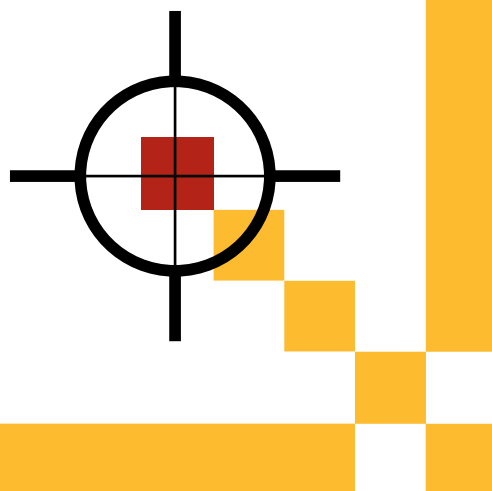


RAPORT O ZAGROŻENIACH BEZPIECZEŃSTWA WITRYN INTERNETOWYCH

Wiadomości z raportu firmy
Symantec o zagrożeniach
bezpieczeństwa pochodzących
z Internetu

Opublikowano w maju 2012 r.

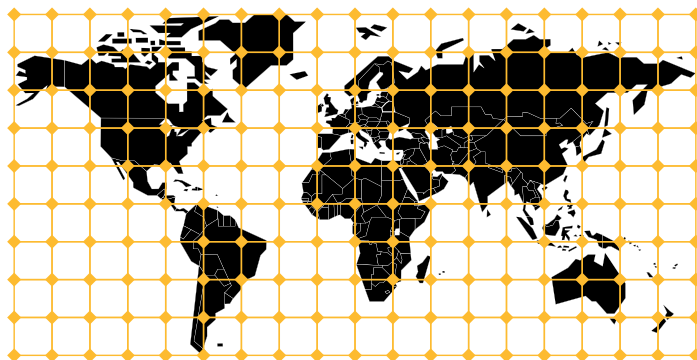


SPIS TREŚCI

Wprowadzenie	3	Wnioski: co nas czeka w roku 2012	16
Rok 2011 miesiąc po miesiącu	4	Zalecane rozwiązania dla firm	17
Rok 2011 w liczbach	7	Zalecane rozwiązania dla użytkowników indywidualnych	20
Streszczenie	8	Dodatkowe informacje	22
Ataki na podmioty certyfikujące	9	Przypisy	23
Tendencje związane ze szkodliwym kodem	10	Informacje o firmie Symantec	24
Szkodliwe oprogramowanie w roku 2011	10		
Szkodliwe oprogramowanie w witrynach internetowych	11		
Szkodliwe oprogramowanie rozprzestrzeniające się pocztą e-mail	12		
Niebezpieczne witryny internetowe	13		
Wykorzystywanie luk w sieci WWW: zestawy narzędzi do ataków, narzędzia typu rootkit i zagrożenia związane z witrynami społecznościowymi	14		
Budowanie wiarygodności i ochrona wrażliwych obszarów	15		

RYSUNEK

<i>Rysunek 1</i> Średnia liczba szkodliwych witryn internetowych wykrywanych dziennie w 2011 r.	11
<i>Rysunek 2</i> Kategorie najbardziej niebezpiecznych witryn w 2011 r.	12
<i>Rysunek 3</i> Proporcje szkodliwego oprogramowania w ruchu e-mail w 2011 r.	13



Wprowadzenie

Firma Symantec stworzyła jedno z najbardziej wyczerpujących na świecie źródeł informacji na temat zagrożeń bezpieczeństwa pochodzących z Internetu. Jest ono oparte na globalnej sieci Symantec™ Global Intelligence Network, złożonej z ponad 64,6 miliona czujników ataków i rejestrującej tysiące zdarzeń na sekundę. Sieć ta monitoruje występowanie ataków w ponad 200 krajach i regionach przy użyciu produktów i usług firmy Symantec – takich jak Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services i produkty Norton™ dla klientów indywidualnych – a także zewnętrznych źródeł danych.

Ponadto firma Symantec ma jedną z najobszerniejszych na świecie baz danych dotyczących luk w zabezpieczeniach, zawierającą ponad 47 662 luk wykrytych (w ponaddwudziestoletnim okresie) w przeszło 40 006 produktach ponad 15 967 producentów.

Dane dotyczące spamu, phishingu i szkodliwego oprogramowania są rejestrowane za pośrednictwem różnych źródeł, na przykład sieci Symantec Probe Network (system ponad 5 milionów fikcyjnych kont), usług Symantec.cloud oraz szeregu innych rozwiązań firmy Symantec z dziedziny zabezpieczeń. Skeptic™, własna technologia heurystyczna stosowana w usługach Symantec.cloud, jest w stanie wykrywać nowe, zaawansowane ataki ukierunkowane, zanim osiągną sieci klientów. Każdego dnia w 15 centrach danych jest przetwarzanych ponad 8 miliardów wiadomości e-mail i ponad 1,4 miliarda żądań dostępu do sieci WWW. Ponadto firma Symantec gromadzi informacje dotyczące phishingu – za pośrednictwem rozbudowanej wspólnoty przedsiębiorstw, producentów rozwiązań z dziedziny zabezpieczeń i ponad 50 milionów użytkowników indywidualnych, stworzonej w celu zwalczaniem oszustw.

Zasoby te stanowią niezastąpione źródła danych dla analityków firmy Symantec. Umożliwiają wykrywanie, analizowanie i kompetentne omawianie rodzących się trendów w zakresie ataków, aktywności szkodliwego kodu, phishingu oraz spamu. Efektem jest coroczny raport firmy Symantec o zagrożeniach bezpieczeństwa pochodzących z Internetu, *Internet Security Threat Report*, który dostarcza przedsiębiorstwom i klientom indywidualnym informacji niezbędnych do skutecznej ochrony systemów zarówno obecnie, jak i w przyszłości.

Niniejsza skrócona wersja tego raportu została opracowana przede wszystkim z myślą o problematyce zabezpieczeń witryn internetowych. Pełna wersja raportu *Internet Security Threat Report* jest dostępna do pobrania [tutaj](#).

ROK 2011 MIESIĄC PO MIESIĄCU



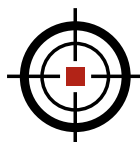
**ZAGROŻENIA
DLA URZĄDZEŃ
PRZENOŚNYCH**



ATAKI HAKERÓW



**ELIMINACJA
BOTNETÓW**



**UKIERUNKOWANE
ZAGROŻENIA**



**SPAM, PHISHING
I 419**



**WITRYNY
SPOŁECZNOŚCIOWE**

STYCZEŃ



W nienadzorowanych sklepach z oprogramowaniem do systemu Android pojawiają się aplikacje z koniem trojańskim typu „tylne wejście” o nazwie Android.Geinimi.



Robak podszywający się pod indonezyjską aplikację na Facebooka zostaje wykorzystany do kradzieży poświadczeń logowania.



Oszuści wykorzystują powódź w Serranie w Brazylii w celu wyłudzenia datków, które rzekomo mają trafić do powodzian.

LUTY



Firma HBGary Federal, specjalizująca się w zabezpieczeniach internetowych, zostaje zhakowana przez grupę Anonymous.



W nienadzorowanych sklepach z oprogramowaniem do systemu Android pojawia się kolejny koń trojański typu „tylne wejście”, Android.Pjapps.



Spamerzy wykorzystują zamieszki w Egipcie i Libii dla celów oszustwa 419 (tzw. nigeryjskiego szwindlu) i ataków ukierunkowanych.

MARZEC



Microsoft Firma Microsoft we współpracy z amerykańskimi organami ścigania eliminuje botnet Rustock.



W oficjalnym sklepie Android Market pojawia się koń trojański Android.Rootcager.



Spamerzy wykorzystują trzęsienie ziemi w Japonii dla celów oszustwa 419, tworzenia fałszywych witryn do wpłacania datków oraz wysyłania szkodliwych załączników.



Hakerzy wykorzystują narzędzie firmy Google do usuwania konia trojańskiego Android.Rootcager i udostępniają go z nowym koniem trojańskim, Android.Bgserv.



Zostają zhakowane podmioty rejestrujące firmy Comodo, InstantSSL.it oraz GlobalTrust.it. Zostają utworzone fałszywe certyfikaty dla domen Google, Hotmail, Yahoo!, Skype i Mozilla.

KWIECIEŃ



Firma Sony wykrywa zhakowanie serwisu Playstation Network. Usługa zostaje wyłączona do czasu przywrócenia zabezpieczeń.



Iran twierdzi, że padł ofiarą kolejnego ataku podobnego do robaka Stuxnet – „Stars”.



Zostaje wykryte szkodliwe oprogramowanie rejestrujące aplikacje przeznaczone na Facebooka.



FBI uzyskuje sądowy nakaz wyłączenia botnetu Coreflood przez wysłanie polecenia „delete” (wpisanego w oprogramowanie bota) do zaatakowanych komputerów.



Spamerzy i handlarze oprogramowaniem FakeAV wykorzystują ślub w brytyjskiej rodzinie królewskiej do kampanii i ataków typu SEO poisoning.

MAJ



Atak z użyciem skryptów generuje zaproszenia na Facebooku.



Śmierć Osamy bin Ladena wywołuje falę ataków przy użyciu szkodliwego oprogramowania i phishingu.



Pojawia się grupa hakerów LulzSec z hasłem „we're in it for the »LULZ«” („robimy to dla śmiechu”).



Okazuje się, że spamerzy tworzą własne usługi skracania adresów URL.



Na Facebooku rozprzestrzenia się kampania spamowa związana z funkcją oznaczania.



Tokeny Facebooka wyciekają do osób trzecich za pośrednictwem aplikacji.



Zostaje wydana/wycieka darmowa wersja popularnego zestawu narzędzi Blackhole służącego do wykorzystywania luk w zabezpieczeniach.

CZERWIEC



Grupa LulzSec hakuje systemy firmy Black & Berg Cybersecurity Consulting i odmawia przyjęcia oferowanej wcześniej „nagrody” w wysokości 10 000 dolarów.



Grupa LulzSec hakuje systemy Senatu Stanów Zjednoczonych, CIA i spółek współpracujących z FBI w odpowiedzi na zapowiedź rządu Stanów Zjednoczonych, że cyberataki mogą być postrzegane jako działania wojenne.



Rozpoczyna się akcja AntiSec; hakerzy są zachęceni do atakowania rządowych witryn internetowych i publikowania znalezionych danych.



Grupa LulzSec pada ofiarą ataku ze strony hakera th3j35t3r z grupy TeaMp0isoN, którego zdaniem LulzSec nie zasługuje na tak duże zainteresowanie.



Zostaje zhakowana usługa wymiany walut w systemie waluty wirtualnej Bitcoin.



Zostaje zhakowany podmiot certyfikujący DigiNotar, co skutkuje upadkiem firmy.

LIPIEC



Microsoft oferuje 250 000 dolarów nagrody za informacje, które doprowadzą do aresztowania twórców botnetu Rustock.



Śmierć Amy Winehouse zostaje wykorzystana do rozprzestrzenienia wirusa Infostealer.Bancos.

SIERPIEŃ



Zostaje wykryty koń trojański Trojan. Badminer, przenoszący obciążenia związane z generowaniem („wydobyciem”) waluty wirtualnej Bitcoin na kartę graficzną.



Występują ataki typu phishing zawierające fałszywe pieczęcie z potwierdzeniem wiarygodności.

WRZESIEŃ



Spamerzy wykorzystują dziesiątą rocznicę ataku terrorystycznego z 11 września do masowego zbierania adresów e-mail.



Wybuch bomby w New Delhi zostaje wykorzystany do spamu farmaceutycznego.



Microsoft wyłącza botnet Kelihos.

PAŹDZIERNIK



Dochodzi do oficjalnego wykrycia konia trojańskiego W32.Duqu. Być może jest to zagrożenie nagłaśniane przez Iran w kwietniu.



Atakujący stojący za udostępnieniem zestawu narzędzi do ataków Blackhole rozpoczynają kampanię spamową związaną ze śmiercią Steve'a Jobsa.



Zostaje opublikowany artykuł przeglądowy „Nitro Attacks” („Ataki Nitro”) z opisami ataków ukierunkowanych na firmy z sektora chemicznego.



Według raportu Microsoft Security Intelligence Report (zeszyt 11) Java jest oprogramowaniem najczęściej wykorzystywanym przez hakerów, wyprzedzając pod tym względem produkty firm Adobe i Microsoft.



Śmierć libijskiego przywódcy Muammara al-Kaddafiego prowadzi do kampanii spamowej rozprzestrzeniającej szkodliwe oprogramowanie.



Na Facebooku zostają wykryte ataki z wykorzystaniem technologii tokenów anti-CSRF.

GRUDZIEŃ



Zostaje zhakowana firma Stratfor, zajmująca się analizami geopolitycznymi.



Ilość spamu spada do najniższego poziomu od 3 lat.

ROK 2011 W LICZBACH

5,5 MLD

ZABLOKOWANYCH ATAKÓW W 2011 R.

ATAKI NA WITRYNY BLOKOWANE CODZIENNIE

VS.
3 MLD W 2010 R.

4,595

62

MLD W 2010 R.

SZACOWANA
SKALA
DZIENNEGO
SPAMU
NA ŚWIECIE

42

MLD W 2010 R.

1,1
MLN

TOŻSAMOŚCI
UJAWNIONYCH
NA
SKUTECZNY
ATAK

1
NA
299

OGÓLNY
WSPÓŁCZYNNIK
PHISHINGU



Streszczenie

W 2011 roku firma Symantec zablokowała ponad 5,5 miliarda ataków z użyciem szkodliwego oprogramowania¹; co oznacza wzrost o ponad 81% w stosunku do poprzedniego roku. Wzrost ten był w znacznej mierze spowodowany gwałtownym zwiększeniem liczby ataków z użyciem polimorficznego szkodliwego oprogramowania, zwłaszcza narzędzi do ataków na witryny internetowe, oraz ataków z użyciem socjotechniki wykorzystujących szkodliwe oprogramowanie rozprzestrzeniane pocztą e-mail. Ataki ukierunkowane wykorzystujące luki „zero-day” były potencjalnie najbardziej podstępne ze wszystkich. W przypadku ataku ukierunkowanego ofiara właściwie nie ma szans na zorientowanie się, że jest celem hakerów, ponieważ ze swej definicji atak ten ma być niemożliwy do wykrycia przez system obronny. W odróżnieniu od dotychczasowych przewlekłych problemów w 2011 roku głośno było o atakach ukierunkowanych, atakach dokonywanych przez hakywistów motywowanych politycznie, naruszeniach integralności danych i atakach na podmioty certyfikujące.

Podmioty certyfikujące i protokół Transport Layer Security (TLS) 1.0 celem ataków w miarę upowszechniania się certyfikatów SSL

Głośne ataki na podmioty certyfikujące, czyli dostawców certyfikatów Secure Sockets Layer (SSL), stanowią zagrożenie dla systemów, które same są gwarancją wiarygodności w Internecie. Jednak w przypadku włamania do firmy DigiNotar i podobnych przypadków działalności hakerów słabym punktem nie była technologia SSL. Ataki te zwróciły uwagę na to, że firmy funkcjonujące w łańcuchu dostaw podmiotu certyfikującego bezwzględnie muszą wzmocnić swoją infrastrukturę oraz wdrożyć bardziej rygorystyczne procedury i zasady zabezpieczeń. Strategia wykorzystywania luk w zabezpieczeniach opartego na szkodliwym oprogramowaniu w przypadku protokołu TLS 1.0 uwydatniła konieczność uaktualnienia systemów SSL do nowszej wersji protokołu TLS, na przykład TLS 1.2 lub późniejszej. Właściciele witryn internetowych dostrzegli potrzebę szerszego stosowania certyfikatów SSL w celu zwalczania ataków typu „man-in-the-middle”, a zwłaszcza do zabezpieczania stron nietransakcyjnych. Przykładem są zawsze aktywne certyfikaty SSL (Always On SSL) wprowadzone w witrynach firm Facebook, Google, Microsoft i Twitter.²

Ataki na podmioty certyfikujące

W 2011 roku ofiarą wielu ataków padły podmioty certyfikujące, które wystawiają certyfikaty SSL ułatwiające szyfrowanie i uwierzytelnianie witryn internetowych oraz innych usług udostępnianych w Internecie.

Oto kilka wartych odnotowania przykładów ataków na podmioty certyfikujące z 2011 roku:



MARZEC

- 1** W wyniku ataku zostają przechwycone poświadczenia dostępu partnera firmy Comodo w Włoszech. Uprawnienia partnera wykorzystano do wygenerowania fałszywych certyfikatów SSL³.

MAJ

- 2** Zostaje zhakowany następny partner firmy Comodo: ComodoBR z Brazylii⁴.

CZERWIEC

- 3** Dochodzi do bezskutecznego ataku na firmę StartCom, podmiot certyfikujący oferujący certyfikaty StartSSL⁵.
- 4** Zostaje zhakowana firma Diginotar. Hakerzy początkowo nie wystawiają żadnych certyfikatów⁶.

LIPIEC

- 5** Podczas wewnętrznej kontroli zostaje wykryte włamanie do infrastruktury firmy DigiNotar, wskazujące na naruszenie bezpieczeństwa jej kluczy kryptograficznych. Wskutek zhakowania systemów firmy DigiNotar zostają wystawione fałszywe certyfikaty, między innymi dla domen firmy Google, dodatków przeglądarki Mozilla i usługi Microsoft Update⁷.

SIERPIEŃ

- 6** Zostają wykryte niekontrolowane certyfikaty wystawione po złamaniu zabezpieczeń systemów firmy DigiNotar. Do ataków na firmy Comodo i DigiNotar przyznaje się haker ComodoHacker, który utrzymuje, że włamał się również do systemów innych podmiotów certyfikujących. Haker twierdzi, że pochodzi z Iranu.

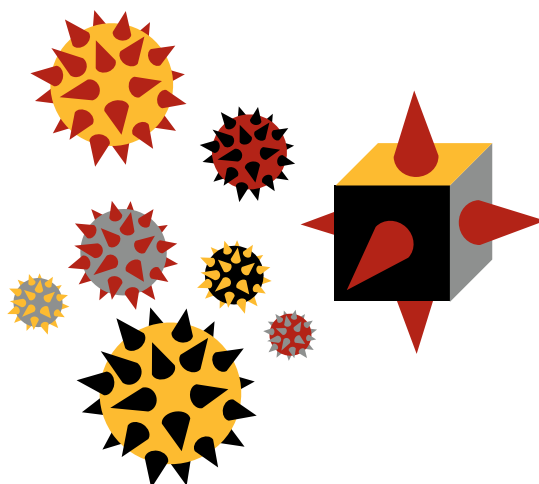
WRZESIEŃ

- 7** Analitycy zabezpieczeń pokazują „Browser Exploit Against SSL/TLS” (BEAST)⁸, technikę umożliwiającą wykorzystanie luki w zabezpieczeniach technologii szyfrowania TLS 1.0, standardu używanego przez przeglądarki, serwery i podmioty certyfikujące.
- 8** Dochodzi do ataku na firmę GlobalSign. Nie udaje się włamać do systemów tego podmiotu certyfikującego; zostaje zhakowany jedynie jego serwer WWW¹⁰. Również do tego ataku przyznaje się ComodoHacker.
- 9** Rząd holenderski i inni klienci firmy Diginotar niespodziewanie muszą wymienić wszystkie jej certyfikaty, ponieważ producenci najpopularniejszych przeglądarek internetowych usunęli Diginotar ze swoich magazynów zaufanych certyfikatów głównych¹¹. Firma DigiNotar składa wniosek o ogłoszenie upadłości.

LISTOPAD

- 10** Digicert Sdn. Bhd. (Digicert Malaysia), podmiot certyfikujący podlegający firmie Entrust (i niemający nic wspólnego z dobrze znanym podmiotem certyfikującym Digicert Inc.), wystawia certyfikaty zabezpieczone słabymi kluczami prywatnymi i pozbawione odpowiednich rozszerzeń użycia oraz informacji dotyczących odwołania. Z tego powodu firmy Microsoft, Google i Mozilla usuwają certyfikaty główne firmy Digicert Malaysia ze swoich magazynów zaufanych certyfikatów głównych¹². Przyczyną incydentu jest nie działalność hakerska, lecz nieodpowiednie procedury bezpieczeństwa firmy Digicert Sdn. Bhd.

Wszystkie te wydarzenia dowiodły, że podmioty certyfikujące są różne. Podniosły one poprzeczkę dla podmiotów certyfikujących i spowodowały konieczność utrzymywania wysokiego poziomu zabezpieczeń w całej branży. Z perspektywy firm widać wyraźnie, jak wiele znaczy wybranie wiarygodnego, dobrze zabezpieczonego podmiotu certyfikującego. I wreszcie użytkownicy indywidualni przekonali się, że powinni używać zaktualizowanych przeglądarek i staranniej sprawdzać, czy w odwiedzanych przez nich witrynach są stosowane certyfikaty SSL wystawione przez znane, wiarygodne podmioty certyfikujące. W rozdziale poświęconym zalecanym rozwiązaniom pod koniec raportu zamieszczamy wskazówki dla obu grup.



Tendencje związane ze szkodliwym kodem

Szkodliwe oprogramowanie w roku 2011

Analizując szkodliwy kod, można ustalić, jakiego rodzaju zagrożenia i techniki ataków wykorzystano. Punkt końcowy jest często ostatnią linią obrony, ale często może być też pierwszą linią obrony przed atakami dokonywanymi z wykorzystaniem pamięci USB, niezabezpieczonych połączeń sieciowych i zhakowanych, zainfekowanych witryn internetowych. Również technologia oparta na chmurze oraz systemy oceny reputacji oferowane przez firmę Symantec mogą pomóc w wykrywaniu i blokowaniu nowych, dotąd niestosowanych ataków, takich jak nowe ataki ukierunkowane z wykorzystaniem wcześniej nieznanymi luk „zero-day”. Analiza tendencji dotyczących aktywności szkodliwego oprogramowania zarówno w chmurze, jak i punktach końcowych, może pomóc wyjaśnić szerszą naturę zagrożeń czyhających na firmy, zwłaszcza ataków hybrydowych i zagrożeń dla pracowników mobilnych.

Stany Zjednoczone, Chiny i Indie pozostały najczęstszymi źródłami szkodliwych działań, proporcjonalnie do dużych populacji użytkowników Internetu. W porównaniu z rokiem 2010 ogólna średnia częstotliwość ataków podejmowanych z obszaru Stanów Zjednoczonych wzrosła o 1 punkt procentowy, tymczasem w Chinach zmalała o 10 punktów procentowych.

Stany Zjednoczone były głównym źródłem wszelkich działań, z wyjątkiem obszarów szkodliwego kodu i zombi rozsyłających spam, w których pierwsze miejsce zajęły Indie. Około 12,6% aktywności botów ma swoje źródło w Stanach Zjednoczonych, podobnie jak 33,5% ataków na witryny internetowe, 16,7% ataków sieciowych i 48,5% witryn służących do phishingu.

Szkodliwe oprogramowanie w witrynach internetowych

Dla użytkowników indywidualnych i firm nadal duże wyzwanie stanowią ataki typu „drive-by” (pobieranie bez wiedzy użytkownika). Leżą one u podłoża setek milionów prób infekcji podejmowanych każdego roku. Do takiego ataku dochodzi, kiedy użytkownik odwiedza witrynę zawierającą szkodliwe oprogramowanie. Może się tak zdarzyć, gdy użytkownik kliknie łącze w wiadomości e-mail lub witrynie społecznościowej albo podczas wizyty w wiarygodnej, ale zainfekowanej witrynie.

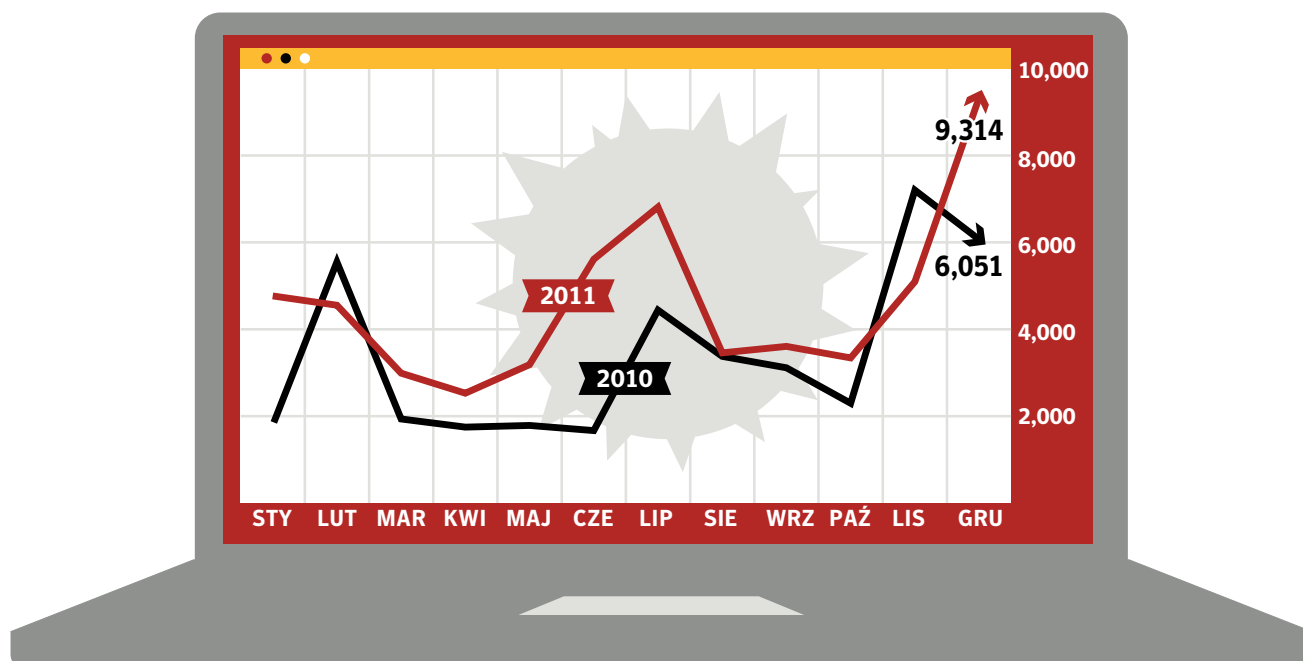
Atakujący stale zmieniają swoje techniki i obecnie stosują bardzo wyrafinowane metody. Nieprzekonujące wiadomości e-mail z błędami ortograficznymi odeszły w przeszłość. Zostały zastąpione przez takie techniki jak „clickjacking” czy „likejacking”, w których użytkownik odwiedza witrynę internetową, aby obejrzeć dobrze się zapowiadający filmik, a kliknięcie to powoduje opublikowanie komentarza widocznego dla wszystkich znajomych tego użytkownika na Facebooku, co skłania ich do kliknięcia tego samego szkodliwego łącza.

W odpowiedzi na Facebooku został wdrożony system „Clickjacking Domain Reputation System” (system oceny reputacji domen pod kątem clickjackingu), dzięki czemu udało się wyeliminować mnóstwo ataków typu clickjacking – w przypadku domen uznanych za niewiarygodne system prosi użytkownika o potwierdzenie zamiaru opublikowania informacji o kliknięciu „Lubię to”.

Na podstawie danych z Norton Safe Web¹³ – rozwiązania firmy Symantec skanującego Internet w poszukiwaniu witryn zawierających szkodliwe oprogramowanie – ustaliliśmy, że 61% szkodliwych witryn to w rzeczywistości zwykłe witryny internetowe zainfekowane szkodliwym kodem.

Rysunek 1

Średnia liczba szkodliwych witryn internetowych wykrywanych dziennie w 2011 r.



Source: Symantec.cloud

Niebezpieczne witryny internetowe

Rysunek 2

Kategorie najbardziej niebezpiecznych witryn w 2011 r.

Miejsce	10 najczęściej atakowanych witryn internetowych według kategorii		% ogólnej liczby zainfekowanych witryn
1	Blogi / witryny społecznościowe		 19.8%
2	Hosting / prywatne witryny w hostingu		 15.6%
3	Biznes / ekonomia		 10.0%
4	Sklepy internetowe		 7.7%
5	Edukacja / źródła wiedzy		 6.9%
6	Komputery i Internet		 6.9%
7	Rozrywka i muzyka		 3.8%
8	Motoryzacja		 3.8%
9	Zdrowie i opieka medyczna		 2.7%
10	Pornografia	XXX	 2.4%

Source: Symantec

Warto zauważyć, że witryny z treściami dla dorosłych/pornografią znajdują się nie w pierwszej piątce, lecz dopiero na dziesiątym miejscu. Pełną listę przedstawia rysunek 2.

Co więcej, w przypadku witryn o tematyce religijnej i ideologicznej występuje średnio trzy razy więcej zagrożeń przypadających na zainfekowaną witrynę niż w przypadku witryn dla dorosłych/pornograficznych. Naszym zdaniem może tak być, ponieważ właściciele witryn pornograficznych zarabiają w Internecie, w związku z czym są zainteresowani tym, by w ich witrynach nie było szkodliwego oprogramowania – nie sprzyja ono utrzymaniu klientów.

W 2011 roku funkcja skanowania witryn internetowych na obecność szkodliwego oprogramowania oferowana przez Symantec VeriSign¹⁴ sprawdziła ponad 8,2 miliarda adresów URL pod kątem zainfekowania szkodliwym oprogramowaniem. Około 1 na 156 witryn zawierało szkodliwe oprogramowanie. Witryny internetowe mające luki w zabezpieczeniach są bardziej narażone na infekcje szkodliwym oprogramowaniem, toteż od października 2011 roku firma Symantec udostępnia swoim klientom wykupującym certyfikaty SSL usługę oceny luk w zabezpieczeniach witryny. Od października do końca roku firma Symantec stwierdziła, że 35,8% witryn miało co najmniej jedną lukę w zabezpieczeniach, a w przypadku 25,3% wykryto co najmniej jedną poważną lukę.

Szkodliwe oprogramowanie rozprzestrzeniające się pocztą e-mail

W 2011 roku wzrosła proporcja szkodliwych wiadomości e-mail w stosunku do całkowitego ruchu e-mail. Największy wzrost odnotowano w dużych firmach (zatrudniających ponad 2500 osób), w których wskaźnik ten osiągnął poziom 1 na 205,1. W przypadku małych i średnich firm (zatrudniających do 250 osób) jako szkodliwą zidentyfikowano 1 na 267,9 wiadomości e-mail.

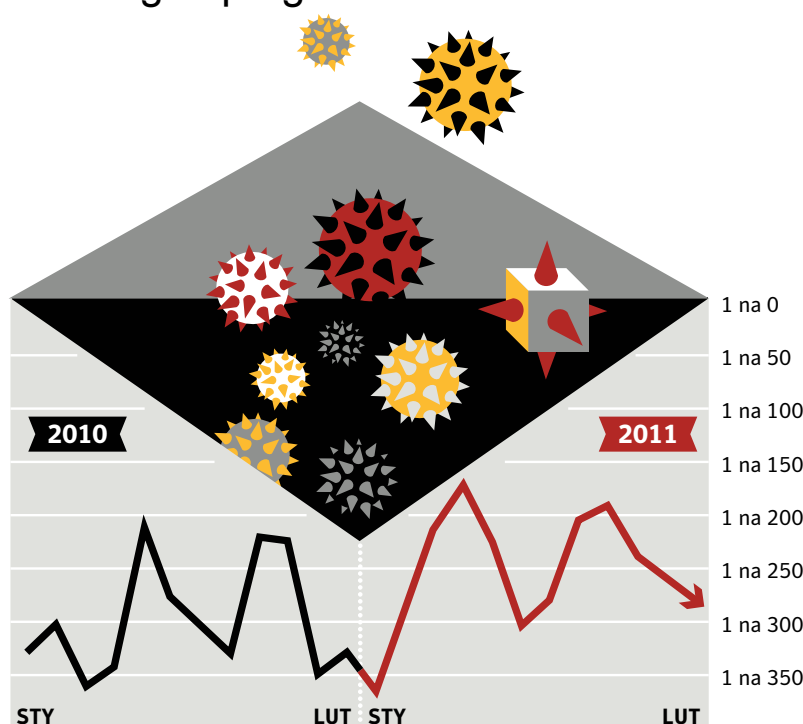
Przestępcy maskują szkodliwe oprogramowanie zawarte w wiadomościach e-mail przy użyciu różnego rodzaju załączników, na przykład plików PDF i dokumentów Microsoft Office. Wiele z tych załączonych plików zawiera szkodliwy kod, który wykorzystuje luki w zabezpieczeniach aplikacji otwierającej załączniki danego typu, a w co najmniej dwóch z tych ataków wykorzystano luki typu „zero-day” programu Adobe Reader.

Twórcy szkodliwego oprogramowania stosują metody socjotechniczne, aby zwiększyć liczbę kliknięć zainfekowanych załączników. Na przykład niedawno zastosowano w atakach wiadomości wyglądające na wysłane przez znane firmy kurierskie w sprawie niedostarczonych przesyłek. W innym przypadku wiadomości e-mail zawierały informację, że załączniki są skanami oraz kopiami ze skanerów i kserokopierek podłączonych do sieci. Stara rada, żeby nie klikać nierozpoznanych załączników, jest niestety wciąż aktualna.

Z dalszych analiz wynika, że 39,1% szkodliwych wiadomości e-mail zawiera hiperłącza prowadzące do szkodliwego kodu, a nie załącznik ze szkodliwym kodem. To znaczny wzrost w stosunku do 23,7% odnotowanych w 2010 roku. Jest to też dodatkowy sygnał, że cyberprzestępcy próbują obejść zabezpieczenia przez zmianę techniki ataku z samej poczty e-mail na wykorzystanie Internetu.

Rysunek 3

Proporcje szkodliwego oprogramowania w ruchu e-mail w 2011 r.



Wykorzystywanie luk w sieci WWW: zestawy narzędzi do ataków, narzędzia typu rootkit i zagrożenia związane z witrynami społecznościowymi

Zestawy narzędzi do ataków, które umożliwiają tworzenie nowego szkodliwego oprogramowania i przygotowywanie ataków bez pisania oprogramowania od podstaw, są stosowane w niemal dwóch trzecich (61%) aktywnych zagrożeń w szkodliwych witrynach internetowych. Ponieważ zestawy te stają się coraz powszechniejsze, skuteczniejsze i łatwiejsze w obsłudze, można się spodziewać, że ta liczba jeszcze wzrośnie. Do takich zestawów szybko dołączane są nowe narzędzia do wykorzystywania luk w zabezpieczeniach. W badanym roku każdemu wydaniu nowej wersji zestawu narzędzi towarzyszył wzrost liczby ataków na witryny internetowe. Gdy pojawia się nowa wersja, zawierająca nową funkcję hakerską, można zaobserwować jej wzmożone stosowanie

w Internecie i wykorzystywanie danej luki, aż potencjalne ofiary zainstalują na komputerach poprawki zabezpieczeń. Na przykład liczba ataków przy użyciu zestawu narzędzi Blackhole, który był bardzo popularny w roku 2010, w połowie 2011 roku spadła do kilkuset ataków dziennie, ale ponownie wzrosła po wprowadzeniu nowszych wersji i pod koniec roku podejmowane były setki tysięcy prób infekcji dziennie.

Zestawy narzędzi do ataków zawierają średnio około 10 programów do wykorzystywania luk w zabezpieczeniach, co dotyczy przede wszystkim luk w zabezpieczeniach wtyczek niezależnych od przeglądarki, takich jak Adobe Flash Player, Adobe Reader i Java. Popularne zestawy narzędzi mogą być aktualizowane co parę dni, a każda aktualizacja może powodować falę nowych ataków.

Takie zestawy można dość łatwo znaleźć i sprzedać na czarnym rynku oraz forach internetowych. Ich ceny wynoszą od 40 do 4000 dolarów.



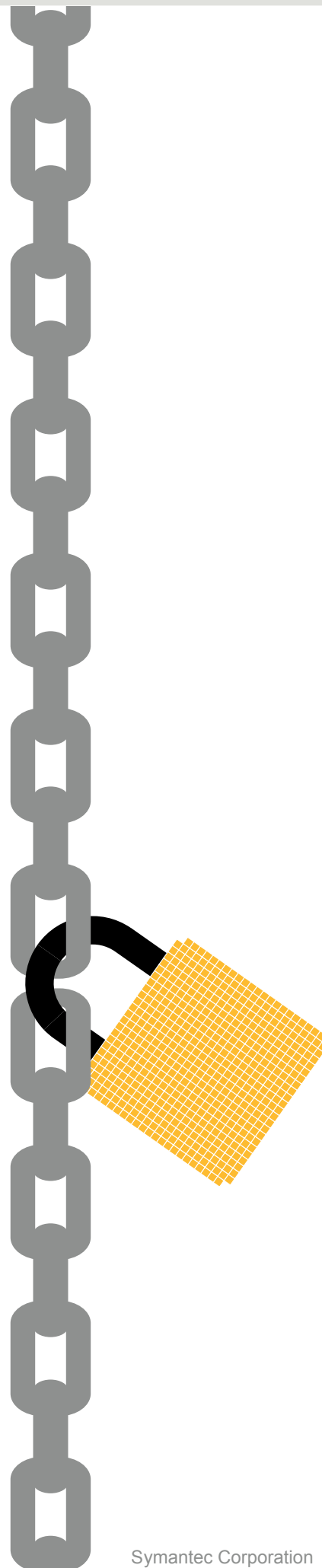
Zestawy narzędzi do ataków na witryny internetowe są używane na dwa podstawowe sposoby:

- 1 Ataki ukierunkowane.** Atakujący wybiera rodzaj użytkownika, który ma być celem ataku. Za pomocą zestawu narzędzi tworzy wiadomości e-mail, wiadomości do komunikatora internetowego lub posty na bloga w celu przyciągnięcia odbiorców do zainfekowanej treści. Zazwyczaj jest to łącze do szkodliwej witryny internetowej, którego kliknięcie spowoduje zainstalowanie szkodliwego oprogramowania na komputerze ofiary.
- 2 Ataki szeroko zakrojone.** Na początek atakujący przypuszcza atak na wiele witryn internetowych, korzystając z metody SQL injection albo luk w zabezpieczeniach aplikacji witryn bądź serwerów. Celem jest wstawienie łącza prowadzącego z zainfekowanej do szkodliwej witryny, która będzie infekować komputery odwiedzających użytkowników. Skuteczny atak powoduje zaatakowanie każdego następnego użytkownika odwiedzającego witrynę.

Budowanie wiarygodności i ochrona wrażliwych obszarów

Uczciwi użytkownicy z pewnością chcieliby, aby Internet był bezpieczny, pewny i wiarygodny. W ostatnim czasie powstało wiele inicjatyw mających na celu zapewnienie wiarygodności w oczach użytkowników:

- **Zawsze aktywne certyfikaty SSL.** Organizacja Online Trust Alliance¹⁵ zatwierdziła standard Always On SSL (Zawsze aktywne certyfikaty SSL) jako nową metodę wdrażania zabezpieczeń SSL w witrynach internetowych. Niektóre firmy, na przykład Facebook¹⁶, Google, PayPal czy Twitter¹⁷, udostępniają użytkownikom opcję ciągłego szyfrowania i uwierzytelniania SSL na wszystkich stronach ich usług (nie tylko na stronach logowania). Dzięki temu nie tylko zmniejsza się zagrożenie atakami typu man-in-the-middle (np. Firesheep¹⁸), ale uzyskuje się także kompleksowy system zabezpieczeń obejmujący każdą stronę w witrynie, bez ograniczania go do stron logowania i transakcji finansowych.
- **Certyfikaty Extended Validation SSL.** Certyfikaty EV SSL zapewniają najwyższy poziom uwierzytelniania, a ponadto informują użytkowników w dobrze widoczny sposób, że odwiedzana witryna jest bezpieczna (nakazując przeglądarkom wyświetlenie zielonego paska adresu). Dzięki temu można uniknąć wielu ataków internetowych. Wyniki sponsorowanych przez firmę Symantec badań zachowań klientów robiących zakupy w Internecie w Europie, Stanach Zjednoczonych i Australii pokazują, że zielony pasek certyfikatu EV SSL poprawia poczucie bezpieczeństwa u 60% osób¹⁹. Warto dodać, że według podobnej ankiety przeprowadzonej w Stanach Zjednoczonych 90% respondentów nie kontynuuje transakcji, gdy zostanie wyświetlona strona z ostrzeżeniem o braku bezpiecznego połączenia²⁰.
- **Podstawowe wymagania w zakresie certyfikatów SSL/TLS.** Organizacja CA/Browser Forum wydała dokument „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” (Podstawowe wymagania w zakresie wystawiania publicznie wiarygodnych certyfikatów i zarządzania nimi). Jest to pierwszy międzynarodowy standard regulujący działanie podmiotów certyfikujących, które wystawiają certyfikaty cyfrowe SSL/TLS uznawane automatycznie za wiarygodne przez przeglądarki. Ten nowy standard został ogłoszony w grudniu 2011 r. i zaczyna obowiązywać 1 lipca 2012 r.
- **Bezpieczeństwo certyfikatów do podpisywania kodu i kluczy prywatnych.** Głośne przypadki kradzieży kluczy prywatnych służących do podpisywania kodu pokazały, że firmy muszą zabezpieczać i chronić klucze prywatne, jeśli używają ich do podpisywania certyfikatów cyfrowych²¹. W przypadku udanej kradzieży tych kluczy hakerzy mogą cyfrowo podpisywać szkodliwe oprogramowanie za pomocą ważnych certyfikatów, przez co ataki przy użyciu takiego oprogramowania są trudniejsze do wykrycia. Dokładnie takie sytuacje miały miejsce podczas ataków Stuxnet i Duqu.
- **DNSSEC.** Ta technologia jest coraz szerzej używana jako metoda zachowania integralności w systemie nazw domen (DNS). Nie zaspokaja ona jednak wszystkich potrzeb związanych z zabezpieczeniami w Internecie – nie zapewnia uwierzytelniania tożsamości witryny ani nie umożliwia szyfrowania. Technologii DNSSEC należy używać w połączeniu z technologią SSL i innymi mechanizmami zabezpieczeń.
- **Wymagania prawne.** W wielu krajach, w tym w krajach członkowskich Unii Europejskiej²² i w Stanach Zjednoczonych (46 stanów)²³, obowiązują przepisy nakazujące powiadamianie o nieupoważnionym dostępie do danych, przynajmniej w określonych sektorach. Oznacza to, że w przypadku wykrycia udanego ataku firmy muszą powiadomić władze oraz (tam, gdzie jest to konieczne) osoby, których dane mogły zostać wykradzione. Te przepisy stanowią przykład dla innych krajów i regionów, w których nie ma podobnych uregulowań. Ponadto dają gwarancję, że w przypadku kradzieży danych użytkownicy zostaną szybko powiadomieni i będą mogli się zabezpieczyć przed potencjalnymi stratami, na przykład zmieniając hasła do kont.





Wnioski: co nas czeka w roku 2012

Pewien mądry człowiek powiedział: „Lepiej niczego nie przewidywać, a już szczególnie przyszłości”. W tym raporcie opieraliśmy się na danych z roku 2011, w podsumowaniu spróbujemy jednak nieznacznie wybiec w przyszłość i przewidzieć tendencje, które mogą wystąpić w roku 2012 i później.

- Ataki ukierunkowane i zaawansowane zagrożenia trwale (Advanced Persistent Threats – APT) będą nadal poważnym problemem. Częstotliwość i stopień złożoności tych ataków będą rosnąć.
- Techniki i luki w zabezpieczeniach używane w atakach ukierunkowanych będą coraz popularniejsze w różnych dziedzinach podziemnej działalności. Szkodliwe oprogramowanie stanie się przez to jeszcze groźniejsze.
- Twórcy szkodliwego oprogramowania i spamerzy będą jeszcze aktywniejsi w witrynach społecznościowych.
- Organizacja CA/Browser Forum²⁴ opracuje kolejne standardy zabezpieczeń dla firm wystawiających certyfikaty cyfrowe, aby poprawić wiarygodność w Internecie i ograniczyć skuteczność przyszłych ataków.
- Konsumeryzacja (korzystanie w firmach z rozwiązań dla klientów indywidualnych) oraz technologie chmur obliczeniowych będą się nadal rozwijać, co może zmienić model prowadzenia działalności i zmusić działy informatyczne firm do znalezienia i wdrożenia nowych metod ochrony użytkowników oraz systemów firmowych.
- Twórcy szkodliwego oprogramowania będą opracowywać kolejne techniki ataków na telefony komórkowe i tablety, bezwzględnie wykorzystując każdą okazję nielegalnego zdobycia pieniędzy.
- W 2011 roku zaobserwowaliśmy częstsze ataki z użyciem szkodliwego kodu na komputery Mac. Użytkownicy tych komputerów byli często kierowani do witryn rozpowszechniających konie trojańskie. Przewiduje się, że w roku 2012 ten trend się utrzyma, a kod używany do takich ataków będzie dołączany do bardziej kompleksowych zestawów narzędzi służących do przygotowywania ataków internetowych.
- Zagrożenia zewnętrzne będą wciąż narastać, ale nie dadzą o sobie zapomnieć także zagrożenia od wewnątrz. Wiele pracowników mniej lub bardziej celowo przyczyni się do wycieku lub kradzieży cennych danych.
- Być może jest już przygotowywany kolejny atak typu APT podobny do tego z użyciem robaka Stuxnet. Robak Duqu mógł być pierwszym wstrząsem zapowiadającym nowy kataklizm, ale może minąć trochę czasu, zanim echa tego wydarzenia dotrą do szerszego grona użytkowników.

Zalecane rozwiązania dla firm

Wdrożenie strategii wielowarstwowej ochrony

Systemy obronne powinny składać się z wielu elementów chroniących te same obszary i wzajemnie się uzupełniających. Stanowi to zabezpieczenie przed skutkami punktowych awarii ważnych składników dowolnej technologii czy metody ochrony. Warunkiem skuteczności tej strategii jest stosowanie regularnie aktualizowanych zapór, a także programów antywirusowych działających w bramie sieci, systemów wykrywania włamań i ochrony przed nimi oraz bram zabezpieczających ruch w obu kierunkach w całej sieci.

Monitorowanie zagrożeń, luk i fałszerstw sieciowych

To rozwiązanie polega na monitorowaniu włamań do sieci, prób rozpowszechniania szkodliwego oprogramowania i wszelkich podejrzanych wzorców ruchu w sieci, a także. prób połączeń ze znanymi szkodliwymi lub podejznanymi hostami. Zapobieganie atakom ułatwiają alerty o nowych lukach i zagrożeniach na różnych platformach. Z kolei alerty dotyczące domen i funkcje zgłaszania fikcyjnych witryn internetowych pozwalają rejestrować przypadki fałszerstw i podszywania się pod markę.

Ochrona antywirusowa w punktach końcowych to za mało

Zastosowanie w punktach końcowych samego oprogramowania antywirusowego opartego na podpisach nie zapewnia ochrony przed współczesnymi zagrożeniami i atakami z użyciem witryn internetowych.

Należy wdrożyć wszechstronne rozwiązanie do zabezpieczania punktów końcowych, składające się z dodatkowych warstw ochrony:

- Funkcja zapobiegania włamaniom w punktach końcowych, która chroni przed atakami polegającymi na wykorzystywaniu niepoprawionych luk w zabezpieczeniach oraz atakami z użyciem socjotechniki, a także uniemożliwia szkodliwym programom dotarcie do punktów końcowych.
- Ochrona przeglądarek przed atakami z użyciem fałszywych witryn internetowych.
- Ochrona przed szkodliwym oprogramowaniem oparta na środowisku chmury. Jest to dobre rozwiązanie prewencyjne chroniące przed nieznanymi zagrożeniami.
- Rozwiązania do sprawdzania reputacji plików i witryn internetowych udostępniające informacje o reputacji dowolnej aplikacji i witryny. Zapobiegają one rozprzestrzenianiu szybko mutującego, polimorficznego szkodliwego oprogramowania.
- Funkcja blokowania działania programów na podstawie zachowania, która sprawdza działanie aplikacji i chroni przed szkodliwymi programami.
- Ustawienia kontroli aplikacji, za pomocą których można zablokować w aplikacjach i wtyczkach do przeglądarek możliwość pobierania niedozwolonych, szkodliwych treści.
- Ustawienia kontroli urządzeń, za pomocą których można określać dozwolone urządzenia USB.

Ochrona witryn internetowych przed atakami typu man-in-the-middle (MITM) i infekcjami

Aby nie narażać na szwank dobrych relacji z klientami, firma powinna wdrożyć następujące rozwiązania:

- Zawsze aktywne certyfikaty SSL.
- Codzienne skanowanie witryny internetowej pod kątem szkodliwego oprogramowania.
- Stosowanie znaczników „secure” w przypadku wszystkich plików cookie w sesji.
- Regularne testowanie witryny pod kątem luk w zabezpieczeniach.
- Stosowanie certyfikatów Extended Validation SSL, powodujących wyświetlanie zielonego paska adresu w przeglądarce.
- Umieszczenie znanych symboli wiarygodności w dobrze widocznych miejscach witryny. To wzbudza zaufanie klientów i świadczy o dbałości o ich bezpieczeństwo.

Należy przy tym pamiętać, aby certyfikaty cyfrowe pochodziły od renomowanego, wiarygodnego podmiotu certyfikującego, który stosuje najlepszy model zabezpieczeń. Istotna jest także ochrona kluczy prywatnych. Ich właściwe zabezpieczenie wymaga zastosowania odpowiednio silnych mechanizmów, szczególnie w przypadku korzystania z certyfikatów cyfrowych. Rozwiązania zalecane przez firmę Symantec są następujące:

- Osobne infrastruktury podpisywania testowego i podpisywania wersji.
- Przechowywanie kluczy w zabezpieczonym, uniemożliwiającym manipulacje, sprzętowym urządzeniu kryptograficznym.
- Zabezpieczenia fizyczne chroniące zasoby firmy przed kradzieżą.

Szyfrowanie w celu ochrony poufnych danych

Należy wdrożyć i egzekwować zasady szyfrowania poufnych danych. Dostęp do informacji tego typu powinien być ograniczony. System powinien obejmować rozwiązanie chroniące przed utratą danych, którego zadaniem jest identyfikacja, monitorowanie i ochrona danych. Jest to zabezpieczenie przed nieupoważnionym dostępem do danych, ale pomaga także złagodzić skutki ewentualnego wycieku danych z firmy.

Zapobieganie kradzieżom danych za pomocą mechanizmu ochrony przed ich utratą

Zastosowane w firmie rozwiązanie chroniące przed utratą danych umożliwia wykrywanie lokalizacji poufnych danych, monitorowanie ich wykorzystania oraz ich właściwą ochronę. Kolejne zadania tego systemu to kontrola przepływu danych wychodzących z firmy do sieci oraz kontrola kopiowania poufnych danych na urządzenia zewnętrzne lub do witryn internetowych. Rozwiązanie chroniące przed utratą danych powinno identyfikować i blokować podejrzaną operację kopiowania oraz pobierania poufnych danych. Konieczna jest także identyfikacja zasobów zawierających tajne lub poufne dane w systemach plików i komputerach podłączonych do sieci. Umożliwia ona wprowadzenie dodatkowych zabezpieczeń przed utratą danych, na przykład szyfrowania.

Wdrożenie zasad dotyczących nośników wymiennych

Tam, gdzie pozwalają na to względy praktyczne, należy ograniczyć możliwość korzystania z niedozwolonych urządzeń, takich jak zewnętrzne przenośne dyski twarde i inne nośniki wymienne. Urządzenia te umożliwiają świadome lub nieświadome rozpowszechnianie szkodliwego oprogramowania, a nawet kradzież własności intelektualnej. Jeśli korzystanie z nośników zewnętrznych jest dozwolone, należy skanować je pod kątem wirusów zaraz po podłączeniu do sieci. Kopiowanie poufnych danych na nieszyfrowane zewnętrzne urządzenia pamięci masowej powinno być monitorowane i ograniczane przez system ochrony przed utratą danych.

Częste i bezzwłoczne aktualizowanie zabezpieczeń

W 2011 roku firma Symantec wykryła ponad 403 miliony odmian szkodliwego oprogramowania. W obliczu takiego zagrożenia aktualizacje definicji wirusów i innych metod ataków powinny być wykonywane co najmniej raz dziennie.

Natychmiastowe instalowanie aktualizacji i poprawek

W firmie należy używać mechanizmów automatycznego aktualizowania opracowanych przez producentów oprogramowania, które umożliwiają szybkie stosowanie aktualizacji i poprawek oraz wycofywanie przestarzałych, niezabezpieczonych przeglądarek, aplikacji i wtyczek do przeglądarek. Większość producentów stara się regularnie wydawać poprawki usuwające luki w zabezpieczeniach. Skuteczność takich poprawek zależy jednak od ich właściwego zastosowania. Podczas wdrażania w firmie standardowych obrazów oprogramowania należy pamiętać, że mogą one zawierać starsze wersje przeglądarek, aplikacji i wtyczek, które są przestarzałe i niebezpieczne.

Gdy tylko jest to możliwe, należy stosować mechanizmy automatycznego instalowania poprawek, aby skutecznie usuwać luki w zabezpieczeniach w całej firmie..

Stosowanie skutecznych zasad dotyczących haseł

Należy używać silnych haseł: składających się z co najmniej 8–10 znaków, w tym liter i cyfr. Użytkownicy nie powinni używać tych samych haseł w wielu witrynach internetowych, a udostępnianie haseł innym osobom powinno być zabronione. Hasła należy zmieniać regularnie, w odstępach co najmniej 90-dniowych. Nie powinno się ich zapisywać.

Ograniczenia dotyczące załączników do wiadomości e-mail

Serwery pocztowe powinny być skonfigurowane tak, aby blokować lub usuwać wiadomości zawierające załączniki w formie plików powszechnie używanych do rozpowszechniania wirusów (np. pliki .VBS, .BAT, .EXE, .PIF i .SCR). Należy także opracować zasady dotyczące plików .PDF, które mają być dozwolone jako załączniki.

Przygotowanie procedur na wypadek infekcji i innych groźnych zdarzeń

- Należy zawsze mieć pod ręką dane kontaktowe dostawcy zabezpieczeń, a także wiedzieć, z kim należy się skontaktować i co zrobić w przypadku wykrycia infekcji systemów.
- W firmie powinien działać mechanizm tworzenia kopii zapasowych i odzyskiwania danych, który umożliwia przywrócenie danych utraconych lub wykradzionych wskutek udanego ataku lub nieszczęśliwego zdarzenia.
- Do określania zainfekowanych systemów należy używać funkcji wykrywania infekcji dostępnych w oprogramowaniu zabezpieczającym bramy i punkty końcowe oraz w zaporach.
- Zainfekowane komputery należy izolować, aby ograniczyć ryzyko rozprzestrzeniania się infekcji w firmie.
- Jeśli usługi sieciowe zostaną zaatakowane przy użyciu szkodliwego kodu lub innej techniki, należy wyłączyć lub zablokować dostęp do tych usług do czasu zastosowania poprawki.
- Zainfekowane komputery należy dokładnie zbadać, a do przywracania danych należy używać wiarygodnych nośników.

Informowanie użytkowników o dynamicznych zmianach zagrożeń

- Nie należy otwierać załączników, które nie były oczekiwane i nie pochodzą ze znanego i wiarygodnego źródła. Nie należy uruchamiać oprogramowania pobranego z Internetu (o ile pobieranie jest w ogóle dozwolone), dopóki nie zostanie ono przeskanowane pod kątem obecności wirusów.

- Należy zachować ostrożność podczas klikania adresów URL w wiadomościach e-mail i witrynach społecznościowych, nawet jeśli adresy te pochodzą z wiarygodnych źródeł lub od znajomych.
- Nie wolno klikać skróconych adresów URL bez ich wcześniejszego wyświetlenia lub rozwinięcia przy użyciu dostępnych narzędzi i wtyczek.
- Użytkownicy powinni zwracać uwagę na to, jakie informacje podają w witrynach społecznościowych. Informacje te mogą posłużyć do przeprowadzenia ataku lub przygotowania szkodliwego, pozornie niegroźnego adresu URL albo załącznika.
- Należy uważać na wyniki zwracane przez wyszukiwarki internetowe. Najlepiej klikać tylko wyniki prowadzące do wiarygodnych źródeł, szczególnie w przypadku tematów cieszących się dużą uwagą mediów.
- Należy zainstalować wtyczki do przeglądarek informujące o reputacji witryn wyświetlanych w wynikach wyszukiwania.
- Oprogramowanie należy pobierać (o ile jest to dozwolone) tylko z udziałów firmowych lub bezpośrednio z witryn producentów.
- Jeśli w systemie Windows po kliknięciu adresu URL lub podczas korzystania z wyszukiwarki zostanie wyświetlone ostrzeżenie o infekcji (tzw. fałszywe infekcje), użytkownik powinien zamknąć przeglądarkę, naciskając klawisze ALT+F4 lub CTRL+W albo z poziomu Menedżera zadań.
- Użytkownicy powinni mieć zainstalowane najnowsze wersje przeglądarek i systemów operacyjnych, aby móc korzystać z automatycznych aktualizacji zabezpieczeń.
- Przed zalogowaniem się lub podaniem dowolnych danych osobowych w witrynie internetowej użytkownicy powinni sprawdzać, czy witryna ma zielony pasek adresu, oznaczenie HTTPS i znane symbole wiarygodności.

Zalecane rozwiązania dla użytkowników indywidualnych

Ochrona własnych zasobów

Należy korzystać z nowoczesnego systemu zabezpieczeń internetowych, który obejmuje następujące funkcje zapewniające maksymalną ochronę przed szkodliwym kodem i innymi zagrożeniami:

- Funkcje ochrony antywirusowej (na poziomie plików i heurystycznej) oraz ochrony przed szkodliwym oprogramowaniem na podstawie zachowania mają za zadanie blokować wykonywanie szkodliwego kodu.
- Zapory dwukierunkowe blokują możliwość wykorzystania przez szkodliwe oprogramowanie ewentualnych luk w aplikacjach i usługach działających na komputerze.
- Funkcja zapobiegania włamaniom chroni przed atakami z użyciem witryn internetowych, atakami polegającymi na wykorzystywaniu niepoprawionych luk w zabezpieczeniach oraz atakami z użyciem socjotechniki.
- Funkcja ochrony przeglądarki dodatkowo zabezpiecza przed atakami z użyciem fałszywych witryn internetowych.
- Narzędzia do sprawdzania reputacji udostępniają informacje o reputacji oraz poziomie wiarygodności plików i witryn internetowych przed pobraniem treści. Sprawdzane są również oceny reputacji i bezpieczeństwa witryn znalezionych przez wyszukiwarki.
- Zalecane jest także zastosowanie międzyplatformowej funkcji kontroli rodzicielskiej, na przykład rozwiązania Norton Online Family²⁵.

Częste aktualizacje

Definicje wirusów oraz inne zasoby związane z zabezpieczeniami należy aktualizować co najmniej raz dziennie (najlepiej częściej). Instalując najnowsze definicje wirusów, można ochronić komputer przed nowymi wirusami i szkodliwym oprogramowaniem, które rozprzestrzeniają się w sieci. Mechanizmy automatycznego aktualizowania oprogramowania (jeśli istnieją) umożliwiają instalowanie aktualizacji systemu operacyjnego, aplikacji, przeglądarki internetowej oraz wtyczek do przeglądarki. Korzystanie z nieaktualnych wersji programów stwarza zagrożenie atakami z użyciem witryn internetowych.

Świadome działanie

Szkodliwe oprogramowanie i aplikacje generujące fałszywe komunikaty o infekcji komputera są często instalowane automatycznie wraz z programami do udostępniania plików, bezpłatnie pobraną treścią lub wersjami freeware i shareware programów.

- Również wszelkie „bezpłatne”, „złamane” lub „pirackie” wersje programów mogą zawierać szkodliwe oprogramowanie lub aplikacje do przeprowadzania ataków z użyciem socjotechniki. Mogą na przykład niezgodnie z prawdą informować o zainfekowaniu komputera i proponować usunięcie infekcji za opłatą.
- Należy uważać, które witryny internetowe się odwiedza. Co prawda zdarza się, że szkodliwe oprogramowanie rozpowszechniają znane witryny, zwykle jednak dotyczy to witryn o złej reputacji (związanych z pornografią, hazardem i nielegalnym oprogramowaniem).
- Należy uważnie czytać umowy licencyjne i przed akceptacją zapoznać się ze wszystkimi postanowieniami. Niektóre groźne programy mogą być instalowane po zaakceptowaniu umowy lub z powodu jej zaakceptowania.

Stosowanie skutecznych zasad dotyczących haseł

- W hasłach należy używać kombinacji liter i cyfr. Trzeba je także często zmieniać. Hasła nie powinny zawierać wyrazów ze słownika. Nie należy używać tego samego hasła w wielu aplikacjach lub witrynach internetowych. Hasła powinny być złożone (wielkie i małe litery, znaki interpunkcyjne). Można też używać tzw. fraz kodujących.

Zachowanie ostrożności

Nie należy wyświetlać, otwierać ani uruchamiać pliku otrzymanego w załączniku do wiadomości e-mail, która nie była oczekiwana i której nadawca nie jest wiarygodny. Uważać należy nawet w przypadku znanych, wiarygodnych użytkowników.

- Należy zachować ostrożność podczas klikania adresów URL w wiadomościach e-mail i witrynach społecznościowych, nawet jeśli adresy te pochodzą z wiarygodnych źródeł lub od znajomych. Nie wolno bez zastanowienia klikać skróconych adresów URL bez ich wcześniejszego rozwinięcia przy użyciu narzędzi lub wtyczek do generowania podglądu.
- W aplikacjach dostępnych w witrynach społecznościowych nie należy klikać łączy zawierających atrakcyjne sformułowania, nawet jeśli pochodzą od znajomych. Kliknięcie takiego adresu URL może uruchomić funkcję wysyłania go do wszystkich znajomych, nawet w przypadku kliknięcia dowolnego miejsca na stronie. Lepiej po prostu zamknąć przeglądarkę.
- Należy zainstalować oprogramowanie sprawdzające adresy URL w przeglądarce, które będzie informować o reputacji i poziomie bezpieczeństwa witryn wyświetlanych w wynikach wyszukiwania. Trzeba uważać na wyniki zwracane przez wyszukiwarki internetowe. Najlepiej klikać tylko wyniki prowadzące do wiarygodnych źródeł, szczególnie w przypadku tematów cieszących się dużą uwagą mediów.
- Należy podejrzliwie traktować pojawiające się nagle ostrzeżenia proponujące instalowanie odtwarzaczy multimedialnych, przeglądarek dokumentów i aktualizacji zabezpieczeń. Takie oprogramowanie należy instalować tylko bezpośrednio z witryny producenta.

Ochrona danych osobowych

Udostępniając swoje dane osobowe w Internecie (szczególnie w witrynach społecznościowych), należy zachować ostrożność. Dane te mogą zostać później użyte w działaniach szkodzących ich właścicielom, na przykład do ataków ukierunkowanych lub do wyłudzenia informacji.

- Nie wolno ujawniać żadnych poufnych informacji osobistych ani finansowych bez sprawdzenia wiarygodności podmiotu proszącego o te informacje.
- Należy często sprawdzać stan konta bankowego, wyciągi z kart kredytowych i inne informacje finansowe pod kątem nieautoryzowanych działań. Nie należy korzystać z usług bankowości ani robić zakupów online na komputerach ogólnodostępnych (w bibliotekach, kafejkach internetowych itp.) lub przy użyciu nieszyfrowanych połączeń Wi-Fi.
- Podczas korzystania z poczty, witryn społecznościowych i witryn do udostępniania plików w sieciach Wi-Fi należy łączyć się za pośrednictwem protokołu HTTPS. Konieczne jest także sprawdzanie ustawień i preferencji używanych aplikacji i witryn internetowych.
- Przed zalogowaniem się lub podaniem dowolnych danych osobowych w witrynie internetowej należy sprawdzić, czy witryna ma zielony pasek adresu, oznaczenie HTTPS i znane symbole wiarygodności.
- W domowej sieci Wi-Fi należy skonfigurować silne uwierzytelnianie oraz zabezpieczyć dostęp do sieci unikatowym hasłem.

Dodatkowe informacje

- Zestawienie zagrożeń globalnych z usług Symantec.cloud:
<http://www.symanteccloud.com/en/gb/globalthreats/>
- Zespół firmy Symantec ds. reagowania na zagrożenia bezpieczeństwa (Symantec Security Response): http://www.symantec.com/security_response/
- Raport „Internet Security Threat Report” (strona zasobów): <http://www.symantec.com/threatreport/>
- Narzędzie Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Narzędzie Norton Cybercrime Index: <http://us.norton.com/cybercrimeindex/>

Przypisy

- 1 W tej liczbie po raz pierwszy uwzględniono dane na temat ataków pochodzące z usług **Symantec.cloud**. W przypadku pominięcia tych danych w celu porównania z rokiem 2010 łączna liczba ataków wyniosłaby 5,1 mld.
- 2 <https://otalliance.org/resources/AOSSL/index.html>
- 3 Udane ataki na podmioty certyfikujące (Comodohacker) i przypadki utraty wiarygodności w roku 2011: Comodo (2 zaatakowane podmioty certyfikujące):
<https://www-secure.symantec.com/connect/blogs/how-avoid-fraudulent-ssl>
<http://www.thetechherald.com/articlesInstantSSL-it-named-as-source-of-Comodo-breach-by-attacker/13145/>
- 4 http://www.theregister.co.uk/2011/05/24/comodo_reseller_hacked/
- 5 Atak na firmę StartCom:
<http://www.internet-security.ca/internet-security-news-archives-031security-firm-start-ssl-suffered-a-security-attack.html>
<http://www.informationweek.com/news/security/attacks/231601037>
- 6 http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/
- 7 Firma DigiNotar pada ofiarą ataku i kończy działalność:
<https://www-secure.symantec.com/connect/blogs/why-your-ca-matters>
<https://www-secure.symantec.com/connect/blogs/diginotar-ssl-breach-update>
http://www.arnnet.com.au/article/399812/comodo_hacker_claims_credit_diginotar_attack/
<http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars>
<http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231600865/comodo-hacker-takes-credit-for-massive-diginotar-hack.html>
http://www.pcworld.com/businesscenter/article/239534/comodo_hacker_claims_credit_for_diginotar_attack.html
- 8 Modele koncepcyjne i analiza ataków: BEAST
<http://blog.ivanristic.com/2011/10/mitigating-the-beast-attack-on-tls.html>
oraz luka w plikach cookie TLS 1.1/1.2, THC-SSL-DOS i LinkedIn SSL
<http://www.wtfuzz.com/blogs/linkedin-ssl-cookie-vulnerability/>
- 9 <http://www.itproportal.com/2011/09/13/globalsign-hack-was-isolated-server-business-resumes/>
- 10 http://www.theregister.co.uk/2011/09/07/globalsign_suspends_ssl_cert_biz/
- 11 http://www.pcworld.com/businesscenter/article/239639/dutch_government_struggles_to_deal_with_diginotar_hack.html
- 12 http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/
- 13 Więcej informacji na temat usługi Norton Safe Web: <http://safeweb.norton.com>
- 14 Więcej informacji na temat usługi oceniania luk w zabezpieczeniach witryn internetowych oferowanej przez firmę Symantec: <http://www.symantec.com/theme.jsp?themeid=ssl-resources>
- 15 <https://otalliance.org/resources/AOSSL/index.html>
- 16 <http://blog.facebook.com/blog.php?post=486790652130>
- 17 <http://blog.twitter.com/2011/03/making-twitter-more-secure-https.html>
- 18 <http://www.symantec.com/connect/blogs/launch-always-ssl-and-firesheep-attacks-page>
- 19 Sponsorowane przez firmę Symantec badania zachowań klientów robiących zakupy w Internecie w Wielkiej Brytanii, Francji, Niemczech, krajach Beneluksu, Stanach Zjednoczonych i Australii z grudnia 2010 r. i stycznia 2011 r. (analizę przeprowadzono w marcu 2011 r.).
- 20 http://www.symantec.com/about/news/release/article.jsp?prid=20111129_01
- 21 <http://www.symantec.com/connect/blogs/protecting-digital-certificates-everyone-s-responsibility/>
- 22 http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport
- 23 <http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/>
- 24 <http://www.cabforum.org/>
- 25 Aby uzyskać więcej informacji dotyczących programu Norton Online Family na stronie <https://onlinefamily.norton.com/>

Informacje o firmie Symantec

Firma Symantec jest światowym liderem w dziedzinie zabezpieczeń, pamięci masowej i zarządzania systemami, który pomaga klientom indywidualnym i firmom bezpiecznie zarządzać informacjami.

Oferowane przez firmę oprogramowanie i usługi zapewniają pełniejszą i skuteczniejszą ochronę przed wieloma zagrożeniami w licznych lokalizacjach, dając użytkownikom poczucie bezpieczeństwa niezależnie od tego, w jakim miejscu informacje są używane lub przechowywane. Siedziba firmy Symantec mieści się w Mountain View (Kalifornia), a jej przedstawicielstwa znajdują się w 40 krajach. Więcej informacji:

www.symantec.pl



© 2012 Symantec Corporation. Wszelkie prawa zastrzeżone. Nazwa Symantec, logo Symantec, logo „V”, Norton Secured i logo Norton Secured są znakami towarowymi bądź zastrzeżonymi znakami towarowymi firmy Symantec Corporation lub jej oddziałów, zarejestrowanymi w USA i innych krajach. VeriSign i inne powiązane marki są znakami towarowymi bądź zastrzeżonymi znakami towarowymi firmy VeriSign Inc. lub jej oddziałów albo spółek zależnych, zarejestrowanymi w USA i innych krajach, a używanymi przez firmę Symantec Corporation na podstawie licencji. Inne nazwy mogą być znakami towarowymi odpowiednich właścicieli.

Wszelkie informacje techniczne udostępnione przez firmę Symantec Corporation stanowią chronioną prawami autorskimi własność firmy Symantec Corporation.

BRAK GWARANCJI. Firma Symantec udostępnia ten dokument w stanie takim, w jakim jest („as is”) i nie udziela żadnych gwarancji jego zgodności z prawdą lub przydatności do jakichkolwiek celów. Informacje zawarte w tym dokumencie mogą zawierać nieścisłości lub błędy typograficzne i mogą nie odzwierciedlać najnowszych osiągnięć. Firma Symantec nie deklaruje ani nie gwarantuje, że są one kompletne, dokładne i aktualne, ani też nie oferuje żadnych poświadczeń czy zapewnień w odniesieniu do jakichkolwiek opinii bądź odniesień przytoczonych w tym dokumencie. Zmiana okoliczności może wpłynąć na dokładność treści tego dokumentu. Przedstawione tu opinie odzwierciedlają osady w chwili publikacji i mogą ulec zmianie. Wszelkie ryzyko związane z jakimkolwiek wykorzystaniem informacji zawartych w niniejszym dokumencie ponosi użytkownik. Firma Symantec nie odpowiada za żadne błędy, niedopatrzenia ani szkody powstałe w wyniku wykorzystania zawartych tu informacji lub opierania się na nich. Firma Symantec zastrzega sobie prawo do wprowadzania zmian w dowolnym czasie bez uprzedzenia.