Politechnika Warszawska

WYDZIAŁ ELEKTRYCZNY

Praca dyplomowa inżynierska

na kierunku Informatyka Stosowana

w specjalności Inżynieria Oprogramowania

Oprogramowanie wykrywające ataki typu ransomware na podstawie analizy statystyk generowanych przez system plików

Maciej Michalski

numer albumu 311351

promotor

dr inż. Radosław Roszczyk

WARSZAWA 2023

Oprogramowanie wykrywające ataki typu ransomware na podstawie analizy statystyk generowanych przez system plików

Streszczenie

Tutaj znajdować się będzie streszczenie Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Słowa kluczowe: ransomware, administracja, cyberbezpieczeństwo

Software to detect ransomware attacks based on analysis of statistics generated by the file system

Abstract

Here will be an abstract of the paper Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Keywords: ransomware, administration, cybersecurity

Spis treści

Rozdział 1

Wprowadzenie

Głównym celem każdej aplikacji cyfrowej, systemu informatycznego czy innego rodzaju usług dostępnych przez sieć jest przetwarzanie informacji cyfrowej. Dzięki dygitalizacji usług oraz utworzeniu kompletnie nowych jej, rodzajów zależnych od technologii cyfrowych ludzkość generuje masywne ilości danych każdego dnia. Jednym z najpopularniejszych środków komunikacji, zwłaszcza dla biznesu, jest poczta elektroniczna. Grupa **Radicati Inc.** spekuluje, że do końca 2023 liczba wysłanych listów elektronicznych powinna przekroczyć 347 miliardów [1]. **Domo, Inc**, które jest jednym z wielu dostawców usług chmurowych, w swoim raporcie zatytułowanym „Data Never Sleeps 10.0" donosi o tym, że wielkość danych, które zostaną utworzone czy skopiowane może wejść w okolicę 181 zettabajtów[1] wielkości do roku 2025 [2]. Znakomita część tych danych musi być przechowywana na stałe, gdyż wymaga tego poprawne działanie systemu lub może wynikać z nakazów prawnych. Z tych powodów jednym z priorytetów przy administracji systemu jest zabezpieczenie przed utratą danych przez instytucje i działalności gospodarcze. Do powodów utraty danych mogą należeć:

- awaria nośników i innych elementów,
- niespodziewane braki w dostawach prądu,
- błąd ludzki,
- wirusy komputerowe.

1.1 Cel pracy

Celem tej pracy było odnalezienie sposobu na zniwelowanie strat danych w wyniku ataku wirusa typu ransomware możliwego do wykorzystania przez administratorów w warunkach rzeczywistego ataku. Zaproponowanym przeze mnie rozwiązaniem jest oprogramowanie analizujące działania na plikach dla systemów operacyjnych z rodziny Linux. Program korzysta z informacji o stanie systemu plików i na bieżąco analizuje wykonywane na nim operacje. Statystyki z obserwowanego obszaru zawierają w sobie m.in. ilości operacji, ścieżkę do użytej komendy, nazwę użytkownika, który dokonuje operacji etc. Dzięki temu administrator może nie tylko dowiedzieć się o potencjalnym zagrożeniu

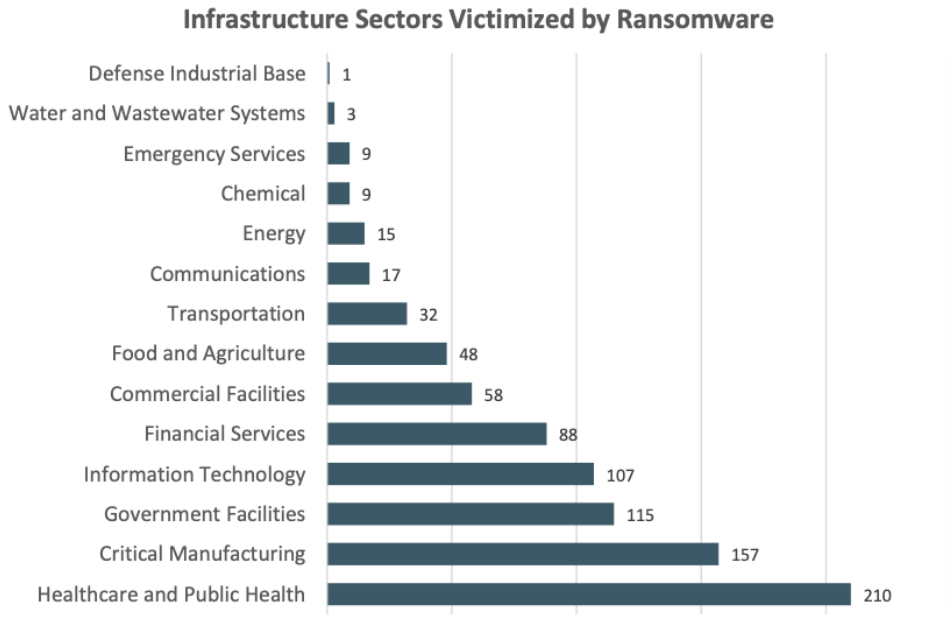
[1] Zetta bajt (skrót **ZB**) w systemie SI to tryliard 10^{21} bajtów i 2^{70}, czyli 1024^7 bajtów.

ataku ransomware, ale też obserwować dowolny, podejrzany ruch na systemie plików. Następnie dokonywana jest analiza zawartości plików i generowany jest raport o zakresie ryzyka. Docelową grupą użytkowników są administratorzy, a więc główne założenia, jakie postawiłem sobie w trakcie tworzenia rozwiązania, miały na celu wytworzenie oprogramowania łatwego dla nich w obsłudze. Tymi założeniami są:

- łatwa instalacja, która nie wymaga aktualizacji sterowników sprzętowych,
- wsparcie dla najpopularniejszych dystrybucji serwerowych[2],
- minimalne zużycie zasobów,
- integracja z bieżącymi popularnymi rozwiązaniami w administracji systemów.

1.2 Opis problemu i znaczenie zagrożeń typu ransomware

Od 2017 roku obserwuje się trend wzrostowy ataków ransomware [3], a w ciągu pierwszej połowy 2022 roku, dokonano 236,7 miliona ataków na całym świecie [4]. Wg. raportu Verizona [3] ataki ransomware stanowią 10% wszystkich naruszeń danych w 2021. Wedle zebranych statystyk wykrycie ich zajęło w aż 49 dni dłużej niż średni czas wykrycia wszystkich naruszeń z tego samego roku. Raport wyjaśnia też, że zagrożona nie jest wyłącznie branża IT, ale też inne sektory, w szczególności sektor ochrony zdrowia.

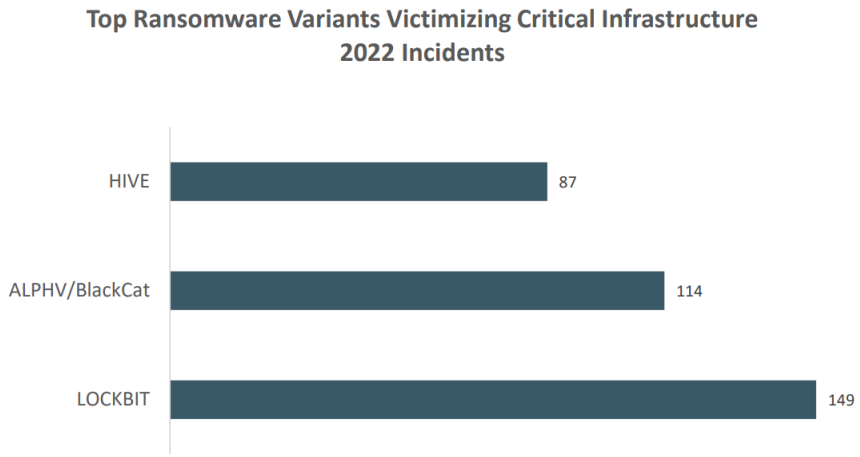


Rysunek 1. Sektory infrastruktury krytycznej, do których odnosiły się skargi IC3. Źródło: *FBI 2022 Internet Crime Report*, s. 14

[2]W3 Techs utrzymuje raport o sieciowych serwerach Linuksowych. Jest on codziennie aktualizowany i można go odnaleźć pod adresem: https://w3techs.com/technologies/details/os-linux

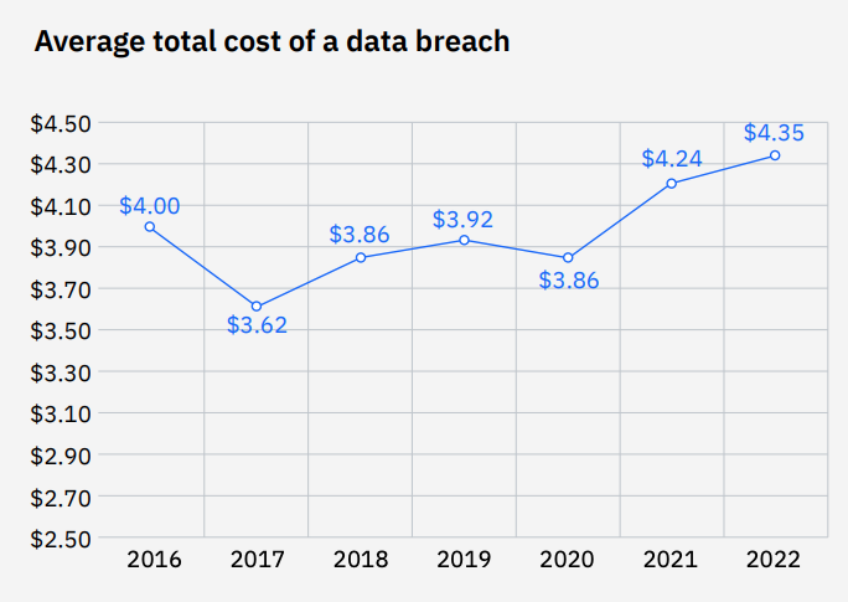
[3]Raport jest odpłatnie dostępny pod linkiem: https://www.verizon.com/business/resources/reports/dbir/2021/results-and-analysis

Raport IC3 z roku 2022 donosi o 870 zarejestrowanych skargach dotyczących ataków, których celem były organizacje infrastruktury krytycznej. Pośród 16 sektorów, 14 z nich padło ofiarą próby ataku.



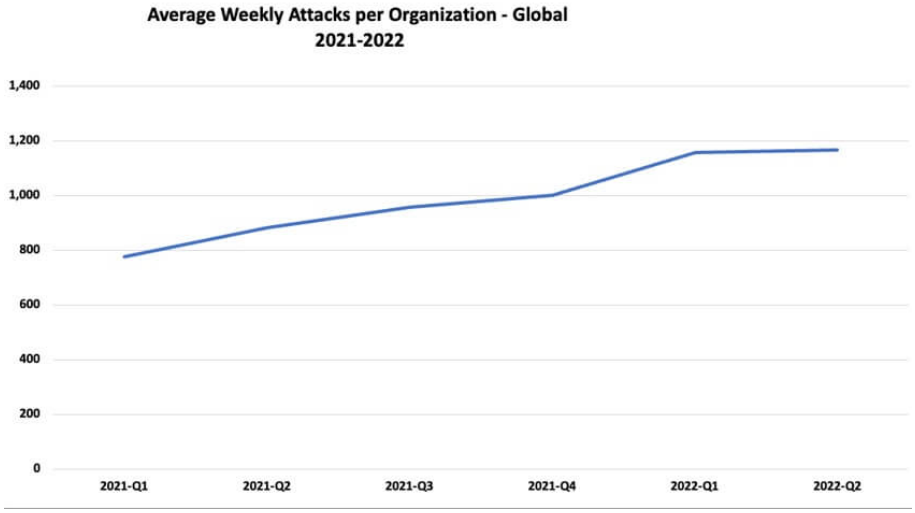
Rysunek 2. Najpopularniejsze warianty wirusów ransomware, zarejestrowane w trakcie incydentów mających na celu atak infrastruktury krytycznej. Należy zauważyć, że wirus „LockBit" sprawiał najwięcej problemów. Jego wersja na system Linux nosi nazwę „LockBit Linux-ESXi Locker ". Źródło: *FBI 2022 Internet Crime Report*, s. 15

Raport grupy „Herjavec" donosi, że aż 70% organizacji medycznych borykało się z poważnymi komplikacjami przez ataki ransomware [5]. W 2022 roku 1 na 42 instytucje ochrony zdrowia były ofiarami tychże ataków, 74% z nich to szpitale [6].



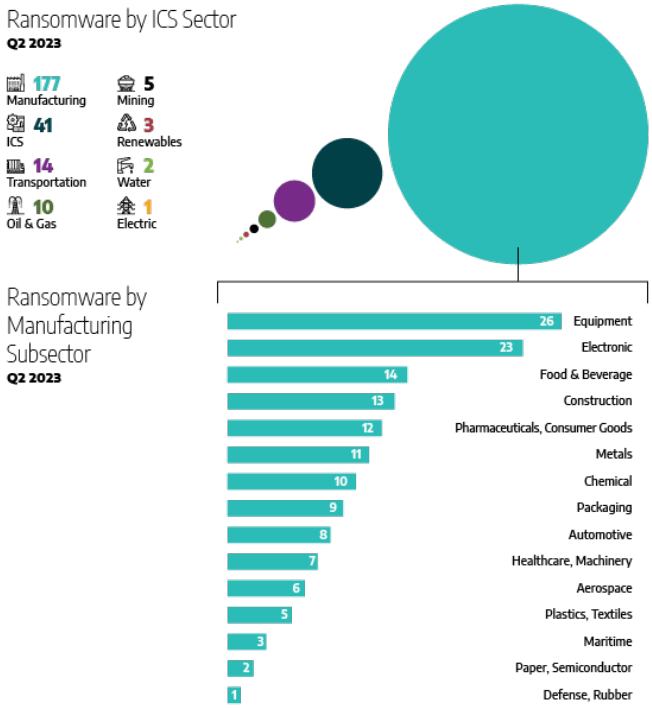
Rysunek 3. Średni koszt naruszenia danych 2016-2022. Źródło: *Cost of a Data Breach Report 2022*, figure 1, s. 9.

Z danych zebranych z ostatnich 5 lat jednoznacznie wynika, że nieumiejętne przeciwdziałanie może zaszkodzić nie tylko finansom zaatakowanej działalności lub osoby indywidualnej, ale również stwarza zagrożenie dla zdrowia i życia. Dodatkowo, mając na uwadze średni koszt naruszenia danych w 2023, którego globalna średnia wynosi 4,45 milionów USD [7], coraz więcej administratorów jest zmuszonych dywersyfikować sposoby zabezpieczania systemów.



Rysunek 4. Globalnie zgłoszone incydenty ataków ransomware per kwartał w roku 2022 zarejestrowanych przez Check Point Research. Organizacja spekuluje, że wzrost ataków mógł być spowodowany lukami bezpieczeństwa „log4j" oraz cyberataków związanych z wojną w Ukrainie. Źródło: *Check Point Research: Weekly Cyber Attacks increased by 32% Year-Over-Year; 1 out of 40 organizations impacted by Ransomware*, figure 1.

Na rynku istnieje wiele popularnych rozwiązań działających prewencyjnie m.in. w tym rozbudowane aplikacje służące do tworzenia i przywracania kopii zapasowych. Należy jednak wziąć pod uwagę, że przywracanie danych nie jest prostym procesem. W zależności od rodzaju użytego nośnika przywracanie może doprowadzić nawet do przypadkowej utraty danych przy zniszczeniu nośnika danych w przypadku taśm. Jest to także proces powolny, co w efekcie może spowodować poniesienie większych kosztów niż wartość okupu.
Rozwiązaniem, które wydaje się być aktualnie najlepszym, jest możliwie jak najwcześniejsze wykrycie potencjalnego źródła ataku. W przypadku, gdy te czynności zawiodą, jedyną możliwością na zmniejszenie strat jest minimalizacja skutków ataku na bieżąco. Aby tego dokonać, konieczne jest wczesne wykrycie ataku.



Rysunek 5. Incydenty ransomware per sektor gospodarki. Źródło: *Dragos Industrial Ransomware Attack Analysis: Q2 2023*, figure 2.

1.3 Krótka charakterystyka ataków ransomware

Ransomware można zdefiniować jako oprogramowanie, które blokuje atakowanemu dostęp do danych, do momentu zapłacenia okupu [8]. Prostsze ataki mogą sprowadzać się do blokady systemu bez uszkadzania plików, jednak większym zagrożeniem są tzw. „cryptovirological attacks" [9], czyli ataki wykorzystujące szyfrowanie danych jako formę blokady danych. Atakowany, jeśli nie posiada kopii zaszyfrowanych danych, musiałby odnaleźć klucz, którego użyto w szyfrowaniu. Nawet jeśli atakowany wie jakiego algorytmu użyto w ataku, to odnalezienie klucza jest problemem trudnym, zwłaszcza dla nowoczesnych algorytmów szyfrowania. Przykładowo, algorytm „AES" w zależności od klucza występuje w wariantach 128,192 oraz 256-bitowych, co daje między 2^{128} a 2^{256} możliwych wartości do sprawdzenia atakiem siłowym.

Przy wyłudzaniu okupu, atakujący stosują również techniki zastraszenia. Przykładowo wirus „WannaCry", którego duża fala ataków miała miejsce w 2017 roku [10], informował, że początkowy okup 300$ per maszyna wzrośnie dwukrotnie po 3 dobach zwłoki. Po upływie tygodnia odzyskanie

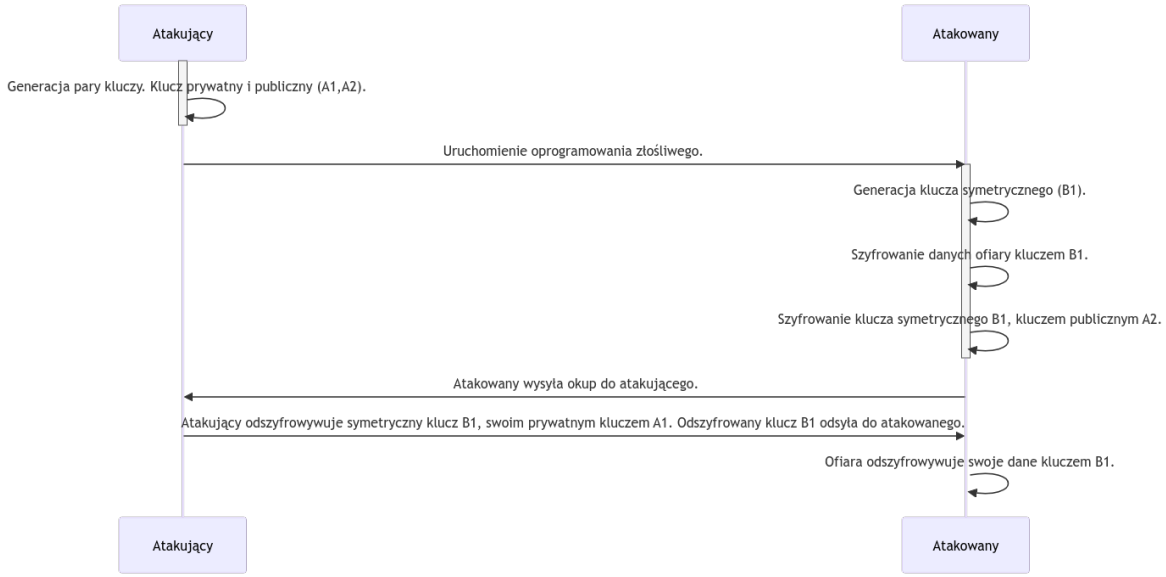
danych miałoby stać się niemożliwe. Atakujący wymagają, aby okup został spłacony w sposób trudny do wyśledzenia przez organy ścigania m.in. za pomocą kryptowalut.

Rysunek 6. Ekran wyświetlający się po zainfekowaniu komputera przez WannaCry. Atakujący wymaga od ofiary zapłaty Bitcoinem.

Ataki ransomware, mogą także założyć blokadę powłoki systemowej lub nawet dokonać modyfikacji partycji rozruchu jak w przypadku wirusa RedBoot [11].

Rysunek 7. Ekran rozruchu przy infekcji wirusem RedBoot.

Konceptualnie „cryptovirological attack" został przedstawiony w 1996 roku na konferencji IEEE Security & Privacy [12]. Opisuje się go jako protokół pomiędzy atakowanym, a atakującym:



Rysunek 8. Diagram sekwencji ataku ransomware.

Generowany klucz symetryczny ma charakter losowy i nie pomoże w odszyfrowaniu danych innej ofiary. Klucz prywatny jest przechowywany wyłącznie przez atakującego. Jedyny kontakt, jaki musi być wykonany bezpośrednio przez atakującego, następuje w momencie kiedy zaszyfrowany klucz symetryczny jest wysyłany do atakującego, a następnie klucz odszyfrowany do atakowanego.
Typowymi sposobami propagacji ransomware są:

- podszywanie się pod znane aplikacje czy strony internetowe,
- skuszenie ofiary do otworzenia niezaufanego załącznika listu elektronicznego,
- luki bezpieczeństwa sieci.

Rozdział 2

Przegląd literatury

W artykule opublikowanym przez firmę Microsoft o tytule „Co to jest cyberbezpieczeństwo ?" [1], trzy z sześciu wymienionych typów zagrożenia to:

- oprogramowanie wymuszające okup,
- inżynieria społeczna,
- wyłudzanie informacji.

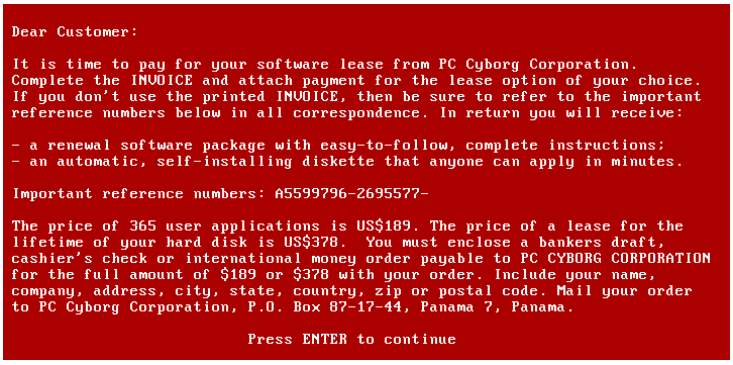
Autorzy prawdopodobnie nie bez powodu nazwali pierwszy z powyższych typów tak, a nie „atak oprogramowaniem wymuszjącym okup". Atak ransomware zawiera w sobie każde z tych zagrożeń. Oprogramowanie złośliwe wymaga od ofiary zaufania ,że to co uruchamia jest nieszkodliwe. Typowo propagacja takiego malware ma miejsce poprzez tzw. „phishing" czyli podszywanie się atakującego za zaufany serwis lub instytucję, z którymi ofiara mogła wejść w interakcję w przeszłości. Aby zrozumieć zakres tych technik oraz możliwe wektory ataku, należy prześledzić ich historię.

2.1 Historia i ewolucja ataków typu ransomware

2.1.1 Wczesna historia

Mimo stopniowego nasilania się ataków ransomware w przeciągu ostatnich 7 lat sama idea utrudnienia dostępu do plików pod groźbą okupu jest znana od dosyć dawna. Już w drugiej połowie lat 80-tych, w USA, cyberprzestępcy w zamian za odzyskanie dostępu do danych wyłudzali okup, który następnie był wysyłany drogą pocztową. Jednym z pierwszych udokumentowanych ataków wirusem ransomware był DOSowy „AIDS trojan" [13] z 1989 roku. Autor programu — Joseph Popp — przekazywał dyskietki drogą pocztową do wybranej grupy ofiar pod przykrywką załącznika do ulotki informacyjnej na temat wirusa AIDS. Program modyfikował plik `AUTOEXEC.BAT`, z którego korzystał w celu zliczenia ilości uruchomień komputera. W momencie przekroczenia liczby 90 uruchomień szyfrował nazwy wszystkich plików na dysku `C:`, tym samym uniemożliwiając korzystanie z systemu.

[1] Artykuł jest dostępny pod adresem: https://www.microsoft.com/pl-pl/security/business/security-101/what-is-cybersecurity



Rysunek 9. Wiadomość ukazująca się po aktywacji wirusa „AIDS trojan"

Atakujący podszywał się pod fikcyjną korporację „PC Cyborg Corporation", na której adres w Panamie miał być wysyłany okup. Paczka razem z dyskietką posiadała również ulotkę z krótkim wprowadzeniem, instrukcją obsługi, a także licencją co było w tamtym czasie powszechną i budzącą zaufanie praktyką. Program nie szyfrował treści samych plików, jedynie ich nazwy. Klucz szyfrowania był kluczem symetrycznym, co sprawiało, że złamanie go mogło pomóc odblokować system, każdej ofierze borykającej się z tą samą wersją wirusa. Eliminacja tej wady była inspiracją dla pracy „Cryptovirology: Extortion-Based Security Threats and Countermeasures", w której przedstawiono pojęcie „cryptovirological attack" [12].
Po roku 1996, w erze upowszechnienia się internetu, pojawiły się sporadyczne ataki ransomware na niewielką skalę, tym razem ulepszone o szyfrowanie hybrydowe. W latach dwutysięcznych pojawił się trudny do wykrycia „PGPCoder" [14] używający 660-bitowego klucza RSA. Innym ransomware występującym w tamtym czasie był „Archievus" [15], również używający klucza RSA, w wersji 1024-bitowej, którego tragiczną wadą było używanie tego samego klucza do szyfrowania każdego pliku na każdej zainfekowanej maszynie. Ataki te, aby zainfekować ofiarę, wykorzystywały phishing i podszywały się pod zaufane strony internetowe.

2.1.2 Historia współczesna

Mimo historii sięgającej jeszcze lat 80 - tych, ataki ransomware nie były szczególnie powszechne w latach dwutysięcznych. Status quo został zachwiany po upowszechnieniu się kryptowalut, umożliwiających poufną i trudną do wyśledzenia wymianę środków między ofiarą a atakującym. Jednak uzyskanie pieniędzy od ofiar niezaznajomionych z kryptowalutami nie było proste, dopiero kantory kryptowalut dały cyberprzestępcom możliwość prostego i poufnego wyłudzenia środków. Pierwsza dekada XXI w. była dla cyberprzestępców czasem udoskonalania „scareware" czyli oprogramowania mającego wystraszyć ofiarę na tyle, żeby zapłaciła za dostęp do stacji, bez wyrządzania szczególnej szkody na danych.
W 2013 roku w annały historii internetu wszedł Windowsowy wirus „CryptoLocker". Wykorzystywał on do szyfrowania 2048-bitową parę kluczy RSA, generowaną na osobnym serwerze, a następnie dostarczał klucz publiczny na stację ofiary w celu szyfrowania jej plików [16]. Tym samym ofiara

nie miała innej możliwości odzyskania plików niż zapłacić okup wynoszący 300 USD. Wirus dostarczany był jako załącznik w liście elektronicznym oraz przez owiany złą sławą „Gameover ZeuS botnet" [17]. Załącznik posiadał w sobie plik `.zip`, który z kolei zawierał w sobie plik `.exe`, z ikonką charakterystyczną dla pliku pdf. Atakujący wykorzystywał domyślne zachowanie Windowsa polegające na ukrywaniu rozszerzenia pliku. Następnie wirus podejmował następujące kroki:

1. rozpakowywał swoje pliki w ścieżce profilu użytkownika,
2. dodawał nową pozycję do windowsowego rejestru, który uruchamiał wirus wraz z rozruchem systemu,
3. pobierał klucz publiczny z jednego z serwerów,
4. wirus inicjował szyfrowanie plików na zamontowanych dyskach, w tym na dyskach sieciowych,
5. wyświetla ekran informujący o zdarzeniu i możliwości opłacenia okupu w BTC do 100 godzin od zaszyfrowania.

Po opłaceniu okupu ofiara miała możliwość pobrania programu dekodującego z załadowanym, odpowiednim kluczem prywatnym. Wirus szyfrował jedynie pliki z odpowiednimi rozszerzeniami m.in. pliki AutoCAD czy dokumenty MS Office.

Rysunek 10. Ekran wyświetlający się po zainfekowaniu komputera przez CryptoLocker.

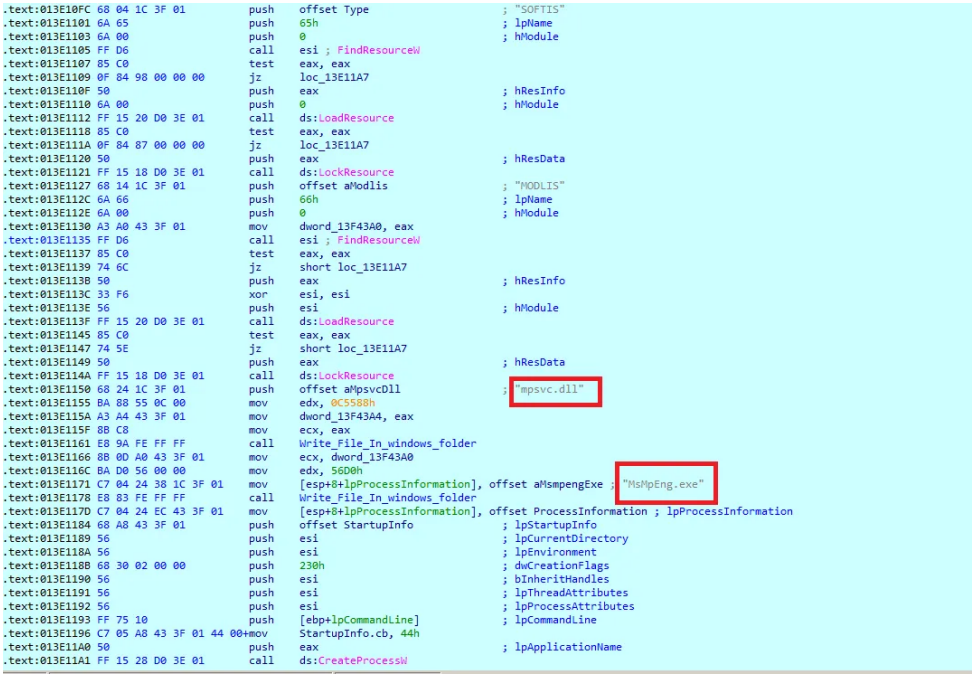
Zagrożenie zostało zneutralizowane w wyniku zainicjowanej przez departament sprawiedliwości USA, operacji „Tovar" [18] w wyniku której udało się uzyskać dostęp do bazy danych zawierającej prywatne klucze RSA na podstawie których możliwe było odzyskanie plików.

„CryptoLocker" był swego rodzaju kamieniem milowym w rozwoju cyberprzestępczości. Złożona natura procederu stała się normą dla ataków ransomware a wraz z coraz większą popularnością kryptowalut i usprawnionymi algorytmami szyfrowania asymetrycznego, ilość ataków oraz generowane przez nie straty stabilnie wzrastają aż do dnia dzisiejszego.
Aktualnie cyberprzestępcy zmienili styl ataku ze skupiającego się na infekcji jak największej ilości stacji, na tzw. „big game hunting" [2]. BGH w dużej mierze polega na koordynacji inżynierii społecznej i zaprojektowania oprogramowania ransomware w sposób, który będzie najbardziej szkodliwy dla dużych organizacji. Obierana jest mniejsza ilość celów na rzecz wyższej kwoty okupu. Raport „CrowdStrike Services" z 2023 roku donosi, że jedną najszerzej stosowanych taktyk BGH jest połączenie ransomware z groźbą upublicznienia skradzionych danych. Typowo dane zostają upubublicznione gdy minie termin zapłaty okupu. Naruszenie danych jest rozłożone w czasie i wykorzystuje narzędzia już dostępne na atakowanym środowisku. Dzięki temu ataki są cięższe do wykrycia [3]. Techniki zastraszenia zostały także dopracowane, aby wywołać możliwie na największą presję na ofiarach. W przypadku „REvil" kradzione dane bywały etapowo upubliczniane, aby zmusić ofiarę do szybszego działania [19].
Z powodu dużej opłacalności takich ataków utworzony został model „ransomware as a service" (RaaS), w którym klienci płacą za dokonanie ataku ransomware programem utworzonym przez inne grupy hakerskie [4].
Jednym z nich jest wcześniej wymieniony „REvil" używany przez grupę „PINCHY SPIDER", którego cechą rozpoznawczą jest postowanie skradzionych danych na blogu „Happy Blog" [19]. W 2021 roku użyto go na wysoką skalę [20] przez podatność Kaseya VSA [5] o identyfikatorze CVE-2021-30116 [21]. Atak ten można podsumować w następujących krokach:

1. użycie komendy `PowerShell` do zakończenia procesów Windows Defender,
2. podstawienie pliku wykonywalnego do katalogu instalacyjnego Windowsa,
3. zgodnie z techniką „Living off the land" wirus pobierał pomocnicze pliki wykonywalne i maskował je nazwami typowymi dla plików pomocniczych Windowsa np. `agent.exe`,
4. pobrane pliki następnie były przenoszone do odpowiednich folderów w celu załadowania ich razem z plikiem wykonywalnym `MsMpeng.exe` techniką nazywaną „DLL sideloading" [6]
5. w momencie wywołania przez `MsMpeng.exe` serwisów, na które ma zależności, ładowany jest podłożony wcześniej plik `.dll`, a razem z nim rozpoczyna się szyfrowanie danych na maszynie,

[2] Dokładniejszą definicję z przykładami można znaleźć pod adresem:
https://www.malwarebytes.com/blog/news/2023/07/ransomware-making-big-money-through-big-game-hunting
[3] Technika ta nosi nazwę „Living off the land"
[4] Wykorzystywane jest oprogramowanie utworzone przez inne osoby, podobnie jak w modelu Software as a Service.
[5] Kaseya VSA jest narzędziem do zarządzania infrastrukturą IT.
[6] DLL siedloading polega na załadowaniu pliku binarnego o innej treści niż oryginalna. Wykorzystuje się ją do aktywacji serwisów lub wykonywania procesów w sposób trudny do wykrycia przez użytkownika.

6. na pulpicie tworzony jest plik z instrukcją tłumaczącą jak spłacić okup w BTC na stronie ukrytej za TORem. [22]



Rysunek 11. Miejsce w pliku binarnym `agent.exe`, w którym wywoływany jest `MsMpeng` oraz ładowany plik `.dll`.

Innym znanym RaaS jest „DarkSide" używany przez grupę „CARBON SPIDER". Do niedawna skupiał się głownie na atakach maszyn Windowsowych, niedawno rozszerzając się na systemy Linux, VMware ESXi i vCenter [23]. Wirus w wersji Windowsowej obchodzi zabezpieczenia kontroli użytkownika za pomocą interfejsu `CMSTPLUA COM` [7], następnie sprawdza na podstawie lokalizacji i języka systemu w celu ominięcia ataku na maszynę z jednej z byłych republik radzieckich. Program podejmuje potem następujące kroki:

1. tworzy plik `LOG.<id użytkownika>.TXT` w którym przechowuje dane tymczasowe na temat progresu ataku,

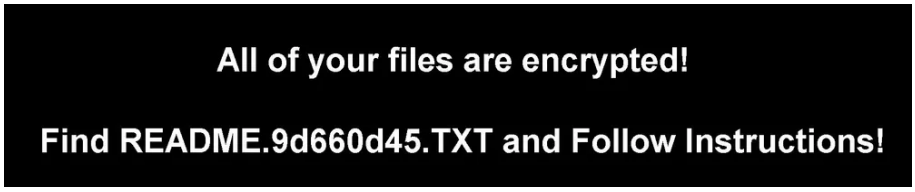
2. usuwa pliki w koszu, programy antywirusowe i zapewniające bezpieczeństwo oraz zamyka procesy blokujące mu dostęp do danych użytkownika,

3. rozpoczyna szyfrowanie algorytmem `Salsa20` przy pomocy losowo wygenerowanego klucza macierzowego,

4. klucz macierzowy jest szyfrowany zakodowanym na twardo kluczem RSA, a następnie łączony z zaszyfrowanym plikiem,

[7] Takie obejście można dokonać programem https://github.com/tijme/cmstplua-uac-bypass

5. pozostawia plik `README.<id użytkownika>.TXT` w którym wskazuje stronę ukrytą za TORem, na której ofiara ma dokonać płatność w BTC lub XMR.



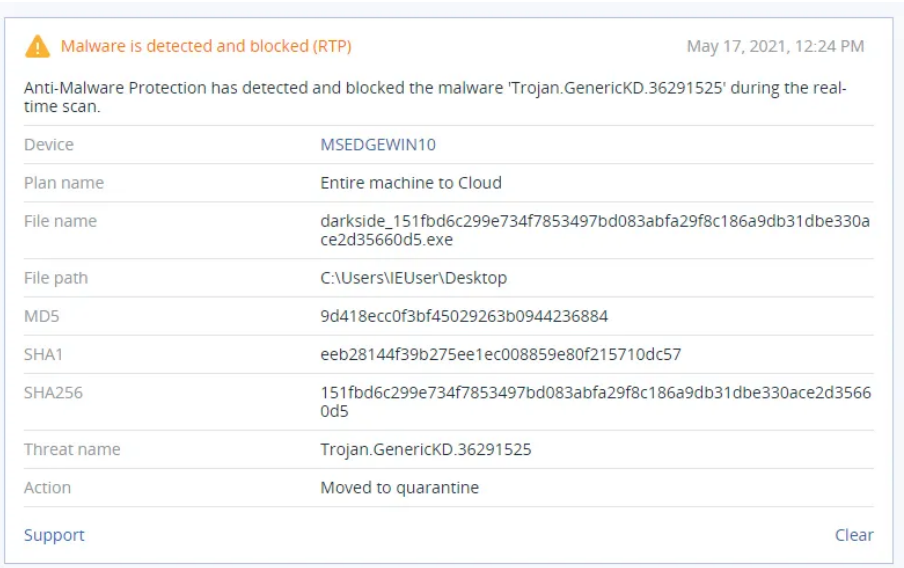
Rysunek 12. W wyniku działania wirusa tapeta użytkownika zostaje zmieniona na taką, jak widać na obrazku..

2.2 Istniejące techniki wykrywania i obrony przed ransomware

Niezależnie od tego czy atakujący korzysta z techniki „living off the land" lub stara się spowodować starty w możliwie najmniejszym przedziale czasowym, kluczem w minimalizacji kosztów ataku ransomware najważniejsza jest szybka reakcja. Aby to osiągnąć należy podjąć inteligentną strategię, która doprowadzi do możliwie jak najwcześniejszego wykrycia ataku. Jeśli administrator zostanie poinformowany dostatecznie wcześnie o zagrożeniu, będzie możliwa izolacja, a pa następnie eliminacja zagrożenia. Takie podejście w połączeniu z zdyscyplinowanym harmonogramem kopii zapasowych, jest w stanie zredukować straty niemalże do zera.
Wyróżnia się trzy główne metody wykrywania ataku: poprzez sygnaturę plików, poprzez analizę nietypowego dla systemu zachowania oraz poprzez monitorowanie ruchu sieciowego [24].

2.2.1 Wykrywanie poprzez sygnaturę plików

Zasada działania tego typu wykrywania jest bardzo prosta. Oprogramowanie ma pewne unikalne cechy, na podstawie których wyliczana jest jego sygnatura. Do tych cech należą zakodowane na twardo nazwy domen, adresy IP oraz inne identyfikatory. Typowo także wykorzystywana jest wartość funkcji skrótu. Aby metoda ta mogła być skuteczna musi istnieć często aktualizowana baza danych zawierająca sygnatury wszystkich napotkanych typów ransomware. Niestety sposób ten jest ograniczony do wirusów napotkanych w przeszłości i nie jest nim możliwe wykrycie unikalnego zagrożenia.



Rysunek 13. Tradycyjne antywirusy tak jak pokazany na obrazku Acronis, korzystają z metody wykrywania poprzez sygnaturę.

2.2.2 Wykrywanie poprzez analizę zachowania systemu

W przeciwieństwie do wcześniej wymienionego sposobu, wykrywanie poprzez analizę zachowania system nie opiera się na sprawdzeniu treści pliku wykonywalnego, a na wykryciu kroków, charakterystycznych dla naruszenia bezpieczeństwa systemu. W przeciwieństwie do poprzedniego rozwiązania, ta metoda jest przystosowana do kontrowania techniki „living off the land". Dziedzina wykrywania behawioralnego wirusów stała się m.in. obiektem badań algorytmami opartymi o sztuczną inteligencję [24]. Branych pod uwagę może być wiele zdarzeń, z których najbardziej charakterystyczne są:

- wywoływanie pewnej grupy komend powłoki systemu,
- pobieranie otwarto-źródłowych programów do penetracji systemów,
- wykorzystywanie pewnej grupy zmiennych środowiskowych jako argumenty wywołań,
- użycie pewnej grupy wywołań systemowych w ciągu, jedno po drugim,
- duży ruch w katalogach domowych użytkowników lub w `/tmp`,
- zmiana atrybutów i właścicieli plików, katalogów czy punktów montowania dysków.

Jedną z najpowszechniejszych metod, używanym przez atakujących do powiadomienia ofiary o ataku i metodzie odzyskania dostępu do danych jest pozostawienie pliku tekstowego w miejscu łatwym do znalezienia np. w katalogu domowym użytkownika. Inną jest tworzenie pliku tymczasowego przechowującego stan zaawansowania ataku. Ze względu na to, część metod wykrywania ransomware skupia się na wyszukiwaniu tego typu plików, na podstawie treści techniką „bag-of-words" [8] w celu

[8] Jest to technika przedstawienia tekstu w modelu nieułożonej kolekcji słów. Wykorzystuje się ją m.in. w przetwarzaniu języka naturalnego.

odnalezienia korelacji między terminami typowymi dla takich dokumentów np. „encrypted", „ransom" etc.

2.2.3 Wykrywanie poprzez analizę ruchu sieciowego

Wykrywanie poprzez analizę ruchu sieciowego polega na ograniczenia analizy behawioralnej do wyłącznie monitorowania adresatów i treści pakietów komunikacji sieciowej. Szczególne zainteresowanie stanowią transfery danych do maszyn o nieznanych i podejrzanych adresach oraz domenach. Zgodnie z techniką „living off the land", atakujący stara się możliwe minimalizować komunikację z serwerami zewnętrznymi które mogą zostać uznane za podejrzane. Mimo to znakomita większość narzędzi hakerskich, jest ogólnodostępna i dobrze znana w branży cyberbezpieczeństwa i tym samym łatwa do wykrycia [25].

Narzędzie	Strona
7zip	7-zip.org
AdFind	joeware.net
Advanced IP Scanner	advanced-ip-scanner.com
AnyDesk	anydesk.com
Proces Hacker	processhacker.sourceforge.io
rclone	rclone.org
WinSCP	winscp.net

Tabela 1. Tabela popularnych narzędzi używanych przez operatorów ransomware i odpowiadające im strony. Dane pochodzą ze strony: https://lots-project.com/

2.3 Podstawy działania systemów plików

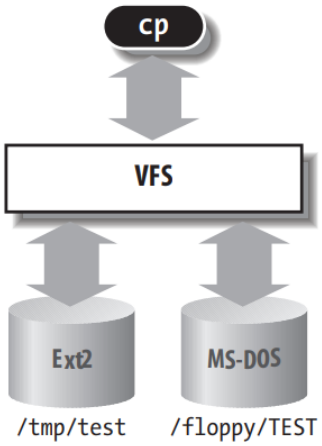
Struktura i działanie systemu plików na Linuksach jest bardzo szerokim tematem. Na potrzeby analizy behawioralnej ataku ransomware przybliżę w tej sekcji po krótce działanie i wybrane, interesujące szczegóły implementacyjne.

2.3.1 Skrócony opis działania systemu plików

Najpopularniejsze dystrybucje systemu Linux korzystają w większości z systemu plików o nazwie `ext4`. Wprowadzony do repozytorium jądra systemowego w 2008 roku, zyskał wielkie poważanie dzięki nowoczesnej obsłudze nośników danych oraz ulepszeniu systemu księgowania operacji, wprodzanego w `ext3`. Księgowanie operacji w systemie plików polega na przechowywaniu zapisów jako *transakcji*. Dopiero jeśli transakcja zakończy zapisywanie na dysk, jej dane zostają wprowadzone na system plików [26]. W efekcie oznacza to, że w wypadku zaniechania działania systemu w trakcie zapisu, transakcja zostanie cofnięta po ponownym rozruchu i tym samym zachowana zostanie spójność systemu plików.

Obsługa wielu rodzajów systemu plików jest możliwa dzięki istnieniu *virtualnego systemu plików*. Jest

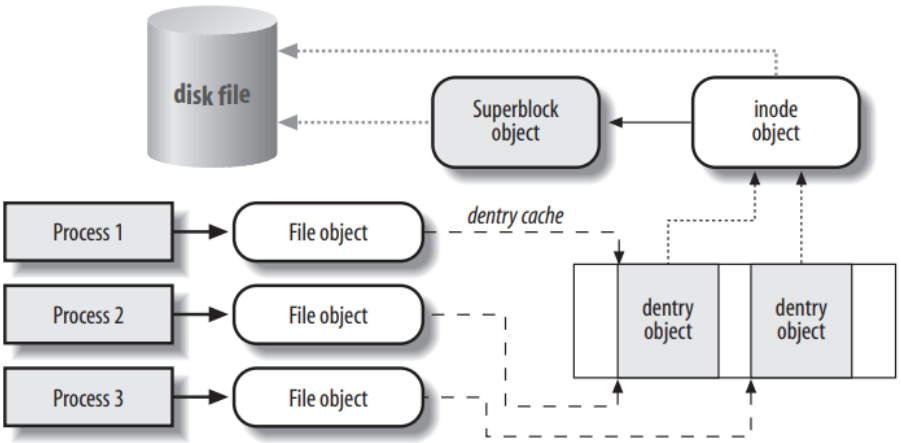
on warstwą abstrakcji pomiędzy konkretnymi jej implmentacjami, a aplikacjami klienckimi. Dzięki temu możliwa jest spójna i ujednolicona interakcja z systemem plików oraz interoperowalność między różnymi jego implementacjami. [27]




```
inf = open("/floppy/TEST", O_RDONLY, 0);
outf = open("/tmp/test",
       O_WRONLY|O_CREAT|O_TRUNC, 0600);
do {
    i = read(inf, buf, 4096);
    write(outf, buf, i);
} while (i);
close(outf);
close(inf);
```

Rysunek 14. Rola wirtualnego systemu plików w operacji kopiowania. Źródło: „Understanding Linux Kernel 3rd edition", Figure 12-1 s. 457.

Ogólna zasada działania wirtualnego systemu plików polegna na podmienianiu przez nią typowych wywołań systemowych takich jak `read` lub `write` na funkcje natywne dla konkretnego systemu plików np. `ZFS` lub wcześniej wymieniony `EXT4`. Każda implementacja musi móc przetłumaczyć swoją wewnętrzną strukturę organizacyjną na model ogólny wirtualnego systemu plików [27].



Rysunek 15. Interkacja pomiędzy procesami a objektami wiortualnego systemu plików. Źródło: „Understanding Linux Kernel 3rd edition", Figure 12-2 s. 460.

Infromacje na temat interakcji pomiędzy otwartym plikiem a procesem są przechowywane w charakterystycznym dla procesu otwierającego plik „file object". Informacje te istnieją *wyłącznie* w pamięci jądra systemu kiedy plik jest otwarty przez proces.

2.3.2 Monitorowanie zmian na systemie plików

Jądro systemu, nie może utrzymywać zakodowanej na twardo implementacji operacji na systemie plików ze względu na ich różnorodność. Utrzymyany jest więc indeks wskaźników do odpowienich implementacji operacji. Taka struktura komunikacji między systemem plików a jądrem pozwala na śledzienie wywołań oprogramowaniem pośrednim. Jądro Linux zawiera w sobie dwie ciekawe z poziomu tematu pracy impelmentacje takich „pośredników": „inotify subsystem" oraz „Linux Auditing Framework".

API inotify

Podsystem inotify został stworzony z myślą o monitorowaniu oraz powiadomianiu o zmianach na dysku [28]. Jego głównym przypadkiem użycia jest automatycze aktualizowanie widoków katalogów, plików konfiuguracyjncyh, zmian logów systemowych i tym podobnych. Rozwiązanie to znajduje się w kodzie źródłowym jądra Linux od sierpnia 2005 roku. Interfejs programowalny dla tego nardzędzia zawiera się w biliotece `inotify-tools`, które zawiera w sobie również pakiet narzędzi będących gotowymi implementacjami funkcjonalności API [29].

```
$ cat inotify-test.sh
#/bin/bash
inotifywait -m /home/user/box -e create -e moved_to |
while read -r directory action file; do
        echo "File has been created!"
done
$ ./inotify-test.sh
Setting up watches.
Watches established.
[1]  + 13180 suspended  ./inotify-test.sh
$ touch box/h2
$ fg
[1]  + 13180 continued  ./inotify-test.sh
File has been created!
```

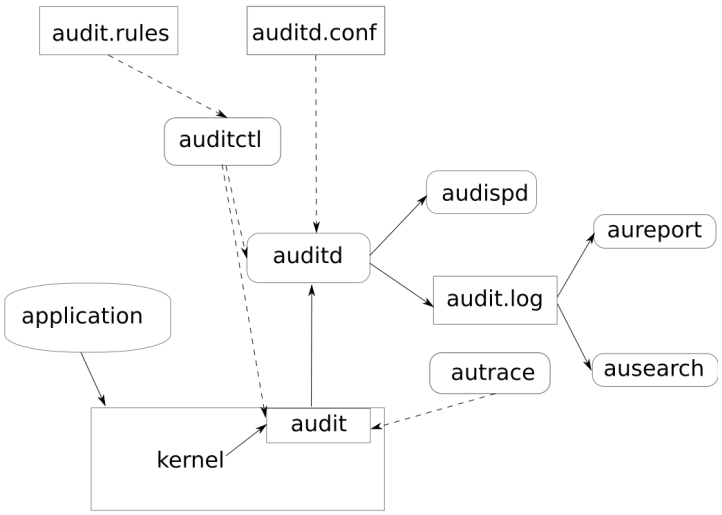
Listing 1. Przykład użycia narzędzia `inotifywait`. Po utworzeniu pliku ukazała się odpowiednia wiadomość

Niestety rowziwązanie to nie jest perefekcyjne i ma swoje limity. Do nich należą:

- brak wsparcia dla rekurencyjnego obserwowania ścieżek,
- „gubienie" niektórych wydarzeń dla starszych wersji jądra Linux,
- brak wsparcia niektórych wydarzeń przed wersją 5.13 jądra Linux [30],
- brak obserwacji dysków sieciowych.

Linux Auditing Framework

Projekt Linux Auditing Framework to podsystem wbudowany w jądro systemu Linux, którego zadaniem jest przechwytywanie, a następnie logowanie operacji systemowych. Jego możliwości nie ograniczają się wyłacznie do obserwacji systemu plików. Jest on w pełni zgodny z CAPP [9], a więc może być używany jako wiarygodne źródło informacji o stanie systemu. Informacje można pobierać dzięki aplikacji po stronie użytkownika o nazwie `auditd`. Ten z kolei ma możliwość zapisania logów do pliku lub stworzyć gniazdko UNIXowe do którego inna aplikacja w przestrzeni użytkownika może się podłączyć i zczytywać dane.



Rysunek 16. Bardzo uproszczony diagram komponentów LAF.
Źródło: https://documentation.suse.com/sles/12-SP5/html/SLES-all/cha-audit-comp.html

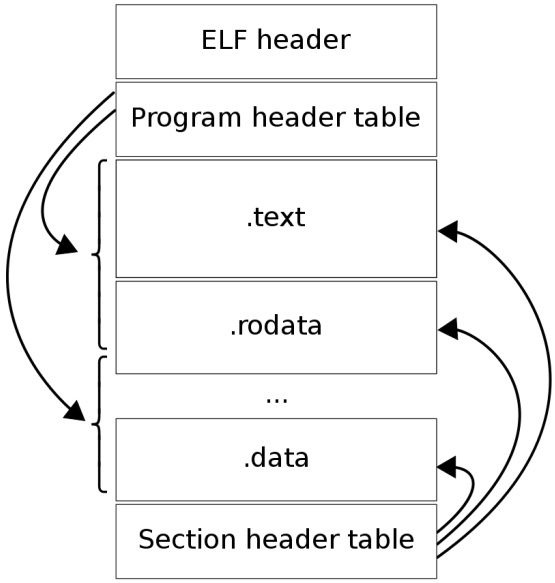
Niestety bardzo ciężko jest znaleźć informacje na temat implementacji części systemu która znajduje się w jądrze, ale na podstawie własnej analizy kodu zawartego w repozytorium głównym projektu [10] , w szczególności w plikach `audit.c`, `audit_fsnotify.c` oraz `auditsc.c` w folderze `kernel`, mogę z dużą dozą pewności stwierdzić, że infromacje wykryte tym narzędziem są wiarygodne i przydatne z perspektywy tematu pracy. W branży administracji systemami jest to narzędzie dobrze znane i poważane dzięki możliwościom łatwej i bezinwazyjnej konfiguracji. Popularne dystrybucje serwerowe takie jak Ubuntu Server, SLES, Red Hat oraz Fedora wspierają w pełni funkcjonalności związane z monitorowaniem systemu plików.

2.3.3 Krótka charakterystyka plików wykonywalnych

System Linux pliki wykonywalne zapisuje i odczytuje w formacie `ELF` czyli „Executable Linking Format" [31]. Najciekawszym elementem teo formatu, z punktu widzenia tej pracy, jest nagłówek.

[9] Controlled Access Protection Profiles to środowisko służące do niezależnej oceny, analizy i testowania produktów w celu ustanowienia wymagań bezpieczeństwa.
[10] Pod adresem: https://github.com/linux-audit/audit-kernel

Mimo, że nie zawiera tak wielu informacji co nagłówki plików wykonywalnych na systemie Windows, warto przyjrzeć się mu aby móc zidentyfikować obecność oprogramowania złośliwego lub narzędzia typowo wykorzystywanego podczas naruszenia bezpieczeństwa systemu.



Rysunek 17. Podział wewnętrzny pliku `ELF`.
Źródło: https://upload.wikimedia.org/wikipedia/commons/7/77/Elf-layout–en.svg

W mojej opinii ciekawą sekcją jest `.note.gnu.build-id` [32]. Cytując `elf(5)` Linuksowego `man pages`: „This section is used to hold an ID that uniquely identifies the contents of the ELF image. Different files with the same build ID should contain the same executable content [...]". Oznacza to, że można dzięki niemu *zidentyfikować konkretną kompilację aplikacji*. W przeciwieństwie do systemu Windows, gdzie typowo użytkownik pobiera już wcześniej przekompilowane pliki wykonywalne, bardzo popularnym rozwiązaniem na Linuksach jest kompilowanie lokalnie. Wyjątkiem są zaufane repozytoria, do których dostęp uzyskuje się przez menadżer pakietów dodawany do danej dystrybucji, np. `apt`. Mimo, że możliwa jest identyfikacja zawartości pliku binarnego poprzez wyliczenie jej wartości funkcji skrótu w niedługim czasie funkcją md5, identyfikator kompilacji dla tych samych warunków kompilacji i zawartości kodu wykonywalnego, będzie dokładnie taki sam. Informacja ta może być wykorzystywana do identyfikacji tego czy podejrzany plik binarny został skompilowalny lokalnie z kodu źródłowego.

```
$ cargo build --release
    Finished release [optimized] target(s) in 0.13s
$ readelf --notes target/release/linux-fs-audit | grep "Build ID"
    Build ID: ff6019887a97bedc98a8eca3267817233a13a8bc
$ rm target/release/linux-fs-audit
$ cargo build --release
    Finished release [optimized] target(s) in 0.04s
$ readelf --notes target/release/linux-fs-audit | grep "Build ID"
    Build ID: ff6019887a97bedc98a8eca3267817233a13a8bc
```

Listing 2. Test rekompilacji aplikacji napisanej w języku Rust. Mimo ponownej kompilacji, przy braku zmiany kodu źródłowego, identyfikator pozostał ten sam. Można więc z dużą pewnością stwierdzić, że plik wykonywalny był skompilowalny na tej maszynie, a nie pobrany z internetu.

2.4 Metody analizy statystyk systemu plików

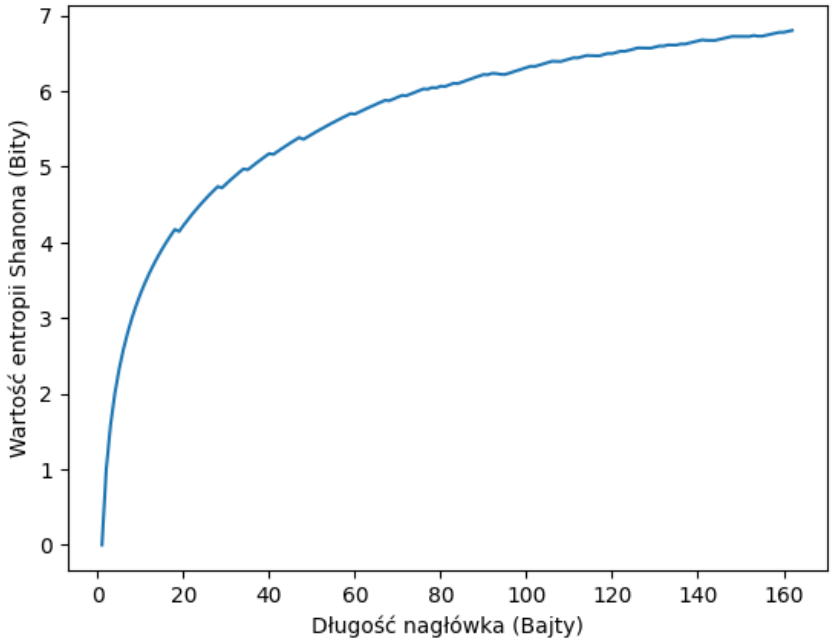
Ta praca skupia się na metodach analizy opisanych po krótce w rozdziale Wykrywanie poprzez analizę zachowania systemu. Metody te zgodnie z naturą pracy będą skupione na zachowaniu i treści systemu plików. Wraz ze wzrostem ryzyka ataków ransomware, wzrosła też ilość prac i teorii na temat tego jak taki atak wykryć na podstawie statystyk systemowych. W tym rozdziale chciałbym wymienić i po krótce wytłumaczyć, w mojej opinii, najciekawsze z nich.

2.4.1 Analiza entropii pliku

W pracy „Differential area analysis for ransomware attack detection within mixed file datasets" [33] przedstawiona jest metoda potencjalnego wykrycia tego czy plik został zaszyfrowany poprzez obliczenie entropii pliku dla różnych wielkości nagłówka. Nagłówek w kontekście tej metody po prostu oznacza ilość bajtów braną pod uwagę w obliczaniu entropii, a niekoniecznie twardo sprecyzowany w specyfikacji rodzaju pliku obszar. Maksymalna możliwa entropia per bajt dla pliku jest równa ośmiu bitom na jeden bajt, wartość sugerująca kompletnie losową naturę pliku. Wzór na entropię H [34] to:

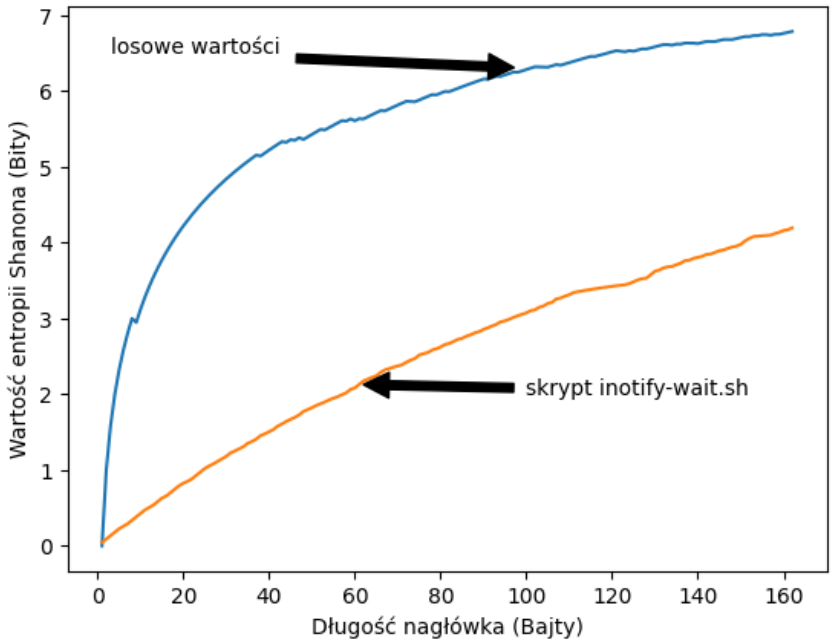
$$H(X) = -\sum_{i=1}^{n} P(x_i) log_2 P(x_i)$$

gdzie n jest liczbą bajtów w próbce, a $P(x_i)$ to prawdopodobieństwo wystąpienia bajtu i w strumieniu bitów. Wyobraźmy sobie, że mamy wygenerowane 150 bajtowy plik który został wygenerowany losowo. Jego wykres entropi naliczonej od długości nagłówka x będzie przypominał funkcję $log_2(x)$.



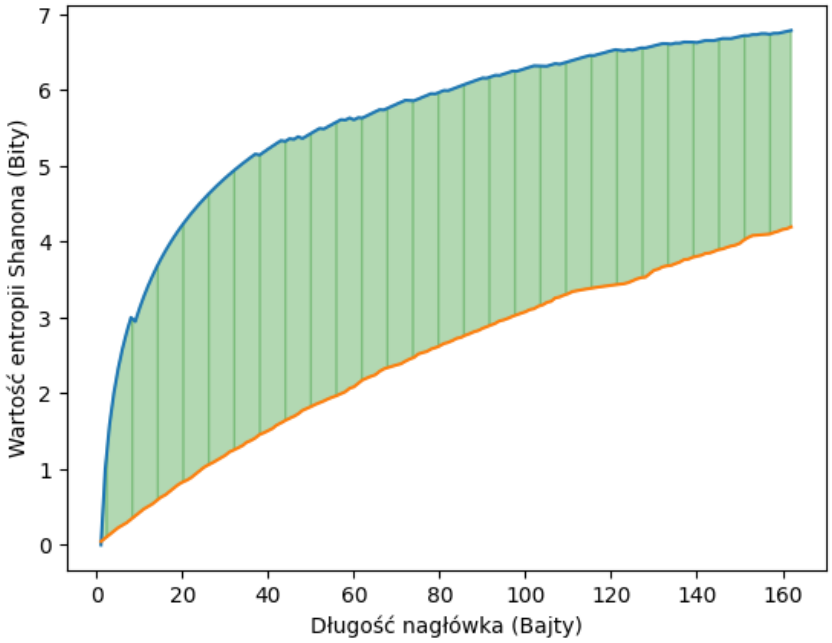
Rysunek 18. Wykres entropii od długości nagłówka dla pliku zawierającego zupełnie losowe dane.

Dla plików, rzeczywistych plik wartość entropii będzie rosnąć w mniejszym tępe, ze względu na powtarzające się schematy w informacji.



Rysunek 19. Zestawienie wykresów entropii od długości nagłz ówka. Jako plik przykładowy wybrałem skrypt z sekcji Monitorowanie zmian na systemie plików.

Miarą tego jak duże jest prawdopodobieństwo, że plik został zaszyfrowany jest pole między tymi dwoma wykresami.



Rysunek 20. Pole między wykresem losowego i rzeczywistego pliku o takich samych długościach.

W pracy „Differential area analysis for ransomware attack detection within mixed file datasets" zasugerowane są pewne wartości klasyfikacyjne, ustalone na podstawie zdobytej dokładności wykrycia zaszyfrowanego pliku.

Table 7 – Classification Accuracy Results (%).

Header Length (Bytes)	Classification Criteria (Bit-Bytes) 8	24	40	56	72
32	63.290	20.097	19.439	14.061	11.767
64	99.010	87.851	46.472	24.227	19.879
96	98.546	99.914	99.842	87.077	51.326
128	98.118	99.903	99.944	99.794	89.289
160	96.736	99.825	99.960	99.934	96.439
192	97.452	99.744	99.957	99.952	98.959
224	97.234	99.631	99.954	99.957	99.517
256	97.055	99.505	99.944	99.962	99.713

Table 8 – Classification Precision Results (%).

Header Length (Bytes)	Classification Criteria (Bit-Bytes) 24	40	56	72
96	99.369	98.503	44.651	17.640
128	100	99.462	98.058	49.324
160	100	99.656	99.371	74.537
192	100	100	99.553	90.923
224	100	100	99.621	95.596
256	100	100	99.690	97.343

Rysunek 21. Skuteczność dla wybranych kryteriów klasyfikacji na długość nagłówka w bajtach. Źródło: Differential area analysis for ransomware attack detection within mixed file datasets, Table 7, Table 8, s. 11.

Metoda ta wydaje się być bardzo obiecująca lecz do jej ograniczeń należą wymagania co do odpowiedniej wielkości pliku.

2.4.2 Automatyczna analiza behawioralna poprzez audyt systemu

W pracy „Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware" [35] opisana jest metoda identyfikacji ransomware poprzez wyciągnięcie z logów audytu podczas rutynowego działania systemu. W przypadku tej pracy poszukiwanie abnormalnych zachowań systemu było oparte **wyłącznie** na wiedzy o tym, że atak ma miejsce. System do audytowania systemu w pracy ma podobne możliwości do wymienionego w sekcji Monitorowanie zmian na systemie plików Linux Auditing Framework.
Przedstawiona metoda opera się o „Term-Frequency-Inverse-Document-Frequency (TF-IDF)" [36] czyli metrykę obliczania wagu słów w oparciu o liczbę wystąpień, dostosowaną do faktu częstszego występowania niektórych słów. Jest to metoda często wykorzysytwana w jako forma wydobywania informacji z tekstów m.in. „text miningu". TF-IDF jest produktem dwóch statystyk: częstotliwości występowania słowa or odwrotnej częstotliwości dokumentu. Częstotliwość występowania słowa zapisuje się wzorem:

$$tf(t,d) = \frac{f_{t,d}}{\sum_{t' \in d} f_{t',d}}$$

a odwrotną częstotliwość dokumentu:

$$idf(t,D) = log \frac{N}{1 + |d \in D : t \in d|}$$

gdzie słowo t, występujące w dokumencie d i wielkości zbuioru dokumentów (corpus) N, występuje z częstotliwością $f(t,d)$.
Niestety metoda ta nie przynosi szczególnych efektów. We wcześniej wymienionej pracy, zostały wykonane dwa eksperymenty: pierwszy w którym były wyłącznie logi z działania wirusa WannaCry oraz normalnych zachowań w systemie w osobnych dokumentach, drugi w którym przemieszane były działania wirusa z normalnym działaniem systemu w tym samym dokumencie.

Name	Meaning
b.wnry	Bitmap file for Desktop image
c.wnry	Configuration file
r.wnry	Q&A file, payment instructions
s.wnry	Tor client
t.wrny	WANACRY! file with RSA keys
u.wnry	@WannaDecryptor@.exe
\msg	Folder containing RTF files with payment instructions in 128 languages (e.g., korean.wnry)
taskse.exe	Launches decryption tool
taskdl.exe	Removes temporary files

Rysunek 22. Tabela plików tymczasowych wykorzystywanych przez wirus WannaCry. Źródło: Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware, Table I, s. 2.

Feature	Ranking (case 1)	Ranking (case 2)
"enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\s.wnry"	1	2
"enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\b.wnry"	2	7
"enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\u.wnry "	4	13
"enhanced:_object=file+event=read+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\t.wnry ", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\msg\\m_korean.wnry ", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\msg\\m_vietnamese.wnry "	7	32
"enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\msg\\m_chinese (traditional).wnry", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\msg\\m_japanese.wnry"	8	36
"enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\msg\\m_chinese (simplified).wnry", "enhanced:_object=file+event=write+data=file: c:\\docume 1\\cuckoo\\locals 1\\temp\\msg\\m_romanian.wnry "	9	40
"enhanced:_object=file+event=write+data=file: c:\\docume 1\\cuckoo\\locals 1\\temp\\msg\\m_bulgarian.wnry " ...**(22 various language features)** "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\msg\\m_turkish.wnry"	10	45
"enhanced:_object=file+event=read+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\c.wnry ", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\c.wnry", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\taskdl.exe", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\taskdl.exe", "enhanced:_object=registry+event=read+data=regkey: \\ activecomputernamemachineguid"	12	54
"enhanced:_object=registry+event=read+data=regkey: hkey_local_machine\\software\\microsoft\\cryptography\\defaults\\provider\\ microsoft enhanced rsa and aes cryptographic provider (prototype)image path"	9	58
"bigram:_api=regcreatekeyexw+arguments=software\\wanacrypt0r", "enhanced:_object=dir+event=create+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\msg", "enhanced:_object=file+event=execute+data=file:attrib +h . ", "enhanced:_object=file+event=execute+data=file:icacls . /grant everyone:f /t /c /q ", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\00000000.pky", "enhanced:_object=file+event=write+data=file: c:\\docume~1\\cuckoo\\locals~1\\temp\\r.wnry"	16	80

Rysunek 23. Tabela wyników z eksperymentu. Eksperyment pierwszy i drugi są tutaj nazwane „case 1" i „case 2". Rankingi są wyliczone na podstawie wartości wagi TF-IDF ze wszystkich dokumentów. Źródło: Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware, Table V, s. 5.

Jak widać z tabelki, waga informacji o działaniu ransomware znacznie zmalała po połączeniu z logami działania systemu. Audyt systemu może być przydatny dla zaznajomionego z infrastrukturą administratora lecz sama jej analiza nie jest skuteczna w wykrywaniu ransomware. Tym samym informacja o dokonaniu operacji na systemie plików, sama w sobie nie wystarczy do wykrycia ataku.

Rozdział 3

Niebanalny tytuł kolejnego rozdziału

Rozdział 4

Podsumowanie

- Teoria: wiemy jak ma działać, ale jednak nie działa.
- Praktyka: działa, ale nie wiemy – dlaczego?
- Łączymy teorię z praktyką: nic nie działa i nie wiemy, dlaczego.

Więcej informacji na temat LaTeXa:

- <https://www.overleaf.com/learn> – przystępny tutorial na stronie Overleaf,
- <https://www.latex-project.org/> – strona domowa projektu,
- <https://www.tug.org/begin.html> – dobry zbiór odnośników do innych materiałów.

Powodzenia!

Bibliografia

[1] THE RADICATI GROUP, I., *Email Statistics Report 2019 2023 Executive Summary*, English, lut. 2019. adr.: https://radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf (term. wiz. 26. 11. 2023).

[2] *Data Never Sleeps 10.0 | Domo*, en. adr.: https://www.domo.com/data-never-sleeps (term. wiz. 26. 11. 2023).

[3] Petrosyan, A., „Worldwide number of ransomware attacks 2022," en, spraw. tech. adr.: https://www.statista.com/statistics/1315826/ransomware-attacks-worldwide/ (term. wiz. 26. 11. 2023).

[4] Petrosyan, A., „Number of ransomware attempts per year 2022," en, spraw. tech. adr.: https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/ (term. wiz. 26. 11. 2023).

[5] Herjavec, G., „Healthcare Cybersecurity Report Q4 2021," spraw. tech. adr.: https://www.herjavecgroup.com/wp-content/uploads/2021/10/2021-Healthcare-Cybersecurity-Report.pdf (term. wiz. 26. 11. 2023).

[6] Check Point Research, T., *Check Point Research: Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends*, en-US, paź. 2022. adr.: https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks/ (term. wiz. 26. 11. 2023).

[7] Petrosyan, A., *Global average cost of a data breach 2023*, en. adr.: https://www.statista.com/statistics/987474/global-average-cost-data-breach/ (term. wiz. 26. 11. 2023).

[8] *Stop Ransomware | CISA*, en. adr.: https://www.cisa.gov/stopransomware (term. wiz. 26. 11. 2023).

[9] Young, A. i Yung, M., „Cryptovirology: extortion-based security threats and countermeasures," w *Proceedings 1996 IEEE Symposium on Security and Privacy*, 1996, s. 129–140. DOI: 10.1109/SECPRI.1996.502676.

[10] Czarnecki, M., „Oto Marcus Hutchins, 22-letni Brytyjczyk, który zatrzymał światowy cyberatak," pl, *wyborcza.pl*, maj 2017. adr.: https://wyborcza.pl/7,75399,21816943,oto-marcus-hutchins-22-letni-brytyjczyk-ktory-zatrzymal-swiatowy.html (term. wiz. 26. 11. 2023).

[11] NHS, *RedBoot - Ransomware that Encrypts the Hard Drive Permanently*, en. adr.: https://digital.nhs.uk/cyber-alerts/2017/cc-1673 (term. wiz. 29. 11. 2023).

[12] Young, A. L. i Yung, M., „Cryptovirology: The Birth, Neglect, and Explosion of Ransomware," *Commun. ACM*, t. 60, nr. 7, s. 24–26, czer. 2017, ISSN: 0001-0782. DOI: 10.1145/3097347. adr.: https://doi.org/10.1145/3097347.

[13] „Virus Bulletin, January 1990," en, 1990.

[14] Tromer, E., „Cryptanalysis of the Gpcode.ak ransomware virus," en,

[15] *Arhiveus Ransomware Trojan Threat Analysis*, en. adr.: https://www.secureworks.com/research/arhiveus (term. wiz. 05. 12. 2023).

[16] *CryptoLocker Ransomware Information Guide and FAQ*, en-us. adr.: https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information (term. wiz. 06. 12. 2023).

[17] *Office of Public Affairs | U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator | United States Department of Justice*, en, czer. 2014. adr.: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (term. wiz. 06. 12. 2023).

[18] *'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge – Krebs on Security*, en-US, czer. 2014. adr.: https://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/ (term. wiz. 06. 12. 2023).

[19] Hern, A., „Ransomware hackers steal plans for upcoming Apple products," en-GB, *The Guardian*, kw. 2021, ISSN: 0261-3077. adr.: https://www.theguardian.com/technology/2021/apr/22/ransomware-hackers-steal-plans-upcoming-apple-products (term. wiz. 06. 12. 2023).

[20] McMillan, R., „Ransomware Attack Affecting Likely Thousands of Targets Drags On," en-US, *Wall Street Journal*, lip. 2021, ISSN: 0099-9660. adr.: https://www.wsj.com/articles/ransomware-group-behind-meat-supply-attack-threatens-hundreds-of-new-targets-11625285071 (term. wiz. 06. 12. 2023).

[21] *Kaseya was fixing zero-day just as REvil ransomware sprung their attack*, en-us. adr.: https://www.bleepingcomputer.com/news/security/kaseya-was-fixing-zero-day-just-as-revil-ransomware-sprung-their-attack/ (term. wiz. 06. 12. 2023).

[22] huntresslabs, *Crticial Ransomware Incident in Progress*, Reddit Post, lip. 2021. adr.: www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/ (term. wiz. 06. 12. 2023).

[23] *New attack vectors for the DarkSide ransomware gang*, en. adr.: https://www.acronis.com/en-sg/cyber-protection-center/posts/new-attack-vectors-for-the-darkside-ransomware-gang/ (term. wiz. 06. 12. 2023).

[24] Vehabovic, A., Ghani, N., Bou-Harb, E., Crichigno, J. i Yayimli, A., „Ransomware Detection and Classification Strategies," en, w *2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Sofia, Bulgaria: IEEE, czer. 2022, s. 316–324, ISBN: 978-1-66549-749-7. DOI: 10.1109/BlackSeaCom54372.2022.9858296. adr.: https://ieeexplore.ieee.org/document/9858296/ (term. wiz. 07. 12. 2023).

[25] *Community Night SANS Secure Australia 2023 - Detecting & Hunting Ransomware Operator Tools: It Is Easier Than You Think! | SANS Institute*. adr.: https://www.sans.org/webcasts/community-night-sans-secure-australia-2023-detecting-hunting-ransomware-operator-tools-its-easier-than-you-think/ (term. wiz. 08. 12. 2023).

[26] *Ext4 Disk Layout - Ext4*. adr.: https://ext4.wiki.kernel.org/index.php/Ext4_Disk_Layout (term. wiz. 08. 12. 2023).

[27] Bovet, D. P. i Cesati, M., *Understanding Linux Kernel 3rd Edition*. adr.: https://doc.lagout.org/operating%20system%20/linux/Understanding%20Linux%20Kernel.pdf (term. wiz. 09. 12. 2023).

[28] Love, R., *Linux system programming*, en, Second edition. Beijing: O'Reilly, 2013, OCLC: ocn827267973, ISBN: 978-1-4493-3953-1.

[29] Biancalana, A., *inotfy-tools wiki*, en. adr.: https://github.com/inotify-tools/inotify-tools/wiki/Home (term. wiz. 10. 12. 2023).

[30] *fanotify(7) - Linux manual page*. adr.: https://man7.org/linux/man-pages/man7/fanotify.7.html (term. wiz. 10. 12. 2023).

[31] Foundation, L., *Tool Interface Standard Portable Formats Specification*. adr.: https://refspecs.linuxfoundation.org/elf/TIS1.1.pdf (term. wiz. 08. 12. 2023).

[32] *elf(5) - Linux manual page*. adr.: https://man7.org/linux/man-pages/man5/elf.5.html (term. wiz. 09. 12. 2023).

[33] Davies, S. R., Macfarlane, R. i Buchanan, W. J., „Differential area analysis for ransomware attack detection within mixed file datasets," en, *Computers & Security*, t. 108, s. 102 377, wrz. 2021, ISSN: 01674048. DOI: 10.1016/j.cose.2021.102377. adr.: https://linkinghub.elsevier.com/retrieve/pii/S0167404821002017 (term. wiz. 10. 12. 2023).

[34] Shannon, C. E., „A mathematical theory of communication," *The Bell System Technical Journal*, t. 27, nr. 3, s. 379–423, 1948. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[35] Chen, Q. i Bridges, R. A., „Automated Behavioral Analysis of Malware: A Case Study of WannaCry Ransomware," w *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2017, s. 454–460. DOI: 10.1109/ICMLA.2017.0-119.

[36] Salton, G. i Buckley, C., „Term-weighting approaches in automatic text retrieval," en, *Information Processing & Management*, t. 24, nr. 5, s. 513–523, sty. 1988, ISSN: 03064573. DOI: 10.1016/0306-4573(88)90021-0. adr.: https://linkinghub.elsevier.com/retrieve/pii/0306457388900210 (term. wiz. 10. 12. 2023).

Spis rysunków

Spis tabel

Spis załączników