ATAKI DENIAL-OF-SERVICE
WPROWADZENIE.

W tej części omówiono ataki typu „odmowa usługi" (DoS) i rozproszona odmowa usługi (DDoS). Ataki te mają na celu uczynienie docelowych systemów i sieci bezużytecznymi lub niedostępnymi przez nasycenie zasobów lub powodowanie katastrofalnych błędów, które zatrzymują procesy lub całe systemy. Co więcej, są one coraz łatwiejsze nawet dla script kiddies (osób, które wykonują wyraźne instrukcje ataku lub wykonują programy ataku). Skuteczne zapobieganie atakom i obrona przed tymi atakami nastąpi tylko wtedy, gdy istnieje szeroka współpraca między wszystkimi dostawcami usług internetowych (ISP) i innymi systemami podłączonymi do Internetu na całym świecie oraz gdy oprogramowanie antymalware jest powszechnie instalowane i aktualizowane w systemach użytkowników. Działając na różne sposoby, atakujący DoS wybiera zamierzony system docelowy i przeprowadza przeciwko nim skoncentrowany atak. Chociaż początkowo uważane są za przede wszystkim uciążliwe, ataki DoS mogą obezwładnić całą sieć, szczególnie te z hostami, które polegają na protokole kontroli transmisji / protokole internetowym (TCP / IP). Ataki DoS na sieci korporacyjne i dostawców usług internetowych spowodowały znaczne szkody w wydajności i przychodach. Ataki DoS można uruchamiać na dowolnej platformie sprzętowej lub systemowej, ponieważ ich celem jest zasadniczo implementacja protokołu internetowego (IP). Ponieważ IP jest typowym celem, narzędzia ataku DoS działające pod jednym systemem operacyjnym (Linux jest powszechnym wyborem) mogą być skierowane na dowolny system operacyjny z IP. Ponadto, ponieważ implementacje IP są podobne dla różnych platform, jeden atak DoS może być ukierunkowany na kilka systemów operacyjnych i działać na każdym z nich. Po napisaniu dla jednej platformy i wydaniu, nowe ataki DoS ewoluują (poprzez badanie i udział hakerów i crackerów), aby w krótkim czasie (około dwóch tygodni) pojawiły się mutacje ataku DoS, które działają na praktycznie wszystkich platformach. Ze względu na krytyczny wpływ ataków DoS nie można ich lekceważyć. Ukierunkowane ataki DoS istnieją w tej czy innej formie od lat 80. XX wieku; w 1999 r. przekształciły się one w ataki DDoS, głównie ze względu na intensywne korzystanie z sieci wewnętrznych i Internetu. Narzędzia DDoS uruchamiają skoordynowane ataki DoS z wielu źródeł jednocześnie na jeden lub więcej celów. Najpierw opiszemy ataki DoS, a następnie DDoS, ponieważ ataki DoS historycznie poprzedzały ataki DDoS. Ponadto niektóre ataki DDoS wykorzystują techniki DoS. Jednak same ataki, terminologia i mechanizmy obronne są na tyle różne, że wymagają osobnej dyskusji.

HISTORIA ATAKÓW DENIAL-OF-SERVICE

Historycznie każdy akt, który uniemożliwiał korzystanie z systemu, można nazwać odmową usługi. Na przykład w niektórych systemach mainframe i minikomputerach wpisanie źle sformułowanego polecenia może spowodować awarię systemu; na przykład na minikomputerze HP3000 około 1982 r. użycie błędnego parametru TERMTYPE w ciągu logowania spowodowało natychmiastową awarię systemu. W HP3000 wpisanie jednego lub więcej znaków w konsoli systemowej bez naciskania klawisza RETURN zablokowałoby wszystkie dalsze komunikaty systemowe w konsoli, powodując zapełnienie buforów systemowych komunikatami nie wyświetlanymi; gdy bufory systemowe (domyślnie 16) są pełne, nie może mieć miejsca żadna akcja systemowa wymagająca powiadomienia do konsoli (np. logowanie, wylogowywanie, żądania w formularzu specjalnym lub żądanie podłączenia do taśmy). Klasyczny DoS bez oprogramowania może wynikać z tego, że odkurzacz odłączy przewód zasilający od gniazdka ściennego, nie zdając sobie sprawy, że przewód zasila jedną lub więcej stacji roboczych. Skonfigurowanie trwałej blokady użytkowników po pewnej liczbie prób złego hasła (zamiast blokady czasowej) doprowadziło do DoS; złośliwi użytkownicy mogą nawet próbować zablokować rootowanie użytkowników poprzez celowe wprowadzanie złych haseł do ich kont. Jednak takie zdarzenia były zwykle wynikiem błędów w systemie operacyjnym, niewystarczającej liczby zasobów systemowych, złego zarządzania systemem lub wypadku. Jeden z pierwszych poważnych incydentów DoS, który spowodował, że nagłówki i zmarszczki były prawdopodobnie przypadkowe. Miało to miejsce w grudniu 1987 r., kiedy pracownik IBM w Europie wysłał świąteczną wiadomość e-mail z pozdrowieniami. Wiadomość e-mail zawierała jednak program, który narysował ładną choinkę na terminalu odbiorcy i

odczytał pliki NAMES i NETLOG odbiorcy zawierające książkę adresową użytkownika, a także adresy e-mail osób, do których ten użytkownik niedawno wysłał pocztę lub otrzymano pocztę od. Program Choinka uruchomił następnie automatyczną transmisję swoich kopii na wszystkie adresy e-mail znalezione w NAMES i NETLOG - i nie zapobiegł ponownemu przesyłaniu do systemów, które już otrzymały lub wysłały powitanie. Powstała burza pocztowa przeciążyła sieć korporacyjną IBM na całym świecie i spowodowała awarię zarówno w Europie, jak i Stanach Zjednoczonych. Ponadto wiadomości uciekały z korporacyjnej sieci IBM i siały spustoszenie w sieciach edukacyjnych i badawczych BITNET / EARN w Ameryce Północnej i Europie. Chociaż pierwotnie uważano, że przyczyną awarii jest wirus komputerowy, a incydent nazwano wirusem, robakiem i dowcipem, wynik był prawdziwą odmową usługi. Być może najsłynniejszy internetowy program DoS powstał z robaka MorrisWorm, zwanego również robakiem internetowym, który został wydany w listopadzie 1988 r. Robert Cornet, absolwent Cornell, napisał artykuł o lukach w systemie Sendmail i opisał finger w systemach UNIX w poprzednim roku . Większość społeczności TCP / IP odrzuciła luki w zabezpieczeniach jako teoretyczne; najwyraźniej Morris chciał wykazać, że luki można faktycznie wykorzystać. Aby zademonstrować problem, jego program musiał zaatakować inny system, odgadnąć niektóre hasła, a następnie zreplikować się. Morris powiedział po incydencie, że chciał, aby program replikował się tylko kilka razy, aby wykazać, że jest on prawdziwy, i dołączył kod zapobiegający szybkiemu rozprzestrzenianiu się; niestety błąd programowy spowodował, że robak replikował się często i szybko, oprócz superinfekcji już zainfekowanych systemów. Robak zatkał Internet setkami tysięcy wiadomości i skutecznie spowodował awarię całej sieci; większość witryn, które nie uległy awarii, zostały odłączone od sieci przez administratorów systemu, aby uniknąć infekcji i umożliwić dezynfekcję. Niezależnie od intencji robak Morris nieumyślnie spowodował DoS. Ponieważ administratorzy witryn nie mieli możliwości komunikowania się z innymi administratorami, a ponieważ rozwiązania, które sam Morris opublikował, nie mogły być zaufane, dużo czasu poświęcono na wyeliminowanie robaka. Jednym z rezultatów było utworzenie Centrum Koordynacji Zespołu Reagowania Komputerowego, obecnie CERT / CC, na Carnegie Mellon University. W piątek, 6 września 1996 r., PANIX, dostawca publicznego dostępu do Internetu na Manhattanie, został dotknięty atakiem DoS, który składał się z wielu wiadomości zalewających serwer ogromną ilością danych. Ataki zostały przeprowadzone na serwery poczty, wiadomości, nazwy i sieci, a także na konta użytkowników powłoki. Atakującym udało się uniknąć wyśledzenia, a ataki trwały kilka dni. Mniej więcej tydzień po rozpoczęciu ataków PANIX opublikował tę historię, a dziesiątki innych dostawców usług internetowych przyznało, że oni także byli ofiarami podobnych ataków. W 1997 r. niezadowolony były pracownik Forbes, Inc. użył hasła byłego kolegi do zdalnego dostępu do systemów komputerowych firmy. Celowo majstrując przy systemie, usunął budżety i informacje o wynagrodzeniach i spowodował awarię pięciu z ośmiu serwerów sieciowych. Kiedy agenci Federalnego Biura Śledczego (FBI) złapali sprawcę, jego dom był wypełniony narzędziami hakerskimi, zastrzeżonymi informacjami z Forbes, Inc. i innymi materiałami obciążającymi. W lutym 1998 r. Hakerzy z Izraela i Północnej Kalifornii zaatakowali Departament Obrony USA (DoD). W starannie zorganizowanym ataku wykorzystującym przepełnienie bufora hakerzy systematycznie przeprowadzali atak DoS, który trwał ponad tydzień na 11 stronach DoD. W marcu 1998 r. W całych Stanach Zjednoczonych administratorzy systemów znaleźli serwery Windows NT pod pozornie zautomatyzowanym atakiem. Systemy ulegały wielokrotnym awariom, dopóki nie zostały zaktualizowane do najnowszych poprawek firmy Microsoft. Wydawało się, że ataki, które trwały dłużej niż jeden dzień, nie spowodowały uszkodzenia pliku. Dotknięte strony obejmowały NASA i inne obiekty wojskowe, a także kilka University of California i innych kampusów uniwersyteckich. Kolejna burza pocztowa wybuchła w maju 1998 r., kiedy australijski urzędnik ustawił automatyczną odpowiedź na swój pakiet e-mail, gdy go nie było. Niestety, niechcący ustawił miejsce docelowe dla tych w większości bezużytecznych wiadomości na 2000 użytkowników w swojej sieci - i poprosił o automatyczne potwierdzenie dostarczenia każdej automatycznej odpowiedzi, która wygenerowała kolejną automatyczną odpowiedź, i tak dalej w nieskończoność. W ciągu czterech godzin jego niekończąca się pętla pozytywnego sprzężenia zwrotnego wygenerowała 150 000 wiadomości, zanim jego automatyczna odpowiedź została wyłączona. Fale trwały kilka dni, a sprawca obarczony był 48 000 wiadomościami w swoim koszyku IN i napływał strumień 1500 dziennie. Był to kolejny przypadek

nieumyślnego ataku DoS. W styczniu 1999 r. Ktoś przeprowadził trwały atak DoS na Ozemail. Usługa e-mail została zakłócona dla użytkowników w Sydney. W marcu 1999 r. Wirus / robak Melissa z obsługą poczty elektronicznej przeniósł świat w ciągu kilku dni, wysyłając swoje kopie pod pierwsze 50 adresów w książkach adresowych e-mail ofiar. Z powodu tego wysokiego wskaźnika replikacji wirus rozprzestrzenia się szybciej niż jakikolwiek poprzedni wirus w historii. W wielu systemach korporacyjnych szybki współczynnik nasyconych wewnętrznych replikacji serwerów e-mail z wychodzącymi automatycznymi wiadomościami-śmieciami. Początkowe szacunki były w zakresie 100 000 systemów zestrzelonych. Firmy antywirusowe zebrały się natychmiast, a aktualizacje wszystkich standardowych produktów były dostępne w ciągu kilku godzin od pierwszych powiadomień z CERT / CC. Wirus makr Melissa został szybko wyśledzony przez wirusa makr PAPA MS-Excel o podobnych właściwościach, który dodatkowo rozpoczął ataki DoS na dwa określone adresy IP. I po tym, jak cała reklama dotycząca problemów Y2K przed przełomem tysiącleci, robak ILOVEYOU, został wydany w maju 2000 r. Robak był załącznikiem Visual BASIC do wiadomości e-mail o temacie „ ILOVEYOU. ”Ten robak wykorzystał tak zwany exploit podwójnego rozszerzenia; załącznik został nazwany LOVE-LETTER-FOR-YOU.txt.vbs, ale ponieważ jest to ustawienie defaultWindows nie wyświetla rozszerzenia, wielu (lub większość) odbiorców sądziło, że jest to nieszkodliwy plik tekstowy. Robak zmodyfikował rejestr zainfekowanego systemu, aby automatycznie uruchamiał program podczas uruchamiania systemu, zastąpił pliki pewnymi rozszerzeniami kopiami samego siebie i wysłał swoje kopie do pierwszych 50 wpisów w książce adresowej programu Outlook.

KOSZTY ATAKÓW DENIAL-OF-SERVICE.

Jakie są skutki tych ataków DoS pod względem wydajności i rzeczywistych kosztów finansowych? Trudno jest podać dokładną wartość pieniężną skutków atakiów DoS. Ataki DoS mogą zakłócać krytyczne procesy w organizacji, a takie zakłócenia mogą być kosztowne. Gdy sieć komputerowa firmy jest niedostępna dla legalnych użytkowników i nie mogą oni prowadzić swojej normalnej działalności, wydajność spada. Negatywny efekt z pewnością przeniesie się na finansowe aspekty działalności. Jednak dokładne określenie tych efektów jest co najwyżej niepewne, a szacunki są szeroko kwestionowane, nawet wśród ekspertów ds. bezpieczeństwa i biznesu. Ponadto wiele firm nie komentuje dokładnych strat, jakie ponoszą, ponieważ obawiają się, że negatywny rozgłos zmniejszy ich udział w rynku. Ta ostatnia kwestia jest znacząca: we wczesnych latach 90. XX w. Badanie firm z Wall Street, niektóre firmy zasugerowały, że gdyby były bez sieci przez dwa do trzech dni, nigdy nie otworzyłyby swoich drzwi. W przypadku robaka choinkowego IBM zajęło kilka dni na oczyszczenie sieci i spowodowało utratę milionów dolarów, zarówno na czyszczenie systemu, jak i na utratę działalności z powodu utraty łączności i związanej z tym wydajności. Dodatkowo doszło do zażenowania ze strony znanej firmy technologicznej IBM. Osoba, która uruchomiła robaka, została zidentyfikowana i odmówiono jej dostępu do dowolnego konta komputerowego, podczas gdy IBM musiał napisać list z przeprosinami do administratorów Europejskiej Sieci Naukowej i Badawczej (EARN). W 1988 r., w czasie robaka Morrisa, Internet składał się z 5 000 do 10 000 hostów, głównie w instytucjach badawczych i akademickich. W rezultacie, mimo że Morris Worm udało się zatrzymać wiele witryn i zyskał na całym świecie rozgłos, wpływ finansowy i produktywności na świat komercyjny był minimalny. Podobny incydent dzisiaj spowodowałby spustoszenie i kosztowałby dziesiątki lub setki milionów dolarów strat. Jednak w 1996 r. komercyjne poleganie na Internecie stało się już popularne Oczywiście, pracując przez całą dobę, zarządzanie w PANIX i Cisco, dostawcy routerów ISP, utrzymywało dostawcę usług i działało, ale sieć otrzymywała 210 fałszywych żądań na minutę. Chociaż systemy nie uległy awarii, tysiące subskrybentów nie było w stanie odbierać wiadomości e-mail. Inne strony zostały zaatakowane w tym samym czasie co PANIX, w tym Voters Telecommunication Watch. Nikt nie wziął odpowiedzialności za te ataki i powszechnie zakładano, że zostały one wywołane przez artykuły o atakach SYN DoS , które niedawno ukazały się w 2600 Magazine i Phrack, czasopismach poświęconych hakerom. Według Forbes, Inc. straty poniesione przez firmę z powodu ataku DoS dokonanego przez niezadowolonego byłego pracownika przekroczyły 100 000 USD. Czy można temu zapobiec? Według firmy jest to bardzo mało prawdopodobne, ponieważ Forbes nie miał powodu

podejrzewać, że dana osoba trzymała w domu poufne i wrażliwe materiały firmy lub że myślał o włamaniu się do systemu komputerowego i celowym wyrządzeniu szkody. Chociaż firma miała zabezpieczenia w swoich systemach, sprawca użył hasła legalnego, autoryzowanego użytkownika. Atak DoS przeprowadzony przeciwko komputerom Departamentu Obrony w 1998 r. Udowodnił, że napastnicy mogli odmówić dostępu do ważnych informacji wojskowych. W tym konkretnym przypadku atak był skierowany przeciwko niesklasyfikowanym maszynom, które miały tylko dokumentację administracyjną i księgową, ale był to cios w zaufanie Departamentu Obrony. Związanie komputerów przez ponad tydzień prawdopodobnie zmniejszyło produktywność, ale rząd nie wypowiedziałby się na temat rzeczywistych kosztów związanych z utratą czasu pracy maszyny i produktywności personelu. Przypadki te pokazują, że atak DoS na komputer lub sieć może być katastrofalny dla organizacji. Ważne ataki powodują wyłączenie ważnego sprzętu i sieci, a nawet całej organizacji. Wczesne zdarzenia DoS często opisywano jako irytujące, frustrujące lub uciążliwe. Jednak wraz ze wzrostem wyrafinowania i zależności od sieci trudno było zachować poczucie humoru związane z takimi zdarzeniami. Zwłaszcza w korporacjach, w których misją jest generowanie zysku dla akcjonariusza, menedżerom firm coraz trudniej jest usprawiedliwić niezdolność do pracy z powodu ataku DoS lub DDoS. W miarę jak te formy ataku stają się coraz bardziej wyrafinowane, narzędzia i metody ich wykrywania i walki z nimi również muszą. Aktualne produkty skanują urządzenia i sieci w poszukiwaniu luk, uruchamiają alerty w przypadku wykrycia nieprawidłowości i często pomagają w wyeliminowaniu wykrytego problemu.

RODZAJE ATAKÓW DENIAL-OF-SERVICE.

Ataki DoS, przypadkowe lub celowe, powodują utratę usługi; system hosta lub serwera przestaje działać lub sieć staje się niedostępna. Ataki DoS są przeprowadzane celowo przez intruza (w tym kontekście termin preferowany). Zagrożone systemy i sieci nazywane są ofiarami. I chociaż ataki DoS można uruchamiać z systemu intruza, często są one uruchamiane zautomatyzowanym procesem, który umożliwia intruzowi zdalne rozpoczęcie ataku za pomocą kilku naciśnięć klawiszy. Programy te są znane jako demony i często są umieszczane w innym systemie, który haker już skompromitował. Istnieją cztery podstawowe typy lub kategorie ataku DoS:
1. Nasycenie. Ten rodzaj ataku ma na celu pozbawienie komputerów i sieci rzadkich, ograniczonych lub nieodnawialnych zasobów niezbędnych do działania komputerów lub sieci. Zasoby tego typu obejmują czas procesora, miejsce na dysku, pamięć, struktury danych, przepustowość sieci, dostęp do innych sieci i komputery i zasoby środowiskowe, takie jak chłodne powietrze i energia.
2. Błędna konfiguracja. Ten typ ataku niszczy lub zmienia informacje o konfiguracji w systemach hosta, serwerach lub routerach. Ponieważ słabe lub źle skonfigurowane komputery mogą nie działać lub działać nieprawidłowo, ten rodzaj ataku może być bardzo poważny.
3. Zniszczenie. Ten rodzaj ataku powoduje fizyczne zniszczenie lub zmianę komponentów sieci. Aby zabezpieczyć się przed tego typu atakami, konieczne jest dobre fizyczne bezpieczeństwo w celu ochrony komputerów i innych elementów sieci.
4. Zakłócenie. Ten atak przerywa komunikację między dwoma urządzeniami poprzez zmianę informacji o stanie - takich jak stan połączenia wirtualnego TCP - tak, że skuteczny transfer danych jest niemożliwy.

SZCZEGÓLNE ATAKI DENIAL-OF-SERVICE.

Poniższa dyskusja opisuje niektóre konkretne ataki DoS jako przykłady ogólnych metod, które można zastosować w DoS lub DDoS. Lista nie jest wyczerpująca.

Narzędzia niszczące.

Narzędzia niszczące to programy, które dokonują nękania lub niszczenia danych. Istnieją rozbieżne opinie na temat tego, jak poważne są narzędzia niszczące, ale jeśli zagrażają one zdolności komputera lub sieci do prawidłowego i wydajnego funkcjonowania, mogą być instrumentami ataków DoS. Wirusy,

bomby pocztowe i narzędzia DoS można uznać za narzędzia niszczące. W rzeczywistości wirusy i bomby poczty e-mail powodują ataki DoS. Niektóre wirusy lub inne złośliwe oprogramowanie są znane z ataków na systemy kontroli sprzętu, na przykład wykorzystujące ataki Stuxnet i Flame.

Bombardowani E-mail (i subskrypcja e-mail).

Zamachy na e-mail i subskrypcje e-mail były jednymi z pierwszych udokumentowanych ataków DoS. Bomba pocztowa składa się z dużej liczby wiadomości e-mail wypełniających skrzynkę elektroniczną ofiary. Ogromna liczba wiadomości może wiązać połączenie internetowe, spowalniać dostarczanie poczty, a nawet przeciążać system serwerów e-mail, aż do awarii systemu. Uważa się, że większość bombardowań przez e-mail to celowe ataki niezadowolonych ludzi; konkretne cele mogą być ofiarami kogoś z określoną urazą. Na przykład makler giełdowy w San Francisco otrzymał 23 września 1996 r. 25 000 wiadomości składających się ze słowa „idiota" od konsultanta, z którym się nie zgadzał. Powódź wiadomości uniemożliwiła mu korzystanie z komputera, więc w grudniu ofiara pozwała pracodawcę sprawcy o 25 000 USD odszkodowania. W przeszłości, na przykład robaka choinkowego i robaka internetowego, DoS uważa się za przypadkowy. Pakiety bomb e-mail automatyzują proces uruchamiania i przeprowadzania ataku DoS bombardującego pocztą e-mail. Z nazwami takimi jak Up Yours, Kaboom, Avalanche, Gatemail i Unabomber, pakiety te mogą być umieszczane na serwerze sieciowym podczas ataku DoS i wykorzystywane do atakowania innych systemów. Administratorzy, którzy znają te nazwy i inne osoby, powinni regularnie skanować dyski w poszukiwaniu powiązanych nazw plików i eliminować je. Aby zabezpieczyć komputery i / lub serwery, filtry poczty i schematy wykluczające mogą automatycznie filtrować i odrzucać pocztę wysyłaną z adresu źródłowego za pomocą pakietów bomb pocztowych. Filtry poczty są dostępne dla systemów UNIX, Windows, Macintosh i Linux. Większość komputerowych systemów operacyjnych i większość dostawców usług internetowych oferuje obecnie narzędzia do filtrowania w celu wyeliminowania niechcianych komercyjnych wiadomości e-mail i innych wiadomości e-mail. Chociaż sprawcy często ukrywają swoją tożsamość i lokalizację przy użyciu fałszywego adresu, większość filtrów można ustawić tak, aby przeskanować i wyeliminować te adresy. Dzięki bombardowaniu subskrypcji e-mail, znanej również jako łączenie list, osoba atakująca subskrybuje dziesiątki list mailingowych bez wiedzy użytkownika. Na przykład ktoś, kto nazywa się „Johnny Xchaotic", popełnił jeden z pierwszych incydentów z bombardowaniem subskrypcji. W sierpniu 1996 r. oskarżono go o masowy atak bombowy polegający na nieuczciwym subskrybowaniu dziesiątek ofiarom setek list mailingowych. W chaotycznym i niespójnym liście opublikowanym w Internecie wypowiedział niegrzeczne uwagi o znanych i mało znanych ludziach, których zdolność do otrzymywania sensownego e-maila została zniszczona przez tysiące niechcianych wiadomości dziennie. Dzisiaj filtrowanie pakietów ma mechanizmy wskazywania i klikania, które zapewniają automatyczne łączenie list. Użytkownik może zacząć otrzymywać setki lub tysiące wiadomości e-mail dziennie, jeśli jest połączony z zaledwie 50 do 100 listami. Po połączeniu z różnymi listami ofiara musi ręcznie wypisać się z każdej indywidualnej listy mailingowej. Jeśli atak ma miejsce, gdy ofiara jest nieobecna i nie ma dostępu do poczty e-mail, użytkownik może mieć zaległe tysiące wiadomości do czasu powrotu. Oprogramowanie serwera list nigdy nie powinno akceptować subskrypcji bez wysłania prośby o potwierdzenie do domniemanego subskrybenta; w obecnym środowisku większość serwerów list wymaga potwierdzenia od domniemanego subskrybenta przed rozpoczęciem regularnych wysyłek. Domyślnie komunikaty potwierdzające ignorują ogłoszenie, jeśli jest fałszywe. Jednak nawet ten mechanizm bezpieczeństwa może generować falę wielu pojedynczych wiadomości e-mail, jeśli bombardier pocztowy nadużyje serwerów list. W rezultacie wiele witryn wprowadziło Całkowicie zautomatyzowany test publicznego Turinga, aby poinformować obrazy Computers and Humans Apart (CAPTCHA) o przeszkadzaniu botom, które próbują subskrybować ofiary. Mówiąc o nieobecności, wiadomości urlopowe i potwierdzenia odbioru to kolejny sposób, w jaki ludzie mogą nieumyślnie rozpocząć burzę e-mailową. Wielu użytkowników ustawia swój adres e-mail na który klienci automatycznie żądają potwierdzenia odbioru wszystkich wysłanych wiadomości. Następnie użytkownicy wyjeżdżają na wakacje i konfigurują wiadomość urlopową z automatyczną

odpowiedzią. Gdy otrzymają wiadomość, klient odeśle wiadomość wakacyjną i poprosi o potwierdzenie. Z kolei otrzymane potwierdzenia generują więcej automatycznych odpowiedzi na wakacje. Kolejny wariant tej pętli informacji zwrotnej występuje, gdy pracownik wyjeżdża na urlop i przesyła wszystkie wiadomości e-mail do zewnętrznego usługodawcy internetowego, który ma lokalny numer dostępu w miejscu wakacji. Jeśli pracownik zdecyduje się nie sprawdzać poczty podczas nieobecności, albo z powodu wysokiej opłaty za dostęp lokalny, albo po to, aby nie zakłócać wakacji, skrzynka pocztowa dostawcy usług internetowych zapełni się przesłanymi wiadomościami. Jeśli skrzynka pocztowa zapełni się, dostawca usług internetowych wyśle wiadomość zwrotną z powrotem do serwera korporacyjnego, który następnie przesyła wiadomość zwrotną z powrotem do dostawcy usług internetowych, który generuje kolejną wiadomość zwrotną. W końcu nawet korporacyjny serwer pocztowy zapełni się wiadomościami pojedynczej osoby, powodując DoS wiadomości e-mail.

PRZEPEŁNIENIE BUFORA

Ataki związane z przepełnieniem bufora mogą być podstępne i szkodliwe. Możliwe jest wysłanie ciągu wejściowego do programu docelowego, który zawiera rzeczywisty kod i jest wystarczająco długi, aby przepełnić przestrzeń pamięci lub bufor wejściowy. Czasami ten tajny kod jest umieszczany na stosie procesów (obszar w pamięci komputera, w którym system operacyjny śledzi dane wejściowe programu i powiązany kod używany do przetwarzania danych wejściowych), a następnie kod jest przetwarzany. Przepełnienie może wystąpić, gdy dane wejściowe przepełnią swoją przestrzeń buforową i wpłyną do stosu, gdzie zastąpią poprzednie dane i adres zwrotny. Jeśli program jest napisany w taki sposób, że adres stosu wskazuje na złośliwy kod znajdujący się w buforze zwrotnym, kod jest wykonywany z uprawnieniami oryginalnego programu. Przepełnienie bufora jest wynikiem złego programowania, w którym programista nie sprawdza wielkości danych wejściowych w porównaniu do bufora wejściowego. Mimo że podstawa błędnego programowania przepełnienia bufora powinna już zostać wyeliminowana, co miesiąc pojawiają się nowe ataki związane z przepełnieniem bufora. Według stanu na styczeń 2013 r. Krajowa baza danych luk w zabezpieczeniach zawierała 6 273 przepełnienia bufora z łącznej liczby 64 398 luk w zabezpieczeniach - około 10 procent. Odsetek ten spada z biegiem lat; w okresie od stycznia 2010 r. do grudnia 2012 r. 1 281 z 14 510 rekordów dotyczyło przepełnienia bufora - tylko 9 procent; w przeciwieństwie do 39 822 zapisów dotyczących luk wprowadzonych przed 2010 r., 5047 (13 procent) dotyczyło przepełnienia bufora. Nie wszystkie przepełnienia bufora pozwalają użytkownikowi wstawić kod wykonywalny. Ataki DoS, takie jak Ping of Death, po prostu dołączają blok danych większy niż dozwolony przez protokół IP (tj. większy niż 65 536 bajtów). Ponieważ pakiety są podzielone na fragmenty do transmisji, udaje im się przedostać przez sieć i prawdopodobnie router i zaporę ogniową. Jednak po ponownym złożeniu w celu pakiety powodują przepełnienie bufora jądra IP i, jeśli nie są właściwie zarządzane, system ulega awarii. Innym przykładem jest stara wada Internetowych usług informacyjnych Microsoft (IIS) firmy Microsoft, którą można wykorzystać, aby umożliwić zatrzymanie usługi sieci Web. Aby to zrobić, osoba atakująca zażąda dokumentu o bardzo długim adresie URL z witryny internetowej opartej na IIS (a jak można zidentyfikować witrynę IIS? Jeśli witryna korzysta ze stron z rozszerzeniami .htm lub .asp, dobrze zgadnąć że w witrynie działają usługi IIS). Po otrzymaniu żądania nastąpiło naruszenie dostępu i serwer został zatrzymany. Mimo że Microsoft wydał łatkę na tę lukę, udane ataki trwały przez lata.

ZUŻYCIE PRZEPUSTOWOŚCI

Zużycie przepustowości obejmuje generowanie dużej liczby pakietów kierowanych do atakowanej sieci. Takie ataki mogą mieć miejsce w sieci lokalnej lub mogą być przeprowadzane zdalnie. Jeśli atakujący ma lub ma dostęp do większej przepustowości niż dostępna ofiara, może on zalać połączenie sieciowe ofiary. Takie nasycenie może się zdarzyć zarówno w przypadku szybkich, jak i szybkich połączeń sieciowych. Chociaż można użyć dowolnego rodzaju pakietu, najczęściej są to komunikaty echa ICMP (Internet Control Message Protocol) (generowane przez pingowanie). Angażując wiele witryn w celu zalania połączenia sieciowego ofiary, osoby atakujące mogą wzmocnić atak DoS. Aby to

zrobić skutecznie, atakujący przekonują system wzmacniający do wysyłania ruchu do sieci ofiary. Śledzenie intruza, który dokonuje ataku polegającego na zużyciu przepustowości, może być trudne, ponieważ osoby atakujące mogą sfałszować swoje adresy źródłowe. Jednym z bardzo częstych ataków polegających na zużyciu pasma jest atak smerfowy. Ten atak jest szczególnie interesujący (i sprytny), ponieważ wykorzystuje narzędzia znajdujące się w każdym systemie IP i zatrudnia stronę zewnętrzną, bez faktycznej kontroli nad dowolnym systemem w dowolnym miejscu. Atak smurf rozpoczyna się, gdy intruz wysyła ciąg bardzo dużych wiadomości ping do transmisji adresu IP nieświadomej strony trzeciej. Intruz fałszuje źródłowy adres IP wiadomości ping, przez co wydaje się, że wiadomości te pochodzą z, powiedzmy, routera w sieci docelowej, router.victim.com. Jeśli intruz wyśle na przykład pojedynczy komunikat ping o wielkości 10 000 bajtów na adres rozgłoszeniowy strony pośredniej z 50 hostami, odpowiedzi zużyją 4 megabity (Mb) . Nawet jeśli ofiarama linię T1 (z przepustowością 1,544 Mb na sekundę), atakujący może zalać linię ofiary jedynie wysyłając pojedynczy duży sygnał ping na sekundę do prawej strony. Witryna pośrednia nazywana jest z oczywistych powodów siecią wzmacniającą; zwróć uwagę, że atakujący nie musi narażać na szwank żadnych systemów. Stosunek oryginalnie przesłanych pakietów do liczby systemów, które odpowiadają, jest znany jako współczynnik wzmocnienia. Wariant ataku smerfowego nazywa się fraggle. W tym wariancie osoby atakujące wysyłają sfałszowane pakiety UDP (User Datagram Protocol) zamiast wiadomości echa na adres rozgłoszeniowy sieci wzmacniającej. Każdy system w sieci wzmacniającej z włączonym konkretnym portem adresu rozgłoszeniowego generuje duży ruch, odpowiadając na hosta ofiary; jeśli port nie jest włączony, system na wzmacniaczu sieć wygeneruje nieosiągalne wiadomości hosta ICMP do hosta ofiary. W obu przypadkach przepustowość ofiary jest zużyta. Ataki paniki na jądro nie wynikają z samego błędu programistycznego, ale z dziury w logice programu. Na przykład procesor Intel Pentium, który nie mógł poprawnie podzielić dwóch konkretnych legalnych danych wejściowych, miał wadę programistyczną. Jądro IP, które zawodzi podczas odbierania pakietu, który nigdy nie powinien wystąpić w pierwszej kolejności, jest rzeczywiście luką w logice programu, ale nie jest tym samym, co brak obsługi legalnych danych wejściowych. W tym przypadku program nie wiedział, jak z wdziękiem zawieść, gdy otrzymał nieoczekiwany sygnał wejściowy. Konkretny przykład paniki jądra występuje w jądrze Linuksa w wersji 2.2.0, gdy zamiast tego do drukowania niektórych plików podstawowych używany jest program zwykle używany do drukowania zależności bibliotek współdzielonych. W pewnych okolicznościach munmap(), wywołanie funkcji używane do mapowania i mapowania urządzeń do pamięci, zastępuje krytyczne obszary pamięci jądra i powoduje panikę i restart systemu. Są też inne przykłady tego rodzaju ataków. Atak lądowy ma miejsce, gdy sfałszowany pakiet jest wysyłany do hosta docelowego, na którym porty TCP i docelowe są ustawione na tę samą wartość, a adresy IP źródłowy i docelowy są ustawione na tę samą wartość. Ponieważ jest to mylące dla systemu operacyjnego hosta, powoduje 100% wykorzystanie procesora, a następnie zatrzymuje się. Ataki lądowe były skierowane na prawie wszystkie systemy operacyjne. Ataki łzy są również wynikiem zachowania podczas odbierania niemożliwych pakietów. Jeśli pakiet IP jest zbyt duży, aby poradzić sobie z określoną siecią, pakiet zostanie podzielony na mniejsze części. Informacje w nagłówku pakietu IP informują hosta docelowego, jak ponownie złożyć pakiet. W ataku Łzy atakujący celowo tworzy pakiety IP, które wydają się nakładać na siebie po ponownym złożeniu. To również może spowodować awarię hosta. Ataki Teardrop zostały wymierzone w systemy operacyjne Microsoft i wszystkie warianty UNIX.

ATAKI NA SYSTEM ROUTIGU I NAZWY DOMEN

Ataki na routing i system nazw domen (DNS) to sprytne ataki, które są powtarzane wielokrotnie. Manipulując przy DNS, nazwa domeny witryny rozwiązuje się na adres IP każdej innej witryny, którą życzy sobie atakujący. Na przykład w sierpniu 1999 r. Niezadowolony inżynier PairGain Technologies podał bezpośredni link do fałszywej, ale autentycznie wyglądającej strony Bloomberg News Service, którą stworzył. Inżynier, który był właścicielem akcji PairGain, opublikował fałszywe informacje o domniemanym przejęciu PairGain przez izraelską firmę, podnosząc cenę akcji PairGain na całym świecie i powodując spustoszenie na rynku poprzez swoje oszustwa. Chociaż to nietradycyjny atak DoS,

działania te uniemożliwiały użytkownikom dostęp do pożądanej witryny, z poważnymi konsekwencjami. Inny przykład miał miejsce w lipcu 1997 r., kiedy Eugene Kashpureff złożył w InterNIC fałszywe informacje dotyczące aktualizacji DNS na ten miesiąc, zmuszając serwery nazw domen na całym świecie do rozpoznawania tymczasowych i nieautoryzowanych adresów internetowych kończących się na .xxx, .mall, .nic i. za. Kilka tygodni później Kashpureff podał fałszywe informacje, które zmusiły ludzi próbujących uzyskać dostęp do strony Network Solutions Inc., aby znaleźć się na stronie AlterNIC, której był właścicielem. W tym samym roku został aresztowany pod zarzutem oszustwa. W innym przykładzie - tym z 2000 r. - ataku na routing i DNS, RSA Security, Inc., po ogłoszeniu, że opracował metodę zwalczania hakerów witryny, stwierdził, że użytkownicy nieświadomie byli przekierowywani na fałszywą Witrynę RSA. Oszukańcza witryna wyglądała dokładnie tak, jak oryginalna witryna RSA, ale wyśmiewała się z faktu, że hakerowi udało się osiągnąć cel DoS. Już w 1997 r. wykryto i udokumentowano słabości dotyczące implementacji BIND w wersjach wcześniejszych niż 4.9.5 + P1. Wcześniejsze wersje buforowały fałszywe informacje DNS, gdy rekursja DNS była włączona. Luka umożliwiła atakującym wykorzystanie procesu mapowania adresów IP na nazwy hostów w tak zwanym fałszowaniu rekordów wskaźników (PTR). Ten rodzaj fałszowania zapewnia możliwość ataku DNS DoS. Ataki DNS są nadal szeroko widoczne. Wyłudzanie informacji jest formą ataku socjotechnicznego, w ramach którego użytkownicy są kierowani do fałszywych, ale wyglądających autentycznie witryn firm bankowych lub kart kredytowych i zachęcani do wprowadzania danych osobowych wykorzystywanych do kradzieży tożsamości. Gdyby jednak użytkownicy uważnie przyjrzeli się adresowi URL witryny, zaobserwowaliby podejrzany adres URL. Pharming to odmiana phishingu oparta na jakiejś formie zatrucia DNS , tak że użytkownik przechodzący do faktycznego adresu URL banku lub wystawcy karty kredytowej zostanie przekierowany na fałszywą stronę. Pojawiły się również inne warianty phishingu, takie jak spearphishing (kierowanie ataku phishingowego na określoną osobę, funkcję lub grupę), vishing (atak phishingowy za pośrednictwem sieci telekomunikacyjnej, taki jak Voice-over-IP [VoIP]), oraz wyłudzanie informacji (wyłudzanie informacji za pośrednictwem usługi krótkich wiadomości [SMS] lub wiadomości tekstowych)

SYN Flooding.

SYN flooding to atak DoS, który pasuje do kategorii zużycia ograniczonych zasobów. Ten atak DoS wykorzystuje trójdrożny handshake używany przez hosty TCP do synchronizacji połączenia logicznego przed wymianą danych. W normalnym połączeniu hosta z hostem TCP dwa hosty wymieniają trzy segmenty TCP przed wymianą danych:

1. Klient wysyła segment do serwera z jego początkowym numerem sekwencyjnym (ISN). Flaga SYN (synchronizacja) jest ustawiona w tym segmencie.
2. Serwer odpowiada, wysyłając segment zawierający swój ISN i potwierdza ISN klienta. W tym segmencie będą ustawione flagi SYN i ACK (potwierdzenie). W tym momencie serwer przydziela zasoby dla połączenia, które ma zostać wkrótce ustanowione, i czeka na trzeci segment.
3. Klient wysyła segment potwierdzający numer ISN serwera. Ten i wszystkie kolejne segmenty do końca sesji będą miały ustawioną tylko flagę ACK. SYN Flooding wykorzystuje trójdrożny handshake oraz fakt, że serwer może mieć tylko skończoną liczbę otwartych połączeń TCP. Atak jest uruchamiany, gdy atakujący inicjuje połączenia, dla których nigdy nie będzie trzeciego segmentu. Gdy serwer wyśle segment w kroku 2, czeka na odpowiedź. W normalnych okolicznościach klient odpowie w ciągu kilku sekund. Serwer może poczekać, powiedzmy, 10 sekund, zanim przekroczy limit czasu i zwolni zasoby. Załóżmy jednak, że atakujący wysyła setki komunikatów o połączeniach na sekundę w sposób ciągły. Gdy te fałszywe połączenia zalewają cel szybciej, niż mogą przekroczyć limit czasu, nie pozostaną żadne zasoby do nawiązania legalnego połączenia. Jest to rodzaj ataku przeprowadzonego przeciwko PANIX w 1996 roku.

GŁÓD ZASOBÓW

Głód zasobów jest kategorią ogólną dla wielu innych rodzajów ataków DoS, które są wynikiem niektórych ograniczonych zasobów - czy to przepustowości, mocy obliczeniowej, zajętego i wyczerpanego miejsca na dysku. Jeden przykład wykorzystuje nowatorski atak UDP DoS, w którym intruz fałszuje pakiety UDP i wykorzystuje je do połączenia usługi echa jednej maszyny (port 7 UDP) z usługą generatora znaków (ładowanie) na innej maszynie (port 19 UDP). Kiedy to nastąpi, oba komputery zużywają całą dostępną przepustowość sieci, a wszystkie maszyny w tych samych sieciach, co maszyny docelowe, mogą mieć wpływ i brakować zasobów. Ale takie ataki mogą również zdarzyć się lokalnie. Niestety, wielu autoryzowanych użytkowników przeprowadza lokalne ataki DoS, które albo zużywają zasoby systemowe, albo odmawiają użytkownikom dostępu. Liczne ataki głodu zasobów i błędy programowe atakują określone systemy. Na przykład przekroczenie narzuconych limitów miejsca na dysku powoduje, że systemy wielu użytkowników mogą cierpieć z powodu ataku głodu zasobów. Większość systemów operacyjnych ogranicza kwotę, o którą użytkownik może przekroczyć limit miejsca na dysku. Windows 2000 ma w tym coś dziwnego; chociaż poszczególne pliki mogą przekroczyć limit tylko o niewielką ilość, to jeśli każdy plik przekroczy limit, użytkownik może zużyć dużo dodatkowego miejsca na dysku. Innym wariantem tego typu ataku jest Slowloris, który atakuje serwery sieciowe i wykorzystuje stosunkowo małą przepustowość atakującego. Korzystając ze schematu Slowloris, osoba atakująca wysyła dużą liczbę żądań połączenia do serwera targetWeb i utrzymuje je otwarte tak długo, jak to możliwe. W niektórych okolicznościach serwer sieci Web, którego dotyczy problem, wyczerpuje swoją pulę zasobów połączeń w przypadku niespełnionych żądań, tym samym odrzucając uzasadnione żądania. Slowloris jest podatny na wiele typów serwerów WWW, w tym kilka wersji Apache. Wariant Slowloris nazywa się R-U-Dead-Yet (RUDY). RUDY wysysa zasoby połączeń z serwera aWeb, wysyłając dużą liczbę wiadomości POST i losowo duże wartości długości treści w nagłówku wiadomości http

ATAKI JAVA, PHP i ASP.

Istnieje wiele ataków ukierunkowanych na luki w zabezpieczeniach programu na stronach internetowych korzystających z Java, PHP (PHP: Hypertext Preprocessor), Active Server Pages (ASP) i innych języków skryptowych po stronie serwera. Jednym z przykładów jest atak DOS z 2011 r., Który spowodował wyczerpanie zasobów procesora. W tym konkretnym ataku osoba atakująca wysyła zmienne na serwer sieciowy przy użyciu metody POST protokołu HTTP. Wysyłając dziesiątki lub setki tysięcy specjalnie wybranych nazw zmiennych, można wymusić kolizje w nazwach tabel skrótów, ostatecznie zużywając wszystkie cykle procesora na obsługę pojedynczego żądania HTTP POST.

ATAKI NA ROUTER

Ataki na router zostały opracowane dla wielu różnych routerów. Ponieważ routery są szkieletem Internetu i bramą, przez którą organizacje łączą się z Internetem, zabicie routera odmawia usługi sieciowej dla setek komputerów. Wydajność i konsekwencje finansowe ataku sprzętowego mogą być bardzo poważne. Popularnymi celami tego rodzaju ataków są routery Ascend, Cisco, Juniper, Lucent i 3Com. Niestety wielu menedżerów sieci ułatwia ataki, wykorzystując Telnet lub HTTP do zdalnego dostępu i niewłaściwie zabezpieczając sieć przed zdalnym dostępem przez kogokolwiek przez Internet.

INNE ATAKI TYPU „ODMOWA USŁUGI”

Nawet ta lista konkretnych ataków DoS nie jest wyczerpująca. Na przykład Bonk i boink (aka bonk.c) to ataki DoS, które powodują awarię docelowego systemu Windows 9x / NT. Arnudp (arnudp100.c) wykuwa pakiety UDP w celu implementacji DoS w stosunku do UUDPports 7 (echo), 13 (w dzień), 19 (chargeen) i 37 (czas), usługi często uruchamiane w systemach UNIX i Windows NT. A cbcb.c to cancelbot, który niszczy istniejące posty grup dyskusyjnych Usenet, które spełniają określone kryteria. (Niektórzy twierdzą, że cbcb.c tak naprawdę nie przeprowadza ataku DoS; jednak po aktywacji program odmawia dostępu do postów dla docelowych użytkowników Usenetu). Przykładem ataku sieciowego

na zasób niesieciowy byłoby miliard śmiechu (bomba XML), atak DoS wymierzony w parsery języka Extensible Markup Language (XML). W XML jednostka jest fragmentem kodu, który pozwala programiście zdefiniować coś, co można łatwo zmodyfikować lub ponownie wykorzystać w innych dokumentach, podobnie jak obiekt programowy. W miliardach śmiechu atakujący tworzy dokument XML zawierający 10 encji, z których każda definiowana jest jako 10 instancji poprzedniej encji (1010 ≈ 1 miliarda, stąd nazwa). Miliardowe śmiechy zostały wprowadzone po raz pierwszy już w 2003 roku, ale pozostały problemem do końca pierwszej dekady 2000 roku. Podsumowując, ataki DoS nie ograniczają się do sieci. Na przykład atak czarnym faksem to prosty, ale skuteczny atak polegający na wyczerpaniu zasobów; atakujący jedynie przesyła faksem stronę zawierającą dużą czarną skrzynkę ofierze, co powoduje, że faks ofiary zużywa dużą ilość czarnego tonera. Wysłanie dużej liczby tych faksów ostatecznie zużyje toner na faksie ofiary i / lub uniemożliwi dostarczenie legalnych faksów. Pewien ekspert ds. bezpieczeństwa skleił ze sobą końce długiego paska papieru, aby stworzyć nieskończoną pętlę w faksie, aby zaatakować spamera faksu, który odmówił przestania wysyłać mu niechciane oferty podróży. Kolejny atak na faksy wykorzystuje zautomatyzowane skrypty do wybierania numeru i wybierania numeru przez komputer docelowy za pomocą tysięcy kopii (zwykle obraźliwych) faksów; zdenerwowani kujony znani są z tego, że wykorzystują ten atak na spamerów faksu, na tyle nierozsądnie, by używać prawdziwych numerów telefonicznych do własnych faksów.

ZAPOBIEGANIE I ODPOWIEDZI NA ATAKI DENIAL-OF-SERVICE.

Atakom DoS najlepiej zapobiegać; obsługa ich w czasie rzeczywistym jest bardzo trudna. Najważniejszym sposobem ochrony systemu jest hartowanie systemów operacyjnych:

* Zainstaluj je z myślą o bezpieczeństwie.
* Monitoruj witryny, aby mieć świadomość luk w zabezpieczeniach.
* W miarę możliwości utrzymuj najnowsze wersje oprogramowania.
* Zainstaluj wszystkie odpowiednie poprawki bezpieczeństwa.

Jednak duża część zapobiegania polega na filtrowaniu pakietów na routerach sieciowych. Ponieważ osoby atakujące często ukrywają tożsamość maszyn używanych do przeprowadzania ataków poprzez fałszowanie adresu źródłowego połączenia sieciowego, techniki znane jako filtrowanie wyjścia i filtrowanie dostępu są powszechnie stosowane jako środki ochronne. Jak omówiono w dalszej części , wychodzenie i filtrowanie wejścia są metodami zapobiegania, odpowiednio, opuszczaniu lub wchodzeniu pakietów do sieci z nieprawidłowym adresem źródłowym. Blokowanie adresów, które nie spełniają kryteriów prawidłowych adresów źródłowych i upewnienie się, że wszystkie pakiety opuszczające witrynę organizacji zawierają prawidłowe adresy, może udaremnić wiele ataków DoS. Inne metody filtrowania pakietów, które pomogą zapobiec DoS, to blokowanie wszystkich wiadomości rozgłoszeniowych i większości wiadomości ICMP. Nie ma powodu, dla którego witryna powinna akceptować wiadomości wysyłane do wszystkich hostów w witrynie. Ponadto prawdopodobnie nie ma dobrego powodu, aby zezwolić wszystkim hostom na odpowiadanie na wiadomości ping lub traceroute; w rzeczywistości większość komunikatów ICMP prawdopodobnie może zostać zablokowana. W niektórych przypadkach ofiary ustawiają listy odpowiedzi uruchamiane w celu wysyłania i ponownego wysyłania w dużych ilościach, aby zalać adres atakującego. Robienie tego na ogół nie jest dobrym pomysłem. Jeśli te wiadomości zostaną wysłane na prawidłowy adres, osoba atakująca może je odebrać i zatrzymać. Ale atakujący zazwyczaj fałszują źródłowy adres IP, więc odpowiedź na prawdopodobnie fałszywą sieć IP nie jest dobrą postawą obronną, ponieważ może zaszkodzić niewinnym ofiarom. Najlepsza obrona będzie obejmować ISP. W przypadkach, w których można zidentyfikować dostawcę usług osoby atakującej i skontaktować się z nim, ofiara może poprosić dostawcę usług o interwencję. W takich przypadkach dostawcy usług internetowych zwykle podejmują odpowiednie działania, aby zatrzymać atak i odnaleźć sprawcę. Jednak w przypadkach, gdy DoS wydaje się naśladować lub naśladować inną formę ataku lub gdy trwa on niezwykle długo, ofiara może chcieć

podjąć bardziej agresywne działania, kontaktując się z CERT / CC, FBI i innymi organami, które mieć doświadczenie w atakach DoS i pewną jurysdykcję, jeśli sprawcy zostaną złapani. Obrona w czasie rzeczywistym jest trudna, ale możliwa. Wiele routerów i zewnętrznych systemów wykrywania włamań (IDS) może wykryć atak w czasie rzeczywistym, na przykład zbyt wiele żądań połączeń na jednostkę czasu z danego hosta IP lub adresu sieciowego. Router może blokować żądania połączenia lub IDS może wysłać komunikat pagera do administratora bezpieczeństwa. Jednak ataki takie jak smerfy mogą pochłonąć całą przepustowość, nawet zanim pakiety dotrą do miejsca docelowego. Aby w pełni zwalczać ataki DoS, wymagana jest współpraca dostawców usług internetowych i witryn użytkowników końcowych. Zostanie to omówione w dalszej części dyskusji na temat odpowiedzi na DDoS.

DISTRIBUTED DENIAL-OF-SERVICE.

Narzędzia DDoS wykorzystują wzmocnienie do zwiększenia siły atakującego. Przekształcając słabo zabezpieczone systemy w wysyłanie skoordynowanych fal oszukańczego ruchu skierowanego do określonych celów, intruzi mogą przytłoczyć przepustowość dowolnej ofiary. W ataku DDoS atakujące pakiety pochodzą z dziesiątek lub setek adresów, a nie tylko z jednego, jak w przypadku standardowego ataku DoS. Jakakolwiek ochrona DoS oparta na monitorowaniu ilości pakietów pochodzących z jednego adresu lub jednej sieci zawiedzie, ponieważ ataki pochodzą z całego świata. Zamiast otrzymywać na przykład 1000 gigantycznych pingów na sekundę z atakującego miejsca, ofiara może otrzymać jeden ping na sekundę z każdego z 1000 atakujących stron. Inną niepokojącą rzeczą dotyczącą ataków DDoS jest to, że moduł obsługi może wybrać lokalizację agentów. Tak więc, na przykład, przewodnik może atakować kilka stron Organizacji Traktatu Północnoatlantyckiego (NATO) jako ofiary i zatrudniać agentów, którzy wszyscy są w krajach, o których wiadomo, że są wrogo nastawieni do NATO. Ludzki napastnik może siedzieć, powiedzmy, w Kanadzie. Podobnie jak ataki DoS, wszystkie ataki DDoS wykorzystują standardowe wiadomości TCP / IP - ale wykorzystują je w niestandardowy sposób. Typowe ataki DDoS obejmują Tribe Flood Network (TFN), Trin00, Stacheldraht i Trinity. W poniższych sekcjach przedstawiono niektóre szczegóły dotyczące tych ataków.

KRÓTKA HISTORIA ROPROSZONEJ ODMOWY USŁUGI

Ataki typu „odmowa usługi" pod wieloma postaciami istnieją od dziesięcioleci. Rozproszone ataki DoS są znacznie nowsze. Na przełomie czerwca i lipca 1999 r. grupy hakerów zainstalowały i przetestowały narzędzie DDoS o nazwie Trinoo w celu przeprowadzania średnich i dużych ataków DDoS. Ich testy obejmowały ponad 2000 złamanych i celów na całym świecie. Większość literatury sugeruje, że pierwszy udokumentowany atak DDoS na dużą skalę miał miejsce w sierpniu 1999 r., kiedy Trinoo zostało wdrożone w co najmniej 227 systemach (z czego 114 w Internecie) w celu zalania jednego komputera University of Minnesota; ten system był wyłączony przez ponad dwa dni. W dniu 28 grudnia 1999 r. CERT / CC wydało swój Poradnik CA-1999-17 oceniający DDoS. W dniu 7 lutego 2000 r. Yahoo! był ofiarą DDoS, podczas którego portal internetowy był niedostępny przez trzy godziny. 8 lutego Amazon, Buy.com, CNN i eBay zostały dotknięte atakami DDoS, które spowodowały, że albo całkowicie przestały działać, albo znacznie spowolniły. 9 lutego 2000 r. Zarówno E ∗ Trade, jak i ZDNet zostały poddane atakom DDoS. Analitycy oszacowali, że w ciągu trzech godzin Yahoo! spadł, poniósł stratę w handlu elektronicznym i przychodach z reklam, które wyniosły około 500 000 USD. Według księgarni Amazon.com, jego szeroko nagłośniony atak spowodował stratę 600 000 USD w ciągu 10 godzin, które upłynęły. Podczas ataków DDoS, Buy.com zmniejszył ze 100 procent dostępności do 9,4 procent, podczas gdy użytkownicy CNN.com spadli poniżej 5 procent normalnego wolumenu, a Zdnet.com i E ∗ Trade.com były praktycznie nieosiągalne. Schwab.com, miejsce online brokera zniżek Charlesa Schwaba, również został trafiony, ale odmówił podania dokładnych liczb strat. Można jedynie założyć, że dla firmy, która co tydzień zarabia 2 miliardy dolarów na handlu online, strata czasu przestoju była ogromna. Innym rodzajem szkód spowodowanych pośrednio przez DDoS był spadek wartości zapasów w ciągu 10 dni po atakach: eBay spadł o 24 procent, Yahoo! spadła o 15 procent, a Buy.com o 44

procent. Ataki te zostały zorganizowane przez 15-letniego Michaela Calce, młodzieńca mieszkającego na zachodnim krańcu wyspy Montreal w Quebecu, którego pseudonim brzmiał Mafiaboy. W końcu przyznał się do winy 56 przestępstw komputerowych i odbył osiem miesięcy pozbawienia wolności. Tego rodzaju ataki DDoS są kontynuowane od lata 1999 r. Jednym z najbardziej znanych incydentów była seria ataków DDoS ponownie na stronie GRC.com Steve'a Gibsona w maju 2001 r. Osoba atakująca miała 13 lat i korzystała z przekaźnika internetowego Bot (IRC), zautomatyzowane programy wykorzystujące systemy korzystające z klientów IRC, by stać się zombie DDoS. Jednak atak DDoS, który miał największy potencjalnie niszczycielski wpływ, miał miejsce 21 października 2002 r., Kiedy wszystkie serwery DNS najwyższego poziomu zostały poddane ciągłemu atakowi przez tysiące zombie. Dziewięć z 13 serwerów głównych DNS zostało usuniętych z Internetu; pozostałe cztery były w stanie kontynuować działanie podczas ataku. Wszyscy główni dostawcy usług internetowych i wiele dużych sieci prywatnych utrzymują własne systemy DNS, chociaż większość serwerów ostatecznie polega na serwerach głównych, aby znaleźć niebuforowane wpisy DNS. Atak trwał zaledwie godzinę lub dwie; gdyby trwało to znacznie dłużej, prawdopodobnie pozostałe serwery zostałyby przytłoczone, skutecznie blokując translację nazwy / adresu hosta DNS. Trendem niepokojącym i rosnącym jest stosowanie DDoS jako narzędzia wymuszeń. Wielu przestępców używa narzędzi DDoS jako sposób na grożenie atakiem, zamiast zakłócania sieci organizacji docelowej. Chociaż kilku dostawców usług sieciowych, bezpieczeństwa i konsultingowych twierdzi, że zarówno oni, jak i wielu ich klientów otrzymało takie żądania wymuszenia, niewielu publicznie podaje nazwy celów, z których wielu przystępuje do zagrożeń i szantażuje. Większość ekspertów zgadza się, że wymuszenia nie powinny być spełnione; postępowanie takie tylko zachęca do zachowania przestępczego. W przypadku otrzymania takiego zagrożenia należy natychmiast skontaktować się z dostawcą usług internetowych organizacji i organami ścigania

ROZPROSZONA TERMINOLOGIA I OMÓWIENIE ODMOWY OBSŁUGI

Aby opisać i zrozumieć ataki DDoS, ważne jest, aby zrozumieć terminologię stosowaną do opisywania ataków i narzędzi. Mimo że branża mniej więcej ustaliła się na niektórych powszechnych warunkach, konsensus pojawił się dopiero po tym, jak wiele ataków DoS / DDoS pojawiło się już w literaturze hakerów i głównego nurtu. Wczesne opisy narzędzi DDoS używały wielu terminów do opisania różnych ról systemów zaangażowanych w atak. Podczas Distributed System Intruder Tools Workshop CERT / CC, które odbyły się w listopadzie 1999 r., wprowadzono pewną standardową terminologię i te terminy zostały użyte w poniższych akapitach. Oto kilka synonimów: aby dostosować te terminy do terminów używanych w literaturze hakerów oraz do wczesnych opisów:
Intruz - zwany także napastnikiem lub klientem.
Master - zwany także programem obsługi.
Daemon - zwany także agentem, programem bcast (broadcast) lub zombie.
Ofiara - zwana także celem.
Ataki DoS / DDoS mają w rzeczywistości dwie ofiary: ostateczny cel i systemy pośrednie, które zostały wykorzystane i załadowane oprogramowaniem demona. W tej części skupiono się na ofiarach DoS / DDoS z końca linii. Ataki DDoS zawsze obejmują wiele systemów. Typowy scenariusz ataku DDoS może z grubsza wykonać następujące trzy kroki:
1. Intruz znajduje jeden lub więcej systemów w Internecie, które mogą zostać naruszone i wykorzystane. Zazwyczaj dokonuje się tego przy użyciu skradzionego konta w systemie z dużą liczbą użytkowników lub nieuważnych administratorów, najlepiej z połączeniem szerokopasmowym z Internetem. (Wiele takich systemów można znaleźć na kampusach uniwersyteckich i uniwersyteckich).
2. Zaatakowany system jest załadowany dowolną liczbą narzędzi do hakowania i łamania, takich jak skanery, narzędzia do eksploracji, detektory systemu operacyjnego, rootkity i programy DoS / DDoS. Ten system staje się masterem DDoS. Oprogramowanie główne pozwala mu znaleźć wiele innych systemów, które same mogą być zagrożone i wykorzystane. Atakujący skanuje szeroki zakres bloków adresów IP w poszukiwaniu systemów z usługami znanymi z luk w zabezpieczeniach. Ta początkowa faza masowej ingerencji wykorzystuje zautomatyzowane narzędzia do zdalnego kompromisu od

kilkuset do kilku tysięcy hostów i instaluje agentów DDoS w tych systemach. Automatyczne narzędzia do wykonania tego kompromisu nie są częścią zestawu narzędzi DDoS, lecz są wymieniane w ramach grup hakerów przestępczych. Te zaatakowane systemy są początkowymi ofiarami ataku DDoS. Te później eksploatowane systemy zostaną załadowane demonami DDoS, które się przeprowadzają faktyczny atak
3. Intruz utrzymuje listę posiadanych systemów (czasami pisanych przez hakerów), zagrożonych systemów z demonem DDoS. Faktyczna faza ataku typu „odmowa usługi" ma miejsce, gdy atakujący uruchamia program w systemie nadrzędnym, który komunikuje się z demonami DDoS w celu uruchomienia ataku. Oto, gdzie zamierzona ofiara DDoS wchodzi do scenariusza.

Komunikacja między urządzeniem głównym a demonami może być zaciemniona, przez co trudno jest zlokalizować komputer główny. Chociaż na jednej lub kilku maszynach w sieci DDoS mogą istnieć pewne dowody dotyczące lokalizacji urządzenia nadrzędnego, demony zwykle są zautomatyzowane, więc nie jest konieczne prowadzenie ciągłego dialogu między urządzeniem głównym a resztą sieci DDoS. W rzeczywistości zwykle stosuje się techniki celowego maskowania tożsamości i lokalizacji urządzenia nadrzędnego w sieci DDoS. Techniki te utrudniają analizę trwającego ataku oraz blokowanie ruchu atakującego i śledzenie go z powrotem do źródła. W większości przypadków administratorzy zainfekowanych systemów nie wiedzą, że demony zostały zainstalowane. Nawet jeśli znajdą i wyeliminują oprogramowanie DDoS, nie mogą pomóc nikomu ustalić, gdzie jeszcze oprogramowanie mogło zostać umieszczone. Popularnymi systemami do wykorzystania są serwery WWW, e-mail, nazwa lub inne serwery witryny, ponieważ systemy te mogą mieć dużą liczbę otwartych portów, dużą ilość ruchu i jest mało prawdopodobne, że zostaną szybko odłączone od sieci, nawet jeśli można do nich przypisać atak

OPISY NARZĘDZI DDoS.

Ta sekcja zawiera szczegółowe informacje o działaniu niektórych głównych narzędzi DDoS.
Trinoo (Trin00). Trinoo lub Trin00 to pierwsze znane narzędzie DDoS, które pojawiło się latem 1999 r. Typowa instalacja Trinoo jest podobna do scenariusza przedstawionego powyżej, w którym atakujący instaluje oprogramowanie obsługi w systemie, a ten z kolei ładuje oprogramowanie atakujące na agenci. Trinoo to rozproszony atak SYN DoS. Trinoo używa wielu portów TCP i UDP:

* Mistrzowie nasłuchują na porcie 27665 TCP w celu komunikacji między atakującym a głównym.
* Demony nasłuchują na porcie UDP 27444 w celu komunikacji master-to-demon.
* Mistrzowie nasłuchują na porcie UDP 31335 w celu komunikacji demon-master.

Są to domyślne numery portów, a warianty używane inne porty. Osoba atakująca może zdalnie sterować nadrzędnym Trinoo (programem obsługi) za pośrednictwem połączenia z portem TCP 27665. Po nawiązaniu połączenia osoba atakująca podaje oczekiwane hasło betaalmostdone. Program główny Trinoo zazwyczaj nosi nazwę master.c, a demonem jest ns.c. Komunikacja między urządzeniem głównym Trinoo (modułem obsługi) a demonami (agentami) odbywa się za pośrednictwem UDP. Komunikacja master-to-demon wykorzystuje datagramy UDP na porcie 27444. Wszystkie polecenia zawierają hasło, domyślnie l44adsl. Wszystkie poprawne polecenia zawierają podciąg l44. Komunikacja z demonów Trinoo do urządzenia nadrzędnego korzysta z datagramów UDP na porcie 31335. Po uruchomieniu demona wysyła komunikat do urządzenia nadrzędnego zawierający ciąg ∗ HELLO ∗. Funkcja utrzymywania przy życiu Trinoo jest realizowana przez wymianę między urządzeniem głównym a demonem: Mistrz wysyła polecenie mping Trinoo, które wysyła ciąg png do demona; demon odpowiada, wysyłając ciąg PONG do mastera. Hasła mają uniemożliwić administratorom systemu przejęcie kontroli nad masterami i demonami tworzącymi sieć Trinoo. Inne domyślne hasła w początkowych atakach to gOrave, aby uruchomić serwer główny Trinoo i killme, aby kontrolować polecenie mdie mistrza, aby zabić procesy Trinoo. Podobnie jak numery portów, osoby atakujące mogą

łatwo zmieniać hasła. Oprogramowanie do wykrywania włamań lub rutynowa analiza systemu może wyszukać wiele rzeczy, które mogą wskazywać na obecność Trinoo:

* System nasłuchujący na porcie UDP 27444 może być demonem Trinoo.
* Komunikacja demona Trinoo będzie zawierać ciąg l44.
* Mechanizm zalewania SYN wybiera port docelowy za pomocą funkcji generatora liczb losowych.
* Demon Trinoo wyśle ciąg PONG, jeśli otrzyma polecenie png.
* System nasłuchujący na porcie TCP 27665 może być urządzeniem głównym Trinoo.
* System nasłuchujący na porcie UDP 27444 może być urządzeniem głównym Trinoo.
* Pakiety UDP będą zawierać ciąg l44adsl.

TRIBE FLOOD NETWORK

Tribe Flood Network (TFN) pojawiła się po Trinoo. TFN działa przede wszystkim na zagrożonych systemach UNIX wykorzystywanych przy użyciu błędów przepełnienia bufora w usłudze zdalnego wywoływania procedur (RPC). Programy klienckie i demoniczne TFN implementują sieć DDoS zdolną do przeprowadzania szeregu ataków, takich jak powódź ICMP, powódź SYN, powódź UDP i ataki typu smurf. TFN wyraźnie różni się od Trinoo tym, że cała komunikacja między klientem (atakującym), programami obsługi i agentami używa pakietów echa ICMP i pakietów odpowiedzi echa. Komunikacja między klientem TFN a demonami odbywa się za pośrednictwem pakietów odpowiedzi echa ICMP. Brak ruchu TCP i UDP czasami utrudnia wykrycie tych pakietów, ponieważ wiele narzędzi do monitorowania protokołu nie jest skonfigurowanych do przechwytywania i wyświetlania ruchu ICMP. Zdalne sterowanie siecią TFN odbywa się poprzez uruchomienie programu w systemie klienta. Program może być również uruchamiany w systemie obsługi przez klienta za pomocą niektórych metod połączenia host-host, takich jak połączenie z wykorzystywanym portem TCP lub za pomocą zdalnej powłoki opartej na UDP lub ICMP. Program musi być dostarczony:

* Lista adresów IP hostów gotowych do przeprowadzenia ataku powodziowego
* Rodzaj ataku, który ma zostać uruchomiony
* Lista adresów IP hostów docelowych
* Numer portu dla ataku SYN

Żadna ochrona hasłem nie jest powiązana z TFN. Każde polecenie do demonów jest wysyłane w polu Identyfikator pakietu ICMP; wartości 345, 890 i 901 rozpoczynają odpowiednio ataki powodziowe SYN, UDP i ICMP. Pole Numer sekwencji w komunikacie odpowiedzi echa jest zawsze ustawione na 0x0000, co sprawia, że wygląda jak odpowiedź na początkowy pakiet echa wysłany przez polecenie ping. Program klienta TFN zazwyczaj nosi nazwę tribe.c, a demonem jest td.c

STACHELDRAHT

Stacheldraht (niem. Drut kolczasty) to narzędzie DDoS, które pojawiło się w sierpniu 1999 r. i łączy w sobie cechy Trinoo i TFN. Zawiera również niektóre zaawansowane funkcje, takie jak szyfrowana komunikacja atakujący-mistrz i automatyczne aktualizacje agentów. Stacheldraht wykorzystuje architekturę klient / serwer podobną do Trinoo. Program obsługi nasłuchuje na porcie TCP 16660 dla poleceń klienta (intruza), a agenci nasłuchują na porcie TCP 65000 dla poleceń z programu obsługi. Odpowiedzi agenta na procedurę obsługi wykorzystują komunikaty odpowiedzi echa ICMP. Możliwe ataki są podobne do ataków TFN; mianowicie powódź ICMP, powódź SYN, powódź UDP i ataki smerfowe. Polecenia wymiany Trinoo i TFN w postaci zwykłego tekstu. Trinoo, oparte na protokole TCP, podlega również częstym atakom TCP, takim jak przejęcie sesji. Stacheldraht usuwa te niedociągnięcia, stosując szyfrującego klienta telnet. (Telnet podobnie jest terminem Stacheldraht.) Klient używa kryptografii z tajnym kluczem. Sieć Stacheldraht obejmuje wiele programów. Atakujący używa klienta szyfrującego o nazwie telnetc / client.c do sterowania jednym lub kilkoma programami

obsługi. Program obsługi nosi nazwę mserv.c, a każdy moduł obsługi może kontrolować do 1000 agentów. Oprogramowanie agenta, leaf / td.c, koordynuje atak na jedną lub więcej ofiar na polecenie przewodnika.

TFN2 K.

Tribe Flood Network 2 K (TFN2 K) został wydany w grudniu 1999 roku i jest przeznaczony dla serwerów UNIX i Windows NT. TFN2K jest złożonym wariantem oryginalnego TFN z funkcjami zaprojektowanymi specjalnie w celu:

* Utrudnij rozpoznawanie i filtrowanie ruchu TFN2K
* Zdalne wykonywanie poleceń
* Ukryj prawdziwe źródło ataku za pomocą fałszowania adresów IP
* Transportuj ruch TFN2K przez wiele protokołów transportowych, w tym UDP, TCP i ICMP
* Zmieszaj próby zlokalizowania innych węzłów w sieci TFN2K, wysyłając pakiety „wabiące”

TFN2 K, podobnie jak TFN, może zużywać całą przepustowość systemu, zalewając zaatakowaną maszynę danymi. Jednak TFN2 K, w przeciwieństwie do TFN, obejmuje również ataki zaprojektowane w celu awarii lub wprowadzenia niestabilności w systemach poprzez wysyłanie zniekształconych lub nieprawidłowych pakietów, takich jak te znalezione w atakach Teardrop i Land. TFN2K wykorzystuje architekturę serwera klienta, w której pojedynczy klient wydaje polecenia jednocześnie do zestawu agentów TFN2K. Następnie agenci przeprowadzają ataki DoS na ofiarę (ofiary). Oprogramowanie agenta jest instalowane na komputerze, który został już przejęty przez atakującego.

SHAFT

Trinoo, TFN / TFN2 K i Stacheldraht były pierwszymi i prawdopodobnie najlepiej zbadanymi narzędziami DDoS. Oczywiście pojawiły się inne narzędzia, które stały się coraz bardziej złożone, ale te wczesne narzędzia pozostają dostępne, a niektóre systemy pozostają podatne na te formy ataku. Na przykład w listopadzie 1999 r. Stało się dostępne narzędzie Shaft DDoS. Sieć Shaft wygląda koncepcyjnie podobnie do sieci Trinoo z programami obsługi klienta zarządzającymi (shaftmaster), które z kolei zarządzają programami agentów (shaftnode). Podobnie jak Trinoo, komunikacja handler-agent korzysta z protokołuUDP, z programami obsługi nasłuchującymi na porcie 20433 i agentami nasłuchującymi na porcie 18753. Klient komunikuje się z programem obsługi przez telnetting do portu TCP 20432. Sam atak jest zalewaniem pakietów atak, a klient kontroluje rozmiar zalewanych pakietów i czas trwania ataku. Jedną sygnaturą Shaft jest to, że numer kolejny dla wszystkich pakietów TCP wynosi zawsze 0 × 28374839.

HTTP ATAK APACHE

W sierpniu 2000 r. po raz pierwszy wykryto atak DDoS na serwery Apache Web. W ataku wykorzystano lukę, w wyniku której adres URL wysłany na serwer Apache zawierający tysiące ukośników (/) wprowadziłby serwer w stan, który pochłonąłby ogromną ilość czasu procesora. Ten konkretny atak został zainicjowany przez ponad 500 komputerów z systemem Windows o zaatakowanym zabezpieczeniu i prawdopodobnie byłby skuteczny przeciwko serwerom WWW Apache przed wersją 1.2.5.

TRINITY

We wrześniu 2000 r. Zgłoszono nowe narzędzie DDoS o nazwie Trinity. Trinity jest w stanie przeprowadzić kilka rodzajów ataków powodziowych na miejscu ofiary, w tym ACK, fragment, RST, SYN, UDP i inne powodzie. Oprogramowanie agenta Trinity musi zostać umieszczone w systemach

Linux zagrożonych przepełnieniem bufora. Kod binarny agenta zwykle znajduje się w /usr/lib/idle.so. Jednak komunikacja od przewodnika lub intruza do agenta odbywa się za pośrednictwem Internet Relay Chat (IRC) lub oprogramowania do przesyłania wiadomości ICQ w America Online. Podczas gdy atakujący musi śledzić adresy IP zainfekowanych systemów za pomocą Trinoo i TFN, wszyscy agenci Trinity zgłaszają się atakującemu, pojawiając się w tym samym pokoju czatu. Oryginalne raporty mówiły, że agent Trinity komunikował się kanałem IRC o nazwie # b3eblebr0x; inne kanały IRC prawdopodobnie również są wykorzystywane do DDoS. IRC korzysta z portów TCP 6665 do −6669, a Trinity wydaje się używać portu 6667. Ponadto plik binarny o nazwie / var / spool / uucp / uucico jest programem typu backdoor, który nasłuchuje połączeń TCP na porcie 33270; atakujący łączący się z tym portem i podający hasło! @ # osiągnie rootkit w systemie, którego dotyczy luka.

SUBSEVEN

Oprogramowanie Zombie nie zawsze jest dystrybuowane przez osobę atakującą wykorzystującą lukę w zabezpieczonym systemie. Rzeczywiście bardzo często winowajcą jest użytkownik. Konie trojańskie są często mechanizmem dystrybucji kodu zombie. Na przykład oprogramowanie SubSeven jest wirusem typu backdoor. SubSeven często dostaje się do systemu użytkownika, ponieważ jest dystrybuowany w ramach programów dostępnych za pośrednictwem sieci Usenet i innych witryn internetowych, takich jak niektóre gry lub programy pornograficzne (np. SexxxyMovie.mpeg.exe). Potencjalni napastnicy często skanują dziś systemy komputerowe, szczególnie systemy domowe podłączone do Internetu za pośrednictwem DSL lub modemu kablowego, w poszukiwaniu obecności SubSeven, co zapewnia potencjalne backdoor do systemów użytkowników; administratorzy systemów uczą się również skanować w poszukiwaniu tego niebezpiecznego programu we własnych systemach.

MYDOOM

Powyższy opis niektórych pierwszych narzędzi DDoS ma na celu ukazanie wczesnej linii bazowej, z której wyewoluowały późniejsze narzędzia, z których wiele jest po prostu odmianą wczesnych narzędzi. Mydoom (akaW32.MyDoom@mm i inne aliasy) to przykład ataku DoS za pośrednictwem robaka pocztowego, uruchomionego po raz pierwszy w 2004 r. Mydoom pojawia się jako wiadomość e-mail z pewnego rodzaju błędną wiadomością w temacie (np. „Błąd” lub „Awaria systemu poczty”). Co ciekawe, wiadomość e-mail można przygotować w kilku różnych językach, w tym w języku angielskim, francuskim i niemieckim. Wiadomość e-mail zawierała załącznik, który, jeśli zostanie wykonany, przekazał robaka na adresy znalezione w różnych plikach w systemie lokalnym, w tym w książce adresowej. Robaka można również skopiować do folderów współdzielonych w witrynach sieci peer-to-peer użytkownika. Wczesne wersje Mydoom zawierały ładunek, który mógłby zainicjować atak DoS przeciwko SCO Group 1 lutego 2004 r .; Grupa SCO była niepopularna, ponieważ w pozwie o wartości 1 miliarda dolarów twierdziła, że kilka dystrybucji Linuksa narusza zasoby intelektualne UNIX SCO. Następnie wydano inne warianty Mydoom, w tym wersję zastosowaną w atakach na Koreę Południową i Stany Zjednoczone w lipcu 2009 r., Która obejmowała uruchomienie botnetu.

LOIC, HOIC i HULK.

Innym wariantem tego rodzaju ataków jest działo Low Orbit Ion Cannon (LOIC). Zaprojektowany do użycia jako test obciążenia sieci, może być również wdrożony jako narzędzie DoS lub DDoS. LOIC działa w zasadzie, zalewając cel pakietami TCP i UDP, aby dowiedzieć się, czy routery potrafią obsłużyć obciążenie i jak zareagują - czy też przejmą całą przepustowość. Oryginalnie napisany w języku C#, pojawił się również wariant JavaScript (LS LOIC) i wersja Web (Low OrbitWeb Cannon). LOIC był szeroko wykorzystywany przez haktywistyczny kolektyw Anonymous. High Orbit Ion Cannon (HOIC) to modyfikacja LOIC. Ma łatwy w obsłudze graficzny interfejs użytkownika, który pozwala atakującym określić cele i skrypty wspomagające, aby kierować wiele stron na docelowym serwerze, podobnie jak strzelba zamiast karabinu. Ustawienie intensywności określa liczbę żądań na sekundę (2 / s dla niskiego

i 8 / s dla wysokiego). HTTP Unbearable Load King (HULK) to odmiana innych narzędzi, które bombardują serwer WWW ogromną liczbą pakietów. Jednak większość wcześniejszych narzędzi wysyła żądania TCP SYN lub inne przewidywalne pakiety, co pozwala zaporze i / lub serwerowi wykryć atak i zamontować obronę. HULK generuje unikalny, nieprzewidywalny zestaw żądań zaprojektowany w celu udaremnienia obrony w oparciu o rozpoznawanie wzorców i filtrowanie pakietów.

ODMOWA USŁUGI PRZY UŻYCIU OPROGRAMOWANIA EXPLOITED

Omawiane narzędzia wykorzystują wspólne podejście DoS: osoba atakująca wykorzystuje lukę w potencjalnej ofierze i wykorzystuje ten system do przeprowadzania ataków na zamierzoną ofiarę. Późniejsze rundy ataków DDoS używają jednak kodu, który jest powszechnie dostępny i który ma znane luki w zabezpieczeniach. I zbyt często luki są wykorzystywane po wydaniu łatki do ich usunięcia, ale są ignorowane przez niektórych administratorów systemu. Przykładem jest seria takich wydawnictw w połowie 2001 roku. W maju 2001 r. w usłudze indeksowania Microsoft IIS odkryto exploit przepełnienia bufora. W połowie czerwca Microsoft wydał biuletyn bezpieczeństwa ostrzegający przed tym administracyjnym skryptem (pliki .ida) i kwerendami danych internetowych (pliki .idq) ,że nie sprawdzały poprawnie granic. Tak się składa, że wydaje się, że większość serwerów IIS nie otrzymała łatki i zasadniczo każdy niezałatany serwer IIS stał się zombie DDoS.

CODE RED

W lipcu 2001 r. eEye Digital Security i kilka innych organizacji zajmujących się bezpieczeństwem w Internecie zobaczyło alarmującą liczbę skanów portu 80 w Internecie. W końcu odkryli coś, co stało się znane jako Code Red Worm. Code Red miał trzy odrębne fazy. Faza propagacji nastąpiła podczas pierwszych 19 dni miesiąca. Podczas tej fazy atakujący system skanował systemy docelowe na porcie TCP 80 i wysłał specjalnie spreparowane żądanie HTTP GET, które wykorzystało przepełnienie bufora IIS (nawet jeśli usługa indeksowania nie jest uruchomiona). Typowy wpis dziennika może
Pojawia się jako:

```
211.5.255.44 - - [16 / sie / 2001: 11: 30: 49 -0400] „GET
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
N
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
N
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN% u9090% u685
8% ucbd3% u7801u9090% u6858% ucbd3% u7801% u9090% u6858% ucbd3% u7801% u9090%
u9090% u8190% u00c3% u0003% u8b00% u531b% u53ff% u0078% u0000% ”400
```

Kiedy exploit się powiedzie, robak uruchomił się w pamięci RAM zainfekowanego serwera i stworzył 99 nowych wątków, aby zaatakować quasi-losowy zestaw adresów IP. Jeśli natywna wersja językowa wykorzystywanego serwera jest w języku angielskim, pagery internetowe serwera zostały zniekształcone komunikatem „Witamy na stronie http://www.worm.com! Zhakowany przez Chińczyków! ”Ta wiadomość pozostanie aktywna przez 10 godzin, a następnie zniknie. Faza powodziowa miała miejsce w dniach 20–27 dnia miesiąca. To wtedy naprawdę miał miejsce atak; codziennie od 20:00 do 23:59 UTC, zaatakowane serwery wysłały pakiety 100 KB na adres IP 198.137.240.91, który wcześniej był przypisany do www.whitehouse.gov. (Po odkryciu działań Code Red adres IP www.whitehouse.gov został zmieniony z adresu docelowego.) Dni od 28 do 31 miesiąca były fazą zakończenia, kiedy robak się uśpił. Code Red był stosunkowo nieszkodliwy w porównaniu z tym, czym mógł być; raz zasnął, robak spał, chociaż można go było ponownie obudzić. Usunięcie robaka z pamięci RAM wymagało jedynie ponownego uruchomienia komputera, a łatka od Microsoft zapobiegałaby dalszej infekcji. Nawiasem mówiąc, chociaż można wykorzystać tylko serwery IIS, wpłynęło to również na wiele innych urządzeń nasłuchujących na porcie 80. Na przykład routery Cisco

600 DSL i urządzenia HP JetDirect nasłuchują na porcie 80 i ulegną awarii, gdy otrzymają pakiet przepełnienia bufora. W Internecie istniały trzy różne warianty Code Red, wszystkie działały zgodnie z opisem. W sierpniu 2001 r. pojawiło się kilka nowych wariantów o nazwie Code Red II. W przeciwieństwie do Code Red, Code Red II nie zniszczył stron internetowych ani nie zainicjował ataku DDoS na żadną witrynę. Zamiast tego robak był destrukcyjny, instalował backdoory na zainfekowanych serwerach, zmieniał wiele ustawień rejestru, instalował wersję explorer.exe konia trojańskiego (Windows Explorer) i wyłączał narzędzie System File Checker (SFC). Robak rozprzestrzeniał się również szybko, wykorzystując do 300 wątków jednocześnie szukających innych systemów do zainfekowania.

NIMDA.

Kolejna ewolucja pojawiła się we wrześniu 2001 roku i została nazwana NIMDA. NIMDA (admin wstecz) był wyjątkowy, ponieważ wykorzystywał wiele słabych punktów w kodzie Microsoft, a mianowicie IIS, Internet Explorer (IE) i interfejs aplikacji komunikatów (MAPI). W rezultacie NIMDA miał cztery wyraźne propagacje wektorów:
1. IIS. Po znalezieniu serwera WWW atakujący próbował wykorzystać różne luki w IIS, w tym sadmind IIS, root.exe Code Red II lub inny program typu backdoor, lub IIS Directory Traversal. Jeśli się powiedzie, atakujący użył Trivial File Transfer Protocol (tftp) z cmd.exe, aby wysłać kod robaka (admin.dll) do ofiary.
2. Przeglądarka internetowa. Robak na zainfekowanym serwerze utworzył swoją kopię w pliku o nazwie readme.eml. Robak zmienił również każdy plik treści WWW w zainfekowanej witrynie za pomocą małego kodu JavaScript wskazującego ten plik. Gdy użytkownik przejrzał serwer zainfekowany Web, kod JS zainfekowanej strony został aktywowany i plik readme.eml został pobrany. Wrażliwe wersje Internet Explorera automatycznie wykonałyby ten plik, podczas gdy większość innych przeglądarek nie.
3. Email. NIMDA wysłał się na wszystkie adresy e-mail znalezione w InBox i książce adresowej zainfekowanego serwera w zakodowanym MIME pliku o wielkości 56 KB o nazwie readme.exe. Plik zawierał sekcję „audio / x-wav", która zawierała robaka. Klienci poczty e-mail używający przeglądarki IE 5.1 lub wcześniejszej do wyświetlania HTML automatycznie wykonają załącznik, jeśli wiadomość zostanie otwarta lub wyświetlona w podglądzie.
4. Udziały sieciowe. W zainfekowanym systemie robak skopiował się do wszystkich lokalnych katalogów hosta ofiary i do wszystkich otwartych, zapisywalnych udziałów sieciowych. Robak ustawiał również udziały na hoście ofiary.
Ponadto konto GUEST w zainfekowanym systemie zostało aktywowane i stało się członkiem grupy Administrator. (Co ciekawe, po lecie rosnącej liczby robaków DDoS prawie cała taka aktywność przestała istnieć po 11 września na wiele miesięcy.) Przez lata ataki DDoS trwały nadal, ale ma to podwójny cel. Niektóre ataki DDoS mają na celu znokautować serwer lub sieć z sieci
sposób, mianowicie przez zassanie całej przepustowości lub innych zasobów. Inne ataki wykorzystują jednak obronę strony docelowej przed sobą; wykonując rozpoznanie, aby zrozumieć, w jaki sposób witryna zareaguje na różne bodźce, atakujący może faktycznie wysłać spreparowany zestaw pakietów do strony docelowej, co spowoduje, że cel sam się ograniczy przepustowość i / lub dopuszczalne adresy źródłowe.

OBRONA PRZED ATAKAMI DDoS.

Podobnie jak w przypadku ataków DoS, strona nie może samodzielnie bronić się przed atakami DDoS. Członkowie społeczności internetowej muszą współpracować, aby chronić każdą witrynę przed staniem się źródłem ataków lub przekazywaniem ataków. W tej sekcji omówiono niektóre sposoby zapobiegania rozprzestrzenianiu się ataków DDoS poprzez ograniczenie dystrybucji narzędzi i ograniczenie rozprzestrzeniania się szkodliwych pakietów ataków. Chociaż nie zostało to tutaj szczegółowo omówione, należy zwrócić uwagę na reakcje na atak DDoS. Jak omówiono później, ofiary

takiego ataku powinny prowadzić szczegółowe dzienniki wszystkich podejmowanych działań i wykrytych zdarzeń. Dzienniki te mogą okazać się nieocenione w zrozumieniu ataku, zapobieganiu innym atakom w pierwotnym celu i innych oraz w działaniach organów ścigania w celu wyśledzenia sprawców.

DZIAŁANIA UŻYTKOWNIKA I ADMINISTRATORA SYSTEMU

Należy podjąć następujące kroki, aby zminimalizować ryzyko, że dany system zostanie naruszony i zaatakowany lub użyty jako odskocznia do atakowania innych:
1. Bądź na bieżąco z lukami w zabezpieczeniach dla całego sprzętu, systemów operacyjnych oraz aplikacji i innego oprogramowania witryny. To brzmi jak zadanie herkulesowe, ale niezbędne jest zabezpieczenie sieci. Zastosuj łatki i aktualizacje tak szybko, jak to możliwe. W miarę możliwości ujednolicaj określony sprzęt, systemy operacyjne i oprogramowanie, aby pomóc w rozwiązaniu problemu.
2. Użyj oprogramowania zapory hosta na stacjach roboczych, aby wykryć atak.
3. Często monitoruj systemy w celu przetestowania pod kątem znanych luk w systemie operacyjnym. Regularnie sprawdzaj, które porty TCP / UDP są używane, używając komendy netstat -a; każdy otwarty port powinien być powiązany ze znaną aplikacją. Wyłącz wszystkie nieużywane aplikacje.
4. Regularnie monitoruj dzienniki systemowe i szukaj podejrzanych działań.
5. Użyj dostępnych narzędzi do okresowego audytu systemów, w szczególności serwerów, aby upewnić się, że nie wystąpiły nieautoryzowane / nieznane zmiany w systemie plików, rejestrze, bazie danych kont użytkowników i tak dalej.
6. Każdy system kliencki musi korzystać z oprogramowania antywirusowego, które stale się aktualizuje, aby być na bieżąco z ciągle zmieniającym się krajobrazem zagrożeń. Skuteczne narzędzia anty-malware obejmują integrację z przeglądarkami w celu automatycznego blokowania dostępu do stron internetowych, o których wiadomo, że zawierają niebezpieczny kod. Takie narzędzia integrują się również z klientami e-mail, aby blokować automatyczne otwieranie załączników. Użytkownikom nie należy zezwalać na wyłączanie oprogramowania antywirusowego.
7. Nie pobieraj oprogramowania z nieznanych, niezaufanych stron. Jeśli to możliwe, poznaj autora kodu. Co więcej, pobierz kod źródłowy, przejrzyj go i skompiluj w wiarygodnym systemie zamiast pobierać pliki binarne lub pliki wykonywalne.
8. Bądź na bieżąco i przestrzegaj zaleceń NIST, US-CERT, laboratoriów antywirusowych, dostawców sprzętu i oprogramowania oraz innych źródeł najlepszych praktyk.

DZIAŁANIA W SIECI LOKALNEJ

Nawet jeśli użytkownicy zablokują swoje systemy, aby żadna luka nie została niezabezpieczona i żadna ekspozycja nie była chroniona, sama sieć lokalna nadal może być zagrożona. Lokalni menedżerowie sieci i administratorzy sieci mogą podjąć kilka kroków w celu ochrony wszystkich swoich użytkowników, a także reszty społeczności internetowej:
1. Każda sieć podłączona do Internetu powinna przeprowadzić filtrowanie adresu wyjściowego na routerze. Filtrowanie wyjściowe oznacza, że router powinien sprawdzić pole Adres źródłowy każdego wychodzącego pakietu IP wysłanego do Internetu, aby upewnić się, że identyfikator NET odpowiada identyfikatorowi NET w sieci. Historycznie zapory ogniowe były używane do ochrony sieci przed atakami ze świata zewnętrznego. Ale te ataki pochodzą skądś, więc strony powinny również używać zapory ogniowej do ochrony świata zewnętrznego.
2. Sieci powinny blokować przychodzące pakiety adresowane na adres rozgłoszeniowy (all-one HOST ID). Nie ma uzasadnionego powodu, aby zewnętrzne urządzenie sieciowe wysyłało komunikat rozgłoszeniowy do każdego hosta w sieci.
3. Aby zapobiec używaniu witryny jako punktu wzmocnienia transmisji, wyłącz funkcję Directed Broadcast na routerze, chyba że jest to absolutnie niezbędne. Jeśli jest to konieczne, ponownie sprawdź sieć, aby sprawdzić, czy nie ma lepszego sposobu lub czy zasięg transmisji można

zminimalizować. Nawet tam, gdzie użyteczne są transmisje bezpośrednie, zwykle są one potrzebne tylko w przedsiębiorstwie i nie są wymagane dla hostów na zewnątrz.
4. RFC 1918 definiuje trzy bloki w przestrzeni adresów IP, które są zarezerwowane dla prywatnych sieci IP; adresy te nie powinny być kierowane przez Internet. Atakujący często używają fałszowania adresów IP, zazwyczaj za pomocą jednego z prywatnych adresów RFC 1918 lub jednego z innych zarezerwowanych adresów. Zapory ogniowe powinny natychmiast odrzucić każdy pakiet zawierający dowolny RFC 1918 lub zastrzeżony adres IP w polu Adres źródłowy lub Adres docelowy; takie pakiety nigdy nie powinny być wysyłane do Internetu.
5. Zablokuj wszystkie nieużywane porty aplikacji w zaporze, w szczególności takie porty jak IRC (6665–6669 / tcp) i te, o których wiadomo, że są powiązane z oprogramowaniem DDoS.
6. Użyj stanowych zapór ogniowych, które mogą lepiej badać pakiet w kontekście całej wymiany pakietów. Bezstanowe zapory ogniowe patrzą tylko na pakiety zgodnie z prostym zestawem reguł, ale nie są świadome całkowitego ruchu pakietów w sieci (np. Filtr pakietów bezstanowych może przekazywać pakiet odpowiedzi echa ICMP, który ma zostać wysłany, ponieważ reguły na to pozwalają; filtr pakietów stanowych przekaże pakiet tylko wtedy, gdy reguła na to zezwoli i pojawi się odpowiednie żądanie echa ICMP).
7. Użyj funkcji wykrywania włamań i zapobiegania włamaniom, aby chronić sieć. Na przykład osobiste oprogramowanie zapory może być zainstalowane na każdej stacji roboczej, aby pomóc wykryć atak na pojedyncze systemy; ta strategia jest szczególnie przydatna w witrynach, które mają dużą liczbę systemów przed zaporą ogniową (np. uczelnie). To nie przypadek, że tak wiele demonów znajduje się na komputerach uniwersyteckich i uniwersyteckich, które zostały zniszczone (tj. przejęte przez hakerów).
8. Regularnie monitoruj aktywność sieci, aby szybko wykryć aberracje w ruchu.
9. Poinformuj użytkowników o zdarzeniach, na które należy uważać w ich systemach, oraz o tym, jak zgłaszać wszelkie nieprawidłowości, które mogłyby wskazywać, że ktoś lub coś sfałszowało ich system. Edukuj dział pomocy technicznej i wsparcie techniczne, aby pomóc użytkownikom, którzy składają takie raporty. Posiadaj system gromadzenia danych wywiadowczych w organizacji, aby takie raporty mogły być koordynowane centralnie w celu wykrycia trendów i opracowania odpowiedzi.
10. Postępuj zgodnie z procedurami NIST, US-CERT i innymi najlepszymi praktykami.

DZIAŁANIA DOSTAWCY USŁUG INTERNETOWYCH

Dostawcy usług internetowych dają ostatnią nadzieję na pokonanie rozprzestrzeniania się ataku DDoS. Chociaż dostawca usług internetowych nie może wziąć odpowiedzialności za blokowanie systemów hosta każdego klienta, dostawcy usług internetowych mają i powinni przyjąć odpowiedzialność za zapewnienie, że ich sieć nie przenosi pakietów zawierających oczywiście „złe” pakiety. Niektóre kroki, które mogą podjąć dostawcy usług internetowych, to:
1. Jak wspomniano, osoby atakujące zwykle wykorzystują fałszowanie adresów IP przy użyciu prywatnego adresu RFC 1918 lub innego adresu zastrzeżonego. O dziwo, wielu dostawców usług internetowych kieruje te pakiety. Rzeczywiście, w ich tablicy routingu nie ma wpisu informującego, gdzie wysłać pakiety; przekazują je jedynie domyślnemu dostawcy usług internetowych. Każdy pakiet zawierający dowolny RFC 1918 lub zarezerwowany adres IP w polu Adres źródłowy IP lub Adres docelowy powinien zostać natychmiast odrzucony.
2. Wykonaj filtrowanie adresu wejściowego (i wyjściowego). Filtrowanie Ingress oznacza, że dostawcy usług internetowych powinni sprawdzać każdy przychodzący pakiet do swojej sieci z witryny klienta i sprawdzać pole Adres źródłowy IP, aby upewnić się, że identyfikator NET odpowiada identyfikatorowi NET ID przypisanemu do tego klienta. Wykonanie tego będzie wymagało dodatkowej konfiguracji na routerze i może nawet spowodować niewielki spadek wydajności, ale kompromis jest z pewnością wart wysiłku. Dostawcy usług internetowych powinni również przeprowadzić filtrowanie wychodzące, aby sprawdzić swoje pakiety wychodzące do dostawców usług nadrzędnych i równorzędnych.
3. Wyłącz transmisje IP.
4. Zwróć szczególną uwagę na głośne systemy (serwery) i klientów.

5. Edukuj klientów na temat bezpieczeństwa i współpracuj z nimi, aby chronić siebie.
Większość społeczności ISP wykonuje co najmniej niektóre z tych kroków. Użytkownicy powinni nalegać, aby ich dostawcy usług internetowych zapewniali przynajmniej te zabezpieczenia i nie powinni robić interesów z tymi, którzy ich nie zapewniają. RFC 3013 i północnoamerykańska grupa operatorów sieci (NANOG) są dobrym źródłem informacji dla dostawców usług internetowych

WYKORZYSTYWANE DZIAŁANIA OBRONNE OPROGRAMOWANIA

Istnieje wiele kroków obronnych, które można podjąć w celu uniknięcia lub złagodzenia problemów z powodu ataków Code Red / NIMDA, które wykorzystują oprogramowanie. Kilka z tych zaleceń budzi kontrowersje z powodu ich domniemanego bojkotu produktów określonego dostawcy.
* Jeśli używasz IIS, rozważ użycie oprogramowania serwera alternateWeb. Jeśli korzystanie z IIS jest niezbędne, utrzymuj IIS i system operacyjny w najnowszej wersji łaty. Na przykład zbiorcza łatka Microsoft IIS nie czyści systemu z wielu backdoorów wykorzystywanych do exploitów.
* Jeśli używasz Internet Explorera, rozważ użycie alternatywnego oprogramowania przeglądarki. Jeśli musisz użyć IE, zabezpiecz go przed automatycznym wykonaniem MIME. Należy zauważyć, że jeszcze we wrześniu 2012 r. US-CERT zgłaszał niezałatane luki w zabezpieczeniach IE6, IE7, IE8 i IE9, a niektóre organy (np. Rząd Niemiec) odradzały stosowanie jakiejkolwiek wersji IE.
* Wyłącz wszystkie nieużywane konta na serwerach i innych systemach. W szczególności włącz konto Gość lub dostęp anonimowy tylko wtedy, gdy jest to absolutnie konieczne.
* Wyłącz JavaScript, Java i ActiveX w przeglądarkach, chyba że jest to absolutnie konieczne.
* Nie wykonuj ani nie otwieraj żadnych załączników wiadomości e-mail, chyba że są oczekiwane, znane i zweryfikowane.
* Używaj najbardziej aktualnych plików sygnatur antywirusowych.
* Usuń powiązanie udostępniania plików i drukarek z TCP / IP. W niektórych przypadkach będzie to wymagało instalacji NetBEUI do udostępniania plików i drukarek.

INNE NARZĘDZIA W TRAKCIE OPRACOWYWANIA LUB ROZPATRYWANIA

Odpowiedzi na ataki DDoS nie ograniczają się do wymienionych wyżej kroków obronnych. Rzeczywiście, proaktywne reakcje na zapobieganie atakom DDoS i ich wykrywanie są aktywnym obszarem badań. Te propozycje są jedynie próbkami niektórych sposobów radzenia sobie z atakami DDoS; pierwszy dodaje nowy sprzęt do Internetu, drugi wymaga zmiany oprogramowania serwera WWW i klienta, a dwa ostatnie wymagają stopniowej zmiany oprogramowania odpowiednio we wszystkich routerach i hostach internetowych. Aktualizacja przeglądarek internetowych jest prawdopodobnie najbardziej praktyczną strategią, mimo że w dystrybucji znajdują się miliony egzemplarzy; zdecydowana większość pochodzi tylko od kilku dostawców, a użytkownicy i tak często dokonują aktualizacji.

MONITOR RUCHU ROZPROSZONEGO

Jedną z proponowanych metod jest zbadanie sieci na poziomie ISP i zbudowanie pewnego rodzaju inteligentnego, rozproszonego monitora ruchu sieciowego; w pewnym sensie byłoby to jak IDS dla Internetu. Dostawcy usług internetowych, punkty peering i / lub główne serwery hostów miałyby sprzęt monitorujący ruch korzystający z IP i Internetu do komunikacji, podobnie jak dzisiejsze protokoły routingu. Każdy węzeł bada pakiety i ich zawartość, wykonując statystyczną analizę ruchu, aby poznać normalne wzorce. Urządzenia te miałyby wystarczającą inteligencję, aby móc wykryć zmiany w poziomie ruchu i ustalić, czy zmiany te odzwierciedlają normalny stan, czy nie. Jako przykład załóżmy, że taki sprzęt na Amazon.com miał zidentyfikować atak DoS przeprowadzony przez dostawcę usług internetowych w Gondwanaland; sieć monitorowania ruchu odcięłaby ruch do Amazona pochodzący od tego ISP tak blisko ISP, jak to możliwe. W ten sposób rozproszona sieć monitorów może wyłączyć ruch u źródła. Sprzęt musiałby być informowany o zmianach w poziomie ruchu spowodowanych

normalnymi zdarzeniami, takimi jak nowa reklama Super Bowl na YouTube lub nowy pokaz mody na stronie internetowej Victoria Secret. Sprzęt musiałby również uniemożliwić społeczności atakujących działanie pod przykrywką tych normalnych zdarzeń.

CLIENT PUZZLE PROTOCOL

RSA Laboratories zaproponowało metody kryptograficzne jako potencjalną obronę przed atakami DDoS przeciwko serwerom WWW. W tym podejściu wykorzystano protokół puzzle klienta zaprojektowany, aby umożliwić serwerom przyjmowanie żądań połączeń od legalnych klientów i blokowanie ich od atakujących. Układanka kliencka to problem kryptograficzny generowany w taki sposób, aby był zależny od czasu i informacji unikalnych dla żądania serwera i klienta. W normalnych warunkach serwer akceptuje każde żądanie połączenia od dowolnego klienta. W przypadku wykrycia ataku serwer selektywnie akceptuje żądania połączenia, odpowiadając na każde żądanie układanką. Serwer przydziela zasoby niezbędne do obsługi połączenia tylko tym klientom, którzy poprawnie reagują na łamigłówkę w określonym czasie oczekiwania TCP. Klient działający w dobrej wierze doświadczy jedynie niewielkiego opóźnienia w uzyskaniu połączenia podczas ataku, podczas gdy atakujący zużyje niewiarygodną moc obliczeniową, aby kontynuować wysyłanie liczby żądań niezbędnych do zauważalnej przerwy w działaniu w miejscu docelowym, szybko renderując atak nieskuteczny (w efekcie odwrotna DoS). Ten schemat może być skuteczny przeciwko atakowi DDoS ze strony stosunkowo małej liczby hostów, z których każdy wysyła dużą liczbę pakietów, ale może mieć ograniczoną skuteczność przeciwko atakowi o małej objętości z dużej liczby systemów lub z botnetu.

ŚLEDZENIE IP.

Niezwykłym mechanizmem, który był przedmiotem poważnych badań na początku do połowy 2000 roku, był IP Traceback. Problem z atakami DoS / DDoS polega na tym, że pakiety pochodzą z dużej liczby źródeł, a fałszowanie adresów IP maskuje te źródła. Oznaczenie śladowe w koncepcji jest stosunkowo prostym pomysłem. Każdy pakiet w Internecie przechodzi przez pewną liczbę routerów ISP. Moc przetwarzania, pamięć i pamięć są dostępne dla routerów do oznaczania pakietów z częściową informacją o ścieżce po ich przybyciu. Ponieważ ataki DoS / DDoS zazwyczaj obejmują dużą liczbę pakietów, mechanizm śledzenia nie musi oznaczać każdego pakietu, a jedynie wielkość próby, która statystycznie prawdopodobnie obejmuje pakiety ataku (np. 1 pakiet na każde 20 000 lub 0,005% ruchu IP). Ta funkcja umożliwiłaby ofierze zlokalizowanie przybliżonego źródła ataku bez pomocy zewnętrznych agencji, a nawet po zakończeniu ataku. Inna propozycja śledzenia mogłaby zdefiniować śledzenie ICMP wiadomość, która zostanie wysłana do strony ofiary, zawierająca częściowe informacje o trasie o próbkowanym pakiecie. Istnieje wiele problemów związanych ze śledzeniem, które muszą zostać rozwiązane, takich jak minimalna liczba zaznaczonych pakietów wymagana do odtworzenia ścieżki z powrotem do atakującego, faktyczny narzut przetwarzania i możliwość wykonania śledzenia podczas trwającego ataku. Ponadto każde rozwiązanie śledzenia wstecznego będzie wymagało zmiany dziesiątek tysięcy routerów w Internecie; jak skuteczne może być śledzenie w okresie stopniowego wdrażania? Zaletą jest oczywiście to, że rozwiązanie jest kompatybilne wstecz i nie ma negatywnych skutków dla użytkowników.

ŁADUNEK TOŻSAMOŚCI HOSTA

Czwarta propozycja polegała na zmodyfikowaniu adresu IP tak, aby był mniej podatny na fałszowanie adresów poprzez uczynienie protokołu mniej zależnym od pola adresu w przypadku czegoś więcej niż routingu. Na przykład ładunek tożsamości hosta (HIP) definiuje protokół wymiany kryptograficznej tożsamości hosta między dwoma komunikującymi się systemami. Ta funkcja przenosi adres IP do użytku wyłącznie jako mechanizmu przekazywania pakietów, a nie jako identyfikatora nadawcy. Zamiast tego identyfikacja nadawcy jest realizowana przez wartość tożsamości hosta, a wszystkie

protokoły wyższej warstwy są powiązane z tożsamością hosta. HIP nie jest jeszcze szeroko wdrożony, ale jest dostępny w niektórych implementacjach TCP / IP.

PROBLEMY ZARZĄDZANIA.

Jednym z największych niedociągnięć w wielu organizacjach jest to, że najwyższe poziomy zarządzania nie do końca rozumieją kluczową rolę komputerów, sieci, informacji i Internetu w życiu organizacji. Trudno wyjaśnić, że istnieje społeczność intruzów, która cały czas aktywnie pracuje nad nowymi narzędziami; a historia pokazała, że w miarę jak narzędzia stają się dojrzałe i coraz bardziej wyrafinowane, wiedza techniczna wymagana od potencjalnego napastnika spada, a liczba ataków ogólnie rośnie. Zbyt wiele firm upiera się, że „nikt nie będzie nam przeszkadzał", nie zdając sobie sprawy, że każda witryna może stać się celem tylko po to, aby tam być. Ataki DoS występują w różnych formach i mają na celu różnorodne usługi, co powoduje większą złożoność i trudność w obronie systemu. Ataki DoS należy traktować poważnie ze względu na potencjalne zagrożenie, jakie stanowią, i należy podjąć wysiłki w celu edukowania personelu operacyjnego przed takimi atakami, dokumentowania ataków DoS, jeśli takie wystąpią, oraz przeglądu dokumentacji i działań podjętych po zakończeniu incydentu . Dyskusja o tym, jakie kroki zostały podjęte, jakie działania weszły w życie i jaki był ogólny wynik, pomoże ustalić, czy przeprowadzone procedury i zastosowane techniki były najlepiej dostosowane do sytuacji. Szczery przegląd i dyskusja pomogą osiągnąć najlepsze, najszybsze i najskuteczniejsze wdrożenie zasobów. Jeśli coś świadczy o splecionej naturze Internetu, jest to obrona przed atakami DDoS. Ataki DDoS wymagają obalenia i koordynacji setek lub tysięcy komputerów, aby zaatakować kilka ofiar. Obrona przed atakami DDoS wymaga współpracy tysięcy dostawców usług internetowych i sieci klientów. Zwalczanie DDoS wymaga ciągłej staranności w blokowaniu wszystkich hostów podłączonych do Internetu, a także fundamentalnych zmian w charakterze protokołów połączeń TCP / IP. Ponadto wiele takich samych technik wykorzystywanych do wstawiania wirusów i robaków, które prowadzą do ataków DoS i DDoS, jest wykorzystywanych do wstawiania złośliwego oprogramowania typu Advanced Persistent Threat (APT). Podobnie jak w przypadku większości problemów związanych z bezpieczeństwem w Internecie, duża część rozwiązania polega na edukacji użytkowników. Należy edukować użytkowników w zakresie obecnych zagrożeń w Internecie i wpływu na odpowiednie aplikacje, co zrobić, gdy pojawi się coś podejrzanego, i jak reagować na coraz bardziej kreatywnych atakujących. Świat, w którym każdy ma swój własny komputer, urządzenie mobilne o niewiarygodnej inteligencji i atmosferę korporacyjną „zabierz ze sobą własne urządzenie" (BYOD), wymaga, aby każdy użytkownik w przedsiębiorstwie był potencjalnie narażony na awarie i musi być odpowiednio edukowany .