Biuletyn

CERT POLSKA

Numer 2 Marzec - Kwiecień 2006

Felieton

Bez CERTowania

Przemysław Jaroszewski

Wolny rynek

Każdy z nas niemal codziennie styka się z najbardziej zliberalizowanym rynkiem na świecie. Tyle, że najpewniej nie zdaje sobie sprawy z jego obecności.

Każdy, komu starcza jeszcze sił na śledzenie bieżących wiadomości z kraju, ma okazję być świadkiem burzliwych rozważań o sensowności niezależności instytucji finansowych czy przewadze państwa opiekuńczego nad liberalnym. Tymczasem warto uzmysłowić sobie, że każdy z nas niemal codziennie styka się z najbardziej zliberalizowanym rynkiem na świecie. Tyle, że najpewniej nie zdaje sobie sprawy z jego obecności. Mam na myśli podziemie internetowe, w którym nowe "przedsiębiorstwa" bez żadnych regulacji tworzą się i ewoluują, dostosowując się do aktualnych możliwości i zapotrzebowań technicznych. Obecna jest konkurencja, wymuszająca obniżanie stawek za usługi, powstają programy lojalnościowe, mające przywiązać klientów do dostawców. Sprzedawcy ani kupujący nie są obciążani podatkami ani obowiązkowymi składkami. Nie ma systemu zezwoleń i koncesji. Obraz mąci jeden, dość istotny szkopuł: większość wymienianych na podziemnym rynku towarów i usług związana jest z internetową przestępczością.

Jeśli zgodzimy się, że faktycznie mamy do czynienia z wolnym, choć nielegalnym rynkiem, powinny na nim działać normalne mechanizmy rynkowej gospodarki. A skoro tak, powinny one w określonych okolicznościach spowodować, że prowadzenie działalności na rynku stanie się nieopłacalne. Zwiększanie świadomości użytkowników, a tym samym zmniejszanie liczby tych, którzy dadzą się łatwo przekonać do zainstalowania złośliwego oprogramowania nie jest niczym innym jak ograniczaniem dostępności zasobów i podnoszeniem kosztów produkcji. Z drugiej strony, jeżeli zmniejszy się skuteczność reklam rozsyłanych poprzez spam a banki będą konsekwentnie stosować mechanizmy sprawiające, że łatwe do pozyskania dane - takie, jak identyfikator użytkownika i hasło, a nawet numer i

W numerze:

data ważności karty kredytowej nie będą wystarczające do tego by dokonać kradzieży, naturalną konsekwencją będzie zmniejszenie podaży. Oba zjawiska, choć niemiłe przedsiębiorcom, w tym specyficznym środowisku wydają się być ze wszech miar pożądane. Oczywiście nie są to jedyne drogi do osiągnięcia sukcesu. I tak, jak na doskonale wolny rynek przystało, chcąc osiągnąć efekty, nie należy liczyć na działania regulacyjne, lecz przede wszystkim wziąć sprawy w swoje ręce. □

Relacja

Black Hat Europe 2006

Siódma edycja znanej konferencji BlackHat Europe odbyła się tradycyjnie w Amsterdamie, w dniach 2-3 marca 2006. Wygłoszono na niej łącznie 25 referatów – wszystkie miały bardzo wysoki poziom. Jak zawsze, prelegenci pochodzili z bardzo różnych środowisk – hakerskich „niezależnych ekspertów", uniwersytetów, komercyjnych producentów systemów zabezpieczających oraz innych firm z branży IT i nie tylko.

Do najciekawszych prelekcji pierwszego dnia należały prezentacje Joanny Rutkowskiej dotyczące nowych technik ukrywania się malware'u oraz Mikko Kiviharju na temat urządzenia do odczytywania i uwierzytelnienia użytkowników za pomocą odcisków palców firmy Microsoft.

Joanna Rutkowska przedstawiła nową klasę złośliwego oprogramowania, mającego funkcjonować jako niewidzialny rootkit w systemie Windows, rezydujący całkowicie w pamięci i niewidzialny dla dzisiejszego oprogramowania antywirusowego oraz anty-rootkitowego. Oprogramowanie to podłącza się do obszarów pamięci jądra, w którym funkcjonuje NDIS (Windows Network Driver Interface Specification) i dysponuje własnym stosem TCP/IP oraz zestawem poleceń. Joanna Rutkowska zademonstrowała przykład połączenia się z backdoorem za pomocą portu TCP 445, równocześnie pokazując, że możliwa pozostaje interakcja z zainfekowanym systemem za pośrednictwem protokołu SMB. Tak funkcjonujący backdoor jest w stanie omijać również firewalle osobiste - takie jak ZoneAlarm.

Mikko Kiviharju wykazał, że sprzedawane przez Microsoft urządzenie biometryczne do uwierzytelniania użytkowników za pomocą odcisków palców (Microsoft Fingerprint Reader) nie nadaje się do poważnych zastosowań - wyklucza go między innymi brak szyfrowania, umożliwiający potencjalne wykradnięcie elektronicznych kopii odcisków i wykorzystanie ich do podszycia się pod użytkownika poprzez atak powtórzeniowy.

Prelegent starał się pokazać na przykładzie wideoklipów z wielu filmów, że prezentowana przez Hollywood wizja hakerów jest zgodna z rzeczywistością. Niewiele brakowało by udało mu się przekonać słuchaczy.

Poruszano również modne tematy wirusów komórkowych (z systemem Symbian) oraz ataków za pomocą Bluetooth.

Pierwszy dzień zakończył się humorystyczną prezentacją Johnny'ego Longa „Hacking, Hollywood Style", w której prelegent starał się pokazać na przykładzie wideoklipów z wielu filmów, że prezentowana przez Hollywood wizja hakerów jest zgodna z rzeczywistością. Niewiele brakowało, by udało mu się przekonać słuchaczy …

W drugim dniu konferencji wyróżnić można prezentacje Philippe Biondi i Fabrice Desclaux dotyczącą komunikatora Skype. Autorzy dokonali „reverse engineering" popularnego komunikatora - wykazując, że chociaż wykorzystanie mechanizmów kryptograficznych zawartych w jego protokole komunikacyjnym wydaje się poprawne, to możliwe jest dokonanie nadużyć, jeżeli jesteśmy w stanie swobodnie posługiwać się protokołem Skype. W tym celu napisali narzędzie, które między innymi jest w stanie wydawać polecenia innym węzłom (komunikatorom). Dzieje się tak, gdyż Skype, zdaniem autorów z założenia w pełni ufa każdemu, kto się jest w stanie z nim dogadać za pomocą protokołu Skype. Warto zapoznać się ze wszystkimi wnioskami autorów.

Kolejną wyróżniającą się prezentacją tego dnia był wykład Gregory Contiego traktujący o roli wizualizacji w analizie zdarzeń sieciowych, w tym analizie ruchu, wykrywaniu ataków i analizie malware'u. Okazuje się, że słynny ekran z Matrixa z opadającymi zielonymi znaczkami niewiele odbiega od prezentowanych przez autora rzeczywistych technik wizualizacji zdarzeń w sieci.

Dzień zakończono kolejną humorystyczną prezentacją Johnny 'ego Longa „Death of a Thousand Cuts - Finding Evidence Everywhere!". Tym razem w formie zabawy z publicznością, polegającej na zgadywaniu, w jakim niespodziewanym gadżecie na biurku znajdować się mogą elektroniczne dowody przestępstwa.

Wszystkie prezentacje a także materiały dodatkowe są dostępne na stronie BlackHat,

http://www.blackhat.com/html/bh-media-archives/bh-archives-2006.html#eu-06

□

Przemysław Jaroszewski

Projekty

SpotSpam

Spam nie jest zjawiskiem nowym i już od kilku lat uważany jest za jedno z najbardziej dokuczliwych dla użytkowników Internetu. Pojawiło się i jest stosowanych praktycznie wiele technicznych metod walki z tym zjawiskiem. Ze sporym opóźnieniem, ale jednak dołączają do nich stopniowo metody prawne. Nadal poważnym problemem pozostaje jednak transgraniczność spamu i konieczność radzenia sobie ze zbieraniem dowodów z wielu miejsc i różnych krajów. Temu zagadnieniu poświęcony jest projekt SpotSpam.

SpotSpam jest projektem współfinansowanym przez Komisję Europejską w ramach Safer Internet Programme (http://europa.eu.int/information_society/activities/sip/index_en.htm), realizowanym przez niemieckie konsorcjum eco wspólnie z Naukową i Akademicką Siecią Komputerową (ściśle: przez zespół CERT Polska) przy udziale Microsoft. Projekt wystartował 26 września 2005 roku i zaplanowany został na 2 lata.

Scenariusz działania zakłada przyjmowanie zgłoszeń od indywidualnych użytkowników Internetu przez krajowe punkty tzw. spambox, zajmujące się problematyką spamu na obszarze krajowym. Spamboxy biorące udział w wymianie danych, niezależnie od własnych działań, przekazywałyby zgłoszenia do bazy SpotSpam. Tutaj dokonywana byłaby ich analiza oraz korelacja, których celem byłoby wydobycie informacji o używanych przez spamera zasobach w sieci oraz grupowanie pojedynczych zgłoszeń w kampanie, czyli grupy identycznych lub bardzo podobnych e-maili wysłanych najprawdopodobniej przez tego samego spamera i zbieranie materiału dowodowego, który mógłby być wykorzystany w potencjalnym przyszłym postępowaniu sądowym. Takie podejście powinno ułatwić ściganie sprawców na podstawie silnych dowodów zarówno dotyczących samej niezamawianej korespondencji, jak i nieuprawnionego wykorzystywania przejętych maszyn.

Formalnie, projekt składa się z 4 modułów:

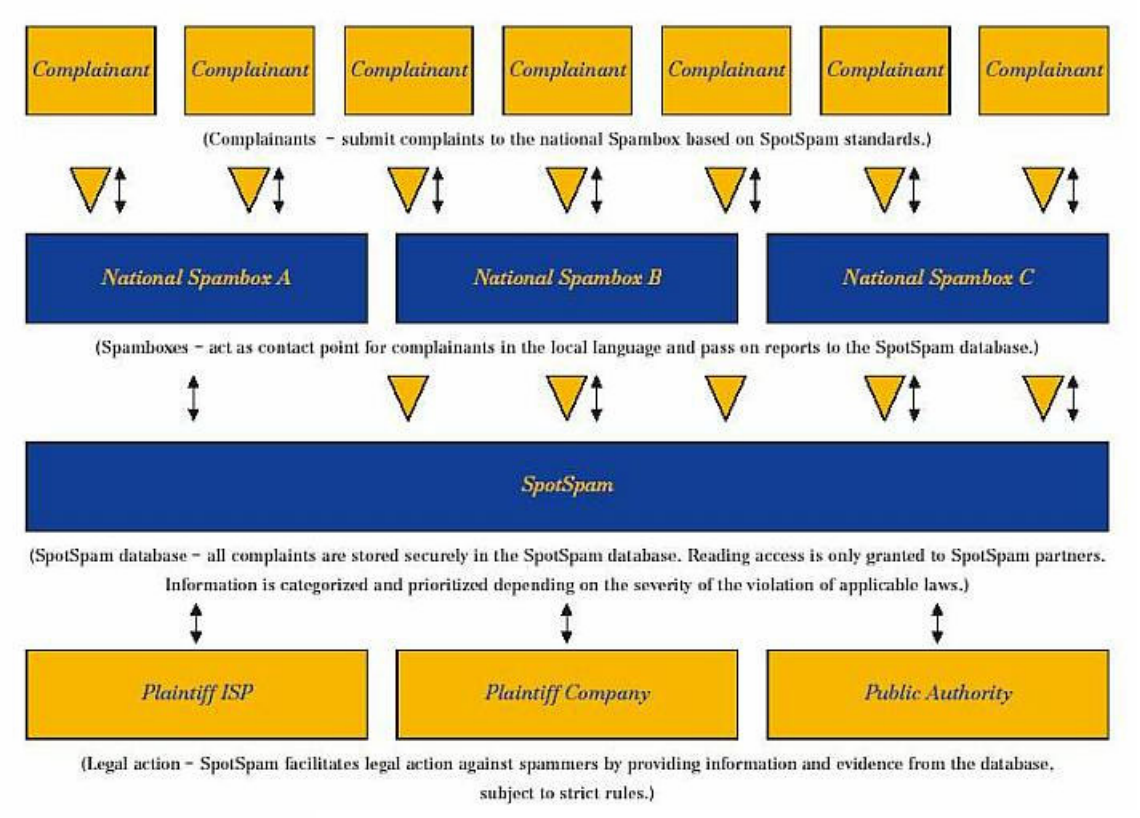
- badania przygotowawcze, dotyczące istniejącego stanu prawnego w poszczególnych krajach UE
- przygotowanie listu intencyjnego dotyczącego zasad zbierania materiału dowodowego
- przygotowanie listu intencyjnego dotyczącego wymiany i udostępniania informacji
- specyfikacja i implementacja prototypu bazy danych wspierającej współpracę

Liczba numeru

ponad

13 500

Tyle przypadków spamu zostało od początku roku odfiltrowanych ze skrzynki, do której trafiają zgłoszenia do naszego zespołu.



CERT Polska odpowiada w szczególności za realizację czwartego, technicznego modułu. Podstawowe problemy, których rozwiązanie należy znaleźć podczas realizacji projektu to:

- umożliwienie indywidualnym użytkownikom przesyłania zgłoszeń zawierających jak największą ilość informacji w jak najprostszy sposób,
- ustrzeżenie się przed „zatruciem" bazy przez wysyłanie zgłoszeń nieprawdziwych lub niebędących spamem,
- ochrona prywatności i danych osobowych

Problemem innej natury, na który nie mamy wpływu w czasie realizacji projektu, jest możliwość rzeczywistego wykorzystania zebranych dowodów, która uzależniona jest od ustawodawstwa (przede wszystkim antyspamowego) poszczególnych krajów. Dla przykładu, w Polsce szczególny przypadek spamu, jakim jest niezamówiona oferta handlowa opisany jest przez ustawę o świadczeniu usług drogą elektroniczną. Na jej podstawie nie jest jednak możliwe ściganie autora całej kampanii, lecz nakazuje ona każdemu z poszkodowanych indywidualne zgłoszenie otrzymania niezamawianej oferty. Być może jednak doświadczenia zebrane przy realizacji SpotSpamu będą mogły zostać spożytkowane przy konstrukcji nowego lub nowelizacji obowiązującego prawa. □

Strona projektu:

http://www.spotspam.net/

Kalendarium CERT Polska

23 - 25 stycznia 2006

Członkowie zespołu CERT Polska uczestniczyli w 17. spotkaniu europejskich zespołów reagujących TERENA TF-CSIRT w Amsterdamie <http://www.terena.nl/activities/tf-csirt/meeting17/> oraz w kolokwium technicznym dla członków organizacji FIRST <http://www.first.org/events/colloquia/jan2006/>. Przemysław Jaroszewski wygłosił prezentację na temat SPF (Sender Policy Framework).

27 stycznia 2006

Odbyło się spotkanie przedstawicieli firmy Gadu-Gadu i CERT Polska, w sprawie wspólnych działań na rzecz bezpieczeństwa w polskiej sieci Internet, w szczególności w odniesieniu do komunikatorów internetowych.

2 lutego 2006

W siedzibie NASK odbyło się drugie spotkanie przedstawicieli zespołów reagujących i komórek bezpieczeństwa polskich operatorów telekomunikacyjnych. W trakcie spotkania wymieniono doświadczenia na temat praktycznych aspektów pracy zespołów, podjęto decyzję o stałych cyklicznych spotkaniach oraz decyzję o zaproszeniu do udziału w spotkaniach przedstawicieli największych polskich portali internetowych.

15-16 lutego 2006

Przemysław Jaroszewski z zespołu CERT Polska uczestniczył w spotkaniu reprezentacji projektu SpotSpam z przedstawicielami firm MessageLabs oraz SpamHaus.org. Spotkanie dotyczyło technicznych metod zwalczania zjawiska spamu.

16 lutego 2006

Członek zespołu CERT Polska (Sławomir Górniak) został oddelegowany w charakterze eksperta narodowego do Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA - http://www.enisa.eu.int). W agencji ENISA pracuje on w zespole odpowiedzialnym m.in. za współpracę z europejskimi zespołami reagującymi.

17 lutego 2006

Delegacja NASK/CERT Polska (Krzysztof Silicki, Przemysław Jaroszewski, Mirosław Maj) wzięła udział w spotkaniu zorganizowanym przez Ministerstwo Transportu i Budownictwa, dotyczącym wypracowania modelu współpracy organów administracji publicznej w zwalczaniu zjawiska spamu. W czasie spotkania CERT Polska przedstawił model algorytmu obsługi spamu zgłaszanego do krajowego *Spamboxu*.

17 lutego 2006

Ukazała się druga edycja raportu CERT Polska dotyczącego bezpieczeństwa przeglądarek internetowych <http://www.cert.pl/news/751>.

28 lutego – 1 marca 2006

W Paryżu, z udziałem przedstawicieli eco Verband der deutschen Internetwirtschaft e.V., przedstawicieli francuskiej administracji rządowej (projekt SignalSpam), Microsoft i CERT Polska, odbyło się spotkanie projektowe projektu SpotSpam oraz spotkanie dotyczące możliwości współpracy pomiędzy projektami SpotSpam i SignalSpam.

2 marca 2006

Mirosław Maj z zespołu CERT Polska wygłosił wykład na konferencji 'Future of Internet Security. Retencja i bezpieczeństwo danych.', organizowanej przez fundację PROIDEA <http://www.fois.proidea.org.pl/>. W panelu dyskusyjnym wziął udział m.in. poseł Bogusław Bosak, który złożył deklarację przedstawienia kwestii dyskutowanych w czasie konferencji i pośredniczenia pomiędzy środowiskiem osób zajmujących się bezpieczeństwem teleinformatycznym, a komisjami sejmowymi poruszającymi zagadnienia z tego obszaru.

7 marca 2006

Delegacja NASK / CERT Polska (Krzysztof Silicki, Mirosław Maj) wzięła udział w spotkaniu organizowanym przez UOKiK, na którym omawiano ideę stworzenia kodeksu dobrych praktyk dla operatorów telekomunikacyjnych, które ograniczyłyby ilość rozsyłanego w sieci spamu. W spotkaniu uczestniczyli przedstawiciele największych polskich operatorów telekomunikacyjnych i dostarczycieli treści w Internecie <http://www.uokik.gov.pl/pl/informacja_i_edukacja/informacja/komunikaty_prasowe/art146.html>.

14 marca 2006

UOKiK wspólnie z NASK zorganizowały konferencję naukową poświęconą zagrożeniom w sieci Internet, w szczególności zjawisku spamu. W konferencji wzięło udział w charakterze prelegentów dwóch członków zespołu CERT Polska: Ireneusz Parafjańczuk, który wygłosił referat o tym, czym jest spam i dlaczego należy z nim walczyć, oraz Przemysław Jaroszewski, który opowiedział o projekcie SpotSpam. Więcej informacji o konferencji znajduje się na stronach UOKiK – http://www.uokik.gov.pl/

Co myślisz o Biuletynie? Wyraź swą opinię!

CERT Polska, NASK

ul.Wąwozowa 18, 02-796 Warszawa
tel. 022 380 82 74, fax. 022 380 83 99
http://www.cert.pl

Redakcja Biuletynu: biuletyn@cert.pl
Kontakt z zespołem: info@cert.pl
Zgłaszanie incydentów: cert@cert.pl