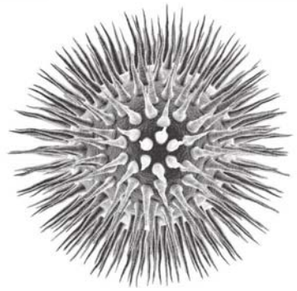


Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

www.checkpoint.com

ŚWIATOWA SIEDZIBA GŁÓWNA
5 Ha'Solelim Street, Tel Aviv 67897, Israel
Tel: 972-3-753-4555 | Fax: 972-3-624-1100
Email: info@checkpoint.com

SIEDZIBA GŁÓWNA W USA
959 Skyway Road, Suite 300, San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4

©2014 Check Point Software Technologies Ltd. [Chroniony] – Wszystkie prawa zastrzeżone

checkpoint@checkpoint.pl

Dystrybucja w Polsce:

CLICO

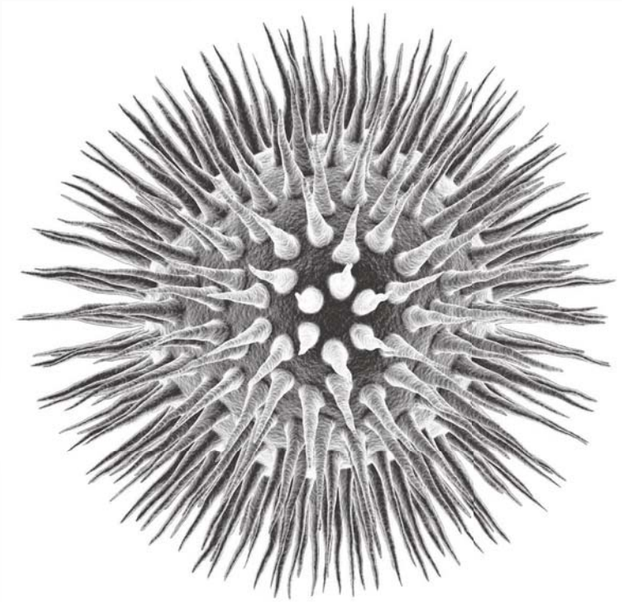
CLICO Sp. z o.o.
Budynek CC Oleandry
30-063 Kraków, ul. Oleandry 2
tel. 12 378-37-00
tel. 12 632-51-66
tel. 12 292-75-22...24
fax 12 632-36-98
e-mail: sales@clico.pl
www.clico.pl

CLICO Oddział Katowice
40-568 Katowice, ul. Ligocka 103
tel. 32 444-65-11
tel. 32 203-92-35
tel. 32 609-80-50...51
fax 32 203-97-93
e-mail: katowice@clico.pl

CLICO Oddział Warszawa
Budynek Centrum Milenium
03-738 Warszawa, ul. Kijowska 1
tel. 22 201-06-88
tel. 22 518-02-70...75
fax 22 518-02-73
e-mail: warszawa@clico.pl

© 2014 CLICO Sp. z o.o. (polska wersja językowa). CLICO i CLICO logo są zarejestrowanymi znakami towarowymi CLICO Sp. z o.o.

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.



CHECK POINT
RAPORT BEZPIECZEŃSTWA
2014

PRZYPISY c.d.

44 http://www.huffingtonpost.com/tag/silk-road-arrest

45 http://www.pcworld.com/article/2093200/torenabled-malware-stole-credit-card-data-from-pos-systems-at-dozens-of-retailers.html

46 http://www.britannica.com/EBchecked/topic/278114/Hydra

47 http://msdn.microsoft.com/en-us/library/aa383015(v=vs.85).aspx

48 http://www.securityweek.com/poison-ivy-kit-enables-easy-malware-customization-attackers

49 http://www.checkpoint.com/defense/advisories/public/2005/cpai-20-Decf.html

50 http://www.emea.symantec.com/web/ShadowIT-enduser/

51 http://www.techrepublic.com/blog/it-security/dropsmack-using-dropbox-to-steal-files-and-deliver-malware/

52 http://vote-il.org/politicianissue.aspx?state=il&id=ilbeanmelissa&issue=buscrime

53 http://www.scmagazine.com/florida-health-department-employees-stole-data-committed-tax-fraud/article/318843/

54 http://www.islingtongazette.co.uk/news/data_leak_lands_islington_council_with_70_000_fine_1_2369477

55 http://healthitsecurity.com/2013/11/12/rotech-healthcare-reports-three-year-old-patient-data-breach/

56 http://www.dailypost.co.uk/news/north-wales-news/anglesey-council-under-fire-over-6330304

57 http://www.informationweek.com/attacks/heartland-payment-systems-hit-by-data-security-breach/d/d-id/1075770

58 https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf

59 http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm

60 http://www.computerworld.com/s/article/9245984/Despite_Target_data_breach_PCI_security_standard_remains_solid_chief_says

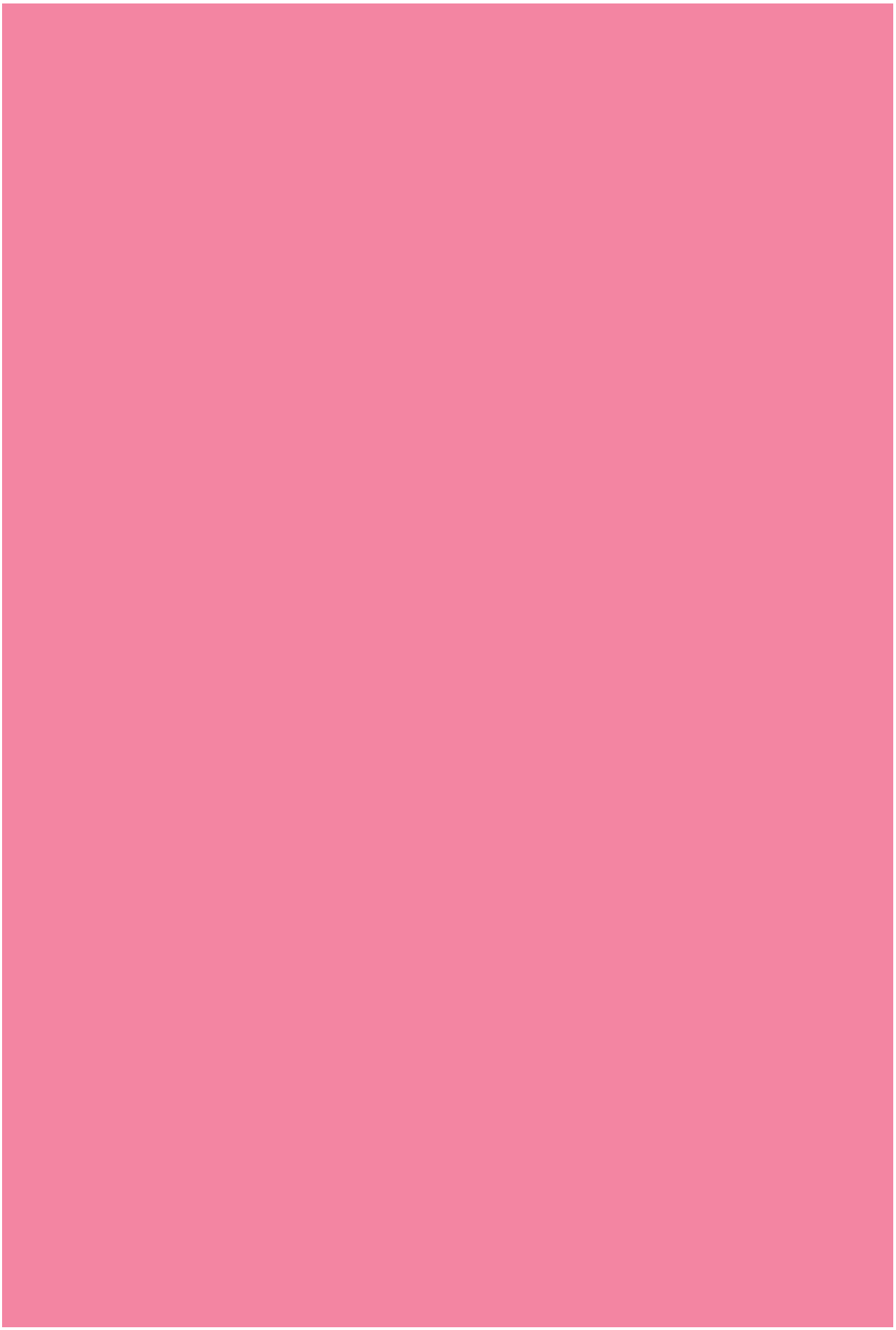
61 http://www.csoonline.com/article/723630/dexter-malware-infects-point-of-sale-systems-worldwide-researchers-say

62 http://www.darkreading.com/vulnerabilities---threats/securestate-releases-black-pos-malware-scanning-tool/d/d-id/1141216

63 http://www.businessweek.com/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

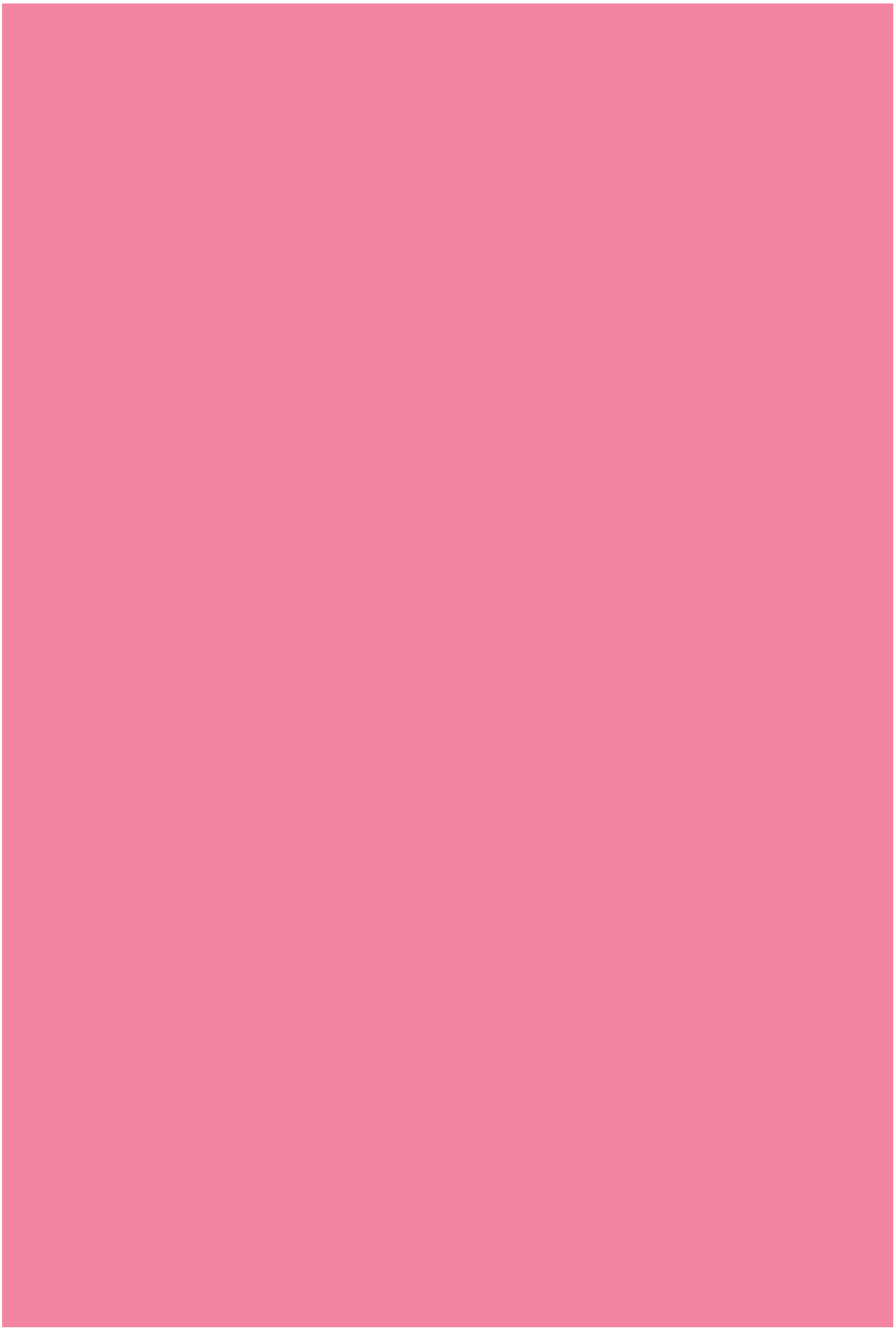
64 http://www.checkpoint.com/sdp

RAPORT BEZPIECZEŃSTWA CHECK POINT 2014



01

WPROWADZENIE I METODOLOGIA



01 WPROWADZENIE I METODOLOGIA

PRZEGLĄDAJĄC WYDRUK, WIDZIAŁEM, JAK HAKER IDZIE ŁOWIĆ NA MILNECIE. WYPRÓBOWAŁ JEDEN ZA DRUGIM PIĘTNAŚCIE KOMPUTERÓW SIŁ POWIETRZNYCH W TAKICH MIEJSCACH, JAK BAZY EGLIN, KIRTLAND I BOLLING. BEZ POWODZENIA. PODŁĄCZAŁ SIĘ DO KAŻDEGO KOMPUTERA, RAZ CZY DWA RAZY NACISKAŁ KLAMKĘ, A POTEM PRZECHODZIŁ DO NASTĘPNEGO SYSTEMU. W KOŃCU SPRAWDZIŁ SYSTEMY KOSMICZNEGO DOWÓDZTWA SIŁ POWIETRZNYCH (ANG. AIR FORCE SYSTEMS COMMAND SPACE DIVISION). NAJPIERW NACISNĄŁ KLAMKĘ, PRÓBUJĄC WEJŚĆ NA KONTO SYSTEMOWE ZA POMOCĄ HASŁA „MENEDŻER". BEZ SKUTKU. POTEM JAKO GOŚĆ, HASŁO „GOŚĆ". NIC Z TEGO. NASTĘPNIE TEREN Z HASŁEM „OBSŁUGA". […] I BUM: DRZWI OTWARTE. ZALOGOWAŁ SIĘ JAKO OBSŁUGA TERENOWA. NIE JAKO ZWYKŁY UŻYTKOWNIK, ALE PRZEZ KONTO Z WSZYSTKIMI PRZYWILEJAMI. […] GDZIEŚ W POŁUDNIOWEJ KALIFORNII, W EL SEGUNDO, HAKER ODDALONY O PÓŁ GLOBU WŁAMYWAŁ SIĘ NA DUŻY KOMPUTER VAX.

Clifford Stoll, The Cuckoo's Egg[1]

Ponad dwadzieścia pięć lat temu pewien administrator UNIX śledził 75-centowy błąd rachunkowy, aż dotarł do siatki szpiegowskiej w Bloku Wschodnim, która próbowała wykraść tajemnice państwowe i wojskowe od Stanów Zjednoczonych. Historia tego, jak podążał ścieżką od początkowych sygnałów ostrzegawczych do odkrycia poważniejszej inwazji i jak musiał zmierzyć się z najeźdźcą – opowiedziana w „The Cuckoo's Egg" – stanowi modelowy przykład wyzwań ochrony cyberprzestrzeni. Technologie, sposoby połączenia, metody nieautoryzowanego dostępu – wszystko to znacznie rozwinęło się od końca lat 80-tych, lecz identyfikowanie narażonych systemów, reakcja na incydenty oraz zabezpieczanie systemów i danych przed możliwymi atakami wciąż wyznaczają podstawowe wyzwania, przed którymi stoją organizacje międzynarodowe, niezależnie od swojej wielkości i branży, w jakiej działają.

W 2013 r. bezpieczeństwo informacji zajęło bardzo ważną pozycję w świadomości społecznej ze względu na głośne przypadki naruszenia danych. Kradzież i publikacja informacji wywiadowczych Stanów Zjednoczonych były na pierwszych stronach gazet przez znaczną część roku 2013 i wstrząsnęły relacjami dyplomatycznymi na całym świecie. W tym roku miały też miejsce zakrojone na szeroką skalę naruszenia danych płatniczych, które zrujnowały okres wakacyjny dla największych detalistów i niezliczonej rzeszy konsumentów. Wojna w cyberprzestrzeni i „haktywizm"[2] zmieniły naturę konfliktów między ludźmi i narodami, tak jak powstanie Internetu przedmiotów[3] (ang. Internet of Things)[3] przeniosło jeszcze więcej aspektów naszego życia codziennego do Internetu, przez co są one bardziej podatne na zagrożenia.

W społeczności zajmującej się bezpieczeństwem eksplozja nieznanego złośliwego oprogramowania (ang. malware) – nie tylko nowych zagrożeń, ale także nowych sposobów tworzenia i rozmieszczania niewykrywalnych zagrożeń na skalę masową – postawiło pytanie o skuteczność istniejących strategii i technologii. Nawet bardziej powszechne rodzaje złośliwego oprogramowania okazały się znacznie bardziej odporne na ustanowione zabezpieczenia, zaś mobilność, konsumeryzacja i systemy-cienie (ang. shadow IT) bez porównania zwiększyły stopień skomplikowania wyzwań, przed którymi stoi bezpieczeństwo.

5 PYTAŃ, JAKIE KAŻDA FIRMA MUSI SOBIE ZADAĆ

1. JAK SZYBKO ZMIENIAJĄCY SIĘ KRAJOBRAZ BEZPIECZEŃSTWA WPŁYNĄŁ NA WASZĄ FIRMĘ?

2. Z JAKIMI ZAGROŻENIAMI MIELIŚCIE DO CZYNIENIA I JAKIE DOPIERO POWSTAJĄCE ZAGROŻENIA NAJBARDZIEJ WAS NIEPOKOJĄ?

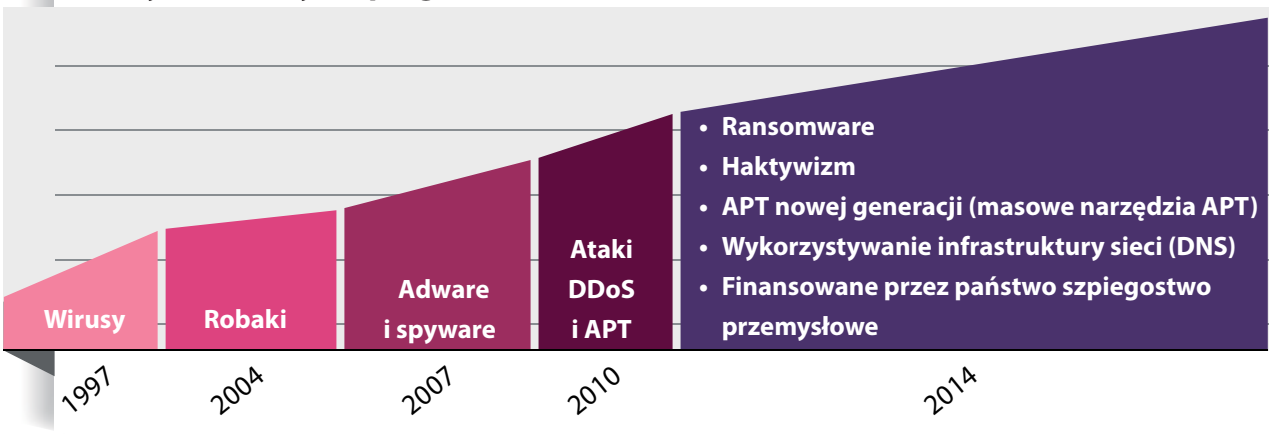
3. CZY UWAŻACIE, ŻE POSIADACIE WŁAŚCIWĄ STRATEGIĘ I ODPOWIEDNIE NARZĘDZIA, ŻEBY SPROSTAĆ WYZWANIU, CZY MOŻE RADZICIE SOBIE CORAZ GORZEJ Z FALAMI NIEPOKOJĄCYCH WYDARZEŃ?

4. JAKIE NOWE KROKI PODEJMIECIE W PRZYSZŁYM ROKU?

5. JAK ZAMIERZACIE POMÓC WASZEJ ORGANIZACJI JAKO CAŁOŚCI OSIĄGNĄĆ WYŻSZY STOPIEŃ BEZPIECZEŃSTWA?

W celu zidentyfikowania najważniejszych trendów w złośliwym oprogramowaniu i bezpieczeństwie informacji w roku 2013, z którymi organizacje będą musiały się zmierzyć w 2014 r. i w latach następnych, zespół Check Point ds. bezpieczeństwa przeanalizował dane incydentów z całego roku dotyczących ponad 10 tysięcy organizacji. „Raport Bezpieczeństwa Check Point 2014" prezentuje wyniki naszych badań. Ta skrupulatna analiza zagrożeń i trendów bezpieczeństwa w 2013 r. pomoże decydentom biznesowym i ds. bezpieczeństwa zrozumieć zakres zagrożeń, przed którymi stoją ich organizacje. Raport obejmuje również rekomendowane działania, których podjęcie umożliwi ochronę przed tymi i przyszłymi zagrożeniami. Najważniejszymi wnioskami z naszych badań są:

Trendy w złośliwym oprogramowaniu:



PRZECIĘTNY DZIEŃ W ORGANIZACJI

Co **1 minutę** host wchodzi na złośliwą stronę

Co **3 minuty** bot kontaktuje się ze swoim centrum dowodzenia i kontroli

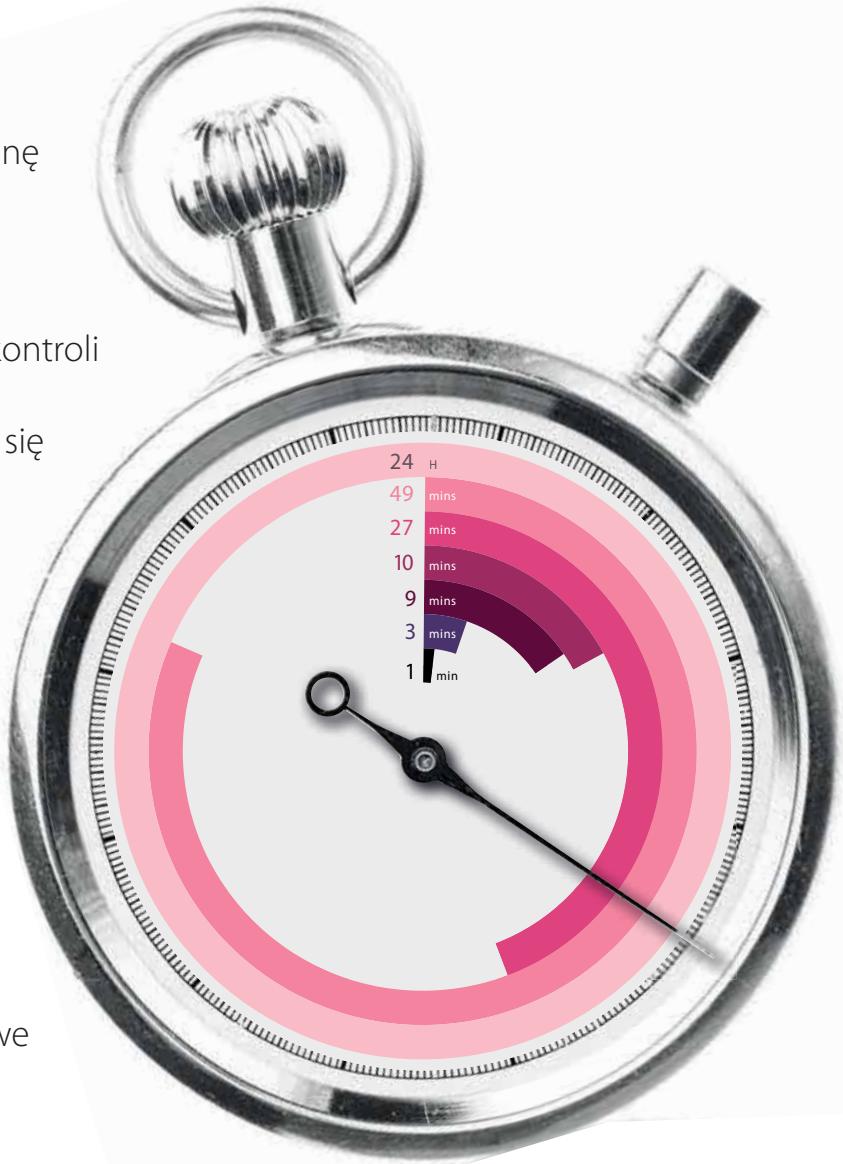
Co **9 minut** korzysta się z aplikacji wysokiego ryzyka

Co **10 minut** pobierany jest znany złośliwy program

Co **27 minut** pobierany jest nieznany złośliwy program

Co **49 minut** wrażliwe dane wysyłane są poza organizację

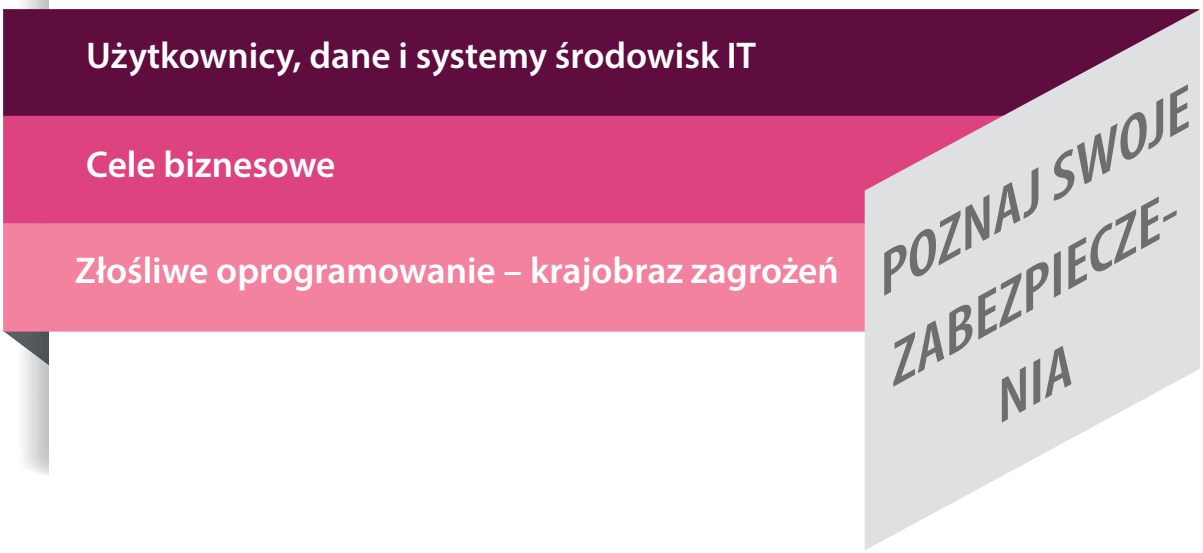
Co **24 godziny** host jest zarażany przez bota



Rycina1-1

Źródło: Check Point Software Technologies

PEŁNY OBRAZ ZAGROŻEŃ



- Znaczące zwiększenie liczby użytkowników nieznanego złośliwego oprogramowania wynikające z trendu masowej indywidualizacji[4] złośliwego oprogramowania – średnio 2,2 nieznane złośliwe programy (złośliwe oprogramowanie, którego wcześniej nie odnotowano) uderzały w organizacje co godzinę;
- Ekspozycja na złośliwe oprogramowanie i infekcja złośliwym oprogramowaniem nieporównywalnie wzrosły, co odzwierciedla sukces kierowanych kampanii malware'owych – w 2013 r. w 73% organizacji wykryto co najmniej jednego bota, w porównaniu do 63% w 2012 r.;
- Każda kategoria programu wysokiego ryzyka zwiększyła swoją obecność w firmach na całym świecie – przykładowo 63% organizacji korzystało z programów BitTorrent, w porównaniu do 40% w 2012 r;
- Wypadki utraty danych były częstsze niezależnie od sektora i rodzaju danych – 88% organizacji doświadczyło przynajmniej jednego wypadku utraty danych, w porównaniu do 54% w 2012 r.

Źródła danych dla raportu

„Raport Bezpieczeństwa Check Point 2014" oparty jest na wspólnych badaniach i analizach wypadków bezpieczeństwa na podstawie raportów Check Point Security Checkup[5] (pol. Badania Kontrolne Zabezpieczeń), czujników Check Point Threat Emulation[6] (pol. Emulacja Zagrożeń), Check Point ThreatCloud[7] (pol. Chmura Zagrożeń) i raportów Check Point Endpoint Security[8] (pol. Zabezpieczenie Punktu Końcowego).

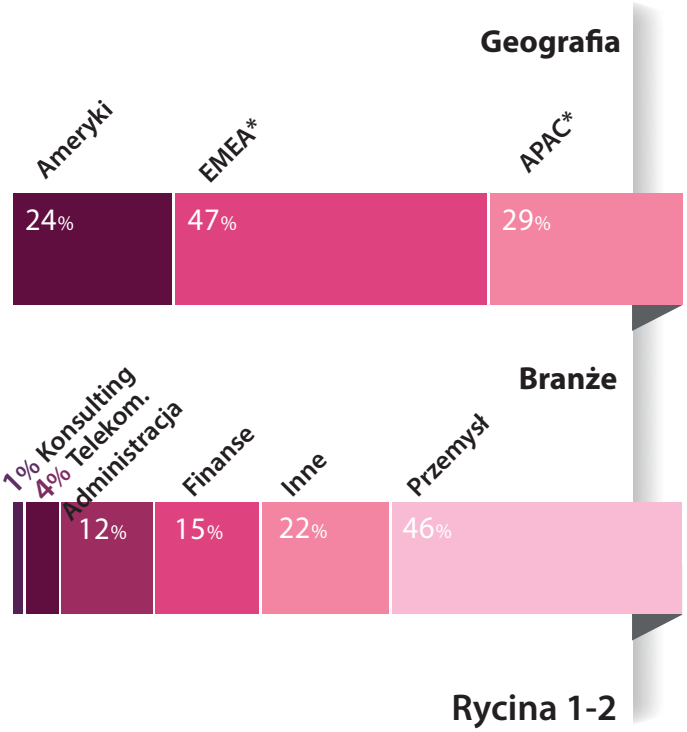
Meta-analizę wypadków bezpieczeństwa w sieci przeprowadzono dla 996 firm przy wykorzystaniu danych zgromadzonych na podstawie szacunków Check Point Security Checkup, które badały przychodzącą i wychodzącą transmisję. Wykorzystano do tego opracowaną przez Check Point wielowarstwową, modułową technologię Software Blade[9], która wykrywa różnorodne programy wysokiego ryzyka, próby wtargnięcia, wirusy, boty, wypadki utraty wrażliwych danych i inne zagrożenia dla bezpieczeństwa. Transmisję monitorowano na żywo dzięki zastosowaniu bram sieciowych bezpieczeństwa Check Point[10] na linii lub w trybie monitorowania (połączenia).

Transmisję dla każdej organizacji monitorowano średnio przed 216 godzin. Firmy biorące udział w naszym badaniu wywodziły się z wielu sektorów, co przedstawia rycina 1-2.

Dodatkowo, na podstawie danych generowanych przez Check Point ThreatCloud przeanalizowano wypadki z 9240 organizacji. ThreatCloud jest potężną bazą danych zabezpieczeń aktualizowaną w czasie rzeczywistym i obejmującą dane zgromadzone na podstawie rozległej sieci globalnych czujników, które strategicznie rozlokowano na całym świecie. ThreatCloud zbiera informacje o zagrożeniach i atakach ze strony złośliwego oprogramowania, dzięki czemu pozwala na identyfikację powstających trendów i zagrożeń bezpieczeństwa, tworząc połączoną sieć mającą walczyć z cyberprzestępczością. Na potrzeby naszych badań zebraliśmy dane z ThreatCloud dotyczące pełnych 12 miesięcy 2013 r., a następnie skonsolidowaliśmy je i poddaliśmy analizie.

Dane zagrożeń ze strony nieznanego złośliwego oprogramowana uzyskano z czujników Check Point Threat Emulation za okres od czerwca do grudnia 2013 r. Check Point Threat Emulation jest opartym na chmurze środowiskiem sandbox, które przeprowadza dynamiczne analizy podejrzanych plików wykrytych przez bramy sieciowe bezpieczeństwa Check Point. Zanonimizowane dane Threat Emulation od 848 organizacji przekazano do ThreatCloud na potrzeby agregacji, korelacji i zaawansowanej analizy.

Wreszcie, przeprowadziliśmy meta-analizę 1036 końcowych raportów bezpieczeństwa dla wielu organizacji. W ramach naszej analizy bezpieczeństwa przeskanowaliśmy każdego hosta, żeby zweryfikować ryzyko utraty danych, ryzyko nieuprawnionego dostępu i ryzyko stawiane przez złośliwe oprogramowanie. Analizę przeprowadzono za pomocą narzędzia raportującego Check Point Endpoint Security, które sprawdza, czy program antywirusowy był uruchomiony na hoście, czy był on aktualny, czy oprogramowanie działało na ostatniej wersji i inne. Narzędzie to jest bezpłatne i powszechnie dostępne. Można je pobrać ze strony internetowej Check Point.

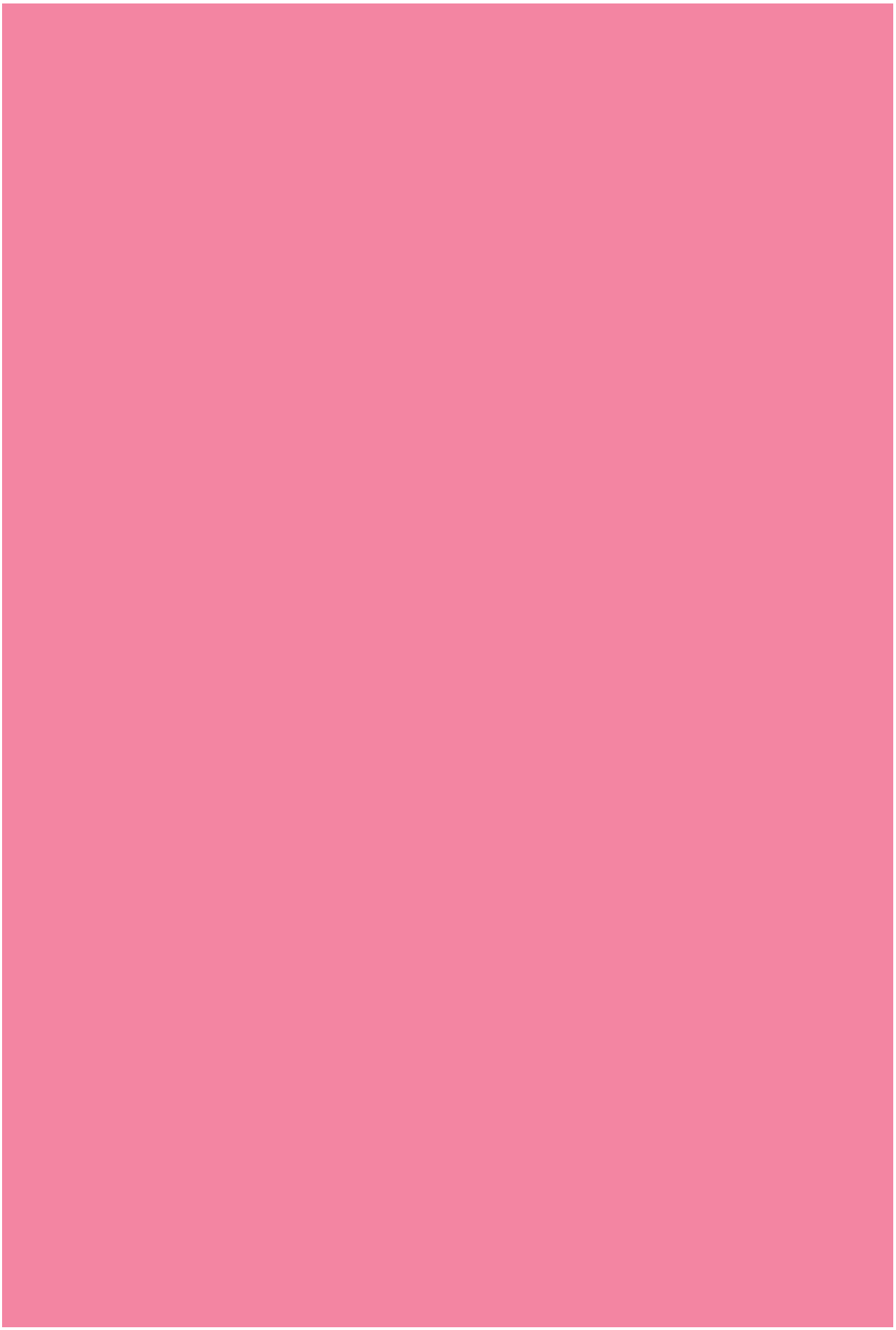


Rycina 1-2

***APAC – Azja Pacyficzna i Japonia;**
***EMEA – Europa, Środkowy Wschód i Afryka**

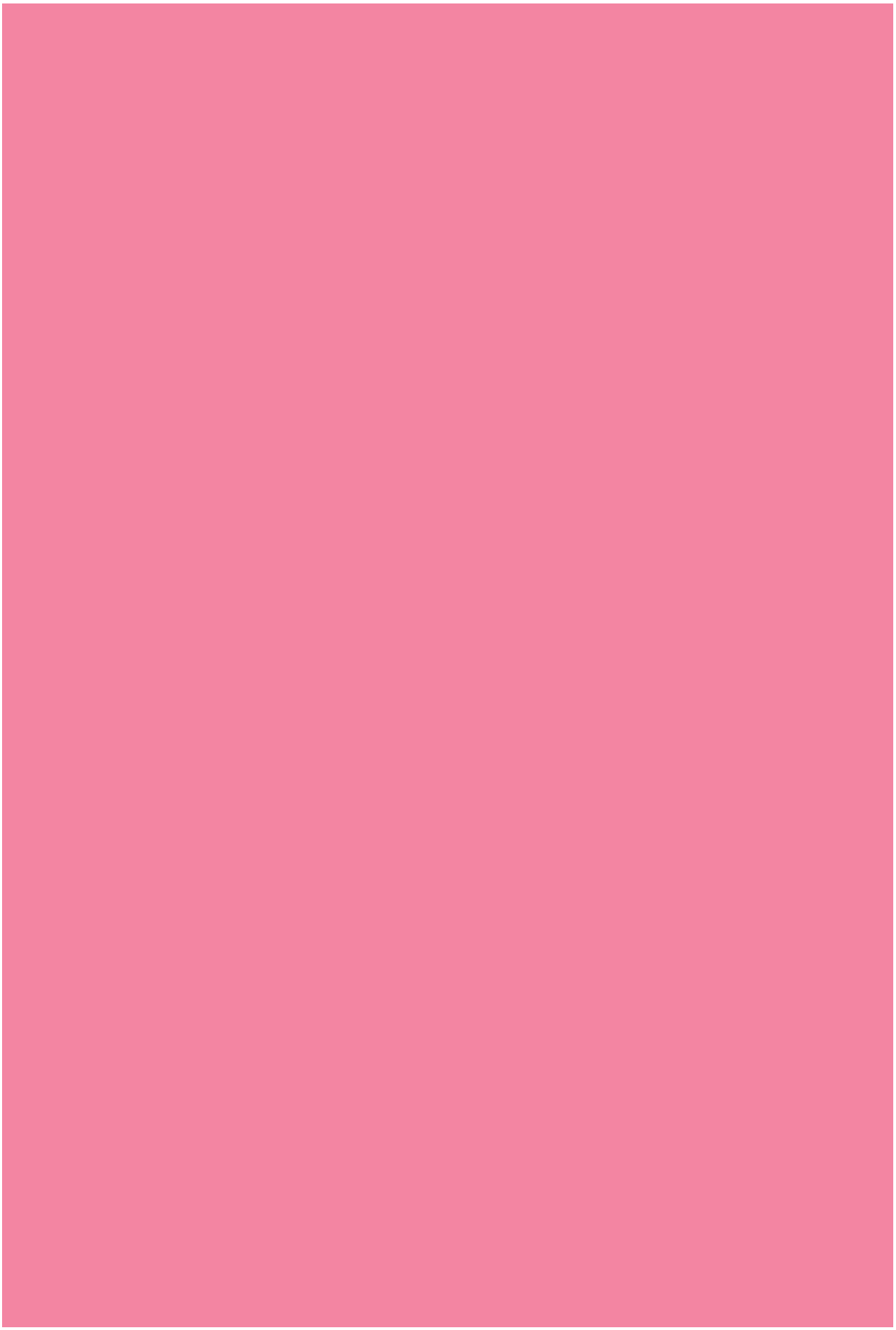
Źródło: Check Point Software Technologies

Kluczowe dane Raportu bezpieczeństwa 2014 Check Point uzupełniono przykładami upublicznionych incydentów, które ukazują cechy charakterystyczne dzisiejszych zagrożeń, ich wpływ na organizacje i implikacje dla społeczności zajmującej się bezpieczeństwem. Rekomendacje ekspertów dają wskazówki, które zapewnią, że wasza strategia bezpieczeństwa i przyjęte rozwiązania będą odpowiednie i skuteczne, jeśli chodzi o ochronę przed dzisiejszymi zagrożeniami bezpieczeństwa. Raport podzielony jest na rozdziały, z których każdy poświęcony jest odpowiednio nieznanemu złośliwemu oprogramowaniu, znanemu złośliwemu oprogramowaniu, programom wysokiego ryzyka i utracie danych.



02

EKSPLOZJA NIEZNANEGO ZŁOŚLIWEGO OPROGRAMOWANIA



02 EKSPLOZJA NIEZNANEGO ZŁOŚLIWEGO OPROGRAMOWANIA

Zagrożenie stawiane przez nieznane złośliwe oprogramowanie

Tradycyjne technologie bezpieczeństwa, jak np. antywirusy czy systemy wykrywania nieautoryzowanego dostępu, bardzo skutecznie wykrywają próby wykorzystania błędów znanego oprogramowania i luk w konfiguracji, a także w pewnym stopniu zapobiegają zagrożeniom ze strony nieznanych eksploitów. Hakerzy zdają sobie z tego sprawę i mogą sobie pozwolić na przetestowanie nowego złośliwego oprogramowania i eksploitów przeciwko tym technologiom, żeby sprawdzić, czy zostaną wykryte.

Ten wyścig zbrojeń między dostawcami rozwiązań bezpieczeństwa a hakerami prowadzi do przyspieszonej ewolucji technik używanych przez hakerów, którzy stale próbują wykorzystywać zarówno nieznane podatności (zwane również jako „zero-day exploits", jako że ich wykrycie i zapobieżenie im zajmuje zazwyczaj godziny lub dni), jak i nieznane metody infekcji w celu obejścia zabezpieczeń.

ZNANE JEST SKOŃCZONE,
NIEZNANE JEST NIESKOŃCZONE.

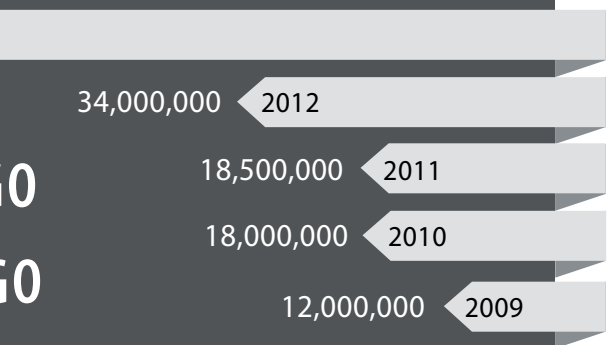
Thomas Henry Huxley[11]

Pod koniec roku 2013 badacze złośliwego oprogramowania z Check Point, pracując na naszej usłudze Threat Emulation, odkryli i przeanalizowali nową odmianę złośliwego oprogramowania, która w wyrafinowany sposób łączyła techniki mające uniemożliwić jego wykrycie przez proxy i rozwiązania anty-malware'owe. Określany jako HIMAN[12] przez badaczy z branży, ten złośliwy program ilustruje cechy charakterystyczne ataków kierowanych i uzmysławia, dlaczego stanowią one wyzwanie dla przedsiębiorstw i profesjonalistów zajmujących się bezpieczeństwem IT na całym świecie.

Bramka bezpieczeństwa obsługiwana przez klienta Check Point korzystającego z usługi Threat Emulation przeskanowała dokument Microsoft Word, który był załączony do wiadomości e-mail od adresu boca_juniors@aol.com o temacie „Reception Invitation" (pol. Zaproszenie na przyjęcie).

144%

WZROSTU NOWEGO ZŁOŚLIWEGO OPROGRAMOWANIA WYKRYTEGO W 2013 R. W STOSUNKU DO 2012 R.



Źródło: AV-Test.org

Rycina 2-1

2.2

NIEZNANE ZŁOŚLIWE PROGRAMY UDERZAŁY W ORGANIZACJĘ CO GODZINĘ

Kiedy dokument zostaje otwarty w środowisku sandbox, wykorzystuje znaną podatność (CVE-2012-0158), żeby umieścić plik „kay.exe" w katalogu użytkownika Local Settings\Temp na zaatakowanym komputerze. Nazwa droppera wydaje się być pułapką i przypomina plik wykonywalny antywirusa Kaspersky[13], zaś samo złośliwe oprogramowanie zdaje się być związane z wcześniejszymi kampaniami malware'owymi, które badacze przypisali jednej lub paru chińskim grupom APT. Analiza wykazała, że plik jest tak naprawdę dwuetapowym dropperem, który zmienia swoją nazwę w procesie instalacji na docelowym systemie, a następnie zaczepia się o plik.exe explorera, żeby załadować złośliwy plik DLL.

Badacze bezpieczeństwa z Check Point sprawdzili bazy danych znanego złośliwego oprogramowania i zauważyli, że żaden dostawca rozwiązań antywirusowych nie był w stanie wykryć tego złośliwego oprogramowania w momencie, kiedy je spostrzeżono.

Złośliwe oprogramowanie wgrywało złośliwą bibliotekę (mswins64.dll), wykorzystując szereg wywołań funkcji i sprawdzeń wzajemnego wykluczania, żeby zainstalować złośliwe oprogramowanie na systemie klienta w taki sposób, żeby uniknąć wykrycia przez istniejące rozwiązania antywirusowe. Tuż po zainstalowaniu złośliwe oprogramowanie dodaje wpis do rejestru, wykorzystując ścieżkę rejestru inną niż te, z których złośliwe procesy powszechnie korzystają, a które są w związku z tym znacznie bardziej monitorowane przez programy antywirusowe. To połączenie rzadziej używanych połączeń API i ścieżek rejestru pozwala złośliwemu oprogramowaniu zwiększyć szanse na uniknięcie wykrycia.

HIMAN pokazuje, że twórcy złośliwego oprogramowania wykorzystują specjalistyczną wiedzę w zakresie wywołań Windows API, zachowania systemu operacyjnego i działania narzędzi anty-malware'owych, żeby uniknąć wykrycia, bez konieczności i nie ponosząc kosztów opracowania lub zakupu prawdziwej podatności „zero-day". To wyrafinowanie dotyczy również komunikacji C&C (command and control) i procesów eksfiltracji: HIMAN może wykorzystać algorytmy brute-force przeciwko serwerowi proxy transmisji wychodzącej dzięki zgromadzonym danym logowania, zaszyfrować zgromadzone dane przy pomocy AES[14] i zastosować techniki zaciemnienia w czasie eksfiltracji, żeby uniknąć filtrowania wychodzącego.

Jak tylko zostanie z powodzeniem zainstalowany i kiedy ustanowi zweryfikowane połączenie z serwerem C&C, HIMAN w dynamiczny sposób tworzy i uruchamia skrypt pozwalający na zbieranie danych o działających usługach, lokalnych kontach posiadających prawa administratora i innych informacji o konfiguracji systemu czy jakichkolwiek części sieci, które są widzialne dla zainfekowanej maszyny. Uzbrojony w tę informację agresor ma mapę sieci lokalnej i punkt zaczepienia w atakowanej organizacji do dalszego rekonesansu, ruchu poprzecznego, eksfiltracji i przeprowadzania ataków na serwery, systemy i procesy biznesowe.

Wykorzystując połączenie znanych i rzadko spotykanych środków, żeby zdobyć punkt zaczepienia w sieci obranej za cel organizacji i wykraść wrażliwe dane, HIMAN stanowi idealny przykład zarówno na elastyczność twórców złośliwego oprogramowania, jak i wyzwania, przed którymi stoją osoby profesjonalnie zajmujące się bezpieczeństwem w 2013 r.

MNIEJ NIŻ 10% SILNIKÓW ANTYWIRUSOWYCH WYKRYŁO ZŁOŚLIWE OPROGRAMOWANIE, KIEDY PIERWSZY RAZ ZŁAPANO JE NA WOLNOŚCI.

TWORZENIE NIEZNANYCH PROGRAMÓW JEST

TAK PROSTE, ŻE DZIECKO POTRAFIŁOBY TO ZROBIĆ

Jak to się stało? Ewolucja nieznanego złośliwego oprogramowania

Przez wiele lat zagrożenia ze strony kierowanych ataków i zaawansowanych zagrożeń długotrwałych (ang. advanced persistent threats, APT) cieszyły się dużym zainteresowaniem świata bezpieczeństwa informacji. APT pojawiły się na scenie w 2010 roku wraz z atakami Stuxnetu[15], w których wysoce wyspecjalizowany, specjalnie skonstruowany złośliwy program zdestabilizował cały system kontroli irańskiej wirówki jądrowej pod wpływem finansowanego przez państwo połączonego ataku kinetycznego i cybernetycznego.

Ta nowa odmiana złośliwego oprogramowania postawiła wyzwanie wielu typowym środkom obronnym z trzech powodów. Po pierwsze, Stuxnet był wysoce wyspecjalizowany, bowiem został opracowany na potrzeby konkretnego systemu, w konkretnym środowisku i miał za zadanie spełnić konkretny cel. Po drugie, był bardzo rzadki, co oznaczało, że nigdy nie był narażony na działanie sieci zbiorczych i analitycznych, jakie dostawcy rozwiązań antywirusowych opracowali, żeby nadążyć za „rynkiem masowym" wirusów i botów, które definiowały krajobraz złośliwego oprogramowania od dziesięciu lat. W związku z tym Stuxnet nie rzucał się w oczy i działał w ukryciu przez niewiadomy okres – potencjalnie latami. W końcu, motyw opracowania Stuxnetu znacznie różnił się od tego, który stał za wirusami i większością robaków, jak np. Code Red[16] lub Sasser[17], które po nich nastąpiły; mianowicie, nie opierał się na zbieraniu punktów o kluczowym znaczeniu. Ze względu na ten motyw było jasne, że ktokolwiek stoi na Stuxnetem, nie da łatwo za wygraną.

W skrócie, Stuxnet stanowił nowy rodzaj złośliwego oprogramowania, z którym istniejące antywirusy i technologie wykrywania nieautoryzowanego dostępu nie potrafiły sobie poradzić – kierowanego, rzadkiego i zmotywowanego. W tym znaczeniu był on awangardą fali zindywidualizowanego złośliwego oprogramowania, które wymagało nowego zestawu narzędzi i strategii. Pojawienie się HIMAN podkreśla trwającą ewolucję tego trendu i zagrożenia, jakie sobą przedstawia.

33%
ORGANIZACJI ŚCIĄGNĘŁO CO NAJMNIEJ JEDEN PLIK ZAINFEKOWANY NIEZNANYM ZŁOŚLIWYM OPROGRAMOWANIEM

KIEROWANY ATAK, GLOBALNA KAMPANIA

22 października 2013 r. pewna firma medialna otrzymała 6 podejrzanych e-maili, które zostały następne przeanalizowane przez usługę Check Point Threat Emulation service.

- Od: No-Replay@UPS.COM
- Temat: UPS Delivery Notification (pol. Informacje o przesyłce UPS)
- Załącznik: invoiceBQW8OY.doc (pol. fakturaBQW8OY.doc)
  (MD5 ad0ef249b1524f4293e6c76a9d2ac10d)

W czasie automatycznej symulacji w wirtualnej piaskownicy, w której użytkownik otwierał potencjalne złośliwy plik, wykryto następujące nienormalne zachowania:

- Microsoft Word zawiesił się, wyłączył się i włączył ponownie, pokazując pusty dokument.
- Dodany został klucz do rejestru.
- Na końcowym urządzeniu uruchomił się nowy proces.

W związku z tym Check Point Threat Emulation uznał, że plik jest złośliwy.

Dalsza analiza przeprowadzona przez analityków bezpieczeństwa Check Point odkryła, że dokumenty ze wszystkich sześciu wiadomości e-mail wykorzystywały podatność CVE-2012-0158 w Microsoft Word. Podatność ta, znana również jako MSCOMCTL.OCX RCE[18], pozwala na zdalne wykonanie kodu na urządzeniu końcowym.

Analiza wykazała, że złośliwym dodatkiem był zindywidualizowany wariant ZBOT Trojan[19], który kradnie informacje za pomocą ataków man-in-the-browser, przechwytywania klawiszy (ang. key logging), przechwytywania danych wysyłanych przez przeglądarkę (ang. form grabbing) i innych metod. Zarejestrowanie tych próbek na VirusTotal[20] wykazało niski (<10 procent) współczynnik wykrycia zarówno dla złośliwego załącznika, jak i odmiany programu ZBOT w momencie zgłoszenia.

Badacze zabezpieczeń z Check Point przeanalizowali różne adresy, z jakich złośliwy dokument był ściągany, i ustalili, że listą unikalnych parametrów przekazywanych zainfekowanym serwerom był w gruncie rzeczy zakodowany w base64 desygnator celu zawierający docelowy adres. Te unikalne URL zawierały adresy e-mail użytkowników w dużych organizacjach międzynarodowych – jak np. instytucjach finansowych, międzynarodowych producentach samochodów, firmach z branży telekomunikacyjnej, agencjach rządowych, a także organizacjach edukacyjnych i miejskich ze Stanów Zjednoczonych – które były celami ataków. Cele te wskazują, że ataki są częścią kierowanej kampanii mającej na celu przechwycenie danych logowania użytkowników, informacji bankowych i innych, które można by wykorzystać, żeby zdobyć dostęp do najbardziej wrażliwych danych atakowanej organizacji.

35%

PLIKÓW ZAINFEKOWANYCH ZŁOŚLIWYM OPROGRAMOWANIEM TO PLIKI PDF

2013: Obiecujący początek, rozczarowujący koniec

Administratorzy bezpieczeństwa posiadają coraz większą wiedzę, nie tylko jeśli chodzi o same kierowane ataki, ale również nowe narzędzia, które pomagają je odeprzeć. Zespoły bezpieczeństwa w dużych przedsiębiorstwach i organach publicznych były dobrze zaznajomione ze zautomatyzowanymi, sieciowymi technologiami sandbox wymierzonymi przeciwko złośliwemu oprogramowaniu. Stosowano je jako dodatkowe warstwy w ramach istniejącej infrastruktury zabezpieczeń, żeby łatwiej wykrywać kierowane złośliwe oprogramowanie, które w przeciwnym razie umknęłoby opartemu na sygnaturze i reputacji systemowi ochronnemu ulokowanemu na bramie i w punkcie końcowym.

Jednakże w 2013 r. odnotowano zdecydowany wzrost częstotliwości użycia „nieznanego złośliwego oprogramowania" – i ataków, które zastosowały techniki zaciemniania i uników właściwe dla APT do znanego złośliwego oprogramowania w kierowanych kampaniach o ogólnoświatowym zasięgu (zob. dodatek „Kierowany atak, globalna kampania"). Podczas gdy precyzyjne, kierowane ataki przy wykorzystaniu wysoce wyspecjalizowanego złośliwego oprogramowania pozostają niemałym wyzwaniem, w dniu dzisiejszym „masowa indywidualizacja" oznacza, że zwiększona skuteczność kierowanego złośliwego oprogramowania dostępna jest zakrojonym na szerszy zasięg kampaniom, które kierują się zyskiem finansowym.

„Nieznane" lub „zero-day"

Trzeba rozróżnić nieznane złośliwe oprogramowanie i to, co powszechnie określa się mianem podatności „zero-day" (pol. dnia zero). Zero-day wykorzystuje nieznaną lub niezgłoszoną uprzednio podatność, dla której nie ma łaty. „Nieznane złośliwe oprogramowanie" odnosi się z kolei do złośliwego kodu, który wykorzystuje znaną podatność, ale którego w momencie jego odkrycia nie potrafią wykryć nawet zaktualizowane programy antywirusowe ani rozwiązania anty-botowe, ani systemy wykrywania nieautoryzowanego dostępu. Okres skuteczności nieznanego złośliwego oprogramowania wynosi często zaledwie 2-3 dni, ponieważ jego istnienie „na wolności" daje dostawcom antywirusowym czas na jego wykrycie w globalnych sieciach i zbudowanie dla niego sygnatur.

Jest to bardzo ważne rozróżnienie, ponieważ pozwala nam zrozumieć prawdziwą naturę złośliwego oprogramowania, które eksplodowało na scenie w 2013 roku.

Poznawanie nieznanego

W 2013 r. silniki emulacyjne Check Point – zaawansowana forma zautomatyzowanego środowiska sandbox złośliwego oprogramowania – rozlokowane na całym świecie wykryły, że 2,2 nieznane złośliwe programy atakowały organizacje każdej godziny, co łącznie daje 53 programy na dzień.

Badania Check Point dowodzą, że dwa główne czynniki przyczyniły się do tego nagłego wzrostu częstotliwości:

1. Napastnicy stosowali zautomatyzowane mechanizmy w celu stworzenia nieuchwytnego, nieznanego złośliwego oprogramowania na wielką skalę, a następnie atakowali organizacje na całym świecie w ramach skoordynowanych kampanii, żeby zmaksymalizować ich skuteczność.
2. Manualne procesy dochodzenia i reagowania, które stosowano, żeby zminimalizować wpływ kierowanych ataków, nie były w stanie sprostać wielkiej liczbie incydentów.

Jak działa środowisko sandbox

Rycina 2-2

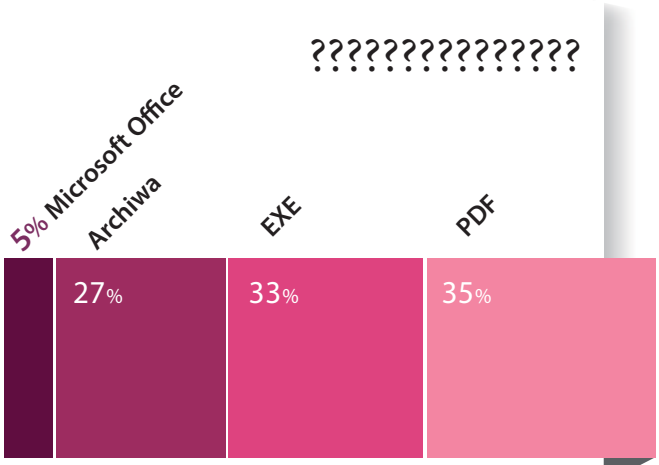
Analiza wykryć w 2013 r. pokazuje, że większość złośliwego oprogramowania trafiło do docelowych konsumentów za pośrednictwem e-maili, najczęściej w postaci załączników. W 2013 r. to format PDF okazał się najpopularniejszy, odpowiadając za niemal 35% plików wykrytych przez emulację jako zawierających złośliwe oprogramowanie, a które miały na celu wykorzystanie niezaktualizowanych wersji programu Adobe Reader (rycina 2-3). Prowadzone badania pokazują, że również formaty EXE i archiwów cieszą się popularnością, odpowiadając odpowiednio za 33% i 27% przeanalizowanych złośliwych plików.

Ze wszystkich formatów plików Microsoft Office najpopularniejszym był Word (.doc), chociaż nasza analiza testowania złośliwego oprogramowania w środowisku sandbox pokazuje, że napastnicy rozprzestrzeniali swoje ataki także za pośrednictwem innych formatów. Ogólnie rzecz biorąc, wykryliśmy nieznane złośliwe oprogramowanie w 15 różnych typach plików Office, w tym szablonach dla Worda i PowerPointa, a także wielu formatach Excela. Chociaż większość złośliwych archiwów miała format ZIP – prawdopodobnie z tego względu, że wszystkie systemy Windows mogą otwierać archiwa ZIP – analiza Check Point wykryła złośliwe oprogramowanie we wszystkich innych popularnych formatach archiwów, jak TAR, RAR, 7z i CAB.

2,2 NIEZNANE ZŁOŚLIWE PROGRAMY ATAKOWAŁY ORGANIZACJE KAŻDEJ GODZINY, CO ŁĄCZNIE DAJE **53 PROGRAMY NA DZIEŃ**

Powódź nowego złośliwego oprogramowania

Analiza danych złośliwego oprogramowania z 2013 r. przeprowadzona przez Check Point zwraca uwagę na dużą częstotliwość wykrywania nieznanego złośliwego oprogramowania na bramach sieciowych na całym świecie. Dane z zewnętrznych źródeł potwierdzają to odkrycie. AV-TEST[21], niezależny instytut bezpieczeństwa IT i badań antywirusowych, rejestruje ponad 220 tysięcy nowych złośliwych programów każdego dnia – w 2013 r. AV-TEST zarejestrował ponad 80 milionów nowych złośliwych programów, ponad dwa razy więcej niż w 2012 r.



Rycina 2-3

Źródło: Check Point Software Technologies

Nasze badania danych złośliwego oprogramowania w 2013 r. rzucają znacznie więcej światła na ten trend i jego duże znaczenie. Z całej naszej grupy badawczej jedna trzecia organizacji ściągnęła przynajmniej jeden plik zarażony nieznanym złośliwym oprogramowaniem.

OPOWIEŚCI Z CRYPTERA

Żeby uniknąć wykrycia przez oprogramowanie anty-malware'owe, współcześni twórcy złośliwego oprogramowania używają specjalnych narzędzi zaciemniających, zwanych crypterami. Żeby sprawdzić, czy ich warianty nie zostały wykryte, twórcy złośliwego oprogramowania unikają antywirusowych platform skanujących online, jak np. VirusTotal czy innych, które dzielą się próbkami z dostawcami rozwiązań anty-malware'owych, zamiast tego korzystając z prywatnych usług, jak razorscanner, vscan (zwany inaczej NoVirusThanks) i chk4me. Społeczności hakerskie dzielą cryptery na UD (UnDetectable, pol. niewykrywalne) i FUD (Fully UnDetectable, pol. całkowicie niewykrywalne) według tego, jak dobrze udaje im się unikać wykrycia przez antywirusy.

W 2013 r. Check Point Threat Emulation wykrył zaszyfrowany i wcześniej nieznany wariant złośliwego oprogramowania mający dostarczyć narzędzie zdalnego administrowania DarkComet (ang. remote administration tool, RAT)[23]. W przypadku naszej wykrytej próbki, wbudowany ciąg PDB ujawnił, że stanowi on produkt iJuan Crypter, który dostępny jest online zarówno w wersji darmowej (UD), jak i płatnej wersji premium (FUD). Z technicznego punktu widzenia można go zaklasyfikować jako Portable Executable (PE)[24] i nie należy mylić go z szyfrującym ransomware, jak np. Cryptolocker[25]. Cryptery tego rodzaju ukrywają pliki wykonywalne dzięki zastosowaniu różnorodnych technik szyfrowania i kodowania, sprytnie połączonych raz i drugi, często wielokrotnie.

Wykrytą próbkę, która była w stanie uniknąć większości rozwiązań antywirusowych, porównano z podobnym przypadkiem z innego kraju, który okazał się odmiennie zaciemnioną wersją ładunku DarkComet, a który komunikował się z tym samym serwerem C&C. Te dwa czynniki łącznie wskazują, że te dwa odrębne przypadki wykrycia – jeden w Europie, drugi w Ameryce Łacińskiej – stanowią tak naprawdę część tej samej kampanii.

Wykrycia te uwydatniają wewnętrzne mechanizmy rodziny zaawansowanych ataków, które zmieniają zarówno krajobraz zagrożeń, jak i zakres rozwiązań, których zarządcy bezpieczeństwa potrzebują, żeby bronić swoich sieci i danych.

Ta eksplozja nieznanego złośliwego oprogramowania napędzana jest w pewnym stopniu przez łatwą dostępność technik zaciemniania, które w przeszłości wymagały specjalistycznej wiedzy, narzędzi lub obu tych czynników (dodatek: Opowieści z cryptera)[22]. Przypadki, jakie przeanalizowaliśmy w tym rozdziale, pokazują sposoby, dzięki którym obecnie rozprowadzane złośliwe oprogramowanie uzyskało wyższy stopień zaawansowania, niż powszechnie towarzyszący zwykłym jego odmianom. Ten wyższy stopień zaawansowania sprawia, że wyzwanie, jakie programy te stawiają, jest jeszcze większe, gdyż wymaga zastosowania bardziej subtelnych i inteligentnych metod wykrycia i analizy, dodatkowo na skalę wykraczającą poza zakres zasobów dostępnych zarządzaniu, monitorowaniu i reagowaniu na wypadki w wielu organizacjach.

Zalecenia

Eksplozja nieznanego złośliwego oprogramowania, jaka miała miejsce w 2013 r., oznacza, że organizacje muszą ponownie przyswoić sobie narzędzia i procesy, które stosuje się głównie do wykrycia niewielkich ataków kierowanych i reagowania na nie. Programy, które pozwalają wyłącznie na wykrywanie, wymagające dodatkowo ręcznego łagodzenia i którym brak funkcji automatycznego blokowania, sprawiają, że zespoły zajmujące się bezpieczeństwem nie radzą sobie w walce z falami złośliwego oprogramowania, jakie atakuje ich sieci, i są przeciążone.

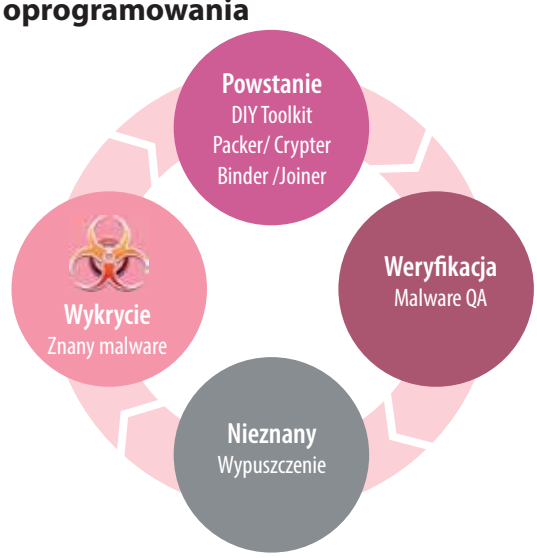
Emulacja i zaawansowane automatyczne izolowanie złośliwego oprogramowania w środowisku sandbox stały się obecnie koniecznymi rozwiązaniami dla każdej organizacji. Nawet najczulsze i najszybsze rozwiązanie antywirusowe, antybotowe i IPS będzie mieć dwu- lub trzydniowe okienko, w czasie którego nieznane złośliwe oprogramowanie nie będzie wykryte – okres, który jest zdecydowanie wystarczający, żeby napastnik zdobył punkt zaczepienia w organizacji.

Cykl życiowy złośliwego oprogramowania

Dly Kit/Malware Tookit
Spy Eye
Zeus Builder
Citadel Builder

Crypter/Packer
UPX GUI
PFE CX
Indectables.net

Joiner/Binder
File joiner
ExeBundle



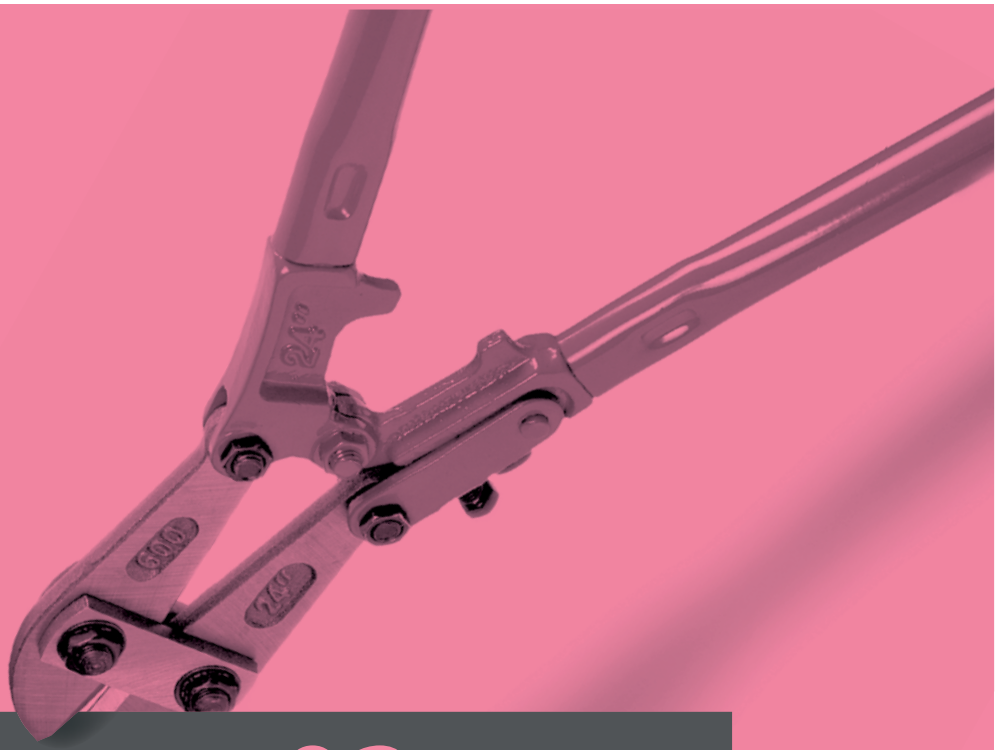
Malware QA
Multi AV Scan
NoVirus Thanks

Co najważniejsze, te rozwiązania muszą stanowić integralną część infrastruktury zabezpieczeń w organizacji, aniżeli dodatkową warstwę, która znajduje się na wierzchu tej infrastruktury. Organizacje powinny szukać rozwiązań emulacyjnych, które zapewnią:

- **Integrację** – bezproblemowa integracja z istniejącą infrastrukturą bram sieciowych, poczty i punktu końcowego jest jedynym sposobem, żeby pokonać i ulokować, nie zwiększając stopnia skomplikowania i kosztów. Integracja poczty jest szczególnie istotna, ponieważ poczta jest głównym wektorem ataku przeciwko klientom w sieci i poza siecią;
- **Prewencję** – podejścia nastawione wyłącznie na wykrycie nie są już skuteczne w starciu z dużymi atakami nieznanego złośliwego oprogramowania. Organizacje muszą poszukiwać rozwiązań prewencyjnych, które zapewnią im możliwość wykrycia i automatycznego blokowania nieznanego złośliwego oprogramowania, zanim będzie mogło ono dotrzeć do celu;
- **Automatyzację** – zminimalizowanie procesów manualnych na potrzeby analizy i łagodzenia pozwala organizacjom sprostać atakom, jednocześnie spełniając inne cele dot. bezpieczeństwa i cele biznesowe. Zautomatyzowana prewencja jest niezmiernie istotna, ale równie ważna dla skutecznego powiadamiania i reagowania jest integracja raportowania i przepływu pracy.

Szybki rozwój nieznanego złośliwego oprogramowania w wyraźny sposób zmienia reguły gry w bezpieczeństwie, wymagając nowych strategii i technologii, a także nowego podejścia do zabezpieczeń, które zapewniłoby skuteczną ochronę, nie uszczuplając jednocześnie zasobów organizacji. Dostosowanie się do tych nowych wymogów powinno być postrzegane jako ścisły priorytet – i to w trybie pilnym – dla każdej organizacji. W tym samym czasie dobrze znane i mające długą tradycję ataki nadal przedstawiają poważne zagrożenie, wymagając stałej czujności i proaktywnych środków zaradczych. W kolejnym rozdziale przyjrzymy się najbardziej aktualnym trendom dotyczącym znanego złośliwego oprogramowania.

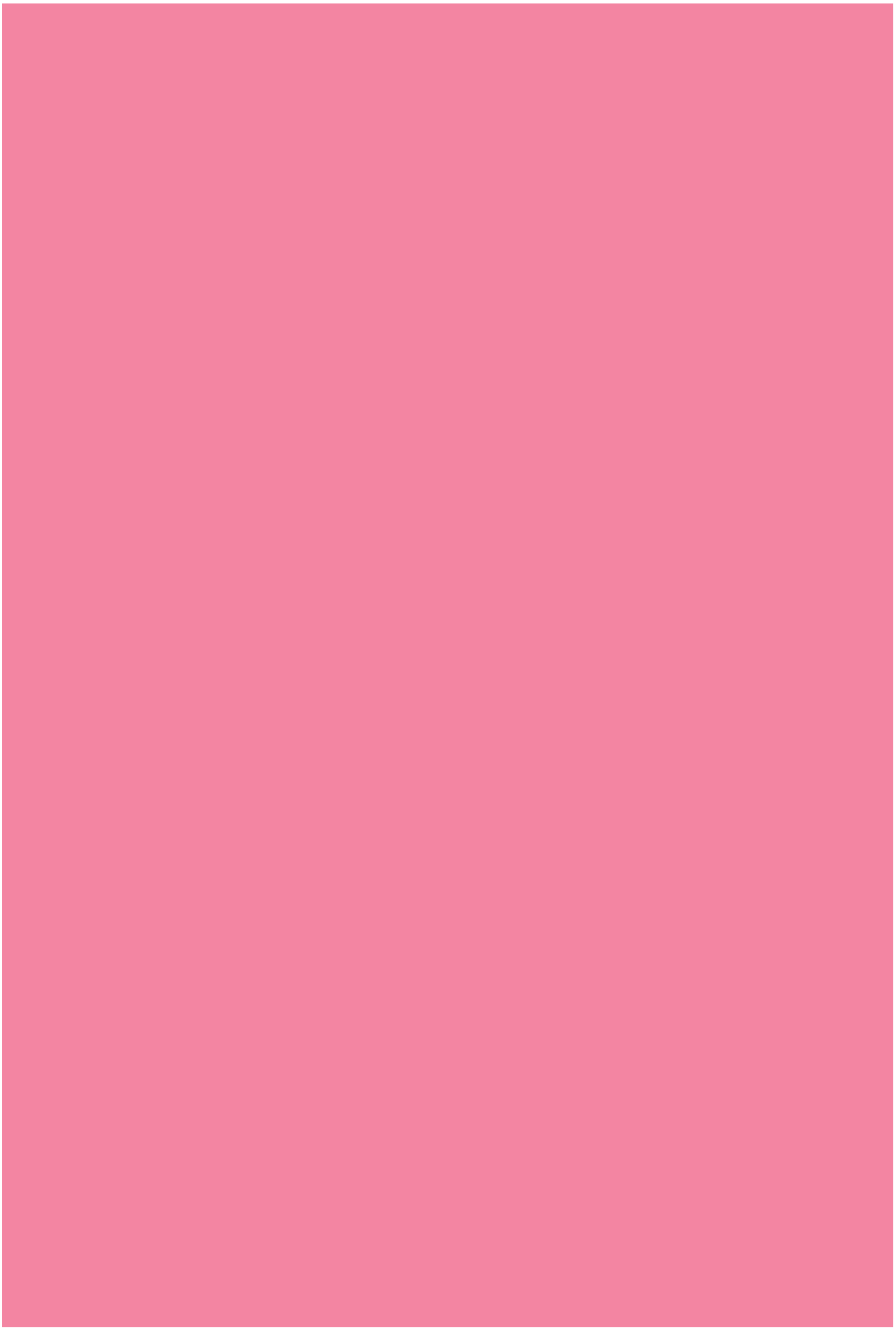
EMULACJA I ZAAWANSOWANE AUTOMATYCZNE IZOLOWANIE ZŁOŚLIWEGO OPROGRAMOWANIA W ŚRODOWISKU SANDBOX STAŁY SIĘ OBECNIE **KONIECZNYMI ROZWIĄZANIAMI** DLA KAŻDEJ ORGANIZACJI.



03

DIABEŁ, KTÓREGO ZNASZ

Złośliwe oprogramowanie w firmie



03 DIABEŁ, KTÓREGO ZNASZ: ZŁOŚLIWE OPROGRAMOWANIE W FIRMIE

Bezpieczeństwo informacji zdominowało pierwsze strony gazet w 2013 r., poczynając od rewelacji o finansowanym przez państwo programie inwigilacji cyberprzestrzeni przez hakowanie organizacji medialnych, jak Washington Post czy Yahoo, aż do głośnych epidemii złośliwego oprogramowania, jak Cryptolocker i naruszeń danych konsumentów detalicznych na skalę, która przyćmiewa wszystko to, co nastąpiło wcześniej.

Rok 2012 sprawia wrażenie bardzo spokojnego w porównaniu do ostatniego roku – a w żadnym razie rok 2012 nie był okresem cybernetycznej ciszy. Tamten rok był sam w sobie szczególny ze względu na ilość i skalę cyberataków, w tym rozwijający się haktywizm, finansowane przez państwo włamania do mediów i przedsiębiorstw oraz naruszenia danych w instytucjach finansowych na całym świecie. Główne trendy dot. złośliwego oprogramowania w 2012 r. na podstawie „Raportu Bezpieczeństwa Check Point 2013"[27] to:

- Demokratyzacja zaawansowanych trwałych zagrożeń;
- Wszechobecność botnetów;
- Wzrost liczby podatności zwiększających powierzchnię ataku.

> PRZEZ DZIESIĘCIOLECIA OBAWIALIŚMY SIĘ BRONI MASOWEGO RAŻENIA. TERAZ NADSZEDŁ CZAS, ŻEBYŚMY ZACZĘLI OBAWIAĆ SIĘ BRONI MASOWEGO ZAKŁÓCANIA.
>
> **John Mariotti**[26]

W naszych badaniach zauważyliśmy, że te trendy nie tylko nadal trwały w 2013 r., ale także rozwinęły się niemal pod każdym względem, czy jeśli chodzi o częstotliwość, z jaką złośliwe oprogramowanie wkracza do organizacji, czy zakres i powagę zarażeń botami.

Szybciej nie zawsze znaczy lepiej

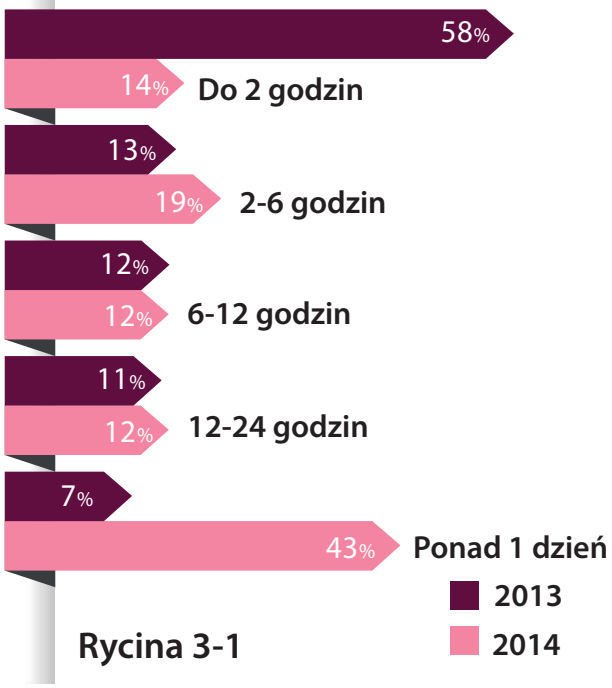
Jeśli istnieje jedna dana statystyczna z badań bezpieczeństwa roku 2013 przeprowadzonych przez Check Point, która najlepiej odzwierciedla wyzwanie stawiane przez złośliwe oprogramowanie, jakie stoi przed administratorami bezpieczeństwa, będzie nią rosnąca częstotliwość, z jaką organizacje przez nas przebadane pobierały złośliwe oprogramowanie (rycina 3-1). W 2012 r. w niemal połowie (43%) organizacji, jakie przeanalizowaliśmy, użytkownicy pobierali złośliwy program w tempie mniej niż jeden na dzień, a pozostałe 57% pobierały złośliwy program co każde 2-24 godziny.

84%

ORGANIZACJI ŚCIĄGNĘŁO ZŁOŚLIWY PLIK

Z kolei w 2013 r. w niemal dwóch trzecich (58%) organizacji użytkownik pobierał złośliwe oprogramowanie co dwie godziny lub mniej. Ten wzrost częstości cyberataków na organizacje znajduje odzwierciedlenie we wszystkich statystykach z naszego ostatniego badania dot. bezpieczeństwa. W tym rozdziale przyjrzymy się specyfice tej zmiany i jej implikacjom dla bezpieczeństwa i administratorów, przy czym najpierw zobaczymy, jakie zmiany w podatnościach stanowią powierzchnię ataku dla twórców złośliwego oprogramowania i hakerów.

Częstość pobrań złośliwego oprogramowania (% organizacji)



Rycina 3-1

Źródło: Check Point Software Technologies

Mniej podatności czy fałszywa nadzieja?

Jedynym zagrożeniem na krajobrazie bezpieczeństwa informacji, które nie wzrosło w 2013 r., jest liczba raportowanych podatności. Na pierwszy rzut oka może wydać się to pocieszające w świetle danych z 2012 r., które sugerowały, że ostatni trend spadkowy, jeśli chodzi o raportowane podatności, odwrócił się, jako że ich liczba wzrosła o 27% w porównaniu do 2011 r. do 5297, jak podaje baza danych Common Vulnerabilities and Exposures (CVE) (rycina 3-2). Faktycznie, w 2012 r. liczba podatności wzrosła, przez co zwiększył się zarówno obszar do ataku, a także

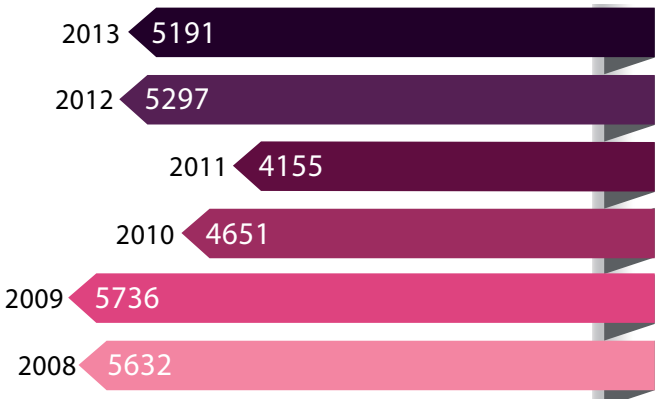
W 58% ORGANIZACJI UŻYTKOWNIK POBIERAŁ ZŁOŚLIWE OPROGRAMOWANIE **CO DWIE GODZINY LUB MNIEJ**

obszar, jakiego administratorzy bezpieczeństwa – już borykający się z wprowadzeniem urządzeń mobilnych i usług konsumenckich do sieci firmy – musieli bronić.

Ale czy tak naprawdę rok 2013 przedstawia pozytywny trend? Pod pewnymi względami na pewno. Obrona przed podatnościami opiera się zazwyczaj na dwóch podejściach:

- Stosowaniu dostępnych łat od dostawcy w celu naprawy podatności w zabezpieczeniach. Dla systemów klienckich dokonywane jest to dziś często automatycznie, po minimalnym okresie testowania lub przy jego całkowitym braku; dla serwerów konieczne jest zazwyczaj dodatkowe testowanie, żeby zweryfikować, czy łaty nie wywołują żadnych skutków ubocznych.
- Rozmieszczaniu systemu wykrywania nieautoryzowanego dostępu (IPS) w celu wykrycia i, jeśli konieczne, zablokowania prób wykorzystania znanych podatności w zabezpieczeniach; rozwiązanie to bywa czasem wykorzystywane tymczasowo do momentu, kiedy będzie można zastosować aktualizację w ramach normalnego cyklu dystrybucji łat. W pozostałych przypadkach IPS jest głównym długoterminowym sposobem obrony dla systemów, którym z rozlicznych powodów nie można dostarczyć koniecznych łat.

Całkowita liczba CVE (powszechnych podatności i ekspozycji)



Rycina 3-2

Źródło: baza danych Common Vulnerabilities and Exposures (CVE)

CO 60 SEKUND HOST WCHODZIŁ NA ZŁOŚLIWĄ STRONĘ INTERNETOWĄ

Liczba nowych raportowanych podatności w zabezpieczeniach ma zazwyczaj bezpośrednią pozytywną korelację z obciążeniem zabezpieczeń i organizacji IT. W tym świetle rok 2013 na pewno przyniósł parę dobrych informacji dla przeciążonych administratorów bezpieczeństwa. Bazy danych CVE dowodzą spadku liczby raportowanych podatności do 5191 na rok, skromny spadek o 2 procent na rok z 2012 r. i obejmowały 9-procentowy spadek liczby raportowanych „krytycznych" luk w zabezpieczeniach.

Ale historia nie jest tak czarno-biała, jak mogłoby się wydawać. Podczas gdy zgłoszono mniej podatności, eksperci branżowi zgadzają się, że coraz większa liczba tych krytycznych odciągana jest przez szare i czarne rynki – zjawisko potencjalnie znacznie bardziej złowieszcze (dodatek: Dzień zero, grube dolary).

DZIEŃ ZERO, GRUBE DOLARY

Pomimo zwiększenia się liczby programów wynagrodzeniowych prowadzonych przez producentów, które nagradzają wykrycie podatności, wysoka wartość rynkowa prawdziwych podatności zero-day sprawia, że odkrywcy sprzedają je „szarym kapeluszom"[28] w agencjach rządowych – tym, którzy pracują razem z hakerami w celu maksymalizacji swoich zdolności obronnych – i profesjonalnym organizacjom zajmujących się testami penetracyjnymi. Jeszcze bardziej lukratywny podziemny rynek obsługuje „czarne kapelusze"; ceny wcześniej niezgłoszonych luk wahają się na nim, w zależności od platformy, poczynając od 5 tysięcy dolarów za Adobe Reader aż do 250 tysięcy dolarów za Apple iOS. Dostępność eksploitów zero-day dla kupujących sprawia, że zaawansowane cyberataki znajdują w zasięgu każdej organizacji niezależnie od jej umiejętności technicznych.

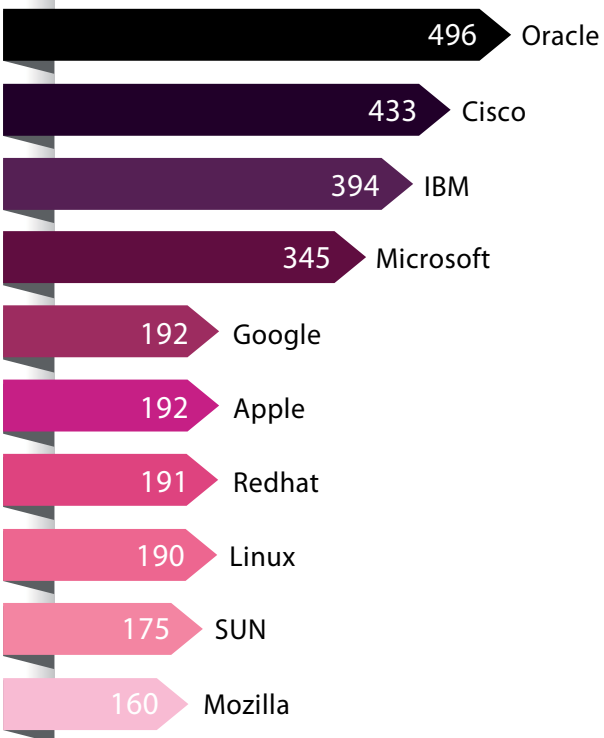
ATAKOWANA PLATFORMA	CENA
Adobe Reader	$5,000-$30,000
Mac OS X	$20,000-$50,000
Android	$30,000-$60,000
Wtyczki Flash lub Java	$40,000-$100,000
Microsoft Word	$50,000-$100,000
Microsoft Windows	$60,000-$120,000
Przeglądarki Firefox lub Safari	$60,000-$150,000
Przeglądarki Chrome lub Internet Explorer	$80,000-$200,000
Apple iOS	Apple iOS

CO 10 MINUT HOST ŚCIĄGA ZŁOŚLIWE OPROGRAMOWANIE

Nawet w miarę, jak nowe podatności znikają z mapy i wpadają być może w ręce twórców złośliwego oprogramowania, dystrybucja zgłoszonych podatności podkreśla kolejne wyzwanie, przed jakim stoją administratorzy bezpieczeństwa i technologii informacyjnych (rycina 3-3). Oracle pozostawał platformą, w której zgłoszono najwięcej podatności, z których część znaleziono w produktach Java, używanych powszechnie w aplikacjach klienckich i serwerowych, stanowiąc tym samym łatwy cel dla napastników. Microsoft z kolei spadł na czwartą pozycję, a więcej podatności zgłoszono w przypadku produktów Cisco i IBM, w tym wielkich serwerów i komponentów infrastruktur sieci, które nie zawsze są objęte polityką ochrony i monitorowania IPS.

Większość organizacji ma dobrze określone procesy terminowego wdrażania łat Microsoftu. Nie odnosi się to jednak do takich aplikacji klienckich, jak Java czy Acrobat Reader, i ta podatność sprawia, że są one wystawione na ataki za pomocą przeglądarki internetowej poprzez spear phishing (kierowane e-maile phishingowe) i strategię tzw. „watering hole", w której napastnik narusza zabezpieczenia popularnej strony internetowej i umieszcza na niej złośliwe oprogramowanie, które może zainfekować każdego narażonego klienta, który obejrzy tę konkretną stronę.

Główne podatności i ekspozycje w 2013 r. z podziałem na producentów
(liczba podatności)



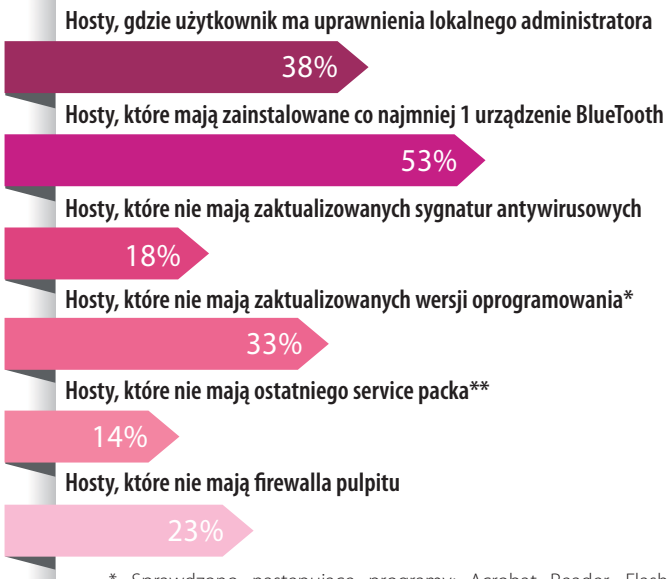
Rycina 3-3

Źródło: baza danych Common Vulnerabilities and Exposures (CVE)

Punkty końcowe: niezałatane, nieograniczone i niegotowe

Statystyki Endpoint Security z naszego badania dotyczącego 2013 r. potwierdzają, że nadążenie za tymi łatami stanowi jedno z największych wyzwań, szczególnie dla systemów klienckich (rycina 3-4). Pomimo powszechnej akceptacji regularnego procesu instalowania łat Microsoftu, 14% przeanalizowanych punktów końcowych nie miało ostatniego dodatku service pack dla Microsoft Windows, który obejmuje wszystkie poprzednie łatki i aktualizacje. Co istotniejsze, 33% punktów końcowych w przedsiębiorstwach nie posiadało aktualnej wersji oprogramowania klienckiego, jak Adobe Reader, Adobe Flash player, Java i Internet Explorer, czego skutkiem były podatności sprawiające, że ci klienci byli narażeni na wiele ataków.

Podatności i błędne konfiguracje punktu końcowego w przedsiębiorstwach
(% hostów)



* Sprawdzono następujące programy: Acrobat Reader, Flash Player, Java, Internet Explorer
** Sprawdzono następujące platformy systemu Microsoft Windows: Windows XP, Windows 2003, Vista, 2008, 2008 R2, Windows 7

Rycina 3-4

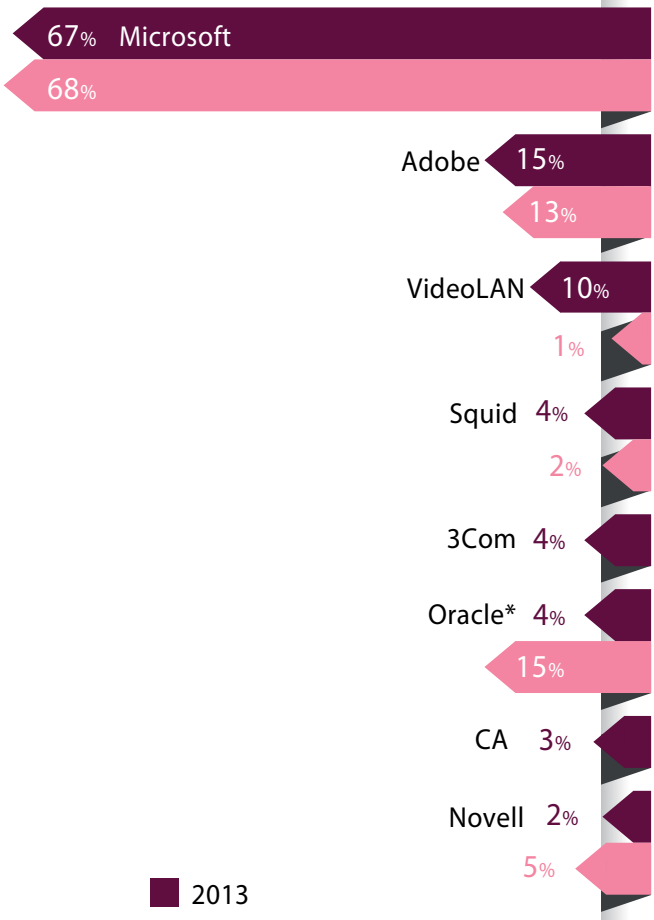
Źródło: Check Point Software Technologies

Podatność tych systemów jest tym większa ze względu na fakt, że niemal jedna piąta (18%) hostów nie miała aktualnych sygnatur dla swoich rozwiązań antywirusowych. Konsekwencje tego przeoczenia mogą być poważne: napastnik, któremu uda się znaleźć punkt zaczepienia w bezbronnym kliencie, może zdobyć w ten sposób solidną płaszczyznę do dalszego eksplorowania sieci atakowanej organizacji. Spośród punktów końcowych firm, które przeanalizowaliśmy, pełne 38% nadało użytkownikom lokalne uprawnienia administratora, przez co uruchomiony złośliwy program mógł działać w kontekście systemu (root), zamiast ograniczać się do użytkownika.

A zatem środowisko w 2013 r. wcale nie sprzyjało oblężonym administratorom bezpieczeństwa i technologii informacyjnej, lecz wręcz było korzystne dla napastników:

- Więcej luk oferowanych na czarnym rynku, gdzie pozostają nieraportowane i niełatane;
- Coraz więcej niechronionych klientów;
- Wzrost liczby podatności w aplikacjach i platformach, dla których łaty dostarczane są z mniejszą regularnością.

Zdarzenia bezpieczeństwa u głównych dostawców oprogramowania
(% organizacji)



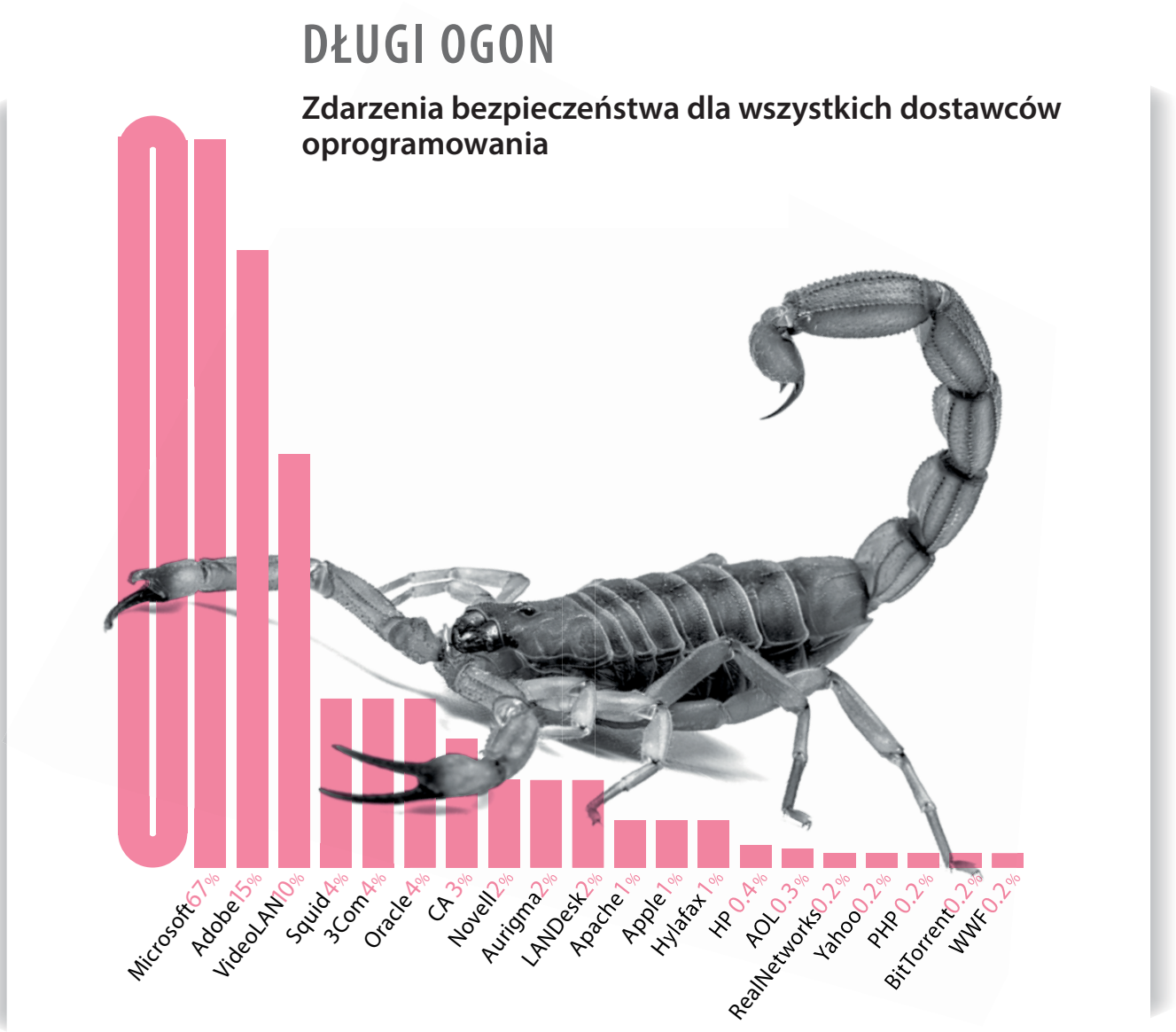
Rycina 3-5

* Java+Oracle+Sunsolaris

Źródło: Check Point Software Technologies

Napastnicy patrzą poza Windows

Dane dotyczące ataków z naszych badań poświęconych 2013 r. pokazują, że napastnicy przystosowują się do tej koniunktury ataków w sieciach przedsiębiorstw (rycina 3-5). Podczas gdy Microsoft nadal był najczęściej atakowaną platformą w 2013 r. i atakowano go co najmniej raz w 67% organizacji, jakie zostały przeanalizowane, stanowi to pewien spadek w stosunku do 2012 r. Zwiększenie się liczby ataków na Adobe (Reader i Flash Player) i VideoLAN (VLC media player) odzwierciedla wzrost ataków na końcowych użytkowników aplikacji, podczas gdy poświęcanie większej uwagi urządzeniom i platformom infrastruktury jasno wynika z większej częstotliwości ataków na systemy ze Squid (proxy i pamięć podręczna), 3com (przełączniki i routery) i CA (analityka i tożsamość). W rzeczy samej, dystrybucja ataków między platformami odzwierciedla „długi ogon" opisywany przez autora Chrisa Andersona[29] w 2006 r. (rycina 3-6). Trop atakowanych platform stanowi linię od „rynków niszowych do nieskończoności" i świadczy o motywowanym gospodarczo i napędzanym przez rynek modelu biznesowym współczesnych cyberataków.



Rycina 3-6

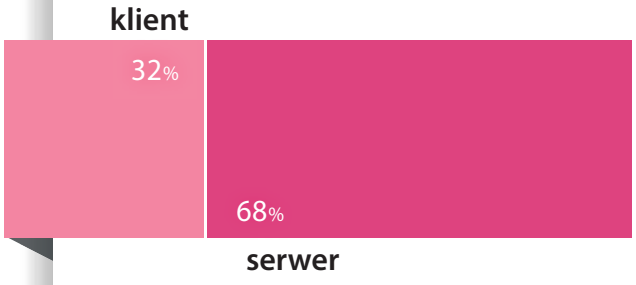
Źródło: Check Point Software Technologies

33%
HOSTÓW NIE POSIADA AKTUALNYCH WERSJI OPROGRAMOWANIA

Pieniądze leżą na serwerach

Badania Check Point z 2013 r. wykazały, że serwery stanowią najczęstszy cel ataków wykrytych przez sieciowe systemy wykrywania nieautoryzowanego dostępu (IPS) i prześcigają inne cele o niemal 100% (rycina 3-7). Biorąc pod uwagę kiepski stan opisanych powyżej systemów klienckich, można się zastanawiać: po co atakować serwery, skoro to właśnie one najpewniej zostaną załatane i będą też najciężej bronione? Dokładnie z tego samego powodu, dla którego Willie Sutton obrabowywał banki. Jak rzekomo to ujął: „Ponieważ tam właśnie są pieniądze"[30]. Serwery aplikacji mają dostęp do sieci, a czasem nawet bezpośredni dostęp do Internetu w strefie zdemilitaryzowanej, w związku z czym zautomatyzowane ataki są bardzo dobrze przystosowane do serwerów, ponieważ mogą wykorzystać podatności w usługach lub aplikacjach bez interakcji z użytkownikiem końcowym. Można przeskanować porty i usługi serwera z zewnątrz sieci lub ze zinfiltrowanego klienta wewnętrznego, a następnie sam serwer można zaatakować przy pomocy programów dostosowanych do wersji aplikacji lub systemu operacyjnego, które są na nim uruchomione. Wniosek z tego jest jasny: pewne ataki zdalne, jeśli się powiodą, dadzą napastnikowi zdalną kontrolę nad systemem.

Zdarzenia bezpieczeństwa według platform w 2013 r.
% wszystkich



Rycina 3-7

Źródło: Check Point Software Technologies

Główne wektory ataku
(% organizacji)

Rycina 3-8

Źródło: Check Point Software Technologies

Głównym wektorem ataków według w naszych badań z 2013 r. (rycina 3-8) jest zdecydowanie zdalne wykonywanie kodu (ang. remote code execution, RCE)[31], przy czym pierwsze trzy wektory według częstości to: wykonanie kodu, uszkodzenie pamięci i przeciążenie bufora. Nawet ataki DoS (ang. denial of service) mogą wspomóc atak na serwer dzięki temu, że posłużą jako zasłona dymna w celu odwrócenia uwagi od znacznie bardziej dyskretnego ataku na serwer, kiedy ten następuje. W momencie, kiedy dym zniknie, atak jest już zakończony, a serwer, który był celem, został zinfiltrowany.

Klienci: niezałatani, nieograniczeni i niegotowi

Również klient stanowi łatwy cel, szczególnie dla ataków sieciowych, które próbują rozprzestrzenić się na całej wewnętrznej sieci lub niezabezpieczonej sieci publicznej. Poza brakującymi łatami i service packami, które naprawiają znane i stanowiące łatwy cel usługi, jak RPC[32], klienci są często podatni na atak z tego powodu, że pewne istotne funkcje obronne zostały u nich wyłączone. Przykładowo, prawie jedna czwarta (23%) punktów końcowych przedsiębiorstw, które zostały przeanalizowane przez Check Point, nie miało włączonego firewalla pulpitu, a ponad połowa (53%) włączyła Bluetooth, narażając się na ataki bezprzewodowe w przestrzeni publicznej.

Systemy klienckie mogą zostać zinfiltrowane na wiele innych sposobów, głównie przez wykorzystanie zachowania użytkownika na poczcie lub w czasie przeglądania stron internetowych. Na tych polach dane z naszej analizy roku 2013 pokazują zarówno zwiększenie aktywności złośliwego oprogramowania, jak i przejście na masową indywidualizację.

ŻART DNIA: KOŃCOWI UŻYTKOWNICY NADAL SĄ SŁABYM OGNIWEM

Poczta e-mail pozostaje najczęstszym wektorem rozprzestrzeniania malware'u. Przykład z 2013 r. pokazuje, że nawet dziś końcowi użytkownicy są nieświadomi najprostszych ataków, przez co tworzą gotowy mechanizm dystrybucji złośliwego oprogramowania pomiędzy wieloma organizacjami.

W październiku 2013 r. użytkownik pracujący u dużego producenta we Francji otrzymał wiadomość e-mail o temacie „Blagounette du jour", co tłumaczymy jako „Żart dnia"[33]. Dołączony do tej wiadomości był plik Microsoft Excel o wadze 6 MB.

Zautomatyzowana analiza podejrzanych dokumentów przychodzących w ramach wirtualnego środowiska sandbox wykazała, że plik Excel wypakowywał obraz z aplikacji Excela do systemu plików na komputerze i zmieniał klucz tapety w rejestrze na nowy obraz. Ponieważ obraz często uznawano za śmieszny, niczego niepodejrzewający użytkownik z dużym prawdopodobieństwem dzielił się tym „żartem" i przekazywał tę wiadomość przyjaciołom i współpracownikom. Dalsza analiza wykazała, że dokładnie to miało miejsce, jako że dokument został przekazany w ten sposób trzem innym dużym organizacjom we Francji.

Na szczęście dla tych organizacji, ten konkretny dokument nie miał żadnego złośliwego ładunku, a jego celem nie było powodowanie szkód na komputerach użytkowników, którzy go otworzyli. Jednakże ma on wszystkie cechy kierowanej kampanii malware'owej. Użytkownicy, którzy otworzyli ten dokument, narażali swoje komputery i organizacje na znaczne ryzyko. Ryzyko to było tym większe, że przekazywali oni go swoim współpracownikom, a także przyjaciołom pracującym w innych organizacjach, którzy stawali się dodatkowym wektorem w rozprzestrzenianiu się kawału dnia, co tak naprawdę nie jest powodem do śmiechu.

Rycina 3-9

Źródło: Check Point Software Technologies

W 2013 r. zauważyliśmy wzrost przypadków, gdzie host wchodził na złośliwą stronę. Nasze badania pokazują, że średnio co 60 sekund host wchodził na złośliwą stronę. Za wyjątkiem hostów z zakresu 1-2, rycina 3-9 pokazuje, że rozmieszczenie liczby hostów wchodzących na złośliwe strony nie uległo dużym zmianom od 2012 r. Ta pozornie dobra informacja skrywa poważniejszy problem, jako że jest ona efektem kampanii spear-phishingowych, które celują w ograniczoną liczbę użytkowników w ramach organizacji i wpływają na profilowanie mediów społecznościowych w celu stworzenia wiadomości e-mail, która z większym prawdopodobieństwem zostanie otwarta przez odbiorcę. Zamiast zasypywać całą organizację łatwo wykrywalnymi wiadomościami phishingowymi, ataki te celują w jednego lub dwóch użytkowników. Jest to znacznie bardziej efektywna metoda, która w porównaniu do 2012 r. zapewniła 20-procentowy wzrost przypadków, w których host wchodzi na złośliwą stronę.

Ten trend wyjaśnia również znaczący wzrost liczby przypadków hostów ściągających złośliwy program, jaki miał miejsce w 2013 r., jako że w 76% przebadanych organizacji od 1 do 4 hostów ściągało złośliwy program, co daje 69-procentowy wzrost w porównaniu do 2012 r., podczas gdy częstość nie zmieniła się lub wręcz zmniejszyła dla wszystkich pozostałych kategorii użytkowników (rycina 3-10).

Niewielka liczba hostów wchodzących na złośliwe strony i ściągających złośliwe programy w większej liczbie organizacji doprowadziła do ogólnego wzrostu działalności malware'owej w 2013 r. A zatem host wchodzi na złośliwą stronę przeciętnie co minutę, a co 10 minut ściągany jest złośliwy program.

49% ORGANIZACJI MIAŁO **7 LUB WIĘCEJ** HOSTÓW ZAINFEKOWANYCH PRZEZ BOTY

73%

ORGANIZACJI POSIADAŁO CO NAJMNIEJ JEDNEGO WYKRYTEGO BOTA, W PORÓWNANIU DO 63% W 2012 R.

BLOKER CRYPTOLOCKERA

Cryptolocker, odmiana złośliwego oprogramowania znana jako ransomware, po raz pierwszy został zidentyfikowany we wrześniu 2013 r. Jak inne postaci ransomware, Cryptolocker instaluje się na komputerze ofiary i pracuje w tle, szyfrując różne dane użytkownika, czego sam końcowy użytkownik nie jest świadomy.

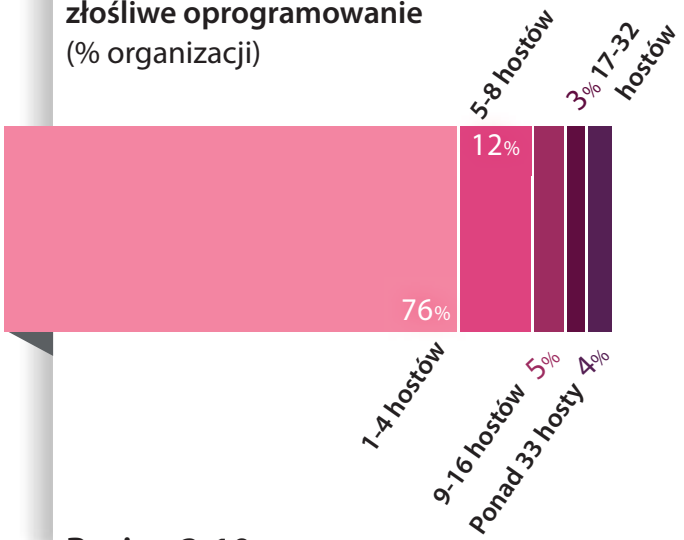
Kiedy okres szyfrowania zakończy się, Cryptolocker wyświetla wiadomość informującą użytkownika, że program „wziął pliki jako zakładników" i wymaga płatności okupu, żeby je odszyfrować. Opis stanowi, że jeśli użytkownik nie spełni żądania w terminie (często krótszym niż 4 dni), prywatny klucz konieczny do odszyfrowania zostanie usunięty z serwera, przez co dane ofiary będą już nie do odzyskania.

W chwili obecnej nie ma żadnej alternatywnej metody odzyskania dostępu do zaszyfrowanych plików.

Istotną własnością Cryptolockera jest to, że agent malware'u musi znaleźć sposób na komunikację i zainicjować ją z serwerem C&C, zanim będzie w stanie rozpocząć proces szyfrowania plików. Najbardziej skuteczną metodą pokonania Cryptolockera jest zatem wykrycie i zablokowanie początkowej próby komunikacji przez agenta, zanim będzie się on w stanie połączyć się z serwerem C&C i zacząć proces szyfrowania.

Cryptolocker pokazał, że wykrywanie botów, często uznawane za środek reakcyjny, może odegrać proaktywną, prewencyjną rolę w zaawansowanym systemie obrony przed złośliwym oprogramowaniem. W czasie eksplozji Cryptolockera pod koniec 2013 r. organizacje, które korzystały z inteligentnych rozwiązań anty-botowych, były w stanie zminimalizować szkody wyrządzone przez infekcje Cryptolockera w sieciach nie tylko dzięki temu, że identyfikowały zainfekowanych klientów, ale również blokowały najważniejszą, początkową komunikację z serwerem C&C.

Liczba hostów, które ściągnęły złośliwe oprogramowanie
(% organizacji)



Rycina 3-10

Źródło: Check Point Software Technologies

HOST WCHODZI NA ZŁOŚLIWĄ STRONĘ PRZECIĘTNIE **CO MINUTĘ**, A **CO 10 MINUT** ŚCIĄGANY JEST ZŁOŚLIWY PROGRAM.

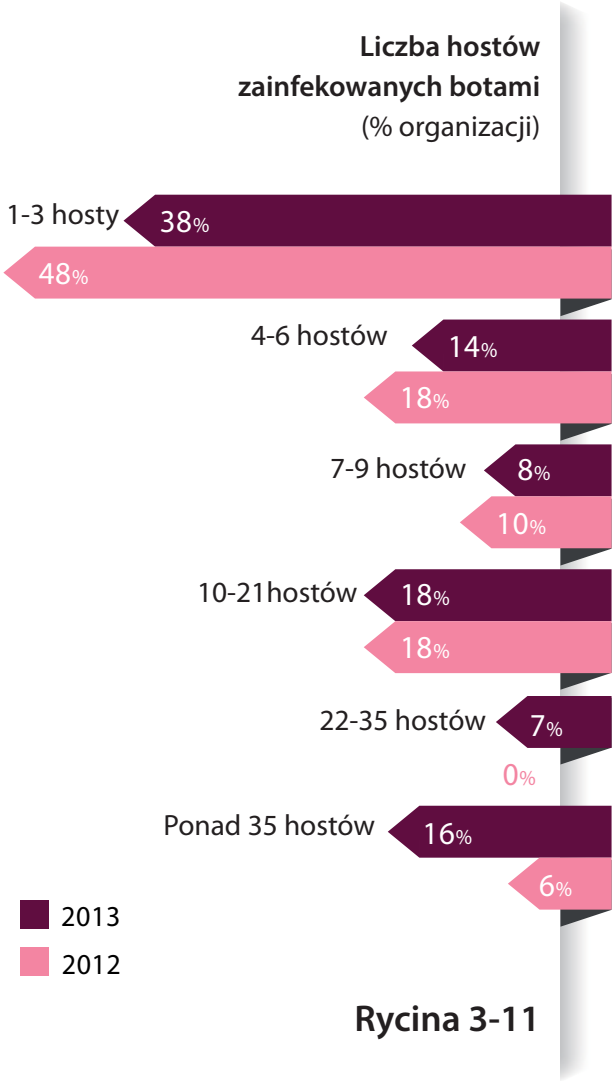
Boty zwiększają zasięg

Jak można by się spodziewać po tym wzroście działalności infiltracyjnej, badanie Check Point wykazało odpowiedni wzrost liczby infekcji botów i działalności botów w 2013 r. Jeśli w przypadku infiltracji zauważyliśmy mniejszą liczbę bardziej kierowanych ataków, do botów można przypisać zjawisko dokładnie odwrotne: wysoka liczba i wysoka częstotliwość. W 2013 r. liczba organizacji, które miały 22 lub więcej zainfekowanych hostów, wzrosła o niemal 400 procent (rycina 3-11), podczas gdy mniejsze infekcje botów w gruncie rzeczy stały się rzadsze.

Nie oznacza to wszakże, że liczba infekcji botów ogólnie zmalała, jako że ponad jedna trzecia (38%) organizacji wciąż miało od 1 do 3 zainfekowanych przez boty hostów.

Co więcej, można by stwierdzić, że stawka ataków botowych coraz bardziej rośnie, a to ze względu na nadejście nowego pokolenia oprogramowania typu ransomware, którego przykładem jest epidemia Cryptolockera pod koniec 2013 r. (dodatek: Bloker Cryptolockera).

Nie tylko organizacje borykają się z bardziej ekstensywnymi plagami botów w swoich środowiskach, ale również same boty stały się bardziej aktywne. Częstotliwość komunikacji botów z serwerami C&C drastycznie wzrosła w 2013 r., przy czym w 47% organizacji wykryto więcej niż jedną próbę komunikacji C&C na godzinę, co daje 88-procentowy wzrost wobec 2012 r. (rycina 3-12). Uśredniając w ramach całej naszej próby, bot próbuje skontaktować się ze swoim serwerem C&C co trzy minuty. Każda z tych prób kontaktu stanowi dla bota sposobność, żeby otrzymać instrukcję i potencjalnie eksfiltrować wrażliwe dane poza atakowaną organizację. To zwiększenie częstotliwości kontaktu stanowi poważne zagrożenie dla organizacji, które walczą o bezpieczeństwo swoich danych i systemów.



Rycina 3-11

Źródło: Check Point Software Technologies

77%

BOTÓW JEST AKTYWNYCH PRZEZ PONAD 4 TYGODNIE

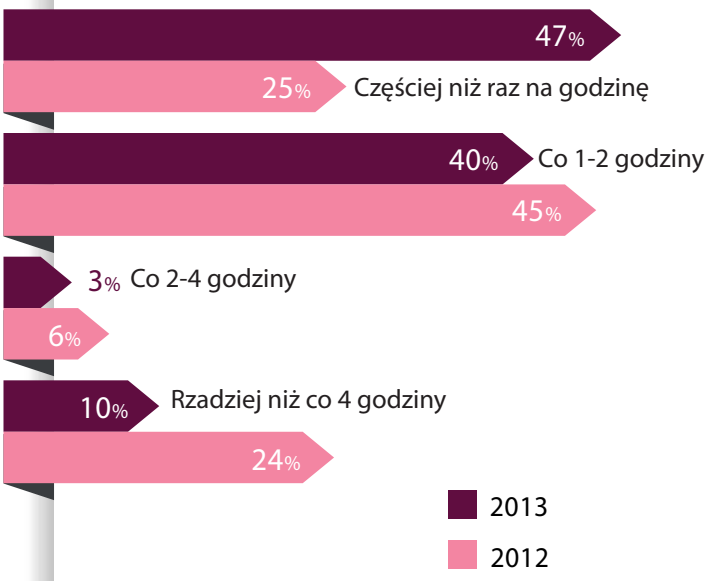
77% ponad 4 tygodnie

poniżej 4 tygodni **23%**

Źródło: Check Point Software Technologies

Rycina 3-13

Częstotliwość kontaktu botów z ich centrum dowodzenia i kontroli
(% organizacji)



Rycina 3-12

Źródło: Check Point Software Technologies

Obrona botów staje się bardziej żywotna i wymagająca

Zwiększona częstotliwość stanowi także szansę dla zarządców bezpieczeństwa do wykrycia, odcięcia i rozpoczęcia likwidacji infekcji botów w sieciach. Wykrycie prób kontaktów botów jest często prostszym zadaniem; usunięcie botów bez ponownej instalacji obrazu systemu stanowi większe wyzwanie. Skuteczne blokowanie kontaktów botów staje się najtrudniejszą częścią wojny z botami ze względu na nowe, bardziej skomplikowane kanały C&C stosowane przez botnety oparte na algorytmie generowania domeny (DGA), żeby uniknąć tradycyjnych narzędzi filtracji i blokowania (dodatek: To nie jest kampania phishingowa jak za dawnych lat)[34].

BOT PRÓBUJE SKONTAKTOWAĆ SIĘ ZE SWOIM SERWEREM C&C **CO TRZY MINUTY**

TO NIE JEST KAMPANIA PHISHINGOWA JAK ZA DAWNYCH LAT

W 2013 r. kampanie phishingowe, jakie przeanalizowano w Check Point Security and Malware Research Group, uwypukliły coraz wyższy stopień skomplikowania technik stosowanych przez dzisiejsze ataki phishingowe. Głównym celem tych technik jest uniknięcie czarnych list, które tworzą rdzeń większości tradycyjnych systemów obronnych. Przykładowo, programy korzystają z pewnej formy dynamicznego schematu URL, który uniemożliwia wykrycie przez statyczne czarne listy. Za to w przypadku kampanii phishingowych opartych na Nuclear exploit kit, techniki te stawiają opór analizom dokonywanym przez badaczy malware'u.

Analiza Cryptolockera przez naszych badaczy ujawniła jeszcze inny aspekt tego trendu: jako botnet oparty na algorytmie generowania domeny (DGA)[35] Cryptolocker stosuje dynamiczne, na pierwszy rzut oka zupełnie losowe nazwy domen w celu zainicjowania komunikacji między botem i serwerem C&C. Boty Cryptolockera generują tysiąc nowych domen każdego dnia, podczas gdy na drugim końcu administratorzy Cryptolockera rejestrują te same 1000 domen, a następnie odrzucają je po 24 godzinach. Na skutek tego technologie, które tworzą i utrzymują czarne listy znanych złośliwych URLów i domen, mają niewielką tylko szansę wykrycia i zarejestrowania złośliwych domen.

Postrzegane jako całość, te ostatnie kampanie malware'owe uwydatniają dużą rolę dynamicznych URLów i nazw domen, jakie stosowane są w tych atakach, w szczególności w unikaniu statycznych czarnych list, które tradycyjnie wykorzystuje się w celu wykrycia i blokowania phishingu i botów. Dynamiczne URL i DGA zmuszają infrastrukturę samego Internetu do generowania niejasnych wariantów lub wariantów jednorazowego użytku, które zaskakują systemy obronne opierające się na poszukiwaniu i blokowaniu transmisji przychodzącej i wychodzącej z adresów, które zostały wcześniej wykryte w sieci globalnej i zaklasyfikowane jako złośliwe.

Te obserwacje odzwierciedlają zdecydowanie szerszy trend w przemyśle malware'owym. Napastnicy wykorzystują słabe punkty systemu nazw domen i tradycyjnych metod wprowadzania URL na czarne listy, żeby unikać istniejących zabezpieczeń i osiągać swoje cele. Anti-Phishing Working Group (APWG)[36] w swoich badaniach za drugi kwartał 2013 r. wykazała, że podczas gdy domena najwyższego poziomu (ang. top-level domain, TLD)[37].com była najczęściej wykorzystywana w kampaniach phishingowych (44% całkowitego phishingu, wzrost z 42% w pierwszym kwartale), domeny najwyższego poziomu niektórych państw są częściej wykorzystywane w atakach phishingowych, niż rejestrowane; przykładowo, Brazylia (.br) ma tylko jeden procent zarejestrowanych domen, ale odpowiada za 4 procent phishingowych domen najwyższego poziomu dla e-maili. Phisherzy i twórcy złośliwego oprogramowania wykorzystują ogromną liczbę możliwych domen najwyższego poziomu dla samych państw, żeby wygenerować niezliczoną liczbę unikalnych nazw domen i URLów, a środki kontroli, które w powszechnym mniemaniu mają zapobiegać tym nadużyciom, nie spełniają swojej funkcji. Analiza „Global Phishing Survey 1H2013: Trends and Domain Name Use"[38] przeprowadzona przez APWG bardziej szczegółowo opisuje rolę nazw domen w atakach phishingowych i dowodzi, że rejestratorzy domen albo śpią, albo aktywnie wspierają phisherów.

Sytuacja ta będzie się tylko pogarszać. W 2013 r. Internet Corporation for Assigned Names and Numbers (ICANN)[39] ogłosił plany zwiększenia liczby domen najwyższego poziomu z obecnych 22 do 1400, wliczając w to domeny najwyższego poziomu mające znaki z nie-łacińskich alfabetów, jak np. arabski, chiński czy cyrylica. Podczas gdy APWG zauważa, że domeny najwyższego poziomu mające znaki z nie-łacińskich alfabetów są już od dawna dostępne i nie cieszyły się dużym zainteresowaniem phisherów, mamy poważne powody sądzić, że napastnicy będą poszukiwać sposobów ich wykorzystania w miarę, jak dostawcy bezpieczeństwa będą coraz skuteczniejsi w zatrzymywaniu URLów i domen phishingowych używających znaków opartych na alfabecie łacińskim. Będzie to stanowić sprawdzian dla wszystkich czarnych list i metod filtrowania URL, które opierają się na listach – niezależnie czy lokalnych, czy opartych na chmurze – znanych złośliwych i podejrzanych URLów i stworzy niemal nieskończoną pulę jednorazowych URLów, które można zastosować w e-mailach phishingowych, i nazw domen, które można wykorzystać na potrzeby botnetów opartych na algorytmie generowania domeny.

Zalecenia

Analiza krajobrazu bezpieczeństwa w 2013 r. dokonana przez Check Point pokazuje, że działalność malware'owa zwiększyła się we wszystkich kategoriach. Ten wzrost miał trzy główne aspekty:

- Większa aktywność infiltracji, w której użytkownicy zostają wystawieni na złośliwe oprogramowanie za pośrednictwem złośliwych stron, wiadomości e-mail lub pobrań;
- Zwiększone poinfekcyjne zagrożenie w postaci większych infekcji botów, które częściej komunikują się ze swoimi serwerami C&C;
- Więcej ataków na różnorodne platformy, których celem są podatności nie tylko na serwerze i kliencie Windows, ale również w sieci i infrastrukturze serwera oraz rzadziej zarządzanych aplikacjach.

Ogólnie rzecz biorąc, to zwiększenie aktywności cyberataków stanowi gigantyczne wyzwanie dla działalności przedsiębiorstw i liderów bezpieczeństwa, którzy już wcześniej musieli podejmować nie lada wysiłki, żeby sprostać wyzwaniom złośliwego oprogramowania opisanym w „Check Point 2013 Security Report". Jedynym sposobem, w jaki organizacje mogą skutecznie poradzić sobie z tym wzrostem aktywności złośliwego oprogramowania i skutecznie walczyć ze zwiększonym tempem ataków, infekcji i eksfiltracji w swoim środowisku jest zautomatyzowanie wielu poziomów obrony i ich jednoczesne koordynowanie. Konieczne środki to m.in.:

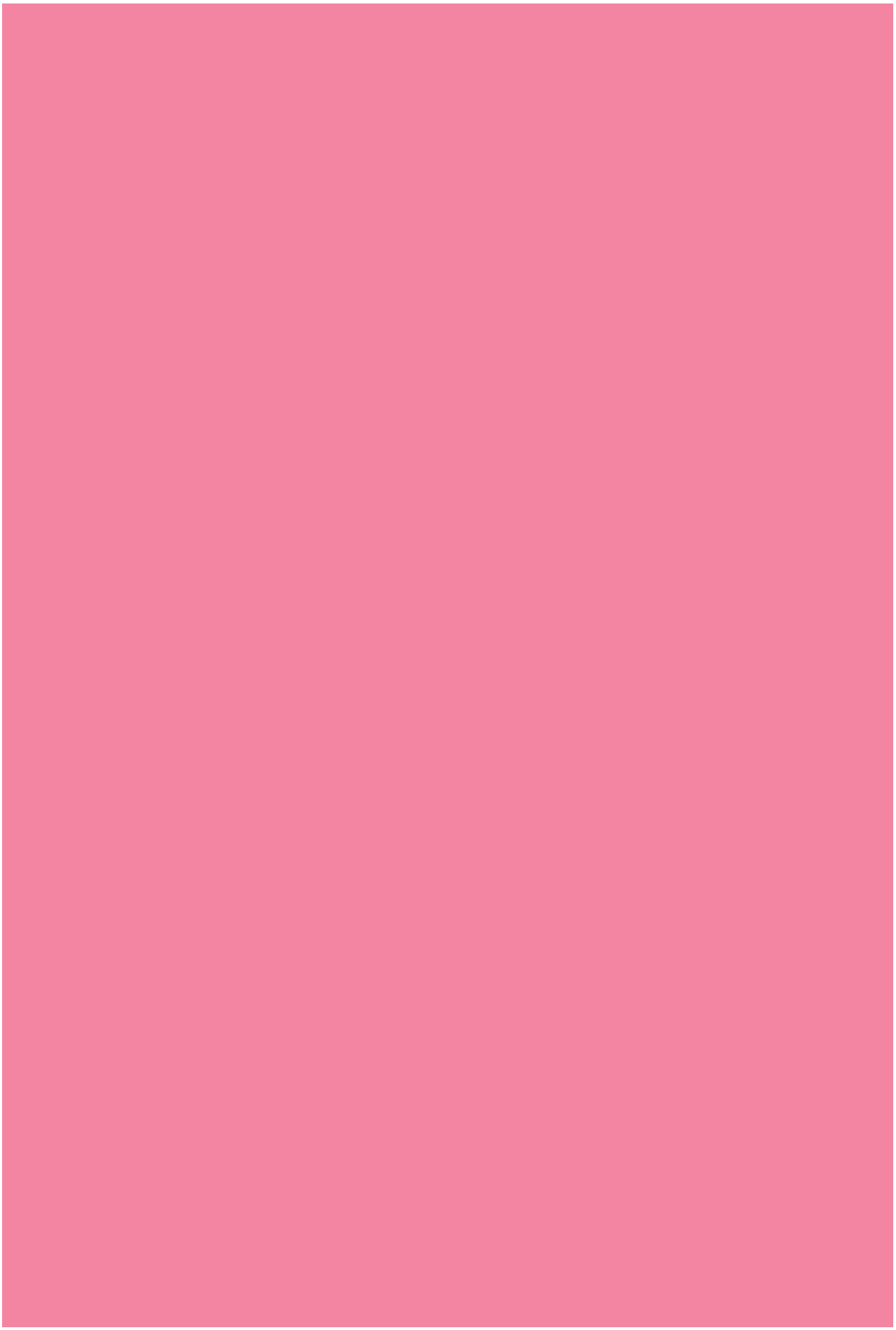
- Antywirusy z filtrowaniem URL na bramach sieciowych i w punktach końcowych – organizacje muszą być w stanie wykrywać i blokować złośliwe oprogramowanie i próby kontaktu ze stronami, które są znanymi dystrybutorami złośliwego oprogramowania;
- Rozwiązania antybotowe na bramach sieciowych – poza funkcją wykrywania złośliwego oprogramowania, rozwiązanie to powinno uniemożliwiać oparty na DGA kontakt z botnetem;
- Zwiększona ochrona IP – poza monitorowaniem, organizacje powinny być w stanie blokować ataki o najwyższym stopniu zagrożenia. System powinien obejmować sieć, serwer i systemy infrastruktury IT od Cisco i innych usługodawców, a także pozostałe platformy, nie tylko Microsoft Windows;
- Kompleksowa obsługa systemu i aplikacji – zapewnienie sytuacji, w której zarządzanie podatnościami i proces dostarczania łat obowiązuje dla wszystkich systemów i aplikacji, w tym Java i Adobe Reader, nie tylko klientów i serwerów Microsoft Windows;
- Najlepsze praktyki konfiguracji klienta i serwera – obejmują one ograniczenie korzystania z uprawnień administratora, wyłączenie Java i innych skryptów, a także ograniczenie aplikacji, które końcowi użytkownicy mogą zainstalować na punktach końcowych.

W kolejnym rozdziale przyjrzymy się wynikom badań za 2013 r. pod kątem aplikacji i zagrożeń, jakie aplikacje te stanowią dla danych przedsiębiorstwa i użytkowników końcowych.

04

APP(ETYT) NA ZNISZCZENIE:

Aplikacje wysokiego ryzyka w firmie



04 APP(ETYT) NA ZNISZCZENIE: APLIKACJE WYSOKIEGO RYZYKA W FIRMIE

Kontrola aplikacji stanowi wewnętrzne wyzwanie, które dopełnia i komplikuje zewnętrzne wyzwania stawiane przez cyberataki. Aplikacje są nieodłączne dla produktywności i codziennej działalności każdej organizacji, ale tworzą one także pewne luki w zabezpieczeniach. Z perspektywy bezpieczeństwa przypominają one mieszkańców „Folwarku zwierzęcego"[41] George'a Orwella: wszystkie aplikacje są równe, ale niektóre są równiejsze.

Aplikacje wysokiego ryzyka są uosobieniem tych wyzwań. W przeciwieństwie do aplikacji „produkcyjnych", jak Microsoft Office czy coraz bardziej akceptowanych aplikacji społecznościowych Web 2.0 jak Facebook, LinkedIn, Twitter, WebEx i YouTube, aplikacje wysokiego ryzyka pozwalają na anonimowe surfowanie w sieci, przechowywanie plików i dzielenie się nimi w chmurze, zdalne użytkowanie aplikacji i danych pulpitowych, a także dzielenie się mediami i innymi plikami między użytkownikami i komputerami. Aplikacje wysokiego ryzyka często funkcjonują na obrzeżach oficjalnie sankcjonowanych technologii informacyjnych i rozwiązań, jeśli nie w całości poza nimi, stanowiąc część coraz bardziej rosnącego cienia informacyjno-technologicznego aplikacji, narzędzi i usług użytkownika, które działają w ramach sieci firm przy minimalnym nadzorze lub wręcz jego braku.

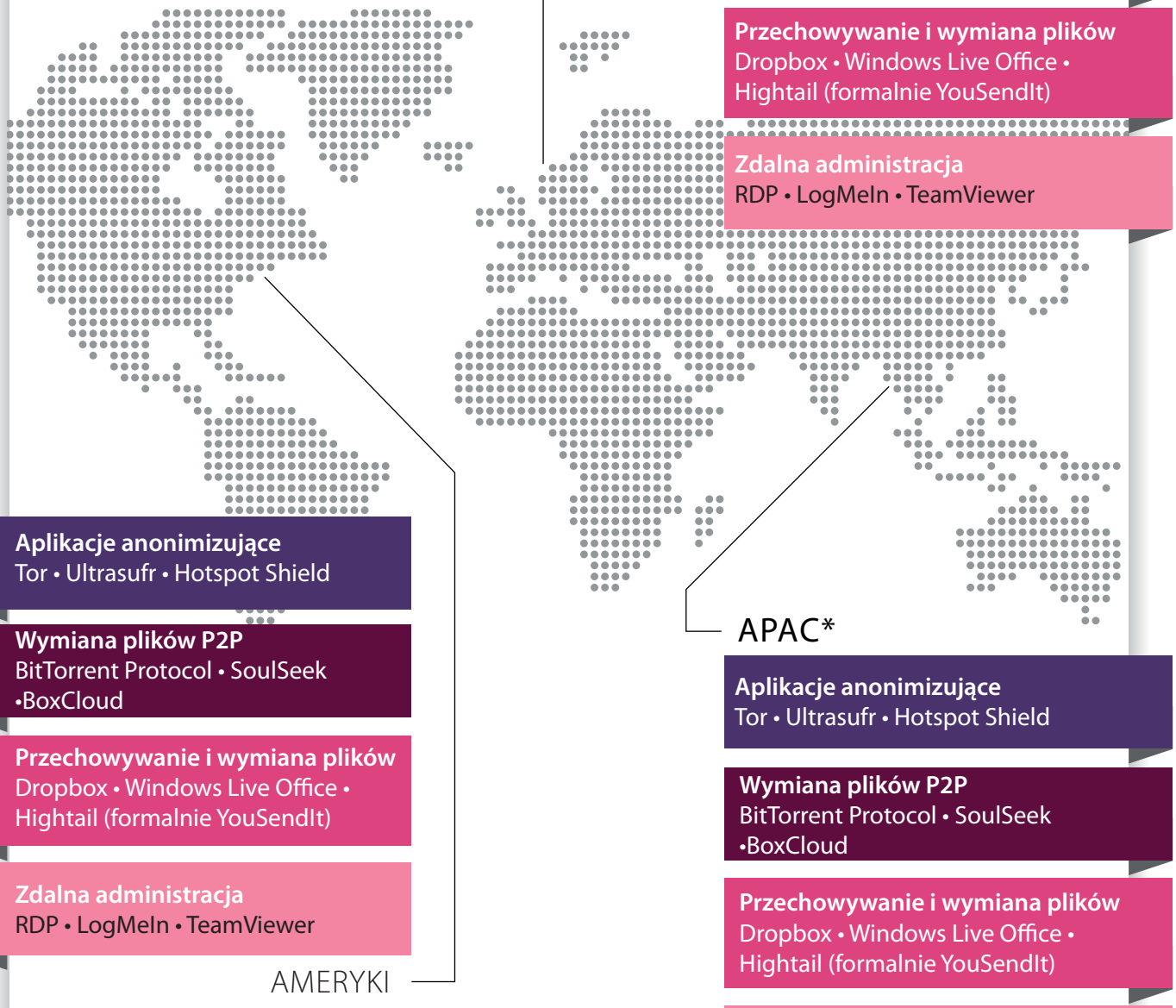
> LECZ KIEDY JESTEŚMY W SIECI,
> CAŁY ŚWIAT JEST LOKALNY.
>
> Neal Stephenson, Cryptonomicon[40]

86%

ORGANIZACJI POSIADA CO NAJMNIEJ JEDNĄ APLIKACJĘ WYSOKIEGO RYZYKA*

*** aplikacje dzielenia się plikami P2P, aplikacje anonimizujace oraz przechowywania plików i dzielenia się nimi**

GŁÓWNE APLIKACJE WYSOKIEGO RYZYKA WEDŁUG REGIONÓW



Rycina 4-1

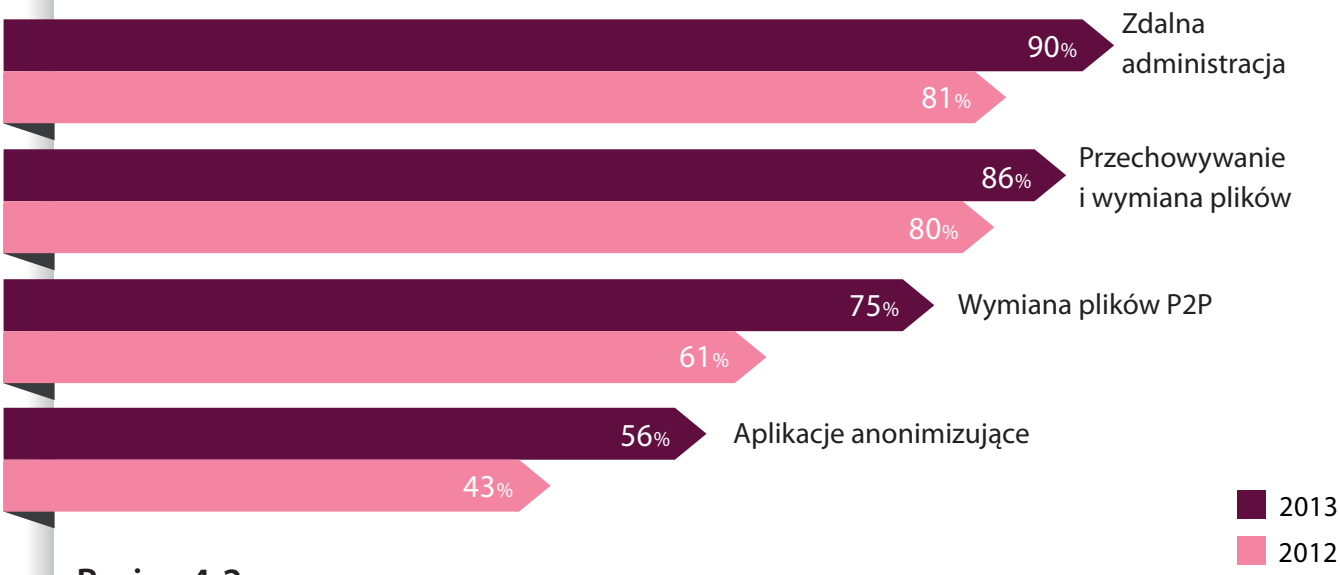
*** APAC – Azja Pacyficzna i Japonia;**

*** EMEA – Europa, Środkowy Wschód i Afryka**

Źródło: Check Point Software Technologies

Procent organizacji korzystających z aplikacji wysokiego ryzyka

(% organizacji)



Rycina 4-2

Źródło: Check Point Software Technologies

W 2012 r. badania bezpieczeństwa przeprowadzone przez Check Point wykazały, że aplikacje wysokiego ryzyka Web 2.0 były wszechobecne w przedsiębiorstwach i przedstawiały znaczące zagrożenie naruszenia zabezpieczeń i wycieku danych. Nasza analiza zabezpieczeń sieci przedsiębiorstw w 2013 r. pokazuje, że pomimo dobrze znanych zagrożeń, częstość występowania aplikacji wysokiego ryzyka wzrosła we wszystkich kategoriach (rycina 4-1). Rozdział ten służy przeanalizowaniu wyników dla każdej z tych kategorii i daje pewne zalecenia mające ułatwić wyzwanie.

BADANIA WYKAZAŁY OGÓLNY **WZROST, JEŚLI CHODZI O KORZYSTANIE Z ANONIMIZATORÓW** W SIECIACH PRZEDSIĘBIORSTWA, PRZY CZYM PONAD POŁOWA (56%) PRZEANALIZOWANYCH ORGANIZACJI MIAŁA CO NAJMNIEJ JEDNEGO ANONIMIZATORA

Niebezpieczeństwo w anonimowości

Aplikacje anonimizujące kojarzy się głównie z tym, że umożliwiają one użytkownikom surfowanie w Internecie i przeglądanie stron bez utraty anonimowości. Zazwyczaj tworzą one zaszyfrowany tunel, żeby założyć serwery proxy HTTP, które pozwalają użytkownikom na obejście firewalli i ograniczeń filtrujących treść. Niektóre z nich, jak Tor, stosują dodatkowe techniki ukrywania routingu, a nawet specjalne wtyczki do oprogramowania lub przeglądarki, żeby pozwolić użytkownikom zatrzeć ślady i zwodzić pracodawcę, państwo lub innych kontrolerów.

W 2013 r. badania Check Point wykazały ogólny wzrost, jeśli chodzi o korzystanie z anonimizatorów w sieciach przedsiębiorstwa, przy czym ponad połowa (56%) przeanalizowanych organizacji miała co najmniej jednego anonimizatora, co stanowi 13-procentowy wzrost w stosunku do roku 2012.

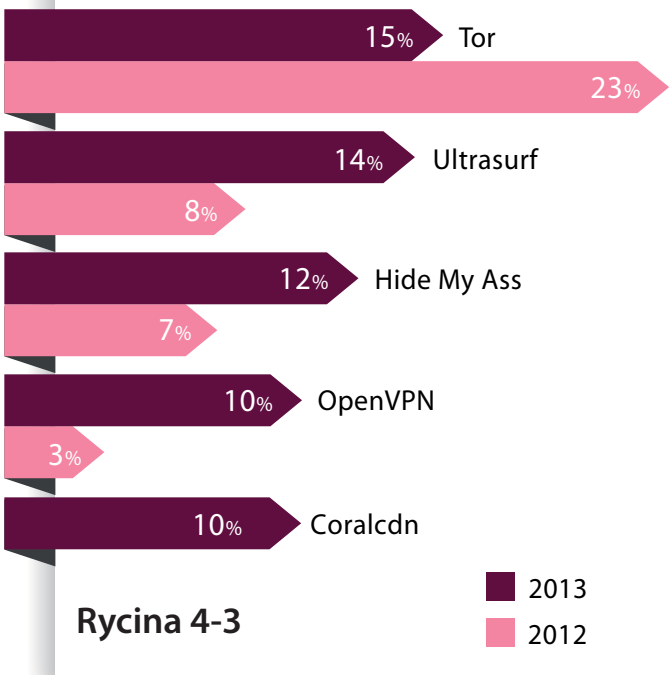
PORTAL DO GŁĘBOKIEJ SIECI

Zwany również Routerem Cebulowym, Tor[42] ponownie był najczęściej wykrytym anonimizatorem według naszego badania za 2013 r. Tor cieszył się już znaczną popularnością z tego powodu, że używany był jako metoda anonimowego przeglądania sieci, która, co więcej, łatwo omija zabezpieczenia w organizacjach, ale w 2013 r. zyskał rozgłos jako portal do głębokiej sieci, mrocznego podbrzusza otwartego i łatwego do przeszukiwania Internetu, tzw. powierzchniowej sieci[43]. Niedostępna dla standardowych narzędzi wyszukiwania, Głęboka Sieć przyciągnęła uwagę w 2013 r. w odpowiedzi na poważne obawy Stanów Zjednoczonych i innych państw w zakresie inwigilacji i prywatności, a także zdobyła złą sławę dzięki aresztowaniom Silk Road[44].

Inne aplikacje anonimizujace stawiają podobne wyzwanie administracyjne, ale rola Tora jako bramki do Onionlandu i innych obszarów głębokiej sieci czyni go szczególnie niebezpiecznym dla zarządców bezpieczeństwa. Podczas gdy zapewnia anonimowość i rynek wymiany dla bezkresnego podziemia, Głęboka Sieć jest także usiana złośliwym oprogramowaniem i oszustami, a organizacje słusznie obawiają się, że pracownicy, którzy korzystają z Tora, żeby uciec od rzeczywistej lub urojonej inwigilacji, w końcu wystawią komputery i całą organizację na duże ryzyko. Ostatnimi czasy śledczy ustalili, że karty kredytowe skradzione licznym detalistom przy pomocy Trojana zdalnego dostępu o nazwie Chewbacca[45] zostały eksfiltrowane do punktów zrzutu serwera za pomocą Tora.

Swoboda wypowiedzi i anonimowość to podstawowe wartości i nie można ich ograniczać w stosunku do zwykłych ludzi. Jednakże dla administratorów bezpieczeństwa w firmach wykrywanie i blokowanie Tora i innych aplikacji anonimizujących w systemach i sieciach firmy musi stanowić ścisły priorytet w 2014 r. i w latach następnych.

Najbardziej popularne aplikacje anonimizujące
(% organizacji)



Rycina 4-3

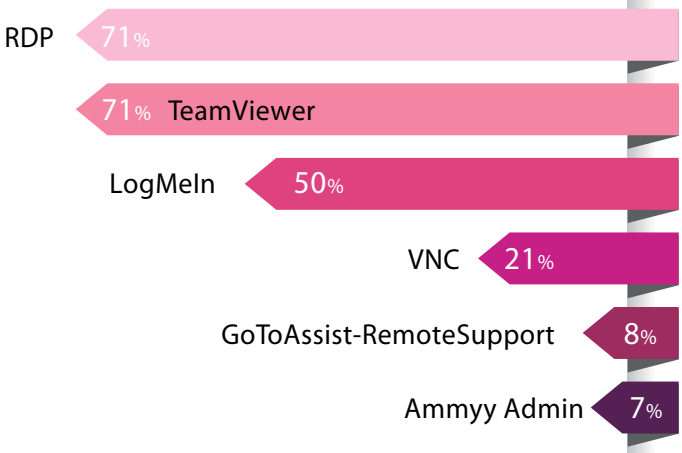
Źródło: Check Point Software Technologies

Poszczególne aplikacje anonimizujące nie doświadczyły jednolitego wzrostu popularności, przy czym Tor został wykryty w mniejszej liczbie organizacji niż w 2012 r.: 15 procent w 2013 r. w porównaniu do 23 procent w 2012 r. (rycina 4-3). Odzwierciedla to fakt, że więcej uwagi – i więcej środków – poświęcono Torowi w firmowej polityce bezpieczeństwa i to z dobrego powodu (dodatek: Portal do głębokiej sieci). Mogło to jednak wynikać również w części z tego, że pracownicy rzadziej anonimowo przeglądali Internet z systemów i sieci firm lub z tego względu, że użytkownicy przeszli na inne aplikacje anonimizujące, które są mniej znane, a co za tym idzie istnieje mniejsze prawdopodobieństwo, że zostaną zablokowane przez zabezpieczenia firmy.

Zachwalane przez zwolenników wolności słowa i prywatności, aplikacje anonimizujące pomogły ochronić tajemnice – nawet życie – dysydentów w krajach doświadczających okresów niepokoju. Ostatnimi czasy, rewelacje o finansowanym przez państwo monitoringu doprowadziły do tego, że wielu użytkowników w Europie i w Azji stosuje takie aplikacje jako azyl przed rzeczywistym i urojonym cyber-wścibstwem. Lokalne różnice, jeśli chodzi o to, jak często wykrywano korzystanie z programów anonimizujących w sieciach firmowych, potwierdzają istotność tego czynnika, a także wskazują na to, że administratorom bezpieczeństwa w Ameryce udało się ograniczyć korzystanie z tej kategorii aplikacji wysokiego ryzyka (rycina 4-4).

Jak w przypadku mitycznej hydry[46], jeśli administratorom udało się powściągnąć Tor w 2013 r., w jego miejsce pojawiło się sześć innych aplikacji anonimizujących. Częstość korzystania z pozostałych głównych aplikacji anonimizujących zwiększyła się w stosunku do 2012 r.

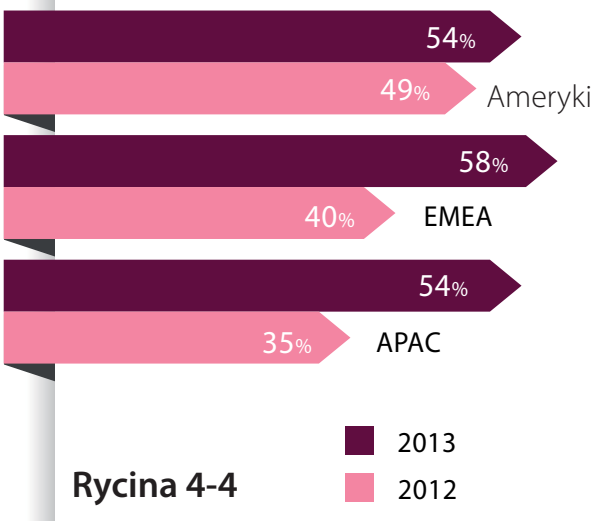
Główne aplikacje zdalnego administrowania
(% organizacji)



Rycina 4-5

Źródło: Check Point Software Technologies

Wykorzystanie aplikacji anonimizujących według regionu
(% organizacji)



Rycina 4-4

Źródło: Check Point Software Technologies

Kto czuje szczura (ang. rat)?

Najczęściej wykrywaną kategorią aplikacji wysokiego ryzyka według naszych badań z 2013 r. były zdalne aplikacje administratora. Najbardziej znaną jest Microsoft Remote Desktop (RDP)[47], ale wiele innych znajduje się w powszechnym użytku na całym świecie, np. TeamViewer znacząco zyskał na popularności w porównaniu do 2012 r. (rycina 4-5). Aplikacje te mają niekiedy uprawnionych użytkowników, kiedy umożliwiają zespołom IT i Helpdesk w firmie obsługiwać i zarządzać pulpitami pracowników na całym świecie (dodatek: Zdalne narzędzia administrowania: Dobry, zły i brzydki).

Jednakże wiele organizacji przyjęło te narzędzia przypadkowo, w oparciu o pewne potrzeby taktyczne, a więc zamiast przyjąć jako standard jedną aplikację zdalnego administrowania, organizacje IT stosują trzy lub nawet więcej w zależności od platformy, połączenia i zadania. W 2013 r. zdalne aplikacje administratora były jedynymi aplikacjami, które najczęściej wykrywano w pionie przemysłowym, przy czym w 90% przedsiębiorstw w tym sektorze wykryto przynajmniej jedną z tych aplikacji.

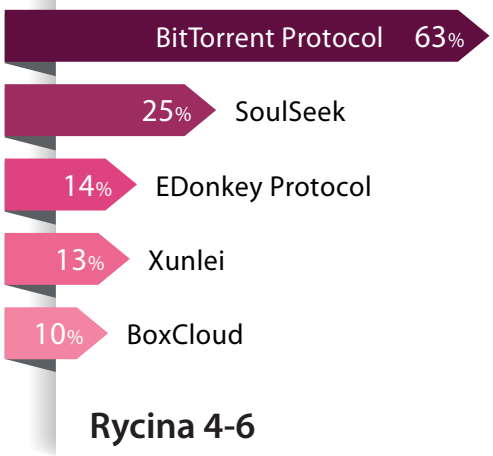
ZDALNE NARZĘDZIA ADMINISTROWANIA: DOBRY, ZŁY I BRZYDKI

Narzędzia zdalnego administrowania (ang. remote administration tools) czasem myli się z narzędziami zdalnego dostępu (ang. remote access tools) ze względu na taki sam akronim: RAT. W praktyce, podczas gdy narzędzia zdalnego administrowania pociągają za sobą istotne zagrożenia bezpieczeństwa i operacyjne, zagrożenia stawiane przez narzędzia zdalnego dostępu takie, jak Chewbacca, Poison Ivy[48], darkComet czy słynny Back Orifice[49], są zupełnie innego rodzaju. W gruncie rzeczy działają one jak programy typu Trojan, nie mają żadnego uzasadnionego zastosowania w sieci organizacji i jako że stanowią poważne zagrożenie, ich wykrycie powinno oznaczać natychmiastowe usunięcie, eliminację i analizę potencjalnej ekspozycji danych.

Z drugiej strony, najbardziej znane narzędzia zdalnego administrowania często pojawiają się w sieciach w odpowiedzi na potrzeby IT i zespołów pomocy technicznej, żeby rozwiązać pewne problemy i zapewnić dostęp do aplikacji i danych na stale rosnącym rynku platform i urządzeń użytkownika końcowego. Teamviewer, jedno z narzędzi zdalnego administrowania, jest dobrym przykładem trendu, jaki panuje wśród tych narzędzi. Obecność Teamviewer w 2013 r. w przebadanych sieciach zdecydowanie się zwiększyła, w czym swój udział miał dostęp do bezpłatnej wersji popularnego LogMeIn i rosnący zakres możliwości, obejmujący kompleksową obsługę platform nieopartych na Windowsie, konferencje i kolaboracje, a także bezproblemowe działanie na wielu różnych połączeniach, bez konieczności wprowadzania zmian do firewalla wymaganych przez RDP.

Ma to swoją cenę, ponieważ cechy, które czynią z niego nowego faworyta dla zespołów IT, sprawiają, że jest on atrakcyjny również dla użytkowników końcowych, którzy chcą mieć zdalny dostęp do swoich komputerów roboczych ze smartfonów, tabletów czy nawet domowych komputerów, tworząc tym samym dziury w sieci firmowej i wystawiając organizacje na ryzyko. W takich sytuacjach nawet pracownik mający dobre intencje może przekształcić dobry RAT w paskudnego szczura (ang. rat).

Główne aplikacje P2P do dzielenia się plikami
(% organizacji)



Rycina 4-6

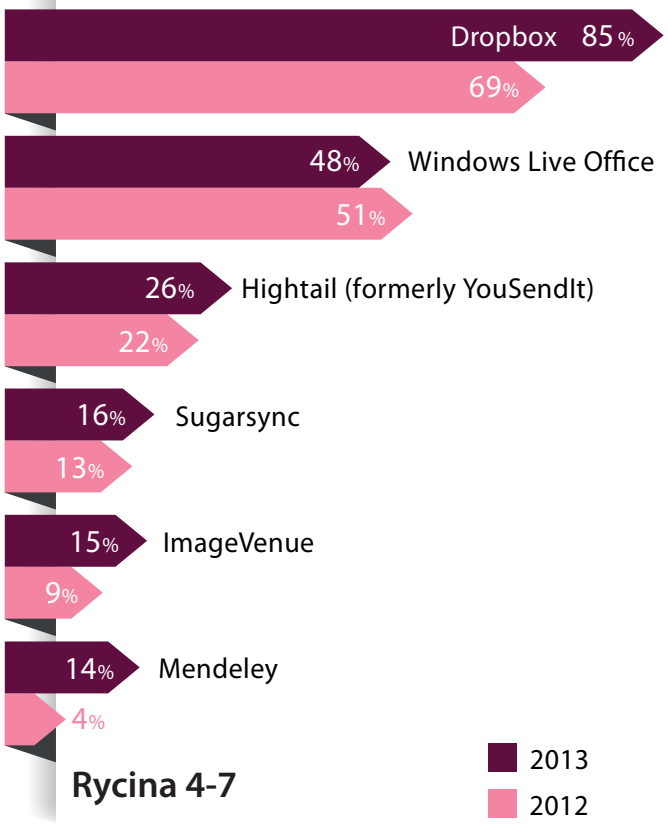
Źródło: Check Point Software Technologies

Peer-to-peer: niebezpieczny w pracy

Aplikacje peer-to-peer (P2P) służą do wymiany plików między użytkownikami. Często używane do dystrybuowania materiałów chronionych prawem autorskim, zarówno legalnego, jak i spiraconego oprogramowania i innych mediów, aplikacje P2P znajdują się w ścisłej czołówce, jeśli chodzi o rozprzestrzenianie malware'ów, które mogą być ukryte w udostępnianych plikach. Poza dystrybuowaniem złośliwego oprogramowania do niespodziewających się i niegotowych użytkowników, aplikacje P2P mogę udostępnić wrażliwe dane na zewnątrz sieci.

Co więcej, częste korzystanie z aplikacji P2P, jak np. BitTorrent, do dystrybuowania chronionej prawem autorskim muzyki czy filmów naraża organizacje na odpowiedzialność ze strony Recording Industry Artists Association (RIAA), która ostatnio bardzo prężnie współpracuje z dostawcami usług internetowych (ISP) w identyfikacji i ściganiu źródeł dystrybucji spiraconych lub nielicencjonowanych treści (rycina 4-6). W 2013 r. BitTorrent stanowił najpopularniejszą aplikację P2P, zaś przypadki jego wykrycia wzrosły z 40%

Główne aplikacje do przechowywania i wymiany plików
(% organizacji)



Rycina 4-7

Źródło: Check Point Software Technologies

w 2012 r. do 63% w 2013 r. Przypadki wykrycia aplikacji P2P konsekwentnie wzrosły we wszystkich regionach.

Przechowywanie plików i oversharing

Możliwość łatwego stworzenia treści i dzielenia się nimi między urządzeniami i użytkownikami jest kluczową cechą aplikacji Web 2.0. Aplikacje do przechowywania plików i dzielenia się nimi w dużym stopniu umożliwiają to dzięki temu, że ułatwiają użytkownikom zapisywanie treści w folderze na jednym urządzeniu, a następnie automatyczne powielanie jej w chmurze i zsynchronizowanie jej pomiędzy wieloma innymi powiązanymi urządzeniami. Rozciągnięcie tej możliwości poprzez dzielenie się z innymi użytkownikami jest często równie proste, co wysłanie łącza do adresata, który może wtedy uzyskać dostęp do udostępnionego pliku, a nawet go modyfikować.

Co oczywiste, ta łatwość dzielenia się wystawia organizacje na poważne ryzyko „oversharingu" – niezależnie, czy umyślnego, czy nie – przez użytkowników, którzy synchronizują wrażliwe dane firmowe z chronionego systemu w pracy do innych, niechronionych urządzeń, a nawet do folderów dzielonych z innymi użytkownikami.

W 2013 r. Dropbox zwiększył swoją przewagę jako najbardziej popularna aplikacja do przechowywania plików i dzielenia się nimi: został wykryty w 85% analizowanych sieci, co stanowi spory wzrost w stosunku do 69% w 2012 r. (rycina 4-7). Jest to zupełnie odwrotna tendencja niż w przypadku pozostałych głównych aplikacji do przechowywania plików i dzielenia się nimi, które straciły na popularności w porównaniu do 2012 r., co częściowo odzwierciedla fakt przejścia firm na jedną, sankcjonowaną przez organizację aplikację, ale również rosnącą popularność Dropboxa wśród końcowych użytkowników, którzy wciągają go w struktury firmowe w ramach infrastruktury „IT ze sfery cienia"[50].

Istoty społeczne

Platformy mediów społecznościowych stanowią integralną cechę Web 2.0 i uzyskały szeroką, aczkolwiek często niechętną, akceptację w środowiskach IT w firmach. W „Check Point 2013 Security Report" opisaliśmy jak to się dzieje, że Facebook wystawia pracowników na ryzyko hakowania i inżynierii społecznej, i zalecaliśmy wzmożone kształcenie użytkowników i zwiększenie obrony w punktach końcowych i w sieci.

DROPBOX ZOSTAŁ WYKRYTY W 85% ORGANIZACJI

DROPBOX SPOLICZKOWANY

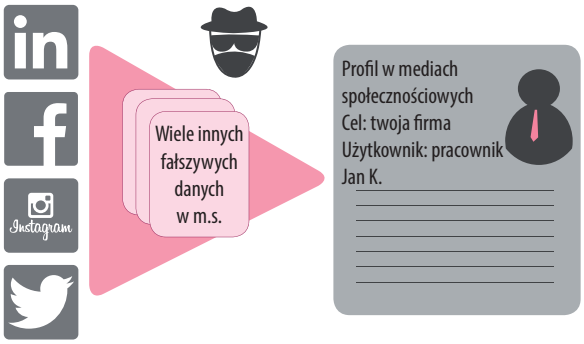
Rok 2013 był znaczący ze względu na to, że napastnicy i badacze uświadomili sobie potencjał aplikacji do przechowywania plików i dzielenia się nimi jako narzędzi do infiltrowania organizacji i eksfiltrowania wrażliwych danych. W marcu odkryto, że hakerzy opracowali mechanizm pozwalający im na wykorzystanie Evernote, żeby umożliwić sieciom botów przeprowadzenie komunikacji C&C i eksfiltrującej.

Niedługo po tym, w kwietniu, pewien badacz opisał mechanizm rozprzestrzeniania złośliwego oprogramowania w organizacji dzięki wykorzystaniu właściwości synchronizujących Dropboxa. Atak ten, zwany DropSmack[51], polega na dodaniu makropoleceń do pliku o rozszerzeniu .doc i prawidłowym nagłówku, a następnie umieszczeniu tego pliku w folderze Dropboxa użytkownika z atakowanej organizacji. Nie ma znaczenia, czy komputer stanowi urządzenie zarządzane przez firmę, czy posiadane przez pracownika; w momencie, kiedy DropSmack zostanie zainstalowany na urządzeniu, tryb automatycznej synchronizacji Dropboxa kopiuje go do folderu Dropboxa na każdym urządzeniu powiązanym z tym kontem. DropSmack pozwala napastnikowi na ominięcie granic, a nawet większości systemów obronnych na poziomie urządzenia na potrzeby infiltracji, C&C, ruchu poprzecznego i eksfiltracji.

Wprowadzenie nowych zabezpieczeń do Dropboxa, jak np. szyfrowania i dwuczynnikowej autoryzacji, miało stanowić odpowiedź na obawy zarządców bezpieczeństwa, ale, jak pokazuje DropSmack, aplikacje te nadal mogą zostać wykorzystane do rozprzestrzeniania malware'u, dlatego należy je uważnie monitorować w środowiskach firmowych, jeśli w ogóle powinny się w nim znajdować.

W 2013 r. zagrożenia te nadal są obecne; co więcej, stały się jeszcze poważniejsze z uwagi na rosnącą rolę mediów społecznościowych jako niezbędnego dla hakerów narzędzia planowania i przeprowadzania kierowanych ataków.

Profil w mediach społecznościowych



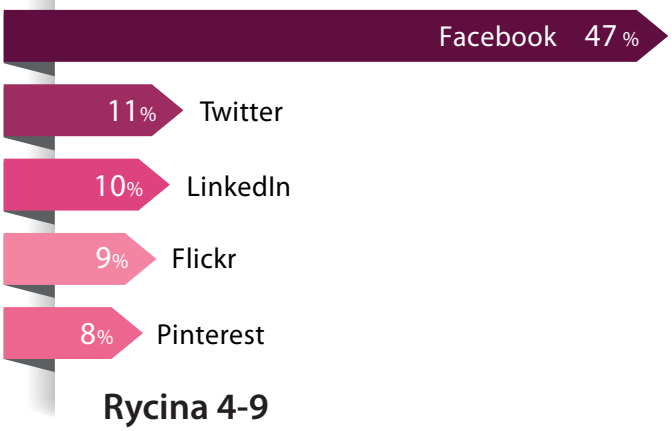
Rycina 4-8

Jak tylko napastnik zaatakuje organizację i zidentyfikuje jednostki w ramach tej organizacji, które mają dostęp do pożądanych przez niego danych, tworzy profil społecznościowy każdego atakowanego pracownika (rycina 4-8). Profil ten daje napastnikowi wartościowe informacje, jak np. często odwiedzane przez pracownika strony internetowe czy sklepy online, jego przyjaciół czy współpracowników, którzy mogą spodziewać się otrzymania od niego wiadomość e-mail, a także ważne wydarzenia, w jakich ostatnio brał udział lub zamierza wziąć udział. Uzbrojony w te dane, napastnik z dużym prawdopodobieństwem powodzenia może stworzyć bardzo wiarygodnie wyglądającą spear-phishingową wiadomość e-mail, która będzie wysłana wziętemu na cel pracownikowi. Wystarczy spojrzeć na wyniki z rozdziału 3, żeby zobaczyć skutki tego profilowania.

(Rycina 4-9) Facebook pozostaje najbardziej popularnym medium społecznościowym, patrząc pod kątem zużycia łącza w środowiskach firm przenalizowanych na potrzeby naszego badania 2013 r.

- Twitter i LinkedIn zajęły odpowiednio drugie i trzecie miejsce, ale doświadczyły ogólnego spadku zasięgu w porównaniu do 2012 r. Ma to z pewnością dużo mniej wspólnego z tym, że pracownicy rzadziej z nich korzystają, niż z tym, że powszechnie korzysta się z nich za pośrednictwem telefonów komórkowych i bezprzewodowych połączeń zamiast z komputerów

Zużycie przepustowości przez transmisję związaną z portalami społecznościowymi (% organizacji)



Rycina 4-9

Źródło: Check Point Software Technologies

w pracy i dostępu poprzez sieć firmową. Podczas gdy ta zmiana mogła spowodować spadek obciążenia sieci firmowych i zmniejszyć bezpośrednie zagrożenie ze strony złośliwego oprogramowania dla firmowych komputerów osobistych, szerokie użycie aplikacji do przechowywania plików i dzielenia się nimi jak Dropbox oznacza, że infekcja z osobistego MacBooka lub tabletu użytkownika może łatwo przedostać się do systemu przedsiębiorstwa (dodatek: Dropbox spoliczkowany).

Zalecenia

Aplikacje wysokiego ryzyka stanowią coraz większe zagrożenie w przedsiębiorstwie, nawet biorąc pod uwagę zmieniające się z czasem narzędzia faworyzowane przez końcowych użytkowników. Podczas gdy niektóre, szczególnie aplikacje anonimizujące czy sieci P2P, nie mają żadnego właściwego zastosowania biznesowego i powinny być całkowicie usunięte, narzędzia zdalnego administrowania czy aplikacje do przechowywania plików i dzielenia się nimi zaspokajają uzasadnione potrzeby użytkowników i IT, przedstawiając bardziej skomplikowane wyzwanie. Nawet powszechnie akceptowane platformy mediów społecznościowych, jak Facebook, LinkedIn czy YouTube, które odgrywają ważną rolę w marketingu mediów społecznościowych i strategiach typu content marketing, mogą stać się atrakcyjnym nosicielem do przeprowadzania ataków spear-phishingowych. Podczas gdy zabezpieczenia przed złośliwym oprogramowaniem mogą opierać się na kompleksowym wykrywaniu, zapobieganiu i likwidowaniu, aplikacje wymagają bardziej zniuansowanego podejścia. Powinno ono obejmować:

Kontrolę aplikacji z podziałem na kategorie – zamiast blokować poszczególne aplikacje jedna po drugiej, administratorzy muszą być w stanie blokować całe rodziny aplikacji, jeśli podejmą taką decyzję. Nie tylko ułatwi to administrowanie, ale również umożliwi zastosowanie kontroli zasad do nowych aplikacji, jeśli zostaną one przyjęte przez pracowników jako zamienniki aplikacji, które zostały zablokowane lub ograniczone.

Standaryzację usankcjonowanych aplikacji – organizacje, które potrzebują narzędzi zdalnego administrowania do wsparcia funkcji IT lub biznesowych, powinny zdecydować się na jedną aplikację, a następnie monitorować sieci pod kątem obecności innych narzędzi zdalnego administrowania. Jeśli blokowanie nie jest możliwe, ich obecność powinna zapoczątkować proces notyfikacji i dochodzenia, żeby ustalić, kto ich używa i w jaki sposób, a także, żeby zweryfikować, czy są to uzasadnione wyjątki od zasad, czy może taktyczne odstępstwa, które należy dostosować do ogólnie panującej polityki. Co więcej, monitorowanie i wdrażanie powinno być ograniczone do konkretnych, autoryzowanych użytkowników lub grup użytkowników, żeby zapewnić, iż tylko pracownicy posiadający istotną potrzebę biznesową są w stanie z nich korzystać. Podobne podejście można zastosować do narzędzi przechowywania plików i dzielenia się nimi; IT powinno wprowadzić bezpieczną, ogólnofirmową usługę lub rozwiązanie, żeby sprostać tej potrzebie. W przeciwnym razie użytkownicy bez wątpienia zwrócą się w stronę „IT ze strefy cienia", żeby umożliwić dzielenie się plikami i synchronizację między urządzeniami, jakie są wymagane w ich pracy.

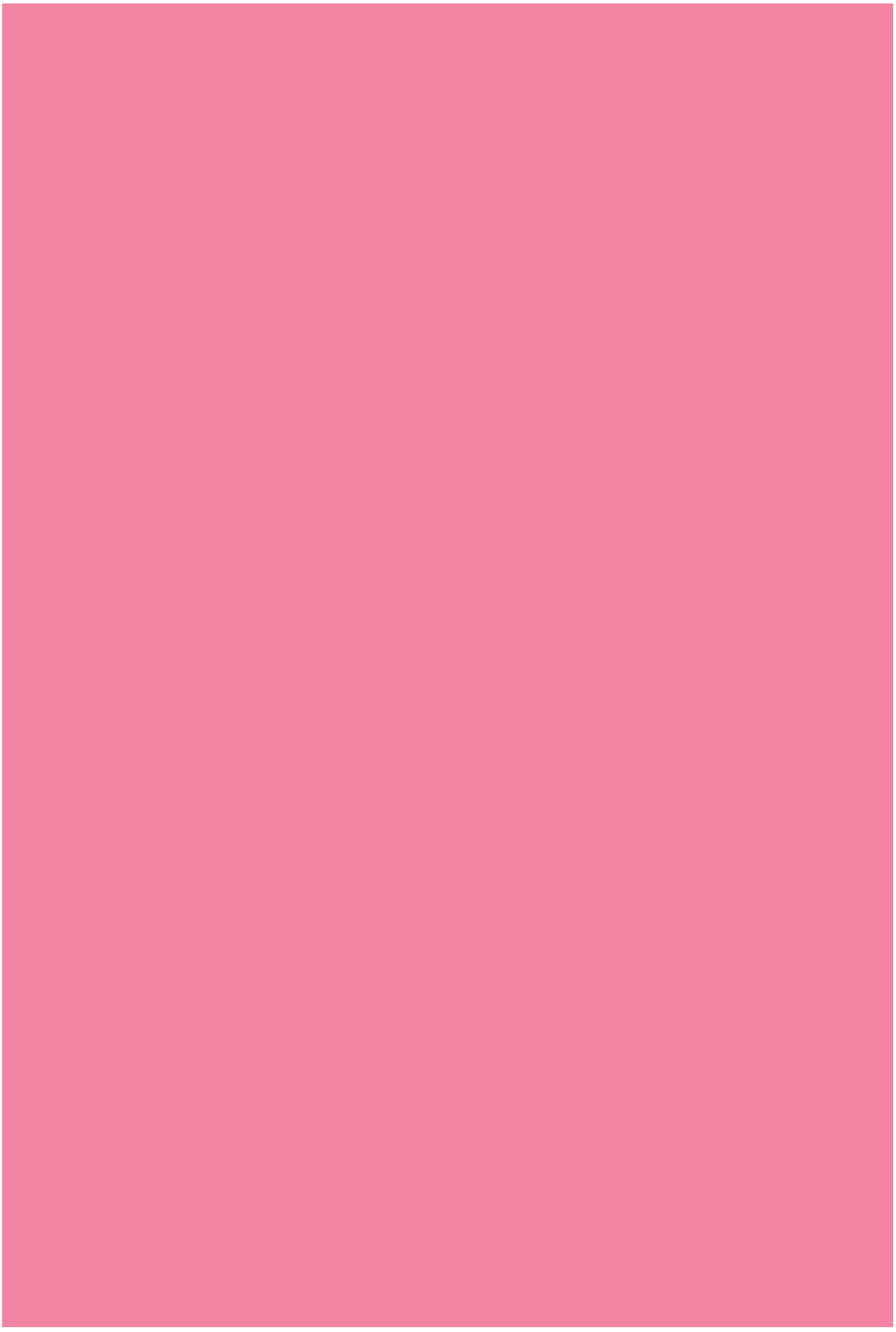
Kształcenie użytkownika końcowego – biorąc pod uwagę niepraktyczność lub niedogodność całkowitego blokowania pewnych kategorii aplikacji, zarządcy IT i bezpieczeństwa powinni opracować kompleksowe i trwałe programy mające informować użytkowników końcowych

o zagrożeniach stawianych przez aplikacje wysokiego ryzyka. Pracownicy muszą zrozumieć konkretne niebezpieczeństwa, jakie przedstawiają rożne typy aplikacji: jak uniknąć spear-phishingu, naruszenia praw autorskich i innych zagrożeń; i jak mogą zaspokoić swoje uzasadnione potrzeby biznesowe i produkcyjne za pomocą bardziej bezpiecznych, sankcjonowanych przez IT narzędzi i praktyk.

Nie zawsze to złośliwe oprogramowanie lub błędnie używana aplikacja odpowiedzialne są za wystawienie waszej organizacji na niebezpieczeństwo. Podczas gdy złośliwe oprogramowanie zdecydowanie odgrywa pewną rolę w wielu wypadkach utraty danych, zbyt często kluczowym czynnikiem jest zwykły błąd ludzki. W kolejnym rozdziale przyjrzymy się najważniejszym wypadkom utraty danych i trendom cechującym to zjawisko w 2013 r.

05

ZAPOEBIEGANIE UTRACIE DANYCH:
Wielki powrót



05 ZAPOBIEGANIE UTRACIE DANYCH: WIELKI POWRÓT

Przypadki utraty danych zyskały na znaczeniu w 2013 r., a Adobe Systems, Target, Neiman Marcus i inne wysoko postawione organizacje doświadczyły poważnych naruszeń danych, które objęły miliony konsumentów.

Dane od długiego czasu stanowią główny cel hakerów, wliczając w to informacje finansowe, własność intelektualną, poufne informacje biznesowe i dane uwierzytelniające. Obecnie zaś istnieje więcej sposobów niż kiedykolwiek, żeby dane te wpadły w niepowołane ręce, np. urządzenia mobilne czy aplikacje IT ze sfery cienia – nowi nosiciele ataków, zwiększający ryzyko utraty danych lub eksfiltracji. Internet przedmiotów tylko pogarsza sprawę, jako że dzięki niemu urządzenia komunikują się ze sobą bezpośrednio i wymieniają informacje o zużyciu energii w domu, położeniu i stanie pojazdu, śledzeniu przesyłek, zdrowiu osobistym i innych. W miarę jak więcej danych przepływa różnymi ścieżkami, coraz trudniej je kontrolować i zabezpieczać. Hakerzy nie są jedynym zagrożeniem dla danych przedsiębiorstwa. Wiele naruszeń ma miejsce nieumyślnie, kiedy użytkownicy przesyłają zły plik do odpowiedniego adresata lub odpowiedni plik do złego adresata – czy nawet zostawiają niezabezpieczony laptop w złym miejscu. Błąd pracownika odgrywał znaczną rolę w wielu incydentach utraty danych w zeszłym roku, lecz niezależnie od tego, czy intencjonalne, czy nie, rezultat może być ten sam: wystawienie wrażliwych danych na niebezpieczeństwo, zdenerwowani konsumenci, utrata reputacji, grzywny za niedopełnienie obowiązków i poważne zakłócenie prowadzenia działalności.

> NUMER UBEZPIECZENIA SPOŁECZNEGO, KONTA BANKOWEGO CZY KARTY KREDYTOWEJ TO NIE TYLKO DANE. W ZŁYCH RĘKACH MOGĄ POZBAWIĆ CZŁOWIEKA JEGO ŻYCIOWYCH OSZCZĘDNOŚCI, POZBAWIĆ KREDYTU I DOPROWADZIĆ DO RUINY FINANSOWEJ.
>
> Melissa Bean[52]

W 2013 R. 88% ORGANIZACJI DOŚWIADCZYŁO CO NAJMNIEJ JEDNEGO INCYDENTU UTRATY DANYCH

MYŚLICIE, ŻE NIE JESTEŚCIE ZAGROŻENI UTRATĄ DANYCH? PRZEMYŚLCIE TO…

Wiele organizacji nadal nie posiada porządnych polityk ochrony danych i kontroli, ponieważ uważają one, że nie są zagrożone naruszeniem danych. Bolesna prawda jest jednak taka, że hakerzy uderzają nie tylko w duże banki i detalistów oraz że każda organizacja posiada wrażliwe dane, które mogą być udostępnione w wyniku źle wysłanego e-maila czy zgubionego laptopa. Poniżej tylko parę przykładów z 2013 r.:

Pracownicy **ukradli dane osobowe**, w tym numery ubezpieczenia społecznego, 3500 pacjentów z Wydziału Zdrowia na Florydzie, żeby wykorzystać je do wypełnienia fałszywych wniosków o zwrot podatku[53].

Rada Islington (Londyn) została ukarana grzywną w wysokości 70 tysięcy funtów brytyjskich po tym, jak zespół wewnętrzny nieopacznie **opublikował** arkusze zawierające **dane osobowe** 2375 mieszkańców, w tym historię zdrowia, na stronie internetowej agencji mieszkaniowej[54].

Rotech Healthcare doniósł o **przypadkowym wycieku danych osobowych i zdrowotnych** dotyczących do 3500 pracowników za sprawą byłej pracownicy działu kadr, której pozwolono zatrzymać jej osobisty komputer, kiedy opuszczała firmę[55].

Brytyjski urząd ds. danych osobowych (ang. Information Commissioner's office) przywołał ponad 60 naruszeń prawa Data Protection Act przez radę miasta Anglesey (Walia) w związku z **niepoprawnym dostępem do danych osobowych mieszkańców**, w tym nieumyślnym opublikowaniem na stronie internetowej i za pośrednictwem wiadomości e-mail[56].

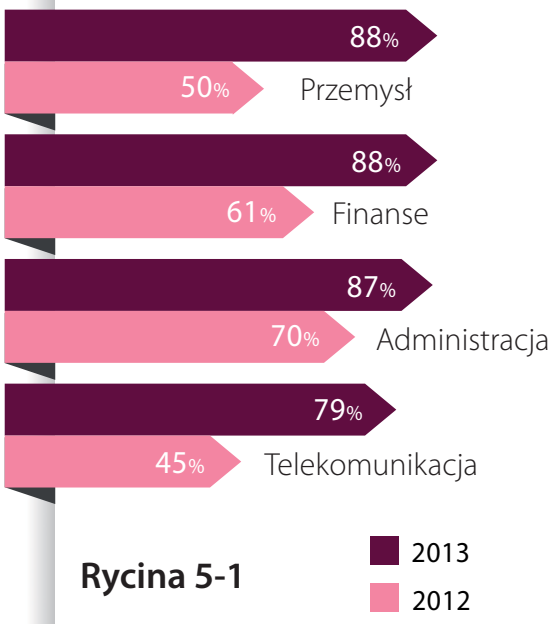
Sektor detaliczny był być możne najważniejszą branżą, której dotknęła utrata danych w 2013 r., ale według badań Check Point organizacje na całym świecie we wszystkich branżach tracą kontrolę nad wrażliwymi danymi; dzieje się to, co więcej, szybciej niż w 2012 r. (rycina 5-1).

Małe organizacje mogłyby uważać, że są zbyt małe, żeby martwić się o utratę danych, ale nic nie może być dalsze od prawdy (dodatek: Myślicie, że nie jesteście zagrożeni utratą danych? Przemyślcie to...). Jeden z największych przypadków naruszenia ochrony danych dotyczył Heartland Payments[57], 700-osobwej firmy, której złodzieje ukradli informacje cyfrowe zakodowane na paskach magnetycznych znajdujących się na tylnej stronie kart kredytowych i debetowych. Każda organizacja w łańcuchu dostawy informacji jest zagrożona atakiem, a nawet względnie niewielka kradzież może okazać się opłacalna dla hakerów.

Badania Check Point wykazały, że 88% przebadanych firm doświadczyło co najmniej jednego potencjalnego przypadku utraty danych, co oznacza, że jakaś wrażliwa informacja została wysłana poza organizację za pośrednictwem poczty e-mail lub przeglądarki internetowej. Stanowi to drastyczny wzrost w porównaniu do 54%, jakie zaobserwowaliśmy w 2012 r. i uwydatnia trwającą walkę organizacji, żeby zabezpieczyć wrażliwe dane przed przypadkowym lub intencjonalnym udostępnieniem.

88 PROCENT PRZEBADANYCH ORGANIZACJI
DOŚWIADCZYŁO CO NAJMNIEJ JEDNEGO
INCYDENTU UTRATY DANYCH W 2013 R.

Procent organizacji z co najmniej jednym przypadkiem potencjalnej utraty danych według branż (% organizacji)



Rycina 5-1

Źródło: Check Point Software Technologies

CO **49 MINUT** WRAŻLIWE DANE BYŁY WYSYŁANE POZA ORGANIZACJĘ. KAŻDEGO DNIA ORGANIZACJA DOŚWIADCZA 29 PRZYPADKÓW POTENCJALNEGO WYCIEKU WRAŻLIWYCH DANYCH.

Innymi słowy, co 49 minut wrażliwe dane były wysyłane poza organizację. Każdego dnia organizacja doświadczała 29 przypadków potencjalnego wycieku wrażliwych danych. Jest to bardzo wysoki wskaźnik utraty danych dla każdej organizacji w każdej branży i podkreśla konieczność bardziej agresywnej kontroli wrażliwych danych.

Według podziału na branże największy przyrost wystąpił w sektorze przemysłowym i konsultingowym, co nie powinno dziwić w kontekście rodzajów danych, jakie były atakowane w 2013 r. (rycina 5-2). Nasze badania pokazują, że kod źródłowy był najpopularniejszym rodzajem danych wysyłanych poza organizację w 2013 r. i odnotował wzrost o niemal 50 procent w stosunku do 2012 r.

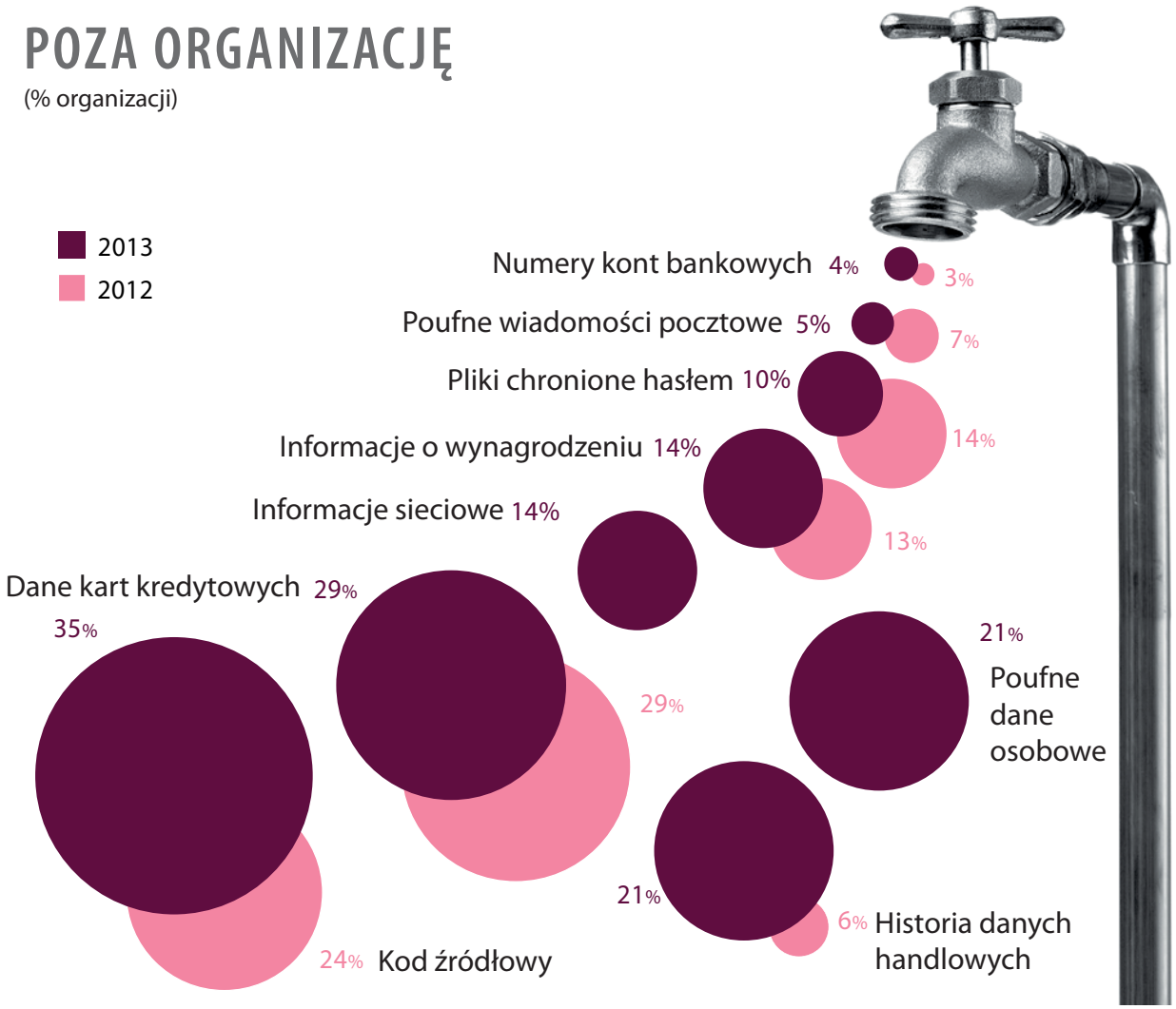
Szacuje się, że kody źródłowe, rejestry danych biznesowych i inne sekrety handlowe stanowią większość aktywów amerykańskich firm, a znajdują się one pod ciągłym atakiem. Ocenia się, że szpiegostwo gospodarcze kosztuje je aż 250-500 miliardów dolarów każdego roku. Podczas gdy banki i służba zdrowia od długiego czasu musiały przestrzegać zewnętrznych regulacji mających chronić dane konsumenta i pacjenta, firmy w takich sektorach, jak wytwórstwo, energia, transport, wydobycie, a nawet rozrywka nie zawsze zajmowały proaktywne stanowisko, jeśli chodzi o ochronę danych. A to właśnie organizacje w tych branżach są coraz częściej celami ataków kampanii wykorzystujących masowo zindywidualizowane złośliwe oprogramowanie, a także bardziej zogniskowane kierowane ataki.

Regulacje również się przystosowują

Pomimo wielu głośnych naruszeń danych kart kredytowych, jakie miały miejsce w 2013 r., badania Check Point wykazały, że liczba incydentów utraty danych kart kredytowych w organizacjach finansowych nieznacznie spadła do 33% z 36% w 2012 r. W przypadku organizacji służby zdrowia i ubezpieczeniowych, jakie zostały poddane analizie, doszło do wzrostu z 16% w 2012 r. do 25% w 2013 r., jeśli chodzi incydenty powiązane z ustawą HIPAA.

DANE WYSYŁANE PRZEZ PRACOWNIKÓW POZA ORGANIZACJĘ

(% organizacji)



Rycina 5-2

Źródło: Check Point Software Technologies

W 33% PRZEBADANYCH INSTYTUCJI FINANSOWYCH INFORMACJE O KARTACH KREDYTOWYCH ZOSTAŁY WYSŁANE POZA ORGANIZACJĘ

W 2013 r. nastąpiła publikacja Payment Card Industry Data Security Standards 3.0, (PCI-DSS 3.0) (pol. Standardów Bezpieczeństwa Danych Branży Kart Płatniczych)[58] zawierających liczne – i na czasie – wymogi dotyczące:

- Praktyk bezpieczeństwa dla systemów użytkowników nie-końcowych, jak punkty sprzedaży (ang. point-of-sale) i inne terminale.
- Zwiększonej edukacji użytkowników o potencjalnych atakach (phishing, USB, itp.) i odpowiedzialnego posługiwania się wrażliwymi danymi.
- Testowania penetrującego systemów kontroli i zabezpieczeń, które określają segmentację między danymi posiadaczy kart i innymi częściami sieci.
- Mechanizmów uwierzytelniających stosowanych przez dostawców usług dla zdalnego dostępu do środowisk konsumentów, którzy podlegają PCI-DSS.

Ogólnie rzecz biorąc, zrewidowane wymogi DSS podkreślają, że „kształcenie, świadomość i bezpieczeństwo to wspólna odpowiedzialność". Standard 3.0 wszedł w życie 1 stycznia 2014 r., a wydarzenia z 2013 r. wytworzyły nowe poczucie pilności, jeśli chodzi o przyjęcie tych nowych wymogów.

Patrząc w przyszłość roku 2014, organizacje będą musiały przyjąć nowe regulacje i wymogi zgodności i ochrony danych, w tym PCI-DSS 3.0 z jego rozszerzonymi wymogami dotyczącymi ochrony systemów POS, a także nowym naciskiem na edukację użytkowników.

W Europie nowa dyrektywa o prywatności danych, Ogólna Regulacja Ochrony Danych (OROD)[59], zacznie obowiązywać również w 2014 r., wprowadzając bardziej surowe wymogi co do ochrony danych obywateli i konsumentów zarówno w państwach, jak i między granicami państw, a także poza UE. Organizacje będą musiały rozwijać swoje strategie i praktyki bezpieczeństwa, żeby dostosować się do nowej regulacji lub będą wystawione na ryzyko poważnych sankcji finansowych.

Zalecenia

Szereg głośnych, szeroko pokazywanych w mediach naruszeń danych w ciągu 2013 r. – dotyczących jednych z najbardziej znanych światowych marek i wielu mniejszych organizacji – pokazuje, że wiele pozostaje do zrobienia w kwestii ochrony informacji osobistych i biznesowych. To wyzwanie będzie coraz poważniejsze w miarę, jak takie trendy, jak mobilność czy Internet przedmiotów na nowe sposoby będą wystawiać dane na kradzież czy przypadkowe udostępnienie. Błąd ludzki odgrywa szczególnie ważną rolę w wielu incydentach utraty danych, a żeby zapewnić, iż dane nie będą narażone lub podatne na kradzież, trzeba będzie przyjąć prawdziwie kompleksowe, holistyczne podejście.

W dzisiejszym świecie coraz powszechniejszych incydentów utraty danych, organizacje muszą podjąć działania mające chronić wrażliwe dane. Najlepszym sposobem przeciwdziałania nieumyślnej utracie danych jest wprowadzenie w firmie zautomatyzowanych metod, które wyłapywałyby takie incydenty, zanim dane opuszczą organizację. Takie metody najlepiej wdrażać dzięki ochronie zapobiegającej utracie danych (ang. Data Loss Prevention, DLP). Zorientowane na treść produkty DLP posiadają szeroki zakres możliwości, zaś ich dodatkową zaletą jest wielość opcji ich rozmieszczenia w ramach organizacji.

Przed wdrożeniem produktu DLP organizacje powinny opracować jasną strategię DLP w oparciu o dobrze określone czynniki jak: Co jest uznawane za informację poufną? Kto może ją wysłać? Gdzie, jak i na jakich urządzeniach można z niej skorzystać? Dzięki wprowadzeniu takiej polityki możecie optymalnie zaimplementować i skonfigurować rozwiązanie, żeby stanowiło oparcie dla unikalnej działalności, jaką prowadzicie, a także dla bezpieczeństwa i wymogów produktywności użytkownika. W celu skutecznego przeciwdziałania przypadkom utraty danych, wasze rozwiązanie powinno obejmować następujące metody i posiadać następujące możliwości:

CZY ZGODNOŚĆ PCI (PAYMENT CARD INDUSTRY) TWORZY FAŁSZYWE POCZUCIE BEZPIECZEŃSTWA?

Duże wycieki danych kredytowych pod koniec 2011 r. sprawiły, że odżyła stara debata o związku między PCI--DSS a bezpieczeństwem, a dokładniej czy firma posiadająca certyfikat zgodności PCI jest faktycznie zabezpieczona przed atakami hakerskimi.

Niektórzy dowodzą, że certyfikat zgodności PCI tworzy fałszywe poczucie bezpieczeństwa u detalistów i wśród społeczeństwa. Naruszenia danych w firmach posiadających rzeczony certyfikat i działania takie, jak retroaktywne cofnięcie certyfikatu bez wątpienia rodzą cynizm, podczas gdy stała ewolucja standardu wywołuje odczucie, że jest to ruchomy cel.

W świetle tych obaw organizacje i praktycy PCI słusznie zwracają uwagę, że przypadki, gdy firmy posiadające certyfikat zgodności PCI, jak np. Target, o których wiadomo było, że stosują bardzo ścisłe procesy bezpieczeństwa, a jednak mimo to doświadczyły naruszenia danych, kierują nas na podstawowy problem, jeśli chodzi o sposób, w jaki praktykuje się zazwyczaj bezpieczeństwo, mianowicie, nie jest to produkt, lecz proces.

Bob Russo, dyrektor PCI Security Standards Council, podkreślił, że certyfikat zgodności PCI jest pewnym „zdjęciem czasu", mówiąc w wywiadzie z Computerworld: „Możesz posiadać zgodność dziś i nie posiadać jej jutro"[60].

Standardy są wartościowymi narzędziami do mierzenia i porównywania stanu bezpieczeństwa względem powszechnych metryk. Niebezpieczeństwo certyfikatu zgodności polega bardziej na tym, że organizacja z samego tytułu przyznania jej tego certyfikatu uzna, że jej bezpieczeństwo jest zapewnione, w związku z czym nie będzie wprowadzać dalszych usprawnień i dostosowywać się do zmieniających się środowisk i praktyk danych.

Klasyfikacja danych – duża precyzyjność w identyfikacji wrażliwych danych jest niezmiernie istotnym elementem rozwiązania DLP. Rozwiązanie DLP musi być w stanie wykrywać dane osobowe, dane związane ze zgodnością (np. HIPAA, SOX, dane PCI data, itd.) i poufne dane biznesowe, w tym zarówno nieszablonowe typy danych, jak i własne zindywidualizowane typy danych. W miarę jak dane przemieszczają się w ramach organizacji i poza nią, rozwiązanie powinno monitorować przepływ treści i egzekwować politykę w najczęściej wykorzystywanych protokołach TCP, w tym SMTP, FTP, HTTP, HTTPS i poczcie elektronicznej, przy wykorzystaniu dopasowywania wzorców i klasyfikacji plików w celu zidentyfikowania typów treści niezależnie od rozszerzenia plików i formatu kompresji. Rozwiązanie DLP musi być w stanie rozpoznać i chronić wrażliwe formy w oparciu o uprzednio określone wzorce i dopasowywanie plików/form.

Eliminacja incydentów przez użytkownika – tradycyjne rozwiązania DLP mogą wykrywać, klasyfikować, a nawet rozpoznawać konkretne dokumenty i różnorodne typy plików, ale nie są w stanie zrozumieć intencji użytkownika, kiedy ten udostępnia wrażliwe dane. Sama technologia nie jest wystarczająca, ponieważ nie może zidentyfikować tej intencji i odpowiednio na nią odpowiedzieć. Z tego powodu najwyższej jakości rozwiązanie DLP musi zaangażować użytkownika, jeśli chce osiągnąć optymalne wyniki. Jednym z możliwych podejść jest umożliwienie użytkownikom wprowadzanie środków zaradczych w czasie rzeczywistym. Innymi słowy, rozwiązanie DLP powinno informować użytkownika, że jego/jej działanie może zaowocować potencjalnym wyciekiem danych, a następnie dać użytkownikowi możliwość podjęcia decyzji, czy odrzucić wiadomość, czy kontynuować jej wysyłanie. Ta metodologia poprawia bezpieczeństwo dzięki temu, że zwiększa świadomość w zakresie polityki przechowywania danych i w czasie rzeczywistym ostrzega użytkowników o potencjalnych błędach, a także zmniejsza wpływ użytkownika dzięki temu, że pozwala na szybką samo-autoryzację uprawnionej komunikacji.

Na skutek tego zarządzanie bezpieczeństwem jest łatwiejsze, ponieważ administrator może śledzić wydarzenia DLP na potrzeby analizy bez konieczności osobistego sprawdzania każdej prośby wysłania danych na zewnątrz, kiedy ta następuje.

Ochrona przed wewnętrznym naruszeniem bezpieczeństwa danych – inną ważną cechą DLP jest możliwość nie tylko powstrzymania wrażliwych danych przed opuszczeniem firmy, ale również monitorowania i kontrolowania wrażliwych wiadomości wysyłanych między wydziałami wewnątrz firmy. Można w związku z tym opracować politykę mającą uniemożliwiać przypadkowe wycieki poufnych danych między wydziałami – przykładowo planów wynagrodzeń, poufnych dokumentów dotyczących pracowników, fuzji i przejęć czy formularzy medycznych.

Ochrona danych na dyskach twardych punktów końcowych – w ramach kompleksowej polityki bezpieczeństwa firmy muszą zabezpieczać dane na laptopach, żeby uniemożliwić osobom z zewnątrz zdobycie wartościowych informacji z zagubionych czy skradzionych komputerów. Możecie uniemożliwić nieuprawnionym użytkownikom uzyskanie dostępu do informacji poprzez zakodowanie danych na dyskach twardych punktów końcowych, w tym danych użytkownika, operacyjnych plików systemowych, a także plików tymczasowych i usuniętych.

Ochrona danych na nośnikach przenośnych – pracownicy często mieszają na urządzeniach USB i innych przenośnych urządzeniach osobiste pliki, jak muzykę, zdjęcia i dokumenty z plikami firmowymi, jak np. plikami finansowymi czy plikami zasobów ludzkich. Sprawia to, że kontrola danych firmowych jest jeszcze bardziej wymagającym przedsięwzięciem. Poprzez zakodowanie przenośnych nośników, uniemożliwiając w ten sposób nieuprawniony dostęp do nich, możecie zminimalizować przypadki naruszenia zabezpieczeń urządzeń zgubionych lub skradzionych.

Ochrona dokumentów – dokumenty biznesowe są stale przesyłane do sieci za pośrednictwem aplikacji przechowywania plików i dzielenia się nimi, wysyłane na osobiste smartfony, kopiowane na przenośne nośniki i udostępniane na zewnątrz partnerom biznesowym. Każde z tych działań wystawia wrażliwe dane na ryzyko utraty i nieodpowiedniego użycia. Żeby zabezpieczyć dokumenty firmowe, rozwiązanie bezpieczeństwa musi być w stanie wdrożyć politykę kodowania dokumentów i przyznawać dostęp wyłącznie uprawnionym jednostkom.

W 25%

PROCENTACH PRZEANALIZOWANYCH ORGANIZACJI SŁUŻBY ZDROWIA I UBEZPIECZENIOWYCH INFORMACJE CHRONIONE NA PODSTAWIE HIPAA ZOSTAŁY WYSŁANE POZA ORGANIZACJĘ

LEKCJA Z ATAKÓW NA PUNKTY SPRZEDAŻY

Podczas gdy włamywanie się na terminale punktów sprzedaży, żeby wykraść dane kart kredytowych, było technicznie możliwe już od dawna, przez wiele lat napastnicy uznawali, że serwery przechowujące te dane są znacznie łatwiejszymi celami. Ulepszenie ochrony na serwerach przechowujących dane kart kredytowych i konsumentów zmusiło jednak napastników do zwrócenia uwagi na źródła tych danych. Rok 2013 stał się punktem przełomowym, jeśli chodzi o włamania na terminale punktów sprzedaży. Podczas gdy zakres i skala tych naruszeń danych detalicznych wielu wydawała się ogromna, dla osób zajmujących się bezpieczeństwem równie interesująca była różnorodność tej kategorii złośliwego oprogramowania.

Złośliwe oprogramowanie służące do atakowania punktów sprzedaży obejmuje programy „zeskrobujące pamięć", jak zwykły Chewbacca czy Dexter[61], skomplikowany blackPOS[62], a także bardziej kierowane oprogramowanie znalezione w Neiman Marcus[63]. Programy te mają jednakże wiele cech wspólnych, które umożliwiają napastnikom przenikać do systemów punktów sprzedaży i wykradać wiele danych kart kredytowych:

- Przestarzałe systemy operacyjne w punktach sprzedaży, które często są nieaktualizowane przez wiele miesięcy nawet wtedy, gdy łata już się ukazała
- Uzyskanie wejścia do systemów punktów sprzedaży za pomocą zainfekowanego klienta lub serwera u atakowanego detalisty
- Umiejętność obejścia kontroli aplikacji i innych blokujących system środków, przykładowo poprzez infekowanie serwera aktualizacji
- Wykorzystanie szyfrowania, zwykłych protokołów i normalnych wzorców ruchu w sieci, żeby ukryć dane, kiedy są one eksfiltrowane
- W wielu sieciach bezpośrednie połączenie do Internetu z urządzenia punktu sprzedaży, często ponieważ w ten właśnie sposób dokonywane są płatności.

Walka z każdym z tych problemów z osobna nie rozwiąże problemu, ponieważ nie rozwiąże leżącej u podstaw przyczyny: słabej lub nieobecnej segmentacji sieci punktów sprzedaży i produkcji. Sieci detaliczne podkreślają potrzebę opracowywania i wprowadzenia najlepszych praktyk segmentacyjnych, które pozwolą organizacjom egzekwować politykę opanowania naruszonego hosta i określić wewnątrzsegmentowe interakcje, które można będzie automatyczne monitorować i egzekwować. Przykładowo, monitorowanie wdrażania kierunku i typów ruchu pod kątem segmentów zawierających urządzenia punktów sprzedaży ograniczyłoby sposobności dla złośliwego oprogramowania do rozprzestrzeniania się i eksfiltrowania danych. Pod tym względem detaliści znajdą się w awangardzie organizacji określających i wprowadzających logiczną segmentację i strategiczne wdrażanie w całych swoich środowiskach IT.

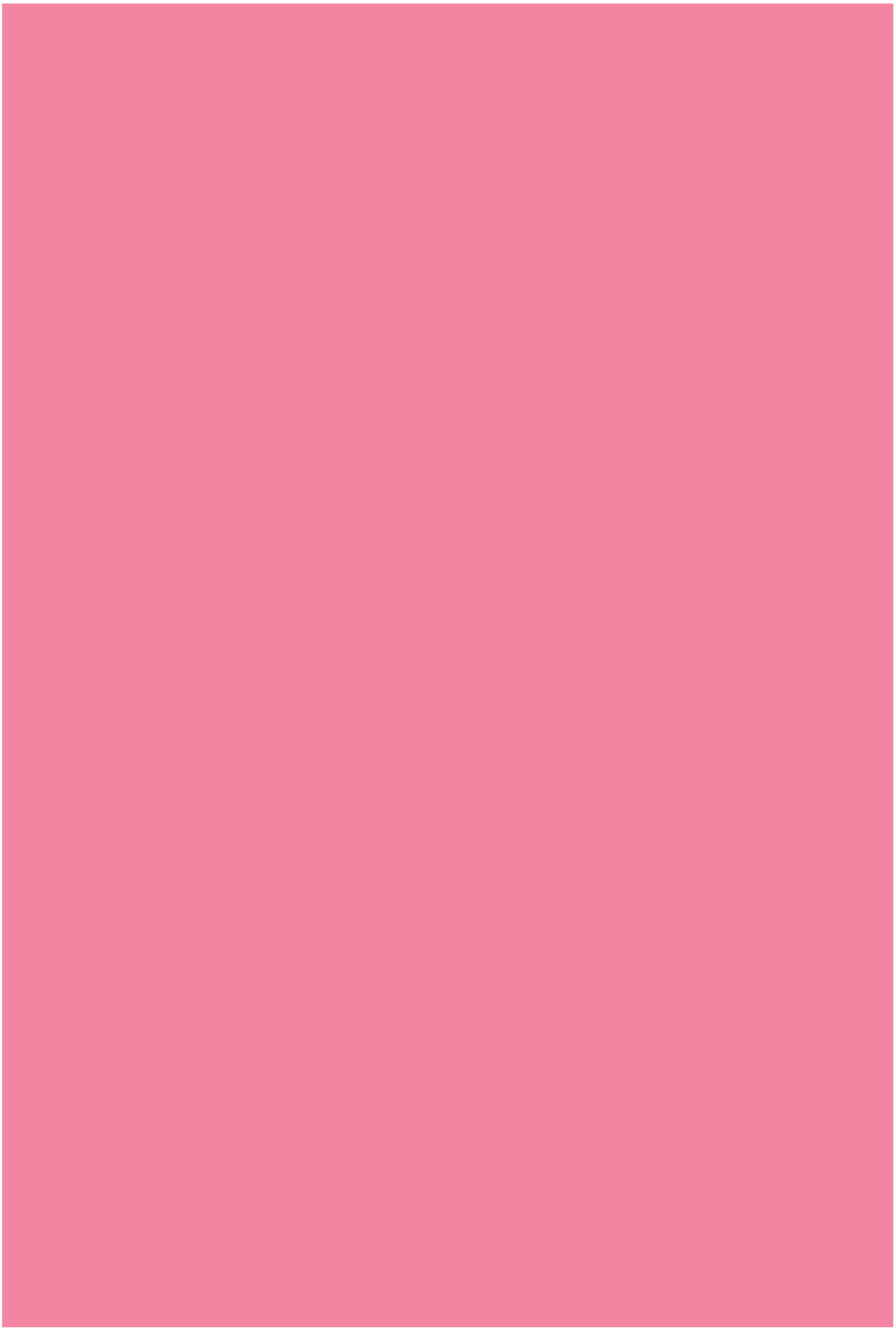
Zarządzanie incydentami – poza określeniem zasad DLP, żeby dostosować je do zasad korzystania z danych w waszej firmie i wprowadzić technologie wspierające i wdrażające, całościowa strategia zabezpieczenia danych przed utratą musi obejmować możliwość skrupulatnego monitorowania i raportowania. Wasze rozwiązanie bezpieczeństwa powinno umożliwić monitorowanie i analizę zarówno obecnych, jak i przeszłych incydentów DLP. Da to administratorowi bezpieczeństwa jasny i szeroki wgląd w informację, jaka wysyłana jest na zewnątrz, a także zapewni organizacji możliwość reagowania w czasie rzeczywistym, jeśli zajdzie taka konieczność.

Kolejny rozdział przedstawia kompleksowy i ogólny plan skutecznej architektury bezpieczeństwa w dniu dzisiejszym.

06

ARCHITEKTURA BEZPIECZEŃSTWA DLA JUTRZEJSZYCH ZAGROŻEŃ

Programowalna ochrona



06 ARCHITEKTURA BEZPIECZEŃSTWA DLA JUTRZEJSZYCH ZAGROŻEŃ PROGRAMOWALNA OCHRONA (SOFTWARE-DEFINED PROTECTION)

ABY PROAKTYWNIE CHRONIĆ ORGANIZACJE, POTRZEBNY JEST NOWEGO PARADYGMAT

„Raport Bezpieczeństwa Check Point 2014" przedstawia wyniki naszej pogłębionej analizy zagrożeń i trendów bezpieczeństwa w 2013 r. Raport ten pomoże decydentom bezpieczeństwa i decydentom biznesowym zrozumieć zakres zagrożeń, jakie czyhają na ich organizacje, i rozważyć nowe działania mające poprawić bezpieczeństwo ich środowiska IT.

Głównymi wnioskami z naszych badań są:

- Nieznane złośliwe oprogramowanie wykorzystywane jest coraz częściej, czego motorem jest trend masowej indywidualizacji złośliwego oprogramowania.
- Zagrożenie złośliwym oprogramowaniem i infekcjami jest zdecydowanie większe, co odzwierciedla rosnące powodzenie kierowanych kampanii złośliwego oprogramowania.
- Każda kategoria aplikacji wysokiego ryzyka zwiększyła swoją obecność w przedsiębiorstwach na całym świecie.
- Incydenty utraty danych były coraz częstsze niezależnie od sektora i typu danych.

Sprostać wyzwaniu

Wyniki niniejszego raportu jasno wskazują, że krajobraz zagrożeń cały czas zmienia się, podczas gdy strategie zabezpieczeń i technologie stosowane w wielu organizacjach są nieadekwatne w starciu z coraz bardziej skomplikowanymi i niszczącymi atakami. Eksplozja nieznanego złośliwego oprogramowania szybko sprawia, że rozwiązania nastawione wyłącznie na wykrywanie stają się niewystarczające. Znane złośliwe oprogramowanie z kolei miażdży istniejącą obronę i uderza w coraz więcej platform. Aplikacje wysokiego ryzyka – jak również Web 2.0, aplikacje do przechowywania plików i dzielenia się nimi, a także zdalne narzędzia administrowania mające uzasadnione zastosowania biznesowe – wciąż mnożą się, otwierając nowe wektory zagrożeń w miarę, jak się rozprzestrzeniają. Jako że zarówno złośliwe, jak i nieumyślne wypadki utraty danych powodują niepowetowane straty dla organizacji niezależnie od ich wielkości i we wszystkich sektorach, i w miarę jak mobilność, konsumeryzacja i Internet przedmiotów zwiększają wyzwanie stawiane bezpieczeństwu danych, organizacje potrzebują lepszej kontroli nad przepływem i wykorzystaniem informacji.

Ale sprostanie ewoluującemu krajobrazowi zagrożeń nie jest jedynym wyzwaniem w świecie IT. Dzisiejsze firmy coraz bardziej opierają się na wolnym przepływie informacji, co sprawia, że sieci w firmach nie mają już jasnych granic. Dane firmowe podróżują w chmurze i urządzeniach mobilnych, promieniując za pośrednictwem idei i postów na portalach społecznościowych. Możliwość wykorzystania prywatnych urządzeń do celów biznesowych („Przynieś własne urządzenie", BYOD), mobilność i cloud computing zrewolucjonizowały statyczne środowisko technologii informacyjnych, wprowadzając konieczność dynamicznych sieci i infrastruktur.

W naszym świecie bardzo wymagających platform infrastrukturalnych i sieci IT, w którym granice nie są już dobrze określone i w którym zagrożenia z dnia na dzień stają się inteligentniejsze, potrzebujemy sposobu na ochronę przedsiębiorstw.

Obecnie widzimy przypływ punktowych produktów bezpieczeństwa, jednakże produkty te są raczej reakcyjne i taktyczne z natury, aniżeli zorientowane architektonicznie. Dzisiejsze korporacje potrzebuję jednej architektury, która łączyłaby wydajne narzędzia bezpieczeństwa sieci z proaktywnymi zabezpieczeniami działającymi w czasie rzeczywistym.

Żeby proaktywnie chronić organizacje, potrzeba nowego paradygmatu.

Architektura zabezpieczeń Software-defined Protection

Żeby sprostać dzisiejszej potrzebie ochrony przed ewoluującymi zagrożeniami, a jednocześnie obsługiwać wymagające infrastruktury IT, Check Point wprowadza Software-defined Protection[64]. Jest to nowa, pragmatyczna architektura i metodologia zabezpieczeń, która oferuje modularną, sprawną, a co najważniejsze bezpieczną infrastrukturę.

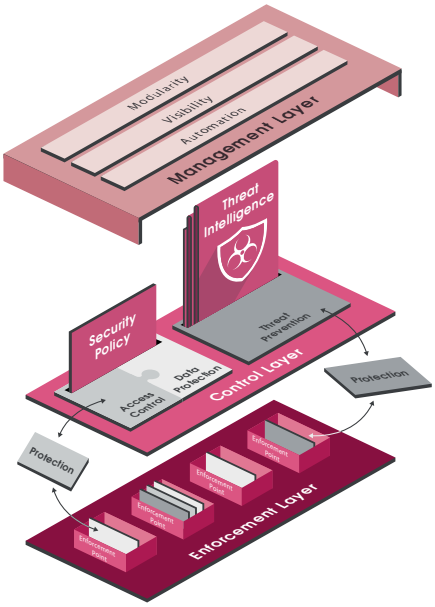
Poprzez wprowadzenie architektury Software-defined Protection organizacje niezależnie od ich wielkości, położone w każdym miejscu na świecie mogą czuć się bezpiecznie, niezależnie, czy chodzi o sieci w kwaterze głównej, oddziały, przeglądanie za pośrednictwem smartfonów lub urządzeń mobilnych czy w czasie korzystania z chmury.

Dzięki Software-defined Protection zabezpieczenia są automatycznie dostosowywane do krajobrazu zagrożeń i nie ma potrzeby, żeby administrator zabezpieczeń ręcznie wdrażał tysiące rad i zaleceń. Te zabezpieczenia gładko integrują się w ramach ogólnego środowiska IT, zaś architektura zapewnia postawę obronną, która zespołowo wpływa zarówno na wewnętrzne, jak i zewnętrzne inteligentne źródła.

Architektura Software-defined Protection (SDP) dzieli infrastrukturę zabezpieczeń na 3 wzajemnie ze sobą połączone warstwy:

- Warstwę egzekwującą, która oparta jest na fizycznych, wirtualnych i umiejscowionych w hoście punktach wykonywania zabezpieczeń i która dzieli sieć, a także egzekwuje logikę bezpieczeństwa w bardzo wymagających środowiskach.
- Warstwę kontrolną, która analizuje różne źródła informacji o zagrożeniach oraz tworzy zabezpieczenia i metody, które będą egzekwowane przez warstwę wykonawczą.
- Warstwę zarządzającą, która organizuje infrastrukturę i zapewnia największy stopień sprawności całej architekturze.

Dzięki połączeniu skuteczności warstwy wykonawczej z bardzo szybko ewoluującą i dynamiczną warstwą kontrolną, architektura SDP zapewnia nie tylko prężność operacyjną, ale również proaktywnie przeciwdziała incydentom w stale zmieniającym się krajobrazie zagrożeń.



Warstwy bezpieczeństwa oparte na oprogramowaniu

Wprowadzenie planu bezpieczeństwa w waszej organizacji

Jedną z największych zalet SDP jest to, że oferuje prostą metodologię wdrażania planu bezpieczeństwa. Check Point Software-defined Protection – Enterprise Security Blueprint szczegółowo opisuje architekturę SDP, jej korzyści i prostą metodologię implementacji. Dostępny jest za darmo na stronie checkpoint.com/sdp.

Kolejne akapity szczegółowo opisują, warstwa po warstwie, jak można wprowadzić SDP w waszej organizacji w celu ochrony przed zagrożeniami przedstawionymi w niniejszym raporcie.

Warstwa egzekwująca

Warstwa egzekwująca ma być niezawodna, szybka i prosta. Składa się zarówno z bram sieciowych bezpieczeństwa, jak i oprogramowania hosta, które funkcjonują jako punkty egzekwujące w sieci przedsiębiorstwa. Punkty te można zaimplementować zarówno jako elementy fizyczne lub wirtualne hosta, lub jako elementy hosta na punktach końcowych w sieci przedsiębiorstwa lub w chmurze.

Gdzie umieścić punkty egzekwujące w naszej sieci? Kiedy sieci były proste, mogliśmy zabezpieczać tylko granice. Ale kiedy granice nie są już tak dobrze określone, gdzie powinniśmy umieścić punkty egzekwujące?

Odpowiedzią jest segmentacja. To ona jest nową granicą. Dzięki dzieleniu skomplikowanego środowiska na mniejsze segmenty w oparciu o profile zabezpieczeń i umieszczaniu punktów egzekwujących na granicach każdego segmentu, środowisko jest bezpieczne!

Warstwa kontrolna

Kolejnym elementem architektury SDP jest warstwa kontrolna. To właśnie tutaj powstają zabezpieczenia, a polityki bezpieczeństwa są przekazywane do punktów egzekwujących. Przy pomocy polityki kontroli dostępu i ochrony danych, administratorzy określają algorytmowe polityki w celu kontrolowania interakcji między użytkownikami, aktywami, danymi i aplikacjami. Jest to w gruncie rzeczy firewall i to firewall następnej generacji.

To właśnie tutaj określa się polityki kontrolujące dostęp do aplikacji wysokiego ryzyka, jakie opisywaliśmy w rozdziale 4, a których przykładem są programy anonimizujące, P2P, magazyny plików, a nawet aplikacje zdalnego administrowania. Polityki te kontrolują również przepływ danych w ruchu i spoczynku, a także chronią przed wyciekami danych takimi, jak te opisane w rozdziale 5.

Polityki kontroli dostępu i ochrony danych już nie wystarczają; istnieje jednak potrzeba ochrony organizacji przeciwko złoczyńcom i ewoluującym zagrożeniom. Żeby osiągnąć ten cel, musimy wprowadzić zabezpieczenia, które mogą zidentyfikować znane i nieznane ataki takie, jak te, które opisaliśmy w rozdziałach 2 i 3.

Dokonuje tego system zapobiegania zagrożeń, druga część warstwy kontrolnej. Zabezpieczenia przed zagrożeniami są tutaj aktualizowane w czasie rzeczywistym i automatycznie chronione przez punkty wykonawcze, więc nie ma potrzeby określać żadnej konkretnej polityki. Wystarczy włączyć mechanizm zapobiegania zagrożeniom.

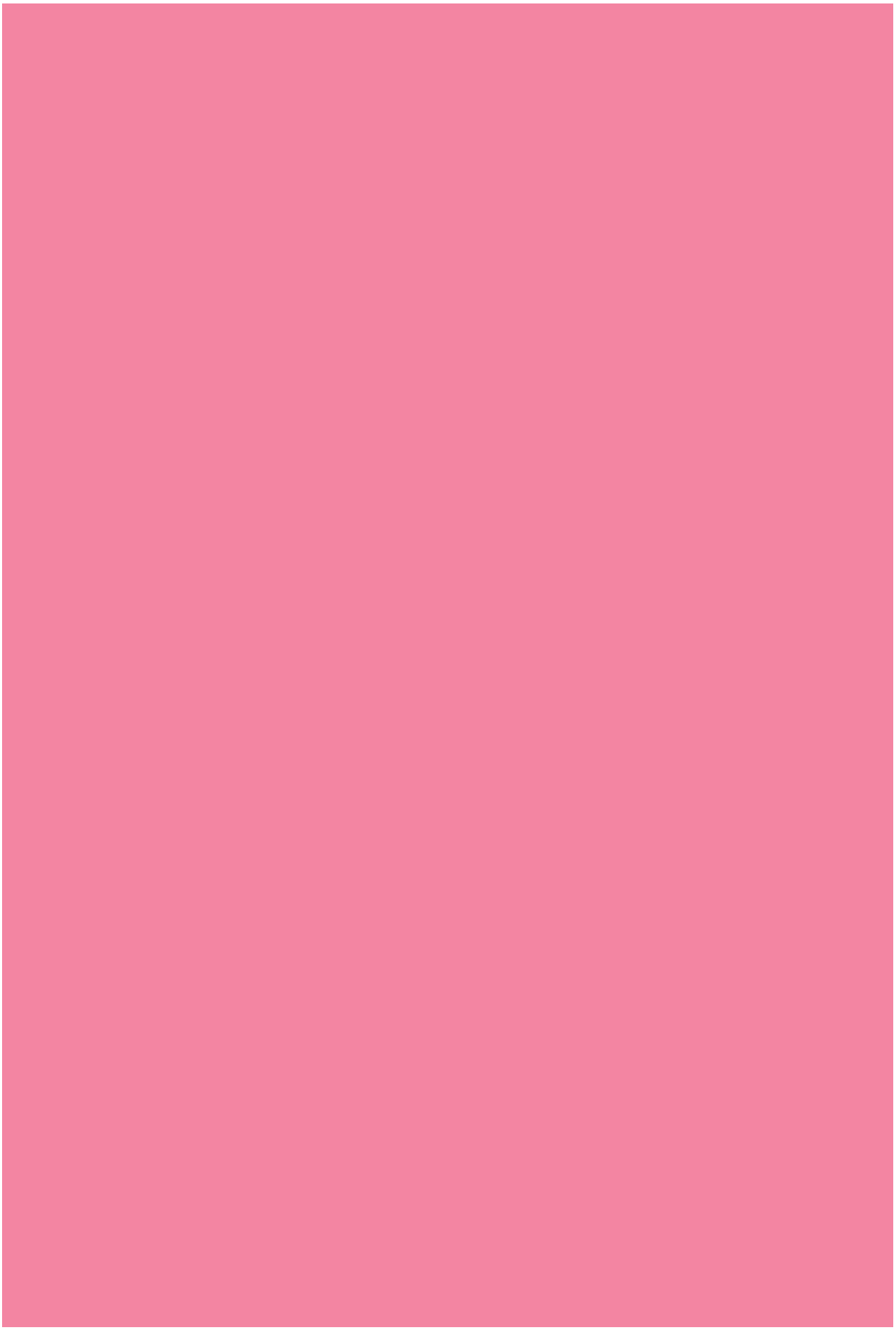
Kluczem do efektywnego zapobiegania niebezpieczeństwom jest wywiad. Wywiad o zagrożeniach powinien opierać się na tylu źródłach, ile to możliwe, a następnie należy przetworzyć i przełożyć go na zabezpieczenia, i przekazać w czasie rzeczywistym do wszystkich punktów egzekwujących.

Warstwa zarządzająca

Trzecią warstwą jest warstwa zarządzająca, która powołuje architekturę SDP do życia i która jest niezbędna do zarządzania całą architekturą. Warstwa zarządzająca cechuje się trzema kluczowymi właściwościami: modularnością, automatyzacją i widocznością.

Modularność zapewnia wielowarstwową politykę, która może posegregować obowiązki administracyjne w celu osiągnięcia optymalnej elastyczności zarządzania. Automatyzacja i otwartość pozwalają zintegrowanym systemom podmiotów zewnętrznych na tworzenie polityk i zabezpieczeń w czasie rzeczywistym. I ostatnia z właściwości: widoczność, możliwość zbierania informacji o zabezpieczeniach ze wszystkich punktów egzekwujących, co daje ogólny ogląd na stan bezpieczeństwa w organizacji.

Software-defined Protection zapewnia modularną i dynamiczną infrastrukturę, która szybko dostosowuje się do ewoluujących niebezpieczeństw i środowisk IT.



07

O TECHNOLOGIACH OPROGRAMOWANIA CHECK POINT

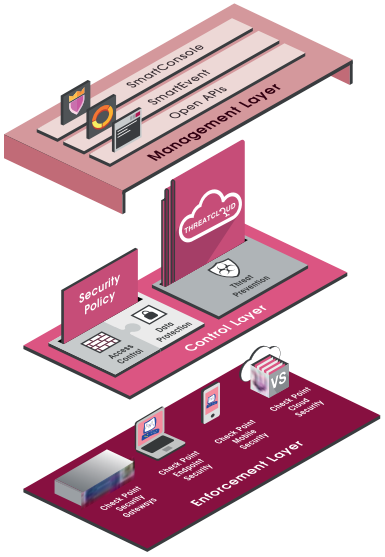
07 O TECHNOLOGIACH OPROGRAMOWANIA CHECK POINT

Od 20 lat misja Check Point polega na zabezpieczaniu Internetu. Od wymyślenia Firewall do przewodzenia branży bezpieczeństwa sieci, Check Point koncentruje się na opracowywaniu technologii potrzebnych do zapewnienia bezpieczeństwa firmom w dobie rozwoju Internetu.

Internet w dniu dzisiejszym jest nie tylko pełnoprawną platformą dla biznesu, lecz także wymarzonym polem dla cyberprzestępców. Biorąc pod uwagę to środowisko, Check Point opracowało architekturę umożliwiającą rozwój wielowarstwowych strategii zwalczania zagrożeń, która zapewnia maksymalną ochronę przeciwko każdemu niebezpieczeństwu, wliczając w to ataki zero-day.

Check Point SDP

Check Point określił i opracował architekturę SDP, zapewniając konieczną elastyczność, żeby poradzić sobie z nowymi zagrożeniami i uwzględnić nowe technologie.



Check Point SDP

Check Point oferuje szeroki zakres punktów wykonawczych, w tym: wydajne urządzenia zapewniające bezpieczeństwo sieci, wirtualne bramki, oprogramowanie hosta na punktach końcowych i mobilne aplikacje. Mogą one być umieszczone w sieci przedsiębiorstwa lub w chmurze.

Jeśli chodzi o warstwę kontrolną, Check Point posiada najbardziej zaawansowany na rynku firewall następnej generacji, zaś nasz system ThreatCloud jest największą otwartą bazą wiedzy o zagrożeniach dostępną w czasie rzeczywistym, która zasila nasze punkty egzekwujące w czasie rzeczywistym.

W końcu, architektura Check Point jest zarządzana z jednolitej konsoli bezpieczeństwa: modularnej, skalowalnej i otwartej dla programów od dostawców zewnętrznych.

Check Point zapewnia architekturę bezpieczeństwa, jakiej współczesne organizacje potrzebują w celu przeciwdziałania jutrzejszym zagrożeniom.

Więcej informacji na temat SDP uzyskacie na stronie www.checkpoint.com/sdp

Check Point łączy holistyczne podejście do bezpieczeństwa z innowacyjnymi rozwiązaniami technologicznymi, żeby sprostać dzisiejszym wyzwaniom i ponownie ustanowić bezpieczeństwo jako motor działalności gospodarczej.

Stale uznawany przez analityków za lidera rynkowego w bezpieczeństwie sieci, Check Point od 20 lat zapewnia klientom innowacyjne, dostosowane do przedsiębiorstw rozwiązania bezpieczeństwa i najlepsze praktyki. Klientela Check Point obejmuje ponad 100 tysięcy organizacji każdej wielkości, w tym wszystkie firmy Fortune and Global 100.

pureAdvantage
CHECK POINT ATC

CLICO

Zapraszamy do uczestnictwa w autoryzowanych szkoleniach, pozwalających uzyskać prestiżowe tytuły:

- CCSA – Check Point Certified System Administrator
- CCSE – Check Point Certified Security Expert
- CCMSE – Check Point Managed Certified Security Expert
- CCEPE – Check Point Certified Endpoint Expert
- CCMA – Check Point Certified Master Architect

Zgłoszenia E-mail: atc@clico.pl

Adres i telefony: CLICO Sp. z o.o., ul. Oleandry 2, 30-063 Kraków
tel. (12) 292-75-25, (12) 632-51-66, wew. 5
fax (12) 292-80-55, (12) 632-36-98

W Centrum Szkoleniowym CLICO można zdawać egzaminy w ramach autoryzowanego ośrodka certyfikacji Pearson VUE położonym w naszym Oddziale w Katowicach w zakresie znajomości produktów firmy Check Point Software Ltd.

Informacje, zgłoszenia: e-mail: Katowice@clico.pl

Adres naszego Centrum Pearson VUE: Clico Sp. z o.o. o/Katowice
ul. Ligocka 103
40-568 Katowice

PRZYPISY

1 Stoll Cliff, The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage, New York, NY: Pocket Books, 2005 (wyd. polskie: Kukułcze jajo, Poznań: Dom Wydawniczy REBIS, 1998)

2 http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/

3 http://www.entrepreneur.com/article/231886

4 http://www.darkreading.com/advanced-threats/mass-customized-attacks-show-malware-mat/240154997

5 http://www.checkpoint.com/campaigns/securitycheckup/index.html

6 http://www.checkpoint.com/products/threat-emulation/

7 http://www.checkpoint.com/threatcloud-central/index.html

8 https://supportcenter.checkpoint.com/supportcenter/portal/role/supportcenterUser/page/default.psml/media-type/html?action=portlets.DCFileAction&eventSubmit_doGetdcdetails=&fileid=20602

9 https://www.checkpoint.com/products/softwareblades/architecture/

10 http://www.checkpoint.com/products/index.html#gateways

11 Huxley Thomas Henry, On the Reception of the Origin of Species, 1887, http://www.todayinsci.com/H/Huxley_Thomas/HuxleyThomas-Quotations.htm

12 http://www.checkpoint.com/threatcloud-central/downloads/check-point-himan-malware-analysis.pdf

13 http://usa.kaspersky.com/

14 http://msdn.microsoft.com/en-us/magazine/cc164055.aspx

15 http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon

16 http://news.cnet.com/Code-Red-worm-claims-12,000-servers/2100-1001_3-270170.html

17 http://www.cnn.com/2004/TECH/internet/05/03/sasser.worm/

18 http://support.microsoft.com/kb/2664258

19 http://www.pcmag.com/article2/0,2817,2370016,00.asp

20 https://www.virustotal.com/

21 http://www.av-test.org/en/home/

22 http://www.checkpoint.com/threatcloud-central/downloads/10001-427-19-01-2014-ThreatCloud-TE-Thwarts-DarkComet.pdf

23 http://contextis.com/research/blog/malware-analysis-dark-comet-rat/

24 http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Portable_Executable.html

25 http://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

26 Mariotti John, The Chinese Conspiracy. Bloomington, IN: iUniverse.com, 2010.

27 http://www.checkpoint.com/campaigns/security-report/download.html?source=google-ngfw-us-sitelink-report&gclid=CIfK-JuOhrwCFZFxQgodsBYA_w

28 https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/3/html/Security_Guide/ch-risk.html

29 Anderson Chris, The Long Tail: Why the Future of Business is Selling Less of More, New York, NY: Hyperion, 2006 (wyd. polskie: Długi ogon. Ekonomia przyszłości - każdy konsument ma głos, Poznań: Media Rodzina sp. z o.o., 2008)

30 http://www.fbi.gov/about-us/history/famous-cases/willie-sutton

31 http://searchwindowsserver.techtarget.com/definition/remote-code-execution-RCE

32 http://searchsoa.techtarget.com/definition/Remote-Procedure-Call

33 https://www.checkpoint.com/threatcloud-central/articles/2013-11-25-te-joke-of-the-day.html

34 http://www.checkpoint.com/threatcloud-central/articles/2013-12-03-new-wave-url-domain-malware.html

35 http://www.checkpoint.com/threatcloud-central/articles/2013-11-14-defeating-cryptocker.html

36 http://www.apwg.org/

37 http://www.checkpoint.com/threatcloud-central/articles/2013-12-03-new-wave-url-domain-malware.html

38 http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf

39 http://newgtlds.icann.org/en/program-status/delegated-strings

40 Stephenson, Neal, Cryptonomicon, New York, NY: Avon, 2002 (wyd. polskie: Cryptonomicon, Warszawa: Wydawnictwo MAG, 2010).

41 Orwell, George, Animal Farm, New York, NY: Signet Books, 1956 (wyd. polskie: Folwark zwierzęcy, Warszawa: Warszawskie Wydawnictwo Literackie MUZA SA, 2008).

42 https://www.torproject.org/

43 http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html