Etyczne hakowanie w analizie złośliwego oprogramowania

Złośliwe oprogramowanie to jeden z narastających problemów, z którymi zmagają się eksperci ds. bezpieczeństwa i z którymi będą się zmagać w dającej się przewidzieć przyszłości. Jako etyczny haker musisz wiedzieć, czym jest złośliwe oprogramowanie, jak działa i jak je analizować w przypadku napotkania. Złośliwe oprogramowanie ewoluowało od bycia uciążliwym do bycia dość niebezpiecznym, aż stało się szkodliwe i zdolne do kradzieży haseł, danych osobowych, pieniędzy i szerokiej gamy innych danych od nieświadomego użytkownika. Złośliwe oprogramowanie nie jest nowe; termin ten został opracowany, aby objąć wiele różnych rodzajów złośliwego kodu, takich jak wirusy, robaki, adware, scareware, spyware, a teraz ransomware. Zjawisko to stale się pogłębia pod wieloma względami ze względu na sposób działania internetu i wzajemne powiązania między danymi, aplikacjami oraz złożoność procesu tworzenia oprogramowania, wprowadzając błędy i luki w zabezpieczeniach, które atakujący wykorzystują. Wreszcie, złośliwe oprogramowanie nadal przedostaje się do systemów, ponieważ użytkownicy, którzy nie rozpoznają zagrożenia, wpuszczają je do systemu, poprawki nie są wdrażane lub nie monitoruje się złośliwej aktywności. Wszystko to przyczynia się do wzrostu liczby złośliwych programów. Omówimy następujące tematy:

• Czym jest złośliwe oprogramowanie?

• Jakie są rodzaje złośliwego oprogramowania?

• Jak złośliwe oprogramowanie przedostaje się do komputerów?

• Jak analizować próbki statycznie i dynamicznie

• Opis laboratorium analizy złośliwego oprogramowania i jego konfiguracji

• Techniki ograniczania ryzyka

Zacznijmy od omówienia, czym jest złośliwe oprogramowanie, jak działa, kto je tworzy i co możemy z nim zrobić.

Wymagania techniczne

Wymagania techniczne dla tego laboratorium obejmują korzystanie z wcześniej zainstalowanej maszyny wirtualnej Kali Linux oraz połączenie internetowe.

Dlaczego istnieje złośliwe oprogramowanie i kto je tworzy i używa?

Zanim zagłębimy się w kwestię, czym jest złośliwe oprogramowanie i jakie są jego rodzaje, omówmy najpierw przyczynę jego powstania, czyli dlaczego. Dlaczego istnieje złośliwe oprogramowanie i kto je tworzy i używa? Złośliwe oprogramowanie tworzy i używa wiele grup osób; niektóre z nich zostały wspomniane w rozdziale 1, gdzie omawialiśmy motywacje. Musimy jednak zagłębić się nieco bardziej i skupić na konkretnej grupie, omawiając historię i trendy w zakresie złośliwego oprogramowania. Z biegiem czasu złośliwe oprogramowanie ewoluowało od pojedynczych atakujących, motywowanych chęcią popisania się swoimi umiejętnościami technologicznymi, do osób, grup i klik, do których należą, w kierunku bardziej skoordynowanych i śmiercionośnych źródeł ataków. Ale kim są te źródła ataków? W wielu przypadkach są to grupy o motywacji politycznej, przestępcy i zorganizowane grupy przestępcze. Oferują one swoje usługi firmom, krajom i organizacjom rządowym. W rezultacie zasoby i motywacje napędzające rozprzestrzenianie się złośliwego oprogramowania uległy drastycznej zmianie, co doprowadziło do rozwoju znaczącego podziemnego rynku zestawów ataków, zainfekowanych hostów i skradzionych danych. Będziemy odwoływać się do historycznych incydentów,

aby lepiej zilustrować różne koncepcje. Oto kilka typowych obszarów lub grup, w których działają atakujący:

• Brokerzy dostępu: Jak sama nazwa wskazuje, termin ten odnosi się do grup lub osób, które handlują i udostępniają dostęp do systemów i organizacji. W niektórych przypadkach grupa mogła uzyskać dane uwierzytelniające lub metody dostępu od kogoś innego lub mogła sama zhakować systemy. Tak czy inaczej, ta grupa lub osoba sprzeda dane uwierzytelniające osobie zainteresowanej organizacją docelową, od której nabywca wykorzysta te informacje, aby uzyskać dostęp do organizacji w dowolnych szkodliwych celach.

• Organizacje cyberprzestępcze: Organizacje cyberprzestępcze to grupa lub grupy hakerów, którzy współpracują ze sobą w celu przeprowadzania ataków, zazwyczaj w celach finansowych. Organizacje te działają globalnie, często wykorzystując fora i inne miejsca spotkań do ukrywania swojej tożsamości i planowania działań. Ich główne cele obejmują zyski finansowe poprzez działania takie jak kradzież danych, ataki ransomware i oszustwa internetowe, stanowiące poważne zagrożenie dla firm, rządów i osób prywatnych na całym świecie.

• Haktywiści/grupy anonimowe: Grupy anonimowe to grupy aktywistów/haktywistów, znane z ataków na organizacje i rządy, opierając się głównie na różnicach ideologicznych, głównie w obszarze postaw społecznych i/lub polityki. Inne grupy działają w tym obszarze, ale grupa anonimowa jest prawdopodobnie najbardziej znana spośród nich.

• Zaawansowane trwałe zagrożenia (APT): APT to luźny termin, ale generalnie odnosi się do zagrożeń i/lub grup, które są częścią państwa narodowego. W związku z tym, są one przede wszystkim zainteresowane infrastrukturą innych państw narodowych w ramach trwających ćwiczeń mających na celu zakłócenie lub wyłączenie kluczowych systemów w przypadku konfliktu.

• Zagrożenie wewnętrzne: Zagrożenie wewnętrzne dotyczy zaufanej osoby w organizacji, zazwyczaj pracownika, ale mogą to być również osoby trzecie. Wykorzystują one swoje uprawnienia dostępu do naruszenia poufnych danych lub systemów. Może to dotyczyć zarówno pracownika celowo ujawniającego poufne informacje dla osobistych korzyści, jak i niezadowolonego pracownika szukającego zemsty poprzez umieszczenie złośliwego oprogramowania w sieci firmy. Identyfikacja i ograniczanie takich zagrożeń często wymaga połączenia solidnej kontroli dostępu, monitorowania pracowników i kompleksowych protokołów bezpieczeństwa.

• Script kiddies: Są to osoby nieposiadające dogłębnej wiedzy technicznej, które polegają na gotowych skryptach lub narzędziach do przeprowadzania ataków. Ataki te są często nieskomplikowane i niezdarne w użyciu. Motywy działania tej grupy mogą być różne, od prostej rozrywki i szukania uwagi, po próby osiągnięcia korzyści finansowych lub złośliwe zamiary. Chociaż ich działania mogą być stosunkowo łatwe do wykrycia i złagodzenia, Script Kiddies wciąż mogą stanowić uciążliwość, ponieważ jest to coś, czym musi zająć się zespół ds. bezpieczeństwa. Dodatkowo, mogą oni wskazywać luki w zabezpieczeniach, które wymagają interwencji zespołu ds. bezpieczeństwa, czasami narażając się na ich zażenowanie.

Teraz, gdy wiesz już coś o osobach stojących za złośliwym oprogramowaniem, przyjrzyjmy się jego rodzajom. Wcześniej omówiliśmy, że złośliwe oprogramowanie to chwytliwe określenie obejmujące wszelkiego rodzaju złośliwe działania i zachowania. Czas lepiej zrozumieć, co dokładnie to oznacza.

Analiza rodzajów złośliwego oprogramowania

Złośliwe oprogramowanie (malware), skrót od malware software, stanowi wszechobecne i stale ewoluujące zagrożenie w cyfrowym krajobrazie, stwarzając poważne ryzyko dla osób fizycznych,

organizacji, a nawet całych państw. Ten ogólny termin obejmuje szeroką gamę szkodliwego oprogramowania, którego celem jest naruszenie poufności, integralności lub dostępności systemów komputerowych i danych. Istnieje kilka rodzajów złośliwego oprogramowania o różnych cechach; mogą one obejmować zarówno ukryte taktyki pozwalające im działać niezauważone, jak i jawne i destrukcyjne zachowania, które mogą sparaliżować całe sieci. Niektóre z typowych kategorii złośliwego oprogramowania, które omówimy w tej sekcji, to:

• Wirusy, które dołączają się do legalnych programów i rozprzestrzeniają się podczas ich uruchamiania

• Robaki, które replikują się niezależnie i rozprzestrzeniają w sieciach

• Trojany, które podszywają się pod nieszkodliwe oprogramowanie, aby oszukać użytkowników

• Ransomware, które szyfruje pliki lub systemy i żąda zapłaty za ich uwolnienie

• Spyware, zaprojektowane w celu ukrytego gromadzenia poufnych informacji

Każdy rodzaj złośliwego oprogramowania stanowi unikalne wyzwanie dla specjalistów ds. cyberbezpieczeństwa, wymagając wielopłaszczyznowego i adaptacyjnego podejścia do obrony. Wraz z ciągłą ewolucją cyfrowego krajobrazu, rośnie również wyrafinowanie złośliwego oprogramowania, co podkreśla kluczowe znaczenie solidnych środków bezpieczeństwa i świadomości użytkowników w ograniczaniu tych zagrożeń. Przyjrzyjmy się bliżej różnym rodzajom złośliwego oprogramowania i jego kategoriom.

Wirus

Termin „wirus”, jak można się domyślić, pochodzi z biologicznego znaczenia tego słowa, stosowanego w odniesieniu do technologii komputerowej. Jest to po prostu program, który po uruchomieniu wstawia swój kod do innych programów w celu replikacji. Istnieją dwa rodzaje wirusów:

• Nierezydentne: Po uruchomieniu wirus skanuje inne pliki docelowe w celu zainfekowania.

• Rezydentne: Wirus staje się częścią systemu operacyjnego i jest uruchamiany po włączeniu komputera. Replikuje się podczas interakcji z innymi plikami.

Termin „wirus” nie oddaje jednak w pełni działania wirusa. Zamiast tego, aby to ułatwić, potrzebne są dalsze klasyfikacje i rozróżnienia. Przyjrzyjmy się bliżej i omówmy niektóre z tych klasyfikacji, zaczynając od robaków.

Robaki

Robaki, w przeciwieństwie do wirusów, mogą replikować się bez pomocy człowieka i nie są zależne od hosta, co oznacza, że nie wymagają załącznika do oprogramowania, aby działać. Luki w zabezpieczeniach mogą być źródłem transmisji robaków, ponieważ exploit może być zautomatyzowany. Mogą być również pobierane z nośników przenośnych i wysyłane jako załączniki za pośrednictwem wiadomości e-mail, bezpośrednich rozmów lub obu tych metod. Po otwarciu te pliki mogą połączyć się ze szkodliwą witryną internetową lub automatycznie uruchomić robaka komputerowego. Po zainstalowaniu robak zaczyna działać po cichu i dyskretnie infekuje komputer, a nawet całe sieci. Inne operacje, które mogą być włączone do robaków, to:

• Stawanie się częścią botnetu

• Kradzież plików lub danych

• Usuwanie lub modyfikowanie plików

• Instalowanie innego złośliwego oprogramowania, w tym backdoorów

• Przeprowadzanie innych ataków, w tym ataków typu „rozproszona odmowa usługi” (DDoS)

• Wdrażanie oprogramowania ransomware

Przyjrzyjmy się kilku historycznym przykładom robaków:

• SQL Slammer: Szkodliwe oprogramowanie typu robak z 2003 roku, znane jako SQL Slammer, uważane za jeden z najszybciej rozprzestrzeniających się robaków w historii, wykorzystywało lukę w programie SQL Server firmy Microsoft. Atak dotknął tysiące serwerów i trwał zaledwie 10 minut.

• Emotet: Emotet, robak z 2014 roku, początkowo był trojanem bankowym, a następnie rozwinął się w bardzo elastycznego i uporczywego dystrybutora złośliwego oprogramowania. Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) określił go mianem „najbardziej kosztownego i destrukcyjnego złośliwego oprogramowania” i miał ogromny wpływ na cały świat.

• WannaCry: W maju 2017 roku WannaCry zainfekował setki tysięcy komputerów. Wykorzystując lukę w zabezpieczeniach systemów Microsoft Windows, szyfrował pliki i żądał okupu w Bitcoinach za ich uwolnienie. Wpływ WannaCry był dalekosiężny, dotykając organizacje z różnych sektorów, w tym opieki zdrowotnej, finansów i administracji publicznej, co podkreśla znaczenie terminowych aktualizacji oprogramowania i solidnych środków cyberbezpieczeństwa. Jednym ze znaczących działań zapobiegających WannaCry było odkrycie i aktywacja wyłącznika awaryjnego przez brytyjskiego badacza bezpieczeństwa, Marcusa Hutchinsa, co skutecznie powstrzymało rozprzestrzenianie się złośliwego oprogramowania. Dodatkowo, poprawki i aktualizacje wydane przez Microsoft w celu wyeliminowania luki w zabezpieczeniach wykorzystywanej przez WannaCry pomogły złagodzić jego skutki i zapobiec dalszym infekcjom. Działania organów ścigania, w tym śledztwa i aresztowania osób związanych z rozwojem i dystrybucją WannaCry, również odegrały rolę w powstrzymaniu jego rozprzestrzeniania się.

• VPNFilter: W 2018 roku pojawił się robak VPNFilter, który był wyjątkowy, ponieważ celowo atakował urządzenia sieciowe, takie jak routery i urządzenia NAS (Network-Attached Storage). Był odpowiedzialny za kradzież danych uwierzytelniających i uszkodzenie zainfekowanych urządzeń, na około 500 000 urządzeń na całym świecie.

Trojany

Zwane również końmi trojańskimi, trojany to rodzaj złośliwego oprogramowania, które jest dołączane do legalnych programów, plików lub oprogramowania lub podszywa się pod nie, aby nakłonić użytkowników do pobrania go i nieświadomego przekazania kontroli nad urządzeniami. Trojan może wykonywać swoją zamierzoną funkcję po zainstalowaniu, niezależnie od tego, czy polega na wykorzystaniu, zakłócaniu, kradzieży lub wyrządzaniu innych szkód w danych lub sieci. Podobnie jak wirusy, trojany muszą wejść w interakcję z użytkownikiem i zostać przez niego aktywowane, aby się rozprzestrzeniać. Różnica między wirusem malware a trojanem polega na tym, że wirus jest zależny od hosta, a trojan nie. Podobnie jak wirusy, trojany nie replikują się samoczynnie. Trojany mogą posiadać następujące możliwości:

• Modyfikowanie, usuwanie lub kradzież plików i danych

• Szpiegowanie systemu i zalogowanych użytkowników

• Wykorzystywanie zainfekowanego hosta do uzyskiwania dostępu do lokalnego systemu plików i sieci hosta

• Pobieranie innego złośliwego oprogramowania lub przeprowadzanie innych rodzajów ataków

W historii pojawiło się kilka poważnych trojanów, które przysporzyły wielu problemów organizacjom i personelowi IT; oto kilka z nich:

• Zeus/Zbot: To trojan bankowy wykorzystujący rejestrowanie naciśnięć klawiszy i przechwytywanie danych w formularzach, aby kraść dane uwierzytelniające i opróżniać salda kont bankowych.

• Emotet: To kolejny zaawansowany trojan bankowy, który istnieje od 2014 roku. Emotet jest trudny do zwalczenia, ponieważ unika wykrycia za pomocą metod opartych na sygnaturach i jest uporczywy, wykorzystując moduły rozprzestrzeniające, które ułatwiają jego rozprzestrzenianie. Wiadomo również, że pobiera inne złośliwe oprogramowanie, co praktycznie uniemożliwia jego eliminację.

• Qbot: Często nazywany Qakbotem lub Pinkslipbotem, to trojan bankowy, który istnieje od około 2007 roku i ma na celu kradzież danych użytkowników i haseł logowania.

• TrickBot: Został zidentyfikowany około 2016 roku i został opracowany i zaprojektowany jako trojan bankowy do kradzieży danych finansowych. TrickBot rozwinął się w modułowe, wieloetapowe złośliwe oprogramowanie, które oferuje użytkownikom kompletny zestaw narzędzi do angażowania się w różnorodne, szkodliwe działania online.

Omówmy teraz jeden z najgorszych typów złośliwego oprogramowania: ransomware.

Ransomware

Jak sama nazwa wskazuje, ransomware to kategoria wirusów, które żądają zapłaty w zamian za ujawnienie danych ofiary. Przejmuje kontrolę nad urządzeniem lub danymi ofiary, blokuje je i szyfruje. Często nazywa się go najgorszym rodzajem złośliwego oprogramowania, ponieważ jest nie tylko destrukcyjny, ale także kosztuje organizację pieniądze w przypadku jego odzyskania. Może to skutkować utratą produktywności i stratami finansowymi, jeśli organizacja zdecyduje się zapłacić okup. W jaki sposób ransomware dostaje się na komputer? Często dzieje się tak, gdy ofiary nieumyślnie instalują to konkretne złośliwe oprogramowanie za pośrednictwem załączników e-mail lub linków z niezaufanych stron internetowych. Po zainstalowaniu złośliwe oprogramowanie może umożliwić hakerom dostęp do urządzenia przez backdoor, a następnie rozpocząć szyfrowanie danych i blokowanie użytkownikom dostępu do urządzeń do czasu zapłacenia okupu w celu odzyskania kontroli. Wraz ze wzrostem świadomości pracowników ochrony na temat ransomware, wdrożono techniki odzyskiwania danych i solidną politykę postępowania w takich przypadkach. Oznaczało to, że wiele organizacji było przynajmniej częściowo odpornych na ataki ransomware. Niezrażeni tym, operatorzy ransomware przyjęli nowe techniki wymuszania okupu. Technika ta, znana obecnie jako podwójne wymuszenie, polega na ujawnieniu naruszenia i/lub skradzionych danych z organizacji w internecie w celu wymuszenia zapłaty. Dla atakującego ma to dwa cele: po pierwsze, bez ujawniania czegokolwiek, ujawnia on publicznie naruszenie. Wywiera to presję na firmę, aby zapłaciła, aby zapobiec ujawnieniu danych. Po drugie, w wielu przypadkach organizacja nie jest do końca pewna, co posiada atakujący. Skradzione informacje mogą spowodować większe szkody wizerunkowe i finansowe niż te, których żądają atakujący. Tak czy inaczej, na tym etapie decyzja biznesowa staje się decyzją czy zapłacić czy nie.

Oprogramowanie ransomware jest zazwyczaj końcowym rezultatem włamania i służy do przetrzymywania urządzeń i danych jako zakładników poprzez szyfrowanie, co skutkuje stratami finansowymi, zarówno w przypadku opóźnienia w odzyskaniu danych, jak i konieczności zapłaty okupu. Znany malware WannaCry pojawił się w maju 2017 roku i zaatakował tysiące komputerów z systemem Windows na całym świecie. Ofiary zostały poproszone o zapłacenie okupu w Bitcoinach, aby odzyskać swoje dane po tym, jak rozprzestrzenił się on w sieciach korporacyjnych.

Boty/botnety

Botnet to rodzaj złośliwego oprogramowania, w którym atakujący wykorzystują je do bezpośredniego wdrażania zainfekowanych urządzeń w celu wykonywania innych operacji. Są one powszechnie wykorzystywane do ułatwiania ataków, takich jak oszustwa związane z kliknięciami czy DDoS. Innym razem boty mogą być wykorzystywane jak pająki przeszukujące internet w poszukiwaniu otwartych portów lub luk w zabezpieczeniach, które atakujący mogą wykorzystać. Chociaż boty lub botnety są powszechnie wykorzystywane do ataków masowych, mogą one również wykonywać inne operacje, takie jak:

• Rejestrowanie lokalnej aktywności urządzeń, takiej jak naciśnięcia klawiszy, kamery internetowe i robienie zrzutów ekranu

• Masowe wysyłanie wiadomości phishingowych z zainfekowanych urządzeń

• Udzielanie zdalnego dostępu w celu dalszej infiltracji sieci hosta

Oto kilka przykładów botnetów:

• Mirai: Ten botnet koncentrował się na urządzeniach Internetu Rzeczy (IoT) wykorzystujących domyślne, znane identyfikatory i hasła do logowania się i przejmowania kontroli. Te zainfekowane urządzenia zostały później wykorzystane w atakach DDoS.

• Echobot: Wykorzystując sukces Mirai, Echobot to wariant Mirai, który atakował różnorodne urządzenia IoT, wykorzystując ponad 50 różnych luk w zabezpieczeniach. Zawierał również exploity dla Oracle WebLogic Server i oprogramowania sieciowego SD-WAN firmy VMware.

Przyjrzyjmy się teraz oprogramowaniu adware i sposobom jego wykorzystywania do wdrażania złośliwego oprogramowania.

Adware

Adware to złośliwe oprogramowanie instalowane na komputerze i wyświetlające ukierunkowane reklamy. Adware, nazywane również oprogramowaniem wspieranym reklamami, wyświetla niechciane reklamy na komputerze, a nawet reklamy pop-up monitorujące aktywność użytkowników w sieci. Oprócz reklam pop-up, niektóre złośliwe programy gromadzą informacje, które następnie są dystrybuowane do innych zainteresowanych stron, które mogą je wykorzystać do kradzieży tożsamości lub oszustw związanych z kartami kredytowymi. Adware był w odwrocie, aż do niedawnego odrodzenia się na rynku mobilnym, za sprawą reklam w aplikacjach. Oprócz oczywistego faktu, że adware jest głównie uciążliwe, oprócz wyświetlania ukierunkowanych reklam, może instalować oprogramowanie szpiegujące i udostępniać dane stronom trzecim. W 2017 roku komputery zainfekowane adware znanym jako Fireball zostały przejęte przez przeglądarki, co zmieniło domyślną wyszukiwarkę i umożliwiło śledzenie aktywności w sieci.

Oprogramowanie szpiegujące

Oprogramowanie szpiegujące to rodzaj złośliwego oprogramowania, które infiltruje urządzenia bez wiedzy właściciela, podobnie jak trojan. Zazwyczaj jest ono dołączone do aplikacji, takiej jak pasek narzędzi przeglądarki. Po zainstalowaniu raportuje o aktywności w internecie i czasami gromadzi inne poufne informacje. Oprócz raportowania aktywności przeglądania, oprogramowanie szpiegujące może czasami gromadzić dane z formularzy, działać jako keylogger i kraść inne dane, w tym dane logowania. Złośliwe oprogramowanie DarkHotel zostało zidentyfikowane jako keylogger, który był używany do

atakowania pracowników rządowych i biznesowych na całym świecie, którzy odwiedzali luksusowe hotele i uzyskiwali dostęp do sieci Wi-Fi.

Malvertising

Malvertising to forma infekcji pochodząca z reklam na zaufanych stronach internetowych i nie należy go mylić z adware. Ofiary malvertisingu są zazwyczaj infekowane poprzez kliknięcie zainfekowanej reklamy. Ponieważ reklamy są częścią wielu legalnych witryn internetowych, atakujący mogą płacić za umieszczanie zainfekowanych reklam na tych stronach, aby dotrzeć do określonych użytkowników lub grup. W 2016 roku kilka organizacji medialnych, w tym „The New York Times" i strona internetowa BBC, nieświadomie wyświetlało czytelnikom złośliwe reklamy, które prowadziły do ataku ransomware.

Złośliwe oprogramowanie bezplikowe

Złośliwe oprogramowanie sklasyfikowane jako bezplikowe wykorzystuje natywne lub wbudowane oprogramowanie, programy i protokoły na urządzeniach do instalowania i wykonywania złośliwych działań. Innymi słowy, w systemie plików nie zostaną znalezione żadne pliki ani artefakty, ponieważ ten typ złośliwego oprogramowania działa wyłącznie w pamięci. To bardzo utrudnia jego wykrycie, wyizolowanie i usunięcie z zainfekowanego systemu. Astaroth to rodzaj bezplikowego złośliwego oprogramowania, które po aktywacji pobiera dodatkowy kod wykonywany tylko w pamięci, nie pozostawiając żadnych śladów, które mogłyby zostać wykorzystane przez skanery podatności do jego identyfikacji. Następnie atakujący pobierają dodatkowe złośliwe oprogramowanie, które kradnie dane uwierzytelniające i przesyła je na zdalny serwer.

Tylne drzwi

Tylne drzwi, jak sama nazwa wskazuje, to błędy oprogramowania lub programy, które umożliwiają zdalny, nieograniczony dostęp do komputerów lub danych użytkownikom z zewnątrz. Mogą to być dowolne aplikacje działające w systemie, takie jak serwer WWW, na którym zainstalowana jest powłoka WWW. Mogą to być przepełnienia bufora, które umożliwiają zdalne wykonywanie. Istnieją również legalne aplikacje, które umożliwiają otwarcie portu dla poleceń, takie jak Netcat, wykorzystywane zarówno przez personel IT, jak i atakujących w celach złośliwych.

Rootkity

Rootkity to ukryte złośliwe oprogramowanie, którego celem jest dostęp do obszarów systemu komputerowego, do których w innym przypadku nie uzyskano by autoryzacji. Robią to poprzez osadzanie się głęboko w systemie operacyjnym lub oprogramowaniu układowym. Rootkity umożliwiają nieautoryzowany dostęp i kontrolę nad systemem, umożliwiając atakującym wykonywanie dowolnych poleceń, manipulowanie danymi i ukrywanie swojej obecności. Niektóre cechy rootkitów to:

• Trudno je znaleźć.

• Mogą umożliwiać uprzywilejowany dostęp do komputera.

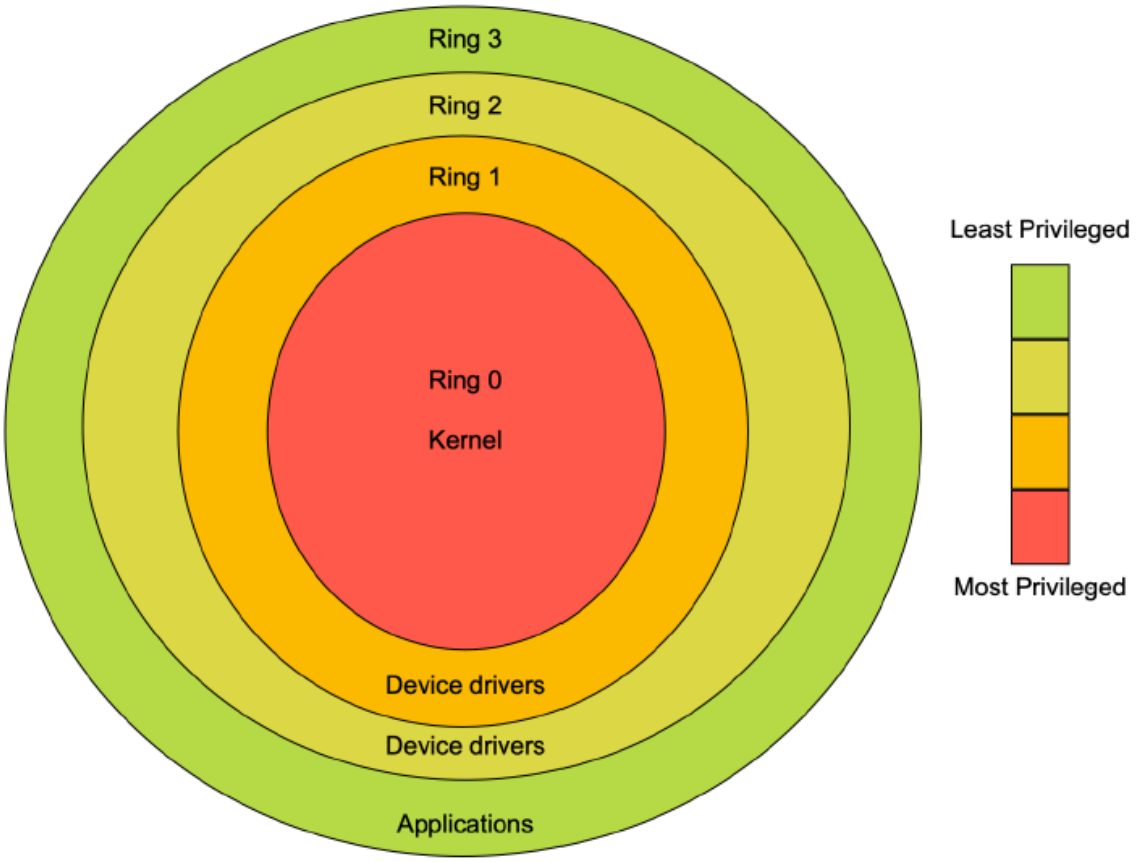
• Ukrywają swoją obecność, manipulując funkcjonalnością systemu operacyjnego.

Rootkity zazwyczaj wykorzystują zaawansowane techniki dostępu do różnych poziomów uprawnień, znanych jako pierścienie. Niektóre z nich obejmują haki na poziomie jądra, ukrywanie procesów i manipulowanie narzędziami systemowymi w celu utrzymania trwałości i uniknięcia wykrycia przez oprogramowanie antywirusowe i inne mechanizmy bezpieczeństwa. Po zainstalowaniu rootkity mogą ułatwiać szeroki zakres złośliwych działań, w tym kradzież danych, szpiegostwo i wdrażanie dodatkowego złośliwego oprogramowania, stwarzając poważne zagrożenie dla integralności,

poufności i dostępności zainfekowanych systemów i sieci. Omówmy teraz pokrótce poziomy uprawnień operacyjnych, znane jako pierścienie.

Pierścienie

Różne poziomy uprawnień w systemie operacyjnym są reprezentowane przez pierścienie. Pierścień 0 to miejsce, w którym uruchamiane jest jądro i stanowi mózg komputera. Następnie przechodzimy do pierścieni 1 i 2, w których ładowane są sterowniki urządzeń. Mogą to być między innymi sterowniki myszy, klawiatur i wyświetlaczy. Na koniec mamy pierścień 3, w którym działają aplikacje użytkownika. Poniżej znajduje się diagram przedstawiający różne pierścienie i ich poziomy uprawnień:



Istnieją dwa główne pierścienie, w których użytkownicy faktycznie wchodzą w interakcję: Pierścień 3 i Pierścień 0. Przyjrzyjmy się ich działaniu bardziej szczegółowo:

• Poziom użytkownika (Pierścień 3): Pierścień 3 to mechanizm bezpieczeństwa wbudowany w systemy operacyjne, który oddziela użytkowników i procesy na podstawie uprawnień. Aplikacje użytkownika, takie jak przeglądarki, poczta e-mail i edytory tekstu, ładują się i działają w Pierścieniu 3. Następnie, gdy aplikacja na tym poziomie musi wykonać operacje wymagające większych uprawnień, takie jak odczyt lub zapis pliku, aplikacja wysyła żądanie wykonania tej funkcji, która jest przekazywana do Pierścienia 0, gdzie ta czynność jest obsługiwana. W przypadku rootkita Pierścienia 3 lub rootkita na poziomie użytkownika, działa on tak samo jak inne aplikacje. Ze względu na mechanizmy bezpieczeństwa wbudowane w pierścienie, możliwości rootkita Pierścienia 3 są ograniczone w porównaniu z rootkitem Pierścienia 0. Obejmuje to następujące funkcje:

- Wykorzystuje API systemu Windows do obsługi swoich funkcji i operacji

- Jest mniej skuteczny i łatwiejszy do wykrycia niż zestawy narzędzi na poziomie jądra

- Jest łatwiejszy do zaprogramowania i bardziej rozpowszechniony

• Poziom jądra (Pierścień 0): Użytkownicy nie mają faktycznego dostępu do Pierścienia 0; jednak wiele żądań musi przejść przez Pierścień 0, aby zostać zrealizowanych. Jak opisano wcześniej, aplikacje działają na poziomie Pierścienia 3, a gdy muszą wykonać funkcje wyższego poziomu, wysyłają żądania, które są wysyłane i przetwarzane w Pierścieniu 0. Ale co dokładnie dzieje się w Pierścieniu 0? W sensie operacyjnym pierścień 0 to miejsce, w którym działa jądro. Jądro ma bezpośredni dostęp do sprzętu na komputerze, na którym działa. Mając to na uwadze, podczas uruchamiania komputera ładuje on małe programy, które współpracują z jądrem, aby usprawnić działanie. Programy te często służą do obsługi sprzętu, takiego jak wyświetlacze, myszy itp. Gdy jeden z nich zostanie skompromitowany lub na tym poziomie zostaną wprowadzone inne złośliwe programy, nazywa się to rootkitem Pierścienia 0. Przyjrzyjmy się ich cechom:

- Działają w trybie „Ring 0", czyli w mózgu

- Oferują nieograniczoną kontrolę nad maszyną i sposobem jej działania

- Są znacznie trudniejsze do wykrycia i zaprogramowania

- Mogą być trudne do wykrycia po uruchomieniu

- Ponieważ zakłócają podstawowe działanie maszyny, mogą powodować jej niestabilność.

Pierścień 0 to granica bezpieczeństwa oddzielająca funkcje wyższego poziomu od aplikacji. Bez tej granicy aplikacje mogłyby wykonywać funkcje wyższego poziomu bez mechanizmów kontroli i równowagi, które zapewniają pierścienie. Teraz, gdy znamy już podstawy niektórych rodzajów złośliwego oprogramowania, przyjrzyjmy się pokrótce, jak złośliwe oprogramowanie przedostaje się na komputery.

Jak złośliwe oprogramowanie przedostaje się na komputery?

Atakujący wykorzystują różne techniki, aby wprowadzić złośliwe oprogramowanie na komputery, a czasami stosują więcej niż jedną technikę. Poniżej przedstawiono kilka z opisanych technik:

• Phishing: E-mail to główna metoda rozprzestrzeniania złośliwego oprogramowania za pośrednictwem różnych rodzajów kampanii phishingowych. Może on być dostarczony jako załącznik lub link do złośliwego adresu URL. Nowsze kampanie wykorzystują kody QR jako metodę omijania niektórych zabezpieczeń, z których korzystają obrońcy, aby uniemożliwić przedostanie się wiadomości phishingowych do systemu.

• Nośniki fizyczne: Atakujący mogą załadować złośliwe oprogramowanie na dyski flash USB, czekając, aż nieświadome ofiary włożą je do swoich komputerów. Nie jest to częste, ale zdarza się. Innym sposobem jest zainfekowanie każdego urządzenia USB podłączonego do zainfekowanego komputera wirusem atakujących, który następnie infekuje każdą maszynę, do której jest podłączony.

• Alerty w wyskakujących okienkach: Obejmuje to fałszywe alerty bezpieczeństwa, które nakłaniają do pobrania fałszywego oprogramowania zabezpieczającego, z których niektóre mogą być nawet złośliwym oprogramowaniem.

• Pobieranie drive-by: ma miejsce, gdy użytkownik odwiedza witrynę internetową, na której znajduje się złośliwe oprogramowanie; ma to charakter oportunistyczny. Odmianą tego ataku jest atak typu

watering-hole, w którym złośliwe oprogramowanie jest umieszczane na określonej zainfekowanej witrynie w celu zainfekowania grupy docelowej, która ją odwiedza.

• Zatruwanie SEO: Zatruwanie SEO polega na manipulowaniu wynikami wyszukiwania przez osoby atakujące w celu generowania ruchu na swoich złośliwych witrynach. Osiągają to, wykorzystując popularne hasła wyszukiwania lub słowa kluczowe związane z popularnymi tematami, aby zwabić niczego niepodejrzewających użytkowników. Po kliknięciu tych

zatrutych wyników wyszukiwania użytkownicy mogą nieświadomie narazić się na złośliwe oprogramowanie, oszustwa phishingowe lub inne cyberzagrożenia, stwarzając poważne zagrożenie dla swojego bezpieczeństwa i prywatności w sieci.

• Wykorzystywanie luk w zabezpieczeniach instalacji lub konfiguracji systemów i sieci w celu wprowadzenia złośliwego oprogramowania.

• Używanie zestawów exploitów zawierających kod, który może celowo atakować i wykorzystywać luki w zabezpieczeniach. Przykładem jest Metasploit.

• Stosowanie technik socjotechnicznych w celu nakłonienia użytkowników do udostępniania poufnych informacji, klikania szkodliwych linków lub pobierania złośliwych załączników poprzez granie na ich emocjach. Przykładami tego są preteksty, vishing, phishing i smishing. Więcej szczegółów na temat socjotechniki i jej działania znajdziesz w rozdziale 12.

To kilka sposobów, w jakie atakujący, a ostatecznie złośliwe oprogramowanie, przedostają się na komputery, a wdrożenie środków zaradczych, takich jak programy antywirusowe, oprogramowanie do ochrony punktów końcowych i szkolenia użytkowników, to doskonały sposób na ograniczenie wielu współczesnych zagrożeń. Czasami jednak złośliwe oprogramowanie po prostu przedostaje się do systemu, dlatego warto je przeanalizować i sprawdzić, aby uzyskać więcej informacji na temat jego natury i możliwości. Zobaczmy, jak to zrobić.

Analiza próbki

Podczas analizy podejrzanego złośliwego oprogramowania, dobrym pierwszym krokiem jest uruchomienie na nim kilku programów antywirusowych. Możesz również przesyłać próbki do wirtualnych piaskownic i narzędzi analitycznych, ale pamiętaj, że po przesłaniu próbki staje się ona publicznie znana, a jeśli Ty lub organizacja staniecie się celem ataku, atakujący będzie wiedział, że znalazłeś ich złośliwe oprogramowanie. Dodatkowo istnieje ryzyko, że w próbce znajdą się informacje firmowe, w tym dane telemetryczne sieci i dane uwierzytelniające, dlatego zachowaj ostrożność. Jeśli chcesz zbadać lub przesłać próbkę, jedną z najlepszych stron do tego celu jest VirusTotal (https://www.virustotal.com). Strona ta nie tylko umożliwia przesłanie próbki do analizy, ale także wyszukiwanie na podstawie kilku wskaźników infekcji (IOC), w tym adresu URL, adresu IP, domeny lub skrótu pliku. Może to być pomocne, jeśli pracujesz z próbką i nie masz pewności, czy organizacja jest celem ataku. Sprawdzenie, czy istnieją już jakieś informacje lub czy ktoś przesłał już próbkę, to bardziej dyskretny sposób na uzyskanie potrzebnych informacji, bez konieczności wykonywania dużej ilości pracy lub analizy. Jeśli jednak te informacje nie są dostępne lub wymagana jest szersza analiza niż ta, która została udostępniona, konieczne będzie przeprowadzenie analizy w czystym środowisku laboratoryjnym. Konfiguracja środowiska laboratoryjnego nie jest skomplikowana, a dzięki szerokiej dostępności maszyn wirtualnych (VM) i kontenerów, można ją wdrożyć szybko. Przyjrzyjmy się niektórym wymaganiom dotyczącym konfiguracji laboratorium analitycznego.

Konfiguracja laboratorium analizy złośliwego oprogramowania

Wraz z wprowadzeniem maszyn wirtualnych, konfiguracja środowiska laboratoryjnego stała się prosta. Laboratoria można skonfigurować dla pojedynczych stacji roboczych, a nawet całych sieci, aby symulować wymagane środowisko. Oto kilka kluczowych elementów niezbędnych dla środowiska laboratoryjnego:

• Musi być odizolowane. Praca ze złośliwym oprogramowaniem stwarza ryzyko infekcji innych, niezamierzonych maszyn lub sieci, jeśli nie zostaną zachowane odpowiednie środki ostrożności. Konieczne jest, aby laboratorium pozostało odizolowane od reszty sieci i internetu.

• Musi być możliwe przywrócenie lub powrót do znanego, czystego stanu. Podczas pracy z próbkami złośliwego oprogramowania, jeśli nie można powrócić do znanego, dobrego stanu, mogą pozostać pewne zachowania lub artefakty, które mogą zostać nieumyślnie przypisane do kolejnej analizowanej próbki.

• Do przeprowadzenia analizy konieczne jest posiadanie i skonfigurowanie narzędzi. Należą do nich edytory heksadecymalne, narzędzia do analizy binarnej, sniffery, debugery itd. Narzędzia te będą podstawą do przeprowadzenia analizy i umożliwią pełne zrozumienie działania złośliwego oprogramowania.

• Analiza musi przebiegać w spójny i powtarzalny sposób. W ten sposób kluczowe elementy nie zostaną pominięte z powodu pominięcia procesu lub procedury. W swoim środowisku możesz wybrać dowolne oprogramowanie do wirtualizacji. Najpopularniejszym jest VMware, ale można również zastosować VirtualBox i Hyper-V. Omówimy bardziej szczegółowo narzędzia analityczne, które powinny znaleźć się w środowisku laboratoryjnym. Tymczasem ostatnie pytanie, na które należy odpowiedzieć, brzmi:

Jak wprowadzić złośliwe oprogramowanie do środowiska laboratoryjnego w celu analizy? Istnieje kilka sposobów, aby to zrobić (skoncentruję się na VMware, ponieważ z niego korzystam). Po pierwsze: należy ostrożnie obchodzić się ze złośliwym oprogramowaniem. Podczas przenoszenia złośliwego oprogramowania, aby zapobiec jego przypadkowemu wysłaniu do miejsca docelowego, najlepszą praktyką jest spakowanie pliku z hasłem. Standardowe hasło branżowe dla tej czynności jest zainfekowane i jest powszechnie stosowane wśród badaczy złośliwego oprogramowania jako sposób ochrony wszystkich. Teraz wróćmy do przenoszenia próbki do środowiska laboratoryjnego:

• Użyj funkcji kopiowania i wklejania VMware, aby skopiować plik(i) z hosta na maszynę wirtualną. Uważam, że jest to jeden z najlepszych sposobów, ponieważ umożliwia operację kopiowania i wklejania z miejsca, do którego host ma dostęp, bez narażania się na bezpośrednie obecność złośliwego oprogramowania na maszynie hosta.

• Inną metodą jest użycie funkcji folderów współdzielonych VMware; umożliwia ona dostęp do wyznaczonego folderu dostępnego dla systemu hosta i udostępnionego maszynie wirtualnej. Może to obejmować udziały sieciowe lub inne zdalne systemy plików.

• Ostatnią opcją jest użycie nośnika wymiennego i zamontowanie go w maszynie wirtualnej. W tej metodzie próbka złośliwego oprogramowania jest kopiowana na nośnik wymienny, zazwyczaj urządzenie USB. Urządzenie to jest montowane, aby stało się dostępne dla maszyny wirtualnej, a następnie jest z niego uruchamiane lub kopiowane na hosta, a następnie uruchamiane.

Istnieją inne metody wprowadzenia próbki do środowiska, ale te są najpopularniejsze. Teraz, gdy próbka znajduje się w środowisku laboratoryjnym, czas rozpocząć ocenę, zaczynając od analizy statycznej.

Analiza statyczna

Analiza statyczna, jak sama nazwa wskazuje, polega na analizie próbki bez jej uruchamiania. Aby to zrobić, stosujemy kilka procesów, aby rozłożyć złośliwe oprogramowanie na czynniki pierwsze i uzyskać podstawowe zrozumienie jego potencjalnych działań. Procesy te obejmują:

• Identyfikacja pliku

• Ciągi znaków

• Importy

Omówimy każdy z tych procesów w kolejnych sekcjach.

Identyfikacja pliku

Jedną z pierwszych rzeczy do zrobienia jest zidentyfikowanie typu pliku, z którym pracujemy. Istnieje kilka sposobów, aby to zrobić:

• Pierwszym z nich jest użycie polecenia file. To polecenie jest częścią systemów Linux i Mac. Przeanalizuje ono plik i wygeneruje dane wyjściowe podobne do poniższego:

% file setup.exe

setup.exe: plik wykonywalny PE32 (GUI) Intel 80386, dla systemu MS Windows

%

• Co mogę zrobić, jeśli moim komputerem analitycznym jest system Windows? System Windows nie zapewnia natywnego sposobu identyfikacji plików; istnieje jednak kilka metod, które można zastosować w celu identyfikacji plików:

- Pierwszą z nich jest TrID, dostępny pod adresem https://mark0.net/soft-trid-e.html. TrID to narzędzie wiersza poleceń, które może identyfikować pliki w systemie za pomocą rozbudowanej bazy definicji plików, jak pokazano na poniższym zrzucie ekranu:

Command Prompt

```
C:\trid_w32>trid.exe camtasia.exe

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found:  16332
Analyzing...

Collecting data from file: camtasia.exe
 40.3% (.EXE) Win64 Executable (generic) (10523/12/4)
 19.3% (.EXE) Win16 NE executable (generic) (5038/12/1)
 17.2% (.EXE) Win32 Executable (generic) (4505/5/1)
  7.7% (.EXE) OS/2 Executable (generic) (2029/13)
  7.6% (.EXE) Generic Win/DOS Executable (2002/3)

C:\trid_w32>
```

TrID może być używany nie tylko do identyfikacji pojedynczego pliku, ale może również akceptować symbole wieloznaczne, umożliwiając identyfikację plików na dużą skalę, identyfikując pliki w całych katalogach lub systemach plików. Ponadto obsługuje funkcje identyfikacji rozszerzeń plików, a z opcją -v (w trybie szczegółowym) może generować dodatkowe informacje, które może pobrać z pliku. TrID to doskonałe narzędzie; istnieje jednak jeszcze prostsza metoda, a mianowicie instalacja emulatora terminala ConEmu, dostępnego pod adresem https://conemu.github.io/. Różni się on od TrID tym, że jest emulatorem terminala, a nie przeznaczonym do konkretnego zadania. Przydatność tego emulatora polega na tym, że po instalacji instaluje on narzędzia wiersza poleceń systemów Unix/Linux, w tym plik, który został omówiony wcześniej.

- Istnieje jeszcze inna metoda identyfikacji plików, polegająca na ręcznej identyfikacji pliku za pomocą magicznej liczby. Magiczna liczba to pierwsze kilka bajtów szesnastkowych pliku, które służą do jego identyfikacji. W ten sposób systemy operacyjne kojarzą aplikację lub proces z plikiem. Aby to zrobić, otwieramy plik w edytorze szesnastkowym i sprawdzamy kilka pierwszych bajtów. Potrzebne bajty zaznaczyliśmy na poniższym zrzucie ekranu:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
0010h	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.....@.....
0020h	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0030h	00	00	00	00	00	00	00	00	00	00	00	00	30	01	00	00	.....0...
0040h	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..º..´.Í!¸.LÍ!Th
0050h	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
0060h	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
0070h	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.....

Jak widać, kod to 4D 5A, czyli kod pliku wykonywalnego systemu Windows. Jeśli jednak go nie znasz, możesz go sprawdzić na stronie https://www.garykessler.net/library/file_sigs.html. Lista jest prowadzona przez Gary'ego Kesslera od 2002 roku i zawiera wiele sygnatur plików, zwanych również listami magicznych liczb. Aby z niej skorzystać, wystarczy wyszukać kod szesnastkowy lub typ pliku, który chcesz wyszukać. Wpis 4D 5A wygląda następująco:

4D 5A	MZ
COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS	Windows/DOS executable file (See The MZ EXE File Format page for the structure of an EXE file, with coverage of NE, TLINK, PE, self-extracting archives, and more.) **Note:** MZ are the initials of Mark Zbikowski, designer of the DOS executable file format.
ACM	MS audio compression manager driver
AX	Library cache file
CPL	Control panel application
FON	Font file
OCX	ActiveX or OLE Custom Control
OLB	OLE object library
SCR	Screen saver
VBX	VisualBASIC application
VXD, 386	Windows virtual device drivers

Po zidentyfikowaniu typu pliku i ustaleniu, czy jest to plik wykonywalny, skrypt powłoki, czy inny typ pliku, musimy przejść do następnego poziomu analizy, czyli analizy ciągów znaków.

Wyodrębnianie informacji z ciągów znaków

Ciągi znaków to sekwencja znaków, które są czytelne dla czytelnika i stanowią część programu, na przykład słowo „the”. Każdy program zawiera pewne informacje w postaci ciągu znaków; w dużej mierze pochodzą one z części programu, która zawiera statyczne, niezmienne informacje. Informacje te mogą obejmować komunikat drukowania, połączenie z adresem URL lub skopiowanie pliku do określonej lokalizacji. Znajdowanie informacji o funkcjonalności programu poprzez przeszukiwanie

ciągów znaków to szybka i łatwa metoda. Na przykład, jeśli oprogramowanie uzyska dostęp do adresu URL, w wynikach ciągu znaków zostanie wyświetlony wpis adresu URL. Ciągi znaków pliku wykonywalnego, zapisane w formacie ASCII lub Unicode, można znaleźć za pomocą programu Strings. Znaki są przechowywane kolejno w formatach ASCII i Unicode, a oba używają terminatora NULL do wskazania, kiedy ciąg znaków jest zakończony. Unicode wymaga 2 bajtów dla każdego znaku, podczas gdy ciągi znaków ASCII używają 1 bajtu. Jest to jeden ze wskaźników używanych przez program Strings do określenia. Jak więc uzyskać listę ciągów znaków? Ponownie, jeśli korzystasz z systemu Linux lub Mac, Strings jest aplikacją natywną. Odpowiednia aplikacja Strings jest dostępna w ramach pakietu Microsoft System Internals Suite pod adresem https://learn.microsoft.com/en-us/sysinternals/downloads/. Możesz pobrać cały pakiet narzędzi, który oferuje wiele funkcji, lub pobrać pojedynczy plik wykonywalny w sekcji Różne. Program Strings oferuje kilka przełączników, które umożliwiają skupienie danych wyjściowych:

usage: strings [-a] [-f offset] [-b bytes] [-n length] [-o] [-s] [-u]

<file or directory>

-a Ascii-only search (Unicode and Ascii is default)

-b Bytes of file to scan

-f File offset at which to start scanning.

-o Print offset in file string was located

-n Minimum string length (default is 3)

-s Recurse subdirectories

-u Unicode-only search (Unicode and Ascii is default)

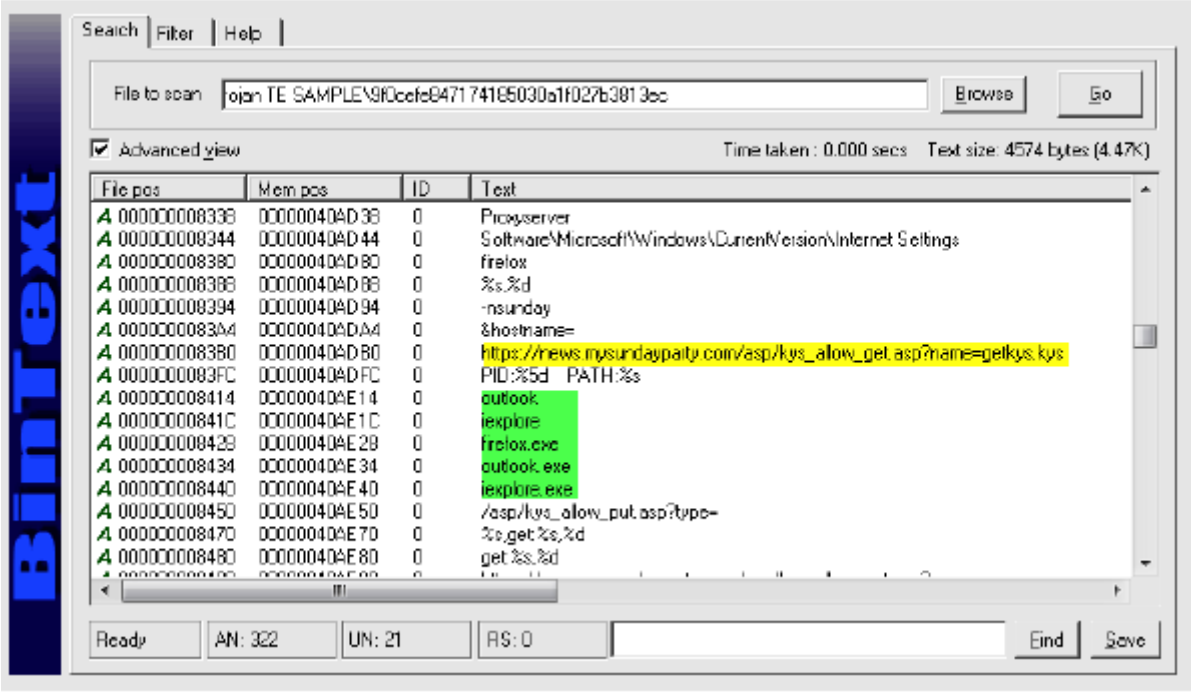
Po uruchomieniu programu zostaną wyświetlone ciągi znaków znalezione w podanym pliku na podstawie podanych przełączników, jak widać na poniższym zrzucie ekranu:

```
C:\Programs\SysinternalsSuite
λ strings RAMMap.exe

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
`.rdata
@.data
.rsrc
@.reloc
P_D
RIched32.dll
CommandLineToArgvW
Shell32.dll
/accepteula
-accepteula
Software\Microsoft\windows nt\currentversion
ProductName
iotuap
Software\Microsoft\Windows NT\CurrentVersion\Server\ServerLevels
NanoServer
Accept Eula (Y/N)?
%ls
This is the first run of this program. You must accept EULA to continue.
Use -accepteula to accept EULA.
Software\Sysinternals
%s\%s
This
tooltips_class32
DllGetVersion
comctl32.dll
ntdll.dll
Software\Classes\
shell\open\command
"%s" -o "%%1"
DefaultIcon
"%s",0
\StringFileInfo\%04X%04X\%s
\VarFileInfo\Translation
%I64d
```

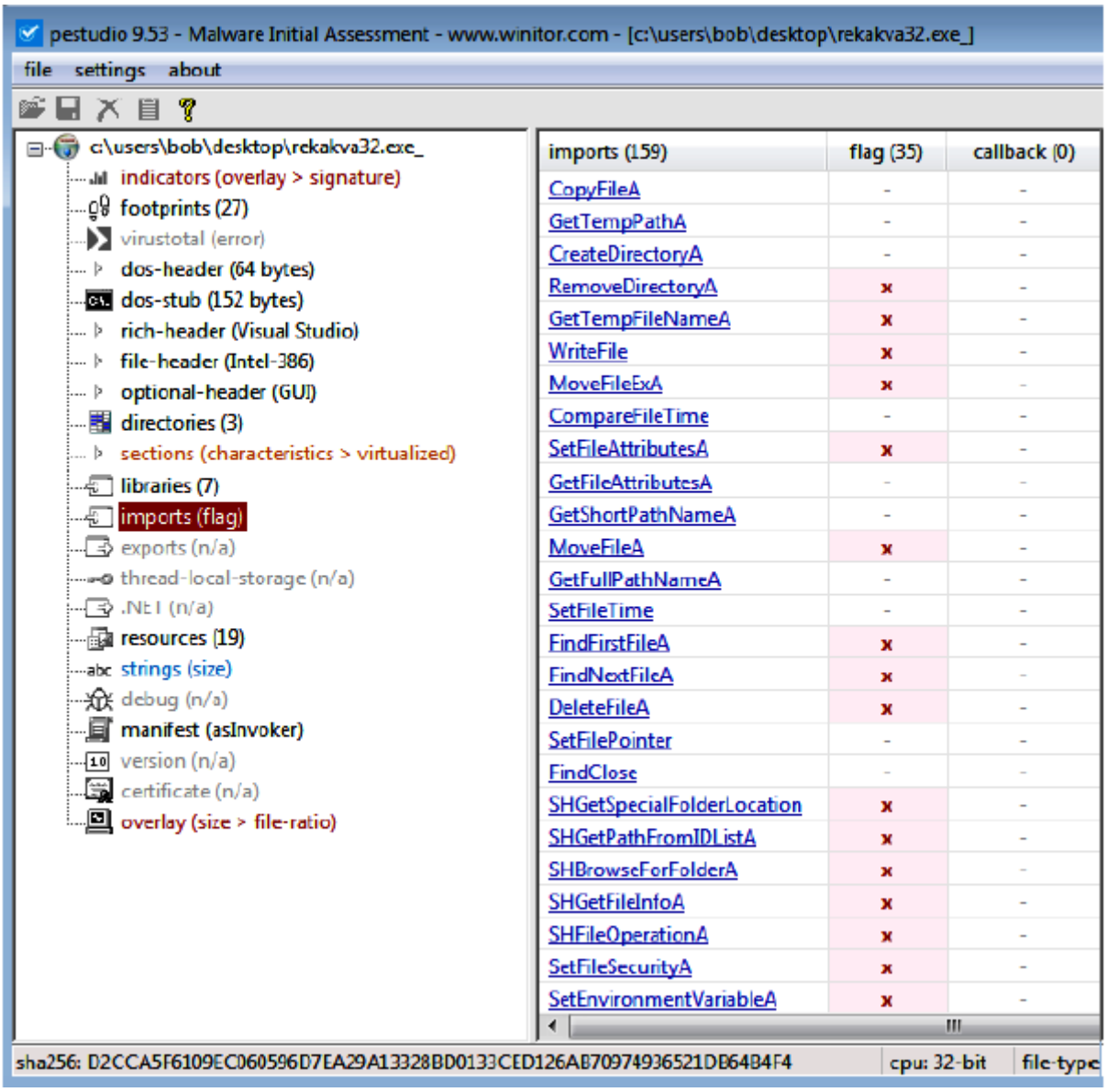
Już po samym przejrzeniu danych wyjściowych możemy dostrzec odwołania do bibliotek DLL (Dynamic-Link Libraries), kluczy rejestru i argumentów wiersza poleceń. To daje nam wgląd w plik i potencjalnie w niektóre funkcje lub działania, które mogą być związane z jego wykonywaniem. Innym programem do pobierania ciągów znaków, które mogą wyświetlać zawartość ASCII, jest BinText. Narzędzie BinText jest dostępne pod adresem https://github.com/mfput/McAfee-Tools/blob/master/BinText303.zip. BinText to aplikacja systemu Windows, która pobiera ciągi znaków z pliku wykonywalnego, aby potencjalnie uzyskać wgląd w działanie aplikacji. Jedną z jej funkcji jest możliwość dostosowania tego, co może być ciągiem znaków lub filtrem, do konkretnego elementu; zobacz przykład na poniższym zrzucie ekranu:



W wynikach BinText można zobaczyć kilka czytelnych ciągów znaków, w tym adres URL i kilka aplikacji. Zidentyfikowaliśmy już rodzaj pliku, z którym pracujemy, i prawdopodobnie pobraliśmy pewne informacje z ciągów znaków. Jeśli mamy do czynienia z plikiem wykonywalnym systemu Windows, musimy przyjrzeć się importom, aby zrozumieć, jakie funkcje może on wykonywać.

Analiza importów

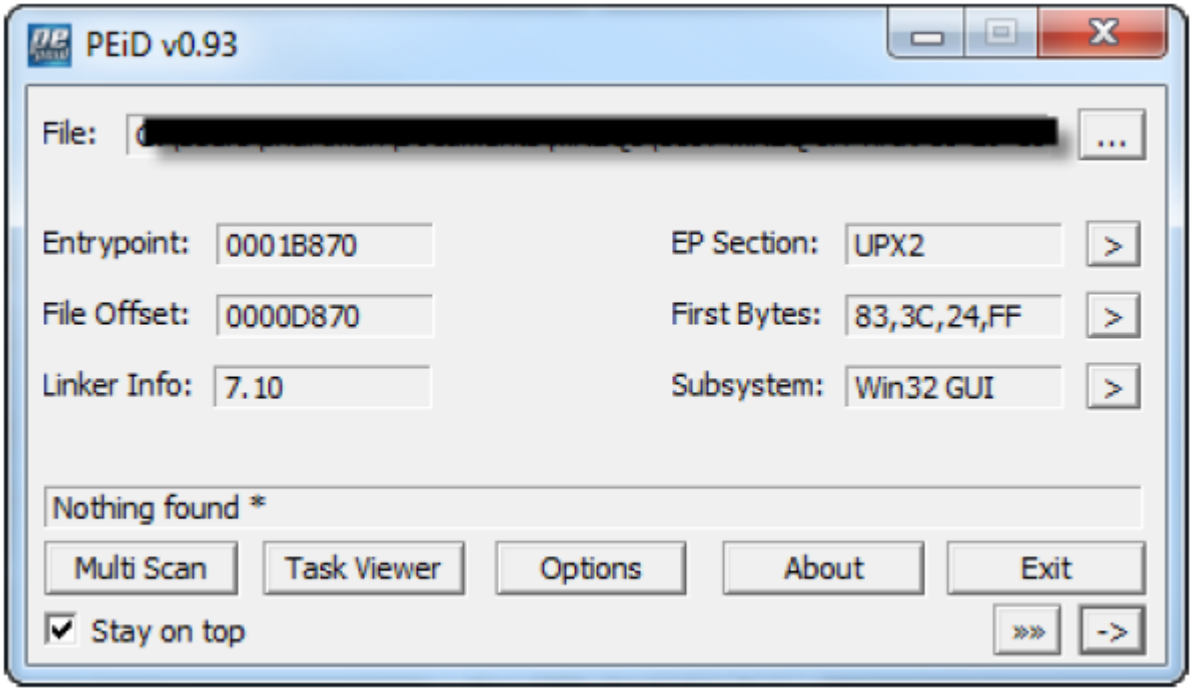
Tworząc aplikacje, programiści muszą wykonywać operacje lub funkcje, które zostały już utworzone. Procesy takie jak zapisywanie pliku lub uzyskiwanie dostępu do adresu URL zostały już utworzone i nie trzeba ich tworzyć ponownie. Funkcje te można włączyć do aplikacji bez konieczności wyważania otwartych drzwi. Gdy wymagana jest konkretna funkcja, programista importuje odpowiednią bibliotekę, która ją zawiera. Przyjrzyjmy się bliżej importom i ich działaniu. Aby zbadać importy, możemy skorzystać z narzędzia takiego jak pestudio firmy Winitor; można je znaleźć pod adresem https://www.winitor.com/download. PeStudio nie tylko identyfikuje importy, o których za chwilę opowiemy, ale także rozkłada strukturę pliku wykonywalnego na komponenty i identyfikuje elementy, które mogą być szkodliwe. Jeśli maszyna analizująca jest połączona z internetem, sprawdza VirusTotal. W plikach wykonywalnych systemu Windows importy służą do wprowadzania innych funkcji. Jeśli podczas programowania pliku chcemy połączyć się z internetem, importujemy odpowiednie biblioteki, aby to zrobić. Sprawdzenie, które biblioteki i funkcje są wczytywane, może dać nam wgląd w możliwości pliku wykonywalnego. Poniższy zrzut ekranu pokazuje przykładowy wygląd ekranu importu w PeStudio:



Jak widać na podstawie niektórych importów, plik wykonywalny obsługuje funkcje takie jak WriteFile, DeleteFile i CreateDirectory, żeby wymienić tylko kilka. Podczas analizy behawioralnej będziemy szukać artefaktów związanych z tymi funkcjami w systemie testowym. Teraz, gdy rozumiemy już importy, musimy przyjrzeć się bliżej i sprawdzić, jakie inne elementy moglibyśmy zidentyfikować bez uruchamiania interesującej nas próbki.

Identyfikacja pliku wykonywalnego

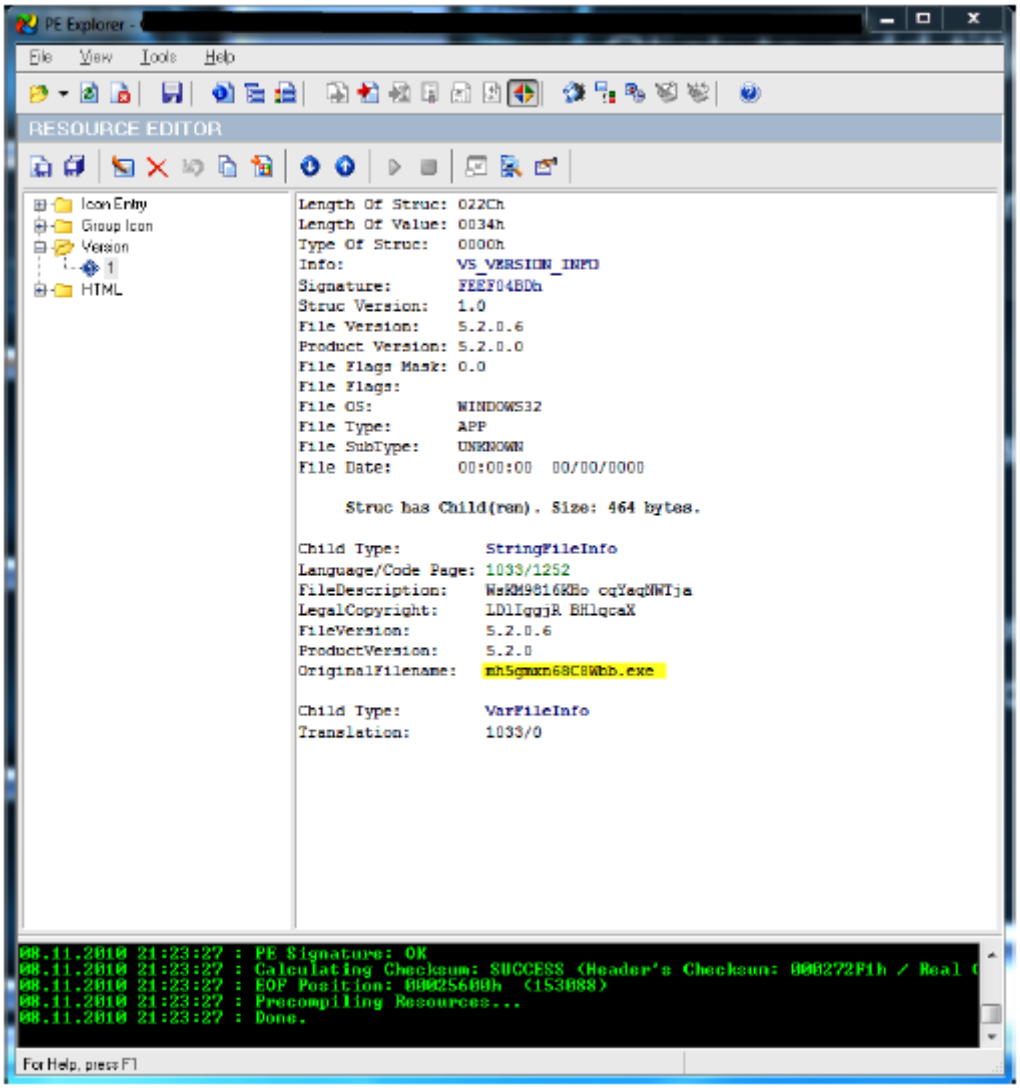
W tym miejscu do gry wchodzą aplikacje takie jak PEiD i PE Explorer. Narzędzie PEiD jest dostępne pod adresem https://github.com/wolfram77web/app-PEiD. Narzędzie takie jak PEiD może dać nam wgląd w aplikację i jej komponenty. Na przykład może zidentyfikować, czy analizowany plik jest plikiem systemu Windows, a także określić, czy jest to biblioteka DLL, plik EXE, aplikacja GUI czy aplikacja konsolowa. Poniżej znajduje się przykład danych wyjściowych PEiD pokazujących punkt wejścia (EP):



W tym przykładzie sekcja EP pokazuje, że próbka jest pakietem z UPX2. Czym właściwie jest UPX lub UPX2? UPX to tak zwany paker. Kompresja pliku polega na jego kompresji, aby był bardziej zwarty i łatwiejszy w transporcie. W ramach tego procesu, jeśli plik jest plikiem wykonywalnym, zostanie on uruchomiony bez konieczności wykonywania dodatkowych operacji, które byłyby konieczne w przypadku pliku skompresowanego. Pakowacze są używane w wielu próbkach złośliwego oprogramowania, głównie w celu ominięcia programów antywirusowych pierwszego poziomu. Co to może mieć wspólnego z identyfikacją pliku? Otóż, podczas kompresji pliku wiele ciągów znaków i innych powiązanych danych jest skompresowanych i niedostępne dla programu Strings. Jednak pliki spakowane przez UPX są łatwo wykrywane i dekompresowane. Zdekompresowany plik można przeglądać tak jak każdą inną próbkę. Poniższy zrzut ekranu pokazuje, jak wygląda nagłówek pliku skompresowany za pomocą UPX w edytorze szesnastkowym:

```
01C0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01D0h: 55 50 58 30 00 00 00 00 00 B0 00 00 00 10 00 00  UPX0.....°......
01E0h: 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00  ................
01F0h: 00 00 00 00 80 00 00 E0 55 50 58 31 00 00 00 00  ....€..àUPX1....
0200h: 00 60 00 00 00 C0 00 00 00 54 00 00 00 04 00 00  .`...À...T......
0210h: 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 E0  ............@..à
0220h: 55 50 58 32 00 00 00 00 00 10 00 00 00 20 01 00  UPX2......... ..
0230h: 00 02 00 00 00 58 00 00 00 00 00 00 00 00 00 00  .....X..........
0240h: 00 00 00 00 40 00 00 C0 00 00 00 00 00 00 00 00  ....@..À........
```

Przyjrzyjmy się teraz PE Explorerowi. Ta aplikacja, podobnie jak PeStudio, pozwala rozłożyć pliki systemu Windows na elementy podstawowe i daje nam wgląd w próbkę. PE Explorer może dostarczyć wielu informacji, co widać na poniższym zrzucie ekranu:



W tym przykładzie plik o nazwie mh5gmxn68C8Wbb.exe może być czymś, co warto przeszukać w celu uzyskania dodatkowych informacji. Teraz, gdy poświęciliśmy trochę czasu na analizę statyczną i to, co możemy uzyskać z próbki bez jej uruchamiania w systemie, możemy przyjrzeć się analizie dynamicznej, w której faktycznie wykonujemy kod i sprawdzamy, jakie operacje i artefakty mogą znajdować się w systemie.

Analiza dynamiczna

Analiza dynamiczna, czasami nazywana analizą behawioralną, to wykonywanie kodu w kontrolowanym środowisku laboratoryjnym. W tym środowisku znajdują się narzędzia do rejestrowania procesów, aktywności sieciowej i artefaktów, które mogą pojawić się w systemie. Nie jest to wyczerpująca lista narzędzi i procedur, jednak stanowi podstawę do rejestrowania informacji, które mogą Cię zainteresować na temat próbki. Zacznijmy od przyjrzenia się procesom.

Aktywność procesów

Process Explorer, będący częścią pakietu Microsoft Sysinternals, to aplikacja umożliwiająca monitorowanie uruchomionych procesów i dostarczająca szczegółowych informacji o procesie w następujących obszarach:

• Ścieżka obrazu lub programu

• Wydajność

• Wykres wydajności

• Wątki – do tego potrzebny jest debuger Microsoft

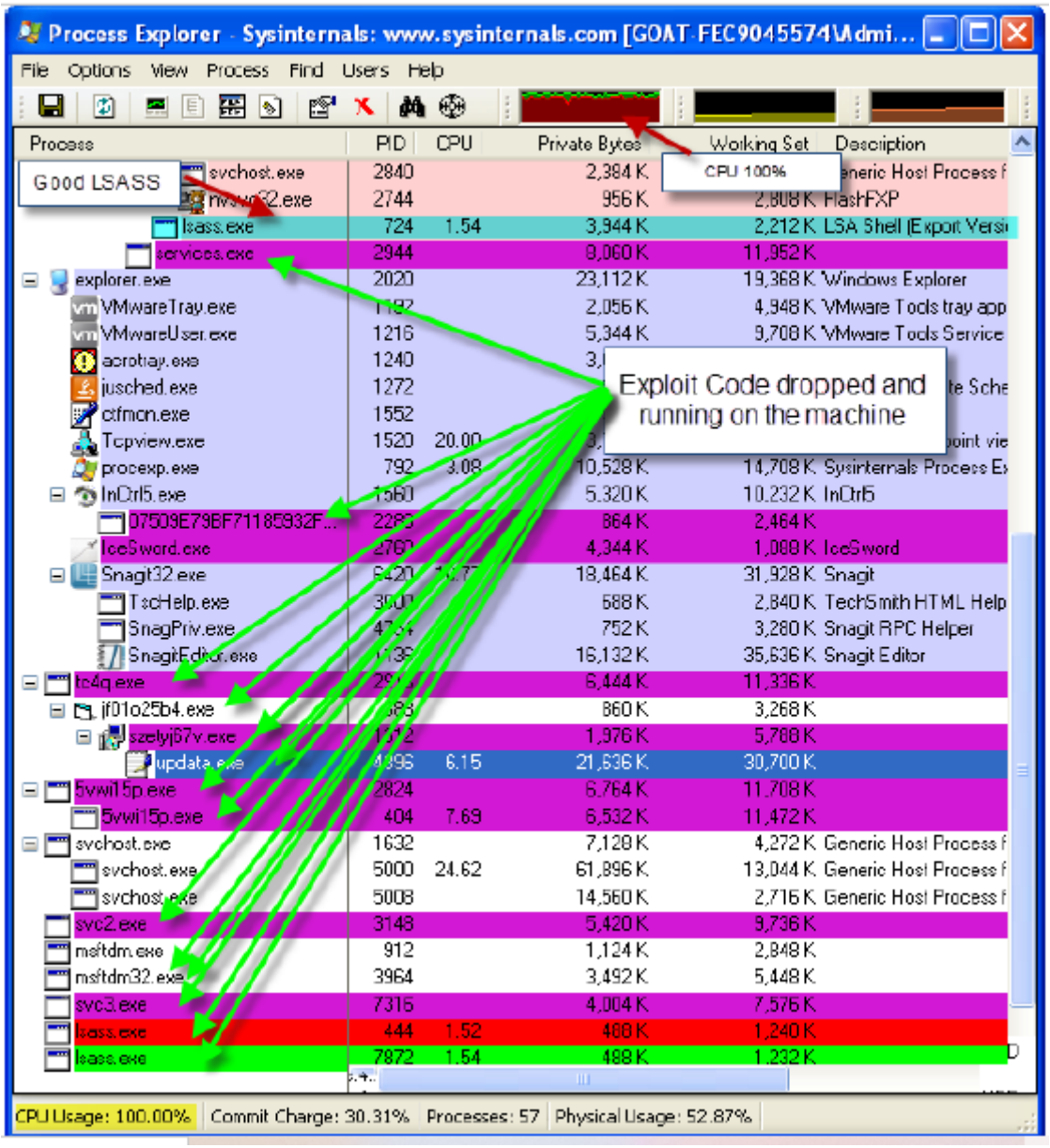
• Połączenie sieciowe

• Bezpieczeństwo

• Środowisko

• Ciągi znaków

Zobacz przykład wyników Process Explorera na poniższym zrzucie ekranu:

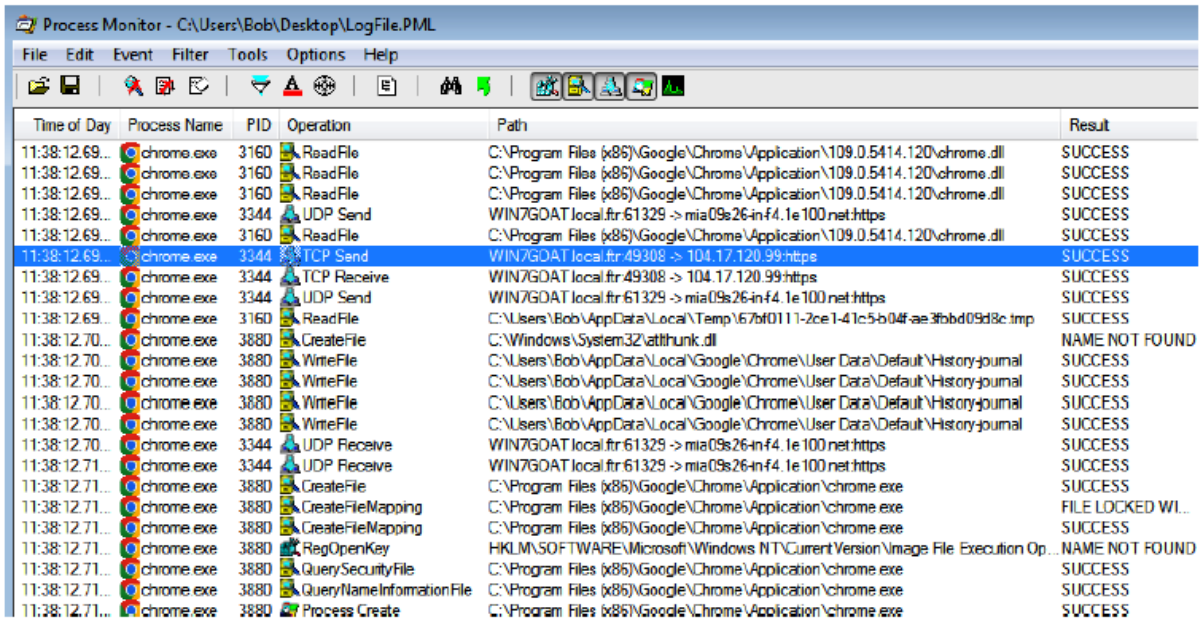


To narzędzie jest niezwykle przydatne do monitorowania i śledzenia procesów oraz drzew procesów podczas wykonywania kodu. Innym narzędziem bardzo podobnym do Process Explorera jest Process Hacker. Chociaż jest niemal identyczny z Process Explorerem, oferuje on dodatkowe funkcje, których

tam nie ma – w szczególności możliwość pobierania ciągów pamięci nie tylko według minimalnej długości, ale także według regionu pamięci: prywatnego, obrazu i/lub mapowanego. Jest to bardziej kompleksowe rozwiązanie niż Process Explorer, który udostępnia jedynie ciągi pamięci bez filtrów. Teraz, gdy możemy monitorować proces i wszelkie procesy potomne utworzone w wyniku wykonania przykładu, musimy wiedzieć, co dzieje się na poziomie systemu operacyjnego i systemu plików.

Monitor Procesów

Istnieje do tego celu inne narzędzie Sysinternals o nazwie Monitor Procesów lub Procmon.exe oraz 64-bitowa wersja Procmon64.exe. To narzędzie monitoruje i rejestruje aktywność na komputerze w czterech głównych obszarach: Rejestrze, Systemie Plików, Sieci oraz Aktywności Procesów/Wątków. Po zakończeniu wykonywania przykładu można zapisać dane wyjściowe, które można filtrować i przeglądać. Domyślne dane wyjściowe są w natywnym formacie Monitora Procesów z rozszerzeniem .pml; można je jednak również zapisać w formatach CSV i XML do wykorzystania z innymi narzędziami. Poniżej znajduje się przykładowy wygląd ekranu Monitora Procesów:

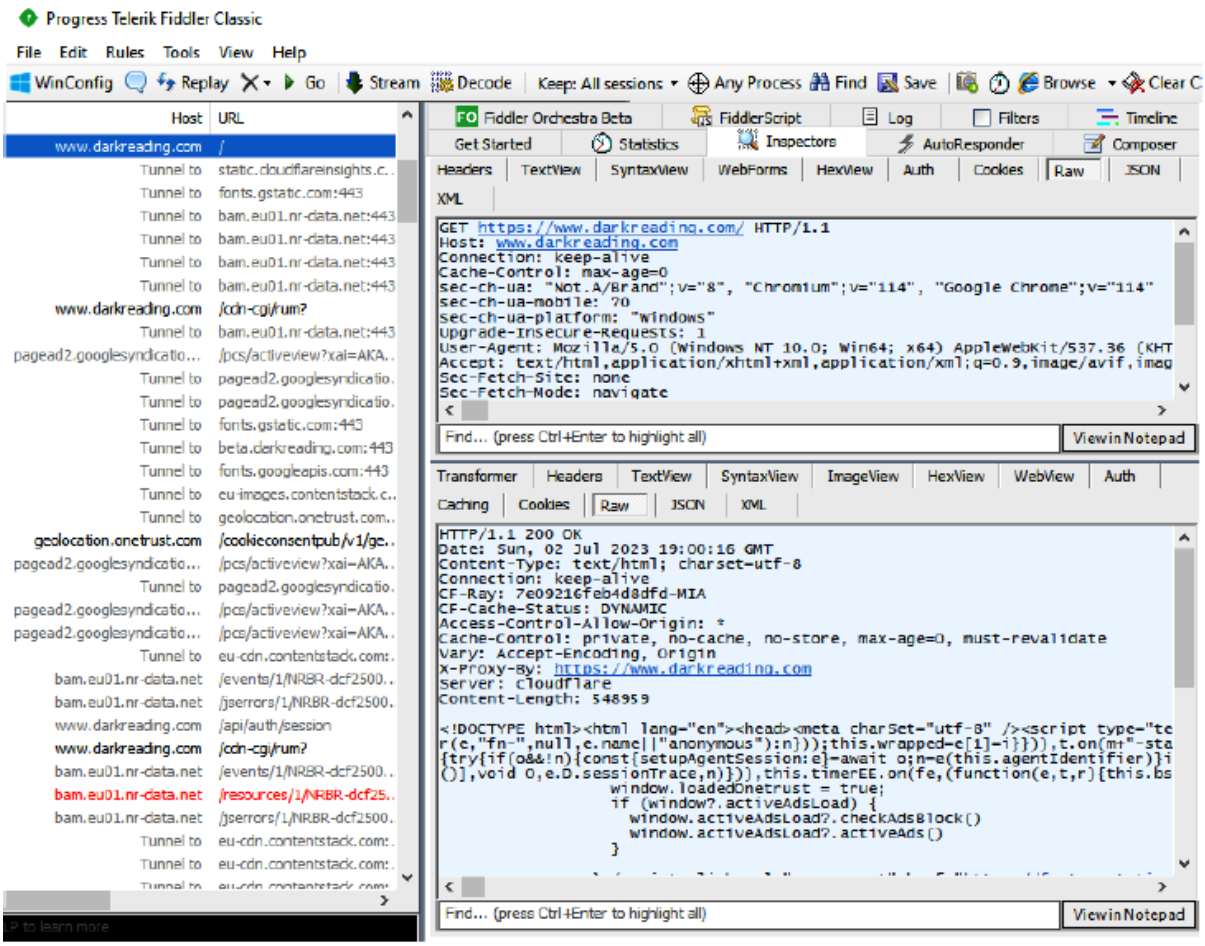


Time of Day	Process Name	PID	Operation	Path	Result
11:38:12.69...	chrome.exe	3160	ReadFile	C:\Program Files (x86)\Google\Chrome\Application\109.0.5414.120\chrome.dll	SUCCESS
11:38:12.69...	chrome.exe	3160	ReadFile	C:\Program Files (x86)\Google\Chrome\Application\109.0.5414.120\chrome.dll	SUCCESS
11:38:12.69...	chrome.exe	3160	ReadFile	C:\Program Files (x86)\Google\Chrome\Application\109.0.5414.120\chrome.dll	SUCCESS
11:38:12.69...	chrome.exe	3344	UDP Send	WIN7GOAT.local.ftr:61329 -> mia09s26-in-f4.1e100.net:https	SUCCESS
11:38:12.69...	chrome.exe	3160	ReadFile	C:\Program Files (x86)\Google\Chrome\Application\109.0.5414.120\chrome.dll	SUCCESS
11:38:12.69...	chrome.exe	3344	TCP Send	WIN7GOAT.local.ftr:49308 -> 104.17.120.99:https	SUCCESS
11:38:12.69...	chrome.exe	3344	TCP Receive	WIN7GOAT.local.ftr:49308 -> 104.17.120.99:https	SUCCESS
11:38:12.69...	chrome.exe	3344	UDP Send	WIN7GOAT.local.ftr:61329 -> mia09s26-in-f4.1e100.net:https	SUCCESS
11:38:12.69...	chrome.exe	3160	ReadFile	C:\Users\Bob\AppData\Local\Temp\67bf0111-2ce1-41c5-b04f-ae3fbbd09d8c.tmp	SUCCESS
11:38:12.70...	chrome.exe	3880	CreateFile	C:\Windows\System32\atlthunk.dll	NAME NOT FOUND
11:38:12.70...	chrome.exe	3880	WriteFile	C:\Users\Bob\AppData\Local\Google\Chrome\User Data\Default\History-journal	SUCCESS
11:38:12.70...	chrome.exe	3880	WriteFile	C:\Users\Bob\AppData\Local\Google\Chrome\User Data\Default\History-journal	SUCCESS
11:38:12.70...	chrome.exe	3880	WriteFile	C:\Users\Bob\AppData\Local\Google\Chrome\User Data\Default\History-journal	SUCCESS
11:38:12.70...	chrome.exe	3880	WriteFile	C:\Users\Bob\AppData\Local\Google\Chrome\User Data\Default\History-journal	SUCCESS
11:38:12.70...	chrome.exe	3344	UDP Receive	WIN7GOAT.local.ftr:61329 -> mia09s26-in-f4.1e100.net:https	SUCCESS
11:38:12.71...	chrome.exe	3344	UDP Receive	WIN7GOAT.local.ftr:61329 -> mia09s26-in-f4.1e100.net:https	SUCCESS
11:38:12.71...	chrome.exe	3880	CreateFile	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	SUCCESS
11:38:12.71...	chrome.exe	3880	CreateFileMapping	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	FILE LOCKED WI...
11:38:12.71...	chrome.exe	3880	CreateFileMapping	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	SUCCESS
11:38:12.71...	chrome.exe	3880	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Op...	NAME NOT FOUND
11:38:12.71...	chrome.exe	3880	QuerySecurityFile	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	SUCCESS
11:38:12.71...	chrome.exe	3880	QueryNameInformationFile	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	SUCCESS
11:38:12.71...	chrome.exe	3880	Process Create	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	SUCCESS

Na zrzucie ekranu filtrowaliśmy Chrome jako nazwę procesu i widzimy, że nawiązuje on połączenie sieciowe, zapisuje dane w plikach w systemie, a nawet uzyskuje dostęp do klucza rejestru. Każdy z tych wpisów można kliknąć, aby uzyskać więcej szczegółów na temat konkretnej aktywności, co daje doskonały wgląd w aktywność systemu. Teraz zwróćmy uwagę na aktywność sieciową.

Aktywność sieciowa

Większość złośliwego oprogramowania próbuje komunikować się przez internet ze swoim serwerem dowodzenia i kontroli, czyli C2. Często nazywane jest to operacją „telefonu domowego", a monitorowanie jej pozwala na wykrywanie i przechwytywanie tych informacji. Istnieją różne narzędzia do przechwytywania aktywności sieciowej, w zależności od tego, co konkretnie chcesz przechwycić. Zacznijmy od ruchu sieciowego. Atakujący z biegiem lat nauczyli się, że ruch wychodzący na dowolnym porcie nie zadziała, ponieważ zapora sieciowa ofiary go blokuje. Atakujący wie jednak również, że ruch HTTP/S jest powszechnie dozwolony i istnieje duże prawdopodobieństwo nawiązania połączeń zewnętrznych. Właśnie tutaj pojawia się Fiddler. Fiddler to serwer proxy przechwytujący cały powiązany ruch kierowany do internetu. Fiddlera można znaleźć pod adresem https://www.telerik.com/fiddler. Oto przykładowy wynik działania Fiddlera:



W tym przypadku korzystaliśmy z przeglądarki Chrome, aby przejść do darkreading.com. Fiddler rejestruje wszystkie inne miejsca, do których kierowane były żądania, w tym treści Google i informacje geolokalizacyjne. Każdy wpis po lewej stronie można wybrać, co pozwala uzyskać więcej szczegółów, w tym ruch sieciowy, informacje o plikach cookie i dane formularzy. To doskonałe narzędzie do rejestrowania ruchu związanego z siecią. W innych sytuacjach, gdy ruch nie jest związany z siecią i jest aktywny na różnych portach lub gdy wolisz całkowicie ograniczyć dostęp komputera testowego do internetu, możesz użyć FakeNet-NG. FakeNet-NG to aplikacja rozwijana przez zespół Flare z Mandiant. FakeNet-NG umożliwia emulację usług sieciowych, jednocześnie gromadząc dane telemetryczne dotyczące aktywności sieciowej. Jedną z doskonałych funkcji FakeNet-NG jest funkcja DumpPackets, która po zakończeniu testów zrzuca zebrane informacje do pliku PCAP, który można dalej analizować za pomocą innych narzędzi, takich jak Wireshark. Mówiąc o Wireshark, jest to jedno z ostatnich narzędzi analitycznych, które omówimy. Wireshark można skonfigurować tak, aby przechwytywał pakiety podczas analizy, lub można go używać wyłącznie do analizy. W każdym razie Wireshark jest niezbędnym narzędziem podczas pracy ze złośliwym oprogramowaniem. Oprócz rejestrowania pakietów, Wireshark umożliwia:

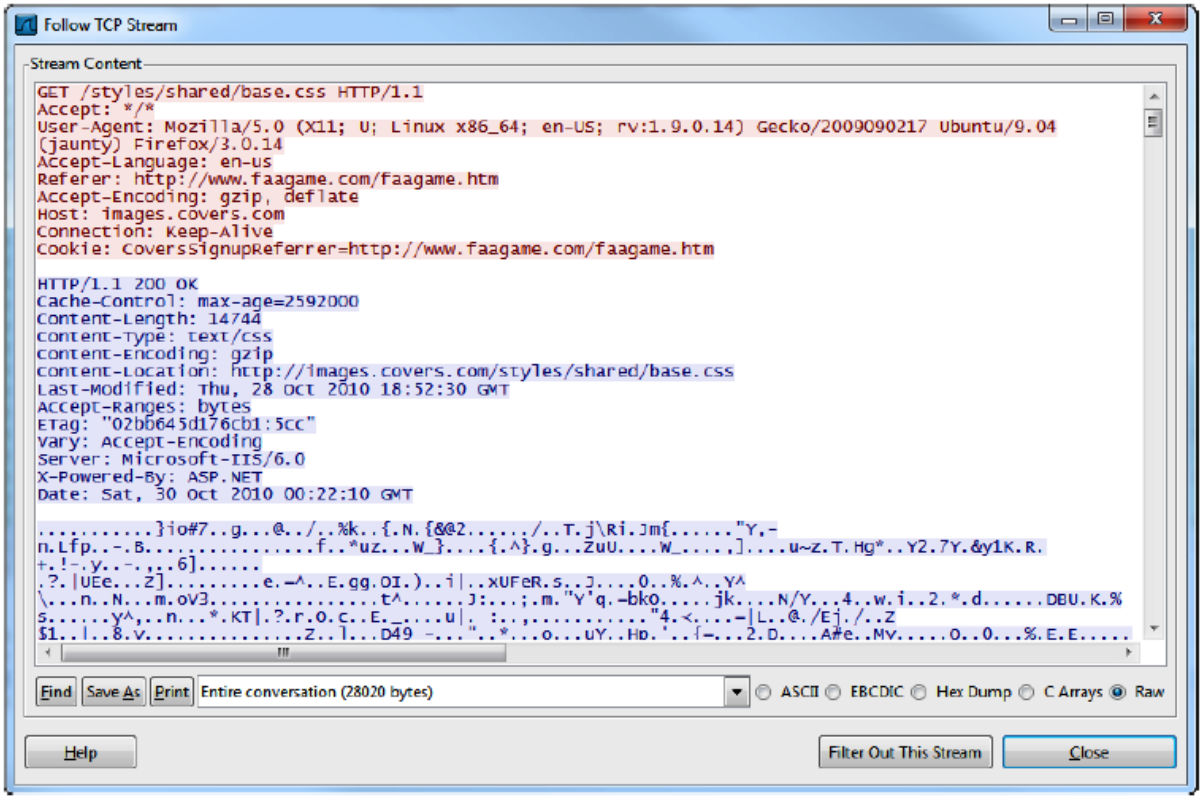
- Przeglądanie konkretnych konwersacji
- Wyodrębnianie plików
- Wyświetlanie punktów końcowych komunikacji
- Wyszukiwanie określonych ciągów znaków w nagłówku i treści

• Analizowanie konkretnej konwersacji poprzez kliknięcie prawym przyciskiem myszy na pakiecie i wybranie opcji Śledź strumień TCP

• Wyświetlanie listy punktów końcowych i liczby pakietów za pomocą opcji Statystyki w menu Wireshark

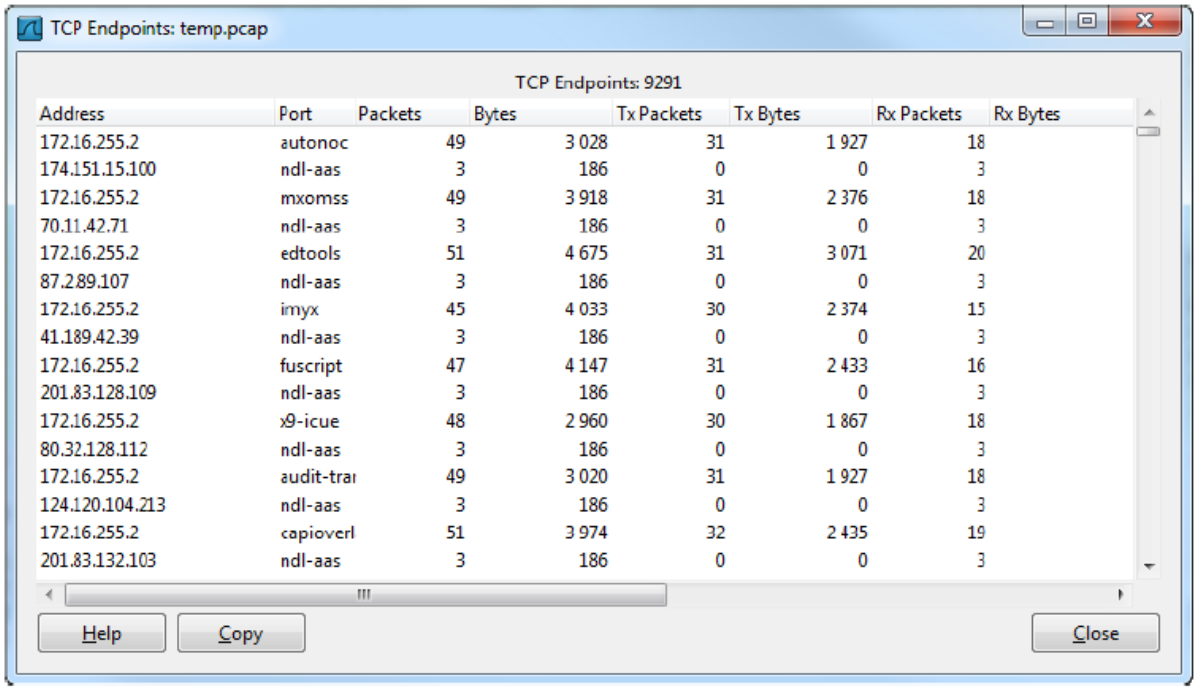
Oto kilka jego funkcji; przyjrzyjmy się niektórym ekranom, aby lepiej zrozumieć, co możemy zobaczyć:

• Poniżej znajduje się przykład funkcji „Śledź strumień TCP". Wireshark zbiera i wyświetla całą konwersję do analizy:



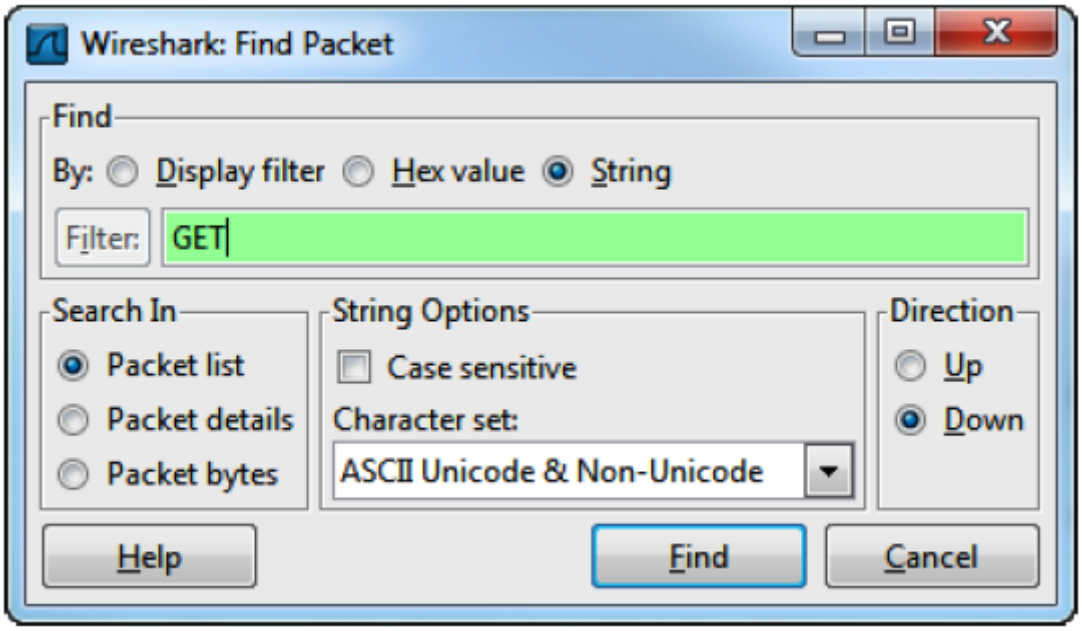
Dodatkowo koduje komunikację kolorami – na czerwono po stronie klienta i na niebiesko po stronie serwera. Ułatwia to szybkie śledzenie aktywności.

• Poniżej znajduje się przykład statystyk punktów końcowych, pokazujący wszystkie adresy IP, z którymi komputer hosta nawiązał kontakt podczas analizy:

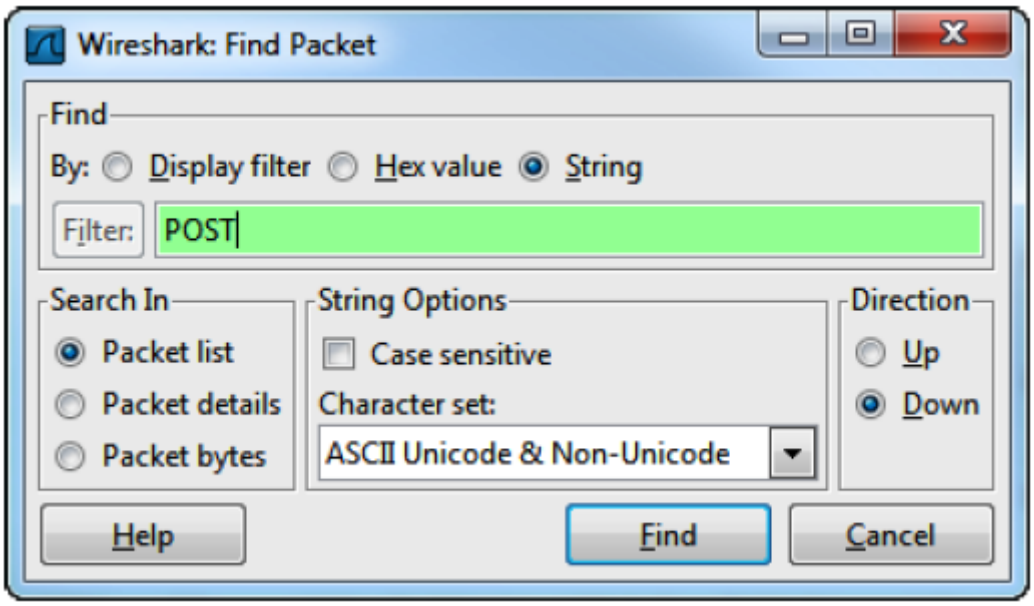


Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
172.16.255.2	autonoc	49	3 028	31	1 927	18	
174.151.15.100	ndl-aas	3	186	0	0	3	
172.16.255.2	mxomss	49	3 918	31	2 376	18	
70.11.42.71	ndl-aas	3	186	0	0	3	
172.16.255.2	edtools	51	4 675	31	3 071	20	
87.2.89.107	ndl-aas	3	186	0	0	3	
172.16.255.2	imyx	45	4 033	30	2 374	15	
41.189.42.39	ndl-aas	3	186	0	0	3	
172.16.255.2	fuscript	47	4 147	31	2 433	16	
201.83.128.109	ndl-aas	3	186	0	0	3	
172.16.255.2	x9-icue	48	2 960	30	1 867	18	
80.32.128.112	ndl-aas	3	186	0	0	3	
172.16.255.2	audit-trai	49	3 020	31	1 927	18	
124.120.104.213	ndl-aas	3	186	0	0	3	
172.16.255.2	capioverl	51	3 974	32	2 435	19	
201.83.132.103	ndl-aas	3	186	0	0	3	

• Kolejną świetną funkcją Wiresharka jest funkcja wyszukiwania. Umożliwia ona wyszukiwanie i znajdowanie aktywności, takich jak HTTP GET i POST. Umożliwia również wyszukiwanie określonych wartości szesnastkowych lub ciągów znaków. Może to być bardzo przydatne, jeśli szukasz wskaźników IOC. Aby skorzystać z funkcji wyszukiwania, przytrzymaj klawisz Ctrl i wybierz F, aby wyświetlić ekran wyszukiwania, jak pokazano na poniższym zrzucie ekranu. Poniżej znajduje się przykład użycia funkcji wyszukiwania do wyszukiwania aktywności HTTP GET. Możesz użyć tej funkcji wyszukiwania, aby znaleźć ogólną aktywność w sieci, w której uzyskiwany jest dostęp do stron internetowych:



• Poniżej znajduje się przykład wyszukiwania aktywności HTTP POST. Możesz użyć tego wyszukiwania, aby znaleźć dane wysyłane do stron internetowych, na przykład dane przesyłane w formularzu:



Możesz skorzystać z tych i innych wyszukiwań z serwerów C2, które publikują i kontrolują zainfekowaną maszynę. Możesz również użyć ich do sprawdzenia, jakie informacje są przesyłane z zainfekowanej maszyny do serwera i odwrotnie. Nie jest to bynajmniej wyczerpująca lista narzędzi i procesów do dynamicznej analizy złośliwego oprogramowania, ale pomoże Ci ona rozpocząć ten proces. Skoro omówiliśmy już analizę dynamiczną, przyjrzyjmy się, jak wykrywać i usuwać złośliwe oprogramowanie. Wykrywanie i usuwanie złośliwego oprogramowania Jedną z pierwszych rzeczy związanych ze złośliwym oprogramowaniem, w zależności od jego rodzaju, jest jego znalezienie i usunięcie, zanim wyrządzi szkody w systemie lub sieci. W tym celu można zastosować wiele narzędzi i technik. Porozmawiajmy teraz o niektórych sposobach wykrywania i usuwania złośliwego oprogramowania w sieci, wykraczających poza użycie oprogramowania antywirusowego:

• Tokeny Canary: Tokeny Canary to pliki i ustawienia celowo umieszczane w sieci lub systemach, które po uzyskaniu do nich dostępu generują alert. Przykłady tego są częstsze w środowiskach sieciowych, na przykład umieszczanie plików w udziale sieciowym o nazwach takich jak Dane finansowe czy Plany na przyszłość. Innym przykładem jest tworzenie kont użytkowników lub usług, które mogą oznaczać wysokie uprawnienia, takie jak Administrator.

• Sygnatury Yet Another Recursive Acronym (YARA): YARA to narzędzie, które wykorzystuje spreparowane pliki tekstowe zwane regułami YARA do wykrywania obecności złośliwych plików w systemach lub sieciach. W niektórych przypadkach YARA jest wbudowana w systemy wykrywania i reagowania na ataki w punktach końcowych (EDR). W innych przypadkach można ją zautomatyzować za pomocą skryptu.

• Open Source HIDS SECurity (OSSEC): OSSEC to narzędzie komercyjne, ale istnieje darmowa wersja open source, z której można korzystać. Podobnie jak Canarytokens, OSSEC może monitorować integralność plików; może to być szczególnie przydatne w przypadku plików konfiguracyjnych, stron internetowych i innych plików, które atakujący mogą wykorzystać, aby systemy zachowywały się inaczej niż zamierzono. Inne aplikacje, które mieszczą się w tym obszarze, to Advanced Intrusion Detection Environment (AIDE), Samhain, syschangemon i osquery.

Te konkretne aplikacje mogą działać w całym przedsiębiorstwie i stanowią część holistycznego podejścia do bezpieczeństwa przedsiębiorstwa. Kolejnym obszarem, na którym należy się skupić, jest ruch przychodzący i wychodzący, ponieważ monitorowanie tej aktywności pozwala na zlokalizowanie wielu złośliwych oprogramowań, więc przyjrzyjmy się temu bliżej.

Monitorowanie obwodowe

Kolejnym obszarem, w którym należy szukać złośliwego oprogramowania lub szkodliwych zachowań, jest obwód. Może to być rejestrowanie zapór sieciowych lub systemy wykrywania włamań (IDS). Monitorowanie obwodu sieci występuje na dwa sposoby:

• Monitory ruchu przychodzącego: Znajdują się one na styku sieci korporacyjnej i internetu. Mogą być częścią oprogramowania filtrującego ruch przychodzący routera granicznego lub zewnętrznej zapory sieciowej, albo mogą być samodzielnymi monitorami pasywnymi. Mogą być częścią routera granicznego lub zewnętrznej zapory sieciowej, albo działać niezależnie jako monitory pasywne. Monitory te mogą wykorzystywać techniki heurystyczne, anomalie lub oparte na sygnaturach do wykrywania ruchu złośliwego oprogramowania. Inną techniką może być wykorzystanie honeypota do wykrywania złośliwej aktywności. Przykładem może być żądanie do serwera lub witryny internetowej dotyczące czegoś, co nie istnieje, ale ma znaną lukę lub lukę w zabezpieczeniach.

• Monitory ruchu wychodzącego: Są one względne i często uważane za granicę między siecią organizacji a internetem; jednak ruch wychodzący może również odnosić się do granicy między dowolnym segmentem sieci. Niektóre organizacje wykorzystują tę technologię do tworzenia oddzielnych grup kontrolnych, na przykład izolując programistów od produkcji. Oprogramowanie filtrujące ruch wychodzący routera LAN lub przełącznika może zawierać monitor ruchu wychodzącego. Monitory ruchu wychodzącego zostały stworzone w celu identyfikacji źródła ataku złośliwego oprogramowania poprzez monitorowanie ruchu wychodzącego pod kątem oznak skanowania lub innej nietypowej aktywności. Monitorowanie to może służyć do wykrywania typowych wzorców sekwencyjnego lub losowego skanowania stosowanych przez atakujących i blokowania ich. Ponadto monitor może być w stanie rozpoznawać i reagować na nietypowo wysoki ruch e-mail generowany przez spam lub eksfiltrację danych.

Skoro omówiliśmy już wykrywanie, monitorowanie i analizę, poświęćmy chwilę na omówienie zapobiegania. Można zastosować kilka technik, aby uniemożliwić złośliwemu oprogramowaniu dostęp do pojedynczego systemu lub sieci.

Zapobieganie złośliwemu oprogramowaniu

Poniżej przedstawiono kilka działań, które można wdrożyć, aby zapobiec, a przynajmniej spowolnić rozprzestrzenianie się złośliwego oprogramowania:

• Wyłączenie automatycznego uruchamiania dla nośników USB i CD-ROM

• Usuwanie nieużywanych programów i ścisła kontrola dozwolonych aplikacji

• Wstępne skanowanie stron internetowych przed wejściem na nie lub użyciem; na przykład:

- Korzystanie z systemu wykorzystującego listę RBL (Ral-time Blackhole List), takiego jak Websense lub Blue Coat

- Alternatywnie, podczas uzyskiwania dostępu do strony internetowej, oprogramowanie antywirusowe komputera, takie jak Avast lub AVG, przeprowadza wstępne skanowanie. Należy pamiętać, że proces ten może potencjalnie spowolnić komputer ze względu na zasobochłonny charakter skanowania.

• Regularne skanowanie i instalowanie poprawek w systemach; na przykład:

- Wdrażanie poprawek w cyklu takim jak Microsoft Tuesday

- Poprawki aplikacji innych firm, takich jak Adobe, Java, Chrome itd.

- Łatanie ujawnionych luk w zabezpieczeniach w miarę ich pojawiania się i monitorowanie prób ich wykorzystania

• Wykorzystanie kontroli dostępu do sieci (NAC) lub ochrony dostępu do sieci (NAP) do kontrolowania sieci dostępowych tylko wtedy, gdy zabezpieczenia są wdrożone i aktualne

• Monitorowanie dzienników zdarzeń, zazwyczaj za pomocą produktu EDR systemu zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM), gdzie dzienniki są scentralizowane. W szczególności ważne jest monitorowanie następujących typów zdarzeń:

- Utworzone konta użytkowników

- Instalacje aplikacji

- Próby dostępu/nieudane logowania

• Monitorowanie lub wyszukiwanie aktywności poza znanymi portami lub udokumentowanymi usługami dla komputerów

• Monitorowanie i przeglądanie logów zapory sieciowej, w szczególności w następujących obszarach:

- Aplikacje i procesy łączące się z infrastrukturą C2

- Nietypowa komunikacja przychodząca lub wychodząca

• System wykrywania zagrożeń (IDS): Przydatne tylko wtedy, gdy system IDS korzysta z odpowiedniej sygnatury wykrywania. Wdrożenie tych elementów pomoże złagodzić ryzyko przyszłych incydentów. Choć nie są one niezawodne, w znacznym stopniu przyczynią się do zabezpieczenia sieci.

Podsumowanie

Omówiliśmy analizę złośliwego oprogramowania i niektóre techniki analityczne. Analiza złośliwego oprogramowania to potężne narzędzie i umiejętność, którą warto posiadać; może ona pomóc w ustaleniu, czy organizacja jest celem ataku, czy też po prostu wpadła w pułapkę oportunistyczną. Analiza złośliwego oprogramowania obejmuje znacznie więcej niż to, co zostało omówione; na przykład frameworki analityczne, takie jak Cuckoo SandBox, oraz kompleksową inżynierię wsteczną z debuggerami. Istnieją pełne kursy obejmujące tę część tematu, a jej zakres wykracza poza zakres jednego rozdziału. Mimo to, omówiono kilka ważnych koncepcji, w tym analizę statyczną i sposób określania rodzaju pliku, z którym pracujemy, czy jest on spakowany, oraz jak określać niektóre jego funkcje na podstawie importu. Omówiliśmy również analizę dynamiczną, w której próbka jest faktycznie wykonywana, a za pomocą narzędzi możemy analizować procesy, a także aktywność sieci, systemu operacyjnego i systemu plików. Poświęciliśmy również trochę czasu na omówienie sposobu, w jaki złośliwe oprogramowanie przedostaje się do komputerów, oraz sposobów wykrywania jego aktywności, gdy program antywirusowy jej nie wykryje. Na koniec krótko omówiliśmy techniki łagodzenia skutków, które można zastosować w przedsiębiorstwach i systemach, aby zapobiec rozprzestrzenianiu się złośliwego oprogramowania na maszyny.

Laboratorium

W tym laboratorium przyjrzymy się pokrótce temu, co można uznać za złośliwe oprogramowanie bez faktycznej infekcji systemu lub potencjalnego zagrożenia dla maszyn. W Metasploit wbudowane są narzędzia i exploity, które możemy poświęcić chwilę na analizę. Poniższe instrukcje pozwolą Ci przeanalizować ekstraktor haseł Mimikatz:

1. Uruchom maszynę wirtualną Kali i zaloguj się.

2. Otwórz sesję terminala na komputerze.

3. Pierwszym narzędziem, którego użyjemy, jest plik, aby zidentyfikować rodzaj pliku, z którym pracujemy.

Aby to zrobić, wpisz i uruchom następujące polecenie:

file /usr/share/windows-resources/mimikatz/x64/mimikatz.exe

Spowoduje to zwrócenie pliku wykonywalnego PE.

4. Następnie hashujemy plik, aby móc sprawdzić jego reputację w zasobach online. W tym celu wpisz i uruchom następujące polecenie:

md5sum /usr/share/windows-resources/mimikatz/x64/mimikatz.exe

Zwróci ono wartość hasha pliku.

5. Następnie sprawdzimy reputację pliku w sieci za pomocą zasobu online VirusTotal.

6. Skopiuj hash MD5 pliku i wklej go w polu wyszukiwania VirusTotal na stronie internetowej VirusTotal: https://www.virustotal.com/gui/home/search. Dzięki temu uzyskasz więcej informacji o pliku, takich jak to, które programy antywirusowe wykryły go podczas pierwszego przesłania itd.

7. Następnie przyjrzymy się ciągom znaków w pliku. Ciągi znaków czasami mogą dać nam wgląd w działanie pliku wykonywalnego. Aby to zrobić, wpisz i uruchom następujące polecenie:

strings /usr/share/windows-resources/mimikatz/x64/mimikatz.exe

-n 15 | more

To polecenie ma dwa dodatkowe komponenty, które pozwalają lepiej zobaczyć, jakie informacje są dostępne:

- Pierwszy to -n 15; informuje on łańcuchy, że liczba znaków ASCII musi być równa lub większa niż 15, aby zostały wyświetlone. To eliminuje wyświetlanie niektórych niepotrzebnych danych. *Uwaga: oznacza to również, że wszelkie cenne dane, które mają mniej niż 15 znaków, również nie będą wyświetlane, więc poeksperymentuj z rozmiarem.

- Drugi komponent jest częścią Linuksa i jest to polecenie more. Pozwala ono po prostu przewijać tekst w dół ekranu. Zamiast tego zatrzymuje się on na długości strony. Aby przejść dalej, użyj strzałki w dół dla jednego wiersza na raz lub spacji dla całej strony na raz.

- Aby się wydostać, użyj kombinacji klawiszy Ctrl + Z.

8. Ostatnim krokiem będzie sprawdzenie magicznego podpisu pliku. W tym celu musimy sprawdzić wartości szesnastkowe pliku. W tym celu wpisz i uruchom następujące polecenie:

hexeditor /usr/share/windows-resources/mimikatz/x64/mimikatz.exe

Spowoduje to wyświetlenie szesnastkowej reprezentacji pliku; poszukaj dwóch pierwszych wartości, które powinny być 4D5A. Zaznacz lub zapamiętaj ten wpis, a następnie zamknij program. Otwórz przeglądarkę internetową z dostępem do internetu i przejdź do strony https://www.garykessler.net/library/file_sigs.html, używając funkcji wyszukiwania w wyszukiwarce, która znajdzie stronę file_sigs dla wpisu 4D5A i sprawdź, jakie informacje otrzymasz.

To kończy laboratorium złośliwego oprogramowania. Masz teraz narzędzia do podstawowej analizy nieznanych plików w swoim środowisku. Jeśli zdecydujesz się na dalsze działania, możesz skonfigurować maszynę wirtualną z systemem Windows, dodać narzędzia omówione w tym rozdziale do dalszej analizy statycznej i rozpocząć proces analizy zachowania. Upewnij się tylko, że maszyna wirtualna jest dobrze odizolowana przed uruchomieniem złośliwego oprogramowania, aby zapobiec infekcji hosta głównego lub sieci, w której pracujesz.

Ocena

1. Czym zajmują się brokerzy dostępu?

A. Tworzeniem exploitów zero-day

B. Tworzeniem złośliwego oprogramowania

C. Atakowaniem podatnych systemów

D. Sprzedażą zhakowanych danych uwierzytelniających

2. Który typ nie jest złośliwym oprogramowaniem?

A. Wirus

B. Ring0

C. Robak

D. Trojan

3. Która z technik jest drugorzędna i jest wykorzystywana przez operatorów ransomware do wyłudzania pieniędzy?

A. Łatwe przetwarzanie Bitcoinów

B. Negocjatorzy okupu

C. Podwójne wymuszenie

D. Przykładowe pliki

4. W jakim pierścieniu działają rootkity na poziomie użytkownika?

A. 1

B. 2

C. 3

D. 4

5. Która strona internetowa pozwala uzyskać informacje o złośliwym oprogramowaniu?

A. Threat Genius

B. Cyber Threat Command

C. Sonar

D. VirusTotal

6. Jaki jest jeden ze sposobów identyfikacji pliku? A. Polecenie identyfikujące

B. Liczba magiczna

C. Ujawnij

D. Wireshark

7. Co to jest UPX?

A. Kompaktor

B. Formatowanie

C. Pakowacz

D. Szyfrator

8. Która aplikacja jest serwerem proxy?

A. Wireshark

B. Fiddler

C. Przechwytywanie procesów

D. MadCap

9. Do których z poniższych celów używane są tokeny Canary?

A. Alarmowanie o nietypowym dostępie do pliku lub konta

B. Przechwytywanie kluczy rejestru

C. Wstrzykiwanie informacji do ruchu sieciowego

D. Identyfikowanie użytkowników powracających na stronę internetową

10. Jakie są dwa typy monitorowania obwodowego (wybierz dwa)?

A. Wschód/zachód

B. Segmentacja/lateralizacja

C. Wejście/wyjście

D. QoS/RIP

Odpowiedzi

1. D

2. B

3. C

4. C

5. D

6. B

7. C

8. B

9. A

10. A, C