Spam, pishing i trojany: ataki mające na celu oszukać

Niechciany adres e-mail i inne szkodniki: kwestia bezpieczeństwa.

Tu omówimy trzy dziwnie nazwane zagrożenia bezpieczeństwa komputera: spam, phishing i kod konia trojańskiego. Spam to niechciany komercyjny e-mail. Wyłudzanie informacji to wykorzystanie oszukańczych niechcianych wiadomości e-mail w celu uzyskania ryb w celu uzyskania poufnych informacji drogą elektroniczną. Kod konia trojańskiego, termin wywodzący się od konia trojańskiego, to oprogramowanie zaprojektowane w celu uzyskania nieautoryzowanego dostępu do systemów poprzez udawanie legalnych aplikacji. Przedstawiamy zagrożenia związane ze spamem, phishingiem i trojanami, a także ich ograniczanie. Zagrożenia te mogą mieć dziwne nazwy, ale nie są obce tym, których działania podważają korzyści technologii informatycznych. Każdego roku, przynajmniej przez ostatnie trzy lata, US Internal Revenue Service (IRS) musiała ostrzegać opinię publiczną przed oszustwami e-mailowymi. Fakt, że IRS stwierdza, że agencja nigdy nie korzysta z poczty e-mail, SMS-ów ani kanałów mediów społecznościowych w celu komunikowania się z podatnikami, jest smutnym komentarzem dla naszego społeczeństwa, ponieważ nie ma dobrego powodu, aby tak było. W końcu agencja zezwala na elektroniczne składanie rocznych deklaracji podatkowych, a każdego dnia setki milionów ludzi na całym świecie wykonują swoje rachunki bankowe i płacą rachunki przez Internet z zachowaniem względnego bezpieczeństwa. Istnieje technologia zapewniająca bezpieczeństwo poczty e-mail. Pod wieloma względami ten rozdział jest katalogiem tego, co się stało, ponieważ nie wdrożyliśmy technologii skutecznie.

Pospolite elementy.

Każde z tych zagrożeń różni się pod pewnymi względami, ale wszystkie trzy mają pewne ważne elementy wspólne; po pierwsze, a przede wszystkim używają oszustwa. Zagrożenia te polegają na łatwowierności użytkowników komputerów i łatwiej osiągają swoje cele, gdy użytkownicy są źle wyszkoleni i źle poinformowani (aczkolwiek wspomagani i wspomagani, w niektórych przypadkach, z powodu złego projektu systemu i złego zarządzania usługami, takimi jak łączność szerokopasmowa) . Po drugie, wszystkie trzy ataki są włączane przez usługi systemowe, które są powszechnie wykorzystywane do legalnych celów. Chociaż to samo można powiedzieć o wirusach komputerowych - są one kodem, a komputery są zbudowane do uruchamiania kodu - trzy zagrożenia, które są przedmiotem naszych badań, zwykle działają na wyższym poziomie, warstwa aplikacji modelu Open Systems Interconnection (OSI) . Rzeczywiście, fakt ten może przyczynić się do zakresu ich wdrożenia - zagrożenia te można przeprowadzić przy stosunkowo niewielkich umiejętnościach technicznych, opierając się bardziej na umiejętnościach związanych z inżynierią społeczną niż z kodowaniem. Na przykład każdy, kto ma połączenie z Internetem i program pocztowy, może wysyłać spam. Ten spam może rozprzestrzeniać gotowego trojana. Korzystając z zestawu narzędzi pełnego skryptów, możesz dodać stronę internetową z formularzem wejściowym do swojego portfolio i wyłudzić dane osobowe w celu ich gromadzenia i nadużyć. Innym powodem wspólnego rozważenia tych trzech zjawisk jest fakt, że często łączą się one w exploity w świecie rzeczywistym. Te same techniki masowego wysyłania e-maili, które służą do wysyłania spamu, mogą zostać wykorzystane do wysyłania wiadomości rozprzestrzeniających kod trojana. Kod trojana może być wykorzystywany do wspomagania operacji phishingowych. Systemy zaatakowane przez kod trojana mogą być wykorzystywane do spamowania i tak dalej. To, co widzimy dziś w tych atakach, jest bardzo szkodliwym i kosztownym wynikiem połączenia stosunkowo prostych strategii i technik ze standardami postępowania, od głupich i nieodpowiedzialnych po bezwstydnie przestępcze. Te trzy zagrożenia mają również tę różnicę, że zostały niedocenione, gdy pojawiły się po raz pierwszy. Wszystkie trzy ewoluowały i rozszerzały się w XXI wieku. Na przykład w 2012 r. Firma Symantec poinformowała, że zagrożenia systemu operacyjnego Android (praktycznie nieznane dziesięć lat wcześniej) przeciwko urządzeniom mobilnym wzrosły

drastycznie między styczniem 2010 r. A końcem 2012 r., Z mniej niż 100 unikalnych wariantów w około 10 rodzinach do około 4500 wariantów w około 170 rodzin. Ponadto w 2012 r. w mediach społecznościowych prowadzono coraz więcej oszustw związanych z wyłudzaniem informacji (phishing), o czym nawet nie wspomniano w odpowiednim raporcie za pierwszą połowę 2006 r. Kolejny czynnik łączy te trzy zagrożenia: ich powiązanie wraz z pojawieniem się korzyści finansowych jako głównego motywatora do pisania złośliwego kodu i nadużywania łączności internetowej. Nadzieja na zarobienie pieniędzy jest głównym motorem spamu. Wyłudzanie informacji ma na celu ułatwienie oszustw w celu zdobycia poprzez kradzież danych osobowych i danych uwierzytelniających, do wykorzystania przez złodzieja lub odsprzedaży w podziemnej gospodarce. Kod trojana służy do osiągania celów zarówno spamerów, jak i sprawców ataków phishingowych. Krótko mówiąc, wszystkie trzy stanowią bardzo realne zagrożenie dla bezpieczeństwa komputerowego, dobrobytu każdej organizacji korzystającej z komputera oraz gospodarki online.

E-MAIL: LEKCJA ANATOMII.

Poczta elektroniczna odgrywa rolę w licznych zagrożeniach dla systemów informatycznych i informacyjnych. Nie tylko umożliwia spam i phishing, jest także wykorzystywany do rozprzestrzeniania kodu trojana, wirusów i robaków. Podstawowa wiedza na temat działania poczty elektronicznej pomoże zrozumieć te zagrożenia i różne opracowane środki zaradcze.

Prosty protokół transportu poczty.

Wszystkie wiadomości e-mail przesyłane przez Internet są wysyłane przy użyciu uzgodnionego standardu branżowego: Simple Mail Transport Protocol (SMTP). Każdy serwer, który mówi SMTP, może działać jako Agent Transferu Poczty (MTA) i wysyłać pocztę na i odbierać pocztę od dowolnego innego serwera, który mówi SMTP.

Opracowany w czasach, gdy zasoby komputerowe były stosunkowo drogie i zaprojektowana do działania nawet wtedy, gdy serwer przetwarzał kilkanaście lub więcej połączeń wiadomości na sekundę, konwersacja SMTP była bardzo prosta, aby była bardzo krótka. Jednak ta prostota jest zarówno błogosławieństwem, jak i przekleństwem. Przed dostarczeniem poczty odbierane są tylko dwie części informacji o tożsamości: tożsamość serwera wysyłającego, w tym przypadku example.com, oraz adres Od, w tym przypadku foo@example.com. SMTP nie ma procesu weryfikacji poprawności tych zapewnień tożsamości, więc oba identyfikatory mogą być trywialnie sfałszowane. Pozostała treść wiadomości e-mail, w tym temat i inne informacje nagłówka, są przesyłane w bloku danych i nie są uważane za znaczącą część rozmowy SMTP. Innymi słowy, nie istnieje żaden mechanizm SMTP służący do weryfikacji takich stwierdzeń, jak: „ta wiadomość pochodzi z banku i dotyczy twojego konta” lub „ta wiadomość zawiera numer śledzenia twojego zamówienia online” lub „oto biuletyn inwestycyjny, o który prosiłeś”. Jak opiszemy bardziej szczegółowo później, niektóre usługi e-mail wykonują wyszukiwanie na białej liście lub czarnej liście na adresie IP protokołu serwera wysyłającego podczas rozmowy SMTP, ale zapytania te mogą znacznie spowolnić przetwarzanie poczty, wymagając dodatkowej pojemności, aby zrównoważyć utrata wydajności. Biała lista identyfikuje zaufanych nadawców e-mail; czarna lista wskazuje te, które nie są zaufane. Utrzymanie białych list może być czasochłonne, a czarne listy mają długą historię nieścisłości i sporów prawnych. Krótko mówiąc, potrzeba prędkości tworzy system, w którym nie ma praktycznie żadnych technicznych konsekwencji dla wprowadzenia w błąd przy dostarczaniu poczty. To właśnie dlatego spamerzy byli i nadal są niezwykle skuteczni w dostarczaniu niechcianych wiadomości e-mail. SMTP jest, jak to ujął to Winston Churchill, najgorszym sposobem robienia e-maili, z wyjątkiem wszystkich innych, które zostały wypróbowane. W rzeczywistości SMTP działa niezawodnie i został szeroko wdrożony. Zastąpienie SMTP czymkolwiek lepszym oznaczałoby hurtowe przeprojektowanie całej globalnej infrastruktury

poczty elektronicznej, zadanie, które niewielu w branży było gotowych podjąć. Niektóre osoby starały się opracować rozwiązania, które mogą jeździć na istniejącej infrastrukturze SMTP, umożliwiając SMTP kontynuowanie wydajnego działania, jednocześnie dając tym, którzy go używają, opcję włączenia bardziej niezawodnych funkcji, które pomogą odróżnić legalną pocztę od spamu.

Heads-up.

Wiadomość e-mail nie może zostać dostarczona bez czegoś, co nazywa się nagłówkiem, a każda wiadomość e-mail ma jedną, część wiadomości, która nie zawsze jest wyświetlana w programie pocztowym odbiorcy, ale mimo to opisuje, skąd wiadomość pochodzi, jak została zaadresowana i jak to zostało dostarczone. Analiza nagłówka może wiele powiedzieć o wiadomości. Zastanów się, jak pojawia się komunikat w Microsoft Outlook Express. U góry widać Od, Do i Temat. Na przykład możesz zobaczyć część wiadomości, która wydaje się być od zjjimwalker8467r21@lycos.com do press@eprivacygroup.com z tematem: ∗ Masz zgodę! Jak można się domyślić, press@eprivacygroup.com nie jest prawdziwą osobą. To tylko adres, który pojawia się na stronie internetowej firmy jako kontakt dla prasy i oczywiście nikt tak naprawdę nie używał tego adresu w wniosku o kredyt hipoteczny. Adres został zebrany przez program, który automatycznie przeszukuje sieć w poszukiwaniu adresów e-mail. Gdy otworzysz tę wiadomość w klientach e-mail (np. Outlook lub Outlook Express) i użyjesz polecenia Plik / Właściwości lub odpowiednika, możesz kliknąć kartę Szczegóły, aby zobaczyć, jak wiadomość dotarła do Internetu. Pierwszą rzeczą, którą zobaczysz, jest pole oznaczone jako „nagłówki". Po przeczytaniu tego dowiesz się, że wiadomość została przekierowana przez kilka różnych serwerów e-mail. Qmail to program pocztowy firmy, który jest pierwszą instancją programu Received. Następne trzy poniżej to pośrednicy, aż dojdziesz do ostatniego, smtp-server1.cflrr.com. Jest to serwer e-mail na środkowej Florydzie (cfl) w sieci modemów kablowych Road Runner (rr), który zapewnia szybki dostęp do Internetu dla dziesiątek tysięcy gospodarstw domowych. Więc kto wysłał tę wiadomość? To bardzo trudno powiedzieć. Jak można się spodziewać, nie ma takiego adresu jak zjjimwalker8467r21@lycos.com. Najlepszym sposobem ustalenia, kto wysłał taką wiadomość spamową, jest sprawdzenie zawartości. Spam nie może się oderwać odrostów. chyba że frajerzy mają jakiś sposób na skontaktowanie się ze spamerem. Czasami jest to numer telefonu, ale w tej wiadomości jest hiperłączem do strony internetowej. Jednak klikanie linków w wiadomościach spamowych jest niebezpiecznym sposobem surfowania - znacznie bezpieczniejszą techniką, aby dowiedzieć się więcej o linkach w spamie, jest kontrola źródła wiadomości. Program Outlook Express zapewnia widok Źródło wiadomości, ale może on wyświetlać tylko zakodowaną treść i nie być czytelny w ASCII. Niektórzy klienci poczty e-mail (np. Outlook) pozwalają ustawić domyślną konwersję wszystkich wiadomości na zwykły tekst; jeśli ktoś chce zobaczyć obrazy, może je pobrać na podstawie komunikatu. Ponadto wielu klientów poczty e-mail może wyświetlić podstawowe szczegóły każdego hiperłącza po najechaniu kursorem na etykietę łącza. Jednym ze sposobów na uzyskanie dostępu do treści takich wiadomości jest przesłanie ich do innego klienta poczty e-mail, na przykład Eudora firmy Qualcomm, a następnie otwarcie pliku skrzynki pocztowej za pomocą edytora tekstu, takiego jak TextPad. Ujawnia to odwołanie http do linku, który ten spamer chce kliknąć odbiorcy. W takim przypadku frajerem, który kliknie link „Aby uzyskać zatwierdzoną kwotę, przejdź tutaj", zostanie wyświetlony formularz, który nie dotyczy kredytów hipotecznych, ale gromadzenia danych. Nie można powiedzieć, do jakiego celu zostaną wykorzystane zebrane w ten sposób dane, ale niewielkie dodatkowe sprawdzenie za pomocą poleceń ping i whois ujawnia, że serwer sieciowy gromadzący dane znajduje się w Pekinie. Szanse na ustalenie, kto go skonfigurował, są niewielkie. Standardowa procedura operacyjna polega na bardzo szybkim konfigurowaniu i usuwaniu strony internetowej, zbierając jak najwięcej danych ktoś zaczyna śledztwo. Jednak w ciągu ostatnich 10 lat zasoby przeznaczone na badanie spamerów były minimalne w porównaniu z zasobami przeznaczonymi na wysyłanie spamu. Nawet jeśli prawodawcy mogą uzgodnić,

co to jest spam i jak uznać go za nielegalny, fundusze rządowe rzadko są przeznaczane na zwalczanie spamu. Odnotowano kilka głośnych aresztowań i postępowań, często prowadzonych przez duże firmy, takie jak Microsoft i AOL, ale spamowanie pozostaje stosunkowo niewielkim ryzykiem nadużyć komputerowych. Jeśli można zidentyfikować link w spamie, usługa Better-Whois (http://betterwhois.com/) może być w stanie podać szczegółowe informacje na temat osób oficjalnie zarejestrowanych jako właściciele i administratorzy strony - pod warunkiem, że nie ukryli się za nią anonimowe firmy, takie jak GoDaddy.com, które mogą ukrywać prawdziwych właścicieli, podając anonimowy adres e-mail, za pomocą którego można próbować komunikować się z właścicielami.

SPAM ZDEFINIOWANY.

Historia spamu to saga od szmat do bogactwa, będąca jedynie uciążliwością, która stała się wielomiliardowym obciążeniem dla zasobów komputerowych na świecie. Mimo wszystkich żartów i żartów na temat spamu może być największym złodziejem zasobów komputerowych i telekomunikacyjnych od czasu wynalezienia komputerów i telekomunikacji.

Być może nie jest zaskoczeniem, że spam stał się kosztownym problemem, ponieważ spam był pierwszym zagrożeniem komputerowym na dużą skalę, którego celem była czysta korzyść. Celem większości spamu jest zarabianie pieniędzy, a pieniądze nie są w stanie zaakceptować, jeśli ludzie ich nie otrzymają. W rzeczywistości oprogramowanie antyspamowe nie wysyła spamu na serwer pocztowy, który ma długi czas reakcji; po prostu przechodzi do innych celów, które mogą odbierać wiadomości e-mail z wysoką szybkością minuty na minutę potrzebną do wygenerowania przychodu przez spam (na podstawie 1 osoby na około 100 000 faktycznie odpowiadającej na wiadomość spamową). Jeśli spam nie generuje dochodu, staje się bezcelowy, ponieważ jego wysłanie wymaga pieniędzy. Potrzebujesz dostępu do serwerów i przepustowości (za które albo musisz zapłacić, albo ukraść). Jak na ironię, kilka prostych zmian w obecnych standardach poczty e-mail może położyć kres większości spamu poprzez bardziej niezawodną identyfikację i uwierzytelnianie nadawców wiadomości e-mail, temat poruszony w dalszej części tego rozdziału.

Geneza i znaczenie (nie spam).

SPAMR jest znakiem towarowym firmy Hormel Foods od ponad 70 lat. Z powodów, które zostaną omówione za chwilę, świat zdecydował się na spam jako termin opisujący niechciane wiadomości handlowe. Jednak wielka litera SPAMR jest nadal znakiem towarowym i kojarzy SPAMR, lub zdjęcia SPAM z czymś innym niż produkt Hormel mogą stanowić poważne naruszenie prawa znaków towarowych. Specjaliści ds. Bezpieczeństwa powinni wziąć to pod uwagę. Słowo „spam" jest dopuszczalne na początku zdania o niechcianym komercyjnym e-mailu, ale spamu można używać w przypadku spamu tylko wtedy, gdy reszta otaczającego go tekstu jest pisana wielkimi literami, jak w

„TIRED OF SPAM CLUTTERING YOUR INBOX?". Użycie słowa „spam" w kontekście wiadomości elektronicznych jest szeroko stosowane wywodzi się ze szkicu komediowego w dwudziestym piątym odcinku serialu telewizyjnego BBC Latający Cyrk Monty Pythona. Po raz pierwszy nadawany w 1968 roku, przed wynalezieniem e-maila, szkic przedstawiał restaurację, w której SPAMR dominowało w menu. Kiedy postać o imieniu Pan Bun pyta kelnerkę: „Czy masz coś bez SPAMR?" odpowiada: „No cóż, jest SPAMR, jajko, kiełbasa i SPAM, nie ma w nim dużo SPAMR". Gaworzenie trwa w tym duchu, dopóki zirytowana żona pana Boka nie krzyczy: „Nie lubię SPAMR!" Jest dodatkowo zirytowana nieprzyzwoitą grupą wikingów śpiewających piosenkę, której teksty składają się prawie w całości ze słowa „SPAMR". Podobne uczucie irytacji, że ktoś naciska na ciebie coś, czego nie chcesz i nie prosiłeś o wyraźnie, pomógł uczynić „spam" odpowiednim terminem na rodzaj niechcianego komercyjnego e-maila, który może zagracać skrzynki odbiorcze i blokować serwery e-mail. W rzeczywistości pierwsze użycie spamu jako terminu nadużycia sieci nie obejmowało wiadomości e-mail.

Krwawe szczegóły spamu zostały dokładnie zbadane w 2003 r. przez Brada Templetona, byłego prezesa zarządu Electronic Frontier Foundation. Według Templetona, początki leżą w irytującym i powtarzalnym zachowaniu obserwowanym w lochach dla wielu użytkowników (znanym również jako akronim MUD, wczesny termin współdzielenia w czasie rzeczywistym dla wielu osób środowisko). Stamtąd termin spam został przeniesiony na tablice ogłoszeń - gdzie został użyty do opisania zautomatyzowanej, powtarzalnej treści wiadomości - stąd do USENET, gdzie został zastosowany do wiadomości, które zostały wysłane do wielu grup dyskusyjnych. Historia USENET i jej związek z historią spamu jest zbawienny z kilku powodów. Przede wszystkim spam prawie zabił USENET, który był kiedyś świetnym sposobem na spotkanie i komunikację z innymi użytkownikami Internetu, którzy mieli wspólne zainteresowania, niezależnie od tego, czy był to humor polityczny, czy kodowanie HTML. Grupy dyskusyjne zostały zatkane spamem do tego stopnia, że użytkownicy szukali alternatywnych kanałów komunikacji. Innymi słowy, cenny i użyteczny środek komunikacji oraz wczesna forma sieci społecznościowych na zawsze zostały skażone złym zachowaniem kilku osób, które były gotowe obnosić się z obowiązującymi standardami postępowania. Drugie połączenie spam-USENET polega na tym, że spam migrował z USENET na e-mail poprzez zbieranie adresów e-mail, technikę, która spamerzy - osoby dystrybuujące spam - stosowały następnie na stronach internetowych i innych potencjalnych źródłach adresów docelowych. Spamerzy stwierdzili, że oprogramowanie może z łatwością zautomatyzować proces czytania tysięcy postów na grupach dyskusyjnych oraz wyodrębniania lub gromadzenia dowolnych adresów e-mail, które się w nich pojawiały. Ważne jest, aby pamiętać, że chociaż dziś może się to wydawać naiwne, praktyka umieszczania własnego adresu e-mail w wiadomości wysyłanej do grupy dyskusyjnej była powszechna do połowy lat 90. XX wieku. W końcu, jeśli opublikowałeś wiadomość szukającą odpowiedzi, wówczas podanie adresu e-mail ułatwiło ludziom udzielenie odpowiedzi. Niektórym użytkownikom komputerów może być trudno wyobrazić sobie czas, w którym adresy e-mail były tak swobodnie udostępniane, ale ten czas warto pamiętać, ponieważ pokazuje, jak łatwo nadużycie systemu przez nielicznych może obniżyć jego wartość dla wielu. Zbieranie, które skutkowało otrzymywaniem spamu na adres e-mail podany w grupie dyskusyjnej publikowanej w celu legalnej komunikacji, było ogromnym postępem w nadużywaniu Internetu i znaczącym zwiastunem przyszłych wydarzeń. Trzeba było opracować skomplikowane środki zaradcze, które utrudniały swobodny przepływ komunikacji. Duża część roli, jaką pełnią grupy dyskusyjne, migruje na zamknięte fora, na których stosuje się coraz bardziej zaawansowane środki, aby zapobiec nadużyciom.

Kopanie w spam.

Około 1996 r., Gdy pierwsi użytkownicy poczty e-mail zaczęli napotykać coraz więcej niechcianych wiadomości e-mail, podjęto starania, aby dokładnie określić, jaki rodzaj wiadomości stanowi spam. Nie było to ćwiczenie akademickie, a stawka była zaskakująco wysoka. Zastosowaliśmy już jedną definicję: niechciany komercyjny e-mail (czasem określany jako UCE). Ta definicja wydaje się dość prosta, ponieważ zawiera dwa istotne punkty: spam to wiadomość e-mail, o którą ludzie nie prosili, a spam ma charakter komercyjny.

Jednak chociaż UCE ostatecznie stało się najczęściej stosowaną definicją spamu, nie zadowoliło wszystkich. Krytycy zwracają uwagę, że nie odnosi się do niechcianych wiadomości o charakterze politycznym lub niekomercyjnym (takich jak polityk ubiegający się o twój głos lub darowizny na cele charytatywne). Co więcej, termin „niezamówiony" jest otwarty na wiele interpretacji, co jest wykorzystywane przez masowe wysyłanie e-maili przez główne firmy, których działy marketingu wykorzystały najcieńsze preteksty, aby uzasadnić wysyłanie e-maili do ludzi. W miarę rozszerzania się świata internautów pod koniec lat 90. XX wieku, obejmując coraz więcej pracowników biurowych i konsumentów, coraz więcej rzeczy na temat spamu stawało się coraz bardziej oczywiste:

1. Ludzie nie lubili spamu.

2. Spamerzy mogą zarabiać pieniądze.

3. Uzasadnione firmy miały ochotę wysyłać niechciane wiadomości e-mail.

Szybko się wzbogacaj.

Ile pieniędzy może zarobić spamer? Rozważ biznesplan jednej firmy z Arizony, C.P. Bezpośrednio, okazało się to bardzo opłacalne, dopóki nie zostało zamknięte w 2002 r. Przez Służbę Celną USA i Departament Bezpieczeństwa Publicznego w Arizonie. Oto niektóre aktywa zajęte przez władze:

* Prawie 3 miliony dolarów w gotówce oraz duża ilość drogiej biżuterii

* Ponad 20 milionów USD na rachunkach bankowych

* Dwanaście luksusowych importowanych samochodów (w tym osiem Mercedesów oraz różne modele z Lamborghini, Rolls-Royce, Ferrari i Bentley)

* Jeden budynek biurowy i różne luksusowe nieruchomości w Paradise Valley i Scottsdale

Zyski te zostały uzyskane ze sprzedaży pigułek o wartości 74 milionów dolarów, które obiecały zwiększyć wymiary różnych części męskiej i żeńskiej anatomii. Firma wykorzystywała spam do sprzedaży tych produktów, ale w rzeczywistości nie została zamknięta w celu wysyłania spamu, którego status prawny pozostaje do dziś niejednoznaczny, ponieważ zostały określone inaczej w różnych jurysdykcjach (w tym między innymi Kongres USA, który prawdopodobnie dokonał skrótu w 2004 roku). C.P. Direct przekroczył kilka linii, z których nie tylko składano fałszywe obietnice dotyczące jego produktów (z których żaden nigdy nie był testowany i z których wszystkie okazały się zawierać te same składniki, niezależnie od tego, jaką część ludzkiej anatomii obiecano ulepszyć). Firma pogłębiła swoje problemy, odmawiając wydania refundacji, gdy produkty nie działały, jak twierdzono. Jednak zamiast zniechęcać spamerów, ta sprawa udowodniła, że spam może sprawić, że staniesz się bogaty i to szybko. Rzeczywiście, nadzieja na szybkie wzbogacenie się pozostaje głównym motorem spamu. Fakt, że garstka ludzi była ścigana za prowadzenie podejrzanego przedsięwzięcia za pomocą spamu, nie była postrzegana jako poważny środek odstraszający.

Zbrodnia i kara.

Spamerzy wciąż spamują, ponieważ ryzyko jest postrzegane jako niewielkie w stosunku do potencjalnych korzyści i innych opcji szybkiego wzbogacenia się. Dwie osoby w centrum C.P., Michael Consoli oraz jego siostrzeniec i partner, Vincent Passafiume, przyznali się do winy wach w sprawie zarzutów podpisanych w sierpniu 2003 r; ale wyszli z więzienia przed majem 2004 r. i wydawało się, że bardzo mało cierpieli wstydu. Dwa lata po zwolnieniu para zwróciła się do stanowego sądu apelacyjnego o uchylenie wyroków skazujących i oddanie wszystkiego, co pozostało z zajętych aktywów.

Zastanów się, co się stało z Jeremym Jaynesem, nazwanym jednym z 10 najlepszych spamerów na świecie w 2003 roku przez Spamhaus, organizację zwalczającą spam. Kiedy oskarżono go o spam, sądzono, że Jaynes wysyła 10 milionów e-maili dziennie. Ile on na tym zarobił? Prokuratorzy twierdzili, że to około 750 000 $ miesięcznie. W 2004 r. Jaynes został skazany za wysyłanie niechcianych wiadomości e-mail z fałszywymi nagłówkami, co stanowi naruszenie prawa Wirginii. Został skazany na dziewięć lat więzienia. Jednak we wrześniu 2008 r. Jaynes, który został zwolniony za kaucją (ustaloną na mniej niż dwa miesiące jego zarobków ze spamu), został skazany przez Sąd Najwyższy Wirginii, który orzekł, że stanowe prawo antyspamowe był niekonstytucyjny - orzeczenie zaatakowane jako

nieuzasadnione przez niektórych krytyków specjalizujących się w przepisach antyspamowych. Innym znanym spamerem był Sanford „Spamford" Wallace, założyciel Cyber Promotions w latach 90., który aktywnie wykorzystywał spam jako usługę komercyjną. W październiku 2009 r. Facebook wygrał przeciwko niemu pozew cywilny za wysyłanie fałszywych wiadomości do jego użytkowników. Wallace został ukarany grzywną w wysokości 711 milionów dolarów - co było mało prawdopodobne, ponieważ złożył wniosek o ogłoszenie upadłości w czerwcu 2009 r. W sierpniu 2011 r. oskarżony przed sądem federalnym w San Jose. Zgodnie z aktem oskarżenia, od około listopada 2008 r. do marca 2009 r. Wallace przeprowadził plan wysyłania spamu do użytkowników Facebooka. Wiadomości te zaatakowały około 500 000 legalnych kont na Facebooku i spowodowały wysłanie ponad 27 milionów wiadomości spamowych za pośrednictwem serwerów Facebooka. Akt oskarżenia twierdzi, że Wallace wysłał spam do użytkowników Facebooka w trzech okresach: po pierwsze, w dniu 5 listopada 2008 r. lub mniej więcej i do około 6 listopada 2008 r. Wallace uzyskał dostęp do sieci komputerowej Facebooka w celu zainicjowania transmisji programu, w wyniku którego do użytkowników Facebooka wysłano ponad 125 000 wiadomości spamowych; Po drugie, w grudniu 28, 2008, Wallace uzyskał dostęp do sieci komputerowej Facebooka, aby zainicjować transmisję programu, która spowodowała wysłanie prawie 300 000 spamu do użytkowników Facebooka; Po trzecie, 17 lutego 2009 r. Wallace uzyskał dostęp do sieci komputerowej Facebooka, aby zainicjować transmisję programu, w wyniku której do użytkowników Facebooka wysłano ponad 125 000 wiadomości spamowych.

Marnotrawstwo gry.

Pod wieloma względami spam jest spadkobiercą klasycznej gry frajerów rozgrywanej w niejawnych reklamach, które obiecują nauczyć Cię, jak „zdobyć gotówkę w skrzynce pocztowej". Sztuczka polega na tym, aby ludzie wysyłali ci pieniądze, aby dowiedzieć się, jak zdobyć gotówkę w swojej skrzynce pocztowej. Jeśli spamer wyśle 25 milionów wiadomości e-mail z reklamą produktu, może sprzedać wystarczającą liczbę produktów, aby osiągnąć zysk, ale rzeczywisty produkt wiąże się z rzeczywistymi kosztami produkcji. Przeciwnie, jeśli wyśle wystarczająco dużo wiadomości reklamującymi listę 25 milionów sprawdzonych adresów e-mail za 79,95 USD, może zebrać wystarczającą liczbę frajerów, którzy zechcą kupić tę listę i zarobić znaczny zysk, ponieważ lista zasadniczo nie kosztuje nic do wygenerowania. Fakt, że większość adresów na takich listach okazuje się bezużyteczna, nie powstrzymuje ludzi przed ich kupowaniem lub sprzedażą.

Jedną z form spamu, która nie polega na sprzedaży produktu, jest oszustwo typu „zrzuć". Wysyłanie milionów wiadomości mówiących o tym, jak gorący stanie się niejasny magazyn, może stworzyć samospełniającą się przepowiednię. Oto jak to działa:

* Kupuj dużo akcji z depozytu zabezpieczającego lub wiele akcji w firmie, która handluje za kilka centów za akcję.

* Rozsyłaj milionom ludzi wiadomość mówiącą o kupionych akcjach.

* Poczekaj, aż cena akcji wzrośnie, a następnie sprzedaj swoje akcje za dużo więcej niż za nie zapłaciłeś.

Taki schemat łamie różne przepisy, ale może okazać się opłacalny, jeśli nie zostaniesz złapany (możesz ukryć swoją tożsamość jako nadawca spamu); niemniej jednak organy regulacyjne nadal mogą przeglądać duże zamówienia kupna i sprzedaży akcji, o których mowa w spamie giełdowym. Przyczyny stałego wzrostu ilości spamu można znaleźć w ekonomii tego medium. Wysyłanie milionów wiadomości e-mail kosztuje nadawcę bardzo niewiele. Zwykły komputer osobisty (PC) podłączony do Internetu za pomocą modemu telefonicznego za 10 USD za miesiąc może wysyłać setki tysięcy wiadomości dziennie; niewielka sieć komputerów podłączonych za pomocą modemu kablowego za 50 USD miesięcznie lub cyfrowej linii abonenckiej (DSL) może wydać miliony. Oczywiście bariera

ekonomiczna w dostępie do schematów szybkiego spamowania polegającego na wzbogacaniu się jest bardzo niska. Ryzyko wpadnięcia w kłopoty z władzami jest również bardzo niskie. Koszty spamu ponoszone są na wiele sposobów przez kilku niechętnych wspólników

Adresat wiadomości e-mail

* Poświęca czas na oddzielanie niepotrzebnych wiadomości e-mail od wiarygodnych wiadomości e-mail. W przeciwieństwie do poczty ślimakowej, która jest zazwyczaj dostarczana i sortowana raz dziennie, e-mail dociera przez cały dzień i noc. Za każdym razem, gdy to sprawdzasz, zmagasz się z marnowaniem czasu na rozproszenie spamu.

* Opłaty za otrzymywanie wiadomości e-mail. Brak wolnych połączeń internetowych. Gdy łączysz się z Internetem, ktoś płaci. Typowy konsument w domu płaci zryczałtowaną stawkę co miesiąc, ale poziom tej stawki zależy częściowo od ilości danych obsługiwanych przez dostawcę usług internetowych (ISP), a spam zawyża ten wolumen, podnosząc w ten sposób koszty.

Przedsiębiorstwo

* Traci wydajność, ponieważ pracownicy, z których wielu musi sprawdzać pocztę e-mail w celach biznesowych, spędzają czas na usuwaniu spamu ze skrzynki odbiorczej firmy. Firmy, które pozwalają pracownikom na dostęp do osobistych wiadomości e-mail w pracy, płacą również za czas stracony na usuwanie spamu.

* Marnuje zasoby, ponieważ spam zwiększa zużycie przepustowości, cykle przetwarzania i przestrzeń dyskową.

Dostawcy usług internetowych (ISP) i dostawcy usług e-mail (ESP)

*Marnują zasoby na obsługę spamu, który zwiększa zużycie pasma, cykle przetwarzania i przestrzeń dyskową.

*Muszą wydawać pieniądze na filtrowanie spamu, administrowanie listą bloków, skargi klientów związane ze spamem oraz skargi związane z filtrowaniem / blokowaniem.

*Muszą przeznaczyć środki na pilnowanie użytkowników, aby uniknąć zablokowania ich na liście. (Więcej informacji na temat filtrów i list bloków znajduje się w następnej sekcji).

Dwa inne czynniki ekonomiczne wpływają na wzrost spamu: ciężkie czasy i szybkość dostarczania. Gdy czasy są ciężkie, coraz więcej osób uważa, że warto spróbować programów wzbogacających, takich jak spamowanie, więc jest więcej spamerów (ciężkie czasy wpływają również na odbiorcę, a odbiorcy chętniej wierzą w fałszywe obietnice wygranych loterii i łatwych pieniędzy być zrobionym). Gdy stawki dostarczania spamu spadną - z powodu zastosowania filtrów antyspamowych i innych technik, które zostaną omówione później

Jak duży jest problem ze spamem?

Istnieją pewne kontrowersje dotyczące odsetka wiadomości e-mail zaklasyfikowanych jako spam. Do 2006 r. stwierdzono, że spam zużywa ponad 90 procent zasobów poczty elektronicznej na całym świecie. To był oszałamiający poziom nadużycia systemu przez dowolny standard. Jednak gdy garstka specjalistów ds. bezpieczeństwa twierdziła, dziesięć lat wcześniej, że spam stanowi zagrożenie dla bezpieczeństwa komputerowego, spotkała się ze znacznym sceptycyzmem i pewnymi podejrzeniami, być może częściowo ze względu na rozczarowanie Y2K; był też niewątpliwie element powtarzającego się podejrzenia, że specjaliści ds. bezpieczeństwa trąbią na nowych zagrożeniach dla rozwoju biznesu - dziwne pojęcie, biorąc pod uwagę odwieczne bogactwo możliwości dla ekspertów w dziedzinie, która

uporczywie informuje o prawie zerowym poziomie bezrobocia. Przydatną historyczną perspektywę przygnębiającego wpływu spamu na wiadomości e-mail zapewniają raporty dostępne bezpłatnie na stronie MessageLabsWebsite. Jej roczne sprawozdania zawierają konserwatywne szacunki wzrostu ilości spamu; na przykład w raporcie rocznym za 2007 r. wykazano, że całkowity spam zawiera około 85 procent wszystkich wiadomości e-mail od 2005 do 2007 r., a nowe odmiany (te wcześniej niezidentyfikowane według typu lub źródła) utrzymują się na stałym poziomie około 75 procent wszystkich wiadomości e-mail. Firma Symantec zgłosiła, że spam stanowi ponad 90 procent całkowitego ruchu pocztowego w 2009 i 2010 roku, ale odsetek ten zaczął spadać w ciągu następnych kilku lat. W czerwcu 2011 r. Firma Symantec zgłosiła współczynnik spamu wynoszący około 73 procent wszystkich wiadomości e-mail; do grudnia 2011 r. zgłosili dalszy spadek do około 70 procent. Według Kaspersky Lab na początku 2013 r. „… udział spamu w ruchu pocztowym stale spadał w 2012 r., osiągając najniższy poziom od pięciu lat. Średnia w tym roku wyniosła 72,1% - o 8,2 punktów procentowych mniej niż w 2011 roku. Tak długi i znaczny spadek poziomu spamu jest bezprecedensowy. ” Inne badanie przeprowadzone w styczniu 2013 r. Sugerowało, że tylko około 60 procent wszystkich wiadomości e-mail stanowiło spam w 2012 r. Szacunki innych ekspertów sugerują, że tylko około 15 procent całkowitego spamu przechodzi przez wszystkie filtry spamu na poziomie ISP i aplikacji. Chociaż większość firm i konsumentów prawdopodobnie zgodzi się, że spam rozrósł się ze zwykłego irytacji do ogromnego obciążenia, niektórzy twierdzą, że spam nie jest dużym problemem. Obejmują one:

* Konsumentów, którzy nie używali e-maila od bardzo dawna

* Użytkowników pakietu Office, którzy nie widzą spamu adresowanego do nich z powodu jakiejś formy urządzenia lub usługi antyspamowej wdrożonej przez ich firmę

Te spostrzeżenia przesłaniają zauważony wcześniej fakt, że spam pochłania ogromne ilości zasobów, które można lepiej wykorzystać. Konsument może uzyskać tańszą, lepszą usługę internetową, jeśli spam nie zużywa tak dużej przepustowości, pojemności serwera, pamięci i siły roboczej. Z doświadczenia związanego z regionalnym dostawcą usług internetowych wynika, że wzrost ilości spamu znajduje bezpośrednie odzwierciedlenie w kosztach serwera. ISP musiał ciągle dodawać serwery do obsługi poczty e-mail. Zanim dotarło do czterech serwerów, 75 procent wszystkich wiadomości e-mail było oznaczonych jako spam. ISP poniósł koszty serwera czterokrotnie wyższe niż potrzebne do obsługi legalnej poczty e-mail. Co więcej, nawet w przypadku czterech serwerów, wzrost liczby spamu powodował awarię serwerów, co powodowało dodatkowy koszt połączeń serwisowych w środku nocy, nie wspominając o utracie subskrybentów spowodowanej awariami. Spam ma bezpośredni wpływ na wydatki na infrastrukturę. Pamięć masowa jest jednym z największych kosztów sprzętu i konserwacji ponoszonych przez pocztę elektroniczną. Jeśli nawet 70 procent wszystkich wiadomości e-mail to niechciane śmieci, to firmy przetwarzające pocztę wydają o wiele więcej na przechowywanie niż gdyby wszystkie e-maile były zgodne z prawem. Wydajność w przypadku firm, których pracownicy marnują czas na usuwanie spamu ze swoich skrzynek odbiorczych, jest również ogromna. Poza tymi kosztami rozważ możliwość, że spam faktycznie hamuje działanie Internetu , mające negatywny wpływ na gospodarki, takie jak gospodarki Ameryki, które czerpią znaczną siłę z towarów i usług związanych z Internetem. Chociaż Internet wydaje się rosnąć w dobrym stanie, może być tak dobrze, że trudno jest określić, jak źle sobie radzimy. Być może jedynym powodem, dla którego taki efekt nie był jeszcze odczuwalny, jest to, że wpływ spamu na nowych użytkowników jest ograniczony. Jak wspomniano wcześniej, kiedy nowi użytkownicy po raz pierwszy otrzymują adresy e-mail, zwykle nie otrzymują dużej ilości spamu. Według niektórych badań znalezienie spamu przez adres e-mail może zająć od sześciu do dwunastu miesięcy, ale kiedy to zrobi, ilość spamu na ten adres może bardzo szybko wzrosnąć. To powoduje, że niektórzy ludzie ograniczają korzystanie z poczty

elektronicznej i Internetu. W „The Economics of Spam" opublikowanym w letnim wydaniu Journal of Economic Perspectives, Justin M. Rao (Microsoft) i David H. Reiley (Google), obaj byli pracownikami Yahoo! Zbadaj, omów zewnętrzność spamu - wykorzystanie zasobów ofiar w celu wspierania zysków przestępców. Piszą,

„Szacujemy, że amerykańskie firmy i konsumenci ponoszą koszty prawie 20 miliardów dolarów rocznie z powodu spamu. Nasza liczba jest bardziej konserwatywna niż 50 miliardów dolarów często cytowanych przez innych autorów, a także zauważamy, że liczba ta byłaby znacznie wyższa, gdyby nie na prywatne inwestycje firm w technologię antyspamową… Po stronie prywatnych korzyści, w oparciu o pracę podstępnych informatyków, którzy infiltrują i monitorują aktywność spamerów… szacujemy, że spamerzy i reklamodawcy spamujący zbierają globalne przychody brutto na rzędu 200 milionów USD rocznie. Zatem „stosunek efektów zewnętrznych" kosztów zewnętrznych do wewnętrznych korzyści związanych ze spamem wynosi około 100: 1 "

Dwustronne zagrożenie spamem.

Gdy serwery pocztowe zwalniają, słabną i ostatecznie ulegają awariom pod naporem spamu, rezultatem są utracone wiadomości, przerwy w świadczeniu usług oraz nieprzewidziane koszty pomocy technicznej i wsparcia technicznego. Brak sprzedaży. Klienci nie otrzymują oczekiwanej usługi. Koszt utrzymania spamu poza skrzynką odbiorczą i przedsiębiorstwem to jedno, a koszt zapobiegania spamowi wpływania na dostępność systemu i operacji biznesowych jest inny; ale istnieje jeszcze druga strona zagrożenia spamem - pokusa, by stać się agresywnym masowym mailerem, znanym również jako spamer. Jest to coś, co spam ma wspólnego z wywiadem konkurencyjnym, znanym również jako szpiegostwo przemysłowe. W przypadku złego wykonania wysyłki masowe, takie jak dane wywiadowcze dotyczące konkurencji, mogą zaszkodzić reputacji firmy. Pomijając kwestię coraz bardziej nieprzyjemnych ładunków dostarczanych ze spamem, takich jak trojany i ataki phishingowe, nawet zwykły stary spam ulepszony przez mężczyzn stanowi zagrożenie zarówno dla infrastruktury sieci, jak i wydajności. Na początek spam stanowi kradzież zasobów sieciowych. Wspomniano już o wpływie inflacyjnym na budżety serwerów. Negatywny wpływ na przepustowość może być mniej oczywisty, ale jest zdecydowanie realny. W 2002 i 2003 roku autor uczestniczył w testach beta prototypowego routera antyspamowego na poziomie sieci. Nie było niczym niezwykłym, że firma instalująca to urządzenie odkryła, że spam zużywał od dwóch trzecich do trzech czwartych przepustowości sieci. Niezależnie od tego, czy wpływ ten był postrzegany jako spadek wydajności czy inflacja kosztów, bardzo niewiele firm chciało usunąć to urządzenie po jego zainstalowaniu. Innymi słowy, gdy firmy widzą, jaka jest ich wydajność sieci i koszt przepustowości, gdy spam jest usuwany z równania, zdają sobie sprawę, jaki negatywny wpływ ma spam. Jest to coś, co w przeciwnym razie może być trudne do wykrycia, biorąc pod uwagę, że z czasem ilość spamu wzrosła. Jeszcze bardziej dramatyczna ilustracja szkód, jakie może powodować spam, pojawia się, gdy sieć jest atakowana przez naprawdę duże działo spamowe (specjalnie stworzona konfiguracja urządzeń MTA podłączonych do naprawdę dużego połączenia szerokopasmowego; na przykład sześciopak zoptymalizowanego MTA mogą wysyłać 3,6 miliona wiadomości na godzinę). Skutkiem jest rozbicie serwera poczty odbierającej, z wszystkimi związanymi z tym kosztami i ryzykiem. Jednym ze sposobów, aby temu zapobiec, oprócz wdrożenia czegoś takiego jak router antyspamowy, jest zarejestrowanie się w usłudze antyspamowej, która przechwytuje wszystkie przychodzące wiadomości e-mail i blokuje spam. Takie rozwiązanie rozwiązuje szereg problemów związanych z pocztą e-mail, ale przy znacznych bieżących kosztach, które nadal stanowią kradzież zasobów przez spamerów. Firma Commtouch.com udostępnia kalkulator kosztów spamu, który generuje interesujące liczby. Rozważ te wartości wejściowe dla średniej wielkości firmy:

Pracownicy: 800

* Średnia roczna pensja: 45 000 $

* Średnia liczba codziennych wiadomości e-mail na jednego odbiorcę: 75

* Średni odsetek wiadomości e-mail będących spamem: 80 procent

Według kalkulatora całkowity roczny koszt spamu dla tej organizacji, która, jak się zakłada, nie stosuje środków antyspamowych, wynosi nieco ponad 1 milion USD. Jest to oparte na pewnych założeniach, takich jak czas potrzebny na usunięcie wiadomości spamowych, ale ogólnie wydaje się dość realistyczne. Oczywiście rozmiar uderzenia produktywności spowodowanego przez spam, który trafia do skrzynki odbiorczej dla pracowników, był gorliwie dyskutowany przez lata, ale jest zdecydowanie więcej niż nieistotny i nie jest jedynym trafieniem. Nawet jeśli wprowadzone zostanie filtrowanie antyspamowe, nadal będzie konieczne sprawdzenie lub dostosowanie decyzji podjętych przez filtr, aby upewnić się, że żadne ważne, wiarygodne wiadomości nie zostaną błędnie poddane kwarantannie lub usunięte. Innymi słowy, nawet jeśli firma wydaje 50 000 USD rocznie na filtrowanie antyspamowe, nie odzyska całego miliona dolarów zmarnowanych przez spam.

Zagrożenie spamem wychodzącym.

Nawet gdy organizacje takie jak Coalition Against Unsolicited Commercial Email (CAUCE) próbowały przekonać firmy że spamowanie było niewłaściwą techniką marketingową, która może przynieść odwrót w postaci bardzo zirytowanych adresatów, i podobnie jak różne podmioty rządowe próbowały stworzyć reguły zakazujące spamu, niektóre firmy z radością wprowadziły zasady i zalały klientów ofertami e-mail, ci konsumenci prosili o nie, czy nie. Doprowadziło to niektórych antyspamerów do potępienia wszystkich firm jednym tchem. Doświadczenie autora, współpracujące z dużymi firmami, które szanowały marki, było takie, że żadna z nich nie chciała obrażać konsumentów. Duże firmy zawsze mają trudności z powstrzymywaniem indywidualnych działań marketingowych, a masowe wysyłanie e-maili jest bardzo kuszące, gdy nieuczciwy pracownik lub po prostu niedoinformowany pracownik jest zmuszony do sprzedaży; ale kierownictwo wyższego szczebla raczej nie zaakceptuje niczego, co mogłoby zostać wzięte za spam. Motywy odpowiedzialności korporacyjnej w wiadomościach e-mail nie są czysto altruistyczne. Inteligentne firmy widzą, że utrwalanie taktyk budzących niechęć do wiadomości e-mail jedynie osłabia ogromny potencjał wiadomości e-mail jako narzędzia biznesowego. Cokolwiek myśli się o spamie, nie można zaprzeczyć, że jako narzędzie biznesowe, masowa poczta e-mail jest potężna. Jest również uwodzicielski. Gdy ktoś ma historię do opowiedzenia lub produkt do sprzedania, a tam właśnie znajduje się duża lista adresów e-mail, masowa poczta e-mail może być bardzo kusząca. Naiwni użytkownicy mogą myśleć: „Gdzie jest szkoda?" i „Kto zamierza się sprzeciwić?" Ale dopóki nie udokumentują pozwolenia na wysłanie wiadomości do osób z tej listy, mądrą decyzją biznesową jest oparcie się pokusie.

Środki masowego e-maila.

Jednym z najbardziej podstawowych biznesowych środków ostrożności dotyczących poczty e-mail jest: Nigdy nie wysyłaj wiadomości, jeśli nie masz pewności, jak będzie ona wyglądać dla osoby, która ją otrzyma. Obejmuje to formatowanie, język używany, a przede wszystkim adresowania. Jeśli chcesz zaadresować tę samą wiadomość do więcej niż jednej osoby na raz, masz trzy główne opcje, z których każda powinna być traktowana ostrożnie:

1. Umieść adresy e-mail wszystkich odbiorców w polu Do lub Kopiuj (DW), aby wszyscy odbiorcy mogli zobaczyć adresy innych osób, do których wysłałeś wiadomość. Czasami jest to odpowiednie w przypadku komunikacji w niewielkiej grupie osób.

2. Jeśli liczba osób w grupie przekracza około 20 lub jeśli nie chcesz, aby wszyscy wiedzieli, kto otrzymuje wiadomość, przenieś wszystkie oprócz jednej do pola Blind Copies (Bcc). Jeden adres w polu Do może być twój. Jeśli ujawnienie adresatów może wywołać jakiekolwiek zakłopotanie, najpierw wykonaj próbną wysyłkę. Wyślij kopię wiadomości do siebie i przynajmniej do jednego współpracownika spoza firmy, a następnie popatrz na wiadomość, aby upewnić się, że wpisy UDW zostały wprowadzone poprawnie.

3. Aby obsłużyć duże grupy odbiorców lub spersonalizować jedną wiadomość do wielu odbiorców, użyj specjalnej aplikacji, takiej jak Group Mail, która może niezawodnie tworzyć indywidualne, dostosowane wiadomości dla każdej osoby na liście. To starannie pomija błędy związane z polami Do i DW. Group Mail przechowuje adresy e-mail w bazie danych i buduje wiadomości w locie za pomocą funkcji scalania, takiej jak edytor tekstu. Możesz wstawić pola bazy danych do wiadomości. Na przykład wiadomość może odnosić się do odbiorcy według nazwy. Program oferuje również obszerne testowanie wiadomości, dzięki czemu można zobaczyć, co zobaczą odbiorcy przed wysłaniem wiadomości. A program ma możliwość wysyłania wiadomości w małych grupach, rozłożonych w czasie, zgodnie z możliwościami twojego połączenia internetowego

To, czy używasz programu, takiego jak Mail Group, do uzyskania prawdziwej poczty e-mail, czy czegoś jeszcze potężniejszego, zależy od kilku czynników, takich jak rozmiar organizacji, liczba wiadomości, które musisz wysłać, oraz twoja polityka prywatności. W grę wchodzi prywatność, ponieważ niektóre oprogramowanie używane do wysyłania wiadomości e-mail, takie jak Poczta Grupowa, umożliwia użytkownikowi programu dostęp do bazy danych zawierającej adresy, na które wysyłana jest poczta. Zasadniczo nie stanowi to problemu w mniejszych firmach lub gdy baza danych składa się wyłącznie z nazw i adresów bez specjalnego kontekstu; ale może to być problem, gdy baza danych zawiera poufne informacje lub kontekst jest wrażliwy. Na przykład lista nazwisk i adresów może być wrażliwa, jeśli osoba obsługująca listę wie lub może wywnioskować, że należą do pacjentów poddawanych pewnego rodzaju leczeniu. Być może nie chcesz zezwalać operatorom systemu, a nawet programistom, na dostęp do poufnych danych po prostu dlatego, że są oni odpowiedzialni za wysyłanie lub programowanie wiadomości. Na szczęście można napisać programy pocztowe, które pozwalają operatorowi pisać i wysyłać pocztą i wyślij, nie widząc nazwisk i adresów osób, do których jest wysyłany. Dane testowe mogą i powinny być wykorzystane do potwierdzenia wysyłki przed jej wykonaniem. Innym podstawowym środkiem ostrożności w przypadku wiadomości e-mail jest to, aby nigdy nie wysyłać wiadomości, które mogłyby urazić odbiorców. Wybierając swoje sformułowania, projekt, przesłanie, poznaj swoich odbiorców. Zachowaj szczególną ostrożność, jeśli chodzi o humor, politykę, religię, seks lub inny delikatny temat. Korzystając z poczty e-mail w celach biznesowych, lepiej oskarżać się o brak humoru niż brak osądu. Szanuj referencje innych osób, jeśli je znasz, dotyczące treści. Jeśli ludzie preferują wiadomości tekstowe, nie wysyłaj im HTML-ów i miej nadzieję, że zdecydują się zmienić zdanie. Zapytaj najpierw, ponieważ ścieżka przebaczenia później nie jest opłacalna, gdy masz do czynienia z tysiącami niezadowolonych odbiorców dzwoniących do centrali. Korzystając z treści HTML, nadal staraj się utrzymywać rozmiar na minimalnym poziomie, chyba że masz odbiorców, którzy specjalnie zażądali dużych, bogatych w multimedia wiadomości. Środki antyspamowe stosowane przez wielu dostawców usług internetowych, firmy i konsumentów czasami generują fałszywe alarmy, oznaczając legalną wiadomość e-mail jako spam, potencjalnie uniemożliwiając dotarcie wiadomości e-mail do zamierzonych odbiorców, nawet jeśli poprosili o jej otrzymanie. Jeśli adres e-mail Twojej firmy zostanie uznany za szczególnie rażący spam, serwer, przez który jest wysyłany, prawdopodobnie zostanie zablokowany. Jeśli jest to ogólny serwer pocztowy Twojej firmy, blokowanie może wpłynąć na dostarczenie znacznie więcej niż spamu. Jeśli serwery, przez które wysyłana jest Twoja duża korespondencja, należą do usługodawcy, a ich serwery zostają zablokowane, może to również stanowić problem. A jeśli korzystasz z usługodawcy, aby wykonać

wysyłkę za ciebie, ale nie wybierasz mądrze, twoja poczta może być oznakowana jako spam tylko z powodu złej reputacji serwerów, przez które przechodzi. Pamiętaj, że używanie spamu do reklamowania produktów może narazić Cię na naruszenie ustawy CAN-SPAM Act z 2003 roku, nawet jeśli sam nie wyślesz spamu. Co można zrobić, aby wiadomości, które nie są spamem, nie stały się ofiarą antyspamu? Przestrzeganie zasad odpowiedzialnego korzystania z poczty elektronicznej to dobry pierwszy krok. Odpowiedzialne zarządzanie serwerami e-mail firmy również potrzebuje pomocy, podobnie jak wybór renomowanych dostawców usług. Powinieneś także rozważyć zlecenie komuś śledzenia środków antyspamowych, aby upewnić się, że Twój e-mail jest tak zaprojektowany, aby w jak największym stopniu unikać wszelkich elementów treści lub prezentacji, które są obecnie oznaczane jako spam. Aby upewnić się, że Twoja firma jest powiązana z odpowiedzialnymi praktykami e-mail, zostań zaznajomiony z „Sześć rezolucjami dla odpowiedzialnych e-maili". Zostały one utworzone przez Radę odpowiedzialnego e-maila (CRE), która powstała pod egidą Association for Interactive Marketing (AIM), spółki zależnej Direct Market Association (DMA). Niektóre z największych firm w kraju i najwięksi uprawnieni użytkownicy poczty e-mail należą do tych organizacji i są oni zainteresowani tym, aby poczta elektroniczna nie była nadużywana. Oto sześć rezolucji:

1. Marketerzy nie mogą fałszować nazwy domeny nadawcy ani używać niereagującego adresu IP bez dorozumianej zgody odbiorcy lub przeniesionej zgody od marketera.

2. Marketingowcy nie mogą celowo fałszować treści tematu lub wprowadzać czytelników w błąd z treści wiadomości e-mail.

3. Wszystkie masowe wiadomości e-mail marketingowe muszą zawierać opcję anulowania przez odbiorcę (usunięcia z listy) otrzymywania przyszłych wiadomości od tego nadawcy, właściciela listy lub menedżera listy.

4. Marketerzy muszą poinformować respondenta podczas zbierania adresu e-mail online w jakim celu marketingowym zostanie użyty adres e-mail respondenta.

5. Marketerzy nie mogą zbierać adresów e-mail z zamiarem wysyłania masowych niechcianych komercyjnych wiadomości e-mail bez wiedzy i zgody konsumentów. (Żniwa są definiowane jako kompilowanie lub kradzież adresów e-mail za pomocą anonimowych procedur zbierania, takich jak pająk internetowy, pokoje czatowe lub inne publicznie wyświetlane obszary zawierające osobiste lub biznesowe adresy e-mail).

6. CRE sprzeciwia się wysyłaniu masowej niechcianej komercyjnej wiadomości e-mail na adres e-mail bez wcześniejszych relacji biznesowych lub osobistych. (Relacja biznesowa lub osobista jest zdefiniowana jako wszelka wcześniejsza inicjowana przez odbiorcę korespondencja, działalność transakcyjna, działalność obsługi klienta, wykorzystanie uprawnień stron trzecich lub sprawdzony kontakt offline).

Te sześć rezolucji można uznać za rozsądny środek między ekstremistami antyspamowymi a dyrektorami ds. marketingu za wszelką cenę. Gdyby wszyscy przestrzegali tych postanowień, nie byłoby spamu, przynajmniej zgodnie z definicją spamu większości ludzi. W końcu, jeśli nikt nie otrzyma więcej niż jednej lub dwóch wiadomości w tygodniu, które były niechciane i nieistotne, nastroje antyspamowe znacznie by ostygły.

Problemy z dołączaniem i pozwoleniami.

Niektórzy zwolennicy prywatności sprzeciwiają się szóstej rezolucji, ponieważ zezwala ona na dołączanie wiadomości e-mail. Jest to praktyka znajdowania adresu e-mail dla klienta, który jeszcze go nie podał. Firmy takie jak Yesmail i AcquireNow zrobią to za opłatą. Na przykład jeśli jesteś bankiem,

prawdopodobnie masz fizyczne adresy dla wszystkich swoich klientów, ale możesz nie mieć adresów e-mail dla wszystkich. Możesz wynająć firmę, aby znaleźć adresy e-mail dla klientów, którzy ich nie podali. Jednak klienci ci mogli nie dać wyraźnego zezwolenia bankowi na kontaktowanie się z nimi za pośrednictwem poczty elektronicznej, więc niektórzy twierdzą, że wysyłanie do nich wiadomości e-mail to spam. Bez względu na to, czy zgadzasz się z tą oceną, czy nie, musisz rozważyć kilka czynników, jeśli Twoja firma rozważa skorzystanie z usługi dołączania wiadomości e-mail. Przede wszystkim upewnij się, że nic w twojej polityce prywatności nie zabrania tego. Następnie zastanów się nad możliwą reakcją klientów, pamiętając, że dołączanie wiadomości e-mail nie jest idealną nauką. Aby dowiedzieć się więcej o tym, jak działa appending, wpisz „append e-mail" jako wyszukiwane hasło w Google - znajdziesz wiele firm oferujących wyjaśnienie, w jaki sposób to robią, dopasowując dane pobrane z wielu różnych źródeł przy użyciu skomplikowanych algorytmów. Innym problemem, który należy wziąć pod uwagę, jest to, że niektóre wiadomości trafią do osób niebędących klientami. Z tego powodu prawdopodobnie chcesz, aby pierwszy kontakt był tymczasowy, na przykład uprzejma prośba o dalszy kontakt. Następnie możesz sformułować odpowiedzi, aby stworzyć prawdziwą listę akceptacji. Jak można się spodziewać, możesz zlecić cały proces outsourcingowi usługi dołączającej, która będzie miała własne, często zautomatyzowane, metody radzenia sobie z odsyłanymi wiadomościami, reklamacjami i tak dalej. Nie dołączaj żadnych poufnych danych osobowych do pierwszego kontaktu, ponieważ nie masz gwarancji, że bob.jones@majorfreemail.net to Robert Jones, na którym masz swoją listę klientów. Kiedy latem 2002 r. Citibank wysłał dołączoną korespondencję, zachęcając obecnych klientów do korzystania z usług kont internetowych banku, spotkał się z poważną krytyką. Chociaż bank nie zapewniał natychmiastowego dostępu online dołączonym klientom, samo postrzeganie tego, w połączeniu z wieloma błędnymi tożsamościami e-mail, wywołało negatywny rozgłos. Oto, co powiedział Citibank w wiadomości, którą wysłał do osób, które uważa za klientów, mimo że osoby te nie podały swojego adresu e-mail bezpośrednio do banku: Citibank chciałby przesyłać Ci wiadomości e-mail, aby informować Cię o Twojej karcie Citi, a także specjalne usługi i korzyści… Z pomocą dostawcy usług e-mail znaleźliśmy adres e-mail, który naszym zdaniem należy do Ciebie. Chociaż przesłanie to jest z pewnością grzeczne, wyraźnie rodzi pytania w umysłach odbiorców. Dwa pytania mogą podważyć dołączanie jako praktyki biznesowej: Gdzie dokładnie ten usługodawca szuka tych adresów e-mail? Dlaczego firma, która chce, aby mój adres e-mail po prostu nie napisała i nie poprosiła o to? Faktem jest, że współczynniki konwersji z kontaktu e-mailowego są wyższe niż z poczty ślimakowej, więc argumentem za usługami dołączającymi jest to, że firmy, które z nich korzystają, szybciej przechodzą na tańsze i lepsze medium poczty elektronicznej niż te, które tego nie robią. Kontrapunkt jest taki, że zbyt wiele osób będzie obrażonych w tym procesie. Zastanów się, na jak długo przedłużasz zasadę wcześniejszych relacji biznesowych, o której mowa w szóstej odpowiedzialnej rezolucji dotyczącej poczty elektronicznej. Bank prawdopodobnie ma silniejsze argumenty za dołączeniem adresów e-mail do listy posiadaczy rachunków niż firma wysyłkowa, która chce dołączyć listę osób, które poprosiły o katalog z zeszłego roku. Zakres, w jakim zwolennicy prywatności przyjmują lub potępiają koncepcję wcześniejszych relacji biznesowych, w dużej mierze zależy od tego, jak rozsądne firmy interpretują je. Marketing na adresy, które nie zostały dostarczone z jasnym zrozumieniem tego byłyby wykorzystywane do takich celów, nie jest wskazane. W zależności od oświadczenia o prywatności może to stanowić naruszenie polityki prywatności firmy. Postępowanie w przypadku takiego naruszenia może nie tylko drażnić klientów, ale także zwrócić uwagę organów regulacyjnych branży, takich jak Federalna Komisja Handlu (FTC). Oczywiście będziesz musiał sam zdecydować, czy Twoim zadaniem lub obowiązkiem jest wskazanie tego kierownictwu. Pamiętaj też, aby zapewnić odbiorcom prosty sposób rezygnacji z dalszych wysyłek. (Najlepiej do tego służy link do formularza internetowego. Unikaj proszenia odbiorcy o odpowiedź na wiadomość. Jeśli adres e-mail, na który wysłałeś wiadomość, nie jest już jej głównym adresem, może mieć problem z rezygnacją).

WALKA ZE SPAMEM.

Walkę z przychodzącym spamem można rozwiązać zarówno szczegółowo, jak w „Co mogę zrobić, aby chronić moje systemy przed spamem?", A ogólnie „Co można zrobić, aby zapobiec spamowi w ogóle?" Oczywiście, jeśli wyeliminowano by spamowanie, wszyscy mieliby jedno mniejsze zagrożenie do zmartwienia.

Wejdź do Spam Fighters.

W pięcioletnim okresie od 1997 do 2002 r. zróżnicowana grupa interesów i organizacji walczyła, aby uświadomić światu problem spamu i zachęcić do podjęcia środków zaradczych. Wysiłki CAUCE, które trwają do dziś, zachęciły ustawodawców do przyjęcia przepisów antyspamowych i pomogły uporządkować proces czarnej listy, na podstawie którego identyfikowane są serwery wysyłające spam. W 1998 r. Spamhaus Project, działalność ochotnicza założona przez Steve'a Linforda, rozpoczęła śledzenie spamerów i działań związanych ze spamem. (Nazwa pochodzi od pseudo-niemieckiego wyrażenia wymyślonego przez Linforda, aby opisać dowolnego dostawcę usług internetowych lub inną firmę, która wysyła spam lub chętnie świadczy usługi dla spamerów.) Grupa robocza ds. zwalczania phishingu (APWG) została założona w 2003 r. iI jest jedną z obecnie najbardziej aktywne i produktywne organizacje antyphishingowe: APWG jest światową koalicją jednoczącą globalną reakcję na cyberprzestępczość w sektorach przemysłu, rządu i organów ścigania. Członkostwo APWG w ponad 2000 instytucji na całym świecie jest tak globalne, jak jego prognozy, a jej dyrektorzy, menedżerowie i naukowcy doradzają: rządom krajowym; globalnym organom zarządzającym, takim jak ICANN; półkuliste i globalne grupy handlowe; oraz wielostronne organizacje traktatowe, takie jak Komisja Europejska, Konwencja Rady Europy o cyberprzestępczości, Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości, Organizacja Bezpieczeństwa i Współpracy w Europie oraz Organizacja Państw Amerykańskich. Członkostwo jest otwarte dla instytucji finansowych, sprzedawców detalicznych, dostawców rozwiązań, dostawców usług internetowych, operatorów telekomunikacyjnych, kontrahentów związanych z obronnością, organów ścigania, grup handlowych, organizacji traktatowych i agencji rządowych. Korzyści dla członków APWG obejmują: izby wymiany danych o zdarzeniach związanych z cyberprzestępczością, narzędzia do reagowania na cyberprzestępczość dla profesjonalistów z sektora prywatnego, publicznego i organizacji pozarządowych, którzy zwalczają cyberprzestępczość; konferencje budujące społeczność dla specjalistów ds. zarządzania cyberprzestępczością; narzędzia edukacji publicznej do zapobiegania cyberprzestępczości; opracowanie standardów wymiany danych o cyberprzestępczości oraz programów promujących badania nad cyberprzestępczością.25 Pod koniec lat 90. zaczęły pojawiać się komercyjne produkty antyspamowe, zaczynając od filtrów antyspamowych, z których mogą korzystać osoby fizyczne. Filtrowanie dostarczane jako usługa dla przedsiębiorstw pojawiło się w formie Brightmail, założonej w 1998 r. I obecnie będącej własnością Symantec, oraz Postini, założonej w 1999 r. I obecnie własnością Google. Wiele innych rozwiązań, niektóre bezpłatne i otwarte, inne komercyjne, próbowało usuń spam z kilku różnych kierunków. Niemniej jednak, pomimo wspólnych wysiłków wolontariuszy, prawodawców i przedsiębiorców, spam nadal wysysa zasoby sieciowe, ewoluując w kierunku subkultury nadużyć systemowych, która obejmuje dostarczanie ładunków, które robią znacznie gorsze rzeczy niż wywoływać oburzenie moralne

Dobra reputacja?

Ponieważ spam jest tworzony przez ludzi, komputer jest w stanie zidentyfikować spam ze 100-procentową niezawodnością, a wręcz niemożliwie. Fakt ten skłonił niektórych bojowników spamu do rozważenia alternatywnego podejścia: wiarygodnego identyfikowania legalnej wiadomości e-mail. Jeśli odbiorca wiadomości e-mail lub Agent przesyłania poczty może zweryfikować, że niektóre wiadomości

przychodzące pochodzą z legalnych źródeł, wszystkie pozostałe wiadomości e-mail można zignorować. Jedną z form tego podejścia jest system reagowania na wyzwania, być może największym wdrożeniem, które Earthlink wdrożył w 2003 r. Gdy wysyłasz wiadomość do kogoś w Earthlink, który używa tego systemu i nie otrzymał od ciebie wiadomości wcześniej Twoja wiadomość nie była natychmiast dostarczana. Zamiast tego Earthlink wysyła wiadomość e-mail z prośbą o potwierdzenie tożsamości w sposób, który byłby trudny do sfałszowania przez maszynę. Odbiorca jest następnie informowany o Twojej wiadomości i decyduje, czy ją przyjąć, czy nie. Niestety takie podejście może być problematyczne, jeśli użytkownik robi wiele e-commerce z wykorzystaniem wiadomości e-mail pochodzących z wielu źródeł, które są zasadniczo zautomatyzowanymi podmiotami odpowiadającymi (które nie mogą przejść wyzwania). Ręczne zbudowanie białej listy dozwolonych respondentów może być męczące, a ich niepodanie może oznaczać, że niektóre wiadomości nie zostaną przesłane (np. jeśli nadawca jest maszyną, która nie wie, jak sobie z tym poradzić). Jednym z rozwiązań tego problemu jest skompilowanie niezależnej białej listy legalnych e-maili, których wiadomości są dozwolone bez pytania. To jest reputacyjne podejście do walki ze spamem i działa w następujący sposób:

* Bank of America zobowiązuje się nigdy nie spamować swoich klientów i wysyłać im tylko wiadomości e-mail, na które się rejestruje (czy to powiadomienie wyciągiem online, czy okazjonalne wiadomości o nowych usługach bankowych).

* E-mail Bank of America jest zawsze przyspieszany przez dostawców usług internetowych i nie jest blokowany jako spam.

* Bank of America pozostaje wierny swojej obietnicy, ponieważ jego reputacja jako legalnego podmiotu wysyłającego pocztę umożliwia mu prowadzenie działań związanych z pocztą elektroniczną z większą wydajnością.

Istnieją znaczne przeszkody finansowe i logistyczne, aby taki system działał i zwykle działa lepiej w przypadku większych przesyłek. Adopcja spotkała się również ze sceptycyzmem ze strony niektórych zwolenników prywatności i antyspamu, którzy podejrzewali, że celem takich systemów była jedynie legalizacja masowych wysyłek firm, które wciąż nie rozumiały potrzeby prowadzenia korespondencji wyłącznie z zezwoleniem. Bezlitosny atak spamu na światowe systemy pocztowe może ostatecznie doprowadzić wszystkie legalne firmy do faworyzowania niechcianych wiadomości e-mail, a tym samym uczynić system reputacji uniwersalnym. Trudne czasy gospodarcze mogą jednak kusić dawne czyste firmy, aby desperacko starały się zwiększyć spam. Inną i bardziej uniwersalną metodą wykluczenia spamu byłoby dostarczanie przez dostawców usług internetowych, a konsumenci akceptowania, tylko tych wiadomości e-mail, które zostały opatrzone weryfikowalną pieczęcią kryptograficzną. Stosunkowo prosty zautomatyzowany system do osiągnięcia tego celu został opracowany w 2001 r. Przez firmę o nazwie ePrivacy Group i okazał się bardzo udany w rzeczywistych próbach przeprowadzonych przez MSN i kilka innych firm. Jeśli zostanie przyjęty powszechnie, taki system może sprawić, że spamowanie stanie się przestarzałe, ale cel ten okazał się nieosiągalny. Sukces tego podejścia zależał od powszechnego wdrożenia, a projekt ostatecznie został skazany na konflikty między większymi dostawcami usług internetowych, pomimo chęci ePrivacy Group do publicznego udostępnienia technologii bazowej domeny. Najlepsze w podejściu opartym na reputacji rozwiązanie problemu spamu może być czymś, na co eksperci od bezpieczeństwa informacji nalegali od lat: powszechne stosowanie szyfrowania wiadomości e-mail. Jeśli coś takiego jak Bezpieczne / Wielofunkcyjne rozszerzenia poczty wewnętrznej (S / MIME) zostanie powszechnie zaimplementowane, każdy może zignorować wiadomości, które nie zostały podpisane przez osoby, od których chętnie otrzymywały wiadomości e-mail. Oczywiście fakt, że szyfrowanie wiadomości e-mail może działać niezawodnie, nie jest dowodem na to, że zawsze tak będzie, a samo podejście do szyfrowania samo w sobie nie rozwiązuje podstawowej bariery dla wszelkich powszechnych wysiłków

zmierzających do zakazania spamu: chęci wszystkich do uczestnictwa . Jedną z cech, które sprawiły, że poczta e-mail stała się najczęściej używaną aplikacją w Internecie, brak centralnej kontroli, jest słabością, jeśli chodzi o wpływ na jakąkolwiek poważną zmianę w jej działaniu.

Przekazywanie problemów

Rozważając ogólnie problem spamu, pytanie brzmi, dlaczego dostawcy usług internetowych pozwalają ludziom na wysyłanie spamu. Faktem jest, że wielu nie. Spamowanie stanowi naruszenie prawie wszystkich warunków świadczenia usług przez każdego dostawcę usług internetowych. Konta używane do spamowania są często zamykane. Jednakże, jest kilka wyjątków. Jak można sobie wyobrazić, niektórzy dostawcy usług internetowych zezwalają spamowi na uzyskiwanie korzyści biznesowych (aczkolwiek firmy, które nie chcą innych). Niektórzy z tych dostawców usług internetowych korzystają z udogodnień w krajach skrajnych, aby uniknąć nadzoru regulacyjnego. Co więcej, niektórzy spamerzy uważają, że łatwiej i taniej jest kraść usługi i korzystać z nieautoryzowanego dostępu do serwerów innych osób w celu wysyłania ich wiadomości. Zjawiskiem wiadomości e-mail jest przekazywanie poczty. Według Janusza Łukasiaka z University of Manchester przekazywanie poczty następuje „gdy serwer pocztowy przetwarza wiadomość pocztową z nieautoryzowanego źródła zewnętrznego, przy czym ani nadawca, ani odbiorca nie są użytkownikiem lokalnym. Serwer pocztowy jest całkowicie niepowiązaną stroną trzecią do tej transakcji i wiadomości nie należy przekazywać przez serwer. ” Problem z nieuwierzytelnionymi stronami trzecimi polega na tym, że mogą ukryć swoją tożsamość. Na początku Internetu wiele serwerów pozostawało otwartych, aby ludzie mogli wygodnie przekazywać pocztę elektroniczną za ich pośrednictwem w dowolnym momencie. Wysyłanie wiadomości e-mail za pośrednictwem dowolnego serwera pocztowego było całkiem do przyjęcia, ponieważ wpływ na zasoby był minimalny. Nadużycia ze strony spamerów, których masowe wiadomości e-mail mają wpływ na zasoby, doprowadziły do wprowadzenia ograniczeń przez dostawców usług internetowych. Niektórzy usługodawcy internetowi wymagają użycia portu 587 do uwierzytelniania SMTP. Inni wymagają zalogowania się na serwerze POP, aby odebrać pocztę przychodzącą przed wysłaniem. Ponieważ wymaga to nazwy użytkownika i hasła, uniemożliwia nieznajomym wysyłanie wiadomości e-mail przez serwer. Otwarte przekaźniki są teraz marszczone. Przekazywanie nadal jednak występuje, częściowo dlatego, że konfigurowanie serwerów w celu uniknięcia tego wymaga wysiłku. Ponadto spamerzy wciąż szukają nowych sposobów wykorzystania zasobów, które nie są całkowicie chronione. Na przykład filtrowanie portu 25, ustanowione w celu ograniczenia spamowania, można ominąć sztuczkami, takimi jak routing asynchroniczny i serwery proxy. Stosunkowo nowym zjawiskiem jest wykorzystywanie botnetów, grup zainfekowanych komputerów do dostarczania spamu. Nieustannie toczy się wojna między spamerami i dostawcami usług internetowych, która rozciąga się na dostawców usług internetowych - większość dostawców usług internetowych faktycznie korzysta z usług jeszcze większego dostawcy usług, takich jak AT&T, MCI i Sprint, które są podstawą Internet. Ile problemów mają te firmy ze spamem?

Już w 2002 roku nadużycia sieciowe (spam) generowały 350 000 zgłoszeń problemów co miesiąc u jednego przewoźnika. Firmy te ciężko pracują, aby uniemożliwić przekazywanie poczty i pokonać najnowsze sztuczki, które spamerzy wymyślili, aby obejść środki zapobiegawcze.

Czarne dziury i listy bloków

Listy czarnych dziur lub listy bloków katalogują adresy IP serwerów od dostawców usług internetowych, których klienci są uważani za odpowiedzialnych za spam, oraz od dostawców usług internetowych, których serwery zostały przejęte w celu przekazywania spamu. Dostawcy usług internetowych i organizacje subskrybują te listy, aby dowiedzieć się, które wysyłające adresy IP

powinny zostać zablokowane. Odbiorca, taki jak dostawca usług internetowych odbiorcy, sprawdza listę pod kątem podłączonego adresu IP. Jeśli adres IP odpowiada adresowi na liście, połączenie zostaje zerwane przed zaakceptowaniem ruchu. Inni usługodawcy internetowi wybierają po prostu ignorowanie lub czarną dziurę pakietów IP na swoich routerach. Wśród lepiej znanych list bloków są RBL, znane również jako MAPS Realtime Blackhole List, Spamcop i Spamhaus. W jaki sposób adres IP jednostki znajduje się na tych listach? Jeśli dostawca usług internetowych otwarcie zezwala na spam lub nie chroni odpowiednio swoich zasobów przed nadużyciami ze strony spamerów, prawdopodobnie zostanie zgłoszony na listę przez jednego lub więcej odbiorców takiego spamu. Raporty są składane przez osoby, które poświęcają czas na sprawdzenie nagłówka spamu, zidentyfikowanie winnego dostawcy usług internetowych i nominację na listę bloków. Różne listy blokowe mają różne standardy weryfikacji nominacji. Niektórzy testują wyznaczony serwer; inne uwzględniają liczbę nominacji. Jeśli dostawca usług internetowych, organizacja lub osoba zarządzająca serwerem pocztowym przypadkowo znajdzie się na liście, może poprosić o usunięcie, co zwykle wiąże się z testem przeprowadzonym przez organizację obsługującą listę bloków. Pamiętaj, że żadne z tych działań blokujących spamowanie nie jest oficjalne. Wszystkie listy bloków są samozwańcze i samoregulujące. Ustanawiają i egzekwują własne standardy. Jedynym środkiem odwoławczym dla podmiotów, które uważają, że zostały niesprawiedliwie zablokowane - a było ich wiele na przestrzeni lat - są działania prawne. Niektóre listy bloków są obsługiwane poza Stanami Zjednoczonymi, ale jeśli zagraniczna organizacja blokuje serwer znajdujący się w Stanach Zjednoczonych, prawdopodobnie można go pozwać w sądzie amerykańskim. Należy jednak pamiętać, że blokowanie nie jest wykonywane przez operatora listy bloków, lecz przez dostawców usług internetowych, którzy subskrybują listy i są nimi kierowani.

Filtry spamu

Systemy z listą bloków odfiltrowują wiadomości z niektórych domen lub adresów IP lub zakresu adresów IP; nie badają treści wiadomości. Filtrowanie spamu na podstawie treści można przeprowadzić na kilku poziomach.

Filtry użytkownika końcowego

Filtrowanie spamu prawdopodobnie rozpoczęło się na poziomie klienta i nawet dziś wielu użytkowników poczty e-mail wykonuje ręczne filtrowanie negatywne pod kątem spamu, identyfikując spam w procesie eliminacji. Jest to łatwe w przypadku dowolnej aplikacji e-mail, która pozwala filtrom lub regułom zdefiniowanym przez użytkownika kierować wiadomości do różnych skrzynek odbiorczych lub folderów. Wiele osób ma osobne skrzynki pocztowe, w których filtrują wszystkie wiadomości, które otrzymują od swoich zwykłych korespondentów, przyjaciół, rodziny, współpracowników, subskrybowanych newsletterów, i tak dalej. Oznacza to, że wszystko, co pozostanie w koszu, prawdopodobnie będzie spamem, z godnym uwagi wyjątkiem wiadomości od nowych korespondentów, dla których nie została jeszcze utworzona osobna skrzynka pocztowa i filtr. Aby wykonać filtr, który pozytywnie identyfikuje spam, należy zidentyfikować elementy wspólne dla wiadomości spamowych. Wiele produktów to robi i zazwyczaj są wyposażone w domyślny zestaw filtrów, które szukają takich rzeczy jak Adresy zawierające wiele liczb i Tekst tematu zawierający wiele znaków interpunkcyjnych - spamerzy często dodają je, próbując pokonać filtry w oparciu o na określonym tekście, więc temat wiersza „You're Approved” może być losowo połączony ze znakami specjalnymi i spacjami takimi jak ten:

„Ap You Ap approved! ∗∗”

W rzeczywistości sztuczki i poprawki wykorzystywane przez spamerów przy tworzeniu wiadomości zaprojektowanych w celu obejścia filtrów są praktycznie nieograniczone. Niemniej jednak nawet

filtrowanie spamu wbudowane w niektóre podstawowe programy pocztowe oferuje przydatną linię obrony. Niestety niektóre języki znajdujące się w spamie pojawiają się również w wiarygodnych wiadomościach, takich jak „Otrzymujesz tę wiadomość, ponieważ subskrybujesz tę listę" lub „Aby anulować subskrypcję, kliknij tutaj". Oznacza to, że domyślne ustawienie w filtrze spamu może blokować niektóre wiadomości, które chcesz otrzymać. Odpowiedzią jest albo osłabienie filtrowania, albo utworzenie białej listy prawidłowych adresów Od, aby filtr antyspamowy przepuścił wszystko z tych adresów. Większość osobistych filtrów antyspamowych może czytać książkę adresową i dodawać wszystkie wpisy do osobistej białej listy. Z czasem można dodawać nowych korespondentów. Większość osobistych filtrów antyspamowych kieruje wiadomości, które identyfikują jako spam, do specjalnego folderu lub koszyka, w którym użytkownik może je przejrzeć, co jest czasem określane jako kwarantanna. Aby uniknąć marnowania miejsca na dysku twardym, oprogramowanie do filtrowania można zaprogramować tak, aby opróżniało folder kwarantanny w ustalonych odstępach czasu lub po prostu usuwało podejrzany spam starszy niż ustalona liczba dni. Takie podejście do kwarantanny daje użytkownikowi czas na sprawdzenie i odzyskanie niesłusznie podejrzanego spamu.

Filtrowanie ISP

W obliczu skarg klientów na wzrost poziomu spamu na przełomie wieków dostawcy usług internetowych zaczęli wprowadzać filtrowanie spamu. Jednak wahali się przed filtrowaniem spamu na podstawie treści, obawiając się, że może to być interpretowane jako czytanie e-maili innych osób i prowadzić do roszczeń o naruszenie prywatności. Jednak dostawcy usług internetowych muszą być w stanie czytać nagłówki, aby kierować wiadomości e-mail, dlatego wprowadzono filtrowanie w polach Adres i Temat (stąd coraz bardziej pomysłowe próby spamerów polegające na losowym zmienianiu tekstu Temat). Niektórzy dostawcy usług internetowych stwierdzili, że niechęć do spamu osiągnęła poziom, na którym niektórzy użytkownicy byli gotowi zaakceptować zmienione warunki umowy, aby umożliwić maszynowy odczyt treści wiadomości e-mail w celu wydajniejszego filtrowania spamu. Nadal jednak istnieją problemy prawne dla dostawców usług internetowych, zwłaszcza że nie ma ogólnie przyjętej definicji spamu i nie ma konsensusu co do zakresu, w jakim wolność słowa dotyczy poczty elektronicznej. Na przykład, czy kandydaci polityczni mają prawo wysyłać niechciane wiadomości e-mail do wyborców? Czy dostawcy usług internetowych mają prawo to zablokować? Są to pytania, na które sądy i opinia publiczna nie wydały jeszcze rozstrzygającego wyroku. Jednym z miejsc, w którym filtry spamowe oparte na treści są wdrażane z niewielkimi lub żadnymi obawami dotyczącymi problemów prawnych, jest sieć korporacyjna. Z uwagi na fakt, że sieć firmowa należy do firmy, prawo do kontrolowania, w jaki sposób jest używana, przeważa nad kwestią prywatności. Pracownicy nie mają prawa do otrzymywania w pracy e-maili, które chcą otrzymywać. I większość firm twierdzi, że praktycznie nie ma korporacyjnego obowiązku dostarczania wiadomości e-mail do pracowników

Usługi filtrowania

Firmy takie jak Brightmail i Postini powstały pod koniec lat 90. XX wieku, aby oferować usługi filtrowania na poziomie przedsiębiorstwa. Brightmail opracował filtry, które znajdują się przy bramie do sieci korporacyjnej i filtrują na podstawie stale aktualizowanych reguł pochodzących z badań w czasie rzeczywistym na temat najnowszych epidemii spamu. Postini faktycznie przekierowuje wszystkie przychodzące wiadomości e-mail firmy na swoje serwery i filtruje je przed wysłaniem. Dzięki specjalizacji usługi filtrujące mogą wykorzystywać szeroki zakres technik walki ze spamem, w tym:

* Listy bloków

* Analiza nagłówka

* Analiza treści

* Filtrowanie w stosunku do bazy danych znanego spamu

* Filtrowanie heurystyczne dla atrybutów podobnych do spamu

* Dodanie do białej listy poprzez systemy reputacji

Ponieważ systemy te stale radzą sobie z ogromną ilością spamu, są w stanie dopracować filtry, zarówno pozytywne, jak i negatywne, szybko i względnie skutecznie. Przechwytują dużo spamu, który w przeciwnym razie dotarłby do konsumentów. Na przykład do 2008 r. Dziewięciu z 12 najlepszych dostawców usług internetowych korzystało z usługi Brightmail, która twierdzi, że ma bardzo niski współczynnik fałszywie dodatnich wyników i 95 procentowy wskaźnik połowu. Niestety nadal oznacza to, że część spamu przedostaje się do sieci, a gdy spamerzy mogą kierować miliony wiadomości na godzinę w sieci, ilość przesyłanych wiadomości wciąż może stanowić zagrożenie. Inne podejście wykorzystuje zbiorową inteligencję subskrybentów do szybkiego identyfikowania spamu i rozpowszechniania wiadomości za pośrednictwem połączeń sieciowych. Na przykład Cloudmark miał kilka milionów subskrybentów, płacąc około 40 USD rocznie, aby otrzymywać niemal natychmiastowe aktualizacje, z serwerów, które odbierają i kategoryzują raporty od członków na temat spamu, który przenika. Wynik wiarygodności członka wzrasta wraz z każdą poprawną identyfikacją spamu i znika z niepoprawnym oznaczeniem prawidłowego e-maila jako spamu (np. Biuletynów, o których członek zapomniał subskrybować). Wiarygodność reporterów pomaga systemowi ukrywać fałszywe informacje od spamerów, którzy mogą próbować zagrać w system, twierdząc, że ich własny spam jest legalny.

Szkody kolateralne

Filtry antyspamowe mają dwie główne wady. Po pierwsze, pozwalają spamerom kontynuować spamowanie. Innymi słowy, ponieważ muszą decydować, po wiadomościach, które wiadomości są spamem, a które nie, filtry zużywają dużo zasobów, w niektórych przypadkach więcej, niż gdyby cały spam został przepuszczony. Gdy listy bloków i białe listy działają dobrze, mogą znacznie zmniejszyć ilość spamu, który dociera do etapu filtrowania, ale ostatecznie wszystkie filtry są szeregowe, a zatem ograniczone zasoby i wymagające dużych zasobów. Po drugie, filtry czasami się mylą, na jeden z dwóch sposobów. Czasami generują fałszywy alarm, oznaczając prawidłową wiadomość jako spam, co uniemożliwia tak potrzebnej wiadomości dotarcie do odbiorcy w odpowiednim czasie. Czasami wytwarzają fałszywe negatywy, pozwalając na wysyłanie spamu do skrzynki odbiorczej. Fałszywe negatywy i fałszywie pozytywne wyniki ograniczają produktywność.

Spamowanie w rakietach śnieżnych

Było nieuniknione, że spamerzy dostosują się do opisanych powyżej środków filtrowania. Pod koniec 2012 r. rosnąca liczba spamerów rozpowszechniała swój spam wśród dużej liczby zainfekowanych serwerów, co doprowadziło do określenia spamowania w rakietach śnieżnych. Firma McAfee Labs podsumowała problem w następujący sposób:

Spamowanie na rakietach śnieżnych jest obecnie jednym z największych problemów ze spamem. Problem wybuchł w ciągu ostatnich dwóch lat i nadal będzie gwałtownie narastał z powodu braku ujawnienia informacji przez organy ścigania i groźby pozwów ze strony firm korzystających z nielegalnych list e-mail. Zjawisko to charakteryzuje się:

* Spamerzy wysyłają codziennie miliony rażąco nielegalnych wiadomości spamowych od nowo wynajmowanych hostów, dopóki nie zostaną eksmitowani z podsieci lub przejdą dalej.

* Odbiorcy bombardowani są w skrzynkach odbiorczych tymi wiadomościami spamowymi i nie mogą zrezygnować z nich, ponieważ nie są wysyłane z legalnego źródła.

* Rezultatem spamowania w rakietach śnieżnych są adresy z czarnej listy, a czasem podsieci.

* Ponieważ spamowanie jest raczej denerwujące niż złośliwe, władze w dużej mierze zignorowały ten problem, pomimo rosnącej liczby niechcianych wiadomości e-mail pochodzących z tych źródeł. Firmy korzystające z tych podejrzanych sprzedawców zagroziły wniesieniem pozwów o zniesławienie, gdy naukowcy próbowali ujawnić tę aktywność

Urządzenia sieciowe

Gwałtowny wzrost ilości spamu pod koniec lat 90. miał miejsce w czasie ogromnych ataków wirusów komputerowych i robaków z obsługą poczty e-mail, wynikających z klasycznej motywacji złośliwego oprogramowania do przechwalania się. Analiza tych problemów, zgodnie z klasycznymi czynnikami: środkami, motywami i możliwościami, ujawniła, że spamerzy znacznie różnią się od twórców wirusów. Spamerzy są głównie motywowani pieniędzmi, a nie chwaleniem się prawami. Ten wgląd otworzył nową linię obrony przed spamem, usuwając tę motywację. Pozostało tylko zrozumieć, w jaki sposób spamerzy zarabiają pieniądze, czyli ekonomię spamu, a następnie znaleźć sposób, by zakłócić tę ekonomię. Klasyczny model spamu polega na wysyłaniu dużej liczby e-maili oferujących produkt lub usługę, opierając się na tym, że przynajmniej niektóre z tych ofert trafią do prawdziwych ludzi, z których przynajmniej niektórzy dokonają zakupu. Jeśli osiągniesz wystarczającą sprzedaż, aby wygenerować zysk przewyższający koszty prowadzenia działalności, spamer będzie nadal działał. Chociaż dobry program edukacyjny i edukacyjny może zmniejszyć liczbę osób, które kupują oferty spamerów, jest mało prawdopodobne, aby odpowiednio zmniejszyć tę liczbę. ponieważ odfiltrowanie spamu ze strumienia wiadomości zmniejsza zwrot z inwestycji w spamera, powoduje, że spamerzy stają się bardziej pomysłowi w swoich próbach pokonania filtrów i wysyłają jeszcze więcej spamu w nadziei, że wystarczająco dużo się uda. W rzeczywistości spamerzy byli w stanie znaleźć firmy chętne sprzedać im przepustowość na masową skalę, w tym dedykowane cyfrowe połączenia telefoniczne T3. Innym sposobem na atak ekonomii spamu jest śledzenie pieniędzy. Każda umowa musi być zamknięta, zazwyczaj za pośrednictwem strony internetowej. Czy można zamknąć strony internetowe spamera? Ta linia zapytań doprowadziła autora do ciekawego odkrycia: spam bardzo szybko staje się przestarzały. Analiza archiwów spamu wykazała, że większość linków w starym spamie była martwa, czasami dlatego, że firma hostingowa zamknęła witrynę, a czasem dlatego, że spamer nie chciał ryzykować identyfikacji. W ten sposób ujawniono klucz do ekonomiki spamu: czas. Jeśli spowolnisz spam, spamerzy nie będą w stanie wygenerować wystarczającej liczby odpowiedzi przed usunięciem witryn z odpowiedziami. Wkrótce po tej realizacji ekspert ds. Bezpieczeństwa sieci David Brussin opracował sposób spowolnienia spamu poprzez kształtowanie ruchu TCP / IP. Ta technologia stała się sercem routera antyspamowego. Zamiast patrzeć po kolei na każdą wiadomość w celu ustalenia, czy jest to spam, router antyspamowy próbkuje ruch wiadomości w czasie rzeczywistym i spowalnia ten ruch, jeśli próbka sugeruje, że ruch zawiera spam. Dla spamerów, a raczej oprogramowania spamującego używanego przez spamerów, sieć chroniona za pomocą routera antyspamowego zachowuje się tak, jakby działała na modemie o prędkości 300 bodów. Innymi słowy, połączenie jest zbyt wolne, aby dostarczyć wystarczająco dużo wiadomości wystarczająco szybko, aby uzyskać trafienie jeden na milion, którego potrzebuje system spamowy, aby zarabiać pieniądze przed zamknięciem strony internetowej. Oprogramowanie do spamowania szybko przerywa połączenie; żadne wiadomości nie zostały utracone i żadne wiadomości nie zostały fałszywie oznaczone jako spam. Nie wpłynęło to na dostarczenie legalnej wiadomości e-mail. Dostarczono jedną lub dwie wiadomości spamowe, ale o wiele mniej niż pozwala na to 95-procentowy współczynnik typowego filtra spamu. Istnieją dwie główne sztuczki tej technologii. Jeden dostraja kształtowanie ruchu TCP / IP, drugi

dostraja proces próbkowania. Ten ostatni potrzebuje regularnych aktualizacji na temat tego, jak obecnie wygląda spam, aby mógł jak najszybciej zidentyfikować spamerskie połączenie. Te aktualizacje mogą pochodzić z usług, które stale identyfikują nowy spam. Panel sterowania aplikacją służy do dostrajania kształtowania ruchu. Administratorzy sieci stwierdzili, że odpowiednio dostrojony router antyspamowy może zmniejszyć wymagania dotyczące przepustowości nawet o 75 procent. Niestety router antyspamowy działa najlepiej w przypadku połączeń o dużej przepustowości, chroniąc MTA u dostawców usług internetowych, większych firm, szkół i agencji rządowych. Nie ma wersji komputerowej. Mimo to technologia stała się cenną częścią arsenału antyspamowego, chociaż plaga spamu nadal trwa.

Potwierdzenie email

Na poziomie technicznym spam może nadal rozprzestrzeniać się w postaci braku uwierzytelnienia nadawcy w protokole SMTP. Kilka inicjatyw próbowało zmienić tę sytuację, zmieniając protokół SMTP lub dodając do niego kolejną warstwę. Jednym z oczywistych sposobów uwierzytelnienia wiadomości e-mail jest nazwa domeny nadawcy i zaproponowano wiele sposobów osiągnięcia tego celu:

* Sender Policy Framework (SPF). Rozszerzenie SMTP, które pozwala oprogramowaniu na identyfikację i odrzucanie fałszywych adresów w SMTP MAIL FROM (Return-Path), które zazwyczaj wskazują na spam. SPF jest zdefiniowany w Experimental RFC 4408.30

* Certyfikowana weryfikacja serwera (CSV). Techniczna metoda uwierzytelniania wiadomości e-mail, która koncentruje się na tożsamości SMTA HELO MTA.

* SenderID. Propozycja ochrony przed kradzieżą z byłej grupy roboczej MARID IETF, która dołączyła do Sender Policy Framework i Caller ID. Identyfikator nadawcy jest zdefiniowany przede wszystkim w eksperymentalnym dokumencie RFC 4406.31

* DomainKeys. Metoda uwierzytelniania wiadomości e-mail zapewniająca kompleksową integralność od MTA podpisującego do MTA weryfikującego działającego w imieniu odbiorcy. Wykorzystuje nagłówek podpisu zweryfikowany przez pobranie i sprawdzenie opinii publicznej nadawcy

klucz przez Domain Name System (DNS).

* DomainKeys Identified Mail (DKIM). Specyfikacja, która łączy DomainKeys i Identified Internet Mail, schemat uwierzytelniania poczty e-mail obsługiwany przez Cisco, w celu utworzenia ulepszonej implementacji.

Po prawidłowym wdrożeniu wszystkie te metody mogą skutecznie zapobiegać fałszowaniu, które umożliwiło dominowanie spamu w poczcie e-mail. Każdy ma różne zalety i wady oraz wymagania. SPF, CSV i SenderID uwierzytelniają tylko nazwę domeny. SPF i CSV mogą odrzucić fałszerstwa przed przesłaniem danych wiadomości. DomainKeys i DKIM używają podpisu cyfrowego do uwierzytelnienia nazwy domeny i integralności treści wiadomości. Aby SenderID i DomainKeys działały, muszą przetwarzać nagłówki, więc wiadomość musi zostać przesłana. Oczywiście schemat taki jak DomainKeys sprawia, że poczta elektroniczna jest bardziej złożona niż SMTP. Wymagane są dodatkowe dane i nakład przetwarzania. Rekordy DNS muszą zostać rozszerzone i utrzymywane. Jednak wysiłek może być tego wart. Chociaż coś takiego jak DomainKeys nie zapobiega nadużyciom e-mail, ułatwia wykrywanie i śledzenie nadużyć e-mail w chronionych domenach, a to zniechęca do spamowania, ponieważ wydano już kilka sztywnych zdań dotyczących spamowania. Od 2004 r. Usługi e-mailowe zarówno Yahoo, jak i Google podpisały wychodzące wiadomości e-mail z DomainKeys, ale nie jest

jeszcze jasne, czy którykolwiek z opisanych schematów lub ich pochodna stanie się standardem dla wszystkich wiadomości e-mail. I na tym polega pocieranie. Spam mógłby zostać skutecznie odsunięty na bok, gdyby wszystkie wiarygodne wiadomości e-mail były wiarygodnie uwierzytelnione; adresaci mogą po prostu zignorować wszystkie nieuwierzytelnione wiadomości. Jest to jednak duże, jeśli.

Inicjatywy branżowe

W 2002 roku, za namową rzeczników konsumenckich, agencji rządowych i wielu dużych korporacyjnych użytkowników poczty elektronicznej, najwięksi dostawcy usług e-mail zaczęli organizować spotkania w celu omówienia jednolitego podejścia do ulepszania poczty elektronicznej i eliminowania spamu. Istniały duże nadzieje, że problem spamu zostanie rozwiązany przez tę grupę, znaną w branży jako AMEY, dla AOL, Microsoft, Earthlink i Yahoo !. Z pewnością było wiele zachęt. Na początku 2003 r. FTC, główna amerykańska agencja ochrony konsumentów, zwołała konferencję na temat spamu, a komisarze jasno stwierdzili, że chcą działań. Rzeczywiście, do końca 2003 r. Kongres uchwalił pierwsze federalne ustawodawstwo antyspamowe. W styczniu 2004 r. Ówczesny prezes i dyrektor generalny Microsoft Bill Gates ogłosił na Światowym Forum Ekonomicznym: „Za dwa lata spam zostanie rozwiązany". Dwa miesiące później firmy AMEY złożyły pozwy przeciwko osobom rzekomo będącym głównymi spamerami, twierdząc, że spam kosztuje firmy w Ameryce Północnej 10 miliardów dolarów rocznie z powodu utraty wydajności, modernizacji sieci oraz zniszczenia lub utraty danych. Jednak do stycznia 2006 r. Spam stanowił ponad trzy czwarte wszystkich wiadomości e-mail. Co poszło nie tak? Wielokrotne wysiłki mające na celu skłonienie firm AMEY do przyjęcia nowego, otwartego, bezpłatnego standardu stały się przedmiotem obaw dotyczących praw własności intelektualnej. Zarówno Microsoft, jak i Yahoo! potwierdzili własność części różnych mechanizmów przedstawionych w celu uwierzytelnienia wiadomości e-mail, a tym samym rozwiązali problem spamu. Jak na ironię brak zaufania między dużymi dostawcami usług internetowych spowodował brak zaufania do dostarczanej przez nich poczty.

Środki prawne

Przepisy dotyczące spamu zostały uchwalone przez wiele krajów, w tym Stany Zjednoczone. Ustawa CAN-SPAM z 2003 r. (Ustawa o kontroli napaści na nieproszoną pornografię i marketing, obowiązująca od 1 stycznia 2004 r.) Ustanowiła pewne wymagania dla każdego, kto wysyła komercyjny e-mail. Prawo przewiduje również kary dla spamerów i firm, których produkty są reklamowane w spamie. Prawo dotyczy „wiadomości e-mail, których głównym celem jest reklama lub promocja komercyjnego produktu lub usługi, w tym treści w Witrynie". Egzekwowanie ustawy CAN-SPAM jest przede wszystkim zadaniem FTC, ale ustawa upoważnia również Departament Sprawiedliwości do egzekwowania sankcji karnych. Inne agencje federalne i stanowe mogą egzekwować prawo wobec organizacji podlegających ich jurysdykcji, a dostawcy usług internetowych mogą również pozywać osoby naruszające CAN-SPAM. Oto główne przepisy prawa, jak stwierdził FTC:

* Zakazuje fałszywych lub wprowadzających w błąd informacji w nagłówku. Informacje Od, Do i informacje o routingu wiadomości e-mail - w tym nazwa domeny i adres e-mail pochodzący - muszą być dokładne i muszą identyfikować osobę, która zainicjowała wiadomość e-mail.

* Zabrania oszukańczych linii tematycznych. Wiersz tematu nie może wprowadzać odbiorcy w błąd co do treści lub tematyki wiadomości.

* Wymaga, aby Twój adres e-mail dał odbiorcom metodę rezygnacji. Musisz podać zwrotny adres e-mail lub inny internetowy mechanizm odpowiedzi, który pozwala odbiorcy poprosić Cię, aby nie wysyłał przyszłych wiadomości e-mail na ten adres e-mail, i musisz honorować prośby. Możesz utworzyć menu opcji, aby umożliwić odbiorcy rezygnację z niektórych rodzajów wiadomości, ale musisz

uwzględnić opcję zakończenia wiadomości komercyjnych od nadawcy. Każdy oferowany przez Ciebie mechanizm rezygnacji musi być w stanie przetwarzać prośby o rezygnację przez co najmniej 30 dni po wysłaniu komercyjnego e-maila. Po otrzymaniu prośby o rezygnację prawo daje ci 10 dni roboczych na zaprzestanie wysyłania wiadomości e-mail na adres e-mail wnioskodawcy. Nie możesz pomóc innemu podmiotowi w wysłaniu wiadomości e-mail na ten adres ani na wysłanie wiadomości e-mail w Twoim imieniu na inny adres. Wreszcie nielegalne jest sprzedawanie lub przekazywanie adresów e-mail osób, które zdecydują się nie otrzymywać wiadomości e-mail, nawet w formie listy mailingowej, chyba że przekażesz adresy, aby inny podmiot mógł przestrzegać prawa.

* Wymaga, aby komercyjny adres e-mail był identyfikowany jako reklama i zawierał prawidłowy fizyczny adres pocztowy nadawcy. Twoja wiadomość musi zawierać wyraźne powiadomienie, że wiadomość jest reklamą lub wezwaniem że odbiorca może zrezygnować z otrzymywania od ciebie więcej komercyjnych wiadomości e-mail. Musi także zawierać ważny fizyczny adres pocztowy. Pamiętaj, że wiadomości oparte na transakcjach lub relacjach - czyli wiadomości e-mail, które „ułatwiają uzgodnioną transakcję lub aktualizują klienta w istniejącej relacji biznesowej" - są również objęte tym, że wiadomości te nie mogą zawierać fałszywych lub wprowadzających w błąd informacji o routingu . reklamodawcy znajdą obszerną dyskusję na temat tego, czy CAN-SPAM był - i może kiedykolwiek - skuteczny, przeszukując Internet za pomocą dowolnej wyszukiwarki. Aby zapoznać się z krytyką prawa opublikowaną w lutym 2004 r., Zobacz „Czy CAN-SPAM może spamować?"

PHISHING

Wyłudzanie informacji to wykorzystanie niechcianego komercyjnego adresu e-mail w celu uzyskania drogą elektroniczną informacji o tobie, informacji, których normalnie nie ujawniłbyś nieznajomemu, takich jak numer konta bankowego, osobisty numer identyfikacyjny (PIN) i inne dane osobowe, takie jak numer ubezpieczenia społecznego. Przed 2002 rokiem praktycznie nie było żadnych działań phishingowych i stosunkowo niewiele w 2003 roku, ale do 2004 roku phishing stał się codziennym zagrożeniem i od tamtej pory jest niesłabnący. Jest to jedna z kategorii zagrożeń, które mogłyby zostać zmiażdżone wraz z resztą spamu, gdyby liderzy branży woleli współpracować niż konkurować o klientów w oparciu o obiecujący „lepszy antyspam niż inni".

Jak wygląda Phish.

Większość z nas po raz pierwszy dowiedziała się o phishingu, gdy otrzymaliśmy wiadomość e-mail o problemie z kontem, zwykle kontem bankowym, ale prawdopodobnie eBayem, PayPal, Amazon lub innym kontem online. Typowa wiadomość phishingowa ma wyglądać tak, jakby została wysłana przez duże przedsiębiorstwo, takie jak Bank of America, wraz z dokładnymi kopiami logo firmy, kroju pisma i terminologii. Na pierwszy rzut oka takie wiadomości mogą być dość przekonujące. Jeśli otrzymasz taką wiadomość, która odwołuje się do instytucji, w której masz konto, możesz ulec pokusie, aby je przeczytać. Możesz nawet ulec pokusie wykonania instrukcji, które prawdopodobnie doprowadzą Cię do strony internetowej, która prosi o poufne informacje. Rozważ tekst typowej wiadomości phishingowej:

„Otrzymujesz tę wiadomość, ze względu na twoją ochronę, nasza internetowa usługa bezpieczeństwa technicznego zagranicznego IP niedawno wykryła, że twoje konto internetowe zostało ostatnio zalogowane od godziny 77.32.11.84 bez międzynarodowego kodu dostępu (IAC) i z niezarejestrowanego komputera, który był niepotwierdzone przez nasz Dział Obsługi Online.

Jeśli ostatnio zalogowałeś się na swoje konto internetowe w poniedziałek, 5 maja 2007 r., do godziny 18:45 z zagranicznego IP ich panika nie jest potrzebna, ale jeśli zalogowałeś się na konto w powyższą datę i godzinę, uprzejmie poświęć 2-3 minuty na doświadczenie w bankowości internetowej, aby

zweryfikować i zarejestrować komputer, aby uniknąć kradzieży tożsamości, twoja ochrona jest naszą przyszłą nagrodą”

To, co na pierwszy rzut oka wydaje się bardzo oficjalnym i technicznym przekazem, okazuje się pełne błędów. Najlepszą rzeczą związaną z tymi wiadomościami jest ich usunięcie. Najgorsze, co można zrobić, to odpowiedzieć na nie. Do czasu gruntownego przeglądu bezpieczeństwa poczty e-mail żadna renomowana instytucja nie będzie używać poczty e-mail do żądania zmian lub aktualizacji poufnych informacji o koncie. Jeśli otrzymałeś wiadomość e-mail taką jak ta omówiona powyżej, ale nie posiadasz konta Bank of America, być może pomyliłeś się. Faktem jest, że osoby wysyłające te wiadomości phishingowe zwykle nie mają pojęcia, czy odbiorcy mają konta w instytucji wymienionej w wiadomości. Rzeczywiście, ten rodzaj niedopasowania jest najłatwiejszym sposobem wykrycia niektórych wiadomości phishingowych. Jeśli jednak phisher, który prawdopodobnie wysłał miliony kopii tego samego e-maila, ma szczęście i zdarza się, że masz konto w wymienionej instytucji lub jeśli wiadomość e-mail jest ogólna, sytuacja staje się nieco trudniejsza. Bardziej prawdopodobne jest, że otworzysz wiadomość, która wydaje się, często dość przekonująco, pochodzić z Twojego banku. Jeśli nie możesz się powstrzymać od spojrzenia na wiadomość e-mail dotyczącą problemu z kontem, oto kilka wskazówek, że wiadomość jest fałszywa. (Należy pamiętać, że nie sugerujemy, że wiadomości pozbawione tych wskazówek są zatem uzasadnione).

* Zwodniczy link. Większość wiadomości phishingowych stara się wyglądać, jakby były uzasadnione, na przykład za pomocą logo i grafiki skradzionych ze strony internetowej docelowej instytucji. Wszystkie wiadomości phishingowe, które widzieliśmy, zawierają również link do strony internetowej, na której użytkownik jest proszony o podanie danych, które phisher próbuje ukraść. Jednak ten link jest zwykle ukryty. Na przykład link może być długi i skomplikowany i zawierać nazwę banku, ale tak naprawdę nie może prowadzić do strony internetowej banku. Alternatywnie, link może wydawać się zwykłym i prostym tekstem, ale w rzeczywistości jest kodowany HTML, aby przejść gdzie indziej. Niektóre programy pocztowe, takie jak Eudora, ostrzegają przed tym oszustwem i pokazują prawdziwy link, gdy najedziesz myszką na tekst linku przed kliknięciem. Projekt linku w schemacie phishingowym może mieć kluczowe znaczenie dla jego sukcesu. Rosnąca liczba użytkowników jest odpowiednio nieufna wobec długich, złożonych lub jedynie liczbowych łączy adresów IP w wiadomości e-mail (np. „Kliknij http://123.212.192.68”). Przy użyciu kodowania HTML wiadomości zwykle zasłaniają adres docelowy. Link jest jednak istotny także w następnym etapie ataku, kiedy ofiara klika link. Jeśli adres URL witryny wyłudzającej informacje pojawi się jako adres numeryczny w polu adresu URL przeglądarki, ofiara może stać się podejrzana. Stosowane są różne techniki, aby ten adres wyglądał na wiarygodny.

* Zmień PIN / Hasło. E-maile z prośbą o zmianę poświadczeń dostępu do konta są bardzo podejrzane. Solidne firmy nie robią takich rzeczy za pośrednictwem poczty elektronicznej, ponieważ e-mail jest tak niewiarygodny. Żadna aktualizacja zabezpieczeń renomowanej witryny bankowej nie będzie wymagać zalogowania się na konto, aby je zresetować lub zapobiec zawieszeniu. I dlaczego uzasadniona wiadomość prosi o użycie hasła, które podobno zostało naruszone? Żadna agencja rządowa nie prosi o podanie danych uwierzytelniających lub danych osobowych za pośrednictwem poczty elektronicznej. Żadna loteria na Ziemi nie używa wiadomości e-mail do powiadamiania zwycięzców. Zignoruj te wiadomości lub zgłoś je jako spam i przejdź dalej.

* Zła pisownia, gramatyka i logika. Kto pomyślał, że te nudne lekcje gramatyki mogą być tak przydatne? Zła gramatyka, pisownia, a nawet błędna logika mogą być najszybszym sposobem wykrycia fałszywych wiadomości e-mail. Rozważ ten przykład: „Dlatego jeśli jesteś prawowitym posiadaczem konta, wypełnij poniższy formularz, abyśmy mogli sprawdzić twoją tożsamość. [Sic]” Jest tu znacząca

literówka (tożsamość dla tożsamości), a logika jest beznadziejna. Pomyśl o tym: dlaczego bank wysłałby do kogoś wiadomość e-mail, jeśli nie byłby pewien, czy dana osoba jest prawowitym posiadaczem konta? Ponownie, to nie jest tak, jak prawdziwe firmy prowadzą dziś działalność, więc po prostu idź dalej.

* Ogólne phish. Ogólne ostrzeżenia dotyczące kont są szczególnie nieprzyjemne. Są jednym ze sposobów, w jaki ataki phishingowe próbują obejść problem niewiedzy, gdzie ofiara (ty) ma konto. Na przykład wszystkie rachunki bankowe w Ameryce są ubezpieczone przez instytucję o nazwie Federal Deposit Insurance Corporation (FDIC). W 2004 roku ktoś dokonał szczególnie paskudnego ataku, który żerował na tym fakcie, potencjalnie porywając każdego z kontem bankowym. Był to jeden z pierwszych ataków phishingowych polegających na sfałszowaniu połączonego adresu URL przy użyciu luki w przeglądarce Microsoft Internet Explorer w celu zamaskowania rzeczywistego adresu URL. Jeśli kliknąłeś link w wiadomości, witryna, do której się udałeś, wyglądała tak, jakby to była www.fdic.gov, ale faktycznie doprowadziła do strony phishera.

Wzrost i zakres phishingu.

Można powiedzieć, że pojawiła się jakakolwiek nowa forma nadużycia komputerowego, gdy dostępny będzie zestaw narzędzi ułatwiający nadużycie. Zestawy phishingowe pojawiły się po raz pierwszy w 2006 roku, oferując skrypty, które umożliwiały atakującym automatyczne konfigurowanie witryn phishingowych fałszujących legalne witryny różnych marek (w tym nielegalne przywłaszczanie obrazów i logo kojarzonych przez konsumentów z tymi markami). Te skrypty pomagają generować odpowiednie wiadomości e-mail typu phishing. Przestępcy kontynuują ewolucję swoich narzędzi bez wytchnienia; w raporcie ze stycznia 2013 r. stwierdzono, że phisherzy włóczni zastosowali nowe narzędzie o nazwie Bouncer, które dostosowuje ich adresy URL w celu uwzględnienia unikalnych identyfikatorów ich zamierzonych ofiar; próba uzyskania dostępu do stron przestępców bez prawidłowego identyfikatora w adresie URL powoduje błąd 404 (brak takiej strony), co zakłóca analizę stron phishingowych przeprowadzoną przez naukowców. W lutym 2013 r. Analitycy stwierdzili, że „kiedy eksperci ds. Bezpieczeństwa przyglądali się niektórym z najbardziej znanych hacków w ostatnich latach - jedna szczególna grupa przestępcza wciąż zwracała na nich uwagę. Grupa komentująca, jak twierdzą znawcy branży, ma siedzibę w Chinach, oferuje hakowanie do wynajęcia - czy to dla osób fizycznych, korporacji czy rządów… ”

Przeszukują poszczególne firmy lub organizacje w celu znalezienia szczegółowych informacji, które pozwalają na bardzo szczegółowe tematy, a nawet treść wiadomości phishingowych. Na przykład dyrektor Coca-Coli rzekomo otworzył wiadomość phishingową od swojego szefa; link, który kliknął na pobrane oprogramowanie szpiegujące do swojego komputera i pozwolił chińskim szpiegom przemysłowym na wydobycie informacji, które utrudniły przejęcie największej chińskiej firmy produkującej napoje bezalkoholowe.

W kwietniu 2013 r. Departament Bezpieczeństwa Krajowego USA (DHS) ostrzegł „organizacje, które publikują wiele informacji biznesowych i osobistych na publicznych stronach internetowych i portalach społecznościowych”, aby tego nie robić. W październiku 2012 r. Phisherzy zebrali szczegółowe informacje o pracownikach z publicznego postu opublikowanego przez firmę energetyczną, która podaje listę uczestników konferencji. Oprócz ataków typu „spear phishing” na nazwane osoby „Złośliwe wiadomości e-mail, które prawdopodobnie pochodziły od jednego z uczestników, zostały wysłane do innych osób na liście, informując ich o zmianie adresu e-mail nadawcy. Odbiorcy zostali uprzejmie poproszeni o kliknięcie załączonego linku, który natychmiast przekierował ich na stronę zawierającą złośliwe oprogramowanie. ” APWG to cenne repozytorium informacji statystycznych na

temat phishingu. Ich raport na temat phishingu w czwartym kwartale 2013 r. Zawiera następujące ustalenia (są to bezpośrednie cytaty sformatowane jako punktory z usuniętymi odnośnikami do stron):

* Ataki phishingowe przeciwko graczom online znacznie wzrosły, z 2,7 procent wszystkich ataków phishingowych w trzecim kwartale do 14,7 procent w czwartym kwartale.

* Usługi finansowe były nadal najbardziej ukierunkowanym sektorem przemysłu w czwartym kwartale 2012 r., A usługi płatnicze były opóźnione.

* Dane uwierzytelniające do gry online są cenne dla niektórych przestępców, którzy sprzedają je na czarnym rynku. Przedmioty w grze przechowywane na tych kontach mogą być również sprzedawane przez phisherów za gotówkę w prawdziwym świecie. Ofiary mogą nawet zostać skradzione z prawdziwej tożsamości.

* Ataki na media społecznościowe podwoiły się do 6 procent, w porównaniu z 3 procentami w trzecim kwartale.

* W czwartym kwartale około 30 procent komputerów osobistych na całym świecie zostało zainfekowanych złośliwym oprogramowaniem.

* Ponad 57 procent komputerów w Chinach mogło zostać zainfekowanych, podczas gdy komputery w krajach europejskich były zainfekowane najrzadziej.

* Z wyjątkiem października 2012 r. Liczba witryn phishingowych zmniejszała się co miesiąc od kwietnia 2012 r. Do grudnia 2012 r.

* W kwietniu 2012 r. Wykryto 63 253 unikalnych witryn phishingowych, spadając do 45 628 w grudniu 2012 r.

* W grudniu APWG otrzymało raporty o 28 195 unikalnych witrynach phishingowych. Suma w grudniu była o 31 procent niższa niż najwyższa z 40 621 raportów z sierpnia 2009 r.

* Używanie oprogramowania przestępczego nieznacznie spadło w tym kwartale w stosunku do poprzedniego, podobnie jak użycie

złośliwego oprogramowania kradnącego dane.

* Wykorzystanie innego złośliwego oprogramowania wzrosło o statystycznie znaczącą ilość w porównaniu z poprzednim kwartałem

Gdzie jest zagrożenie?

Phishing wydaje się początkowo problemem osobistym, kwestią bezpieczeństwa komputerów konsumenckich, a nie bezpieczeństwa informacji w przedsiębiorstwie. Rzeczywiście, agencja federalna odpowiedzialna za ochronę konsumentów, FTC, aktywnie edukuje konsumentów na temat problemu i sposobów unikania oszustw przez te wiadomości. Jednak phishing stanowi również komputerowe zagrożenie dla informacji i dobrobytu firm, a także ogólnie dla handlu elektronicznego. Ataki phishingowe zbierają nazwy użytkowników i hasła. Wiele osób korzysta z tych samych danych uwierzytelniających w systemach związanych z pracą, jak w systemach osobistych (w tym szef bardzo tajnego urzędu rządowego, który, jak się okazało, używa swojego bankowego numeru PIN bankomatu jako ściśle tajnego hasła sieciowego). Wiadomo, że hakerzy kryminalni przenikali do systemów, zbierając osobiste dane uwierzytelniające i stosując je do loginu biznesowego celu. Tak więc firmowy program uświadamiający bezpieczeństwo komputerów dobrze by zawierał ostrzeżenia przed atakami phishingowymi. Oprócz zagrożenia przenikaniem phishing może podważyć zaufanie konsumentów do

firmy. Chociaż nie wydaje się uczciwe, aby konsumenci mieli pretensje do Bank of America, ponieważ przestępca próbował ich oszukać, nadużywając tożsamości banku, takie resentymenty istnieją i należy je rozumieć w kontekście biznesowym. Automatyzacja poprawia opłacalność bankowości, dlatego banki zachęcają klientów do korzystania z usług online i oferują zachęty do rezygnacji z wyciągów papierowych i powiadomień. Jeśli jednak postrzega się banki jako zapewniające automatyzację na niskich kosztach, z wbudowanymi niewystarczającymi zabezpieczeniami chroniącymi prywatność klientów i dostęp do konta, niektórzy konsumenci sprzeciwiają się, spowalniając tempo automatyzacji i zagrażając wzrostowi wydajności, potencjalnie wpływając na wynik finansowy.

Walka z phishingiem

Przedstawiono pewne sprytne zabezpieczenia technologiczne specyficzne dla phishingu, takie jak metody umożliwiające przeglądarkom weryfikację adresów URL, ale najlepszą obroną jest dwojakie podejście, które jest całkowicie oczywiste. Pierwszym krokiem jest edukacja na poziomie konsumenckim i korporacyjnym, która uczy ludzi rozpoznawania ataków phishingowych i unikania ich ofiary. Drugim krokiem jest ustalenie podstaw wiadomości e-mail w sposób opisany wcześniej w odniesieniu do spamu. Z technicznego punktu widzenia mamy już do tego technologię. Brakuje tylko chęci wiodących dostawców usług do podjęcia skoordynowanych działań. Być może banki i inne instytucje mogą je do tego zachęcić, jeśli poczta elektroniczna będzie bezpieczniejsza. Brak działania w zakresie bezpieczeństwa poczty e-mail kosztował już miliardy dolarów zainwestowanych zasobów i utratę produktywności, ale efekty idą dalej, o czym świadczy pojawiająca się relacja między phishingiem, spamowaniem, hakowaniem przestępczym, kodem trojana, zbieraniem danych osobowych i naruszeniem bezpieczeństwa konta . Zastosowanie umiejętności takich jak pisanie wirusów i robaków do celów komercyjnych zostało umożliwione przez gotowość spamerów do płacenia za zainfekowane hosty, za pomocą których można przeprowadzać ataki i zbierać dolary i / lub dane. Techniki spamowania umożliwiły rozwój phishingu, co z kolei utrwaliło czarny rynek zainfekowanych hostów i skradziono dane osobowe. Nowe typy ataku stale wyłaniają się z tego bezbożnego sojuszu między programistami i przestępcami. Adresy e-mail zebrane przez spam mogą być wykorzystywane do ataków typu „phishing spear", na które określona firma jest kierowana za pośrednictwem wiadomości e-mail wysyłanych do znanych klientów lub pracowników (Departament Obrony stanął w obliczu wysypki ataków typu „spear phishing" w 2006 r.). Kod trojana rozpowszechniany metodami spamowymi został wykorzystany do uszkodzenia lokalnych serwerów nazw domen i wywoływania tego samego efektu, co bałagan w phishingu: użytkownicy są przekierowywani na złośliwe strony internetowe poprzez kliknięcie pozornie poprawnego adresu URL. (Ataki DNS tego typu są określane jako pharming).

KOD TROJANA.

Podobnie jak oryginalny koń trojański, wdrożony przez Greków w celu pokonania Trojan chronionych przez nie do zdobycia mury miasta Troja, trojan komputerowy jest złą rzeczą przebraną za dobrą rzecz (gdzie Troja jest twoim komputerem, a Grecy są osoby, które chcą uzyskać nieautoryzowany dostęp). Technologia przeszła długą drogę od „wierzchowca o monstrualnej wysokości" opisanego w Eneidzie Wergiliusza, ale cel kodu trojana jest taki sam jak w przypadku oryginalnego konia trojańskiego: oszukać obrońcę z chronionego miejsca, aby umożliwić dostęp osobom postronnym. Niemal jak tylko Internet umożliwił rozpowszechnianie kodu wykonywalnego, linków do pobrania lub załączników do wiadomości e-mail, niektóre osoby postanowiły wykorzystać tę możliwość do rozpowszechniania swojego kodu bez wyraźnej zgody. Innymi słowy, niewinna partia może ulec pokusie pobrania pozornie niewinnego pliku wykonywalnego, co w rzeczywistości było czymś innym. Osoba wykonująca

pobieranie robi to celowo, ale nie zna intencji osoby, która spreparowała kod trojana w pliku wykonywalnym.

Klasyczne i najnowsze trojany.

Pomimo faktu, że ekrany dzisiejszych komputerów nie wymagają zapisywania, wygaszacze ekranu nadal są źródłem kodu trojana. Niektórzy użytkownicy najwyraźniej uważają obietnicę animowanych wodospadów i akwariów za trudną do oparcia. To prowadzi użytkowników do pobierania wygaszaczy ekranu, które napotykają na stronach internetowych lub otwierania plików wygaszacza ekranu, które otrzymują w wiadomości e-mail. Twórca tego wygaszacza ekranu trojana, odkryty w lutym 2007 r., Najwyraźniej był niezadowolony z popularnej w Japonii sieci udostępniania plików o nazwie Winny. Gdy ten wygaszacz ekranu jest otwarty, trojan wyświetla obraz ostrzegający operatora komputera przed użyciem Winny. Ta taktyka przypomina niektóre z najwcześniejszych wirusów, które starały się rozprzestrzeniać stosunkowo nieszkodliwe wiadomości, a nie powodować szkody. W rzeczywistości kod nie musi być złośliwy, aby zostać uznanym za trojana - wystarczy, że zostanie zainstalowany bez pozwolenia. Niestety w tym konkretnym przypadku trojan niszczy dane, zastępując niektóre pliki (np. Pliki z rozszerzeniami .txt i .jpg). Innym przykładem trojana wygaszacza ekranu jest ten, który krąży jako załącznik e-mail o nazwie bsaver.zip w lipcu 2007 r. Po otwarciu pliku w załączniku ZIP system zostaje zainfekowany koniem trojańskim Agent-FZB, który następnie upuszcza dwa rootkity, aby uniknąć wykrycia przez oprogramowanie zabezpieczające i udostępnić system nieautoryzowanym użytkownikom. Ten wygaszacz ekranu był dystrybuowany przez kampanię spamową zawierającą takie tematy wiadomości jak Życie jest piękne, Życie będzie lepsze, Dobre lato i pomoc. Tekst wiadomości zawierał zwroty typu „Dzień dobry / wieczór, stary! Naprawdę fajny wygaszacz ekranu twoje przywiązanie! ” Nowsze raporty o trojanach obejmują następujące przypadki i badania:

* Trojan BackDoor.Wirenet.1 został zidentyfikowany w sierpniu 2012 r .; szkodliwe oprogramowanie „to pierwszy koń trojański, który działa na platformach Mac OS X i Linux i jest przeznaczony do kradzieży haseł przechowywanych przez wiele popularnych aplikacji internetowych”.

* „PandaLabs Q1 Report” za 2013 r. Wykazał, że „trojany ustanowiły nowy rekord, powodując prawie 80 procent wszystkich infekcji komputerowych

na całym świecie. Pomimo niezdolności do replikacji trojany są zdolne do wywoływania masowych infekcji za pośrednictwem zainfekowanych witryn sieci Web, które wykorzystują luki we wtyczkach przeglądarek, takich jak Java, Adobe Reader itp. Ta metoda ataku umożliwia hakerom zainfekowanie tysięcy komputerów

w ciągu zaledwie kilku minut z tym samym trojanem lub innymi, ponieważ atakujący mają możliwość zmiany używanego trojana na podstawie wielu parametrów, takich jak lokalizacja ofiary, używany system operacyjny itp. ”

* W marcu 2013 r. Kaspersky Labs poinformował, że nowy atak spyware na działaczy wolności Tybetu wykorzystał trojana zaprojektowanego dla systemu operacyjnego Android na telefony komórkowe.

* Trojan Flashback zainfekował ponad 600 000 komputerów Macintosh na początku kwietnia 2013 r., Wykorzystując lukę w Javie.

* W kwietniu 2013 r. Przestępcy wysłali zaproszenia do obejrzenia materiału wideo z zamachu bombowego w Bostonie. Trojan zdalnego dostępu został zainstalowany jako „Sterownik pakietu WinPcap (NPF)”, aby uniknąć powiadomienia.

* W maju 2013 r. Graham Cluley z Sophos poinformował o trojanie (Mal / BredoZp-B) rozpowszechnianym w wiadomości e-mail rzekomo od Tiffany & Co., która twierdziła, że zawiera szczegółowe informacje na temat pozwolenia na wywóz i faktury płatniczej.

Trojan próbuje wyglądać na użyteczny lub interesujący, aby użytkownicy go zainstalowali, ale w nim ukryty jest nieautoryzowany, nieudokumentowany kod nieautoryzowanych funkcji, z których niektóre są wymienione tutaj:

* Usuwanie plików lub folderów lub całych dysków

* Zmiana danych w subtelny lub dramatyczny sposób

* Szyfrowanie danych (ewentualnie w celu wymuszenia)

* Kopiowanie danych na inne komputery (być może do celów szpiegostwa przemysłowego)

* Pobieranie plików bez zgody użytkownika (być może w celu nielegalnego handlu elektronicznego, nielegalnego udostępniania plików, hostingu strony z pornografią, taniego przechowywania)

* Uszkadza oprogramowanie przeglądarki i pliki sieciowe, aby przekierować użytkownika z legalnych stron do fałszywych, fałszywych, złośliwych stron

* Umożliwienie zdalnego dostępu do zaatakowanego systemu (czasem określanego jako RAT, dla trojana zdalnego dostępu), często wykorzystywanego do przekształcania komputerów w zombie, które można agregować w botnety (w celu spamowania, phishingu i wykonywania ataku typu „odmowa dostępu" ataki usługowe)

* Pomoc w rozprzestrzenianiu się wirusów za pomocą kodu kroplomierza w celu spowodowania infekcji

* Wyłączanie programów antywirusowych i zapory ogniowej

* Wyłączanie konkurencyjnych form złośliwego oprogramowania

* Rejestrowanie naciśnięć klawiszy w celu uzyskania danych, takich jak hasła i numery kart kredytowych

* Zgłaszanie aktywności przeglądania (włączenie programów szpiegujących)

* Zbieranie adresów e-mail w celu spamowania i innych działań, takich jak phishing

Motywy stojące za kodem trojana zazwyczaj należą do jednej lub więcej z trzech kategorii: złośliwości, praw do chwalenia się i zysków finansowych. Zyski można zrealizować na kilka sposobów. Dane skradzione można sprzedawać. Dostęp do zainfekowanych maszyn można sprzedać. Zaszyfrowane lub skradzione dane można okupować. Do wymuszenia można wykorzystać zagrożenia typu „odmowa usługi". Niektóre firmy wykorzystały nawet trojany do zwiększenia sprzedaży i zainstalowanej bazy oprogramowania.

Podstawowe taktyki anty-trojanowe.

Niestety trojany mogą być trudne do zwalczenia. Pierwszą linią obrony są dobrze wykształceni użytkownicy, którzy wiedzą lepiej, aby nie wykonywać kodów o wątpliwym pochodzeniu. Ostrzeżenia w tym zakresie powinny być częścią każdego programu uświadamiającego bezpieczeństwo komputerowe, a program uświadamiający bezpieczeństwo komputerowe powinien być częścią każdego modelu bezpieczeństwa przedsiębiorstwa. Techniczne środki mogą być użyte do zwalczania trojanów, ale ponieważ żaden z nich nie jest doskonały, nie ma sensu polegać na nich z powodu

zaniedbania edukacji użytkowników końcowych. W rzeczywistości myślenie o użytkownikach końcowych jako o operatorach komputerów, a nie o użytkownikach komputerów, może być dobrym początkiem, biorąc pod uwagę, że rola użytkownika implikuje względnie pasywną rolę w utrzymaniu integralności i zdrowia komputera, podczas gdy operator dokładniej odzwierciedla poziom odpowiedzialności wymaganej od każdego, kto zatrudnia komputer w pracy lub rekreacji. (Użytkownika komputera można przyrównać do osoby, która jedynie prowadzi samochód i nigdy nie sprawdza oleju ani opon; operator jest bliżej kierowcy, który wie, że bezpieczne i niezawodne przejście z punktu A do punktu B wymaga znacznie więcej niż tylko trzymania kierownicy i naciśnięciu odpowiedniego pedału.) Środki techniczne przeciwko trojanom zaczynają się od aktualizowania wszystkich poprawek systemu operacyjnego i aplikacji, uniwersalnego użycia rezydentnego oprogramowania antywirusowego, które skanuje przychodzące pliki, oraz regularnego skanowania całego systemu w stosunku do regularnie aktualizowanych baza wirusów. Jednocześnie pomaga uruchamiać rezydujące w pamięci oprogramowanie antybotowe, takie jak Norton AntiBot, zaprojektowane do rozpoznawania i udaremniania aktywności wskazującej na działanie botnetów. To oprogramowanie nie chroni bezpośrednio trojanów przed dostaniem się do komputera, ale minimalizuje szkody, które może powodować trojan. Konieczne jest również dobre rozwiązanie antyspamowe, ponieważ spam jest głównym wektorem ataków trojanów. Jeśli Jim w księgowości nigdy nie otrzyma takiej wiadomości o fajnym wygaszaczu ekranu, nigdy nie będzie miał ochoty otworzyć załączonego pliku. Kuszące mogą być nie tylko wygaszacze ekranu. W kwietniu 2007 r. Wykorzystano techniki spamowe do masowej dystrybucji wiadomości o nagłówkach takich jak „Worm Alert!" i „Wykryto robaka". Wiadomości przychodziły z załącznikiem pliku ZIP, który przedstawiał się jako łatka, która zapobiegałaby fałszywemu atakowi. Kiedy odbiorcy, zaniepokojeni działaniem, otworzyli plik ZIP, stwierdzili, że jest chroniony hasłem, a niektórzy uznali to za znak autentyczności. (Hasło zostało dołączone do wiadomości.) Kontynuacja instalacji doprowadziła do rootkita, wyłączenia oprogramowania zabezpieczającego, kradzieży poufnych informacji z komputera, którego dotyczy problem, i rejestracja w botnecie zainfekowanych komputerów. W ciągu 24 godzin Postini policzył prawie 5 milionów kopii tego trojana spamowego skierowanego do użytkowników jego usługi antyspamowej. Firma obliczyła, że ten jeden spam stanowił 87 procent wszystkich złośliwych programów rozprzestrzenianych w tym czasie za pośrednictwem poczty elektronicznej.

Blokowanie i kwarantanna.

Bardziej drastyczne środki anty-trojanowe obejmują zapobieganie nieautoryzowanym zmianom lub dodatkom do plików wykonywalnych oraz zapobieganie łączeniu się systemów z sieciami do czasu ich weryfikacji. Pomysł pokonania złośliwych plików wykonywalnych przez zamrożenie systemu operacyjnego i autoryzowanych aplikacji w znanym dobrym stanie sięga daleko, przynajmniej do początkowych dni działań antywirusowych. Jednak złożoność większości systemów operacyjnych i kodu aplikacji sprawia, że takie podejście jest co najmniej trudne. Rozważ pojawienie się Patch Patch jako standardowego sposobu utrzymania najczęściej używanego systemu operacyjnego na świecie. Rzeczywiście, od wielu lat wiele rozwoju oprogramowania opiera się na założeniu, że łatki i aktualizacje można zawsze wypchnąć, jeśli potrzebne, prawdopodobnie prowadzące do znacznie mniej rygorystycznej praktyki kodowania niż wtedy, gdy kod produkcyjny został wypalony na dysk, znacznym kosztem, a zmiany wymagały dalszej wysyłki dysków. Pomysł poddania komputerów kwarantannie podczas próby połączenia z siecią przy użyciu jakiejś formy kontroli dostępu do sieci oferuje nieco inne podejście do idei blokowania komputerów, aby nie można było zainstalować nieautoryzowanego kodu. Niektórzy menedżerowie ds. Bezpieczeństwa sieci w przedsiębiorstwach stosują to podejście, ponieważ coraz trudniej jest kontrolować niektóre punkty końcowe sieci, takie jak laptop firmowy, który podróżuje z pracownikiem do lokalizacji klienta i konferencji, hoteli i hotspotów WiFi, a nawet spędzać czas w miejscu pracy pracownika samochód i dom. Użyte w ten sposób laptopy napotykają

dowolną liczbę wektorów ataku. Do tych punktów końcowych można zastosować tradycyjne mechanizmy obrony, w tym ochronę hasłem, uwierzytelnianie biometryczne, szyfrowanie dysku i programy antywirusowe. Jednak może to nie wystarczyć, ponieważ wiele przedsiębiorstw odkryło, że ich koszt. Dlaczego więc nie uniemożliwić tym komputerom łączenia się z siecią korporacyjną, dopóki nie zostaną przeskanowane w poszukiwaniu nieautoryzowanych plików wykonywalnych, takich jak rutynowa kontrola kondycji? Takie podejście jest obiecujące, ale nie jest łatwe do wdrożenia. Ponadto pozostawia maszyny otwarte na atak, gdy są one z dala od sieci korporacyjnej. Rozpowszechniane spamem ćwiczenie phishingowe lub wygaszacz ekranu może nadal lobotomizować punkt końcowy między przeglądami i zagrażać poufności danych osobowych lub firmowych. Jak widać z Załącznika 20.5, tabeli opracowanej przez Symantec w 2011 r. W celu pokazania cen zapłaconych za różne formy danych w podziemnej gospodarce w 2009 i 2010 r., Zachęty finansowe dla takich działań są realne.

UWAGI KOŃCOWE.

Zagrożenia omówione tutaj wciąż ewoluują, podobnie jak omówione tutaj środki zaradcze, chociaż niektóre z nich mogą stać się przestarzałe z powodu nowych osiągnięć. Jeśli jest jedna lekcja, którą specjaliści ds. Bezpieczeństwa mogą wyciągnąć ze studiowania omawianych tutaj zagrożeń, jest tak, że ciągłe niepowodzenie w poprawianiu podstawowego bezpieczeństwa poczty elektronicznej przedłuży atak spamu, ataków phishingowych i trojanów. Druga lekcja polega na tym, że musimy nadal edukować użytkowników komputerów, aby nie padli ofiarą oszustw komputerowych. Trzecią lekcją może być potrzeba skuteczniejszego ścigania przestępców komputerowych oraz surowszych wyroków.