Poznanie typowych cyberataków

Istnieje wiele różnych rodzajów cyberataków - tak wiele, że można by napisać o nich całą serię książek. My nie omawiamy jednak szczegółowo wszystkich rodzajów zagrożeń, ponieważ w rzeczywistości prawdopodobnie czytasz to, aby dowiedzieć się, jak zachować cyberbezpieczeństwo, a nie o sprawach, na które nie masz wpływu, takie jak formy ataków, które zwykle są skierowane na agencje szpiegowskie, sprzęt przemysłowy lub uzbrojenie wojskowe. W tym rozdziale dowiesz się o różnych typach problemów, które cyberataki mogą stworzyć w wyniku ataków, które zwykle dotykają osoby i małe firmy.

Ataki zadające obrażenia

Atakujący przeprowadzają pewne formy cyberataków z zamiarem wyrządzenia szkód ofiarom. Zagrożenie stwarzane przez takie ataki nie polega na tym, że przestępca bezpośrednio wykradnie twoje pieniądze lub dane, ale że napastnicy wyrządzą ci krzywdę w inny określony sposób - sposób, który może ostatecznie przełożyć się na korzyści finansowe, militarne, polityczne lub inne. napastnikowi i (potencjalnie) wyrządzeniu szkody ofierze.

Typy ataków, które powodują obrażenia, obejmują

* Ataki typu Denial-of-Service (DoS)

* Rozproszone ataki typu „odmowa usługi” (DDoS)

* Botnety i zombie

* Ataki niszczące dane

Ataki typu „odmowa usługi” (DoS)

Atak typu „odmowa usługi” to taki, w którym osoba atakująca celowo próbuje sparaliżować komputer lub sieć komputerową, zalewając ją dużą ilością żądań lub danych, które przeciążają cel i uniemożliwiają mu prawidłowe odpowiadanie na uzasadnione żądania. W wielu przypadkach każde żądanie wysłane przez atakującego jest uzasadnione - na przykład normalne żądanie załadowania strony internetowej. W innych przypadkach prośby nie są zwykłymi prośbami. Zamiast tego wykorzystują wiedzę o różnych protokołach do wysyłania żądań, które optymalizują, a nawet zwiększają efekt ataku. W każdym razie ataki typu „odmowa usługi” polegają na przytłaczaniu jednostek centralnych (CPU) i / lub pamięci systemów komputerowych, wykorzystując całą dostępną przepustowość komunikacji sieciowej i / lub wyczerpując zasoby infrastruktury sieciowej, takie jak routery.

Rozproszone ataki typu „odmowa usługi” (DDoS)

Rozproszony atak DoS to atak DoS, w którym wiele pojedynczych komputerów lub innych podłączonych urządzeń w różnych regionach jednocześnie zalewa cel żądaniami. W ostatnich latach prawie wszystkie poważne ataki typu „odmowa usługi” miały charakter rozproszony, a niektóre polegały na wykorzystaniu podłączonych do Internetu kamer i innych urządzeń jako pojazdów ataku, a nie klasycznych komputerów. Celem ataku DDoS jest wyłączenie ofiary z sieci, a motywacja do tego jest różna. Czasami cel ma charakter finansowy: wyobraź sobie, na przykład, szkody, jakie mogą wyniknąć dla firmy sprzedawcy internetowego, jeśli pozbawiony skrupułów konkurent wyłączy jego witrynę podczas Czarnego Piątku. Wyobraź sobie oszusta, który ogranicza zapasy dużego sprzedawcy zabawek tuż przed rozpoczęciem ataku DDoS na tego sprzedawcę dwa tygodnie przed Bożym Narodzeniem. Ataki DDoS pozostają poważnym i rosnącym zagrożeniem. Przestępcze przedsiębiorstwa

oferują nawet usługi DDoS do wynajęcia, które są reklamowane w ciemnej sieci jako oferujące za opłatą „wyłączenie witryn konkurenta w opłacalny sposób". W niektórych przypadkach wyrzutnie DDoS mogą mieć motywy polityczne, a nie finansowe. Na przykład skorumpowany polityk może dążyć do usunięcia witryny swojego przeciwnika w trakcie sezonu wyborczego, ograniczając w ten sposób zdolność konkurenta do rozpowszechniania wiadomości i otrzymywania wkładów do kampanii online. Haktywiści mogą również przeprowadzać ataki DDoS w celu niszczenia witryn w imię „sprawiedliwości" - na przykład atakując strony organów ścigania po zabiciu nieuzbrojonej osoby podczas kłótni z policją. W rzeczywistości, według badania przeprowadzonego w 2017 r. przez Kaspersky Lab i B2B International, prawie połowa firm na całym świecie, które doświadczyły ataku DDoS, podejrzewa, że ich konkurenci mogli być w to zamieszani. Ataki DDoS mogą wpływać na osoby na trzy istotne sposoby:

* Atak DDoS na sieć lokalną może znacznie spowolnić cały dostęp do Internetu z tej sieci. Czasami te ataki powodują, że łączność jest tak wolna, że połączenia z witrynami kończą się niepowodzeniem z powodu ustawień limitu czasu sesji, co oznacza, że systemy kończą połączenia po tym, jak żądanie odpowiedzi trwa dłużej niż pewien maksymalny dopuszczalny próg.

* Atak DDoS może uniemożliwić dostęp do witryny, z której dana osoba planuje korzystać. Na przykład 21 października 2016 r. wielu użytkowników nie było w stanie dotrzeć do kilku znanych witryn, w tym Twittera, PayPal, CNN, HBO Now, The Guardian i dziesiątek innych popularnych witryn, z powodu masowego ataku DDoS na strony trzecie świadcząca różne usługi techniczne dla tych witryn i wiele innych.

Możliwość ataków DDoS jest jednym z powodów, dla których nie należy czekać do ostatniej chwili z wykonaniem transakcji bankowej online - strona, z której należy skorzystać, może być niedostępna z wielu powodów, z których jednym jest trwający atak DDoS .

* Atak DDoS może doprowadzić użytkowników do uzyskania informacji z jednej witryny zamiast z innej. Uniemożliwiając dostęp do jednej witryny, internauci poszukujący konkretnych informacji mogą ją uzyskać z innej witryny - zjawisko, które umożliwia atakującym albo rozpowszechnianie dezinformacji, albo uniemożliwia ludziom usłyszenie pewnych informacji lub punktów widzenia w ważnych sprawach. W związku z tym ataki DDoS mogą być wykorzystywane jako skuteczny mechanizm - przynajmniej krótkoterminowy - do cenzurowania przeciwstawnych punktów widzenia.

Botnety i zombie

Często ataki DDoS wykorzystują tak zwane botnety. Botnety to zbiór zainfekowanych komputerów należących do innych podmiotów, które haker zdalnie kontroluje i wykorzystuje do wykonywania zadań bez wiedzy prawowitych właścicieli. Przestępcy, którym udało się zainfekować milion komputerów złośliwym oprogramowaniem, mogą na przykład potencjalnie wykorzystać te maszyny, znane jako zombie, do jednoczesnego wysyłania wielu żądań z jednego serwera lub farmy serwerów w celu przeciążenia celu ruchem.

Ataki niszczące dane

Czasami napastnicy chcą zrobić coś więcej, niż tymczasowo przenieść stronę do trybu offline, przytłaczając ją żądaniami - mogą chcieć zaszkodzić ofierze, niszcząc lub uszkadzając informacje i / lub systemy informacyjne celu. Przestępca może próbować zniszczyć dane użytkownika poprzez atak polegający na zniszczeniu danych - na przykład, jeśli użytkownik odmówi zapłacenia okupu za pomocą oprogramowania wymuszającego okup, którego żąda oszust. Oczywiście wszystkie powody przeprowadzania ataków DDoS (patrz poprzednia sekcja) to również powody, dla których haker może również próbować zniszczyć czyjeś dane.

Ataki wiper to zaawansowane ataki polegające na niszczeniu danych, w których przestępca wykorzystuje złośliwe oprogramowanie do usuwania danych z dysku twardego lub dysku SSD ofiary w taki sposób, że ich odzyskanie jest trudne lub niemożliwe. Mówiąc prościej, jeśli ofiara nie ma kopii zapasowych, ktoś, którego komputer zostanie wyczyszczony przez program, prawdopodobnie utraci dostęp do wszystkich danych i oprogramowania, które były wcześniej przechowywane na zaatakowanym urządzeniu.

Personifikacja

Jednym z największych niebezpieczeństw, jakie stwarza Internet, jest łatwość, z jaką psotne strony mogą podszywać się pod innych. Na przykład przed erą Internetu przestępcy nie mogli łatwo podszyć się pod bank lub sklep i przekonać ludzi do oddania pieniędzy w zamian za obiecaną stopę procentową lub towary. Fizycznie wysyłane listy, a później rozmowy telefoniczne stały się narzędziami oszustów, ale żadna z tych wcześniejszych technik komunikacji nigdy nie zbliżyła się do potęgi Internetu, aby pomóc przestępcom próbującym podszyć się pod strony przestrzegające prawa. Stworzenie witryny internetowej, która naśladuje witrynę banku, sklepu lub agencji rządowej, jest dość proste i czasami zajmuje kilka minut. Przestępcy mogą znaleźć niemal nieskończoną ilość nazw domen, które są wystarczająco zbliżone do nazw domen legalnych stron, aby skłonić niektórych ludzi do uwierzenia, że witryna, którą widzą, jest prawdziwą okazją, gdy tak nie jest, dając oszustom typowy pierwszy składnik przepisu do podszywania się pod inne osoby online. Wysyłanie wiadomości e-mail, która wydaje się pochodzić od kogoś innego, jest proste i umożliwia przestępcom popełnianie wszelkiego rodzaju przestępstw w Internecie.

Wyłudzanie informacji

Phishing odnosi się do próby przekonania osoby do podjęcia pewnych działań poprzez podszywanie się pod zaufaną osobę, która może zasadnie poprosić użytkownika o podjęcie takiego działania. Na przykład przestępca może wysłać wiadomość e-mail, która wydaje się być wysłana przez duży bank i zawiera prośbę o kliknięcie łącza w celu zresetowania hasła z powodu możliwego naruszenia danych. Gdy użytkownik kliknie odsyłacz, zostaje przekierowany na stronę internetową, która wydaje się należeć do banku, ale w rzeczywistości jest repliką prowadzoną przez przestępcę. W związku z tym przestępca wykorzystuje fałszywą witrynę internetową do zbierania nazw użytkowników i haseł do witryny bankowej.

Spear phishing

Spear phishing odnosi się do ataków phishingowych zaprojektowanych i wysłanych w celu wymierzenia w określoną osobę, firmę lub organizację. Jeśli na przykład przestępca stara się uzyskać dane uwierzytelniające w systemie poczty e-mail określonej firmy, może wysyłać wiadomości e-mail spreparowane specjalnie dla określonych osób w organizacji. Często przestępcy, którzy szpiegują phish, badają swoje cele online i wykorzystują nadmiernie rozpowszechnione informacje w mediach społecznościowych w celu tworzenia szczególnie legalnie brzmiących wiadomości e-mail. Na przykład następujący typ wiadomości e-mail jest zazwyczaj dużo bardziej przekonujący niż „Zaloguj się do serwera poczty i zresetuj hasło”: „Cześć, za dziesięć minut lecę samolotem. Czy możesz zalogować się do serwera Exchange i sprawdzić, kiedy mam spotkanie? Z jakiegoś powodu nie mogę wejść. Możesz najpierw spróbować zadzwonić do mnie telefonicznie ze względów bezpieczeństwa, ale jeśli za mną tęsknisz, po prostu sprawdź informacje i wyślij mi je e-mailem - ponieważ wiesz, że otrzymuję w samolocie, który ma się rozpocząć ”.

Oszustwo CEO

Oszustwo CEO jest podobne do spear phishing, ponieważ polega na tym, że przestępca podszywa się pod dyrektora generalnego lub innego członka zarządu określonej firmy, ale instrukcje podane przez „CEO" mogą polegać na podjęciu działania bezpośrednio, a nie na logowaniu w systemie, a celem może nie być przechwycenie nazw użytkowników i haseł itp.

Oszust może na przykład wysłać wiadomość e-mail do dyrektora finansowego firmy z poleceniem wysłania przelewu do konkretnego nowego dostawcy lub wysłania wszystkich formularzy W2 organizacji za dany rok na określony adres e-mail należący do księgowego firmy. Oszustwa dyrektorów generalnych często przynoszą przestępcom znaczne korzyści i sprawiają, że pracownicy, którzy ulegają oszustwom, wydają się niekompetentni. W rezultacie ludzie, którzy padają ofiarą takich oszustw, są często zwalniani z pracy.

Smishing

Smishing odnosi się do przypadków phishingu, w których osoby atakujące dostarczają swoje wiadomości za pośrednictwem wiadomości tekstowych (SMS), a nie poczty elektronicznej. Celem może być przechwycenie nazw użytkowników i haseł lub nakłonienie użytkownika do zainstalowania złośliwego oprogramowania.

Vishing

Vishing, czyli phishing głosowy, to phishing przez POTS - co oznacza „zwykłą starą usługę telefoniczną". Tak, przestępcy używają starych, sprawdzonych metod do oszukiwania ludzi. Obecnie większość takich połączeń jest transmitowana przez systemy Voice Over IP, ale ostatecznie oszuści dzwonią do ludzi na zwykłe telefony w taki sam sposób, w jaki oszuści robią to od dziesięcioleci.

Wielorybnictwo

Wielorybnictwo odnosi się do phishingu typu spear, którego celem jest kierownictwo znanych firm lub urzędników państwowych.

Manipulowanie

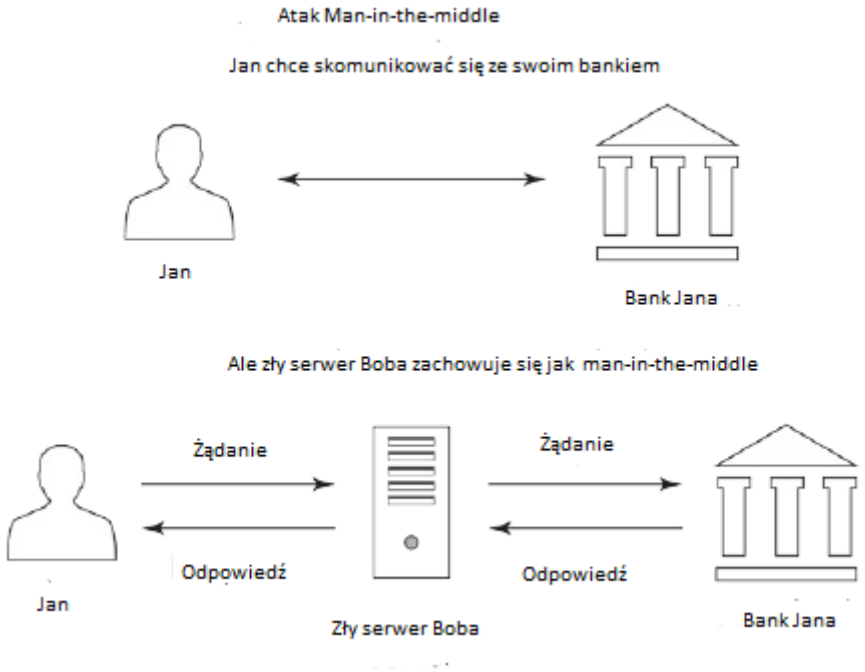
Czasami osoby atakujące nie chcą zakłócać normalnych działań organizacji, ale zamiast tego próbują wykorzystać te działania w celu uzyskania korzyści finansowych.

Często oszuści osiągają takie cele, manipulując danymi podczas przesyłania lub gdy znajdują się one w systemach ich celów w procesie znanym jako manipulowanie. W podstawowym przypadku ingerencji w przesyłane dane, na przykład, wyobraź sobie, że użytkownik bankowości internetowej poinstruował swój bank, aby przelał pieniądze na określone konto, ale w jakiś sposób przestępca przechwycił żądanie i zmienił odpowiedni numer rozliczeniowy i numer konta na swoje. posiadać. Przestępca może również włamać się do systemu i manipulować informacjami w podobnych celach. Korzystając z poprzedniego przykładu, wyobraź sobie, że przestępca zmienił adres płatności powiązany z konkretnym odbiorcą, tak że gdy dział rozrachunków z dostawcami dokonuje płatności online, środki trafiają do niewłaściwego miejsca docelowego (cóż, przynajmniej jest to błędne w oczach płatnik).

Przechwycenie

Przechwytywanie ma miejsce, gdy atakujący przechwytują informacje przesyłane między komputerami. Jeśli dane nie są odpowiednio zaszyfrowane, strona, która je przechwytuje, może być w stanie je niewłaściwie wykorzystać. Jeden specjalny rodzaj przechwytywania jest znany jako atak man-in-the-middle. W tego typu ataku przechwytujący przekazuje dane między nadawcą a odbiorcą, próbując ukryć fakt, że dane są przechwytywane. W takim przypadku proxy odnosi się do człowieka

pośrodku przechwytywania żądań, a następnie przesyłanie ich (w zmodyfikowanej lub niezmodyfikowanej formie) do pierwotnie zamierzonych miejsc docelowych, a następnie odbieranie odpowiedzi od tych odbiorców i przesyłanie ich (w zmodyfikowanej lub niezmienionej formie) z powrotem do nadawcy. Wykorzystując proxy, pośrednik utrudnia nadawcy poznanie, że jego komunikacja jest przechwytywana, ponieważ kiedy komunikuje się z serwerem, otrzymuje odpowiedzi, których oczekuje. Na przykład przestępca może założyć fałszywą witrynę banku i przekazać wszelkie informacje, które ktoś wejdzie na fałszywą stronę, do rzeczywistej witryny banku, aby przestępca mógł odpowiedzieć tymi samymi informacjami, które przesłałby legalny bank. Pośrednictwo dla tego rodzaj nie tylko pomaga przestępcy uniknąć wykrycia - użytkownik, który podaje oszustom swoje hasło, a następnie wykonuje swoje normalne czynności związane z bankowością internetową, może nie mieć pojęcia, że podczas sesji bankowości internetowej wydarzyło się coś nienormalnego - ale także pomaga przestępca upewnij się, że przechwyci właściwe hasło. Jeśli użytkownik wprowadzi niepoprawne hasło, przestępca będzie wiedział, aby poprosić o prawidłowe. Rysunek przedstawia anatomię man-in-the-middle przechwytującego i przekazującego komunikację.



Kradzież danych

Wiele cyberataków obejmuje kradzież danych ofiary. Atakujący może chcieć ukraść dane należące do osób fizycznych, firm lub agencji rządowej z co najmniej jednego z wielu możliwych powodów. Ludzie, firmy, organizacje non-profit i rządy są narażeni na kradzież danych.

Kradzież danych osobowych

Przestępcy często próbują ukraść dane ludzi w nadziei na znalezienie przedmiotów, na których mogą zarabiać, w tym:

* Dane, które można wykorzystać do kradzieży tożsamości lub sprzedać złodziejom tożsamości

* Kompromitujące zdjęcia lub dane zdrowotne, które można sprzedać lub wykorzystywać jako część programu szantażu

* Informacje, które zostały skradzione, a następnie usunięte z komputera użytkownika, za które może zostać zapłacony okup

* Listy haseł, których można użyć do naruszenia innych systemów

* Poufne informacje o sprawach związanych z pracą, które mogą zostać wykorzystane do nielegalnego handlu akcjami na podstawie informacji poufnych

* Informacje o nadchodzących planach podróży, które można wykorzystać do planowania napadu na dom ofiary

Kradzież danych biznesowych

Przestępcy mogą wykorzystywać dane skradzione z firm do wielu niecnych celów:

* Dokonywanie transakcji giełdowych: posiadanie wcześniejszej wiedzy na temat tego, jaki okaże się kwartał, daje przestępcy informacje poufne, na temat których może nielegalnie handlować akcjami lub opcjami i potencjalnie osiągnąć znaczny zysk.

* Sprzedaż danych pozbawionym skrupułów konkurentom: przestępcy, którzy kradną dane o sprzedaży ,informacje o rurociągach, dokumenty zawierające szczegóły przyszłych produktów lub inne wrażliwe informacje mogą sprzedawać te dane pozbawionym skrupułów konkurentom lub pozbawionym skrupułów pracownikom konkurencji, których kierownictwo może nigdy nie dowiedzieć się, w jaki sposób tacy pracownicy nagle poprawili swoje wyniki.

* Wyciek danych do mediów: poufne dane mogą zawstydzić ofiarę i spowodować spadek jego akcji (być może po krótkiej sprzedaży niektórych akcji).

* Wyciek danych objętych przepisami dotyczącymi prywatności: Ofiara może zostać ukarana grzywną.

* Rekrutacja pracowników: rekrutując pracowników lub sprzedając informacje innym firmom, które chcą zatrudnić pracowników o podobnych umiejętnościach lub znających systemy konkursowe, przestępcy, którzy kradną wiadomości e-mail i odkrywają komunikację między pracownikami, która wskazuje, że jeden lub więcej pracowników jest niezadowolonych ze swoich obecnych stanowiska mogą sprzedawać te informacje stronom pragnącym zatrudnić.

* Kradzież i korzystanie z własności intelektualnej: strony, które kradną kod źródłowy oprogramowania komputerowego, mogą uniknąć płacenia opłat licencyjnych prawowitemu właścicielowi oprogramowania. Strony, które kradną dokumenty projektowe utworzone przez innych po przeprowadzeniu szeroko zakrojonych badań i rozwoju, mogą z łatwością zaoszczędzić miliony - a czasem nawet miliardy - na kosztach badań i rozwoju

Złośliwe oprogramowanie

Złośliwe oprogramowanie lub złośliwe oprogramowanie to wszechstronne określenie oprogramowania, które celowo wyrządza szkody użytkownikom, którzy zazwyczaj nie mają pojęcia, że je uruchamiają. Złośliwe oprogramowanie obejmuje wirusy komputerowe, robaki, trojany, ransomware, scareware, spyware, kopacze kryptowalut, adware i inne programy przeznaczone do wykorzystywania zasobów komputera w niecnych celach.

Wirusy

Wirusy komputerowe to przypadki złośliwego oprogramowania, które po uruchomieniu replikują się, wstawiając własny kod do systemów komputerowych. Zazwyczaj wstawianie odbywa się w plikach danych (na przykład jako nieuczciwe makra w dokumencie programu Word), w specjalnej części

dysków twardych lub dysków półprzewodnikowych, które zawierają kod i dane używane do rozruchu komputera lub dysku (znane również jako sektory rozruchowe) lub inne programy komputerowe. Podobnie jak wirusy biologiczne, wirusy komputerowe nie mogą się rozprzestrzeniać bez hostów do zarażenia. Niektóre wirusy komputerowe znacząco wpływają na zainfekowane hosty. Niektóre wirusy komputerowe znacząco wpływają na wydajność ich hostów, podczas gdy inne są przynajmniej czasami prawie niezauważalne. Podczas gdy wirusy komputerowe nadal wyrządzają ogromne szkody na całym świecie, większość poważnych zagrożeń w postaci złośliwego oprogramowania pojawia się obecnie w postaci robaków i trojanów.

Robaki

Robaki komputerowe to samodzielne fragmenty złośliwego oprogramowania, które replikują się same bez potrzeby rozprzestrzeniania się hostów. Robaki często rozprzestrzeniają się za pośrednictwem połączeń, wykorzystując luki w zabezpieczeniach docelowych komputerów i sieci. Ponieważ zwykle zajmują przepustowość sieci, robaki mogą wyrządzać szkody nawet bez modyfikowania systemów lub kradzieży danych. Mogą spowalniać połączenia sieciowe - a niewiele osób, jeśli w ogóle, lubi, gdy ich połączenia wewnętrzne i internetowe zwalniają.

Trojany

Trojany (odpowiednio nazwane na cześć historycznego konia trojańskiego) to złośliwe oprogramowanie, które jest zamaskowane jako nieszkodliwe oprogramowanie lub ukryte w legalnej, nieszkodliwej aplikacji lub danych cyfrowych. Trojany najczęściej rozprzestrzeniają się za pomocą jakiejś formy inżynierii społecznej - na przykład poprzez nakłonienie ludzi do kliknięcia łącza, zainstalowania aplikacji lub uruchomienia załącznika do wiadomości e-mail. W przeciwieństwie do wirusów i robaków trojany zazwyczaj nie rozmnażają się samodzielnie przy użyciu technologii - zamiast tego polegają na wysiłku (a dokładniej na błędach) ludzi.

Oprogramowanie ransomware

Ransomware to złośliwe oprogramowanie, które żąda zapłacenia okupu przestępcy w zamian za to, że zainfekowana strona nie odniesie żadnej szkody. Ransomware często szyfruje pliki użytkownika i grozi usunięciem klucza szyfrowania, jeśli okup nie zostanie zapłacony w stosunkowo krótkim czasie, ale inne formy oprogramowania ransomware obejmują przestępcę kradnącego dane użytkownika i grożącego opublikowaniem ich online, jeśli okup nie zostanie zapłacony. Niektóre oprogramowanie ransomware w rzeczywistości kradnie pliki z komputerów użytkowników, a nie po prostu szyfruje dane, aby upewnić się, że użytkownik nie ma możliwości odzyskania swoich danych (na przykład za pomocą narzędzia chroniącego przed oprogramowaniem ransomware) bez płacenia okupu. Ransomware jest najczęściej dostarczane ofiarom jako trojan lub wirus, ale z powodzeniem jest również rozprzestrzeniane przez przestępców, którzy umieścili je w robaku. W ostatnich latach wyrafinowani przestępcy stworzyli nawet ukierunkowane kampanie ransomware, które wykorzystują wiedzę o tym, jakie dane są najcenniejsze dla określonego celu i ile ten cel może zapłacić okup. Rysunek poniżej przedstawia ekran żądania okupu w WannaCry - odmianę oprogramowania ransomware, które wyrządziło szkody w wysokości co najmniej setek milionów dolarów (jeśli nie miliardów) po początkowym rozpowszechnieniu w maju 2017 r. Wielu ekspertów ds. Bezpieczeństwa uważa, że rząd Korei Północnej lub inni pracujący dla niego stworzyli WannaCry, który w ciągu czterech dni zainfekował setki tysięcy komputerów w około 150 krajach.

Scareware

Scareware to złośliwe oprogramowanie, które starszy ludzi i zmusza do podjęcia pewnych działań. Jednym z typowych przykładów jest złośliwe oprogramowanie, które zmusza ludzi do kupowania oprogramowania zabezpieczającego. Na urządzeniu pojawia się komunikat, że urządzenie jest zainfekowane wirusem, który może usunąć tylko określony pakiet zabezpieczeń, wraz z łączem umożliwiającym zakup tego „oprogramowania zabezpieczającego”.

Programy szpiegujące

Oprogramowanie szpiegowskie to oprogramowanie, które potajemnie i bez pozwolenia zbiera informacje z urządzenia. Oprogramowanie szpiegujące może przechwytywać naciśnięcia klawiszy użytkownika (w takim przypadku nazywa się to keyloggerem), wideo z kamery wideo, dźwięk z mikrofonu, obrazy ekranu i tak dalej. Ważne jest, aby zrozumieć różnicę między oprogramowaniem szpiegującym a oprogramowaniem inwazyjnym. Niektóre technologie, które mogą zostać uznane za oprogramowanie szpiegowskie, jeśli użytkownikom nie powiedziano, że są śledzeni w Internecie, są używane przez legalne firmy; mogą być inwazyjne, ale nie są złośliwym oprogramowaniem. Te rodzaje oprogramowania niebędącego oprogramowaniem szpiegującym, które również szpiegują, obejmują sygnały nawigacyjne, które sprawdzają, czy użytkownik załadował określoną stronę internetową, oraz śledzące pliki cookie zainstalowane przez witryny internetowe lub aplikacje. Niektórzy eksperci argumentują, że każde oprogramowanie, które śledzi lokalizację smartfona, gdy aplikacja nie jest aktywnie używana przez użytkownika urządzenia, również zalicza się do kategorii oprogramowania niebędącego oprogramowaniem szpiegującym, które również szpieguje - jest to definicja obejmująca popularne aplikacje, takie jak Uber.

Górnicy kryptowaluty

Kopacze kryptowaluty to złośliwe oprogramowanie, które bez zgody właścicieli urządzeń przejmowało kontrolę nad mózgiem urządzeń (cyklami procesora) w celu wygenerowania nowych jednostek określonej kryptowaluty (którą złośliwe oprogramowanie przekazuje przestępcom obsługującym szkodliwe oprogramowanie), rozwiązując złożone problemy matematyczne, które wymagają znacznej mocy obliczeniowej do rozwiązania. Rozprzestrzenianie się kopaczy kryptowalut eksplodowało w 2017 roku wraz ze wzrostem wartości kryptowalut. Nawet po późniejszym spadku cen górnicy są nadal wszechobecni, ponieważ gdy przestępcy zainwestują w ich tworzenie, ich dalsze wdrażanie jest niewielkie. Nic dziwnego, że gdy ceny kryptowalut zaczęły ponownie rosnąć w 2019 roku, zaczęły pojawiać się również nowe odmiany kryptowalut - niektóre z nich są skierowane specjalnie do smartfonów z Androidem. Wielu cyberprzestępców z niższej półki preferuje używanie kryptowalut. Nawet jeśli każdy górnik samodzielnie płaci napastnikowi bardzo niewiele, górników można łatwo zdobyć i bezpośrednio zarabiać na cyberatakach bez konieczności wykonywania dodatkowych czynności (takich jak pobieranie okupu) lub konieczności stosowania zaawansowanych systemów dowodzenia i kontroli.

Oprogramowanie reklamowe

Adware to oprogramowanie, które generuje przychody dla strony obsługującej, wyświetlając reklamy online na urządzeniu. Oprogramowanie reklamowe może być złośliwym oprogramowaniem - to znaczy instalowane i uruchamiane bez zgody właściciela urządzenia - lub może być legalnym składnikiem oprogramowania (na przykład instalowanym świadomie przez użytkowników jako część bezpłatnego pakietu z reklamami). Niektórzy specjaliści ds. bezpieczeństwa określają to pierwsze jako oprogramowanie adware, a drugie jako oprogramowanie reklamowe. Ponieważ nie ma konsensusu, najlepiej wyjaśnić, o którym z nich mowa, gdy ktoś wspomina tylko o ogólnym terminie adware.

Mieszane złośliwe oprogramowanie

Mieszane złośliwe oprogramowanie to złośliwe oprogramowanie, które w ramach ataku wykorzystuje wiele typów technologii złośliwego oprogramowania - na przykład łącząc funkcje Trojana robaka i wirusa. Mieszane złośliwe oprogramowanie może być dość wyrafinowane i często pochodzi od wykwalifikowanych napastników.

Złośliwe oprogramowanie typu zero day

Złośliwe oprogramowanie typu „zero day” to każde złośliwe oprogramowanie, które wykorzystuje lukę, która nie była wcześniej znana opinii publicznej ani dostawcy technologii zawierającej tę lukę, i jako taka jest często niezwykle silna. Regularne tworzenie złośliwego oprogramowania typu „zero day” wymaga znacznych zasobów i rozwoju. Jest dość drogi i często jest tworzony przez cyberarmie państw narodowych, a nie przez innych hakerów. Komercyjni dostawcy złośliwego oprogramowania typu „zero day” pobierają ponad 1 milion dolarów za jeden exploit.

Zatrute ataki usług sieciowych

Wiele różnych typów ataków wykorzystuje luki w zabezpieczeniach serwerów, a nowe słabości są stale odkrywane, dlatego specjaliści ds. cyberbezpieczeństwa mają pracę na pełny etat, zapewniając bezpieczeństwo serwerów. Na taki temat, który oczywiście wykracza poza zakres tej pracy, można napisać całe książki - a nawet kilka serii książek. To powiedziawszy, ważne jest, abyś zrozumiał podstawowe pojęcia dotyczące ataków serwerowych, ponieważ niektóre takie ataki mogą mieć bezpośredni wpływ na Ciebie. Jedną z takich form ataku jest zatruty atak na usługę internetową lub zatruty atak na stronę internetową. W tego rodzaju ataku osoba atakująca włamuje się do serwera

WWW i wstawia na nim kod, który powoduje, że atakuje użytkowników, gdy uzyskują dostęp do strony lub zestawu stron, które serwer obsługuje. Na przykład haker może przejąć kontrolę nad serwerem WWW obsługującym www.abc123.com i zmodyfikować stronę główną udostępnianą użytkownikom uzyskującym dostęp do witryny, tak aby zawierała złośliwe oprogramowanie.

Jednak haker nie musi nawet koniecznie naruszać systemu, aby zatruwać strony internetowe! Jeśli witryna, która umożliwia użytkownikom komentowanie postów, nie jest odpowiednio zabezpieczona, na przykład, może pozwolić użytkownikowi na dodanie tekstu różnych poleceń w komentarzu - poleceń, które, jeśli są odpowiednio spreparowane, mogą być wykonywane przez przeglądarki użytkowników. podczas wczytywania strony, na której jest wyświetlany komentarz. Przestępca może wstawić polecenie uruchomienia skryptu w witrynie internetowej przestępcy, który może otrzymać dane uwierzytelniające użytkownika w oryginalnej witrynie, ponieważ jest wywoływany w kontekście jednej ze stron internetowych tej witryny. Taki atak jest znany jako cross-site scripting i nadal stanowi problem nawet po ponad dziesięciu latach jego rozwiązywania.

Zatrucie infrastruktury sieciowej

Podobnie jak w przypadku serwerów internetowych, wiele różnych typów ataków wykorzystuje luki w infrastrukturze sieciowej, a nowe słabości są stale odkrywane. Zdecydowana większość tego tematu wykracza poza zakres naszej nauki. To powiedziawszy, podobnie jak w przypadku zatrutych serwerów internetowych, musisz zrozumieć podstawowe pojęcia związane z atakami serwerowymi, ponieważ niektóre takie ataki mogą mieć bezpośredni wpływ na Ciebie. Na przykład przestępcy mogą wykorzystać różne słabości, aby dodać uszkodzone dane systemu nazw domen (DNS) na serwer DNS. DNS to katalog w Internecie, który tłumaczy adresy czytelne dla człowieka na ich numeryczne odpowiedniki, które mogą być używane przez komputer (adresy IP). Na przykład, jeśli wpiszesz https://JosephSteinberg.com w przeglądarce internetowej, DNS przekieruje Twoje połączenie na adres 104.18.45.53.

Wstawiając niepoprawne informacje do tabel DNS, przestępca może spowodować, że serwer DNS zwróci niepoprawny adres IP do komputera użytkownika. Taki atak może z łatwością spowodować przekierowanie ruchu użytkownika do komputera wybranego przez atakującego zamiast do zamierzonego przez niego miejsca docelowego. Jeśli na przykład przestępca utworzy fałszywą witrynę banku na serwerze, do którego kierowany jest ruch, i podszywa się na tym serwerze pod bank, do którego użytkownik próbował się dostać, nawet użytkownik, który wprowadzi adres URL banku do swojej przeglądarki (w przeciwieństwie do zwykłego kliknięcia linku) może paść ofiarą po przekierowaniu na fałszywą stronę. (Ten typ ataku jest znany jako zatruwanie DNS lub pharming). Ataki na infrastrukturę sieciową mogą przybierać różne formy. Niektórzy próbują kierować ludzi do niewłaściwych miejsc. Inni starają się przechwytywać dane, podczas gdy inni dążą do wprowadzenia warunków odmowy usługi. Najważniejsze, aby zrozumieć, że instalacja w Internecie jest dość złożona i nie zostało początkowo zaprojektowane z myślą o bezpieczeństwie, i jest podatne na wiele form nadużyć.

Malvertising

Malvertising to skrót od słów złośliwej reklamy i odnosi się do wykorzystywania reklam internetowych jako narzędzia do rozprzestrzeniania złośliwego oprogramowania lub przeprowadzania innych form cyberataku. Ponieważ wiele witryn wyświetla reklamy, które są obsługiwane i zarządzane przez sieci stron trzecich i które zawierają linki do różnych innych stron trzecich, reklamy online są doskonałym narzędziem dla atakujących. Nawet firmy, które odpowiednio zabezpieczają swoje witryny internetowe, mogą nie podejmować odpowiednich środków ostrożności, aby zapewnić, że nie będą one dostarczać problematycznych reklam tworzonych przez kogoś innego i przez niego zarządzanych.

W związku z tym złośliwa reklama czasami pozwala przestępcom na umieszczanie swoich treści w renomowanych i znanych witrynach z dużą liczbą odwiedzających (coś, co byłoby trudne do osiągnięcia dla oszustów w innym przypadku), z których wielu może dbać o bezpieczeństwo i które nie zostałyby ujawnione do treści przestępcy, gdyby została opublikowana w mniej renomowanej witrynie. Ponadto, ponieważ witryny internetowe często zarabiają pieniądze dla swoich właścicieli na podstawie liczby osób, które klikają różne reklamy, właściciele witryn zazwyczaj umieszczają reklamy w swoich witrynach w sposób, który przyciągnie użytkowników do reklam. W związku z tym złośliwe reklamy pozwalają przestępcom dotrzeć do dużej liczby odbiorców za pośrednictwem zaufanej witryny bez konieczności hakowania czegokolwiek. Niektóre złośliwe reklamy wymagają od użytkowników klikania reklam w celu zarażenia się złośliwym oprogramowaniem; inne nie wymagają udziału użytkownika - urządzenia użytkowników są infekowane w momencie wyświetlenia reklamy.

Pobieralne pliki do pobrania

Drive-by download to swego rodzaju eufemizm odnoszący się do oprogramowania, które użytkownik pobiera bez zrozumienia tego, co robi. Pobieranie automatyczne może wystąpić na przykład wtedy, gdy użytkownik pobierze złośliwe oprogramowanie, przechodząc do zatrutej witryny, która automatycznie wysyła je na urządzenie użytkownika, gdy ten otwiera witrynę. Pobrania typu „drive-by" obejmują również przypadki, w których użytkownik wie, że pobiera oprogramowanie, ale nie jest świadomy pełnych konsekwencji takiego działania. Na przykład, jeśli użytkownikowi zostanie wyświetlona strona internetowa z informacją, że na jego komputerze występuje luka w zabezpieczeniach i która nakazuje mu kliknięcie przycisku Pobierz, aby zainstalować poprawkę zabezpieczeń, użytkownik udzielił autoryzacji na (złośliwe) pobieranie - ale tylko dlatego, że został oszukany i uwierzył, że natura pobierania była znacznie inna niż w rzeczywistości.

Kradzież haseł

Przestępcy mogą kraść hasła na wiele różnych sposobów. Dwie metody obejmują:

* Kradzieże baz danych haseł: jeśli przestępca wykradnie bazę haseł ze sklepu internetowego, każdy, kogo hasło pojawia się w bazie danych, jest narażony na ryzyko złamania hasła. (Jeśli sklep prawidłowo zaszyfrował swoje hasła, może minąć trochę czasu, zanim przestępca wykona tak zwany atak mieszający, ale mimo to hasła - zwłaszcza te, które prawdopodobnie zostaną przetestowane na wczesnym etapie - mogą nadal być zagrożone. Do chwili obecnej kradzież haseł jest najczęstszym sposobem podważania haseł.

* Ataki socjotechniczne: Ataki socjotechniczne to ataki, w których przestępca nakłania kogoś do zrobienia czegoś, czego by nie zrobił, gdyby zdał sobie sprawę, że osoba składająca żądanie w jakiś sposób go oszukuje. Jednym z przykładów kradzieży hasła za pomocą inżynierii społecznej jest sytuacja, w której przestępca udaje członka działu pomocy technicznej pracodawcy swojego celu i mówi jego celowi, że musi zresetować określone hasło do określonej wartości, aby powiązane konto zostało przetestowane jako jest potrzebny po odzyskaniu sił po jakimś naruszeniu, a cel jest posłuszny.

* Ataki uwierzytelniające: Ataki uwierzytelniające to ataki mające na celu uzyskanie dostępu do systemu poprzez wprowadzenie bez autoryzacji prawidłowej kombinacji nazwy użytkownika i hasła (lub innych potrzebnych informacji uwierzytelniających). Te ataki dzielą się na cztery główne kategorie:

-Brute force: Przestępcy używają zautomatyzowanych narzędzi, które próbują wszystkich możliwych haseł, aż trafią na właściwe.

- Ataki słownikowe: Przestępcy używają zautomatyzowanych narzędzi do przekazywania każdego słowa ze słownika do witryny, aż trafią na właściwe.

-Obliczone ataki: przestępcy wykorzystują informacje o celu, aby odgadnąć jego hasło. Przestępcy mogą na przykład wypróbować nazwisko panieńskie matki, ponieważ łatwo mogą je zdobyć dla wielu osób, przeglądając najczęstsze nazwiska swoich znajomych na Facebooku lub z postów w mediach społecznościowych.

- Ataki mieszane: Niektóre ataki wykorzystują kombinację powyższych technik - na przykład wykorzystując listę popularnych nazwisk lub wykorzystując technologię ataku brute force, która znacznie poprawia jej skuteczność poprzez wykorzystanie wiedzy o tym, jak użytkownicy często tworzą hasła.

* Złośliwe oprogramowanie: jeśli oszustom uda się dostać złośliwe oprogramowanie na czyjeś urządzenie, może przechwycić hasła.

* Wąchanie sieci: jeśli ktoś prześle swoje hasło do witryny bez odpowiedniego szyfrowania podczas korzystania z publicznej sieci Wi-Fi, przestępca korzystający z tej samej sieci może zobaczyć to hasło podczas przesyłania - podobnie jak inni przestępcy podłączeni do sieci wzdłuż ścieżki od użytkownika do danej witryny.

* Wypychanie poświadczeń: w przypadku wypychania danych logowania ktoś próbuje zalogować się do jednej witryny przy użyciu nazw użytkowników i kombinacji haseł skradzionych z innej witryny.

Możesz skorzystać z haseł i strategii haseł, które mogą pomóc pokonać wszystkie te techniki

Wykorzystywanie trudności w utrzymaniu

Utrzymanie systemów komputerowych nie jest sprawą trywialną. Dostawcy oprogramowania często wydają aktualizacje, z których wiele może mieć wpływ na inne programy uruchomione na komputerze. Jednak niektóre łatki są absolutnie niezbędne do zainstalowania na czas, ponieważ naprawiają błędy w oprogramowaniu - błędy, które mogą wprowadzać możliwe do wykorzystania luki w zabezpieczeniach. Konflikt między bezpieczeństwem a przestrzeganiem odpowiednich procedur konserwacyjnych to niekończąca się walka - a bezpieczeństwo rzadko wygrywa. W rezultacie zdecydowana większość komputerów nie jest aktualizowana. Nawet osoby, które włączają automatyczne aktualizacje na swoich urządzeniach, mogą nie być aktualne - zarówno dlatego, że aktualizacje są sprawdzane okresowo, a nie co sekundę każdego dnia, a także dlatego, że nie wszystkie programy oferują automatyczne aktualizacje. Co więcej, czasami aktualizacje jednego oprogramowania wprowadzają luki w innym oprogramowaniu działającym na tym samym urządzeniu.

Zaawansowane ataki

Jeśli posłuchasz wiadomości podczas doniesień o dużej cyberprzestrzeni, często usłyszysz komentatorów odnoszących się do zaawansowanych ataków. Podczas gdy niektóre cyberataki są wyraźnie bardziej złożone niż inne i wymagają większej sprawności technicznej do przeprowadzenia, nie istnieje żadna konkretna, obiektywna definicja zaawansowanego ataku. To powiedziawszy, z subiektywnego punktu widzenia, można rozważyć każdy atak, który wymaga znacznych inwestycji w badania i rozwój, aby został pomyślnie przeprowadzony, za zaawansowany. Oczywiście definicja znacznej inwestycji jest również subiektywna. W niektórych przypadkach wydatki na badania i rozwój są tak wysokie, a ataki są tak wyrafinowane, że istnieje niemal powszechna zgoda co do tego, że atak został przyspieszony. Niektórzy eksperci uważają, że każdy atak typu zero-day jest zaawansowany, ale inni się z tym nie zgadzają. Zaawansowane ataki mogą być oportunistyczne, ukierunkowane lub stanowić kombinację obu. Ataki oportunistyczne to ataki wymierzone w jak największą liczbę celów, aby znaleźć te, które są podatne na rozpoczęty atak. Atakujący nie ma listy predefiniowanych celów - jego cele to w rzeczywistości wszystkie osiągalne systemy, które są podatne na atak, który uruchamia.

Te ataki są podobne do strzelania z ogromnej strzelby w obszarze z wieloma celami z nadzieją, że jeden lub więcej pocisków trafi w cel, który może przebić. Ataki ukierunkowane to ataki skierowane na konkretną stronę i zazwyczaj polegają na zastosowaniu szeregu technik ataku, aż w końcu uda się przeniknąć do celu. Dodatkowe ataki mogą zostać uruchomione później, aby poruszać się po systemach celu.

Ataki oportunistyczne

Celem większości ataków oportunistycznych jest zwykle zarabianie pieniędzy - dlatego atakujących nie obchodzi, czyje systemy naruszają; pieniądze są takie same, niezależnie od tego, czyje systemy zostały naruszone, aby to zrobić. Ponadto w wielu przypadkach oportunistyczni napastnicy mogą nie przejmować się ukrywaniem faktu, że doszło do naruszenia - zwłaszcza po tym, jak zdążyli zarabiać na naruszeniu, na przykład sprzedając listy haseł lub numery kart kredytowych, które ukradli. Chociaż nie wszystkie ataki oportunistyczne są zaawansowane, niektóre z pewnością są. Ataki oportunistyczne różnią się znacznie od ataków ukierunkowanych.

Ataki ukierunkowane

Jeśli chodzi o ataki ukierunkowane, udane włamanie do systemów spoza listy celów nie jest uważane za nawet niewielki sukces. Na przykład, jeśli rosyjski agent zostanie przydzielony do misji włamania się do systemów pocztowych partii demokratycznej i republikańskiej i kradzieży kopii wszystkich wiadomości e-mail na serwerach pocztowych stron, jego misja zostanie uznana za sukces tylko wtedy, gdy osiąga dokładnie te cele. Jeśli uda mu się ukraść milion dolarów z banku internetowego przy użyciu tych samych technik hakerskich, które kieruje na swoje cele, nie zmieni to niepowodzenia w złamanie zamierzonych celów w nawet niewielki sukces. Podobnie, jeśli celem atakującego przeprowadzającego atak ukierunkowany jest zniszczenie witryny internetowej byłego pracodawcy, który go zwolnił, usunięcie innych witryn nie przyniesie żadnego efektu w umyśle atakującego. Ponieważ tacy napastnicy muszą naruszać swoje cele bez względu na to, jak dobrze chronione są te strony, ataki ukierunkowane często wykorzystują zaawansowane metody ataków - na przykład wykorzystując luki w zabezpieczeniach nieznane publicznie lub producentom, którzy musieliby je naprawić. Jak można się domyślić, zaawansowane ataki ukierunkowane są zwykle przeprowadzane przez strony o znacznie większej sprawności technicznej niż te, które przeprowadzają ataki oportunistyczne. Często, ale nie zawsze, celem ataków ukierunkowanych jest niewykryta kradzież danych lub wyrządzenie poważnych szkód, a nie zarobienie pieniędzy. W końcu, jeśli celem jest zarabianie pieniędzy, po co wydawać zasoby na dobrze chronioną witrynę? Przyjmij oportunistyczne podejście i przejrzyj najsłabiej chronione, trafne witryny. Niektóre zaawansowane zagrożenia wykorzystywane w atakach ukierunkowanych są określane jako zaawansowane trwałe zagrożenia (APT):

* Zaawansowane: wykorzystuje zaawansowane techniki hakerskie, prawdopodobnie z dużym budżetem na B + R

* Trwały: ciągle próbuje różnych technik, aby złamać system celu i nie przejdzie do kierowania na inny system tylko dlatego, że początkowy cel jest dobrze chroniony

* Zagrożenie: może spowodować poważne szkody

Ataki mieszane (oportunistyczne i ukierunkowane)

Innym rodzajem ataku zaawansowanego jest atak oportunistyczny, częściowo ukierunkowany. Jeśli na przykład przestępca chce ukraść numery kart kredytowych, może nie dbać o to, czy uda mu się ukraść równoważną liczbę aktywnych numerów z Best Buy, Walmart lub Barnes & Noble. Najprawdopodobniej wszystko, na czym mu zależy, to uzyskanie numerów kart kredytowych - nie ma

znaczenia, od kogo są kradzione. Jednocześnie przeprowadzanie ataków na witryny, które nie mają danych kart kredytowych, jest stratą czasu i zasobów atakującego