DLACZEGO BADAĆ HISTORYCZNE ZAPISY?

Każda dziedzina nauki i ekspertyzy rozwija wspólną wiedzę, która odróżnia profesjonalistów od amatorów. Jednym z elementów tej wiedzy jest wspólna historia znaczących wydarzeń, które ukształtowały rozwój tej dziedziny. Ta część zawiera krótki przegląd niektórych bardziej znanych (lub notorycznych) przypadków przestępstw komputerowych (w tym tych ataków na komputery i tych, w których pośredniczą komputery) w ciągu ostatnich czterech dekad.

PRZEGLĄD

Oto kilka ogólnych trendów z lat 60. XX wieku do połowy 2013 r :

* We wczesnych dekadach nowoczesnej technologii informatycznej przestępstwa komputerowe były dużej mierze popełniane przez niezadowolonych i nieuczciwych pracowników.

* Fizyczne uszkodzenie systemów komputerowych było znaczącym zagrożeniem do lat 80.

* Przestępcy często wykorzystywali autoryzowany dostęp do osłabionych systemów bezpieczeństwa, modyfikując dane w celu uzyskania korzyści finansowych lub niszcząc dane w celu zemsty.

* Wczesne ataki na systemy telekomunikacyjne w latach 60. doprowadziły do obalenia dalekosiężnych systemów telefonicznych w celach rozrywkowych i kradzieży usług.

* W miarę jak technologia telekomunikacyjna rozprzestrzenia się na cały świat IT, hobbystów o tendencjach kryminalnych nauczyło się przenikać systemy i sieci.

* Programiści w latach 80. zaczęli pisać złośliwe oprogramowanie, w tym programy samoreplikujące się, aby zakłócać działanie komputerów osobistych.

* Ponieważ Internet zwiększył dostęp do coraz większej liczby systemów na całym świecie, przestępcy wykorzystywali nieautoryzowany dostęp do słabo chronionych systemów w celu wandalizmu, działań politycznych i zysków finansowych.

* W miarę postępów lat 90. przestępczość finansowa polegająca na penetracji i obaleniu systemów komputerowych wzrosła.

* Rodzaje złośliwego oprogramowania zmieniły się w latach 90., wykorzystując nowe luki i wymierając, gdy systemy operacyjne zostały wzmocnione, tylko po to, by ulec nowym wektorom ataków.

* Nielegalne zastosowania poczty e-mail gwałtownie wzrosły od połowy lat 90. XX wieku, generując torrenty niezamówionych komercyjnych i fałszywych wiadomości e-mail.

* Przestępczość zorganizowana coraz bardziej angażuje się w systematyczną penetrację systemów finansowych i ukierunkowane oszustwa.

* Wspierani przez rząd agenci cywilni i wojskowi coraz częściej używają komputerowego szpiegostwa przemysłowego, aby uzyskać znaczącą przewagę ekonomiczną nad przemysłem i handlem w Ameryce Północnej i Europie.

Lata 60. i 70. XX wieku : SABOTAGE . Wczesne przestępstwa komputerowe często wiązały się z fizycznym uszkodzeniem systemów komputerowych i wywróceniem dalekosiężnych sieci telefonicznych.

Bezpośrednie uszkodzenie centrów komputerowych : W lutym 1969 r. doszło do największych zamieszek studenckich w Kanadzie, kiedy wezwano policję, aby położyć kres studenckiej okupacji kilku pięter budynku Hall. Studenci protestowali przeciwko profesorowi oskarżonemu o rasizm, a kiedy

weszła policja, wybuchł pożar i dane komputerowe i mienie uniwersyteckie zostały zniszczone. Łączne straty wyniosły 2 miliony dolarów, a 97 osób zostało aresztowanych. Thomas Whiteside skatalogował litanię wczesnych fizycznych ataków na systemy komputerowe w latach 60 i 70:

1968 Olympia, Waszyngton : IBM 1401 w tym stanie zostaje dwukrotnie postrzelony przez intruza z pistoletem

1970 University of Wisconsin : Bomba zabija jednego i rani trzy osoby oraz niszczy dane komputerowe za 16 milionów dolarów przechowywanych na serwerze

1970 Fresno State College : Koktajl Mołotowa powoduje uszkodzenie systemu komputerowego o wartości 1 miliona dolarów

1970 New York University : Radykalni studenci umieszczają bomby ogniowe na komputerze Komisji Energii Atomowej, próbując uwolnić uwięzioną Czarną Panterę

1972 Johannesburg, Republika Południowej Afryki : Komputer miejski jest wgnieciony przez cztery pociski wstrzelone przez okno

1972 Nowy Jork : Rdzeń magnetyczny w komputerze Honeywell został zaatakowany przez kogoś z ostrym narzędziem, powodując szkód za 589 000 $

1973 Melbourne, Australia : Protestujący przeciw wojnie strzelają do komputera amerykańskiej firmy za pomocą strzelby z podwójną lufą

1974 Charlotte, Karolina Północna komputer sfrustrowanego operatora zostaje zastrzelony przez komputer Charlotte Liberty Mutual Life Insurance Company Company

1974 Dayton, OH : Baza sił powietrznych Wright Patterson: Podejmowane są cztery próby sabotażu komputerów, w tym za pomocą magnesów, poluzowanych drutów i wyżłobień w sprzęcie

1977 Rzym, Włochy : Czterech terrorystów wylewa benzynę na komputer uniwersytecki i pali ją na popiół

1978 Lompoc, Kalifornia : Baza sił powietrznych Vandenburg: aktywistka pacyfostyczna niszczy nieużywany IBM 3031 za pomocą młotka, łomu, noża i akumulatorowej wiertarki elektrycznej jako protest przeciwko systemowi nawigacji satelitarnej NAVSTAR, twierdząc, że daje to Stanom Zjednoczonym zdolność pierwszego uderzenia

Incydenty związane z fizycznym wykorzystywaniem systemów komputerowych nie ustały, gdy wzrosły inne formy przestępstw komputerowych. Na przykład w 2001 r. Redaktorzy NewsScan podsumowali raport Wired Magazine:

Ankieta przeprowadzona przez brytyjskiego producenta komputerów Novatech, mająca na celu rzetelne spojrzenie na usterki techno, ujawniła ciemniejszą stronę komputerów. Według 4200 respondentów jeden na cztery komputery został fizycznie zaatakowany. W kwietniu 2003 r. Narodowe Centrum Ochrony Informacji i Departament Bezpieczeństwa Krajowego zgłosiło:

Nic nie zatrzymuje sieci tak łatwo i szybko, jak uszkodzenie fizyczne. Jednak ponieważ transmisja danych staje się siłą napędową korporacyjnej Ameryki, większość dużych firm nie dołożyła należytej staranności, aby ustalić, jak naprawdę odporne są na uszkodzenia ich linie życia danych. Tylko 20 procent średnich i dużych firm poważnie odrzuciło to, co dzieje się z ich połączeniami danych po wyjściu poza zaporę firmową, mówi Peter Salus z MatrixNetSystems, firmy zajmującej się optymalizacją sieci z Austin w Teksasie.

W połowie XXI wieku obawy dotyczące fizycznego bezpieczeństwa elektronicznych systemów głosowania wzrosły do poziomu świadomości społecznej. Na przykład:

Wózek elektronicznych urządzeń do głosowania Diebold został dziś dostarczony do pokoju wspólnego tego pensjonatu w Berkeley w Kalifornii, który będzie miejscem głosowania we wtorkowych wyborach głównych. Maszyny znajdują się na wózku owiniętym w folię (tak samo jak rzeczy, których używamy w kuchni). Kilka zamków kablowych (wydaje się, że zamki rowerowe) zapewniają pozory bezpieczeństwa fizycznego, ale nie są przewleczone przez każdą maszynę. Co więcej, ktoś majstruje przy blokadach kablowych, jak mi powiedziano, po niespełna minucie igrania ogłosił, że znalazł trzycyfrową kombinację jako tę samą małą liczbę całkowitą, powtarzaną trzy razy

1970–1972: Albert Sabotażysta.

Jeden z najbardziej pouczających wczesnych przypadków sabotażu komputerowego miał miejsce w National Farmers Union Service Corporation z Denver, gdzie komputer Burroughs B3500 doznał 56 awarii głowicy dysku w ciągu dwóch lat od 1970 do 1972 roku. Przestój trwał aż 24 godziny na awarię, średnio 8 godzin na zdarzenie. Eksperci Burroughs przylecieli kiedyś z całej USA i doszli do wniosku, że awarie muszą być spowodowane wahaniami mocy. Do czasu naprawy całego sprzętu i zainstalowania nowego okablowania, generatorów silników, wyłączników automatycznych i monitorów linii zasilania w sali komputerowej całkowite wydatki na sprzęt i budowę wyniosły ponad 500 000 USD (w 1970 r.). Łączne wydatki związane z przestojami i utratą możliwości biznesowych spowodowanymi opóźnieniami w dostarczaniu zarządowi informacji na czas nie są uwzględnione w tej wartości. W każdym razie, po tych wszystkich kosztach, awarie trwały sporadycznie, jak poprzednio. W tym czasie eksperci zaczęli zastanawiać się nad ich analizą. Po pierwsze, wszystkie wypadki miały miejsce w nocy. Czy to może być sabotaż? Na pewno nie! Stary Albert, operator nocnej zmiany, był bardzo pomocny przez te wszystkie lata; od razu bezzwłocznie wezwał do katastrofy, poszedł po kawę i pączki dla ekip remontowych i skrupulatnie zapisywał dokładne czasy i warunki każdej katastrofy. Jednak wszystkie awarie miały miejsce podczas jego zmiany. Kierownictwo zainstalowało kamerę telewizyjną (CCTV) w sali komputerowej - bez informowania Alberta. Przez kilka dni nic się nie działo. Pewnej nocy nastąpiła kolejna katastrofa. Na monitorze CCTV ochroniarze zobaczyli, jak dobry Albert otworzył szafkę na dyski i wsunął kluczyk do solenoidu głowicy odczytu / zapisu, powodując zwarcie i powodując 57. awarię głowy. Następnego ranka kierownictwo skonfrontowało Alberta z jego filmem i poprosiło o wyjaśnienie. Albert rozkleił się z mieszanym wstydem i ulgą. Przyznał się do przytłaczającej chęci wyłączenia komputera. Badanie psychologiczne wykazało, że Albert, któremu od lat wolno było pracować na nocnych zmianach, po prostu stał się samotny. Przybył dokładnie kiedy wszyscy inni wychodzili; wychodził , gdy wszyscy przybywali. Mijałyby godziny i dni bez najmniejszej interakcji człowieka. Nigdy nie chodził na kursy, nigdy nie uczestniczył w komitetach, nigdy nie czuł się związany z innymi w swojej firmie. Kiedy pierwsze wypadki głowy zdarzyły się spontanicznie - był zaskoczony i podekscytowany przybyciem ekipy remontowej. Czuł się przydatny, krzątał się i mówił im, co się stało. Kiedy wypadki stały się rzadsze, mimowolnie i prawie nieświadomie odtworzył przyjazną atmosferę zespołu kryzysowego. Zniszczył dyski, ponieważ potrzebował towarzystwa.

PODSZYWANIE

Używanie insygniów i specjalistycznego języka urzędników w ramach inżynierii społecznej ma długą historię przestępczości; dramatyzacja tych technik znajduje się w popularnym filmie Catch Me If You Can o Franku Williamie Abagnale Jr., nastoletnim oszuście i fałszerzu, który udawał pilota, lekarza i prokuratora, zanim ostatecznie stał się głównym uczestnikiem walki z podrabianiem przez rząd USA , a następnie założył dużą firmę ochroniarską. Kilku przestępców zaangażowanych w przestępstwa za pośrednictwem komputera lub zorientowane na komputer stało się znanych z podszywania się.

1970: Jerry Neal Schneider . Notoryczna przestępczość komputerowa rozpoczęła się w 1970 roku, kiedy nastolatek Jerry Neal Schneider użył Dumpster w celu pobrania wydruków z firmy Pacific Telephone and Telegraph (PT&T) w Los Angeles. Po latach gromadzenia miał wystarczającą wiedzę na temat procedur, że był w stanie podszyć się pod personel firmy przez telefon. Zebrał jeszcze bardziej szczegółowe informacje na temat procedur. Występując jako niezależny pisarz czasopism, nawet zwiedził skomputeryzowany magazyn i informacje o procedurach zamówień. W czerwcu 1971 r. zamówił wysłanie 30 000 USD sprzętu do normalnego punktu odbioru PT&T - i szybko go ukradł i sprzedał. W końcu miał magazyn o powierzchni 6000 stóp kwadratowych i 10 pracowników. Ukradł ponad milion dolarów sprzętu - i sprzedał część z nich PT&T. W końcu został zakapowany przez jednego ze swoich niezadowolonych pracowników i po zakończeniu odsiadki został konsultantem ds. bezpieczeństwa komputerowego

1980–2003: Kevin Mitnick

Urodzony w 1963 roku, Kevin Mitnick wcześnie zaangażował się w przestępczość, wykorzystując specjalny stempel do transferów autobusowych, aby uzyskać bezpłatne przejazdy w dowolnym miejscu w dolinie San Fernando w Kalifornii, gdy był nastolatkiem. Jego własne komentarze autobiograficzne pokazują, że brał udział w wyłudzaniu telefonicznym, złośliwych dowcipach i włamywaniu się do komputerów w Digital Equipment Corporation (DEC) za pomocą inżynierii społecznej. W 1981 roku on i jego przyjaciel Lewis De Payne wykorzystali socjotechnikę, aby uzyskać nieautoryzowany dostęp do centrum operacyjnego Pacific Bell; „Sąd dla nieletnich zlecił diagnostyczne badanie psychologiczne Mitnicka i skazał go na roczny okres próbny". W 1987 r. Został aresztowany za włamanie do komputerów operacji Santa Cruz, twórcy SCO UNIX, i skazany na trzyletni okres próbny. Latem 1988 roku Mitnick i jego wspólnik i przyjaciel Lenny DiCicco ponownie złamali komputery Uniwersytetu Południowej Kalifornii i sprzeniewierzyli setki MB miejsca na dysku (dużo w tym czasie) do przechowywania plików źródłowych VAX VMS skradzionych z Digital Equipment Corporation (DEC). Mitnick został aresztowany przez Federalne Biuro Śledcze (FBI) za kradzież kodu źródłowego VAX VMS. Podczas procesu opisano go jako cierpiącego na zaburzenie kontroli impulsów. W lipcu 1989 r. Został skazany na rok więzienia i sześciomiesięczną rehabilitację. Później próbował zostać prywatnym detektywem i specjalistą ds. bezpieczeństwa. Był ogólnie traktowany z wrogością przez ustanowioną społeczność bezpieczeństwa informacji. W listopadzie 1992 r. Mitnick ponownie zszedł do podziemia, kiedy FBI dostało nakaz aresztowania pod zarzutem kradzieży czasu komputerowego od firmy telefonicznej. Zlokalizowano go dwa lata później, kiedy popełnił błąd, pozostawiając obraźliwe wiadomości na komputerze i systemach poczty głosowej fizyka i eksperta od bezpieczeństwa internetowego Tsutomu Shimomury. Shimomura był tak zirytowany, że pomógł organom ścigania śledzić uciekiniera do Karoliny Północnej, gdzie Mitnick został aresztowany w lutym 1995 r. I uwięziony w toku. Mitnick został skazany przed sądem federalnym w Dystrykcie Centralnym Kalifornii w dniu 9 sierpnia 1999 r. I skazany na 46 miesięcy pozbawienia wolności za „cztery przypadki oszustw elektronicznych, dwa przypadki oszustw komputerowych i jeden przypadek nielegalnego przechwycenia komunikacji przewodowej". Mitnick był wcześniej skazany przez sędziego Pfaelzera na dodatkowe 22 miesiące więzienia, za posiadanie sklonowanych telefonów komórkowych, kiedy został aresztowany w Karolinie Północnej w 1995 r., oraz za naruszenie warunków nadzorowanego zwolnienia nałożonego po skazaniu go za niezwiązane z nim oszustwo komputerowe. Przyznał się do naruszenia warunków nadzorowanego wydania poprzez włamanie się do poczty głosowej PacBell i innych systemów oraz do współpracy ze znanymi hakerami komputerowymi, w tym przypadku współodpowiedzialnym Louisem De Payne. Po zwolnieniu z więzienia we wrześniu 2000 r. Mitnick miał odbyć trzyletnie zwolnienie warunkowe, podczas którego jego dostęp do komputerów był ograniczony, a jego zyski z pisania lub mówienia o karierze kryminalnej miały zostać zwrócone w celu zwrotu ofiarom. Mitnick utrzymywał się z cyklu wykładów i ostatecznie założył własną firmę konsultingową w

zakresie bezpieczeństwa. Przez lata po wyjściu z więzienia współpracował przy pisaniu kilku książek na temat inżynierii społecznej. Być może jego najbardziej znaczącą pozycją w historii przestępczości komputerowej jest to, że stał się ikoną podziemia przestępczego. „FREE KEVIN" był popularnym składnikiem wandalizmu internetowego przez wiele lat, a Eric Corley, wieloletni redaktor kryminalnej publikacji 2600: „The Hacker Quarterly" nakręcił nawet film „Freedom Downtime" na temat tego, co przestępcze podziemie określa jako rażąco niesprawiedliwe traktowanie Mitnicka przez rząd federalny i media.

Oszustwo związane z kartą kredytową .

Kredyty w lokalnych firmach sięgają nieudokumentowanej przeszłości. W Stanach Zjednoczonych karty kredytowe pojawiły się w połowie lat dwudziestych XX wieku, kiedy firmy benzynowe zaczęły wydawać karty rozpoznawane na stacjach w całym kraju. W 1950 r. Frank X. McNamara założył Diners Club, pierwszą firmę obsługującą karty kredytowe obsługującą wiele rodzajów firm; firma rozpoczęła praktykę pobierania opłaty procentowej za każdą transakcję, a także pobierała od swoich klientów opłatę członkowską. Karta VISA ewoluowała z Bank of America w 1951 r. Bank of America, a wkrótce potem konsorcjum banków w Kalifornii ustanowiło MasterCard. Program American Express rozpoczął program kart w 1958 roku. Wykorzystanie kart wzrosło i, co nie dziwi, oszustwo związane z kartami kredytowymi było powszechne. Kradzież poczty stała się również powszechna, gdy pozbawione skrupułów osoby odkryły, że koperty zawierające karty kredytowe są jak koperty pełne gotówki. I niewiele było rzeczy, które powstrzymywałyby producentów kart przed wysyłaniem kart, o które klienci nigdy nie prosili, nie spodziewali się i nie mogli wiedzieć, że zostały skradzione, dopóki firma wydająca nie zaczęła żądać zapłaty za naliczone opłaty. Te przestępstwa i inne problemy wynikające z bezlitosnego wypychania kart przez banki doprowadziły bezpośrednio do uchwalenia ustawy o uczciwych rachunkach kredytowych z 1974 r., A także wielu innych przepisów mających chronić konsumenta. W połowie lat 90. oszustwa związane z kartami kredytowymi stały się szybko rosnącym problemem dla konsumentów i organów ścigania. W raporcie FBI z 1997 r. Stwierdzono: na całym świecie straty związane z oszustwami z wykorzystaniem kart bankowych w przypadku samych kart Visa i Master-Card wzrosły ze 110 milionów USD w 1980 roku do około 1,63 miliarda USD w 1995&hellip';Stany Zjednoczone poniosły większość tych strat - około 875 milionów dolarów w samym 1995 roku. Nie jest to zaskakujące, ponieważ 71 procent wszystkich na świecie odnawialnych kart kredytowych w obiegu zostało wydanych w tym kraju … Organy ścigania stale stawiają czoła nowym i złożonym systemom obejmującym oszustwa związane z kartami kredytowymi popełnione przeciwko instytucjom finansowym i firmom wydającym karty bankowe. Sprawcy prowadzą gamę od osób z łatwym dostępem do informacji o karcie kredytowej - takich jak urzędnicy agencji kredytowej, podmioty zajmujące się obsługą bagażu lotniczego i przewoźnicy pocztowi, zarówno publiczni, jak i prywatni, po zorganizowane grupy, zwykle o podobnym pochodzeniu etnicznym, zaangażowane w kradzież kart na dużą skalę , manipulowanie i podrabianie. Chociaż obecne operacje związane z oszustwami z użyciem kart bankowych są liczne i zróżnicowane, kilka programów stanowi większość w branży straty wynikające z zastosowania przestarzałej technologii, zaniedbań ze strony klientów oraz przepisów właściwych dla branży.

Powstaje kradzież tożsamości

Pod koniec lat 90. i w dekadzie po 2000 r. oszustwa związane z kartami kredytowymi zostały zaliczone do szerszej kategorii kradzieży tożsamości. Zamiast ograniczać swoje deprecjacje do płacenia rachunków za skradzione lub sfałszowane konta kart kredytowych, złodzieje, często w zorganizowanych kręgach, stworzyli fałszywe równoległe tożsamości, inicjując niespłacone kredyty bankowe, kupując samochody na kredyty innych ludzi i siejąc spustoszenie kredytami niewinnych ofiar oceny, sytuacje finansowe, a nawet ich codzienne życie. Ofiary skrajnych przypadków utraciły zdolność

do uzyskiwania kredytów hipotecznych, kupowania nowych domów i przyjmowania nowych miejsc pracy. Co gorsza, ciężar dowodu niewinności spadł na ofiary, w gorzkim odwróceniu założenia niewinności leżącego u podstaw brytyjskiego prawa zwyczajowego i jego pochodnych we Wspólnocie i Stanach Zjednoczonych. W sierpniu 2008 r. Departament Sprawiedliwości USA ogłosił25 największy i najbardziej złożony przypadek kradzieży tożsamości, jaki kiedykolwiek został oskarżony w tym kraju. Uczestniczyło w nim jedenaście osób z pięciu różnych krajów, w tym dwie ze Stanów Zjednoczonych i dwie z Chińskiej Republiki Ludowej, które ukradły ponad 40 000 000 kart kredytowych u jednego z głównych sprzedawców detalicznych w USA. Przejeżdżali lub spacerowali po budynkach, w których znajdowały się sieci bezprzewodowe, i instalowali sniffery, które rejestrowały hasła, numery kart i dane konta. O ile nie zostaną szybko zainstalowane odpowiednie środki zapobiegawcze, na pewno wystąpią kolejne takie przerażające wydarzenia. Raport Urzędu Statystycznego USA z 2011 r. „Kradzież tożsamości zgłoszona przez gospodarstwa domowe, 2005–2010" zawiera dodatkowe informacje. Streszczenie zawiera następujące najważniejsze elementy:

* W 2010 r. 7,0 procent gospodarstw domowych w Stanach Zjednoczonych lub około 8,6 miliona gospodarstw domowych miało co najmniej jednego członka w wieku 12 lat lub starszego, który doświadczył jednego lub więcej rodzajów wiktymizacji kradzieży tożsamości.

* Wśród gospodarstw domowych, w których co najmniej jeden członek doświadczył jednego lub więcej rodzajów kradzieży tożsamości, 64,1% doświadczyło niewłaściwego użycia lub próby niewłaściwego użycia istniejącego konta karty kredytowej w 2010 r.

* Od 2005 do 2010 r. Odsetek wszystkich gospodarstw domowych z co najmniej jednym rodzajem kradzieży tożsamości, które poniosły bezpośrednie straty finansowe, wzrósł z 18,5 procent do 23,7 procent. Raport Javelin Strategy & Research dotyczący oszustw związanych z tożsamością w 2012 r. Zawierał następujące spostrzeżenie w podsumowaniu: „Częstość występowania oszustw związanych z tożsamością wzrosła w 2012 r. Drugi rok z rzędu, dotykając 5,26% dorosłych w Stanach Zjednoczonych. Wzrost ten był spowodowany dramatycznymi skokami w dwóch najpoważniejszych typach oszustw: nowym oszustwie na koncie (NAF) i oszustwie związanym z przejęciem konta (ATF). "

TELEFONY

Nawet w pierwszych dniach telefonii nastoletni chłopcy bawili się nową technologią, która spowodowała spustoszenie. Pod koniec lat 70. XIX wieku nowy amerykański system AT&T musiał przestać wykorzystywać nastolatków jako operatorów centrali: chłopcy byli otwarcie nieuprzejmi wobec klientów. Rozmawiali z subskrybentami, wygłupiali się, wypowiadali żartobliwe uwagi i generalnie wypowiadali się. Dranie zabrali Dzień Świętego Patryka bez pozwolenia. A przede wszystkim grali w sprytne sztuczki z wtyczkami centrali: rozłączając połączenia, przełączając linie, aby klienci rozmawiali z nieznajomymi i tak dalej. To połączenie siły, mistrzostwa technicznego i skutecznej anonimowości wydawało się działać jak kocimiętka u nastoletnich chłopców

2600 Hz

Pod koniec lat 50. AT&T zaczął przełączać swoje sieci telefoniczne na bezpośrednie połączenia dalekosiężne, używając określonych tonów częstotliwości do komunikacji między przełącznikami. Około 1957 r. niewidome siedmioletnie dziecko Josef Engressia o doskonałym słucu i emocjonalnej fiksacji na temat telefonów nauczyło się gwizdać o częstotliwości 2600 Hz, która przerywała rozmowy telefoniczne na duże odległości i pozwalała mu wykonywać bezpłatne rozmowy na odległość w dowolnym miejscu na świecie. Ta zaburzona emocjonalnie osoba ostatecznie przemianowała się na „Joybubbles" i jest często opisywana jako twórca phishingu telefonicznego - manipulacji systemem telefonicznym w celu uzyskania nieautoryzowanego dostępu do usług. John Draper był w lotnictwie

USA w 1964 roku, kiedy zaczął pomagać kolegom w wykonywaniu bezpłatnych połączeń telefonicznych. Za sugestią Joybubbles użył gwizdków z pudełek płatków zbożowych Cap'n Crunch, aby wygenerować ton 2600 Hz, a następnie, nazywając siebie Kapitanem Crunch, zaczął tworzyć elektroniczne syntezatory tonów zwane niebieskimi skrzynkami. W latach 70. założyciele Apple, Steve Woźniak i Steve Jobs, budowali niebieskie skrzynki i za pomocą tych urządzeń robili takie psikusy, jak wzywanie Watykanu, udając Henry'ego Kissingera. Znaczącym czynnikiem przyczyniającym się do wzrostu phreakingu w latach 70. była publikacja w 1971 roku artykułu o phreaking w magazynie Esquire, który przyciągnął uwagę wielu młodych technofilów.

1982–1991: Kevin Poulsen

Gdy system telefoniczny przeszedł na większe poleganie na komputerach, granica między phreakingiem a hackowaniem zaczęła się zacierać. Jednym z ważnych nazwisk z okresu fascynacji telefonami z lat 80. był Kevin Poulsen. Kevin Poulsen po raz pierwszy zyskał rozgłos w 1982 roku, kiedy biuro prokuratora okręgowego hrabstwa Los Angeles napadło go za nieautoryzowany dostęp do tuzina komputerów w ARPANET, prekursorze nowoczesnego Internetu. Mając wówczas siedemnaście lat, nie został oskarżony, a następnie pracował jako programista i nadzorca bezpieczeństwa komputerowego w SRI International w Menlo Park w Kalifornii, a następnie jako administrator sieci w Sun Microsystems. W 1987 r. Agenci ochrony Pacific Bell odkryli, że Poulsen i jego przyjaciele penetrowali komputery i budynki firmy telefonicznej. Dowiedziawszy się, że Poulsen pracował również dla kontrahenta w dziedzinie obrony, gdzie posiadał poświadczenie bezpieczeństwa SECRET, FBI zaczęło budować sprawę szpiegostwa przeciwko hakerowi. W obliczu perspektywy pozbawienia go kaucji Poulsen stał się zbiegiem. Podczas ucieczki uzyskał informacje na temat metod nadzoru elektronicznego FBI i utrzymywał się, włamując się do komputerów Pacific Bell, aby oszukiwać w konkursach telefonicznych stacji radiowych, wygrywając wakacje na Hawajach i Porsche 944-S2 Cabriolet. . Po dwóch występach w nierozwiązanych tajemnicach NBC Poulsen został ostatecznie schwytany 10 kwietnia 1991 r. W sklepie spożywczym Van Nuys przez agenta ochrony Pacific Bell działającego na podstawie wskazówek informatora. 4 grudnia 1992 r. Poulsen stał się pierwszym hakerem, który został postawiony w stan oskarżenia na podstawie amerykańskich przepisów szpiegowskich, gdy Departament Sprawiedliwości oskarżył go o kradzież informacji niejawnych. (18 U.S.C. 793). Poulsen był przetrzymywany bez kaucji, podczas gdy energicznie walczył z zarzutem szpiegostwa. Oskarżenie zostało oddalone 18 marca 1996 r. Poulsen odbył pięć lat, dwa miesiące, z 71-miesięcznego wyroku za przestępstwa, które popełnił jako zbieg, oraz hakowanie telefonu, które rozpoczęło jego sprawę. Został zwolniony 4 czerwca 1996 r. I rozpoczął trzyletni okres nadzorowanego wydania, zakaz posiadania komputera przez pierwszy rok, a także zakazano korzystania z Internetu przez następne półtora roku. Od czasu wydania Poulsen pojawił się na MSNBC i na ABC Nightline, a także był przedmiotem wadliwej książki Jona Littmana „The Watchman - The Twisted Life and Crimes of Serial Hacker Kevin Poulsen". Po zwolnieniu z więzienia Kevin Poulsen zajął się dziennikarstwem. Został redaktorem dla SecurityFocus, a następnie został zatrudniony jako starszy redaktor w Wired News. Jest poważnym reporterem śledczym (np. złamał historię drapieżników seksualnych na MySpace) i często współtworzy bloga „Poziom zagrożenia"

KANTOWANIE DANYCH

Jedną z najczęstszych form przestępczości komputerowej od początku elektronicznego przetwarzania danych jest nielegalna lub nieuprawniona zmiana danych. Zmiany te mogą wystąpić przed i podczas wprowadzania danych lub przed wyjściem. Sprawy związane z przetwarzaniem danych obejmowały dane bankowe, listy płac, dane inwentaryzacyjne, dane kredytowe, transkrypcje szkolne, konfiguracje przełączników telefonicznych i praktycznie wszystkie inne zastosowania przetwarzania danych.

Oszustwo związane z Equity Funding (1964–1973).

Jednym z klasycznych oszustw związanych z wczesnymi oszustwami związanymi z danymi była sprawa Equity Funding, która rozpoczęła się od problemów z komputerem w Equity Funding Corporation of America, giełdowej i odnoszącej sukcesy firmie z dobrym pomysłem. Chodziło o to, aby inwestorzy kupowali od firmy polisy ubezpieczeniowe, a także inwestowali w fundusze inwestycyjne w tym samym czasie, a zyski byłyby przekazywane klientom i akcjonariuszom. Pod koniec lat sześćdziesiątych akcje Equity zawirowały w zawrotnej cenie, a artykuły prasowe opowiadały o tym dziwacznym świecie biznesu z Los Angeles. Problemy z komputerem wystąpiły tuż przed końcem roku budżetowego w 1964 r. Już niedługo miał zostać wydrukowany raport roczny, ale ostatecznych danych nie można było pobrać z komputera głównego. W rozpaczy szef przetwarzania danych powiedział prezeswoi złe wieści; raport musiałby zostać opóźniony. Bzdury, powiedział prezes ekspansywnie (w każdym razie w filmie); po prostu nadrobić dolną linię, aby pokazać około 10 milionów dolarów zysków i obliczyć inne liczby, aby wyszło w ten sposób. Z niepokojem szef DP zobowiązał się. Wydawało się, że racjonalizuje to, myśląc, że jest to tylko tymczasowe rozwiązanie, i może zostać naprawione później w prawdziwych księgach finansowych. Oczekiwany zysk nie zmaterializował się, a kilka miesięcy później do menedżerów w Equity dotarło, że mogą utrzymać wysoką cenę akcji, wytwarzając fałszywe polisy ubezpieczeniowe, które sprawią, że firma będzie wyglądać dobrze dla inwestorów. Dlatego zaczęli umieszczać fałszywe informacje o nieistniejących ubezpieczających w skomputeryzowanych rejestrach używanych do obliczania kondycji finansowej akcji. Z czasem pracownicy korporacji Equity stali się jeszcze bardziej zachłanni. Nie zadowalając się podniesieniem ceny swoich akcji, postanowili sprzedać polisy innym towarzystwom ubezpieczeniowym za pośrednictwem systemu redystrybucji zwanego reasekuracją. Firmy reasekuracyjne płacą pieniądze za kupowane polisy i rozkładają ryzyko, sprzedając część zobowiązania innym towarzystwom ubezpieczeniowym. Pod koniec pierwszego roku emitujące zakłady ubezpieczeń muszą zapłacić reasekuratorzy - część składek opłacanych przez ubezpieczających. Tak więc w pierwszym roku sprzedaż wymyślonych polis reasekuratorom przyniosła duże ilości prawdziwej gotówki. Jednak kiedy premie były należne, ekipa Equity „zabiła" wyobrażonych ubezpieczających z zawałami serca, wypadkami samochodowymi i, w jednym pamiętnym przypadku, rakiem macicy - u wyobrażonego ubezpieczającego płci męskiej. Pod koniec 1972 r. Szef DP obliczył, że do końca dekady w takim tempie Equity Funding ubezpieczałby całą populację świata. Jego aktywa przewyższą produkt narodowy brutto planety. Prezes jedynie nalegał, aby pokazano, jak dobrze firma sobie radzi. Program się rozpadł, gdy zły operator, który musiał pracować w godzinach nadliczbowych, powiedział władzom o machlojkach w Equity. Plotki rozeszły się po całej Wall Street i branży ubezpieczeniowej. W ciągu kilku dni Komisja Papierów Wartościowych i Giełd poinformowała Kalifornijski Departament Ubezpieczeń, że otrzymała informacje o ostatecznej formie kradzieży danych: taśmy zostały usunięte. Funkcjonariusze firmy zostali aresztowani, osądzeni i skazani na kary więzienia.

1994: Vladimir Levin i Citibank Heist.

W lutym 1998 r. Vladimir Levin został skazany na trzy lata więzienia przez sąd w Nowym Jorku. Levin był głównym konspiratorem w 1994 r., W ramach którego gang nielegalnie przekazał 12 mln USD aktywów z Citibank na kilka międzynarodowych kont bankowych. Przestępstwo zostało zauważone po tym, jak w lipcu 1994 r. skradziono pierwsze 400 000 USD, a Citibank współpracował z FBI i Interpolem w celu wyśledzenia przestępców. Levinowi nakazano spłacić 240 000 USD, czyli kwotę, którą udało mu się wypłacić przed aresztowaniem. Incydent doprowadził do zatrudniania przez Citibank Stephena R. Katza jako pierwszego głównego dyrektora ds. Bezpieczeństwa informacji (CISO).

OSZUSTWA SALAMI

W technice salami przestępcy kradną pieniądze lub zasoby naraz. Krążą dwie różne etymologie dotyczące pochodzenia tego terminu. Jedna ze szkół specjalistów ds. bezpieczeństwa twierdzi, że

odnosi się to do cienkiego dzielenia danych - jak salami. Inni twierdzą, że oznacza to budowanie znacznego przedmiotu lub kwoty z drobnych skrawków - jak salami. Udokumentowano przypadki oszustw salami w latach 70. i 80. XX wieku, ale jeden z bardziej uderzających incydentów wyszedł na jaw w styczniu 1993 r., kiedy czterech kierowników franczyzy Value Rent-a-Car na Florydzie zostało oskarżonych o oszustwo co najmniej 47 000 klientów korzystających z technika salami. Sąd federalny w Fort Lauderdale stwierdziło, że oskarżeni zmodyfikowali komputerowy program rozliczeniowy, aby dodać pięć dodatkowych galonów do rzeczywistej pojemności zbiorników paliwa w swoich pojazdach. W latach 1988-1991 każdy klient, który zwrócił samochód bez dopłaty, ostatecznie płacił zawyżone stawki za zawyżoną sumę benzyny. Kradzieże wahały się od 2 do 15 USD na jednego klienta, raczej grube plastry salami, ale mimo to są trudne do wykrycia przez ofiary. Niestety ataki salami mogą być trudne do wykrycia. Jedyną nadzieją jest to, że losowe audyty, zwłaszcza danych finansowych, wykryją rozbieżności i doprowadzą do odkrycia. Jak ostrzega każdy księgowy, nawet niewielki błąd należy wyśledzić, ponieważ może to wskazywać na znacznie większy problem. Na przykład słynne przygody Cliffa Stolla w poszukiwaniu tropów szpiegów w Internecie rozpoczęły się od niewyjaśnionej rozbieżności 0,75 USD między dwoma różnymi systemami rozliczania zasobów na komputerach UNIX w Obserwatorium Keck w Lawrence Berkeley Laboratories. Zdecydowanie Stoll, aby zrozumieć, w jaki sposób mógł wystąpić problem, ujawnił nieznanego użytkownika; dochodzenie doprowadziło do odkrycia, że rekordy rozliczania zasobów były modyfikowane w celu usunięcia dowodów użycia systemu. Resztę historii opisano w książce Clifforda Stolla „Jajko kukułki”

BOMBY LOGICZNE

Bomba logiczna to program, który celowo został napisany lub zmodyfikowany w celu uzyskania wyników, gdy spełnione są określone warunki, które są nieoczekiwane i nieautoryzowane przez legalnych użytkowników lub właścicieli oprogramowania. Bomby logiczne mogą znajdować się w samodzielnych programach lub mogą być częścią robaków (programów, które ukrywają ich istnienie i rozprzestrzeniają swoje kopie w systemach komputerowych i za pośrednictwem sieci) lub wirusów (programów lub segmentów kodu, które ukrywają się w innych programach i rozprzestrzeniają kopie sami). Bomby zegarowe są podklasą bomb logicznych, które „wybuchają” w określonym czasie. Według pracownika Rady Bezpieczeństwa Narodowego, rządu Stanów Zjednoczonych który autoryzował wprowadzenie bomby zegarowej do oprogramowania do sterowania gazociągiem transsyberyjskim, o którym wiedzieli, że zostanie skradziony ze źródeł amerykańskich przez rząd radziecki. „Rezultatem była najbardziej monumentalna eksplozja niejądrowa i ogień, jaką kiedykolwiek widziano z kosmosu”, powiedział Thomas C. Reed. Niesławny wirus jerozolimski (znany również jako wirus Piątek, trzynastego) z 1988 roku był bomba logiczną. Powielał się w każdy piątek i trzynastego miesiąca, powodując spowolnienie systemu; w każdy piątek 13 po 13 maja 1988 r. uszkodził także wszystkie dostępne dyski w zainfekowanych systemach. Inne przykłady znanych bomb czasowych to:

* Powszechny wirus komputerowy z lat 80., Cascade, sprawił, że wszystkie znaki spadły do ostatniego rzędu ekranu w ciągu ostatnich trzech miesięcy każdego roku.

* Wirus Michelangelo z 1992 roku został zaprojektowany w celu uszkodzenia katalogów dysków twardych 6 marca każdego roku.

* W 1992 r. Programista Michael Lauffenburger został ukarany grzywną w wysokości 5000 USD za pozostawienie bomby logicznej w firmie General Dynamics. Zamierzał wrócić po tym, jak program usunął krytyczne dane i otrzymać wynagrodzenie za naprawienie problemu.

Najbardziej znaną bombą zegarową ostatnich lat był problem Y2K (rok 2000). W skrócie, stare programy stosowały dwucyfrowe kody roku, które były oparte na założeniu, że miały zastosowanie do XX wieku. W miarę zbliżania się XXI wieku analitycy ostrzegali przed katastrofalnymi konsekwencjami,

jeśli programy nie zostaną skorygowane tak, by używały czterocyfrowych lat lub w inny sposób dostosowały się do zmiany wieku. W przypadku działania naprawcze zadziałały i nie doszło do katastrof. Późniejsza analiza wykazała dodatnią korelację między inwestycjami w rekultywację Y2K a późniejszą rentownością.

WYMUSZENIE

Dane komputerowe mogą być przechowywane w celu okupu. Na przykład według Whiteside w 1971 r. na międzynarodowym lotnisku w Los Angeles skradziono dwie rolki taśmy magnetycznej należące do oddziału Bank of America. Złodzieje żądali pieniędzy za ich zwrot. Właściciele zignorowali groźbę zniszczenia, ponieważ mieli odpowiednie kopie zapasowe. Inne wczesne przypadki wymuszenia z udziałem komputerów:

* W 1973 r. Zachodnioniemiecki operator komputerowy ukradł 22 taśmy i otrzymał okup wielkości 200 000 USD. Ofiara nie miała odpowiednich kopii zapasowych.

* W 1977 r. Programista w biurach Imperial Chemical Industries, Ltd. (ICI) w Rotterdamie ukradł wszystkie taśmy swojego pracodawcy, w tym kopie zapasowe. Na szczęście ICI poinformowało Interpol o próbie wymuszenia. W wyniku szczerości firmy złodziej i wspólnik zostali aresztowani w Londynie przez oficerów ze Scotland Yardu.

W latach 90. jednym z najbardziej znanych przypadków wymuszeń była kradzież 300 000 rekordów kart kredytowych klientów z witryny CD Universe przez 19-letniego Rosjanina „Maxus". Wysłał notkę z okupem z napisem: „Zapłać mi 100 000 $, a naprawię twoje błędy i na zawsze zapomnę o twoim sklepie… albo sprzedam twoje karty [dane kredytowe klienta] i opowiem o tym incydencie w wiadomościach". Właściciel CD Universe natychmiast wydał 25 000 numerów kart kredytowych za pośrednictwem strony internetowej, która stała się tak popularna wśród przestępców, że Maxus musiał ograniczyć dostęp do jednego skradzionego numeru na wizytę.

KONIE TROJAŃSKIE

Trojany to programy, które udają, że są użyteczne, ale zawierają również szkodliwy kod lub są po prostu szkodliwe.

1988 Fałszywy zastrzyk grypy . Jedną z najgorszych sztuczek rozgrywających się w świecie użytkowników wczesnego mikrokomputera był incydent FLU-SHOT-4 z marca 1988 r. z reklamą przypisywaną szkodom powodowanym przez niszczące, samoreplikujące się programy wirusowe dystrybuowane za pośrednictwem elektronicznych systemów tablic ogłoszeń (BBS) , wydawało się naturalne, że programiści publiczni podejmą wyzwanie i zapewnią ochronę. Flu-Shot-3 był przydatnym programem do wykrywania wirusów. Flu-Shot-4 pojawił się na BBS i wyglądał jak wersja 3; jednak faktycznie zniszczyło krytyczne obszary dysków twardych i dyskietki obecne podczas uruchamiania programu. Instrukcje, które spowodowały uszkodzenie, nie były obecne w pliku programu, dopóki nie został uruchomiony; ta technika modyfikowania kodu szczególnie utrudnia identyfikację trojanów poprzez proste sprawdzenie kodu na poziomie asemblera.

Scrambler, 12-Tricks i PC Cyborg . Inne wczesne i notoryczne Trojany na komputery PC z końca lat 80. XX wieku, które są nadal pamiętane w branży, to:

* Scrambler (znany również jako trojan KEYBGR), który udawał sterownik klawiatury (KEYBGR.COM), ale w rzeczywistości losowo uśmiechał się na ekranie.

* Trojan 12-Tricks, który podszywał się pod CORETEST.COM, program do testowania prędkości dysku twardego, ale w rzeczywistości spowodował 12 różnych rodzajów uszkodzeń (np. zZniekształcające działanie drukarki, spowolnienie wyświetlania ekranu i formatowanie dysku twardego) .

* Trojan Cyborg na PC (lub „Trojan AIDS"), który twierdził, że jest programem informacyjnym AIDS, ale faktycznie szyfrował wszystkie wpisy katalogu, zapełnił cały dysk C i symulował COMMAND.COM, ale wygenerował komunikat o błędzie w odpowiedzi na prawie wszystkie polecenia.

*1994: Ttrojan sprzętowy Datacomp

8 listopada 1994 r. Korespondent zgłosił się do RISKS Forum Digest, że padł ofiarą ciekawego rodzaju trojana: Niedawno kupiłem komputer Apple Macintosh w „supersklepie komputerowym" jako osobne komponenty - Apple CPU i Apple monitor i klawiaturę innej firmy rozliczane jako pochodzące od firmy o nazwie Sicon. W miniony weekend, próbując trochę edytować tekst, musiałem na chwilę zostawić komputer w spokoju. Po powrocie z przerażeniem odkryłem, że tekst „welcome datacomp" został wstawiony do edytowanego tekstu. Byłem pewien, że nie napisałem tego na maszynie, a moja żona potwierdziła, że też tego nie zrobiła. Szybka ankieta wykazała, że „schowek" (repozytorium informacji przetwarzanych za pomocą operacji wycinania / wklejania) nie był źródłem obrażającego tekstu. Jak zwykle początkową reakcją było podejrzenie wirusa. Dezynfekcja, wiodącą aplikacją antywirusową dla Macintosha, dała systemowi czysty rachunek zdrowotny; ponadto opisy znanych wirusów nie wspomniały o żadnych objawach podobnych do moich doświadczeń. Zrestartowałem system w całkowicie minimalnej konfiguracji, uruchomiłem edytor i czekałem. Rzeczywiście, po (dość długim) oczekiwaniu tekst „welcome datacomp" ponownie pojawił się sam. Dalsze dochodzenie ujawniło, że ktoś umieścił nieautoryzowany kod w układzie ROM wykorzystywanym w klawiaturze kilku marek. Jedynym rozwiązaniem była wymiana klawiatury. Czytelnicy zrozumieją możliwe konsekwencje użycia klawiatury, która wstawia nieautoryzowany tekst do, powiedzmy, kodu źródłowego. Winn Schwartau, uznany ekspert ds. Bezpieczeństwa komputerów, ukuł słowo „chipping", odnosząc się do takiej nieautoryzowanej modyfikacji oprogramowania układowego.

Trojany Keylogger

W połowie 2000 roku trojany programowe i sprzętowe zaprojektowane do przechwytywania dzienników naciśnięć klawiszy, a czasem do przesyłania tych dzienników przez ukryte połączenia internetowe, stały się dobrze znanym narzędziem szpiegostwa przemysłowego. Departament Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych wydał ostrzeżenie w grudniu 2005 r., Które zawierało ten przegląd:

Według branżowych ekspertów ds. bezpieczeństwa największą luką w zabezpieczeniach, na jaką narażeni są użytkownicy komputerów i sieci, jest poczta elektroniczna z ukrytymi programami niszczącymi oprogramowanie koni trojańskich, które udają łagodne aplikacje i osadzają łącza do rzekomo niewinnych stron internetowych, które pobierają złośliwy kod. Chociaż architektura zapory blokuje bezpośrednie ataki, poczta e-mail stanowi wrażliwą drogę do wewnętrznej sieci organizacji, za pośrednictwem której osoby atakujące mogą niszczyć lub kraść informacje. Atakujący próbują ominąć techniczne bloki instalacji szkodliwego kodu, wykorzystując użytkowników komputerów socjotechnicznych do nieświadomego podjęcia działań, które pozwalają na zainstalowanie kodu i narażenie danych organizacji. Techniki wykorzystywane przez atakujących do instalowania programów koni trojańskich za pośrednictwem poczty e-mail są szeroko dostępne i obejmują sfałszowanie identyfikacji nadawcy, użycie oszukańczych wierszy tematu i osadzanie złośliwego kodu w załącznikach e-mail. Rozwój przenośnych urządzeń pamięci masowej wielkości kciuka oraz pojawienie się wyrafinowanego oprogramowania i urządzeń do rejestrowania naciśnięć klawiszy ułatwia atakującym odkrywanie i kradzież ogromnych ilości informacji w ukryciu

Trojan Haephrati

Sprawa, która wywołała tę wiadomość w połowie 2000 roku, rozpoczęła się, gdy izraelski pisarz Amon Jackont był zdenerwowany, gdy znalazł w Internecie fragmenty rękopisu, nad którym pracował. Potem ktoś próbował ukraść pieniądze z jego konta bankowego. Podejrzenie padło na byłego męża pasierbicy, Michaela Haephrati. Policja odkryła rejestrator klawiszy na komputerze Jackonta. Okazało się, że Haephrati sprzedawał także oprogramowanie szpiegowskie klientom; trojan został ukryty w czymś, co wyglądało na poufny e-mail. Po zainstalowaniu na komputerach ofiar oprogramowanie przesyła dane z nadzoru na serwer w Londynie w Anglii. Haephrati został zatrzymany przez brytyjską policję i rozpoczęto dochodzenia w Niemczech i Izraelu. Dwanaście osób zostało szczegółowo opisanych w Izraelu; ośmiu innych było aresztowanych w domu. Podejrzani to prywatni detektywi i kierownictwo z firm przemysłowych, a wśród nich Hewlett-Packard, sklepy ze sprzętem Ace i firma zajmująca się łącznością kablową. Michael i Ruth Haephrati zostali poddani ekstradycji z Wielkiej Brytanii na proces w Izraelu w dniu 31 stycznia 2006 r. Zostali oni oskarżeni o zainstalowanie programu koni trojańskich, który aktywował rejestrator kluczy z możliwością zdalnego raportowania. W marcu 2006 r. Para została oskarżona w Tel Awiwie za szpiegostwo korporacyjne. Przyznali się do winy pod zarzutem i zostali skazani odpowiednio na cztery i dwa lata więzienia, a także ukarani grzywnami. Historia się jednak nie skończyła. Dwa lata później „Czterech członków izraelskiej prywatnej firmy śledczej Modi'in Ezrahi zostało skazanych w poniedziałek po tym, jak zostali uznani za winnych wykorzystywania złośliwego oprogramowania trojana do kradzieży poufnych informacji od konkurentów swoich klientów.” Raport kontynuuje: Asaf Złotowski, kierownik w firmie detektywistycznej Modi'in Ezrahi został skazany na 19 miesięcy więzienia. Dwaj inni pracownicy, Haim Zissman i Ron Barhoum, zostali skazani na karę więzienia odpowiednio na 18 i 9 miesięcy. Były dyrektor naczelny firmy, Yitzhak Rett, ofiara widocznego wypadku, kiedy spadł ze schodów podczas przerwy w przesłuchaniu przez policję w 2005 r., Uniknął kary więzienia na podstawie umowy przetargowej. Rett został ukarany grzywną w wysokości 250 000 szekli izraelskich (36 500 funtów) i polecono mu odbyć dziesięciomiesięczny okres próbny w związku z jego udziałem w oszustwie. Jednak w artykule z kwietnia 2008 r. Podano, że Michael Haephrati „twierdził, że nie było więzienia i że był całkowicie wolny. W rzeczywistości zamierzał nadal oferować usługę konia trojańskiego, ale tym razem będzie współpracował tylko z „organami ścigania”.

Trojany sprzętowe i wojna informacyjna

Pod koniec XXI wieku w wielu wiadomościach omówiono niebezpieczeństwa związane z rosnącą zależnością od chińskich komponentów komputerowych. Źródła Departamentu Obrony USA twierdzą prywatnie, że poziom chińskich cyberataków zobowiązuje ich do unikania chińskiego sprzętu i oprogramowania we wszystkich klasyfikowanych systemach i tak wielu niesklasyfikowanych systemach, jak to tylko możliwe pod względem fiskalnym. Wysokie zagrożenie chińskimi cyberprzestępstwami w amerykańskich sieciach obronnych zostanie zwiększone, gdy Pentagon coraz bardziej traci krajowe źródła „zaufanych i sklasyfikowanych” mikroczipów. Odkrycie podrobionych routerów Cisco pogorszyło obawy o niezawodność chińskiego sprzętu sieciowego. FBI, Immigration and Customs Enforcement (ICE) , Customs and Border Protection (CBP) oraz Royal Canadian Mounted Police (RCMP) współpracowały ze sobą w celu śledzenia masowej liczby podrobionych urządzeń sieciowych, w tym routerów Cisco; w wyniku tych dochodzeń i konfiskat pojawiły się pytania dotyczące niezawodności i wiarygodności takiego sprzętu, z którego większość została wyprodukowana w Chińskiej Republice Ludowej. Chociaż naukowcy z Cisco zbadali niektóre podrobione urządzenia i nie znaleźli tylnych drzwi, obawy były na tyle poważne, że agencje rządowe stworzyły chipy testowe, aby zakwestionować procesy zapewnienia jakości u kontrahentów wojskowych:

W kwietniu [2008 r.] Agencja Zaawansowanych Projektów Badawczych Obrony, będąca częścią Departamentu Obrony, rozpoczęła dystrybucję chipów z ukrytymi obwodami koni trojańskich

kontrahentom wojskowym uczestniczącym w programie agencyjnym Trusted Integrated Circuits. Celem jest przetestowanie technik kryminalistycznych w celu znalezienia ukrytych elektronicznych drzwi pułapkowych, które mogą być irytujące. Jan Walker, rzeczniczka agencji, nie jest jeszcze gotowa do ogłoszenia wyników testu.

Raport z 2011 r. Na temat przesłuchań przed amerykańską komisją ds. Nadzoru i reformy rządu na temat backdoorów trojańskich w importowanym oprogramowaniu i sprzęcie zawierał to stwierdzenie wraz z odniesieniami do każdego tematu:

… [E] wbudowane złośliwe oprogramowanie czające się w technologiach konsumenckich nie jest nowym zjawiskiem. Ponieważ dzieje się to od lat i nie jest tajemnicą bezpieczeństwa narodowego, nie jest jasne, dlaczego Schaffer wahał się tak długo, zanim odpowiedział. Było wiele incydentów, w których produkty zainfekowane złośliwym oprogramowaniem wysyłane były do konsumentów, od sprzętu, po oprogramowanie, a nawet skażone urządzenia peryferyjne. Złośliwe oprogramowanie zostało wstępnie załadowane w produktach takich jak USB, mikroczipy, aparaty fotograficzne, ładowarki akumulatorów, cyfrowe ramki do zdjęć, kamery internetowe, drukarki, telefony komórkowe, płyty główne lub płyty systemowe i dyski twarde.

ZNANE ROBAKI I WIRUSY

Kolejne sekcje krótko opisują niektóre z incydentów, o których często wspominają dyskusje na temat historii złośliwego oprogramowania

* 1970–1990: Wczesne epidemie złośliwego oprogramowania.

ARPANET był prekursorem Internetu. Według kilku raportów:

Na początku lat 70. wykryto wirusa Creeper w ARPANET, amerykańskiej wojskowej sieci komputerowej, która była prekursorem współczesnego Internetu. Program ten, napisany dla popularnego wówczas systemu operacyjnego Tenex, był w stanie uzyskać dostęp niezależnie przez modem i skopiować się do zdalnego systemu. Zainfekowane systemy wyświetliły komunikat: „Jestem twórcą: Złap mnie, jeśli potrafisz”. Wkrótce potem program Reaper został anonimowo stworzony, aby usunąć Creeper. Reaper był wirusem: rozprzestrzenił się na maszyny w sieci, a gdyby znalazł wirusa Creeper, Reaper usunąłby go. Nawet uczestnicy nie są w stanie stwierdzić, czy Reaper był odpowiedzią na Creeper, czy też został stworzony przez tę samą osobę lub osoby, które stworzyły Creeper w celu skorygowania swojego błędu. ”

W 1981 roku komputer Apple II był popularnym systemem wśród hobbystów; wirus Elk Cloner rozprzestrzenia się za pośrednictwem zainfekowanych dyskietek i jest uważany za „pierwszy na świecie wybuch wirusa komputerowego na dużą skalę.

W 1986 r. Wirus sektora rozruchowego Brain był pierwszym złośliwym oprogramowaniem dla komputerów IBM, które rozprzestrzeniło się na całym świecie. Został stworzony przez dwóch braci z Lahore w Pakistanie i zawierał ten tekst:

Witamy w Dungeon (c) 1986 Brain & Amjads (pvt) Ltd VIRUS SHOE RECORD V9.0 Dedykowane dynamicznym wspomnieniom milionów wirusów, które nie są już z nami dzisiaj - Dzięki GOODNESS !! Uwaga na… WIRUS: ten program łapie program

następuje po tych wiadomościach…. $ # @% @ !!

Wirus Lehigh pojawił się na Uniwersytecie Lehigh w Pensylwanii w 1987 r. i uszkodził akta kilku profesorów i studentów. Ten wczesny infektor programu celował tylko w command.com i dlatego jego

zasięg był bardzo ograniczony. W 1988 r. Wirus Jeruzalem, infektor plików, który rozmnażał się po wstawieniu kodu do plików EXE i COM, spowodował globalną epidemię komputerów. Kolejna godna uwagi infekcja w 1988 r. Pochodzi od samoszyfrującego wirusa Cascade z 1988 r., Który dezorientował wielu naiwnych użytkowników, którzy interpretowali spadające symbole na ekranie jako część nieoczekiwanego wygaszacza ekranu. Wirus ten był jednym z najwcześniejszych przykładów prób przeciwdziałania produktom antywirusowym opartym na sygnaturach.

2 grudnia 1987 r :

Robak choinkowy. W grudniu 1987 r. Użytkownicy komputerów mainframe IBM podłączonych do Europejskiej Sieci Badań Naukowych (EARN), BITNET i firmy VNET firmy IBM zostali zalewani wiadomościami e-mail zawierającymi choinkowe przedstawienie postaci. Student z Technische Universitat Clausthal w Niemczech uruchomił „robaka napisanego w języku REXX specyficznym dla IBM". Robak wykorzystał listę korespondentów ofiary, aby wysłać swoje kopie wszystkim na liście.

2 listopada 1988:

Morris Worm . 2 listopada 1988 r. Internet wstrząsnął gwałtownym pojawieniem się nieautoryzowanego kodu w systemach na całym świecie. O 17:00 EST 2 listopada 1988 r. Robert T. Morris, student Cornell University w Ithaca w stanie Nowy Jork, wypuścił robaka do Internetu. Do północy zaatakował komputery VAX z 4 komputerami BSD UNIX i SUN Microsystems Sun 3 w całych Stanach Zjednoczonych. Jednym z najciekawszych aspektów postępu robaka w Internecie była prawie całkowita niezależność jego drogi od normalnych ograniczeń geograficznych. Czasami skakał z wybrzeża na wybrzeże szybciej, niż dotarł do fizycznie sąsiadujących systemów komputerowych. Robak graficznie pokazał, że cyberprzestrzeń ma swoją własną geografię. Robak często infekuje hosty, co prowadzi do spowolnienia ogólnej prędkości przetwarzania. Pierwsze internetowe ostrzeżenie („Jesteśmy atakowani") zostało opublikowane o 02:38 3 listopada na liście TCP-IP przez naukowca z University of California w Berkeley. O 03:34 Andy Sudduth, przyjaciel Morrisa z Harvardu, anonimowo opublikował ostrzeżenie („W Internecie może być wirus)" i zamieścił kilka komentarzy na temat tego, jak zatrzymać robaka. Niestety, pisze Spafford, robak tak poważnie zahamował Internet, że ta wiadomość nie była szeroko rozpowszechniana przez ponad 24 godziny. Do 6:00 rano 3 listopada wiadomości krążyły w Internecie ze szczegółami dotyczącymi działania robaka. Wiadomości rozprzestrzeniają się za pośrednictwem grup dyskusyjnych, takich jak lista TCP-IP, poprawki Usenix 4bsd-ucb i grupa usenet news.announce.important. Spafford oraz jego przyjaciele i koledzy w Internecie gorliwie współpracowali przy tworzeniu łatek przeciwko robakowi. W międzyczasie wraz z rozpowszechnianiem się wiadomości o ataku niektórzy administratorzy systemów zaczęli odcinać swoje sieci od Internetu. Agencja Komunikacji Obronnej oddzieliła od siebie swoje sieci Milnet i Arpanet około 11:30 3 listopada. W południe maszyny w centrum naukowo-technologicznym Instytutu Badawczego Stanford zostały zamknięte. Pod koniec 4 listopada opublikowano obszerny zestaw poprawek do ochrony systemów przed robakiem. Tego wieczoru reporter New York Times powiedział Spaffordowi, że znaleziono autora robaka. Do 8 listopada Internet wydawał się znów normalny. Grupa zaniepokojonych informatyków spotkała się w National Computer Security Center, aby zbadać incydent i zastanowić się, jak zapobiec ponownemu wystąpieniu takich ataków. Spafford umieścił incydent w perspektywie, komentując, że dotknięte systemy to nie więcej niż 5 procent hostów w Internecie. Głupotą byłoby odrzucenie elektronicznego wandalizmu Morrisa jako dowcipu lub twierdzenie, że robak ostrzegł menedżerów o słabym bezpieczeństwie ich systemów. Niemniej prawdą jest, że incydent przyczynił się do powołania zespołu reagowania na awarie komputerowe w Instytucie Inżynierii Oprogramowania Uniwersytetu Carnegie-Mellon. Za te błogosławieństwa nie jesteśmy jednak wdzięczni Robertowi T. Morrisowi. W 1990 r. Morris został uznany za winnego na podstawie ustawy o oszustwach i nadużyciach komputerowych z 1986 r. Maksymalne kary obejmowały pięć lat

więzienia, grzywnę w wysokości 250 000 USD i koszty restytucji. Morrisowi powierzono 400 godzin służby społecznej, skazano go na trzyletni okres próbny i zapłacono grzywną w wysokości 10 000 USD. Został wydalony z Cornell University. Jego prawnicy odwołali się od wyroku do Sądu Najwyższego Stanów Zjednoczonych. Ich argumenty obejmowały brak złych zamiarów (nie chciał wyrządzić krzywdy, szczerze - mimo że jego robak podjął nadzwyczajne środki ostrożności, aby się ukryć) i wyrazili ubolewanie z powodu skandalicznego zachowania władz Uniwersytetu Cornell, które miały ochotę przeszukać własną pocztę elektroniczną system wiadomości w celu zlokalizowania dowodów obciążających Morrisa. Prawnicy argumentowali również, że wysłanie wiadomości e-mail może stać się przestępstwem, jeśli Morris utrzyma wyrok skazujący. Sąd Najwyższy podtrzymał decyzję odmawiając rozpatrzenia apelacji. Robert T. Morris ostatecznie został profesorem nadzwyczajnym na Wydziale Inżynierii Elektrycznej i Informatyki Massachusetts Institute of Technology oraz członkiem Laboratorium Informatyki i Sztucznej Inteligencji.

Złośliwe oprogramowanie w latach 90.

Najbardziej znaczącym rozwojem złośliwego oprogramowania w latach 90. było wydanie w lipcu 1995 r. Pierwszego na świecie szeroko rozpowszechnionego wirusa makr języku. Wirus macro.concept pojawił się w dokumentach MS-Word dla Windows. Pokazano, jak korzystać z języka programowania makr, wspólnego dla wielu produktów Microsoft, do generowania makr odtwarzających się w różnych dokumentach. W ciągu kilku miesięcy pojawiły się wyraźnie destrukcyjne wersje tego wirusa demonstracyjnego. Makrowirusy były niebezpiecznym nowym zjawiskiem. Jak wyjaśniono w najnowszej historii wirusów i antywirusów:

* Umieszczanie samoreprodukującego się kodu w łatwo i często wymienianych plikach, takich jak dokumenty, znacznie zwiększyło zakaźność wirusów.

* Twórcy wirusów przenieśli swoją uwagę na znacznie łatwiejszy język programowania niż asembler.

* Wymiana zainfekowanych dokumentów pocztą elektroniczną była znacznie bardziej skutecznym mechanizmem infekcji wirusowej niż wymiana zainfekowanych programów lub dysków.

* „[M]akro wirusy nie były specyficzne dla platformy ani specyficzne dla systemu operacyjnego. Były oparte na aplikacjach. ”

W drugiej połowie lat 90. makrowirusy zastąpiły wirusy sektora rozruchowego i wirusy infekujące pliki jako główny rodzaj złośliwego złośliwego oprogramowania do samoreprodukcji; w tym okresie wzrosły również dodatkowe typy robaków sieciowych opartych na skryptach. Roger Thompson podsumowuje rozwój złośliwego oprogramowania w latach 90. XX wieku w następujący sposób:

Około 2000 roku wirusy makr przestały być problemem, ponieważ nowa wersja MS-Office 2000 zawierała funkcje blokujące wirusy makr. Kolejnym krokiem w ewolucji złośliwego oprogramowania były masowe programy pocztowe, takie jak robak ILOVEYOU, a następnie robaki sieciowe. Można je było łatwo napisać i zaciemnić, zmieniając zawartość tekstu, a tym samym pokonując skanery podpisów. Robaki te rozprzestrzeniały się bardzo szybko do momentu wydania dodatku Service Pack 2 dla systemu Windows XP, który wymusił domyślną obsługę Zapory systemu Windows. Po tym zdarzeniu na poziomie wyginięcia przestępcy przeszli do tworzenia masowych mailerów i botów, które mogłyby rozprzestrzeniać złośliwe oprogramowanie i spam lub powodować rozproszoną odmowę usługi poprzez komunikację za pośrednictwem zaufanych witryn internetowych, do których dostęp uzyskuje się za pomocą przeglądarek tworzących tunel przez zaporę ogniową.

5 marca 1999 r : Melissa . W piątek 26 marca 1999 r. CERT / CC otrzymał wstępne raporty o szybko rozprzestrzeniającym się nowym wirusie makr MS-Word. „Melissa” została napisana w celu

zainfekowania takich dokumentów; po załadowaniu korzysta ze standardowej książki adresowej e-mail ofiary, aby wysłać swoje kopie do pierwszych 50 osób na liście. Wirus dołącza zainfekowany dokument do wiadomości e-mail o temacie „Temat: Ważna wiadomość od < nazwa >", gdzie < nazwa > to nazwisko przypadkowego nadawcy. Wiadomość e-mail brzmi: „Oto dokument, o który prosiłeś… nie pokazuj nikomu ;-)" i zawiera plik MS-Word jako zainfekowany załącznik. Oryginalny zainfekowany dokument „list.doc" był kompilacją adresów URL stron pornograficznych. Jednak w miarę rozprzestrzeniania się wirusa mógł on wysyłać wszelkie inne zainfekowane dokumenty utworzone przez ofiarę. Z powodu tego wysokiego wskaźnika replikacji wirus rozprzestrzenia się szybciej niż jakikolwiek poprzedni wirus w historii. W wielu systemach korporacyjnych szybki współczynnik nasyconych wewnętrznych replikacji serwerów e-mail z wychodzącymi automatycznymi wiadomościami-śmieciami. Początkowe szacunki były w zakresie 100 000 systemów zestrzelonych. Firmy antywirusowe zebrali się natychmiast, a aktualizacje wszystkich standardowych produktów były dostępne w ciągu kilku godzin od pierwszych powiadomień z CERT / CC. Poszukiwania twórcy wirusów / robaków pocztowych Melissa rozpoczęły się natychmiast po wybuchu epidemii. Wstępne ustalenia prześledziły wirusa w Access Orlando, dostawcy usług internetowych na Florydzie (ISP), którego serwery zostały zamknięte na mocy nakazu FBI do badania sądowego; systemy zostały następnie skonfiskowane. To zdarzenie zostało następnie przypisane do Source of Kaos, witryny o swobodnym mowie, w której wirus może leżeć w stanie uśpienia od miesięcy na zamkniętych, ale nie usuniętych stronach dystrybutora wirusów. Śledczy odkryli numer seryjny w dokumencie wektorowym napisanym za pomocą MSWord; nieudokumentowany numer seryjny pomógł organom ścigania, gdy śledczy rozpowszechnili go w sieci, aby wyśledzić sprawcę. Kolejne kroki dotyczyły sieci AOL o wartości dodanej, w której wirus został udostępniony publicznie. Informacje giganta ISP pomogły zidentyfikować potencjalnego podejrzanego i do 2 kwietnia FBI aresztowało Davida L. Smitha (30 lat) w Aberdeen, New Jersey. Smith najwyraźniej spanikował, gdy usłyszał, że FBI jest na tropie Melissy, i wyrzucił swój komputer - głupio, do śmieci we własnym budynku mieszkalnym. Smith został oskarżony o przestępstwa drugiego stopnia polegające na przerwaniu komunikacji publicznej, spisku mającym na celu popełnienie przestępstwa i próbie popełnienia przestępstwa, kradzieży usług komputerowych trzeciego stopnia oraz uszkodzeniu trzeciego stopnia lub niewłaściwym dostępie do systemów komputerowych. Jeśli zostanie skazany, Smith zostanie ukarany maksymalną grzywną w wysokości 480 000 USD i 40 lat więzienia. 10 grudnia 1999 r. Smith przyznał się do winy do wszystkich zarzutów federalnych i zgodził się na każdy akt oskarżenia, w tym szacunki Międzynarodowego Stowarzyszenia Bezpieczeństwa Komputerowego o co najmniej 80 mln USD szkód następczych z powodu infekcji Melissą

Maj 2000 r : I LOVE YOU . Począwszy od około 4 maja 2000 r. użytkownicy poczty e-mail otwierali wiadomości od znajomych korespondentów o temacie „Kocham cię"; wielu z nich otworzyło załącznik LOVE-LETTER-FOR-YOU.txt.vbs, który zainfekował książkę adresową użytkownika i zainicjował masową wysyłkę do wszystkich kontaktów. „Love Bug" był najszybciej rozprzestrzeniającym się robakiem, infekującym komputery na całym świecie , poczynając od Azji, a potem Europy. 11 maja filipiński student informatyki Onel de Guzman z AMA Computer College w Manili przyznał władzom, że „mógł przypadkowo uruchomić niszczycielski wirus Love Bug wywołany młodzieńczym entuzjazmem. "Nie przyznał, że sam stworzył szkodliwe oprogramowanie; jednak nazwa GRAMMERSoft pojawiła się w kodzie komputerowym wirusa, i to była nazwa grupy komputerów, do której należał 23-letni de Guzman. We wrześniu 2000 r. De Guzman uczestniczył w czacie na żywo prowadzonym przez CNN.com; energicznie bronił się przed pisaniem wirusów i obwiniał twórców wrażliwych systemów o wydanie źle zaprojektowanego oprogramowania. Odmówił przyjęcia odpowiedzialności za napisanie robaka. Władze filipińskie próbowały oskarżyć de Guzmana, ale w sierpniu 2000 r. Musiały porzucić swoje próby z powodu braku wystarczających dowodów. Ze względu na brak przepisów dotyczących

przestępczości komputerowej w tym czasie inne kraje, takie jak Stany Zjednoczone, nie mogły ekstradycji podejrzanego: Międzynarodowe zasady podwójnej karalności wymagają równoważnych przepisów w obu jurysdykcjach, zanim będzie można kontynuować ekstradycję. Do października 2000 r. De Guzman odmówił przyjęcia odpowiedzialności za napisanie robaka i publicznie stwierdził: „Przyznaję, że tworzę wirusy, ale nie wiem, czy to mój. Gdybym otrzymał kod źródłowy, mógłbym na niego spojrzeć i zobaczyć. Może to sprawa kogoś innego, a może została mi skradziona ". Sprawa „I Love You" była sygnałem alarmowym dla społeczności międzynarodowej, aby pomyśleć o standaryzacji przepisów dotyczących przestępczości komputerowej na całym świecie.

Lipiec 2010 r. Stuxnet . W lipcu 2010 r. Pojawiły się raporty o zero-dniowym zagrożeniu dla systemów SCADA za pomocą oprogramowania SimaticWinCC i PCS 7 firmy Siemens AG. Analitycy stwierdzili, że robak Stuxnet został zaprojektowany do szpiegostwa przemysłowego; jednak te same techniki mogły zostać użyte do sabotażu. Eksperci wyrazili zaniepokojenie, że robak został podpisany przy użyciu ważnych certyfikatów cyfrowych od tajwańskich firm i że złożony kod sugeruje znaczną znajomość oprogramowania SCADA71. Dalsza analiza kodu złośliwego oprogramowania sugeruje, że oprogramowanie zostało opracowane przez Stany Zjednoczone i Izrael i wykorzystywane w przynajmniej w listopadzie 2007 roku.

SPAM

W tej części omówiono wyłącznie nadużywanie USENET w 1994 r. I trendy w spamie w ciągu następnej dekady.

1994: Spam na loterii zielonej karty . 2 kwietnia 1994 r. Laurence A. Canter i Marthas S. Siegel zamieścili ogłoszenie dotyczące usług prawnych związanych z loterią Zielonej Karty Rządu USA dla ponad 6000 grup USENET. Zamiast krzyżować swoje wiadomości komercyjne, użyli skryptu, aby opublikować kopię wiadomości osobno dla każdej grupy. Poprzednia metoda pokazałaby wiadomość użytkownikom USENET raz; Nadużywanie USENET przez Cantera i Siegela sprawiło, że ich reklama wyświetlała się w każdej grupie, której dotyczy subskrypcja. Reakcja na całym świecie była ogromna. Zautomatyzowane anulujące roboty trollowały USENET usuwając niechciane wiadomości; dostawca usług internetowych dla adwokatów był tak przepełniony skargami e-mailowymi, że jego serwery uległy awarii. Canter i Siegel byli oczerniani w postach i artykułach prasowych. Ich niesmaczne pochodzenie opublikowano w grupach dyskusyjnych, w tym szczegóły dotyczące przesłuchań dyscyplinarnych przed barem na Florydzie oraz oskarżenia o nieuczciwość i nieprofesjonalne zachowanie. Nie zdziwiona para opublikowała książkę o tym, jak nadużywać Internetu za pomocą spamu i broniła swoich działań w wywiadach jako wyraz wolności słowa; odrzucili krytyków jako „fanatyków o dzikich oczach" lub jako interesy handlowe mające na celu kontrolowanie Internetu dla własnego zysku. Canter został ostatecznie zablokowany w Tennessee, częściowo za jego spamowanie. Pozostał skruszony; W 2002 r. wysłał spam do 50 000 nauczycieli K-12 z reklamą książki, której tytuł mu się podobał, aby mógł zbierać opłaty za skierowania z Amazon

Spam staje się globalny

W ciągu następnej dekady liczba spamu gwałtownie wzrosła. Do 2007 r. Obserwatorzy spamu i firmy antyspamowe poinformowały o tym ,że 88 procent całego ruchu pocztowego w Internecie stanowił spam. Spamerzy wywołali tyle irytacji, że firmy opracowały oprogramowanie i rozwiązania sprzętowe do filtrowania wiadomości e-mail według treści. Spamerzy zareagowali zwiększeniem liczby obrazów w spamie, co utrudnia filtrowanie treści. W pewnym momencie ilość spamu wzrosła o 17 procent między jednym dniem a drugim, gdy spamerzy zaczęli pompować pliki PDF do potoków spamowych. Botnety odradzające się przez zainfekowane maszyny zombie utworzyły nieuczciwe węzły SMTP przy użyciu niewinnych (i nieświadomych) komputerów użytkowników PC oraz trwałych szybkich połączeń

internetowych. Spam stanowi obecnie główny wektor oszustwa polegającego na oszustwie, w tym w szczególności zaliczki 4-1-9 oszustwa i ataki phishingowe. Oszustwo związane z zaliczkami zwykle polega na zachęcaniu do udziału w kradzieży nieuczciwie zdobytych korzyści, takich jak depozyty bankowe należące do osób zmarłych lub skradzione z biednych krajów; ofiarom, które zgodzą się uczestniczyć w takiej nielegalności, obiecuje się miliony dolarów - tylko po to, by powiedzieć, że nagle muszą wysłać gotówkę za nieoczekiwane łapówki lub opłaty. Jeśli to zrobią, zostaną poproszeni o więcej … i więcej &hellip i więcej. Phishing polega na wysyłaniu wiadomości e-mail, które powinny wyglądać jak oficjalne, zwykle alarmujące, ostrzeżenia z banków i innych instytucji; ofiary klikają linki, które wyglądają jak jedno, ale faktycznie przechodzą na strony internetowe przestępców. Tam ofiary chętnie wpisują swoje dane identyfikacyjne użytkownika, hasła, numery kont bankowych i wszelkie inne poufne informacje przydatne w przypadku kradzieży tożsamości.

DENIAL OF SERVICE

Odmowa usługi wynika z wyczerpania lub zniszczenia niezbędnych zasobów. Jednak kilku atakujących typu „odmowa usługi" wyróżnia się spośród wszystkich pozostałych w ciągu ostatnich dwudziestu lat: Unamailer i Mafiaboy.

1996: Unamailer

W sierpniu 1996 r. Ktoś posługujący się pseudonimem „johnny [x] chaotic" oskarżył się o masowy atak bombowy polegający na nieuczciwym przypisywaniu dziesiątek ofiar setkom list mailingowych. Odmowa usługi była wynikiem części naiwności menedżerów list, którzy zaakceptowali subskrypcje na dowolny adres e-mail z dowolnego innego adresu e-mail. W chaotycznym i niespójnym liście opublikowanym w sieci (-ach) napisał niegrzeczne uwagi na temat sławnych i mało znanych osób, których zdolność otrzymywania znaczących wiadomości e-mail została następnie zatarta przez tysiące niechcianych wiadomości dziennie. „Pierwszy atak, przeprowadzony w sierpniu, skierowany był do ponad 40 osób, w tym Billa Clintona i Newta Gingricha, i przyniósł strumień skarg od osób, które znalazły swoje nazwiska jako subskrybentów, około 3000 osób z listy e-mail. "Ktoś, kto twierdzi, że jest tym samym„ Unamailer "(jak podają go media w związku z Unabomber), pod koniec grudnia rozpoczął podobny masowy abonament bombowy. Szacuje się, że atak ten obejmuje 10 139 grup przeglądających listy, 3 razy większą niż ta, która miała miejsce latem, również za namową xchaotic. Gdyby każda lista mailingowa w tym ataku wysłała do wybranych subskrybentów zaledwie 10 listów na komputery subskrybentów, osoby te otrzymałyby ponad 100 000 wiadomości. Gdyby każdy system aukcji wysłał 100 wiadomości - i wiele z nich - to łączna liczba wiadomości mogłaby sumować 1 000 000. W grudniu osoby atakujące wyśmiewały administratorów list za nieużywanie uwierzytelniania przed zezwoleniem na subskrypcje i napisały, że będą kontynuować ataki do czasu zmiany praktyk. Częściowo w wyniku kradzieży Unamailera administratorzy list w rzeczywistości zmienili swoje praktyki - nie dlatego, że ktoś dziękował Johnny'emu chaotycznie za jego metodę perswazji.

2000: MafiaBoy

8 lutego 2000 r. Serwis Yahoo.com doznał trzygodzinnej powodzi w wyniku rozproszonego ataku typu „odmowa usługi" (DDoS) i utracił zdolność do udostępniania stron internetowych odwiedzającym. Następnego dnia ta sama technika została rozszerzona na Amazon.com, eBay.com, Buy.com i CNN.com. Późniejsze informacje wykazały również, że Charles Schwab, internetowy makler giełdowy, został poważnie utrudniony w obsłudze swoich klientów z powodu DDoS. Menedżerowie Buy.com byli szczególnie zaniepokojeni ponieważ atak miał miejsce w dniu ich pierwszej oferty publicznej. W wyniku ataków wiele firm utworzyło konsorcjum do walki z atakami DDoS. Śledztwo przeprowadzone przez RCMP i FBI zlokalizowało 15-letnie dziecko w zachodnim Montrealu, które wykorzystało modem do kontrolowania zombie w swojej eskapadzie DDoS: 15 kwietnia 2000 r. RCMP aresztował kanadyjskiego

nieletniego znanego jako Mafiaboy na 8 lutego DDoS atak na CNN w Atlancie w stanie Georgia. W dniu 3 sierpnia 2000 r. Mafiaboy został obciążony 64 dodatkowymi obliczeniami. 18 stycznia 2001 r. Mafiaboy pojawił się przed Sądem ds. Młodzieży w Montrealu w Kanadzie i przyznał się do winy w 56 osób.Liczby te obejmowały zgorszenie własności ponad 5000 USD w stosunku do stron internetowych, w tym CNN.com, w związku z atakami z lutego 2000 r. Pozostałe dane dotyczą nieautoryzowanego dostępu do kilku innych stron internetowych, w tym stron amerykańskich uniwersytetów. 12 września 2001 r. Mafiaboy pojawił się przed sądem ds. Młodzieży w Montrealu w Kanadzie i został skazany na osiem miesięcy „otwartej opieki", rocznego okresu próbnego i ograniczonego korzystania z Internetu. Nazwa MafiaBoy nie została ujawniona przez władze kanadyjskie z powodu kanadyjskich przepisów chroniących nieletnich, chociaż kilku amerykańskich reporterów rozpowszechniło swoją tożsamość w swoich publikacjach. Jego główny wkład w historię kryminalistycznych komputerów pokazał asymetryczne działania wojenne w cyberprzestrzeni. Jego działania pokazały, że nawet nieświadome dziecko z małą wiedzą na temat komputerów może użyć sprzętu i narzędzi o niskiej technologii, dostępnych dla każdego w Internecie, aby okaleczyć duże organizacje.

PODZIEMIE HACKERSKIE .

Nowicjusze w dziedzinie zapewniania informacji napotkają odniesienia do podziemia komputerowego w tekstach, artykułach i dyskusjach. Poniższe sekcje zawierają szkice miniatur niektórych kluczowych grup i wydarzeń w cienistym świecie hakowania kryminalnego (znanego jako czarne kapelusze, w przeciwieństwie do białych kapeluszy, które są ekspertami w zakresie egzekwowania prawa i bezpieczeństwa w zakładach), - umyślni buntownicy, którzy używają niekonwencjonalnych środków, stanowią wyzwanie dla korporacji i rządów w związku z tym, co postrzegają jako awarie bezpieczeństwa (ludzie ci nazywani są często szarymi kapeluszami).

1981: Chaos Computer Club

12 września 1981 r. Grupa niemieckich entuzjastów komputerów o silnej radykalnej orientacji politycznej utworzyła Chaos Computer Club (CCC) w Hamburgu. Jednym z ich pierwszych osiągnięć było wykazanie poważnego problemu w nowej Interaktywnej usłudze wideotekstowej Bilschirmtext (BTX) w 1984 r w Bundespost (niemiecka poczta)., Niedługo po ogłoszeniu usługi CCC wykorzystało luki w zabezpieczeniach BTX do przeniesienia znacznej kwoty pieniędzy na własne konto bankowe za pomocą skryptu, który działał przez noc jako demonstracja dla prasy (publiczne zwracanie pieniędzy). Po ogłoszeniu 1 stycznia 1999 r. Przez Legion of Underground (LoU), że zaatakują i dezaktywują systemy komputerowe Chińskiej Republiki Ludowej i Iraku, koalicja organizacji hakerskich, w tym CCC, ogłosiła sprzeciw wobec tego ruchu. „Zdecydowanie sprzeciwiamy się wszelkim próbom użycia siły hakowania, aby zagrozić lub zniszczyć infrastrukturę informacyjną kraju z dowolnego powodu" - powiedziała koalicja. „Wypowiadanie wojny krajowi jest najbardziej nieodpowiedzialną rzeczą, jaką może zrobić grupa hakerów. Nie ma to nic wspólnego z haktywizmem ani etyką hakerów i nie jest niczym, z czego haker mógłby być dumny - powiedziała koalicja w oświadczeniu. CCC, ogólnie rzecz biorąc, podważyło ogólny pogląd, że „haker" musi koniecznie oznaczać „hakera kryminalnego". Ich doroczne Chaos Communications Conference okazały się miejscem wymiany technologii i poważnych dyskusji na temat bezpieczeństwa informacji. Ich ciągłe zaangażowanie w praworządność (z wyjątkiem sytuacji, w których dotyczą ich własne działania) oraz chęć angażowania władz w sądy, gdy jest to konieczne, zapewniły im niezwykłą wiarygodność i akceptację w środowisku bezpieczeństwa informacji jako stosunkowo jasnoszare kapelusze

1982: 414.

Pewnego ranka w czerwcu 1982 r. Administrator systemu dla minikomputera DEC VAX 11/780 w Memorial Sloan-Kettering Cancer Center na Manhattanie znalazł swój system złamanym. Dochodzenie

doprowadziło do odkrycia, że jego i dziesiątki innych systemów w całym kraju zostały zhakowane przez nastolatków z obszaru Milwaukee i innych w wieku od 15 do 22 lat. Młodzi nazywali się 414 po numerze kierunkowym Milwaukee. Korzystając z komputerów domowych podłączonych do zwykłych linii telefonicznych, włamali się do komputerów w Stanach Zjednoczonych i Kanadzie, w tym jednego w banku w Los Angeles, drugiego w firmie cementowej w Montrealu i, złowieszczo, niesklasyfikowanego komputera w laboratorium broni jądrowej w Los Alamos, [Nowy Meksyk]. W marcu 1984 r. „Dwóch członków Gangu 414 Milwaukee rzyznało się do winy za wykroczenia związane z wykonywaniem nieprzyzwoitych lub nękających połączeń telefonicznych. Maksymalna kara za każdą opłatę: sześć miesięcy w więzieniu i grzywna w wysokości 500 USD. ”

1984: Cult of the Dead Cow.

Inną wpływową grupą hakerów kryminalnych jest Cult of the Dead Cow (cDc), który uprawiał zabawne (choć celowo obraźliwe dla niektórych) bajki, takie jak krucyfiks krowy. cDc było znane z konsekwentnego używania humoru i parodii; na przykład artykuł „Swamp Rat” z 1985 r. na temat budowy „Niesławnej BOMBY GERBIL FEED” zawierał instrukcje, takie jak „Zapal bezpiecznik, jeśli go włożysz. Jeśli wrzuciłeś do niego zapałkę, przejdź do najbliższego telefonu, wybierz „911” i powiedz miłym ludziom, że w dolnej części ciała znajduje się duża liczba odłamków szkła. Niedługo powinna tam być karetka pogotowia ”. CDC stało się ważnymi zwolennikami haktywizmu w latach 90. XX wieku - wykorzystywania technik hakerskich w celach przestępczych do celów politycznych. Wydali także szereg narzędzi hakerskich, z których Back Orifice (BO), a zwłaszcza Back Orifice 2000 (BO2K), były znanymi przykładami. BO2K był rzekomo narzędziem do zdalnej administracji, ale w rzeczywistości był trojanem działającym w trybie ukrytym i pozwalającym na zdalne sterowanie zainfekowanymi maszynami. Niektórzy obserwatorzy uważali, że przedstawienie BO2K jako legalnego narzędzia było kolejnym przykładem satyrycznej skłonności cDc: pomysł, że każdy uzna oprogramowanie napisane przez hakerów za wiarygodne narzędzie administracyjne, uznał je za niedorzeczne.

1984: 2600 : The Hacker Quarterly

Kwartalnik hakerów. Eric Corley założył 2600:The Hacker Quarterly w 1984 roku. Publikacja ta stała się standardem dla zwolenników hackowania przestępczego. Magazyn publikował stałe objaśnienie sposobów wykorzystania określonych luk w szerokim zakresie systemów operacyjnych i środowisk aplikacji. Ponadto filozofia polityczna redaktora wpłynęła na więcej niż jedno pokolenie hakerów w czarnych kapeluszach i szarych kapeluszach: według światopoglądu z 2600 r. Niewielka grupa braci technokratów (rzadko sióstr) jest oblężoną awangardą prawdziwie wolnej i uczciwej . Reszta świata jest wiriem przestępczości korporacyjnej i korupcji na wysokim szczeblu rządowym, niekiedy łagodzonych przez dobrze rozumną ignorancję. Przeczytanie kilku numerów z rzędu oznacza koszmar podobny do Sołżenicyna, nieco złagodzony faktem, że 2600 jest często niezwykle zabawny.

1984: Legion of Doom . Imperium DC Comics stworzyło serial animowany o nazwie Super Friends, który pojawił się w 1973 roku; wystąpili w niej bohaterowie DC Comics, tacy jak Superman, Aquaman, Wonder Woman i Batman. W kolejnej serii zatytułowanej Wyzwanie super przyjaciół, która trwała od 1978 do 1979 r., Arcy wrogami tych bohaterów była grupa znana jako Legion of Doom, w skład której wchodził Lex Luthor, arcywróg Supermana. Grupa phreakerów telefonicznych, którzy później przeszli na hakowanie kryminalne, nazwała się Legion of Doom (LOD); ich założyciel nazwał się „Lex Luthor”. Innym ważnym członkiem był Loyd Blankenship („Mentor”). Bruce Sterling opisuje LOD jako wpływową podziemną grupę hakerów z lat 80. i jedną z pierwszych, która korzysta z regularnej publikacji swoich odkryć luk w zabezpieczeniach i exploitów w systemie telefonicznym, a następnie w sieciach komputerowych: członkowie LOD zdawali się instynktownie rozumieć, że droga do prawdziwej władzy w podziemiu prowadzona była przez potajemną reklamę. LOD były rażące. Była to nie tylko jedna z

pierwszych grup, ale członkowie starali się szeroko rozpowszechniać swoją nielegalną wiedzę. Niektórzy członkowie LOD, jak „Mentor", byli bliscy ewangelizacji. Dziennik techniczny Legion of Doom zaczął pojawiać się na deskach w całym podziemiu. LOD Technical Journal został nazwany okrutną parodią starożytnego i honorowego czasopisma technicznego AT&T. Materiał w tych dwóch publikacjach był dość podobny - większość z nich pochodzi z czasopism publicznych i dyskusji w społeczności telekomunikacyjnej. A jednak drapieżne podejście LOD sprawiło, że nawet najbardziej nieszkodliwe dane wydawały się głęboko złowrogie; oburzenie; jasne i obecne niebezpieczeństwo. W późnych latach osiemdziesiątych LOD czasami pomagał organom ścigania, powstrzymując złośliwych hakerów. Jednym z najbardziej znanych członków był Chris Goggans, którego pseudonimem był „Erik Bloodaxe"; był także redaktorem Phrack, a później stał się częścią Masters of Deception (MOD), które było zaangażowane w konflikt z LOD w 1990 i 1991 roku, znane w kręgach hakerów jako „Wielka wojna hakerów". Innym znanym hakerem, który rozpoczął pracę w LOD i przeniósł się do MOD, był Mark Abene („Phiber Optik"), który ostatecznie został uwięziony na rok po przyznaniu się w sądzie federalnym do spisku i nieuprawnionego dostępu do komputerów będących przedmiotem zainteresowania federalnego (naruszenie 18 USC 1030 (a), Ustawa o oszustwach i nadużyciach komputerowych z 1986 r.). Kara Abene była przedmiotem wielu protestów w społeczności hakerów i gdzie indziej.

1985: Phrack

Phrack zaczął publikować w listopadzie 1985 roku. Z nowym numerem co miesiąc lub dwa, magazyn elektroniczny kontynuował nieprzerwanie dystrybucję informacji technicznych i rad. Nieocenzurowany komentarz dał fascynujące spojrzenie na niektóre osobowości i światopoglądy jego autorów i redaktorów, w tym Taran King i Craig Neidorf (później zasłynął jako „Błyskawica rycerza" oraz za jego udział w nieudanym ściganiu z udziałem dokumentów Bell-South) . Na przykład Phrack opublikował coś, co stało się znane jako „Manifest hakera", popierany przez hakerów kryminalnych jako światło dla narodów („Napisane prawie 15 lat temu przez Mentora, powinno być przyklejone obok monitora każdego, aby przypomnieć, kto jesteśmy, to zadzwoniło do hakerów, ale teraz dzwoni prawdą do generacji Internetu. "), ale sceptycznie patrzą na nią specjaliści od bezpieczeństwa. Po części brzmi: To jest teraz nasz świat… świat elektronów i przełączników, piękno bod. Korzystamy z usługi, która już istnieje, nie płacąc za coś, co mogłoby być tanie jak brud, gdyby nie było prowadzone przez spekulujące żarłoków, a ty nazywasz nas przestępcami. Badamy ... a ty nazywasz nas przestępcami. Szukamy wiedzy… a ty nazywasz nas przestępcami. Istniejemy bez koloru skóry, bez narodowości, bez uprzedzeń religijnych ... a wy nazywacie nas przestępcami. Budujesz bomby atomowe, prowadzisz wojny, mordujesz, oszukujesz i okłamujesz nas i próbujesz sprawić, że uwierzymy, że to dla naszego własnego dobra, a jednak jesteśmy przestępcami. Tak, jestem przestępcą. Moją zbrodnią jest ciekawość. Moim przestępstwem jest osądzanie ludzi na podstawie tego, co mówią i myślą, a nie jak wyglądają. Moją zbrodnią jest przechytrzenie cię, coś, za co nigdy mi nie wybaczysz. Jestem hakerem i to jest mój manifest. Możesz zatrzymać tę osobę, ale nie możesz nas wszystkich zatrzymać ... przecież wszyscy jesteśmy tacy sami. W latach 90. częstotliwość publikacji uległa zmniejszeniu, spadając raz na trzy do sześciu miesięcy, dopóki redaktorzy nie ogłosili ostatniego numeru, nr 63, w sierpniu 2005 r. Jednak publikacja została wznowiona pod nowym kierownictwem redakcyjnym w maju 2007 r. Z numerem 64; Biorąc pod uwagę, że numer 65 ukazał się dopiero w kwietniu 2008 r., okres świetności magazynu prawdopodobnie minął.

1989: Masters of Deception (MOD)

Masters of Deception (MOD) to nowojorska grupa hakerów działająca od około 1989 do 1992 r. Wśród najbardziej znanych hakerów kryminalnych w tej grupie był „Phiber Optik" (Mark Abene, urodzony w 1972 r.), który był niezwykle widoczny w mediach: W szczególności Phiber Optik miał wykorzystać ten

dzień w 1990 roku. Adiunkt z kręgu 2600 i niezłomny z grupy hackerów nowojorskich „Masters of Deception”, Phiber Optik był wspaniałym przykładem intruza komputerowego jako oddanego dysydenta. Osiemnastoletni Optik, licealista i mechanik komputerowy w niepełnym wymiarze godzin, był młodym, inteligentnym i bezwzględnie obsesyjnym, ostro ubranym, gadatliwym, cyfrowym facetem, który był absolutnie i wyraźnie pogardliwy wobec zasad innych niż własne. Pod koniec 1991 roku Phiber Optik pojawił się w Harper's, Esquire, New York Times, w niezliczonych publicznych debatach i konwencjach, nawet w programie telewizyjnym prowadzonym przez Geraldo Riverę.

1990: Operacja Sundevil.

Po dwóch latach śledztwa, w dniach 7, 8 i 9 maja 1990 r. 150 agentów FBI, wspomaganych przez władze stanowe i lokalne, dokonało nalotu na organizacje podejrzane o włamanie do organizacji przestępczych rzekomo zaangażowanych w nadużywanie kart kredytowych i kradzież usług telefonicznych. Przejęli 42 komputery i 23 000 dysków z lokalizacji w 14 miastach. Celami były głównie strony prowadzące fora dyskusyjne, z których niektóre zostały sklasyfikowane jako „fora hakerów”. Jednak dwa lata po nalocie były tylko trzy akty oskarżenia (skutkujące trzema winnymi zarzutami). Zaczęły gromadzić się dowody na to, że większość dowodów zgromadzonych podczas nalotów była bezużyteczna. Bruce Sterling spędził półtora roku badając tę operację i doszedł do wniosku, że był to w dużej mierze wysiłek propagandowy: Bezprecedensowe działanie o wielkiej ambicji i wielkości, motywy Sundevila można określić tylko jako polityczne. Był to wysiłek public relations, mający na celu przekazywanie pewnych wiadomości, mający na celu wyjaśnienie pewnych sytuacji: zarówno w umyśle ogółu społeczeństwa, jak iw umysłach różnych grup społecznych społeczności elektronicznej. Po pierwsze - i ta motywacja była niezbędna - od organów ścigania do cyfrowego podziemia zostanie wysłana „wiadomość”. To samo przesłanie zostało wypowiedziane w wielu słowach Garry M. Jenkins, zastępca dyrektora tajnych służb USA na konferencji prasowej Sundevil w Phoenix w dniu 9 maja 1990 r., Bezpośrednio po nalotach. Krótko mówiąc, hakerzy mylili się w swoim głupim przekonaniu, że mogą ukryć się za „względną anonimowością swoich terminali komputerowych”. Przeciwnie, powinni w pełni zrozumieć, że policjanci stanowi i federalni aktywnie patrolowali rytm w cyberprzestrzeni - że byli na zegarek wszędzie, nawet w tych obskurnych i tajemniczych norach cybernetycznych występków, podziemnych tablicach.

1990: Steve Jackson Games.

Dwa miesiące przed nalotami na Operację Sundevil, ale (w przeciwieństwie do popularnego połączenia tych dwóch) w zupełnie odrębnej operacji, firma zajmująca się grą RPG o nazwie Steve Jackson Games w Austin w Teksasie została zaatakowana 1 marca 1990 r. Tajna służba przejęli komputery i dyski w biurach firmy, a także w domu jednego z ich pracowników, Loyda Blankenshipa - „Mentora”, dawniej LOD. Blankenship pisał grę RPG o nazwie GURPS Cyberpunk, którą agenci interpretowali jako „podręcznik przestępstw komputerowych”. Część sprzętu skonfiskowanego podczas nalotu zwrócono cztery tygodnie później; większość, ale nie wszystko, została zwrócona cztery miesiące później. Firma prawie zbankrutowała w wyniku sekwestracji zasobów krytycznych. Oburzenie społeczności komputerowej rozprzestrzeniło się poza podziemia. Mitch Kapor, John Barlow i John Gilmore założyli Electronic Frontier Foundation częściowo ze względu na oburzenie związane z traktowaniem Steve Jackson Games:

…Zaangażowaliśmy prawników, a następnie poprosiliśmy ich, aby zbadali, co się dzieje z różnymi dochodzeniami i postępowaniami rządowymi. Zidentyfikowaliśmy kilka szczególnych sytuacji prawnych, takich jak Craig Neidorf w Chicago i Steve Jackson Games, gdzie wydawało nam się, że nastąpiło znaczne przekroczenie granic przez rząd oraz naruszenie prawa do wolności słowa i wolności prasy. Właśnie decydowaliśmy, jak to zrobić by interweniować, gdy bardzo wyraźnie zdaliśmy sobie

sprawę, że nie chcieliśmy być funduszem obrony prawnej, ponieważ było to zbyt wąskie. Naprawdę potrzebna była poprawa dyskursu o tym, w jaki sposób technologia będzie wykorzystywana przez społeczeństwo; musimy robić rzeczy w obszarze publicznym edukacji i rozwoju polityki. …

Steve Jackson Games pozwał Tajne Służby o odszkodowania i przyznano im 50 000 USD odszkodowania oraz ponad 25 000 USD honorariów adwokackich. Sprawa miała trwały wpływ na sposób, w jaki funkcjonariusze organów ścigania przeprowadzali dochodzenia w sprawie przestępstw komputerowych i konfiskaty dowodów elektronicznych.

1992: L0pht Heavy Industries.

W 1992 r. Grupa entuzjastów komputerów zorganizowała przechowywanie zapasowego sprzętu w wynajętej powierzchni w Bostonie. Współpracowali przy analizie słabych punktów, w szczególności słabych punktów produktów Microsoft, i zyskali reputację dzięki poważnym badaniom w tej dziedzinie oraz pojawianiu się na konferencjach dotyczących bezpieczeństwa. Ich program „L0phtCrack" został przyjęty przez wielu administratorów systemu do testowania plików haseł w celu zlokalizowania łatwych do odgadnięcia haseł; członkowie nawet zeznawali przed Senacką Podkomisją ds. Cyberbezpieczeństwa Rządowego w 1998 r. (mówiąc, że mogą zdjąć Internet za pół godziny) . Słynne rączki z grupy to „Brian Oblivion", „Kingpin", „Mudge", „Space Rogue, "„ Stefan von Neumann, „Tan" i „Weld Pond". Grupa spowodowałaszum w podziemnych i naziemnych społecznościach bezpieczeństwa, gdy ich firma, L0pht Heavy Industries, została zakupiona przez firmę ochroniarską @stake, Inc. w 2000 roku. ostatecznie kupiony przez Symantec w 1994 roku.

2004: Shadowcrew

Kradzież fizycznych kart kredytowych i tworzenie fałszywych kart to część techniki kryminalnej zwanej „carding". Jednym ze znaczących sukcesów dochodzenia i ścigania międzynarodowego pierścienia oszustw związanych z kartami kredytowymi w 2000 roku rozpoczęły się od operacji zapory ogniowej US Secret Service pod koniec 2004 roku. Śledczy odkryli sieć ponad 4000 członków komunikujących się przez Internet i spiskowców, którzy używają phishingu, spamu, fałszywej tożsamości dokumenty (np. fałszywe prawa jazdy), tworzenie fałszywych plastikowych kart kredytowych, odsprzedaż kart podarunkowych kupowanych za pomocą fałszywych kart kredytowych, ogrodzenie skradzionych towarów za pośrednictwem serwisu eBay oraz międzypaństwowe lub międzynarodowe transfery środków przy użyciu pieniędzy elektronicznych, takich jak E-Gold i Web Money . W październiku 2004 r. Departament Sprawiedliwości postawił w stan oskarżenia 19 przywódców Shadowcrew. Do listopada 2005 r. 12 z tych osób przyznało się już do oskarżeń o spisek i korki przy skradzionych numerach kart kredytowych przy stratach przekraczających 4 miliony dolarów. W lutym 2006 r. Przywódca Shadowcrew, 41-letni Kenneth J. Flury z Cleveland Ohio, został skazany na 32 miesiące więzienia z trzyletnim nadzorowanym zwolnieniem i 300 000 USD w restytucji na Citibank. W czerwcu 2006 r. Współzałożyciel Andrew Mantovani, 24, ze Scottsdale, Arizona została ukarana grzywną w wysokości 5000 $, a także otrzymała 32 miesiące więzienia z trzyletnim nadzorowanym zwolnieniem. Pięciu innych postawionych w stan oskarżenia kryminalistów skazano z nim. Do tego czasu w sumie 18 z 28 podejrzanych zostało już uznanych za winnych.

Pod koniec 2000 roku: Russian Business Network (RBN) .ussian Business Network (RBN) mogła powstać jako legalna firma hostingowa w 2006 roku:

Według firmy Verisign zajmującej się bezpieczeństwem internetowym, która w czerwcu opublikowała szeroko zakrojone dochodzenie w sprawie rosyjskiego stroju (tinyurl.com/ywvgpg), RBN został zarejestrowany jako strona internetowa w 2006 r. Początkowo znaczna część jej działalności była legalna. Ale najwyraźniej założyciele wkrótce odkryli, że bardziej opłacalne jest prowadzenie

nielegalnych działań i zaczęli wynajmować swoje usługi przestępcom. Verisign mówi po prostu, że jest teraz „całkowicie nielegalne”. Od tego czasu jego działania były monitorowane przez wiele organizacji, w tym londyńską grupę antyspamową Spamhaus. „RBN należy do najgorszych na świecie sieci spamerskich, pornografii dziecięcej, złośliwego oprogramowania, phishingu i cyberprzestępczości” - mówi rzecznik. „Zapewnia„ kuloodporny ”hosting, ale prawdopodobnie jest również zamieszany w przestępstwo.”

Badacz Internet Storm Center, „David Bizeul”, spędził ostatnie trzy miesiące na badaniu rosyjskiej sieci biznesowej (RBN). RBN jest wirtualnym schronieniem dla rosyjskich przestępców odpowiedzialnych za ataki złośliwego kodu, ataki phishingowe, pornografię dziecięcą i inne nielegalne operacje… ”Badanie Bizeula to 70-stronicowy raport z obszerną dokumentacją na temat działalności przestępczej RBN. Grupa wspiera rozpowszechnianie złośliwego oprogramowania, spam, phishing, odmowę usługi, dystrybucję narzędzi do cyberataków, pornografię i pornografię dziecięcą. Raport Davida Goldmana z 2011 r. Zawierał następujące przydatne informacje:

„To nie jest mafia, to mafia prowadząca te operacje”, powiedział Karim Hijazi, dyrektor generalny firmy monitorującej botnety Unveillance. „Rosyjska mafia to najbardziej płodni cyberprzestępcy na świecie. Zorganizowana cyberprzestępczość to prawdziwie międzynarodowa sprawa, ale najbardziej zaawansowane ataki zwykle pochodzą z Rosji. Rosyjski tłum jest niesamowicie utalentowany z jakiegoś powodu: po zniesieniu żelaznej kurtyny w latach 90. wielu byłych cyberprzestępców z KGB zdało sobie sprawę, że mogą wykorzystać swoje umiejętności eksperckie i szkolenie, aby zarobić na zhakowanych informacjach, które wcześniej pozyskiwali dla rządu cele szpiegowskie. Byli szpiedzy zgrupowani razem, tworząc Rosyjską Sieć Biznesu, przestępcze przedsiębiorstwo, które jest zdolne do niektórych naprawdę przerażających ataków. To tylko jedna z wielu zorganizowanych organizacji cyberprzestępczych, ale jedna z najstarszych i największych.

„Rosjanie zmagali się z umiejętnościami technicznymi” - powiedział Greg Hoglund, CEO firmy cyberbezpieczeństwa HBGary. „Rosyjscy przestępcy mają niedorzeczny zestaw narzędzi. W wielu przypadkach kierują reklamy do użytkowników końcowych, dlatego muszą być wyrafinowani ”.

Anonymous

W 2003 roku działacze polityczni z zamiłowaniem do umiejętności obsługi komputera utworzyli luźne stowarzyszenie nazywające się Anonimowym dla współpracy w szeregu cyberataków na cele, których członkowie nie lubili. Filozofia grupy wyraźnie odrzuca wszelkie scentralizowane kontrole; każdy może twierdzić, że jest członkiem Anonimowego. W 2008 r. Samozidentyfikowani członkowie ruchu opisywali swoje wysiłki Chanology zaatakował Kościół Scjentologii. Członkowie nękali także organizacje próbujące zaostrzyć przepisy dotyczące własności intelektualnej oraz ograniczenia egzekwowania prawa i zwalczania piractwa. Inne cele tej organizacji to Epilepsy Foundation, hip-hopowe strony internetowe, kampania polityczna Sarah Palin, rząd Iranu, rząd Australii oraz oddział Tea Party w Oregonie. Jedna z najbardziej nagłośnionych kampanii poparła Juliana Assange'a, lidera Fundacji WikiLeaks, którego grupa upubliczniła ponad milion dokumentów sklasyfikowanych przez USA i inne rządy jako zastrzeżone lub tajne i ujawniła zawstydzające szczegóły kilku wojen i komunikacji wewnętrznej wśród dyplomatów. W styczniu 2013 r. Członkowie ogłosili, że udostępnią duże ilości informacji zastrzeżonych przez rząd USA. Informują świat o swoich planach, publikując swoje wiadomości na zhakowanej stronie internetowej rządu USA.

2013: Unlimited Operations

W maju 2013 r. Ośmiu hakerów kryminalnych, członkowie znacznie większego światowego kręgu cyberprzestępców nazywających się Unlimited Operations, zostali oskarżeni o kradzież o wartości

ponad 45 milionów dolarów z bankomatów na całym świecie. Gang „zastosował wyrafinowane techniki włamań do włamania się do systemów globalnych instytucji finansowych, kradzieży danych kart debetowych przedpłaconych i wyeliminowania limitów wypłat. Skradzione dane karty były następnie rozpowszechniane na całym świecie i wykorzystywane do dokonywania fałszywych wypłat z bankomatów na dużą skalę na całym świecie"

W pierwszej fazie przestępcy włamali się do Narodowego Banku Ras Al-Khaimah PSC (RAKBANK) w Zjednoczonych Emiratach Arabskich. Korzystając z tych zainfekowanych danych, sieć przestępcza przeprowadziła ponad 4500 transakcji bankomatowych w ciągu 20 godzin i ukradła ponad 5 milionów dolarów. Drugi etap rozpoczął się „… po południu 19 lutego i trwał do wczesnego rana 20 lutego 2013 r. Ta operacja ponownie naruszyła sieć procesora kart kredytowych, który obsługiwał przedpłacone karty debetowe MasterCard, tym razem wydane przez Bank of Muscat , z siedzibą w Omanie. "Całkowite straty z 36 000 transakcji w 24 krajach zarobiły 40 milionów dolarów w gotówce z bankomatów.

SZPEIGOSTWO PRZEMYSŁOWE

Po co wydawać pieniądze na opracowywanie konkurencyjnych produktów, skoro można ukraść pracę, gdy jest gotowa do zastosowania? Wiele firm w krajach, w których praworządność jest słaba lub nie ma jej wcale, skorzystało ze złego bezpieczeństwa, outsourcingu i liberalnej polityki imigracyjnej, aby ukraść własność intelektualną i konkurować ze zniżką z pomysłodawcami.

* W 2001 r. JunshengWang z Bell Imaging Technologies przyznał się do naruszenia 18 USC 132 (a) (2) poprzez kradzież tajemnic handlowych z Acuson Corporation. W raporcie Countinintelligence News and Developments (CIND) stwierdzono: „Wang, przyznając się do winy, przyznał, że przed 24 sierpnia 2000 r. wziął bez autoryzacji i skopiował dla Bell Imaging dokument przedstawiający architekturę urządzenia ultrasonograficznego Sequoia, które zawierało handel tajemnice Acuson Corporation. Zgodnie z umową Wanga, był on w stanie uzyskać dostęp do tajemnic handlowych Acuson, ponieważ jego żona była zatrudniona jako inżynier w tej firmie i ponieważ przyniosła ten dokument do ich domu. Po skopiowaniu dokumentu zabrał go ze sobą w podróż służbową do Chińskiej Republiki Ludowej, przekazując go firmie Bell Imaging w 2000 r"

* W maju 2001 r. władze federalne aresztowały dwóch naukowców Lucent i trzeciego człowieka opisanego jako ich partner biznesowy 4 maja, oskarżając ich o kradzież kodu źródłowego oprogramowania powiązanego z PathStar Access Server Lucent i udostępniając go Datang Telecom Technology Co., Pekin firma będąca w większości własnością rządu chińskiego. Oprogramowanie jest uważane za „klejnot koronny" firmy. Obywatele chińscy Hai Lin i Kai Xu byli uważani za „wybitnych członków" personelu Lucenta aż do ich aresztowania. Motywacją kradzieży, zgodnie z dokumentami sądowymi, było zbudowanie potęgi sieciowej podobnej do „Cisco of China". Mężczyźni stanęli wobec zarzutów spisku mającego na celu popełnienie oszustwa w sieci, karanego maksymalnie pięcioletnim więzieniem i grzywną w wysokości 250 000 USD. W kwietniu 2002 r. Obaj zostali również oskarżeni o kradzież tajemnic czterech firm oprócz Lucent: Telenetworks, NetPlane Systems, Hughes Software Systems i Ziatech. Oskarżono także dodatkowego obywatela chińskiego, Yong-Qing Chenga. Opracowali spółkę joint venture z Datang Telecom Technology Company z Pekinu, aby sprzedać klon systemu transmisji danych i głosu Lucent Path Star do dostawcy Internetu w Chinach.

* We wrześniu 2002 r. Firma 3DGeo w Mountain View w Kalifornii oskarżyła Shan Yanming, pracownika China National Petroleum Corporation, od pożyczek dla firmy, o szpiegostwo przemysłowe za próby kradzieży oprogramowania zaprojektowanego do wykorzystywania danych sejsmicznych do mapowania złóż ropy. Został przyłapany na próbie pobrania danych korporacyjnych na swój komputer osobisty i został aresztowany przez agentów FBI.

* W kwietniu 2003 r. Biuro Prokuratora Stanów Zjednoczonych dla Północnego Dystryktu Kalifornii ogłosiło, że 9 kwietnia 2003 r. Tse Thow Sun przyznał się do winy za kradzież tajemnic handlowych. Przyznał, że na początku 2002 r., Pracując dla firmy tłumaczącej język, dostarczył laptopa i dysk twardy zawierający tajemnice handlowe i poufne informacje zastrzeżone dla konkurenta i zapytał o płatność w wysokości 3 milionów USD. Sun, 32-letni obywatel Singapuru, został oskarżony przez Sąd Federalny w dniu 9 kwietnia 2002 r. Został oskarżony o kradzież tajemnic handlowych, z naruszeniem 18 U.S.C. § 1832 (a) (3); próba kradzieży tajemnic handlowych, z naruszeniem 18 U.S.C. § 1832 (a) (4); i międzystanowy transport skradzionych towarów, z naruszeniem 18 U.S.C. §2314. Na podstawie umowy w sprawie zarzutu pan Sun przyznał się do kradzieży tajemnic handlowych.

* W maju 2003 r. Trzech szwedzkich pracowników LM Ericsson zostało oskarżonych o szpiegostwo za rzekome kradzież własności intelektualnej i wysłanie jej rosyjskim szpiegom. „[Afshin] Bavand został aresztowany 5 listopada 2002 r. Podczas rozmowy z rosyjskim agentem wywiadu na przedmieściach Sztokholmu. Policja przeszukała Rosjanina, który nie został zidentyfikowany, i znalazła 4000 dolarów w gotówce i dokumentach Ericsson

* Seria ataków o kryptonimie „Titan Rain" została odkryta przez Shawna Carpentera pod koniec 2003 roku. Carpenter zauważył powódź działalności hakerów skupiających się na kradzieży danych z szerokiej gamy „najbardziej wrażliwych baz wojskowych, kontrahentów i firm lotniczych". odkrył, że „ataki pochodziły tylko od trzech chińskich routerów, które działały jako pierwszy punkt połączenia z sieci lokalnej do Internetu". Carpenter współpracował z armią amerykańską i śledczymi FBI, aby dowiedzieć się więcej o atakach i atakujących. Według Thornburgha wielu analityków ocenia, że „Uważa się, że Titan Rain należy do najbardziej rozpowszechnionych zagrożeń cyberszpiegowskich, jakie kiedykolwiek miały sieci komputerowe w USA.

* W lipcu 2004 r. Indyjski inżynier oprogramowania zatrudniony w amerykańskim centrum rozwoju oprogramowania w Indiach został oskarżony o „spakowanie" zastrzeżonego kodu źródłowego oprogramowania do drukowania kart identyfikacyjnych i przesłania go na osobiste konto e-mail. W rezultacie Jolly Technologies zakończyło działalność w Bombaju

* W 2005 i 2006 r. EMC wniosła pozew przeciwko kilku pracownikom o rzekome kradzież tajemnic handlowych.

* W grudniu 2006 r. Dwóch obywateli chińskich, Fei Ye i Ming Zhong, przyznało się w grudniu 2006 r. do zarzutów o szpiegostwo gospodarcze w imieniu Chińskiej Republiki Ludowej. Zostali aresztowani w listopadzie 2001 r. Ze skradzionymi tajemnicami handlowymi w bagażu; informacje pochodzą z Sun Microsystems i Transmeta Corporation. Agenci planowali zaprojektować konkurencyjnego mikroprocesora przy użyciu skradzionych projektów; zyski miały zostać podzielone z miastem Hangzhou i prowincją Zhejiang. Firma agentów została częściowo sfinansowana z chińskiego Narodowego Programu Badań i Rozwoju Zaawansowanych Technologii.

* W kwietniu 2008 r. Śpiący agent Chi Mak, naturalizowany obywatel USA, który mieszkał w Los Angeles przez 20 lat, został skazany na 24,5 lat więzienia federalnego za szpiegostwo przemysłowe. Ukradł szczegółowe plany dotyczące sprzętu marynarki wojennej USA, w tym podwodnych systemów napędowych, i próbował wysłać je do Chin za pośrednictwem swojego brata i szwagierki.

* W 2009 r. Siobhan Gorman, pisząc w TheWall Street Journal, podała, co następuje:

Według obecnych i byłych urzędników ds. Bezpieczeństwa cyberprzestępcy przeniknęli do sieci elektrycznej w USA i pozostawili programy, które mogłyby zostać wykorzystane do za kłócenia działania systemu. Urzędnicy powiedzieli, że szpiedzy przybyli z Chin, Rosji i innych krajów podobno mieli misję

poruszania się po amerykańskim systemie elektrycznym i jego elementach sterujących. Intruzi nie próbowali uszkodzić sieci energetycznej ani innej kluczowej infrastruktury, ale urzędnicy ostrzegali, że mogą spróbować podczas kryzysu lub wojny. „Chińczycy próbowali zmapować naszą infrastrukturę, taką jak sieć elektryczna", powiedział starszy urzędnik wywiadu. „Podobnie Rosjanie". Szpiegostwo wydawało się wszechobecne w USA i nie jest skierowane do żadnej firmy ani regionu, powiedział były urzędnik Departamentu Bezpieczeństwa Wewnętrznego. „Są ingerencje i narastają", powiedział były urzędnik, odnosząc się do systemów elektrycznych. „W zeszłym roku było ich wiele."

* Biuro National Counterintelligence Executive (ONCIX) opublikowało swój raport do Kongresu w sprawie Zagranicznego Poboru Gospodarczego i Szpiegostwa Przemysłowego 2009–2011 zatytułowany „Zagraniczni szpiedzy kradnący tajemnice gospodarcze USA w cyberprzestrzeni". Streszczenie zawierało ten komentarz:

Wrażliwe informacje i technologie gospodarcze w USA są atakowane przez służby wywiadowcze, firmy sektora prywatnego, instytucje akademickie i badawcze oraz obywateli dziesiątek krajów.

* Chińscy aktorzy są najbardziej aktywnymi i stałymi na świecie sprawcami szpiegostwa gospodarczego. Amerykańskie firmy z sektora prywatnego i specjaliści ds. Bezpieczeństwa cybernetycznego zgłosili atak włamań do sieci komputerowej, które powstały w Chinach, ale IC nie może potwierdzić, kto był za to odpowiedzialny.

* Rosyjskie służby wywiadowcze prowadzą szereg działań w celu zebrania informacji gospodarczych i technologii od celów USA.

* Niektórzy amerykańscy sojusznicy i partnerzy korzystają ze swojego szerokiego dostępu do amerykańskich instytucji w celu uzyskania poufnych informacji ekonomicznych i technologicznych w USA, przede wszystkim poprzez agresywne pozyskiwanie i inne taktyki wywiadu ludzkiego (HUMINT). Niektóre z tych stanów mają zaawansowane możliwości cybernetyczne.

* Raport z marca 2012 r. Wyszczególniał, w jaki sposób firma American Superconductor Corporation (AMSC), odnosząca sukcesy firma nadzorująca i gromadząca dane (SCADA), została praktycznie zniszczona ekonomicznie przez głównego klienta, chińską firmę Sinovel, która ukradła ich własne oprogramowanie turbin wiatrowych i następnie przestał płacić za jakiekolwiek dalsze usługi oprogramowania.

* Na początku 2013 r. Raport firmy Symantec dotyczący zagrożeń bezpieczeństwa w Internecie w 2012 r., poinformował, że małe firmy są coraz częściej atakowane przez cyberataki i szpiegostwo przemysłowe: „W 2012 r. 50 procent wszystkich ukierunkowanych ataków było wymierzonych w firmy zatrudniające mniej niż 2500 pracowników. W rzeczywistości największym obszarem wzrostu ukierunkowanych ataków w 2012 r. były firmy zatrudniające mniej niż 250 pracowników; 31 procent wszystkich ataków było ich ".