

Raport „Zagrożenia bezpieczeństwa w Internecie” firmy Symantec

Specyfika ataków zaobserwowanych w III i IV kwartale 2002 r.

WYDAWCA

Mark Higgins
Kierownik sekcji trendów i analiz
w dziale usług zabezpieczeń
zarządzanych firmy Symantec

ZESPÓŁ DS. BADAŃ I ANALIZ

David Ahmad
Kierownik ds. programowania w dziale
reakcji na zagrożenia firmy Symantec

Cori Lynn Arnold

Analityk ds. zabezpieczeń
w dziale usług zabezpieczeń
zarządzanych firmy Symantec

Brian Dunphy

Dyrektor ds. analiz
w dziale usług zabezpieczeń
zarządzanych firmy Symantec

Michael Prosser

Główny analityk trendów
w dziale usług zabezpieczeń firmy
Symantec

Vincent Weafer

Dyrektor ds. programowania
w dziale reakcji na zagrożenia firmy
Symantec

KONTAKTY Z MEDIAMI

Candice Garmoe
310-449-4324

OPINIE O RAPORCIE

threatreport@symantec.com

Streszczenie dla Zarządu

Raport „Zagrożenia bezpieczeństwa w Internecie” (*Internet Security Threat*) firmy Symantec umożliwia społeczności użytkowników Internetu szczegółowe zapoznanie się z kierunkami zmian zachodzących w czasie w zagrożeniach związanych z korzystaniem z Internetu. Raport zawiera dane na temat trendów dotyczących ataków zaobserwowanych w największej na świecie sieci systemów wykrywania włamań (*intrusion detection system* — IDS) i w zaporach wdrożonych na całym świecie. Zakres tej edycji raportu jest nieco szerszy niż zazwyczaj — oprócz bardziej szczegółowej analizy ataków sieciowych zawiera on także analizę luk w zabezpieczeniach oraz dane o różnych formach niebezpiecznego kodu. Dzięki połączeniu tych zasobów, raport „Internet Security Threat” jest jedynym opracowaniem udostępniającym kompleksowy wgląd w problematykę ochrony danych. Przegląd ten opiera się na zasobach danych zgromadzonych przez firmę Symantec. Obejmują one jedno z największych na świecie repozytoriów danych o atakach na zabezpieczenia, najpełniejszą na świecie bazę danych o lukach w zabezpieczeniach oraz miliony przykładów niebezpiecznego kodu zgłoszonych przez klientów firmy Symantec korzystających z jej oprogramowania antywirusowego. Informacje te ułatwią kierownikom ds. informatyki zrozumienie specyfiki zmian zachodzących w zagrożeniach bezpieczeństwa oraz wpływu rozmaitych czynników na niebezpieczeństwa zagrażające ich firmom.

Z raportu tego wynika, że zagrożenia związane z korzystaniem z Internetu nasiliły się i zmieniły pod wieloma względami, pod innymi zaś pozostają relatywnie stabilne. Jeśli nie liczyć robaków i zagrożeń hybrydowych, liczba cyberataków po raz pierwszy nieco zmalała — w ciągu ostatnich sześciu miesięcy zanotowano jej spadek o 6% . Pomimo tej malejącej tendencji wiele firm, w tym

również z sektora usług finansowych, stwierdziło znaczny wzrost liczby ataków oraz skali ich następstw. Natomiast inne firmy, zwłaszcza korzystające z usług monitoringu zabezpieczeń, znacznie obniżyły poziom zagrożenia. Liczba ataków z podziałem na kraje, z których je przeprowadzono, nie uległa na ogół zmianie w porównaniu do wyników poprzednich badań. 80% ataków przeprowadzono z poziomu lub za pośrednictwem systemów zlokalizowanych zaledwie w 10 krajach. Krajem, w którym liczba ta była zdecydowanie największa, są Stany Zjednoczone.

Do zwiększenia ryzyka ataków przyczynił się dodatkowo znaczny wzrost liczby luk w zabezpieczeniach, wykrytych w ubiegłym roku w nowych produktach informatycznych. Łączna liczba nowych, udokumentowanych luk w zabezpieczeniach wykrytych w 2002 r. była o 81,5% wyższa niż w 2001 r. Luki wykryte w ubiegłym roku zaliczały się w zdecydowanej większości do defektów relatywnie niebezpiecznych. Ponadto około 60% tych udokumentowanych luk w zabezpieczeniach można było z łatwością wykorzystać, z uwagi na powszechną dostępność umożliwiających to zaawansowanych narzędzi lub z uwagi na to, że narzędzia takie wcale nie były potrzebne. W konsekwencji, korzystając z tak znacznej liczby luk w zabezpieczeniach, autorom złośliwego kodu udało się w ciągu ostatnich sześciu miesięcy opracować szereg skutecznych zagrożeń hybrydowych. Wiele spośród nich błyskawicznie, zaledwie

w ciągu kilku godzin od wprowadzenia w obieg, potrafi rozprzestrzenić się na wiele firm połączonych z Internetem. Kilka krąży w Internecie do dziś, infekując kolejne tysiące systemów na całym świecie.

Podsumowując — jest wiele oznak, że dla firm podłączonych do Internetu ryzyko ataku lub zainfekowania złośliwym kodem jest nadal bardzo duże. Możliwość pojawienia się całkiem nowych i potencjalnie jeszcze bardziej niszczących form złośliwego kodu oraz narzędzi ataku będzie stanowić ogromne ryzyko również w przyszłości. W dalszej części niniejszego raportu szczegółowo omówiono główne kierunki zmian zachodzących w tych zagrożeniach, a także najważniejsze związane z nimi problemy na przyszłość. Przedstawione dane pozwolą informatykom zapoznać się ze specyfiką stale zmieniających się zagrożeń związanych z korzystaniem z Internetu, co pozwoli opracowywać efektywniejsze strategie zabezpieczeń.

Najważniejsze fakty przedstawione w raporcie

W ciągu ostatnich sześciu miesięcy ogólny poziom zagrożenia wyrażający się liczbą cyberataków, luk w zabezpieczeniach i podatnością na nowe formy złośliwego kodu był nadal bardzo poważny, a specyfika tych zagrożeń ulegała ciągłym zmianom. W przypadku firm, które nie stosują właściwych środków zaradczych, zagrożenia te znacznie zwiększyły ryzyko kompromitacji. Konkretnie dane potwierdzające ten wniosek przedstawiono w tym rozdziale raportu w następujących podpunktach: „Specyfika cyberataków”, „Wykaz luk w zabezpieczeniach” i „Specyfika różnych form złośliwego kodu”.

SPECYFIKA CYBERATAKÓW

W ciągu ostatnich sześciu miesięcy częstotliwość ataków przeprowadzonych z sieci, nie licząc robaków i zagrożeń hybrydowych, zmalała w porównaniu z poprzednim półroczem o 6%.

- W ciągu ostatnich sześciu miesięcy notowano średnio 30 ataków na firmę w tygodniu, podczas gdy w poprzednim półroczu występowały 32 ataki na firmę w tygodniu.
- Około 85% tych działań zakwalifikowano jako rekonesans poprzedzający atak, pozostałe 15% — jako różne (również udane) formy prób wykorzystania luk w zabezpieczeniach.
- Pomimo spadku liczby ataków w okresie minionych sześciu miesięcy, średnia liczba ataków na firmę zanotowana w ciągu tego półrocza była o 20% wyższa od ich liczby zanotowanej w analogicznym okresie 2001 r.

Wskaźnik częstotliwości groźnych incydentów zanotowanych w ciągu ostatnich sześciu miesięcy był nieznacznie mniejszy niż w poprzednim półroczu.

- W ciągu ostatnich sześciu miesięcy 21% firm z losowo wybranej grupy doświadczyło co najmniej jednego groźnego incydentu, w porównaniu do 23% w poprzednim półroczu.
- Bieżący wskaźnik częstotliwości występowania groźnych incydentów jest znacznie niższy od zanotowanego w analogicznym półroczu 2001 r., gdy jego wartość wyniosła 43%.

Stwierdzono występowanie kilku istotnych schematów działania napastników,

związanych z przeprowadzaniem ataków w określonych przedziałach czasu.

- Liczba ataków i skala ich następstw były w soboty i niedziele znacznie niższe niż w ciągu pozostałych dni tygodnia, co potwierdza obserwacje z poprzedniego półrocza.
- Stwierdzono, że fluktuacje aktywności napastników są raczej funkcją czasu lokalnego obowiązującego w miejscach lokalizacji systemów atakujących, niż czasu lokalnego obowiązującego w miejscach lokalizacji ofiar ataku.
- Firmy połączone z Internetem notowały znaczny wzrost aktywności napastników w godzinach pomiędzy 12:00 a 21:00 czasu GMT (*Greenwich Mean Time*), niezależnie od lokalizacji i strefy czasowej poszczególnych sieci. Jest to prawdopodobnie efekt występowania kilku szczególnie aktywnych regionalnych źródeł ataków, osiągających szczytową aktywność w przybliżeniu w tym samym czasie.

Liczba odnotowanych ataków i skala ich następstw nadal różniły się w zależności od specyficznych cech firmy, w tym od branży, wielkości oraz czasu pracy.

- Częstotliwość ataków była najwyższa a skala ich następstw najpoważniejsza w przypadku firm z branży energetycznej.
- Firmy prowadzące działalność niedochodową odnotowały wzrost częstotliwości ataków, a firmy z sektora usług finansowych wzrost i skali ich następstw.
- Wzrost liczby ataków i skali ich następstw zaobserwowały także firmy zatrudniające dużą liczbę pracowników.
- Poziom zagrożenia firm malał w miarę zwiększania się zakresu monitorowania w czasie pracy. W firmach, które wykupiły te usługi na okres krótszy niż 12 miesięcy, wskaźnik groźnych incydentów osiągnął wartość 29%, natomiast w przypadku firm, które wykupiły je na okres dłuższy od 12 miesięcy, jego wartość wyniosła 17%.

Ogólny poziom intensywności ataków z podziałem na kraje, z których je zainicjowano, nie uległ w ciągu ostatnich miesięcy zmianom; stwierdzono jednak wystąpienie kilku istotnych zmian w aktywności tych działań¹

- Z 10 krajów będących źródłem największej liczby ataków wykonano 80% wszystkich ataków wykrytych w okresie ubiegłych sześciu miesięcy; największą liczbę ataków wykonano ze Stanów Zjednoczonych, skąd przeprowadzono 35,4% ogólnej ich liczby.
- Liczba ataków przeprowadzonych z Korei Południowej wzrosła w ciągu ostatnich miesięcy o 62%. Kraj ten znalazł się więc na drugiej pozycji pod względem ogólnej liczby przeprowadzonych z nich ataków oraz na pierwszej pozycji pod względem liczby ataków przypadających na 10 000 użytkowników Internetu wśród krajów tzw. pierwszej kategorii (*Tier One*)². Jednym z czynników będących przyczyną tej tendencji jest szybki rozwój na terenie Korei Południowej infrastruktury szerokopasmowej użytkowanej przez klientów indywidualnych. W miarę wzrostu dostępności infrastruktury szerokopasmowej w innych krajach może w nich również wzrosnąć poziom zagrożenia złośliwymi atakami komputerowymi i udział mieszkańców tych krajów w dokonywaniu takich ataków — o ile nie wyprzedzi się ich, wdrażając na szeroką skalę technologie zabezpieczające.
- Wysoki wskaźnik liczby ataków przypadających na 10 000 użytkowników Internetu zanotowano w kilku krajach Europy Wschodniej i Środkowej. Na drugiej i trzeciej pozycji znalazły się tu odpowiednio Polska i Czechy, zaliczające się do krajów kategorii pierwszej. Na liście krajów kategorii drugiej znalazły się: Rumunia, Łotwa, Litwa i Słowacja.

Firma Symantec nie stwierdziła w okresie ostatnich sześciu miesięcy żadnych możliwych do udowodnienia aktów cyberterroryzmu.

- Ataki przeprowadzone z krajów znajdujących się na liście potencjalnych cyberterrorystów (*Cyber Terrorist Watch List*) stanowiły mniej niż 1% ogólnej liczby zanotowanych ataków.

Przypadki nadużyć wewnętrznych stanowiły ponad 50% incydentów wymagających pomocy działu interwencji.

- Oprócz wzrostu ogólnej liczby ataków zewnętrznych, firmy samodzielnie oceniające poniesione szkody stwierdziły także szczególnie wiele nadużyć wewnętrznych.
- Wysoki poziom zniszczeń stwierdzonych przez firmy w połączeniu ze stosunkową prostotą środków, jakie stosowali ich sprawcy, należy potraktować jako sygnał ostrzegawczy, wskazujący na to jak ogromnie ważne jest zabezpieczenie się przed zagrożeniami z wewnątrz.

¹ Ustalenie „prawdziwego” źródła ataków jest niezwykle trudne. Napastnicy mogą przeskakiwać przez wiele systemów i krajów, zanim uderzą w zamierzony cel. Z tego względu dane przedstawione w tym rozdziale odnoszą się jedynie do lokalizacji ostatniego punktu, z którego wykonano uderzenie na cel.

² Pod względem liczby ataków na 10 000 użytkowników Internetu kraje podzielono na dwie kategorie. Do kategorii pierwszej (*Tier One*) zaliczono kraje, w których liczba użytkowników Internetu przekracza 1 mln, do kategorii drugiej zaś (*Tier Two*) — kraje, w których liczba ta mieści się w przedziale 100 tys. – 1 mln. Podział ten pozwala odróżnić kraje o dobrze rozwiniętej infrastrukturze internetowej od krajów, w których infrastruktura ta dopiero się tworzy.

SPECYFIKA LUK W ZABEZPIECZENIACH

W ubiegłym roku Symantec udokumentował wykrycie 2524 nowych luk w zabezpieczeniach, co oznacza wzrost w stosunku do 2001 r. o 81,5%

- W ubiegłym roku Symantec wpisywał do swoich rejestrów średnio 7 nowych luk w zabezpieczeniach dziennie.
- Do potencjalnych przyczyn wzrostu liczby ujawnionych luk w zabezpieczeniach można zaliczyć pojawienie się ruchu znanego pod nazwą „Responsible disclosure” (ruch na rzecz odpowiedzialnego ujawniania luk w zabezpieczeniach), pojawienie się kilku nowych metod wykorzystywania błędów w oprogramowaniu i zwiększone zainteresowanie mediów osobami zajmującymi się wykrywaniem luk w zabezpieczeniach.

Wzrost liczby luk wykrytych w zabezpieczeniach jest także efektem znacznego wzrostu liczby średnio lub bardzo niebezpiecznych luk.

- Ogólna liczba średnio lub bardzo niebezpiecznych luk udokumentowanych w 2002 r. była o 84,7% wyższa niż w 2001 r. Dla porównania liczba niegroźnych luk w zabezpieczeniach była tylko o 24% wyższa niż w 2001 r.
- Najistotniejszym czynnikiem leżącym u podstaw tej tendencji wydaje się być szybkie tempo opracowywania i wdrażania użytkowanych zdalnie aplikacji internetowych.

Relatywna łatwość, z jaką napastnicy mogli wykorzystywać nowe luki w zabezpieczeniach nie uległa zmianie w ciągu ostatniego roku.

- Około 60% nowych luk w zabezpieczeniach można było łatwo wykorzystać, gdyż nie wymagały użycia specjalnego kodu lub wymagany specjalny kod był powszechnie dostępny.
- Jednakże, o ile w 2001 r. kod pozwalający na wykorzystanie luki w zabezpieczeniach był dostępny do 30% tych luk, których wykorzystanie wymagało użycia specjalnego kodu, to w 2002 r. kod taki był dostępny do 23,7% luk tego rodzaju.

Sądząc z luk w zabezpieczeniach wykrytych w 2002 r., pojawiła się pewna liczba luk stanowiących poważne zagrożenie na przyszłość, które napastnicy i autorzy niebezpiecznego kodu dopiero zaczynają wykorzystywać.

- Znane zagrożenia hybrydowe wykorzystują jedynie niewielką część udokumentowanych obecnie luk w zabezpieczeniach. Z uwagi na fakt, że dawne zagrożenia hybrydowe skutecznie wykorzystywały luki w zabezpieczeniach znane już od kilku miesięcy, można sądzić, że wiele spośród ostatnio wykrytych luk w stanowi bardzo prawdopodobny cel zagrożeń, które pojawią się w przyszłości.
- W ciągu ostatniego roku zaatakowano z ukrycia wiele aplikacji z otwartym dostępem do kodu źródłowego, wprowadzając do nich konie trojańskie. Zaatakowane przy tym zostały [wysokiej klasy witryny dystrybucyjne], w których zabezpieczenie włożono bardzo wiele wysiłku. Może to stanowić ostrzeżenie nie tylko dla innych projektów z otwartym dostępem do kodu źródłowego, ale i dla producentów oprogramowania komercyjnego. Zamiast koncentrować się na pojedynczych systemach, napastnicy ewidentnie poszukują nowych sposobów na zaatakowanie dużej liczby systemów w krótkim czasie.
- W ciągu kolejnego roku należy uważnie obserwować luki w zabezpieczeniach klientów internetowych, zwłaszcza gdy mają one wpływ na przeglądarkę Internet Explorer firmy Microsoft. Liczba tych luk oraz skala ich następstw znacznie się w ubiegłym roku zwiększyły.

SPECYFIKA RÓŻNYCH FORM ZŁOŚLIWEGO KODU

Największe niebezpieczeństwo dla społeczności użytkowników Internetu nadal stanowią zagrożenia hybrydowe³

- Przyczyną prawie 80% zgłoszeń dotyczących złośliwego kodu przekazanych w ciągu ostatnich sześciu miesięcy do działu interwencji firmy Symantec (*Symantec Security Response*) były trzy hybrydy (znane pod nazwami Klez, Bugbear i Opaserv).
- Ponadto znaczny procent cyberataków wykrytych przez dział usług zabezpieczeń zarządzanych firmą Symantec (*Symantec Managed Security Services*) spowodowało zaledwie kilka zarówno starych jak i nowych hybryd, w tym Bugbear, Nimda i Code Red.
- Z uwagi na fakt, że ostatnie formy niebezpiecznego kodu, takie jak Bugbear, skutecznie korzystały z luk w zabezpieczeniach znanych już od co najmniej miesiąca, wydaje się, że społeczność użytkowników Internetu jako całość jest nadal bardzo podatna na zagrożenia hybrydowe wykorzystujące do rozprzestrzeniania się znane luki w zabezpieczeniach.

W ciągu ostatniego półrocza zmieniły się kierunki infekowania (metody rozprzestrzeniania) i ulubione metody przeciążania systemów.

- Zanotowano znaczny wzrost liczby samoreplikujących się masowo wiadomości przesyłanych pocztą elektroniczną. Tego typu charakter miało osiem spośród 50 najpoważniejszych zagrożeń zgłoszonych w ciągu ostatnich sześciu miesięcy, podczas gdy w analogicznym okresie 2001 r. zgłoszono tylko 1 tego typu zagrożenie.

- W ciągu ostatniego półrocza wzrosła także znacznie liczba zgłoszeń złośliwego kodu wykradającego należące do użytkowników poufne informacje. Możliwość ujawniania sekretów handlowych, cennych informacji finansowych i innych danych będących własnością firmy może radykalnie zwiększyć niebezpieczeństwo potencjalnych strat.

Technologie wkraczające właśnie na rynek masowy stanowią źródło wyjątkowo atrakcyjnych możliwości dla autorów niebezpiecznego kodu.

- Intensywna penetracja rynku oraz coraz częstsze nieuprawnione korzystanie z aplikacji do natychmiastowego przesyłania wiadomości oraz z aplikacji do komunikacji równorzędnej (*peer-to-peer* — P2P) powoduje, że stanowią one atrakcyjny kierunek infekowania dla przyszłych zagrożeń hybrydowych.
- W latach 2003 i 2004 oczekuje się znacznego rozpowszechnienia się na rynku urządzeń bezprzewodowych. Urządzenia te, często wyposażone w stosunkowo słabe zabezpieczenia, stanowią wyjątkowo atrakcyjnym kierunkiem infekowania niebezpiecznym kodem.

³ Zagrożenia hybrydowe łączą w sobie cechy wirusów, robaków, koni trojańskich oraz niebezpiecznego kodu, wykorzystując luki w zabezpieczeniach serwerów i Internetu do inicjowania, przenoszenia i nasilania ataków. Dzięki wykorzystaniu wielu metod i technik zagrożenia hybrydowe najczęściej szybko się rozprzestrzeniają i powodują rozległe szkody.