

German
Data
Security



G Data Whitepaper 2009

Jak złośliwe oprogramowanie trafia do komputera firmowego?

Ralf Benz Müller & Werner Klier
G Data Security Labs



Go safe. Go safer. G Data.

Spis treści

1. Do czego służy złośliwe oprogramowanie	2
2. Jak cyberprzestępcy zarabiają pieniądze na złośliwym oprogramowaniu	3
2.1 Sieci botnet	3
2.2 Spam	3
2.3 Szantaż.....	3
2.4 Kradzież danych.....	4
2.5 Programy typu „adware”	5
3. Jak złośliwe oprogramowanie trafia do komputera?	6
3.1 Wystarczy połączenie	6
3.2 Za pomocą poczty elektronicznej	7
3.3 Poprzez komunikator internetowy	8
3.4 Poprzez portal aukcyjny	9
3.5 Poprzez nośniki danych	9
3.6 Poprzez lokalne sieci.....	9
3.7 Poprzez stronę internetową	10
4. Przebieg typowej fali zarażania komputerów	14
4.1 Przygotowanie infekcji	14
4.2 Realizacja.....	14
4.3 Korzystanie z zainfekowanego komputera.....	15
5. Jak można się chronić	16

1. Do czego służy złośliwe oprogramowanie

Powody tworzenia oraz rozpowszechniania złośliwego oprogramowania znacznie zmieniły się w ostatnich latach. O ile w początkowym okresie istnienia wirusów komputerowych ich tworzeniu towarzyszyła niemal sportowa chęć rywalizacji w formie konfrontacji sił pomiędzy specjalistami z dziedziny informatyki, o tyle dziś najistotniejszym motywem działania atakujących są w pierwszym rzędzie korzyści czysto finansowe.

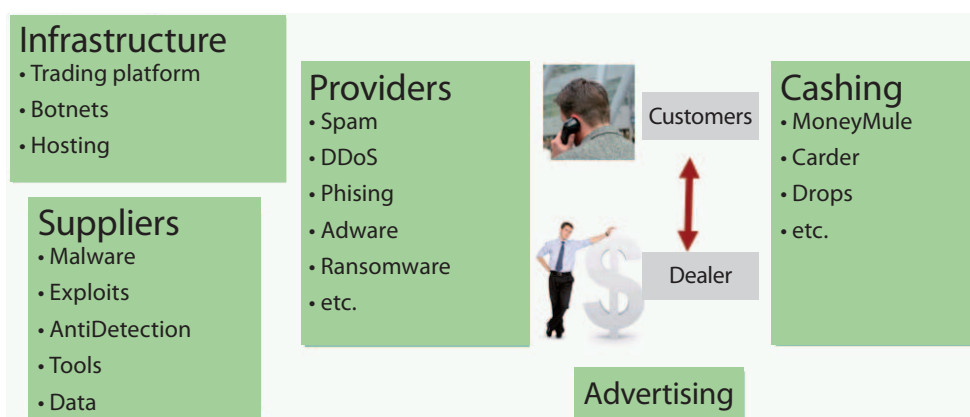
W „elektrycznym podziemiu” powstała prawdziwa szara strefa, w której w ramach dokładnie określonych, bezbłędnie zorganizowanych struktur profesjonalnie tworzy, doskonali oraz rozprowadza się złośliwe oprogramowanie.

Cyberprzestępczość umożliwia rozkwit handlu wszelkimi możliwymi towarami oraz usługami elektronicznymi. Odpowiednie platformy handlowe oferują zarówno dostęp do informacji o nowo odkrytych lukach w zabezpieczeniach, jak i dostosowane do nich złośliwe programy, których autorzy udzielają dziś nawet gwarancji na ich działanie, bezpłatnie dostarczając swoim klientom w okresie jej obowiązywania zmodyfikowane wersje owych programów.

Całe armie zainfekowanych komputerów, które stały się częściami sieci botnet jako tzw. komputery zombie, wynajmowane są na bazie stawek godzinowych lub dziennych do przeprowadzania kampanii spamowych lub celowych ataków na niepożądane strony internetowe lub serwery pocztowe.

Na elektronicznym rynku cyberprzestępczości realizuje się nawet ostatnie ogniwo przestępczego łańcucha tworzenia wartości, czyli zamianę wyłudzonej informacji, takich jak np. dane z kart kredytowych na gotówkę. W tym celu fikcyjne firmy wynajmują nieświadomych niczego użytkowników komputerów w charakterze „agentów finansowych”, którzy udostępniają swoje prywatne konta bankowe dla celów przeprowadzania podejrzanych transakcji.

Tworzenie złośliwego oprogramowania, zaprojektowanego wyłącznie z myślą o rozprzestrzenianiu się, nie jest już od dawna głównym celem. Atakujący coraz częściej interesują się sieciami firmowymi, aby śledzić w nich wszelkie informacje, które można sprzedać lub by wykorzystywać ich infrastrukturę w celach przestępczych.



Rys. 1: Zestawienie poszczególnych działów cyberprzestępczości

Jak pokazuje rys. 1 cyberprzestępczość prezentuje się jako splot ścisłych powiązań wielu najróżniejszych „dziedzin gospodarki”. Za kulisami działają właściwi sprawcy, dostarczający złośliwe oprogramowanie, informacje o nowych lukach w zabezpieczeniach oraz sprzedający wykradzione dane. Handlarze-pośrednicy sprzedają lub wynajmują owe dane „klientom” ze świata przestępczego, zamieniając je ostatecznie na żywą gotówkę za pośrednictwem wynajętych, przeważnie nieświadomych niczego, podstawionych osób (tzw. cashing).

2. Jak cyberprzestępcy zarabiają pieniądze na złośliwym oprogramowaniu

Cyberprzestępcy uzyskują korzyści finansowe wykorzystując najróżniejsze sposoby. Ważną rolę odgrywa w tym wykorzystanie całych armii zainfekowanych komputerów, kontrolowanych przez atakujących. Owe tak zwane sieci botnet mogą wykonać szereg nielegalnych czynności, dzięki którym można zarobić dużo pieniędzy w elektronicznym podziemiu.

2.1 Sieci botnet

Sieci botnet stanowią centralną oś funkcjonowania infrastruktury cyberprzestępczości. Służą one nie tylko do wysyłania spamu czy przeprowadzania ataków Denial of Service (DoS). Komputery zombie wykorzystywane są także jako hosty stron służących do wyłudzenia informacji (tzw. phishing), które zawierają złośliwe oprogramowanie oraz w celu zdobywania informacji o adresach serwerów pocztowych. Nie dziwi zatem, że liczba komputerów należących do sieci botnet znacznie wzrosła do chwili obecnej. Ponieważ sieci botnet podzielone są na segmenty zawierające mniejsze jednostki po kilka tysięcy komputerów zombie, obserwuje się znaczny wzrost ilości owych sieci.

Podczas gdy pierwotnie sterowano niemal wyłącznie przez IRC (Internet Relay Chat – oparty na tekście system pogawędek internetowych), w kolejnej fazie rozwoju pojawiło się wiele sieci botnet, wykorzystujących inne protokoły sterowania. Nowoczesne sieci botnet, takie jak ciesząca się złą sławą sieć botnet Storm, są zbudowane w oparciu o architekturę Peer-to-Peer (P2P). Równie potężna sieć botnet Zunker komunikuje się za pośrednictwem protokołu HTTP. Po zamknięciu podejrzanego dostawcy usług internetowych McColo kilka z sieci botnet utraciło swoje serwery sterujące i nie mogło dłużej działać. Jako kolejne zniknęły sieci botnet Srizbi oraz Storm. Nowsze sieci botnet, takie jak np. Waledac czy Conficker, generują dziś różnorodne możliwości kontaktowania się, aby w każdej chwili móc rozporządzać sieciami. Mechanizmy ukrywania stają się ponadto coraz bardziej wyrafinowane, a częste aktualizacje oraz programy typu Rootkit pozwalają na skuteczne schowanie oprogramowania typu Backdoor. Programy oraz dane dotyczące danego zadania są przesyłane bezpośrednio przed jego zleceniem, a po jego wykonaniu ponownie usuwane.

2.2 Spam

Spam to wielki biznes. Zarabiają na nim nie tylko firmy oferujące reklamowane produkty. Dystrybucja wiadomości e-mail ze spamem odbywa się przeważnie poprzez sieci botnet. Spamer Solomon zapłacił 195 dolarów za rozesłanie dwóch milionów wiadomości e-mail przez okres 14 dni. Z kolei 20 milionów wiadomości e-mail kosztowało 495 dolarów. Handel nieskutecznymi pigułkami, kradzionym oprogramowaniem oraz nic nie wartymi podróbkami opłaca się nawet przy najmniejszym obrocie, przy czym sprzedawane ilości wcale nie są małe. Reklamowane przez spam półlegalne produkty posiadają większą niż się powszechnie przypuszcza klientelę. Należy także stwierdzić, że nie wszyscy handlujący w ten sposób to oszuści, którzy nie dostarczają swoim klientom zapłaconego przez nich towaru. Jeremy Jaynes, w swoim czasie ósmy co do wielkości spamer świata, uzyskiwał miesięczne zarobki w wysokości do 750 000 dolarów.

2.3 Szantaż

Jeśli sklep internetowy danej firmy przynosi duże zyski lub jest uzależniony od szybkiego odpowiadania na wiadomości e-mail, może stać się obiektem szantażu poprzez ataki na te usługi. Połączone komputery zombie funkcjonujące w ramach sieci botnet mogą bombardować daną

stronę internetową lub serwer poczty e-mail bezsensownymi zapytaniami. Masowe zapytania pod adresem serwera powodują takie przeciążenie systemu, że nie jest on w stanie normalnie funkcjonować.

Tego rodzaju rozproszone ataki prowadzące do przeciążenia (ang. Distributed Denial of Service, ataki DDoS) można wykorzystywać nie tylko do szantażowania internetowych bukmacherów czy kasyn. Firmy, których godzinne obroty to kwoty pięcio- czy sześciocyfrowe, a także takie, które muszą dostarczać usługi do serwisów gier online, są dziś gotowe zapłacić okup, który często stanowi jedynie niewielką część utraconego zysku. Przeważnie chodzi o kwoty czterocyfrowe. Istnieje jeszcze bardzo dużo niewiadomych.

Ataki DDoS wykorzystywane są także do celów politycznych. Pod koniec kwietnia i na początku maja 2007 roku zostały sparaliżowane serwery estońskich ministerstw, organów rządowych, banków, gazet oraz przedsiębiorstw. Usunięcie pomnika żołnierzy radzieckich spowodowało niezadowolone ludności rosyjskiej. Gdy do stłumienia demonstracji użyto siły, przeciwnicy sięgnęli po sieci botnet jako środki nacisku politycznego.

Oprócz wymienionego już szantażu poprzez rozproszone ataki przeciążeniowe (DDoS), istnieją inne możliwości wyłudzenia pieniędzy od ofiar. Oprogramowanie ransomware, takie jak np. GPCoder, szyfruje określone pliki na komputerze. Ten, kto chce odzyskać dostęp do treści swoich plików, musi nabyć program dekodujący, który w zależności od danego przypadku kosztuje od 12 do 200 dolarów.

W firmach funkcjonują jednak także inne modele. Koń trojański może przesłać na zarażony komputer pracownika zdjęcia z pornografią dziecięcą, nielegalne oprogramowanie i/lub zabezpieczone przed kopiowaniem pliki audio lub wideo. Atakujący może wówczas szantażować pracownika grożąc mu poinformowaniem jego przełożonych lub też całą firmę sugerując złożenie doniesienia na policji.

2.4 Kradzież danych

Handel wykradzionymi danymi nie ogranicza się jedynie do numerów kart kredytowych oraz bankowych haseł dostępu. Poprzez ataki związane z wyłudzeniem danych, kradzione są obecnie hasła dostępu do portalu eBay, sieci społecznościowych, sklepów internetowych, kont e-mail i in. Przy pomocy programów typu keylogger - czyli złośliwego oprogramowania rejestrującego naciskane klawisze - można wykraść jeszcze więcej danych. Chodzi tu o takie dane jak hasła dostępu do serwerów firmowych czy też do gier typu RPG, o treści (poufnych) wiadomości e-mail i dokumentów, jak również o kody dostępu do innych serwerów, forów czy sieci VPN. Jeśli świeżo wyczyszczony serwer internetowy po upływie kilku dni jest ponownie zainfekowany, przyczyną może być fakt, że administrator systemu utracił swoje hasła dostępu do keyloggera. Pliki systemowe (do logowania) takich keyloggerów dostępne są na nielegalnych forach internetowych w cenie kilkuset euro za dziesiątki gigabajtów. Informacje takie są następnie analizowane przez inne grupy, a następnie odsprzedawane.

Wykradzione dane wykorzystywane są do różnych celów:

- Dane dotyczące kart kredytowych wykorzystywane są do „drukowania” fałszywych kart lub do robienia zakupów w sklepach internetowych.
- Dane bankowe wykorzystuje się do wykonywania nieautoryzowanych przelewów. Ponieważ w przypadku prywatnych kont bankowych istnieje limit kwoty przelewu (od 5000 euro obowiązują specjalne zabezpieczenia), ograniczona jest także wartość łupu. Ograniczeń takich nie posiada wiele rachunków firmowych. Dlatego też grasujący w sieci złodzieje bankowi intensyfikują swoje działania, aby dotrzeć do tego typu kodów dostępu.

- Wykradzione konta na portalu eBay wykorzystuje się po to, by poprzez zakup towaru „wyprac” zrabowane pieniądze.
- Dostęp do sieciowych gier RPG wykorzystywany jest do wykradania wirtualnych pieniędzy oraz narzędzi.
- Dzięki hasłom dostępowym do kont pocztowych oraz sieci społecznościowych w imieniu nieświadomych ofiar rozsyłany jest spam.
- Skradzione dane osobowe wykorzystywane są do tego, by otwierać konta na określonych forach internetowych. Konta te są następnie wykorzystywane do prowadzenia nielegalnej działalności oraz do oszustw.

2.5 Programy typu „adware”

W chwili obecnej programy typu adware rejestrują zachowanie użytkownika w sieci, wyświetlają reklamę przy otwieraniu określonych stron lub manipulują akcjami wyszukiwania. Zapłata za program typu adware następuje albo na podstawie wykonanych kliknięć (w takim wypadku zainfekowane komputery mogą np. manipulować stroną startową wyszukiwarki) albo w oparciu o każdą instalację oprogramowania. Odpowiednie programy partnerskie można znaleźć na odnośnych forach internetowych. Mimo, że w ubiegłym roku nawet duże firmy z branży adware poniosły porażki na polu prawnym, ilość złośliwego oprogramowania związanego z reklamą oraz potencjalnie niepożądanych programów wzrosła w ostatnich dwóch latach ponad pięciokrotnie.

Ciekawostka: W żadnym wypadku nie są to wszystkie modele transakcji prowadzonych przez cyberprzestępców. Należy sobie jednak uświadomić, że cyberprzestępczość to wielki biznes, powodujący każdego roku straty sięgające od kilkudziesięciu do kilkuset miliardów, czyli więcej niż handel narkotykami. Wymienione obszary transakcji prezentują główne punkty zainteresowania przestępców rozpowszechniających złośliwe programy. Ich najważniejszym instrumentem są sieci botnet. Stanowią one podstawowe narzędzie do rozsyłania spamu oraz ataków związanych z wyłudzeniem informacji (phishingiem). Szantaż, kradzież danych oraz wyświetlanie pasującej reklamy to inne obszary zainteresowania.

3. Jak złośliwe oprogramowanie trafia do komputera?

Po naświetleniu sytuacji związanej z motywacją podmiotów rozpowszechniających złośliwe programy, możemy skupić się na zasadniczym temacie niniejszego opracowania. Istnieje wiele dróg, którymi złośliwe oprogramowanie może przeniknąć do komputera firmowego. W określonych przypadkach wystarczy podłączyć komputer do Internetu lub do lokalnej sieci. Złośliwe programy mogą być jednak zawarte także w wiadomościach e-mail, na portalach aukcyjnych, w komunikatorach internetowych a nawet na nośnikach danych. W chwili obecnej najbardziej niebezpieczne są jednak spreparowane strony internetowe, które albo bezpośrednio wpuszczają plik albo w sposób niezauważony zarażają komputer, działając w tle jako tak zwane ataki drive-by-download.

3.1 Wystarczy połączenie

Nieliczone robaki i boty internetowe, które stale niezależnie krążą w Internecie, stanowią ciągłe zagrożenie dla komputerów podłączonych do Internetu. Bez przerwy generują w sposób bardziej lub mniej przypadkowy adresy IP, sprawdzając, czy przyporządkowane im komputery nadają się do tworzenia luk w zabezpieczeniach. Wybór adresów IP jest często ograniczony, tak że wybrane zostają tylko określone obszary sieci – np. konkretnego dostawcy Internetu lub danego regionu. To, jakie luki w zabezpieczeniach zostaną wybrane, zmienia się w miarę upływu czasu. Sprawdzane są nawet te luki, które już dawno zabezpieczono, jak miało to miejsce w przypadku robaków Blaster (2003) oraz Sasser (2004). Częste cele ataków zaprezentowano na poniższej liście:

- Plug'n'Play (MS05-039) poprzez TCP/445, TCP/139
- RPC-DCOM (MS03-026/MS03-039) poprzez TCP/135, TCP/445, TCP/1025
- LSASS (MS04-011) poprzez TCP/445
- MySQL poprzez TCP/3306
- Arkeia poprzez TCP/617
- Veritas poprzez TCP/6101
- Veritas poprzez TCP/10000
- WINS poprzez TCP/42
- Arcserve poprzez TCP/41523
- NetBackup poprzez TCP/13701
- Workstation Service (MS03-049) poprzez TCP/135, TCP/445
- WebDaV poprzez TCP/80
- DameWare poprzez TCP/6129
- MyDoom-Backdoor poprzez TCP/3127
- Bagle-Backdoor poprzez TCP/2745
- IIS 5.x SSL PCT (MS04-011) poprzez TCP/443
- Konta z trywialnymi hasłami (połączenie poprzez TCP/139 lub TCP/445)
- Serwer MSSQL z trywialnym hasłem (np. konto „SA” z pustym hasłem) poprzez TCP/1433

W ramach opracowania przez okres trzech miesięcy mierzono ataki na różne architektury komputerowe. Komputery z środowiskiem Windows atakowano średnio co 38 sekund. Niektó-

rzy administratorzy systemów przeżyli sytuacje, gdy nowo podłączany komputer atakowano i przejmowano już po kilku sekundach podczas pobierania plików aktualizacyjnych. W sieciach z wieloma klientami końcowymi (np. T-Online) częstotliwość ataków jest znacznie wyższa niż średnia wartość wynosząca 38 sekund. W ostatnich latach profesjonalizowano także tworzenie kodów typu Exploit. Czasami kody typu Exploit wykorzystujące luki w zabezpieczeniach pojawiają się już kilka dni po pierwszych doniesieniach o owych słabych punktach. Rośnie także liczba programów typu Exploit, które są wykrywane dlatego, że wykorzystuje je złośliwe oprogramowanie. Najbardziej aktualnym przykładem był tu robak Conficker, który do rozprzestrzeniania się wykorzystuje oprócz automatycznego przenikania także lokalne, słabo chronione dostępy oraz mechanizm Autostartu pamięci USB.

Ten rodzaj ataku funkcjonuje bez aktywności użytkownika komputera, a w większości przypadków także bez jego wiedzy. Dobrze skonfigurowana zaporą sieciową lub router chronią przed tego rodzaju atakami.

3.2 Za pomocą poczty elektronicznej

Wiele złośliwych programów nadal rozprzestrzenia się za pomocą poczty elektronicznej. Całe rzesze komputerów zaatakowanych przez takie programy jak Loveletter, Melissa czy Sobig i Netsky, które sparaliżowały działanie niektórych serwerów pocztowych, stają się coraz radsze i nie są celem przestępców rozpowszechniających robaki. Sober, Nyxem i Warezov były ostatnimi robakami przenoszonymi przez pocztę, które wzbudziły duże poruszenie w mediach. Ich miejsce zajęły mniejsze fale infekcji wirusami, ograniczone czasowo i terytorialnie. W odróżnieniu od infekcji robakami internetowymi przebiegających całkowicie automatycznie, robaki rozprzestrzeniane za pomocą poczty e-mail stają się niebezpieczne dopiero z chwilą otarcia załącznika przez odbiorcę. Samo otrzymanie zainfekowanej wiadomości e-mail nie stanowi jeszcze niebezpieczeństwa, tylko w nielicznych przypadkach wystarczy samo podświetlenie wiadomości (np. w przypadku robaków Bubbleboy i Klez). Większość wiadomości e-mail wymaga współpracy odbiorcy, który przy pomocy różnorodnych zabiegów socjotechnicznych nakłaniany jest do otwarcia załącznika. W tym celu fałszuje się wszelkie możliwe informacje zamieszczane w nagłówku wiadomości e-mail. Dotyczy to w szczególności adresu nadawcy. Tylko pierwsze pokolenie robaków e-mail przenikało dalej posługując się nazwą ofiary. Dziś nieprawdziwe są niemal wszystkie adresy nadawcze tego typu robaków.

Ponieważ wszelkie zarażone pliki w wiadomościach e-mail są dziś usuwane (albo przez bramę sieciową albo przez program pocztowy) i wzrosła świadomość niebezpieczeństwa użytkowników poczty elektronicznej, autorzy szkodliwego oprogramowania zmienili strategię. Zamiast załączników rozsyła się wiadomości e-mail z łączami do plików w Internecie. Tego rodzaju wiadomości nie od razu są rozpoznawane jako zainfekowane. W najlepszym wypadku może je wychwycić filtr spamu. Procedura postępowania użytkownika jest jednak bardzo podobna. Klika on łącze, wyszukiwarka pyta, co ma zrobić, proponując zwykle otwarcie pliku. Po niedługim czasie łącza przekierowujące bezpośrednio na strony ze złośliwymi programami także uznano za szkodliwe. Dlatego też autorzy złośliwych programów odsyłają obecnie do strony internetowej, na której odbiorca uruchamia na nowo pobieranie plików lub rozpoczyna się ono automatycznie poprzez liczne przekierowania.

Przynętą, nakłaniającą ofiary do otwarcia pliku lub stron internetowych (tak zwana socjotechnika), jest nadawca, nagłówek i/lub treść wiadomości. Aby nadać takiej próbie oszustwa pozory wiarygodności, wykorzystuje się także nazwę załącznika, podwójne zakończenia rozszerzeń plików, popularne ikony czy nazwę domeny łącza. Jordan i Goudey (2005) wyłonili dwanaście następujących czynników oddziaływania na psychikę, wykorzystanych w latach 2001 – 2004 przez najskuteczniejsze robaki:

- brak doświadczenia,
- ciekawość,
- chciwość,
- brak pewności siebie,
- uprzejmość,
- miłość własna,
- łatwowierność,
- pragnienia,
- pożądanie i miłość,
- strach,
- wzajemność,
- przyjazność.

M. Braverman dodał:

- ogólną konwersację, krótkie wypowiedzi, takie jak „cool” i tym podobne;
- ostrzeżenia przed wirusami oraz aktualizacje oprogramowania;
- znajdowanie złośliwych programów na komputerze;
- raporty dotyczące wirusów zamieszczane na końcu wiadomości;
- informacje lub doniesienia dotyczące kont: np. koń trojański, podający się za zawyżony rachunek telefoniczny;
- zgłoszenia błędów w przesyłaniu wiadomości e-mail;
- atrakcyjność fizyczną (zazębia się z punktem pożądanie wymienionym przez Jordana i Goudeya);
- oskarżenia: np. koń trojański w BKA (Federalnym Urzędzie Kryminalnym), który rzekomo znalazł nielegalne pliki;
- aktualne wydarzenia;
- gratyzy: niektórzy ludzie lekceważą wszelkie środki ostrożności, słysząc o czymś darmowym.

Próby wprowadzania w błąd nie ustają jednak z chwilą, gdy złośliwy program osiągnął cel i został zainstalowany. Po przeprowadzeniu ataku chodzi o to, by uniemożliwić ofierze rozpoznanie, że została zarażona. W tym celu otwiera się zgłoszenia błędów, obrazy lub (czasami puste) dokumenty. Niektóre robaki, takie jak Sircam czy Magistr podczepiają się pod plik i uruchamiają się wraz z otwarciem oryginalnych aplikacji. W ten sposób zarażenie robakiem pozostaje niezauważone.

3.3 Poprzez komunikator internetowy

Większość robaków przenikających do komunikatorów internetowych rozsyła wiadomości z łączami do stron internetowych. Nie korzysta się już prawie z możliwości bezpośredniego przesyłania plików. Także tu, podobnie jak w przypadku wiadomości e-mail, ataki oparte są na zabiegach socjotechnicznych. Niektóre działające w komunikatorach robaki posiadają nawet własne programy typu chat engine i są w stanie prowadzić rozmowy, zdobywając w ten sposób zaufanie.

Jeśli w firmie korzysta się z komunikatora internetowego, należy wybrać program pocztowy, umożliwiający kontrolę przychodzących plików. Niektóre programy pocztowe umożliwiają uruchomienie polecenia skanowania programem antywirusowym.

3.4 Poprzez portal aukcyjny

W ramach przeprowadzonego przez G Data badania szukaliśmy w portalach aukcyjnych P2P pojęć związanych z grami online, należącymi aktualnie do czołowej dwudziestki (Top 20). Na początku badania 33% spośród niemal 1000 pobranych plików było zainfekowane złośliwym oprogramowaniem. Nieco ponad dwie trzecie (68%) złośliwych programów zidentyfikowano jako adware, 23% stanowiły konie trojańskie a 5% oprogramowanie typu Backdoor.

W trakcie prowadzonych przez sześć miesięcy badań już ponad połowa kontrolowanych plików z portali aukcyjnych P2P była zainfekowana złośliwymi programami. Odsetek ten osiągnął najwyższą wartość pod koniec okresu badań, gdy stwierdzono ponad 65% zarażonych plików.

Liczby te potwierdzają, że portale aukcyjne P2P są nadal niezwykle popularne wśród autorów złośliwego oprogramowania. Ci, którzy korzystają z nich w firmie, powinni się bezwzględnie zabezpieczyć.

3.5 Poprzez nośniki danych

Ciągle jeszcze zdarza się, że takie nośniki danych jak twarde dyski, płyty DVD czy odtwarzacze MP3, są fabrycznie zainfekowane złośliwym oprogramowaniem. Słyszeliśmy także o przypadkach umyślnego „gubienia” na parkingach firmowych kluczy pamięci zawierających programy szpiegowskie. Kilku pracowników chcących sprawdzić, co jest na dysku, wpuściło do swojego komputera program szpiegowski.

Omawiany w mediach na początku roku 2009 robak o nazwie Conficker do rozprzestrzeniania się za pośrednictwem przenośnych dysków wykorzystywał między innymi funkcję automatycznego uruchamiania systemów operacyjnych Windows. Robaki z rodziny Autorun także korzystają z tej „funkcji” systemu Windows, co spowodowało w drugim półroczu 2008 roku powrót owych programów. Rady, by po prostu wyłączyć funkcję automatycznego uruchamiania, nie przynosiły początkowo efektów, gdyż stało się to możliwe dopiero w późniejszym terminie dzięki odpowiedniej poprawce firmy Microsoft.

Przypadki te pokazują, że firmy, zwłaszcza wtedy, gdy przechowują cenne dane, są atakowane także nietypowymi metodami i że dbałości o bezpieczeństwo nigdy nie jest za dużo.

3.6 Poprzez lokalne sieci

Inna droga rozpowszechniania złośliwych programów to udostępnianie katalogów w sieciach lokalnych. Niektóre robaki przekopiuwają się na wszystkie dostępne obszary. W wielu wypadkach wykorzystują przy tym listy z popularnymi hasłami dostępu. Ten słaby punkt był jedną z dróg wykorzystywanych przez Confickera. Dlatego też firmy powinny stosować solidne hasła, regularnie, najlepiej codziennie kontrolując miejsca dostępu do sieci pod kątem występowania złośliwego oprogramowania. Niektóre warianty robaków Rbot oraz Conficker używają m.in. następujących loginów:

„ADMIN”, „ADMINISTRADOR”, „ADMINISTRAT”, „ADMINISTRATEUR”, „ADMINISTRATOR”, „ADMINS”, „COMPUTER”, „DATABASE”, „DB2”, „DBA”, „DEFAULT”, „GUEST”, „NET”, „NETWORK”, „ORACLE”, „OWNER”, „ROOT”, „STAFF”, „STUDENT”, „TEACHER”, „USER”, „VIRUS”, „WWWADMIN”

oraz haseł:

„0”, „000”, „007”, „1”, „12”, „123”, „1234”, „12345”, „123456”, „1234567”, „12345678”,

„123456789“, „1234567890“, „12345678910“, „2000“, „2001“, „2002“, „2003“, „2004“, „ACCESS“, „ACCOUNTING“, „ACCOUNTS“, „ADM“, „ADMIN“, „ADMINISTRADOR“, „ADMINISTRAT“, „ADMINISTRATEUR“, „ADMINISTRATOR“, „ADMINS“, „BASD“, „BACKUP“, „BILL“, „BITCH“, „BLANK“, „BOB“, „BRIAN“, „CHANGEME“, „CHRIS“, „CISCO“, „COMPAQ“, „COMPUTER“, „CONTROL“, „DATA“, „DATABASE“, „DATABASEPASS“, „DATABASEPASSWORD“, „DB1“, „DB1234“, „DB2“, „DBA“, „DBPASS“, „DBPASSWORD“, „DEFAULT“, „DELL“, „DEMO“, „DOMAIN“, „DOMAINPASS“, „DOMAINPASSWORD“, „ERIC“, „EXCHANGE“, „FRED“, „FUCK“, „GEORGE“, „GOD“, „GUEST“, „HELL“, „HELLO“, „HOME“, „HOMEUSER“, „HP“, „IAN“, „IBM“, „INTERNET“, „INTRANET“, „JEN“, „JOE“, „JOHN“, „KATE“, „KATIE“, „LAN“, „LEE“, „LINUX“, „LOGIN“, „LOGINPASS“, „LUKE“, „MAIL“, „MAIN“, „MARY“, „MIKE“, „NEIL“, „NET“, „NETWORK“, „NOKIA“, „NONE“, „NULL“, „OAINSTALL“, „OEM“, „OEMINSTALL“, „OEMUSER“, „OFFICE“, „ORACLE“, „ORAINSTALL“, „OUTLOOK“, „OWNER“, „PASS“, „PASS1234“, „PASSWD“, „PASSWORD“, „PASSWORD1“, „PETER“, „PWD“, „QAZ“, „QWE“, „QWERTY“, „ROOT“, „SA“, „SAM“, „SERVER“, „SEX“, „SIEMENS“, „SLUT“, „SQL“, „SQLPASS“, „STAFF“, „STUDENT“, „SUE“, „SUSAN“, „SYSTEM“, „TEACHER“, „TECHNICAL“, „TEST“, „UNIX“, „USER“, „VIRUS“, „WEB“, „WIN2000“, „WIN2K“, „WIN98“, „WINDOWS“, „WINNT“, „WINPASS“, „WINXP“, „WWW“, „WWWADMIN“, „XP“, „ZXC“

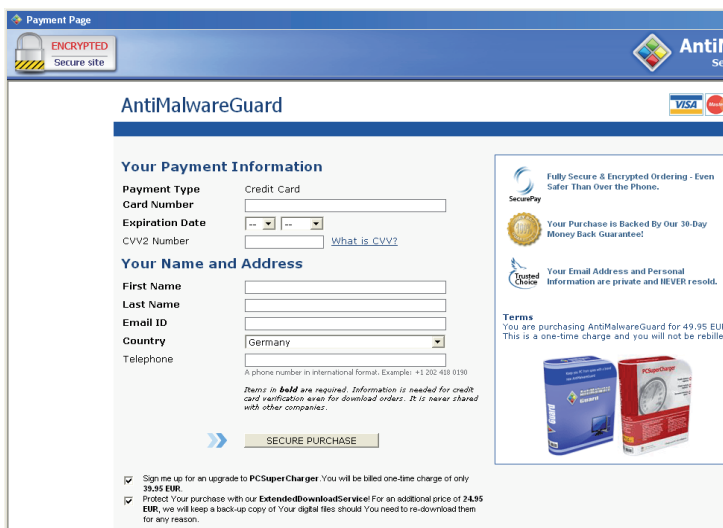
Dlatego też użytkownicy sieci powinni zrezygnować z tych oraz podobnych haseł – także z ich tłumaczeń na język ojczysty.

3.7 Poprzez stronę internetową

W chwili obecnej najważniejszym miejscem przenikania nowych złośliwych programów są strony internetowe. Wykorzystują one strukturalne słabe punkty w pracy skanerów antywirusowych. Skanery antywirusowe sprawdzają pliki albo wtedy, gdy chce z nich skorzystać któryś z elementów systemowych (OnAccess) lub na żądanie (OnDemand). Sprawdzenie przez skaner antywirusowy odbywa się zatem dopiero wtedy, gdy złośliwy program ma już formę pliku. Gdy za pomocą protokołu HTTP przesyła się do przeglądarki dane strony, najpierw w pamięci roboczej owej wyszukiwarki interpretowane oraz realizowane są zawarte w nim kody HTML oraz polecenia skryptowe. Po pewnym czasie wyszukiwarka podejmuje decyzję o zapisaniu treści na dysku twardym. Możliwe jest, że skaner antywirusowy uruchomi wtedy alarm. Złośliwe programy są już jednak wówczas zainstalowane. Aby skaner antywirusowy mógł skutecznie chronić przed szkodliwymi witrynami internetowymi, należy sprawdzać zawartość przepływających informacji, zanim dotrą one do przeglądarki.

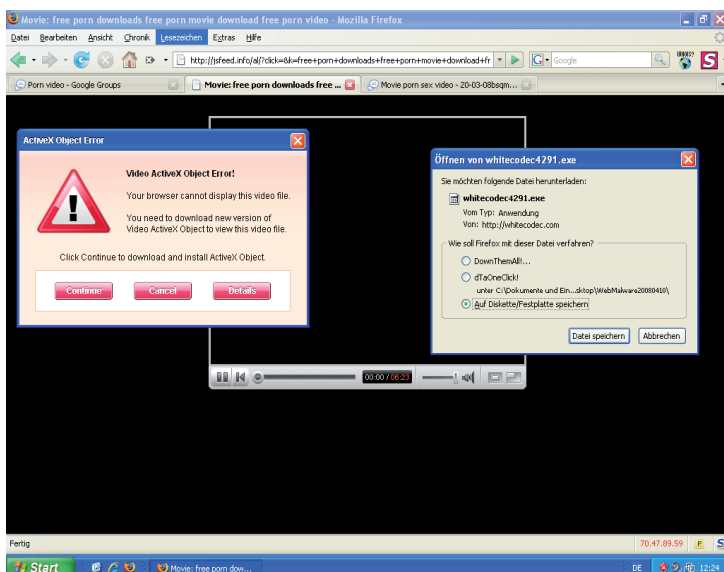
W związku z wiadomościami e-mail zgodzono się co do tego, że pliki ze złośliwym oprogramowaniem mogą być pobierane ze stron internetowych. Odbywa się to albo przez bezpośrednie łącze odsyłające do pliku ze złośliwym programem, poprzez dalsze przekierowania lub poprzez nakłanianie użytkownika sztuczkami do tego, by klikając przycisk lub łącze pobrał i otworzył na komputerze dany plik.

Prezentujemy w skrócie dwa typowe triki, służące do nakłaniania użytkownika do pobrania i zainstalowania złośliwego oprogramowania. Tak zwane programy typu scareware sugerują ofercie przy pomocy fałszywych ostrzeżeń, że system jej komputera jest zarażony złośliwym oprogramowaniem. Aby się go pozbyć ofiara musi podać informacje dotyczące swojej karty kredytowej, płacąc około 50 dolarów za rzekomą „pełną wersję” oszukańczego skanera antywirusowego.



Rys. 2: Strona internetowa z programem typu scareware pyta o informacje dotyczące karty kredytowej ofiary

Chętnie stosuje się także sztuczkę polegającą na zachęcaniu ofiary do wejścia na stronę, na której ma się rzekomo znajdować film wideo. Film taki może zawierać treść erotyczną lub nawiązywać do aktualnych wydarzeń, nagłaśnianych w danym momencie przez media (klęska żywiołowa, katastrofa lotnicza, wybory prezydenckie, wydarzenie sportowe). Aby obejrzeć zachwalany film, odwiedzający daną stronę musi rzekomo zainstalować specjalny program do odbioru filmów wideo lub najnowszą wersję programu Flash Player, w których ukryte jest złośliwe oprogramowanie. Za łączem tym kryje się za każdym razem złośliwe oprogramowanie, które zostaje zainstalowane na komputerze zamiast aplikacji Flash Player.



Rys. 3: Rzekoma strona internetowa z plikiem wideo oraz żądaniem zainstalowania zainfekowanego programu.

Istnieje także inna technika ataku, przy której nie jest konieczna współpraca ze strony ofiary: chodzi o tak zwane drive-by-downloads. Podczas, gdy wszelkie instalacje programów musi zainicjować odwiedzający daną stronę internetową, ataki drive-by-downloads przebiegają, jak wskazuje sama nazwa, w sposób niezauważony podczas surfowania w Internecie. W tym celu na kontrolowanym przez cyberprzestępców serwerze zapisuje się skrypty sprawdzające, jakiej przeglądarki oraz jakiego systemu operacyjnego używa komputer danego gościa strony internetowej. Złośliwy program zostaje pobrany w wersji odpowiednio dostosowanej do danej kombinacji, sprawdzając przeglądarkę oraz jej elementy pod kątem luk w zabezpieczeniach. Jeśli poszukiwanie okaże się owocne, dochodzi do instalacji złośliwego oprogramowania

wykorzystującego ową lukę w celu przejścia komputera. Są to złośliwe programy typu Exploit (z ang. „wykorzystać”). Najwięcej programów typu Exploit przeznaczonych jest do komputerów z systemem Windows oraz przeglądarką Internet Explorer. Korzystają one także ze słabych punktów takich systemów jak Firefox, Opera czy Safari. Do właściwego zainstalowania skryptów służą takie narzędzia jak MPack IcePack czy FirePack. W chwili obecnej autorzy złośliwego oprogramowania wykorzystują najczęściej następujące luki w zabezpieczeniach:

- CVE 2007-0071 Adobe Flash
- CVE 2008-1309 RealPlayer
- ourgame_GLIEDown2 Internet Explorer
- CVE 2006-0003 MS06-01, MDAC
- CVE 2007-5601 RealPlayer

Gdy serwer jest przygotowany, rozpowszechniający złośliwe oprogramowanie musi jedynie zwabić gości na swoją stronę. Odbywa się to z jednej strony przy pomocy e-maili ze spamem, zachęcających do odwiedzin strony obietnicami uzyskania ciekawych informacji, specjalnych ofert czy wygranych. Coraz częściej manipuluje się zapytaniami realizowanymi za pomocą takich wyszukiwarek jak Google, Yahoo czy Bing w taki sposób, że strony ze szkodliwym oprogramowaniem pojawiają się na samym początku wyników wyszukiwania. Także błąd we wpisywanej w wyszukiwarce nazwie łączy może odesłać nas na niepożądaną stronę. Dwa przykłady: „microsoft.com”, „goggle.com” czy też „mcaffe.de” jak też wiele innych domen, których pisownia przypomina nazwy znanych stron www, są już od lat rejestrowane po to, by prezentować na nich reklamę. Tak więc dzięki rozpowszechnianiu programów typu adware czy też złośliwego oprogramowania można zarobić dodatkowo dużo pieniędzy.

O wiele bardziej skuteczne jest jednak umieszczenie złośliwego oprogramowania na stronach znanej domeny. Jeśli atakującemu uda się przejąć kontrolę nad danym serwerem internetowym, przy pomocy wymienionych już narzędzi Web Exploit Toolkits do każdej strony dodaje się jeden wiersz, który powoduje pobieranie złośliwego oprogramowania z innego serwera (np. przy pomocy funkcji IFRAME lub SCRIPT). W międzyczasie dostępne są także narzędzia służące do napaści na serwery internetowe, które poprzez ataki słownikowe próbują odgadnąć hasło dostępu administratora. Do przejmowania serwerów internetowych wykorzystuje się także luki w zabezpieczeniach popularnych aplikacji internetowych takich jak systemy zarządzania treścią, programy do blogów i forów oraz narzędzia administrowania. W większości przypadków ataki te nie ograniczają się do pojedynczych serwerów internetowych, lecz prowadzone są masowo i automatycznie. Skutek: złośliwe oprogramowanie czyha nie tylko w mrocznych zakamarkach Internetu, lecz może ukryć się na każdej domenie.

Inną możliwość stanowią reklamy wyświetlane na popularnych stronach internetowych. Niemal wszystkie popularne domeny korzystają z możliwości zarabiania pieniędzy za umieszczenie na nich reklamy. Banery reklamowe są zwykle wyświetlane na stronach przy pomocy pływających ramek IFRAME, tak by administrator nie miał wpływu na umieszczone w nich treści. Obowiązkiem reklamującego jest sprawdzenie treści dostarczanej reklamy. Łatwiej to jednak powiedzieć niż wykonać. Złośliwe skrypty, tworzone przy pomocy programu MPack czy podobnych narzędzi, są doskonale ukryte i zaszyfrowane (stworzenie polimorficznego złośliwego kodu jest możliwe także w językach skryptowych). W ten sposób udaje się umieścić złośliwy kod na legalnych stronach internetowych. Do około 80% wszystkich infekcji typu drive-by dochodzi na legalnych stronach www.

Złośliwy kod można także przesłać bez łamania zabezpieczeń serwera internetowego. Łączy w forach, blogach czy w wiadomościach e-mail mogą zawierać złośliwe kody, uruchamiane na

odwiedzanej stronie. Interaktywny Internet Web 2.0 oferuje niezliczone fora dyskusyjne oraz strony typu Wiki, do których uczestnicy mają dopisywać własne treści i dołączać pliki. Czasem może się na nich znaleźć także złośliwe oprogramowanie lub łącze do strony z tego typu aplikacją. Pewnego razu jednemu z autorów Wikipedii udało się umieścić w artykule na temat robaka Blaster łącze do usuwającego go narzędzia, które jak stwierdzono później, było koniem trojańskim. Na forach takich działają także ludzie (lub ich maszyny), nie mających dobrych zamiarów. Dzięki niezliczonej ilości skradzionych tożsamości mają łatwy dostęp do większości miejsc, pozostając przy tym w ukryciu.

Jednak nie jest to bezwzględnie konieczne do umieszczenia złośliwego kodu na serwerze. Już samo łącze odsyłające do dowolnej witryny może zawierać złośliwy kod, który uaktywnia się na docelowej stronie. Tego rodzaju atak nosi nazwę cross site scripting (XSS). Atak XSS jest możliwy zawsze wtedy, gdy wpisy użytkownika pokazują się ponownie na kolejnej stronie i nie są kontrolowane pod kątem uruchamianej zawartości. Jeśli np. nazwisko podane w formularzu ponownie wyświetla się w kolejnym zamówieniu, jest to bardzo przydatne. Jeśli w miejsce swojego nazwiska atakujący wprowadzi kod JavaScript, to - o ile nie usuną go filtry - zostanie on uruchomiony przez przeglądarkę. Przykład ataku typu cross site scripting: Formularz żąda nazwy/nazwiska. Zamiast nazwy atakujący wprowadza następujący kod:

```
<SCRIPT>alert(„You`re pwned“)</SCRIPT>
```

Po wysłaniu formularza kod ten nie pojawia się już na kolejnej stronie, lecz jest uruchamiany. W prezentowanym przypadku pojawia się ostrzeżenie. Prawdziwy atak zawiera niebezpieczniejszy kod.

Ale nawet wtedy, gdy wpisy do formularza są filtrowane, istnieje możliwość wpisania kodu bezpośrednio do łącza przekierowującego na wywołaną stronę. Na przykład w taki sposób:

```
http://www.myserver.dom/site.php?name=<SCRIPT>alert(„You`re pwned“)</SCRIPT>
```

Tego typu łącza może ukryć się za każdym tekstem, przechowywanym na forum lub na blogu. Jeszcze perfidniejsze jest jednak, gdy tego typu łącza XSS pojawiają się w wynikach wyszukiwania przez Google. Autorzy złośliwego oprogramowania optymalizują skorumpowane wpisy na blogach dla potrzeb robotów indeksujących wyszukiwarki Google, co zawsze udaje się przy pomocy kilku sztuczek maskujących, mimo że Google nie szczędzi wysiłków w celu wykrycia tego rodzaju łączy XSS i eliminowania ich z wyników wyszukiwania.

Podobnie jest w przypadku wielu nowych możliwości, oferowanych przez Web 2.0. Ten, kto w sytuacji zagrożenia wpadłby na pomysł, że korzystne byłoby niedopuszczanie do wyszukiwarki aktywnych treści lub języków skryptowych, wyłączyłby się w ten sposób z nowego pięknego świata Web 2.0, rezygnując z jego nieskończonych możliwości. Mnogość owych nowych funkcji stwarza jednak możliwości nadużyć, zwiększając ilość potencjalnych luk w zabezpieczeniach. Pod koniec roku 2005 robak XSS o nazwie Samy poprzez atak cross site scripting (XSS) na sieć Myspace zdobył w ciągu 18 godzin ponad milion przyjaciół. Niebezpieczeństwo ataków cross site scripting jest jednak w dalszym ciągu niedoceniane.

Domeny rozpowszechniające złośliwe kody można więc znaleźć nie tylko w mrocznych zakamarkach Internetu, na popularnych portalach (np. Rapidshare) czy na stronach ze złamanymi zabezpieczeniami, lecz także pod legalnymi adresami WWW oraz w wynikach wyszukiwania Google. Ciekawostka: złośliwe kody mogą być wpisane w każdą stronę internetową.

4. Przebieg typowej fali zarażania komputerów

Atak cyberprzestępców przebiega z reguły według charakterystycznego schematu. Typowa infekcja uległa w ciągu ostatnich lat znacznym zmianom. Robaki takie jak NetSky czy MyDoom posiadały duże załączniki, zawierające monolityczne złośliwe oprogramowanie z wieloma zintegrowanymi funkcjami. W ostatnich latach przekształciły się one w liczne małe, zwarte i wysoko wyspecjalizowane moduły, które pobiera się w zależności od potrzeb. Infekcja przebiega wieloetapowo. Po przygotowaniu konkretnego złośliwego programu i wybraniu potencjalnych ofiar, dochodzi do zasadniczego ataku. W następstwie zainfekowane systemy, znajdujące się od tej chwili pod kontrolą atakującego można wykorzystywać do niemalże dowolnych działań przestępczych.

4.1 Przygotowanie infekcji

Najpierw należy stworzyć złośliwe oprogramowanie, które ma być rozpowszechniane. Nie trzeba tego powtarzać od nowa przy każdej fali infekcyjnej. Jeśli autor złośliwego oprogramowania stworzy określony kod, na podstawie opracowanego wzorca może przy pomocy programów typu runtime packer, innych kompilatorów i narzędzi do ukrywania stworzyć jego różne warianty przeznaczone dla nowych fal i to tak długo, jak nie będą ich rozpoznawały najpopularniejsze programy antywirusowe. Jeśli dany złośliwy kod przewiduje dopuszczenie skanera antywirusowego do zainfekowanych komputerów, wystarczy zapewnić, by dla najpopularniejszych programów antywirusowych istniała zawsze nierozpoznawana przez nie wersja szkodliwego programu. Ci, którzy nie chcą czynić tego sami, znajdują na nielegalnych forach ludzi, którzy za odpowiednią cenę oferują poszukiwane przez nich usługi z gwarancją ich wykonania.

Gdy złośliwy program zostanie opracowany, atakujący musi zdecydować się na jedną (lub kilka) dróg jego rozpowszechniania. Można go na przykład wprowadzić poprzez przeprowadzony automatycznie atak na lukę w zabezpieczeniach. W takim przypadku ofiara wcale nie zauważa ataku czy też infekcji. Aby nakłonić użytkownika do uruchomienia złośliwego oprogramowania atakujący może się również zdecydować na jeden z powszechnie stosowanych trików. W pierwszym z przypadków atakujący potrzebuje programu typu Exploit, który przejmie komputer, w drugim strony internetowej i/lub wprowadzającej w błąd wiadomości e-mail czy też komunikatora internetowego, które nakłonią użytkownika do otwarcia pliku. Jeśli dana strona miałaby przejść hosting złośliwego programu, należy zarejestrować domenę i umieścić na niej odpowiednie pliki. Dla większości wymienionych działań istnieją łatwe w obsłudze narzędzia.

4.2 Realizacja

Po przejściu komputera przeważnie uruchamia się konia trojańskiego typu downloader. Tenże dba o to, by szkodliwe pliki dotarły do komputera i zostały otwarte. Najpierw informuje się sprawcę ataku o pomyślnym przebiegu infekcji oraz o zajęтым systemie. Później wyłącza się ustawienia zabezpieczeń zainfekowanego komputera. Jest on wówczas bezbronny wobec dalszej aktywności złośliwego oprogramowania. W następnej kolejności następuje pobranie do komputera kolejnych złośliwych programów. Do realizacji kolejnych etapów można wykorzystać wiele plików ze złośliwymi programami.

W wielu przypadkach pierwszym pobranym złośliwym programem jest oprogramowanie typu Backdoor, ukryte np. za programem typu Rootkit, który niezauważony działa w tle. Dzięki temu „tylnemu wejściu” zarażony komputer zyskuje nowego właściciela, który może z nim postępować według własnego upodobania. Korzystając z IRC, P2P lub HTTP program typu Backdoor umożliwia między innymi synchronizowanie komputera z wieloma innymi komputerami na świecie. W taki sposób komputer staje się częścią olbrzymiej dziś armii komputerów zombie.

Po zainstalowaniu oprogramowania typu Backdoor następuje dokładniejsza kontrola zainfekowanego systemu, a atakujący podejmuje decyzję dotyczącą dalszego postępowania z komputerem. Komputery, których zabezpieczenia zostały złamane, przeszukiwane są przez programy szpiegowskie pod kątem użytecznych danych i/lub wyposażane w programy typu adware. Jeśli dany komputer dysponuje dobrym łączem internetowym, może zostać wykorzystany do rozsyłania spamu, proponować pobranie nielegalnych plików lub zajmować się hostingiem stron internetowych zawierających oprogramowanie do wyłudzenia informacji (phishingu) lub inne złośliwe programy.

4.3 Korzystanie z zainfekowanego komputera

Gdy należące do danej sieci botnet komputery zombie mają być wykorzystane do rozsyłania spamu, administrator takiej sieci nagrywa na zainfekowanym urządzeniu przy pomocy oprogramowania typu Backdoor pakiet złośliwych programów, zawierający między innymi wzorzec wiadomości, listę adresów e-mail oraz oprogramowanie do rozsyłania poczty. Gdy plik taki jest gotowy, uruchamia się go i rozpoczyna wysyłkę. Po rozesłaniu wszystkich wiadomości e-mail, oprogramowanie wraz ze wszystkimi danymi zostaje wykasowane z komputera. Pozostaje w nim jedynie oprogramowanie typu Backdoor, które – dobrze ukryte – oczekuje na kolejne polecenia.

5. Jak można się chronić

Ochrona komputerów firmowych przed złośliwym oprogramowaniem to tylko jedna z dziedzin zabezpieczeń IT, którą należy zawsze powiązać z całościowym bezpieczeństwem IT danego zakładu. Bezpieczeństwo IT to nie stan, lecz proces. W każdym przedsiębiorstwie istnieją szczególnie zagrożone obszary lub grupy użytkowników, wymagające specjalnej ochrony. W procesie tym każde przedsiębiorstwo musi podejmować różnorodne decyzje, prowadzące do całkowicie indywidualnych rozwiązań.

Z ochroną przed złośliwym oprogramowaniem wiąże się w pierwszym rzędzie zastosowanie procesów technicznych, które chronią (powinny chronić) przed zdefiniowanymi zagrożeniami. Do najważniejszych technicznych środków bezpieczeństwa należą:

- Ochrona antywirusowa, która powinna być zainstalowana zarówno na serwerach jak i w programach pocztowych. Powinna sprawdzać ponadto przepływ danych w protokołach HTTP oraz dane z komunikatorów (ICQ, IRC) pod kątem występowania złośliwych kodów.
- Ochrona antyspamowa. Ponieważ wiadomości e-mail zamiast załączonych plików zawierają jedynie łącza do stron ze złośliwym oprogramowaniem, ochrona przed spamem staje się jednocześnie zabezpieczeniem przed szkodliwym oprogramowaniem.
- Zapora, systemy wykrywania wtargnięć i zapobiegania wtargnięciom. Dane z ruchu w sieci można wykorzystywać do wykrywania i uniemożliwiania powszednich ataków robaków internetowych.

Do ochrony antywirusowej przyczyniają się także inne środki techniczne. Zarządzanie poprawkami, wirtualizacja oprogramowania, uprawnienia użytkowników do komputerów firmowych, kontrole dostępu w odniesieniu do plików oraz obszarów sieci oraz wiele innych działań uzupełnia znane środki bezpieczeństwa. Poszczególne możliwości nie mogą i nie powinny być tu dokładniej omawiane. Wydana przez Federalny Urząd Bezpieczeństwa Technologii Informacyjnych (BSI) instrukcja dotycząca podstawowej ochrony IT stanowi tu obszerny materiał źródłowy.

Techniczne środki nie wystarczają jednak do skutecznej ochrony sieci danego przedsiębiorstwa. Środki bezpieczeństwa muszą być akceptowane i realizowane przez pracowników. Ramy wyznaczają tutaj uzgodnione z kierownictwem firmy wytyczne dotyczące obchodzenia się z komputerami, nośnikami danych oraz innymi informacjami ważnymi dla bezpieczeństwa. Należy także uwzględnić warunki ramowe natury prawnej i etycznej. Środki bezpieczeństwa muszą znaleźć odzwierciedlenie w strukturze organizacji. Na przykład wszelkie naruszenia obowiązujących wytycznych powinny być obwarowane sankcjami. Wszystkich pracowników należy ponadto poinformować o źródłach niebezpieczeństw w Internecie oraz w codziennej pracy. Gdy uważni pracownicy uzupełnią techniczne środki bezpieczeństwa, zabezpieczenie komputerów firmowych przed złośliwym oprogramowaniem może się powieść.