Ryszard Szpyra, Wiesław Otwinowski

Współczesne formy prowadzenia ataków informatycznych

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 3, 77-90

2010

Artykuł został opracowany do udostępnienia w internecie przez Muzeum Historii Polski w ramach prac podejmowanych na rzecz zapewnienia otwartego, powszechnego i trwałego dostępu do polskiego dorobku naukowego i kulturalnego. Artykuł jest umieszczony w kolekcji cyfrowej bazhum.muzhp.pl, gromadzącej zawartość polskich czasopism humanistycznych i społecznych.

Tekst jest udostępniony do wykorzystania w ramach dozwolonego użytku.

MUZEUM HISTORII POLSKI

Ryszard SZPYRA
Wiesław OTWINOWSKI
Wyższa Szkoła Bezpieczeństwa z siedzibą w Poznaniu

WSPÓŁCZESNE FORMY PROWADZENIA ATAKÓW INFORMATYCZNYCH

W ramach walki w sferze przetwarzania danych cyfrowych[1] atakowane mogą być dowolne systemy, które wykorzystują kody cyfrowe do gromadzenia, analizowania, przetwarzania i dystrybucji informacji i umożliwiają skryte wprowadzenie do nich kodu cyfrowego. Rozważając zakres możliwych obiektów ataku zauważyć warto, iż z polityczno-militarnego punktu widzenia dla atakującego byłoby najlepiej gdyby niemalże każdy system wrażliwy na atak został skrycie zainfekowany odpowiednim kodem, który byłby kontrolowany przez atakującego. Z przyczyn praktycznych jest to jednak niemożliwe. Dlatego też obiekty ataku muszą być oceniane i waloryzowane według hierarchii ich ważności tak samo, jak to jest czynione dla potrzeb ataków konwencjonalnych. Wyłanianie i klasyfikowanie obiektów uderzeń poprzedzać powinna intensywna analiza:

Atakowanego systemu, a w nim, jaki typ danych jest przetwarzany? Jaki jest stopień znajomości tego procesu i czy istnieje możliwość zbudowania lub znalezienia odpowiedniego kodu, który mógłby być zastosowany? W jaki sposób atakujący kod może być umieszczony i jakie jest prawdopodobieństwo wykrycia go zanim wykona on swoje zadanie?

Cel ataku, tzn., co należy osiągnąć, jaki efekt i jakie jest prawdopodobieństwo sukcesu? Jakie są polityczne i ogólne cele konfliktu?

Konkretne silne i słabe strony przeciwnika? Jak atak w sferze przetwarzania danych cyfrowych będzie je wykorzystywać? Czy przeciwnik będzie dysponować zapasowymi komponentami, które może użyć by zastąpić zaatakowane elementy? Czy przeciwnik może osiągnąć swój cel bez użycia zautomatyzowanych systemów, które mają być obiektem ataku?

Przypuszczalny sposób działania od góry do poziomu taktycznego. Jak atak w sferze przetwarzania danych cyfrowych wpłynie na sposób wykonywania zadania przeciwnika? Czy dowodzenie i kontrola są zcentralizowane czy zdecentralizowane? Jak wykonanie ataku w sferze przetwarzania danych cyfrowych wpłynie na ogólny wysiłek w konflikcie?

Należy pamiętać o tym, że walka w sferze przetwarzania danych cyfrowych powinna być stosowana w koordynacji z innymi formami działań militarnych i niemilitarnych po to by osiągać najlepsze efekty w zakresie pożądanego celu działań. Walka ta nie jest jedynym narzędziem, ale jednym z tych, które powinny być użyte w skoordynowany sposób z innymi formami walki zbrojnej i niezbrojnej.

Walka w sferze przetwarzania danych cyfrowych może być stosowana na znacznie zróżnicowane sposoby. Może ona być wysoce dokładna precyzyjnie kierowana broń, zabójcza jedynie dla obiektu ataku z nieznacznymi lub żadnymi zniszczeniami towarzyszącymi. Przykładowo odpowiednia pamięć EPROM zainstalowana w samolocie myśliwskim przed jego eksportem, paraliżująca system kontroli lotu, gdy pojawi się odpowiedni sygnał radiowy lub wirus zainstalowany

[1] Szerzej: R. Szpyra: *Militarne operacje informacyjne*. Warszawa 2003

w sieci ğŃcznoŜci przeciwnika, który paraliŻuje utajnionŃ ğŃcznoŜŃ przeciwnika w okreŜlonym czasie moŻe byĺ takŃ broniŃ. UŻycie jej w cyberprzestrzeni stanowi ekwiwalent pocisku kierowanego czy nawet pocisku typu Cruise Missile.

O tym, Ŝe nie jest to tylko teoria Ŝwiadczy wiele przykğadów o jednym z nich piszŃ E.R. Koch i J. Sperber: „Sowiecka sğuŻba specjalna wyraziğa szczególne zainteresowanie „prototypowym softwarem systemowym w kodzie Ŧródğowym, kompilatorami i sterowaniem procesami produkcyjnymi, ponadto róŻnymi programami do wspomaganego komputerowo konstruowania elementów mechanicznych, elektrycznych i elektronicznych w budowie pojazdów, samolotów i przy produkcji chipów, a takŻe informacjami o wojskowym wykorzystaniu amerykaŃskich komputerów i banków danych.ò Tak wielkie zainteresowanie KGB kodem Ŧródğowym Ŝwiadczy o tym, Ŝe Sowieci obawiali siŃ zakupów oprogramowania systemowego na Zachodzie. Podejrzewali, Ŝe mogŃ sobie sprowadziĺ konia trojaŃskiego, gdyŻ nie majŃ Ŝadnej kontroli nad kupowanym softwarem. ByĺmoŻe, mieli juŻ zğe doŚwiadczenia z towarami objŃtymi embargiem, które sprowadzali z Zachodu nielegalnymi kanağami.

Monachijska MI Group zajmowağa siŃ swego czasu kontrolŃ sowieckiej misji wojskowej w Berlinie Wschodnim, która miağa prawo poruszaĺ siŃ swobodnie w dawnych strefach okupacyjnych aliantów, a wiŃc w Niemczech Zachodnich. Tak samo amerykaŃskie, brytyjskie i francuskie misje wojskowe miağy prawo wjeŻdŻaĺ do NRD. Sowieci zamówili wówczas swojŃ flotŃ samochodów dyplomatycznych u Opla. „Z tğ owoce" otrzymağy zlecenie umieszczenia w samochodach elektronicznych pluskiew. W tym teŻ celu wprowadzono do Opla agenta jako pracownika firmy, a dodatkowo straŻnika, ponieważ akcjŃ zamierzano przeprowadzaĺ nocŃ. Przed rozpoczŃciem operacji grupa Ćwiczyğa na terenie monachijskich koszar McGraw rozbieranie i fachowe skğadanie samochodu-atrapy.

Kiedy nadszedğ czas, agenci z US-Army zjechali z róŻnych krajów do Frankfurtu, zostali przewiezieni do odpowiedniej hali i zabrali siŃ za rozbieranie pierwszego wozu dyplomatów. W jego ramy wbudowali miniaturowy nadajnik, poğŃczyli go z wieloma pluskwami rozmieszczonymi na „niebie" samochodu, a nastŃpnie zğoŻyli cağego opla. W przeciŃgu kilku miesiŃcy Amerykanie obsğuŻyli z tuzin samochodów dla sowieckiej misji w Berlinie Wschodnim. Akcja zakoŃczyğa siŃ powodzeniem. Podsğuchane rozmowy umoŻliwiğy zdemaskowanie wielu agentów radzieckich w Zachodnich Niemczechò.[2]

Z drugiej strony walka w sferze przetwarzania danych cyfrowych stosowana bŃdzie dla wywoğania zniszczeŃ na szerokŃ skalŃ. Wirus zainstalowany w komputerze kontrolujŃcym sieĺ energetycznŃ regionu spowodowağby rozlegğe spustoszenia majŃce swoje konsekwencje w sferze militarnej i cywilnej. Zaatakowanie sieci finansowej kraju i paraliŻ gğównych wŃzğów komunikacji finansowej mogğoby spowodowaĺ dğugoterminowy efekt dewastujŃcy ekonomiŃ tego kraju. Takie lub jeszcze rozleglejsze uŻycie walki informacyjnej moŻe przynosiĺ skutki porównywalne z uŻyciem broni jŃdrowej.

[2] E.R. Koch, J. Sperber: *Infomafia. Szpiegostwo komputerowe, handel informacjŃ tajne sğuŻby*. Gdynia 1999, s. 246

Atak informatyczny

Atak informatyczny[3] jest formą walki w sferze przetwarzania danych cyfrowych (*Digital Data Warfare*) i polega na skrytym wprowadzeniu przez atakującego zgubnego kodu komputerowego do określonego systemu komputerowego lub sieci komputerowej dla osiągnięcia pożądanych celów.

Zgubne kody walki informatycznej mogą przybierać głównie formę: wirusów, robaków, bomb logicznych, bomb programowanych czasowo, koni trojańskich lub ich kombinacji odpowiednich do specjalnych funkcji. Różnią się one od hackerskich kodów, jako że służą atakowaniu konkretnych systemów (lub sieci tych systemów) dla osiągnięcia jasno określonych celów w sposób przewidziany przez atakującego.

Atakującym może tu być zarówno militarna jak i państwowa, ale także i terrorystyczna organizacja czy też międzynarodowa lub prywatna korporacja a nawet pojedyncza osoba posiadająca wiedzę i zasoby niezbędne do sporządzenia i zainstalowania takiego kodu. D.L. Pipkin pisząc o typach intruzów[4] wyróżnia:

- intruzów zewnętrznych;
- hakerów;
- konkurentów;
- intruzów wewnętrznych;
- niezadowolonych pracowników;
- pracowników kontraktowych i okresowych;
- partnerów w biznesie;
- intruzów profesjonalnych;
- hakerów do wynajęcia;
- przestępczość zorganizowaną;
- aktywistów;
- terrorystów.

Atakujący w sferze przetwarzania danych cyfrowych może oddziaływać na atakowany system przy zastosowaniu jednego z następujących sposobów:

1) Wzbranianie – uniemożliwianie atakowanemu obiektowi użycia systemu komputerowego, jego danych lub informacji, której ten system dostarcza. Może to być osiągane przez użycie zgubnego kodu, który spowoduje awarię sprzętu lub destrukcję programów lub danych.
2) Degradacja – degradowanie atakowanego systemu do stanu, w którym nie może on efektywnie wykonywać swojego zadania. Może to być osiągnięte przez zmuszenie przeciwnika do wycofania z użycia zainfekowanej jednostki z sieci przez zagrożenie rozprzestrzeniania infekcji lub przez wprowadzenie robaka, który przeciąża możliwości przetwarzania danych tego systemu.
3) Dezinformacja (mylenie) – wprowadzenie w błąd atakowanego systemu i spowodowanie generowania fałszywej informacji lub potraktowanie fałszywych danych za prawdziwe.

---

[3] L.G. Jr. Downs: *Digital Data Warfare: Using Malicious Computer Code as a Weapon. A Research Report Submitted to the Faculty in Fulfillment of the Curriculum Requirement. Air War College Air University*, Maxwell AFB 1995

[4] Patrz: D.L. Papkin: *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*. Warszawa 2002, s. 223-236

4) Eksploatacja ï uÕycie Ôrodków za pomocÑ, których nastñpuje transmisja informacji z atakowanego systemu do atakujÑcego.

Przy stosowaniu tej formy walki w grñ wchodziÍ moÕe szeroka gama celów. JednakÕe w kaÕdym przypadku rozwaÕyÍ naleÕy potrzeby i techniczne moÕliwoÔci zanim opracuje siñ plan zastosowania walki w sferze przetwarzania danych cyfrowych.

Fazy ataku w sferze przetwarzania danych cyfrowych

Atak w sferze przetwarzania danych cyfrowych skãada siñ z serii kolejnych kroków nastñpujÑcych w okreÔlonej wczeÔniej kolejnoÔci. W ramach tego ataku uÕyte mogÑ byÍ wirusy, robaki, bomby logiczne, bomby programowane czasowo, konie trojaÒskie lub ich odpowiednie kombinacje. Wszystkie one sÑ formÑ zgubnych kodów. Atak w sferze przetwarzania danych cyfrowych skãada siñ z nastñpujÑcych faz:

- penetracji ï wówczas to nastñpuje wprowadzenie zgubnego kodu do atakowanego systemu zwykle przez jego najsãabiej zabezpieczone pogÑczenie;
- rozwoju ï wtedy to zgubny kod przenika przez system w kierunku zaplanowanego obiektu ataku;
- uÔpienia ï w tym okresie wprowadzony kod pozostaje w ukryciu do czasu jego aktywacji;
- realizacji ï wówczas to nastñpuje aktywacja kodu i wykonanie przez niego zaplanowanego dziaãania;
- zakoÒczenia ï po wykonaniu swego zadania zgubny kod powraca do stanu uÔpienia i gotowoÔci do wykonania kolejnego ataku lub ulega samolikwidacji w celu zatarcia Ôladów swojego dziaãania.

Penetracja

Wprowadzenie kodu komputerowego do atakowanego systemu jest prawdopodobnie najtrudniejszÑ fazÑ ataku. ZwiÑzane sÑ z tym dwa aspekty, które naleÕy rozwaÕyÍ. SÑ nimi miejsce oraz metoda penetracji. Zgubny kod moÕe byÍ wprowadzony do atakowanego systemu bezpoÔrednio (penetracja bezpoÔrednia) lub moÕe przeniknÑÍ do urzÑdzeÒ peryferyjnych lub sãabiej zabezpieczonych wñzgobÑcznoÔci, a nastñpnie przemieÔciÍ siñ do docelowego miejsca (penetracja poÔrednia). Czñsto atakowany system jest dobrze zabezpieczony i odporny na bezpoÔrednie ataki. Dlatego teÕ atakujÑcy zmuszany jest do szukania sposobów penetracji poÔredniej. WyróÕnia siñ przenikanie czogobowe (front-door coupling) i tylne.

Przenikanie czogobowe okreÔlane jest jako wnikanie do obiektu ataku przy wykorzystaniu typowych dla danego urzÑdzenia noÔników. Przykãadem moÕe tu byÍ wgrÑÕenie dyskietki do czytnika dyskietek lub skierowanie fal radiowych na antenñ odbiorczÑ. W czasie uÕycia tej metody penetracji zgubny kod przyjmuje zwykle formñ ukrytego w legalnym programie konia trojaÒskiego.

Przenikanie tylne to uÕycie wszelkich moÕliwych technik, które umoÕliwiajÑ przenikniñcie zgubnego kodu przez media nietypowe dla danego systemu. Przenikanie takie moÕe na przykãad nastÑpiÍ przez sieÍ energetycznego zasilania, urzÑdzenia stabilizujÑce zasilanie, propagacjñ fal radiowych wysokiej czñstotliwoÔci lub starannie kontrolowane impulsy elektromagnetyczne. MoÕliwe jest takÕe umieszczanie ukrytych zgubnych kodów w podzespoãach dostarczanych przeciwnikowi urzÑdzeÒ lub w innych przypadkach umoÕliwiajÑcych ich blokadñ, gdy dostanÑ siñ

w niepowoğane rňce. Program w formie konia trojaŒskiego moŽe byÍ uaktywniony przez zakodowany sygnağ radiowy. Szczególnie ciekawŃ metodŃ jest zaprojektowanie zainfekowanego procesora i umoŽliwienie jego skopiowania po to by umieszczony zostağ w systemie przeciwnika.

Faza rozwoju

Z chwilŃ przenikniňcia zğoŠliwego kodu do systemu, kod ten musi dotrzeÍ do planowanego miejsca ataku. Obiektem ataku mogŃ byÍ wszystkie komponenty systemu lub konkretny zestaw danych. Atak moŽe byÍ dokonywany zarówno na oprogramowanie, jak i na podzespoğy (hardware). MoŽe to byÍ zarówno serwer przechowujŃcy najwaŽniejsze dane, jak i wňzeğ gŃczności. NajwaŽniejszŃ sprawŃ jest tu szczególnie staranne uŠwiadomienie sobie celu ataku i w odniesieniu do tego sprecyzowanie atakowanego obiektu. JeŠli zğoŠliwy kod zostağ wprowadzony bezpoŠrednio do systemu musi zlokalizowaÍ miejsce przeznaczenia i ukryÍ siň do czasu aktywacji. W wielu sytuacjach bğędem byğoby projektowanie kodu, który miağby atakowaÍ wszystkie komponenty systemu, gdy cel mógğby byÍ osiŃgniňty przez zaatakowanie jednego elementu systemu. ProjektujŃc atak naleŽy braÍ pod uwagň jego skrytoŠÍ i dŃŽyÍ do minimalizacji moŽliwoŠci jego wykrycia. Kod, który siň rozprzestrzenia po cağym systemie jest ğatwiejszy do wykrycia, a jeŠli zostanie wykryty jest mniejsze prawdopodobieŒstwo wykonania przez niego zadania. Chwilowo moŽe byÍ koniecznym badanie komponentów systemu po to by znaleŽÍ wğaŠciwy. JednakŽe z chwilŃ ulokowania siň w miejscu przeznaczenia atakujŃcy kod powinien siň skasowaÍ w miejscach, w których jest niepotrzebny.

Faza uŠpienia

Z chwilŃ dotarcia do miejsca przeznaczenia zğoŠliwy kod moŽe siň zamaskowaÍ i pozostawaÍ w uŠpieniu do czasu wyznaczonego ataku. Niekiedy wyczekiwanie nie jest potrzebne i atak nastňpowağ bňdzie bezpoŠrednio po infekcji. JednakŽe w wiňkszoŠci przypadków czas ataku jest waŽny dla osiŃgniňcia ogólnych celów atakujŃcego. Przykğadowo zgrupowanie militarne dŃŽyÍ bňdzie do sparaliŽowania sieci dowodzenia i kontroli przeciwnika bezpoŠrednio przed swojŃ ofensywŃ. Grupa terrorystyczna moŽe chcieÍ powiŃzaÍ atak z jakimŠ innym zdarzeniem lub chcieÍ wykonaÍ atak o okreŠlonej porze doby. To znacznie utrudnia identyfikacjň czasu i miejsca przenikniňcia kodu do systemu. Co jeszcze waŽniejsze zniszczenia mogŃ zostaÍ dokonane na dğugo przed wykryciem i odpowiedŽ moŽe byÍ niemoŽliwa.

ZğoŠliwy kod ataku w sferze przetwarzania danych cyfrowych moŽe pozostaÍ w systemie w stanie uŠpienia w cağym okresie eksploatacji i nigdy nie byÍ aktywowany. PozostajŃc w uŠpieniu moŽe oczekiwaÍ na aktywujŃcy go sygnağ z zewnŃtrz i jeŽeli zainfekowany system nie zostağ wybrany na obiekt ataku moŽe nie byÍ w ogóle aktywowany. W tym wypadku zğoŠliwy kod moŽe stanowiÍ zabezpieczenie przed moŽliwym zastosowaniem w nieprzyjaznym celu i umoŽliwia odpowiednie przeciwdziağanie. Faza uŠpienia trwa do czasu aktywacji kodu przez odpowiedni mechanizm.

Faza realizacji

Faza realizacji zaczyna siň, gdy odpowiedni mechanizm aktywacji wyprowadza kod ze stanu uŠpienia i uruchamia jego dziağanie. PozostajŃcy w uŠpieniu zğoŠliwy kod moŽe siň uaktywniÍ w okreŠlonym czasie odmierzonym przez zegar systemowy lub uruchomiÍ siň po wykonaniu okreŠlonej iloŠci cykli pracy systemu. Niektóre kody uruchomiŃ siň natychmiast po wnikniňciu do wğaŠciwego komponen-

tu systemu. Inne zostanń uruchomione za pomocń mechanizmów takich, jak transmisja odpowiedniego sygnału radiowego, logowanie siń określonego odpowiednimi danymi użytkownika lub nawet pojawienie siń w systemie odpowiednich danych (na przykład pojawienie siń informacji o prośbie na lńdowanie samolotu z określonym znakiem wywoławczym może uruchomić wirusa w systemie kontroli ruchu lotniczego).

Niektóre kody majńce postać robaków działajń natychmiast i nie potrzebujń mechanizmu aktywacji. Jeżeli celem działania robaka bńdzie paraliż sieci telemonitoringu to bezpośrednio po wniknińciu bńdzie siń on mnożył w systemie do czasu przeładowania możliwości przetwarzania danych i zdegradowania systemu do poziomu pożńdanego przez atakujńcego.

Uruchomiony złośliwy kod wykonuje działanie prowadzńce do osińgnińcia jednego z pożńdanych celów, jakimi sń: wzbranianie, degradacja, dezinformacja i eksploatacja.

Wzbranianie. Złośliwy kod może uniemożliwić atakowanemu obiektowi użycie jego systemu. Może tego dokonać na wiele sposobów. Wśród nich najskuteczniejszym jest zniszczenie danych i zainstalowanych programów wykonawczych. Innym sposobem bńdzie atak na komponenty sprzńtowe systemu. Przykładowo wirus, który może zmienić czństotliwość taktowania zegara głównego procesora może spowodować jego przegranie i samo destrukcjń. Złośliwy kod może również atakować dynamiczne komponenty systemu wprowadzajńc je w przeciążenia, których nie sń w stanie wytrzymać, jak na przykład cińgłe i nieustanne przemieszczanie głowicy dysku magnetycznego komputera do czasu awarii. Wirus może także znieść ograniczenia programowe sterujńce pracń poszczególnych komponentów komputera wprowadzajńc je w strefń przeciążeń niszczńcych.

Degradacja. Wprowadzony do systemu wspomniany już robak może go przeładować i drastycznie obniżyć jego efektywność pracy, co uniemożliwi wykonanie zadania, do którego został przeznaczony. W 1988 roku wprowadzony do Internetu robak zaatakował 6000 komputerów podłńczonych do światowej sieci i blokujńc je powodujńc niemalże paraliż sieci. Wiele firm na całym świecie poniosło już wielkie straty w wyniku takich ataków.

Jeżeli nawet w takiej sytuacji system komputerowy nie został całkowicie sparaliżowany to świadomość czństkowego zainfekowania i obawa przed złymi konsekwencjami rozprzestrzeniania siń infekcji zmusza do wycofania tego systemu z eksploatacji. Może to być wystarczajńcym efektem dla atakujńcego.

Innń formń degradacji sń efekty z obszaru „psycho-elektroniki". Wprowadzony do systemu wirus może powodować szkodliwń dla operatorów pracń monitorów, wskaźników radarowych i innych urzńdzeń zobrazowania informacji wywoływajńc bóle głowy i inne negatywne reakcje organizmu.

Dezinformacja. Jednń z form dezinformacji jest umożliwienie normalnego funkcjonowania systemu przy jednoczesnym zmuszeniu go do traktowania wprowadzanych fałszywych danych jako prawdziwe. Niewielka modyfikacja programy sprawdzania ważności kart kredytowych może być powodem wielkich strat. Wprowadzenie fałszywych danych w sferze militarnej może mieć jeszcze większe konsekwencje. Możliwość imitowania wykrytych obiektów w przestrzeni powietrznej w sytuacji, gdy one nie istniejń i odwrotnie ignorowania rzeczywistych środków napadu powietrznego może umożliwić uzyskanie zaskoczenia, co jest wartością nie do przecenienia.

Niezbędna do uzyskania pożądanego efektu modyfikacja programu nie musi być wielka. Prosta zmiana znaku ‘<’ na ‘>’ może wystarczyć dla osiągnięcia celu atakującego. Przykładowo system kontroli ognia, którego program zostałzmodyfikowany przez wirusa tak by zamiast ignorować nadlatujące obiekty o prędkości mniejszej niż dźwiękowa ignorowałobiekty o prędkości większej niż dźwiękowa zamiast atakować nadlatujące pociski rakietowe zwalczałbędzie własne samoloty poddźwiękowe, które powinny być bezpieczne.

Eksploatacja. Eksploatacja dotyczy uzyskiwania konkretnej informacji z atakowanego systemu. Zakres, w jakim może to być osiągnięte zależy od stopnia dostępu atakującego do atakowanego systemu. Jeżeli atakujący ma jakikolwiek dostęp do atakowanego systemu stosowany złośliwy kod może gromadzić informację w wielu miejscach dostępnych dla atakującego. Jeżeli atakujący pozostaje na zewnątrz systemu dostęp jest trudniejszy, lecz nie niemożliwy. W tym celu wykorzystane mogą być różne skryte kanały komunikowania do przekazania sygnałów, które użyte w odpowiednie sekwencje mogą nieść wiadomość dla kogoś, kto wie jak ją odczytać. Przykładowo, jeżeli istnieją zasady postępowania zapobiegające transmisji sygnałów z systemu na zewnątrz atakujący może zastosować kombinację pogwałceń zasad i braku tych pogwałceń. Kombinacja ta jak kod Morse’a może zawierać wiadomość. Atakujący potrzebuje jedynie odwrócić działanie zespołu logowania by uzyskać mechanizm informowania. Systemy komputerowe stają się coraz bardziej zintegrowane za pomocą coraz rozleglejszych sieci, dlatego też stają się one coraz bardziej podatne na ataki w ramach walki w sferze przetwarzania danych cyfrowych.

Faza zakończenia

Zależnie od ogólnych celów atakującego użyty kod może być zaprogramowany na całkowite samozniszczenie po wykonaniu zadania. Postępując w ten sposób osiąga się następujące korzyści:

- jeżeli atak nie był oczywistym dla atakowanego obiektu, co może mieć miejsce w wypadku skrytych działań, usunięcie atakującego kodu może uniemożliwić zidentyfikowanie prawdziwej przyczyny awarii lub przesłanki tego, że doszło do ujawnienia tajnej informacji;
- w przypadku, gdy obiekt ataku jest świadomy zaistnienia tego ataku, jednak nie rozpoznaje natury tego ataku, usunięcie atakującego kodu może utrudnić ocenę szkód i zakresu ataku;
- nawet, gdy obiekt ataku jest całkowicie świadomy, co do formy i skali ataku to usunięcie atakującego kodu znacznie utrudni zidentyfikowanie sposobu penetracji i podjęcie właściwych przedsięwzięć zapobiegawczych przeciwko przyszłym atakom;
- usunięcie atakującego kodu czyni także znacznie trudniejszym dla atakowanego ustalenie źródła ataku i identyfikacji napastnika; ustalenie tych danych może prowadzić do poważnych konsekwencji prawnych lub sankcji militarnych w stosunku do atakującego.

W niektórych, szczególnych przypadkach atakujący może chcieć ponownie wprowadzić atakujący kod w stan uśpienia i gotowości do wykonania kolejnego ataku. Przykładowo złośliwy kod zainstalowany w eksportowanym zestawie przeciwlotniczym może spowodować gwałtowny skręt w prawo i ominięcie celu w sytuacji, gdy transmitowany jest pewien ustalony wcześniej sygnał. Dla zaatakowanego zestawu przeciwlotniczego wyglądałto może na przypadkową awarię i może on

być dalej utrzymywany w eksploatacji gdyż prawdziwy powód nie zostanie odkryty. Wszystkie, bowiem testy i przypadki użycia przeciwko samolotom nie wysyłających skrytych sygnałów wypadają pomyślnie. Jednakże atakujący będzie wiedziała że jego samoloty emitujące odpowiednie sygnały pozostaną bezpieczne przed atakiem dostarczonym zainfekowanym zestawem przeciwlotniczym.

Pozostawienie atakującego kodu w stanie uśpienia jest ryzykowne, ponieważ atakujący nie będzie wiedziała czy przy następnym ataku zostanie on wykryty przy następnej aktywacji. Atakowany może przygotować przeciwdziałanie lub wykorzystać wykryty kod do wykonania ataku odwetowego. Dlatego też znacznie rozsądniejszym podejściem jest usuwanie atakującego kodu po wykonaniu przez niego zadania. Jedynie, gdy penetracja jest skrajnie trudna a ryzyko przeciwdziałania mniej ważne można tę opcję rozważać.

Metody przeprowadzania ataków na sieci

Hakerzy najczęściej włamują się do sieci w celu uzyskania dostępu na poziomie administracyjnym i przejęcia kontroli nad komputerem, serwerem czy elementem wyposażenia sieciowego.

Tylne wejścia (*backdoors*)

„Tylne wejścia" (*backdoors*) to środek[5] lub technika stosowana przez hakera do uzyskania dostępu do systemu sieciowego, utrzymania go i korzystania z niego. W szerszym znaczeniu określa się w ten sposób luki w systemie zabezpieczeń. Dla hakera istotne jest zachowanie możliwości dostępu do raz zdobytego systemu, również w obliczu wprowadzania nowych zapór, filtrów, serwerów proxy czy uaktualnień.

„Tylne wejścia" dzielą się na dwie kategorie: aktywne i pasywne. Aktywne mogą być wykorzystywane w dowolnym czasie. „Tylnego wejścia" pasywnego użyć można dopiero po pewnym czasie lub po wystąpieniu określonego zdarzenia systemowego. Wybór pomiędzy nimi uzależniony powinien być od architektury bram zabezpieczających sieć.

Przeciążanie (*flooding*)

W systemie, którego interfejs sieciowy powiązany został z protokołem TCP/IP i który jest połączony z Internetem łączem stałym lub telefonicznym, części lub wszystkie usługi mogą stać się niedostępne. Pojawić się może wówczas komunikat w stylu: „Połączenie utracone lub zerowane przez serwer".

Komunikat taki jest często symptomem ataku przeciążeniowego (*flooding*). Przedstawimy teraz atak SYN, gdzie haker ukierunkowuje się na komputer lub wybraną usługę TCP, takĄ jak na przykład usługa HTTP (port 80). Atak wymaga protokołu TCP, stosowanego przez wszystkie komputery w Internecie.

Współczesne techniki przeciążania uwzględniają również zacieranie śladów ataku.

Zacieranie śladów (*log bashing*)

Przykładem zacierania śladów jest modyfikowanie dziennika nadzoru (*audit trail editing*) przy użyciu programów czyszczących, określane najczęściej nazwami *log bashers* lub *wipers*, oraz modyfikowania śladów (*track-editing*), takich jak tzw. *anti-keyloggers*.

[5] J. Chirillo: *Hack Wars. Na tropie hakerów*. Gliwice 2001

Hakerzy modyfikujĄ dziennik nadzoru, aby ukryĆ Ślady swoich operacji dostĆpu do systemu. PoniewaŻ wiĆkszoŚĆ metod pozwala caŁkowicie usunĄĆ wszelkie pozostaŁoŚci po bezprawnych czynnoŚciach w obcym systemie, zapoznanie z tymi metodami jest istotnym czynnikiem uŁatwiajĄcym ich póŹniejsze wykrycie.

W zwykŁych okolicznoŚciach róŻne osoby mogĄ samodzielnie wprowadziĆ uŻycie programów rejestrujĄcych. MogĄ one monitorowaĆ na przykŁad, jak komputer wykorzystujĄ dzieci i co przeglĄdajĄ w Internecie. MogĄ równieŻ pomóc w ustaleniu, kto korzysta z komputera pod nieobecnoŚĆ wŁaŚciciela. Rejestrowane sĄ wówczas wciĆniĘcia klawiszy i aktywnoŚĆ dysku twardego. Tak samo wykorzystujĄ programy tego typu, nazywane *keyloggers*, hakerzy. Ich celem jednak jest przechwycenie haseŁ i numerów kart kredytowych.

Log bashing pozwala usunĄĆ zarejestrowane informacje o wciĆniĘciach klawiszy, korzystajĄc z prostych procedur usuwajĄcych lub wyŁĄczajĄcych korzystanie z okreŚlonych plików. Efektem jest ominiĘcie mechanizmów monitorowania systemu.

Bomby pocztowe, spam i podrabianie korespondencji

Bomby pocztowe to wiadomoŚci *email*, których celem jest uniemoŻliwienie funkcjonowania skrzynki pocztowej odbiorcy. MogĄ one przyjmowaĆ postaĆ pojedynczej wiadomoŚci z duŻymi zaŁĄcznikami lub tysiĘcy wiadomoŚci, które przeciĄŻajĄ skrzynkĘ lub serwer. IstniejĄ programy do generowania duŻych iloŚci wiadomoŚci i przesyŁania ich do wskazanej skrzynki pocztowej ð efektem jest awaria serwera poczty lub uniemoŻliwienie korzystania z przepeŁnionej skrzynki.

Wysyłanie tzw. spamu lub spamowanie (*spamming*) to kolejna forma naduŻycia. Jego celem jest dostarczenie wiadomoŚci elektronicznych do osób, którego nie ŻyczĄ sobie pewnego rodzaju korespondencji. Najbardziej typowym przykŁadem jest rozsyŁanie reklam. W Internecie moŻna wykupiĆ tego rodzaju usŁugi od firm dysponujĄcych setkami tysiĘcy adresów zasypywanych spamem. Sytuacja taka utrzymuje siĘ i do momentu, gdy sprzedawane produkty pozostajĄ legalne, nie moŻna jej w zasadzie zapobiec.

Kolejnym szeroko rozpowszechnionym zjawiskiem jest podrabianie wiadomoŚci pocztowych (*email fraud, email spoofing*), polegajĄce na wprowadzeniu w pole *From* (Od) wiadomoŚci faŁszywego adresu e-mail i rozesŁaniu w duŻej iloŚci egzemplarzy do róŻnych odbiorców z instrukcjĄ nakazujĄcĄ przesŁanie odpowiedzi. Wszystkie odpowiedzi trafiajĄ wówczas do skrzynki ofiary. Na tego typu działania zwracajĄ szczególnĄ uwagĘ usŁugodawcy Internetu, ponieważ powodowały one niejednokrotnie zakŁócenie pracy całych sieci.

Autorzy programów typu *email bombers* zapewniają często, że korzystanie z ich narzĘdzi gwarantuje anonimowoŚĆ prawdziwego nadawcy. Łatwo jednak zorientujemy siĘ, Że nie jest to takie proste. Istotnym uzupeŁnieniem pakietu do rozsyŁania bomb pocztowych jest lista serwerów SMTP, które (jak dotĄd) nie rejestrujĄ adresów IP. WŁaŚnie dziĘki nim funkcjonuje wiĘkszoŚĆ programów rozsyŁających Śmiechcianków pocztĘ, dostĘpnych dla platformy Windows.

Łamanie haseŁ (*password cracking*)

Zapomniałeś hasła? Twoje hasła uległy zniszczeniu? Musisz dostaĆ siĘ do plików czy systemu zabezpieczonego hasŁem? Zwolniony pracownik nie usunĄŁ zabezpieczeŃ ze swoich plików? A moŻe po prostu chcesz siĘ dowiedzieĆ, w jaki sposób haker moŻe uzyskaĆ dostĘp do Twojej sieci, systemu czy plików?

W typowym systemie komputerowym kaŻdy uŻytkownik korzysta z jednego, zawsze tego samego hasła tak długo, aŻ sam, lub administrator, zdecyduje o jego zmianie. Po wprowadzeniu przez uŻytkownika mechanizmy uwierzytelniania komputera szyfrujĄ hasło, zamieniajĄ na ciĄg znaków i porównujĄ z długĄ listĄ, przechowywanĄ najczęŚciej w jednym z plików systemu. Odnalezienie dopasowania ciĄgu hasła i nazwy logowania warunkuje dostęp do systemu. Takie rozwiĄzanie powoduje, Że często podstawowym celem ataku hakera jest włamanie plik haseł. W zaleŻnoŚci od konfiguracji uzyskanie pewnego poziomu dostępu umoŻliwia utworzenie kopii takiego pliku. Wówczas pozostaje juŻ tylko uruchomienie odpowiedniego programu do łamania haseł, który przetworzy zaszyfrowane ciĄgi znaków na właŚciwe hasła.

Podstawą działania programów do łamania haseł jest szyfrowanie, kolejno, długiej listy róŻnorodnych ciĄgów znakowych, na przykład całego słownika, i porównywanie ciĄgów wynikowych z odnalezionymi w pliku. Znalezienie tylko jednego dopasowania umoŻliwia uzyskanie dostępu. Atak taki nie wymaga duŻych umiejętnoŚci, a w Internecie dostępnych jest wiele pomocnych programów. CzęŚć systemów chroni się przed tego rodzaju włamaniami, zabezpieczajĄc mocno plik haseł.

Zdalne przejęcie kontroli

Wraz z rozwojem Internetu i współpracy sieciowej pojawia się coraz więcej programów, przy których nawet najgroŹniejszy wirus wydaje się niemal nieszkodliwy. Celem takich programów jest umoŻliwienie osobie nieuprawnionej przejęcia kontroli nad serwerem sieciowym lub osobistĄ stacjĄ roboczĄ. Po zainstalowaniu takiego demona haker moŻe przejmowaĆ hasła, korzystaĆ z dostępu do kont (równieŻ pocztowych), modyfikowaĆ dokumenty, udostępniaĆ dyski, rejestrowaĆ wciŚnięcia klawiszy, zawartoŚć ekranu, a nawet wykorzystaĆ mikrofon komputera do podsłuchiwania rozmów.

Aby w pełni uŚwiadomić sobie znaczenie takiego przejęcia kontroli, należy wiedzieć, jakie moŻliwoŚci uzyskuje haker: moŻe dysponowaĆ naszymi kontami online, przeglĄdaĆ prywatnĄ korespondencję, rozsyłaĆ spam lub szkodzĄce odbiorcom wiadomoŚci pocztowe, a nawet podglĄdaĆ zawartoŚć naszego ekranu. Wyjątkowo niebezpieczne odmiany tego rodzaju oprogramowania oferujĄ funkcje czyszczenia całych dysków albo wręcz doprowadzania do uszkodzenia monitora. Znane sĄ sytuacje, gdy ofiara tego rodzaju ataku spokojnie uŻywała swojego komputera do własnej pracy w czasie, gdy ten był wykorzystywany do popełniania przestępstwa. Trudno w takiej sytuacji udowodniĆ własnĄ niewinnoŚć, zwłaszcza Że po popełnieniu powaŻnego przestępstwa, haker dba szczególnie dokładnie o usunięcie Śladów swojej działalnoŚci (stosujĄc przedstawione wcześniej techniki zacierania Śladów).

Programy służĄce do zdalnego przejmowania kontroli określa się nazwĄ demonów zdalnego sterowania (remote-control daemons). SĄ one najczęŚciej rozprowadzane jako programy-Żarty, gry, obrazki, wygaszacze ekranu, Życzenia Świąteczne albo pomocne narzędzia. Jako najbardziej rozpowszechnione należy wymienić trzy: Netbus, Back Orifice i SubSeven. Ich liczba jest jednak znacznie większa.

Pakiety antywirusowe czy wyszukujĄce konie trojaŃskie, jak dotĄd często nie dotrzymujĄ kroku szybkiemu powstawaniu coraz to nowych kompilacji. Co gorsza, dystrybucja i korzystanie z tych programów nie wymaga duŻych umiejętnoŚci.

Większość z nich wyposażona zostaną w programy klienckie z interfejsem GUI i bogatym menu. Dość aktualnym przykładem jest rozpowszechniana przez hakerów jako załącznik do emaliowego spamu mutacja popularnego demona zdalnego sterowania BackDoor-G, nazwana BACK-AGN. Adres nadawcy jest zazwyczaj podrobiony – oznacza to, że można spodziewać się zupełnie dowolnej, rzekomej tożsamości nadawcy. Gdy użytkownik uruchamia załącznik, program instaluje się w systemie. BACK-AGN to pracujący w systemie Windows 9x internetowy koń trojański, otwierający w systemie lukę umożliwiającą praktycznie nieograniczony dostęp do systemu.

Niepokojącym zjawiskiem jest to, że wciąż dostępnych jest wiele wersji programów, takich jak BackDoor-G, których działanie pozostaje niemal niewykrywalne dla przeciętnego użytkownika, mimo że pliki, które instalują w folderach Windows i Windows System są dość charakterystyczne. Obie wymienione tu mutacje korzystają z pliku BackDoor-G.,ldr, umieszczanego w folderze Windows. Jest to program ładujący z tego samego folderu właściwy moduł serwera, BackDoor-G.srv. Odbiera on i wykonuje przesyłane Internetem polecenia. Dodatkowo wykorzystywana jest biblioteka DLL o nazwie WATCHING.DLL lub LMDRK_32.DLL, przechowywana w folderze Windows\ System. Program prowadzi nasłuch w oczekiwaniu połączeń realizowanych przez klienta, którego głównym plikiem jest BackDoor-G.dll. Dalsze elementy to program klienta, BackDoor-G.cli, i program konfiguracyjny, BackDoor-G.cfg.

Monitorowanie komunikacji (*sniffing*)

Sniffery lub „podsłuchiwacze sieciowe" to programy, które pasywnie przechwytują i kopiują pakiety komunikacji sieciowej systemu, serwera, routera lub bramy. Pożytecznym zastosowaniem tego rodzaju oprogramowania jest monitorowanie i rozwiązywanie problemów z siecią. Używane przez hakerów *sniffery* „cichego" stanowią poważne zagrożenie sieci, głównie ze względu na małą wykrywalność i możliwość przeprowadzania autoinstalacji w niemal dowolnym systemie.

Większość odmian podsłuchiwaczy sieciowych przewiduje możliwość wykrywania i wybierania do kopiowania danych, które zawierają na przykład nazwę logowania i hasło. Najbardziej podatne na przechwycenie są dane logowania zdalnego, telefonicznego, połączeń wirtualnych, ekstranetów itp., ze względu na ilość pośredniczących w komunikacji bram. Wyobraźmy sobie tysiące nazw logowania i haseł, które można przechwycić, lokując nieautoryzowany szperacz sieciowy na jednej z istotniejszych bram w Internecie.

Jak już wspomniano, podsłuchiwacz sieciowy może być nieocenioną pomocą w diagnozowaniu problemów z siecią.

Podstawą działania *sniffera* jest tworzenie kopii danych odbieranych i wysyłanych przez interfejs sieciowy lub modem. Znaleźć można wśród nich najróżniejsze informacje. Narzędzia te znakomicie pomagają w monitorowaniu i testowaniu komunikacji jako sługi do odczytywania pakietów sieciowych na różnym poziomie warstw OSI. Jednak i one mogą posłużyć mniej wzniosłym celom. Monitor sieciowy może umożliwić szybkie przechwycenie nazwy i hasła, skąd już tylko krok do rozszerzenia włamania na dalsze komputery.

Najpopularniejsze szperacze automatycznie dekodują i tłumaczą istotne informacje. Przykładami mogą być SpyNet, EtherSpy i Analyzerfor PC-DOS. Jeden z najlepszych internetowych szperaczy, SpyNet (CaptureNet) dla Windows 95/98/NT, przechwytuje wszelkiego rodzaju pakiety sieciowe. Jego dodatkowy

moduğ PeepNet, przeprowadza interpretacjń i próbń rekonstrukcji sesji. Program moŨe rejestrowaĺ operacje w sieci, trwale znakujŃc godzinń ich przeprowadzenia (co ma znaczenie jako dowód przestŕpstwa). Liczbń przechwytywanych pakietów moŨna ograniczyĺ filtrami, rozpoznawane sŃ podstawowe protokoğy sieci Ethernet, program moŨe pracowaĺ równieŨ na ğŃczach telefonicznych.

Sniffery o podobnych moŨliwoŝciach, pracujŃce w systemach UNIK i Macintosh, to przede wszystkim *EtherReal* i *Spy.c.*

Podrabianie IP i DNS (*spoofing*)

Podrabianie IP i DNS stosowane jest gğównie w celu przejńcia toŨsamoŝci stacji zaufanej, aby oszukaĺ zabezpieczenia i uzyskaĺ moŨliwoŝĺ nieuprawnionej komunikacji ze stacjŃ docelowŃ. Gdy podrabiany jest adres IP, haker najpierw wyğŃcza stacjń zaufanŃ z komunikacji i dopiero w drugim kroku przyjmuje jej toŨsamoŝĺ. Stacja docelowa kontynuuje wówczas komunikacjń ze stacjŃ nieuprawnionŃ. Zapoznanie z mechanizmem podrabiania IP wymaga dobrej znajomoŝci protokoğów IP i TCP oraz procedury wymiany potwierdzeŒ (*handshaking*). Pisaliŝmy o nich we wczeŝniejszych rozdziağach.

Podrobienie adresu IP wymaga znajomoŝci odpowiedniego adresu zaufanej stacji oraz zmodyfikowania nagğówków wysyğanych przez niŃ pakietów, tak aby nie miağy one postaci pakietów uprawnionych do komunikacji. Jak juŨ powiedzieliŝmy, podszycie siń pod stacjń zaufanŃ wymaga wyğŃczenia jej z komunikacji. Podrobienie adresu Ğródğowego jest moŨliwe dziğki temu, Ũe wińkszoŝĺ oprogramowania komunikacji międzysieciowej nie kontroluje tego pola w przekazywanych pakietach. Aby wğŃczyĺ siń do komunikacji, haker musi jednak przewidzieĺ przesyğane przez stacjń docelowŃ sekwencje TCP.

Najbardziej typowe techniki podrabiania IP obejmujŃ przechwytywanie i modyfikowanie przesyğanych między dwoma stacjami pakietów, przekierowywanie trasy lub (i) pakietów ze stacji docelowej do atakujŃcej, przewidywanie odpowiedzi stacji docelowej oraz róŨne odmiany nńkania przeciŃŨeniowego TCP SYN.

W typowym przypadku po wğamaniu do systemu haker kompiluje Ğylne wejŝcie, które umoŨliwi kolejne wğamania i przejmowanie kontroli nad systemem. Teoretycznie funkcjń takŃ pełniĺ moŨe fağszowanie adresu IP ð wykorzystywane usğugi opierajŃ uwierzytelnienie wyğŃcznie na adresie sieciowym.

Wiele wysiğku wğoŨono ostatnio w badanie przypadków podszywania siń pod usğugń DNS. ZastŃpienie buforujŃcego serwera DNS umoŨliwia hakerowi ğŃczenie uŨytkowników z innŃ lokalizacjŃ niŨ zamierzona.

KorzystajŃc z tej postaci podszywania siń, haker wymusza na podrzędnym serwerze DNS przesğanie pewnego ŨŃdania do serwera nadrzędnego, po czym podrabia odpowiedĹ. Mechanizm taki moŨe funkcjonowaĺ dziğki stosowaniu przez wińkszoŝĺ demonów DNS zapytaŒ Ğekurencyjnych. UmoŨliwiajŃ one wysyğanie ŨŃdania do dowolnego serwera DNS w sieci. W celu jego zrealizowania serwer wysyğa odpowiednie zapytania do pewnych, trwale okreŝlonych serwerów centralnych. Haker wykorzystuje wówczas moŨliwoŝĺ przewidzenia, jakie ŨŃdanie będzie przesyğane, i podsuwa przygotowanŃ odpowiedĹ. W trakcie dobrze przygotowanego ataku odpowiedĹ hakera odebrana zostaje przed odpowiedziŃ wğaŝciwego serwera. Dalej z pomocŃ przychodzi mechanizm buforowania uzyskanych danych przez okreŝlonŃ liczbń godzin. Udana modyfikacja wpisu takiej nazwy jak na przykğad www.yahoo.com kierowaĺ będzie licznych uŨytkowników zmodyfikowanej usğugi DNS do witryny wskazanej przez wğamywacza.

Konie trojaCEskie

Konie trojaCEskie to szkodliwe, tworzNce luki w zabezpieczeniach, programy, które rozpowszechnia siň najczňSciej jako oprogramowanie Ăpodarowaneò uÛytkownikowi komputera - program narzňdziowy, Ûart czy wersja demonstracyjna gry. Jak pisaliÛmy we wczeÛniejszych rozdziaģach, mechanizm konia trojaCEskiego wykorzystuje siň czňsto do zainstalowania Ătylnego wejÛciaò do systemu. RosnNca obecnie liczba ĂzaraÛeCE tego rodzaju jest wynikiem prostej, technologicznej konieczno Ûci korzystania z portów. Usģugi na portach o niÛszych numerach sģuÛNczňsto do przechwytywania haseģ, które sN nastňpnie przesyģane hakerowi pocztNelektroniczn lub udostňpniane w katalogach FTP. Porty dalsze obsģugujN przede wszystkim programy zdalnego dostňpu, umoÛliwiajNce komunikacjň z komputerem przez Internet, sieN, kanaģ VPN lub poģNczenie telefoniczne.

Istotnym problemem z koniami trojaCEskimi jest lawinowo rosnNca liczba ich mutacji. W roku 1997 powstaģo ich 7, w kolejnym - 81, w 1999 - 178 i liczba ta podwajaģa siň w latach nastňpnych. Nie istnieje program antywirusowy czy do usuwania koni trojaCEskich, który wykrywa wszystkie jeszcze niezbadane mutacje. Programy majNce rzekomo chroniN system, wykrywajN jedynie uģamek groÛNcych komputerom niebezpieczeCEstw. Jeszcze bardziej niepokojNce jest to, Ûe wciNÛ w Internecie dostňpne sN kody Ħródģowe, umoÛliwiajNcy tworzenie coraz nowszych wersji szkodliwego oprogramowania.

Infekcje wirusowe

Termin Ăwirusò bňdzie oznaczaģ dla nas program komputerowy, tworzNcy kopie samego siebie przy uÛyciu programu ģ ównego. Oznacza to, Ûe wirus wymaga takiego programu ģ ównego. Poza wiňc plikami uruchamialnymi zaraÛony moÛe byN, i czňsto jest, moduģ obsģugi dysku twardego. Wraz z uruchomieniem zaraÛonego oprogramowania rozpoczyna siň wykonywanie i replikowanie kodu wirusa.

Wirusy rozprowadzane przez hakerów sģuÛNzazwyczaj do rozprowadzania pewnego ģadunku (*payload*). Ma on uaktywniN siň i wprowadziN zniszczenia w zaraÛonym systemie dopiero po upģywie pewnego okresu czasu. ĂZniszczeniaò oznaczaN mogN uszkodzenie plików, usuniňcie danych, a nawet wszystkich plików z twardego dysku. Wirusy najczňSciej dystrybuowane sN jako zaģNczniki pocztowe, ukryte Ădodatkiò do pirackich kopii oprogramowania albo razem z zaraÛonymi dyskietkami.

DestrukcyjnoSN wirusa Ûci Ûle zaleÛy od jego rodzaju. Do sģynnych Ămajsterszty kówò naleÛy kod inicjujNcy zdarzenie w momencie otwarcia wiadomo Ûci e-mail (niesģawne *I Love You* i *Donald Duck*). Tradycyjnie wyróÛnia siň w cyklu Ûycia wirusa trzy stadia: aktywacji, replikacji i operacji.

1) Aktywacja. Pierwszy moment Ăzģapaniaò wirusa, najczňSciej z zaufanego Ħródģa.
2) Replikacja. W tej fazie wirus zaraÛa, moÛliwie najwiňcej obiektów.
3) Operacja. Moment uaktywnienia Ăģadunkuò wirusa ð pewna data (jak 13 w piNtek czy 1 stycznia) lub zdarzenie (trzeci restart, uruchamiana za pomocN Harmonogramu zadaCE procedura porzNdkowania dysku itp.).

Wirusy klasyfikuje siň odpowiednio wedģug sposobu ich dziaģania. WyróÛniane sN: wirusy ģ ównego sektora rozruchowego (*boot sektor*), wirusy sektora rozruchowego partycji, wirusy plikowe, wirusy polimorficzne, wirusy wieloczňSciowe, wirusy-konie trojaCEskie, robaki i makro wirusy.

Gđ˙wnym problemem, któremu stawiajŃ czođ˙ programy antywirusowe jest szybka utrata ich aktualnoŜci. Hakerzy korzystajŃ z róŨnorodnych Ăzestawów do tworzenia wirusówò (jak The Nuke Randomic Life Generator lub Yirus Creation Lab) i kreujŃ coraz to nowe wcielenia, pozostawiajŃce charakterystyczne tylko dla nich samych Ŝlady. StŃd potrzeba regularnego uaktualniania oprogramowania ochronnego zarówno w zakresie nowych danych, jak i nowych mechanizmów wyszukiwania zaraŨeŒ.

Wardialing

Skanowanie portów w poszukiwaniu istniejŃcych w zabezpieczeniach luk - idea sprawdzenia moŨliwie duŨej liczby Ămasđ˙chujŃcychò i wybrania z nich tych, które mogŃ zostaĺ zaatakowane lub w okreŜlonym celu wykorzystane - nie jest niczym nowym. Na podobnej zasadzie przeprowadzaĺ moŨna przeglŃd kodów systemu telefonicznego. Dziađ˙ania takie okreŜla siň terminem *wardialing* - polegajŃ one na skanowaniu numerów telefonów i rejestrowaniu tych z nich, które odpowiadajŃ sygnađ˙em na moŨliwoŜĺ nawiŃzania pođ˙Ńczenia.

Napisanych zostađ˙o wiele wspaniađ˙ych programów, pozwalajŃcych skanowaĺ cađ˙e zakresy numerów telefonicznych. Dobrymi przykđ˙adami sŃ Toneloc, THC Scan i Phone-Sweep, Ũeby wymieniĺ przynajmniej kilka. Zasada jest prosta: jeŨeli po wybraniu numeru modem dostarcza wstňpnej informacji o uzyskaniu komunikatu CONNECT, numer jest rejestrowany, a komputer rozđ˙Ńcza siň i przechodzi do sprawdzania kolejnego. Jest to wiňc dziađ˙anie bardzo podobne do opisywanego wczeŜniej skanowania EP i portów.

Znacznie programów typu *wardialers* maleje w ostatnich czasach, gdy coraz wiňcej pozostajŃcych w krňgu zainteresowania hakerów komputerów pođ˙Ńczonych jest tylko z sieciŃ lokalnŃ czy Internetem bez moŨliwoŜci dostňpu telefonicznego. Przeprowadzenie ich skanowania wymaga pewnej techniki Ăpođ˙nego przeglŃduò i wysyđ˙ania duŨej iloŜci pakietów róŨnych protokođ˙ów. Jest to w zasadzie jedyna metoda ustalenia, które usđ˙ugi sŃ aktywne.

Programy typu *wardialers* zyskađ˙y popularnoŜĺ w chwili pojawienia siň na rynku niedrogich modemów, umoŨliwiajŃcych telefoniczny dostňp do sieci. Narzňdzie to wybiera kolejno numery z listy telefonów i oczekuje na sygnađ˙ fali noŜnej komunikacji danych. Po utworzeniu listy wykrytych modemów haker moŨe przejĺ do kolejnego etapu - wyszukiwania dostňpnych w nich luk. Dostňpne wspóđ˙czeŜnie oprogramowanie, wyposaŨone w odpowiednie moduđ˙ wtyczek, potrafi zapewniĺ wykrycie nie tylko modemu, ale i niezabezpieczonego hasđ˙em PC z oprogramowaniem zdalnego dostňpu. Automatycznie wysyđ˙ane sŃ teŨ podstawowe skrypty umoŨliwiajŃce wđ˙amanie.

THC-Scan to jedno z najbardziej rozbudowanych narzňdzi tej grupy. Jest równieŨ szeroko stosowane. To w zasadzie nowa wersja programu Toneloc, okreŜlana jako skaner grupy The Hacker's Choice (THC) autorstwa niesđ˙awnego guru van Hausera (prezesa The Hacker's Choice). Ta nowa implementacja wniosđ˙a na arenň *wardialingu* wiele nowych elementów (automatycznie wykrywa prňdkoŜĺ, liczbň bitów danych i stopu oraz ustawienie parzystoŜci modemu docelowego). Narzňdzie moŨe teŨ wykrywaĺ typ systemu operacyjnego. CiekawŃ moŨliwoŜciŃ jest funkcja rozpoznawania kolejnego tonu wybierania - umoŨliwia ona atakujŃcemu wykorzystanie centrali PBX ofiary do przeprowadzania darmowych pođ˙ŃczeŒ.