identifikované Služby zjišťující veřejnou IP adresu

IP adresa	Domnévé jméno	cílový port
104.27.143.232	addomain.men	80
107.21.206.81	api.ipify.org.herokudns.com	80
147.229.9.22	tereza.fit.vutbr.cz	5222
147.229.9.23	www.fit.vutbr.cz	80
158.69.242.138	freegeoip.net	80
172.217.23.206	redirector.gvt1.com	80
178.248.232.65	rukzak.kiev.ua	80
188.92.40.78	flashscore.com	80
192.150.16.37	linuxdownload.wip4.adobe.com	80
195.74.38.149	ip.nu	80
212.20.119.140	mail.webzone.cz	25
212.61.180.100	dbctr.gq	80
213.46.255.60	mail.upcmail.cz	25
216.34.181.97	kmeleonbrowser.org	80
37.252.172.12	fra1-ib.adnxs.com	80
42.62.94.2	app02.nodes.gslb.mi-idc.com	443
50.19.93.247	api.ipify.org.herokudns.com	80
52.206.174.109	app.getsitecontrol.com	80
54.243.128.120	client.hola.org	80
54.254.192.56	resolver.gslb.mi-idc.com	80
64.233.167.28	gmail-smtp-relay.l.google.com	587
67.106.145.165	www.gw.qsstats.com.akadns.net	80
77.234.44.67	ip-info.ff.avast.com	80
77.93.211.82	www.akpzl.cz	80
85.118.128.140	navlas.cz	80
85.94.211.82	www.dnsqueries.com	80
88.198.46.60	ping.eu	80
91.189.94.25	geoip.ubuntu.com	80
91.198.174.192	www.wikipedia.org	80
93.99.92.116	dla.uloz.to	80

Tabulka C.1: Identifikované služby zjištující veřejnou IP adresu

Příloha D

Kryptografické algoritmy Ransomware

Jméno	**Použitý algoritmus**
CryptoHasYou.	AES(256)
777	XOR
7h9r	AES
8lock8	AES (256)
Alma Ransomware	AES(128)
Alpha Ransomware	AES(256)
Anubis	AES(256)
Bandarchor	AES(256)
BitStak	Base64 + String Replacement
BlackShades Crypter	AES (256)
Blocatto	AES (256)
Brazilian	AES(256)
BrLock	AES
Bucbi	GOST
Cerber	AES
Coverton	AES(256)
CryFile	Moves bytes
CrypMIC	AES(256)
Crypt38	AES
Cryptear	AES(256)
CryptFIle2	RSA
CryptoBit	AES and RSA
CryptoFortress	AES (256), RSA (1024)
CryptoHost	AES(256) (RAR implementation)
CryptoJoker	AES-256
CryptoLuck / YafunnLocker	AES(256)
CryptON	RSA, AES-256 and SHA-256
CryptoRoger	AES
CryptoShield	AES(256) / ROT-13

Tabulka D.1: Kryptografické algoritmy použité v ransomware

Jméno	**Použitý algoritmus**
CryptoShocker	AES
CryptoTrooper	AES
CryptoWire	AES(256)
CryPy	AES
CTB-Locker	RSA(2048)
CTB-Locker WEB	AES(256)
CuteRansomware	AES(128)
Damage	Combination of SHA-1 and Blowfish
DEDCryptor	AES-256
DetoxCrypto	AES
DMALocker	AES(256) in ECB mode, Version 2-4 also RSA
DMALocker 3.0	AES(256)XPTLOCK5.0
Domino	AES(256)
Donald Trump	AES
DoNotChange	AES(128)
EDA2 / HiddenTear	AES(256)
Enigma	AES (128)
Erebus	AES
Exotic	AES (128)
Fantom	AES(128)
FireCrypt	AES(256)
GhostCrypt	AES (256)
Globe v1	Blowfish
Globe v2	Blowfish
Globe v3	RC4AES(256)
GNL Locker	AES (256)
HappyDayzz	3DES, AES(128), AES(192), AES(256), DES, RC2, RC4
HDDCryptor	Custom (net shares), XTS-AES (disk)
Heimdall	AES-128-CBC
Herbst	AES(256)
Hermes	AES
Hi Buddy!	AES(256)
HolyCrypt	AES
Hucky	AES, RSA (hardcoded)
JapanLocker	Base64 encoding, ROT13, and top-bottom swapping
Jeiphoos	RC6 (files), RSA 2048 (RC6 key)
Jigsaw	AES(256)
Job Crypter	TripleDES
Karma	AES
KeRanger	AES
KillDisk	AES(256)
KimcilWare	AES
Korean	AES(256)
Kozy.Jozy	RSA(2048)
KryptoLocker	AES(256)

Tabulka D.2: Kryptografické algoritmy použité v ransomware

Jméno	**Použitý algoritmus**
LambdaLocker	AES(256)
LLTP Locker	AES-256
LockLock	AES(256)
Locky	AES(128)
Magic	AES(256)
MaktubLocker	AES(256), RSA (2048)
Marlboro	XOR
Matrix	GnuPG
MIRCOP	AES
MireWare	AES(256)
MM Locker	AES(256)
NanoLocker	AES (256), RSA
Nemucod	XOR(255)7zip
Netix	AES(256)
NMoreira	mix of RSA and AES-256
Nuke	AES
ODCODC	XOR
PClock	XOR
Petya	Modified Salsa20
Philadelphia	AES(256)
PokemonGO	AES(256)
Popcorn Time	AES(256)
Polyglot	AES(256)
Potato	AES(256)
PowerWare	AES(128)
PowerWorm	AES, but throws key away, destroys the files
Radamant	AES(256)
Ranion	AES(256)
RansomLock	Asymmetric 1024
Razy	AES(128)
RektLocker	AES(256)
Revenge	AES(256)
Rokku	Curve25519 + ChaCha
Samas-Samsam	AES(256) + RSA(2096)
Sanction	AES(256) + RSA(2096)
Sanctions	AES(256) + RSA(2048)
Serpent	AES(256)
Serpico	AES
Shark	AES(256)
Simple_Encoder	AES
SkidLocker / Pompous	AES(256)
SNSLocker	AES(256)
Stampado	AES(256)
Strictor	AES(256)
Surprise	AES(256)

Tabulka D.3: Kryptografické algoritmy použité v ransomware

Příloha E

HTTP POST - False positivy

Cíl. IP	Port	Version	Host	Content-Length
23.23.141.169	80	HTTP1.1	idreams.herokuapp.com	121
178.62.60.58	80	HTTP1.1	www.virtualvcp.com	168
151.101.193.69	80	HTTP1.1	stackoverflow.com	74
178.255.83.1	80	HTTP1.1	ocsp.comodoca.com	83
52.28.12.177	80	HTTP1.1	hit-pool.upscore.io	197
54.72.254.170	80	HTTP1.1	l.ooyala.com	1
64.15.159.224	80	HTTP1.1	update.pdfarchitect.org	351
198.41.214.186	80	HTTP1.1	ocsp.msocsp.com	86
23.42.27.27	80	HTTP1.1	tj.symcd.com	83
207.171.162.180	80	HTTP1.1	www.imdb.com	67
85.10.224.199	80	HTTP1.1	api.infinario.com	451
52.5.30.51	80	HTTP1.0	locker.data.ksmobile.net	133
54.86.98.229	80	HTTP1.1	api.kiip.me	689
54.238.60.168	80	HTTP1.1	i.doit.im	11
162.254.197.29	80	HTTP1.1	valve519.steamcontent.com	524
185.92.220.61	80	HTTP1.1	thor.rtk.io	306
185.92.220.61	80	HTTP1.1	thor.rtk.io	308
109.123.210.73	80	HTTP1.1	ut.performax.cz	211
188.165.220.20	80	HTTP1.1	www.rybarska-specialka.cz	15
217.67.30.154	80	HTTP1.1	www.floowie.com	14
54.76.191.65	80	HTTP1.1	tupperware.ipapercms.dk	206
54.238.60.168	80	HTTP1.1	i.doit.im	11
193.189.143.34	80	HTTP1.1	www.netvibes.com	15
104.25.234.23	80	HTTP1.1	www.thingiverse.com	138
37.187.250.48	80	HTTP1.1	www.loupak.cz	100
91.214.192.124	80	HTTP1.1	www.ndbrno.cz	459
52.16.45.93	80	HTTP1.1	urlauth.ksmobile.net	128
87.240.131.117	80	HTTP1.1	api.vk.com	150
203.205.128.104	80	HTTP1.1	szminorshort.weixin.qq.com	219
85.10.255.245	80	HTTP1.1	api.infinario.com	480

Tabulka E.1: Identifikované false positivy

Příloha F

Hodnoty atributu User-agent

User-agent:
GenericHttp/VER_STR_COMMA
Internet Explorer
Mozilla
mozilla/2.0
Mozilla/3.0 (compatible; Indy Library)
Mozilla/4.0
Mozilla/4.0 (compatible; MSIE 2.0; Windows NT 5.0; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET ...
Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Mozilla/4.0 (compatible; Synapse)
Mozilla/5.0
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/5.0)
Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0);(b:7601;c:INT-8760;l:09)
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.0) Opera 12.14
Mozilla/5.0 (iPad; CPU OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/534.55.3 (KHTML
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_7; da-dk) AppleWebKit/533.21.1 (KHTML
Mozilla/5.0 (Windows NT 6.0; rv:34.0) Gecko/20100101 Firefox/34.0
Mozilla/5.0 (Windows NT 6.1)
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/535.36 (KHTML
Mozilla/5.0 (Windows NT 6.1; rv:22.0) Gecko/20130405 Firefox/22.0
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:2.0b8pre) Gecko/20101114 Firefox/4.0b8pre
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0) Gecko/20130401 Firefox/21.0
Mozilla/5.0 (Windows NT 6.3 rv:11.0) like Gecko
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US)
Opera 10.1
Opera/9.80 (Windows NT 5.1; U; en) Presto/2.9.168 Version/11.51

Tabulka F.1: Odpozorované hodnoty HTTP atributu `User-agent`.