NASK

CERT POLSKA

Raport

Przejęcie domen botnetu Virut

25 lutego 2013

Spis treści

1 Streszczenie

Na przełomie stycznia i lutego 2013 roku Naukowa i Akademicka Sieć Komputerowa i działający w jej strukturach CERT Polska dokonały przejęcia kontroli nad 43 nazwami domenowymi z końcówką .pl, służącymi do zarządzania botnetem Virut, a także do rozprzestrzeniania złośliwego oprogramowania. Działania były poprzedzone szczegółową analizą prawną oraz techniczną i wspierane przez firmy Spamhaus oraz VirusTotal. Wśród przejętych domen znajdowały się także takie, które stanowiły ważną część infrastruktury całego botnetu - także poza domeną `.pl`. W wyniku tych działań ruch z komputerów zarażonych złośliwym oprogramowaniem Virut do centrum zarządzającego (C&C) botnetu został przekierowany do serwera kontrolowanego przez CERT Polska. Uniemożliwia to kontrolowanie tych maszyn przez przestępców i pozwala na gromadzenie cennych danych o miejscach infekcji. Informacje te są udostępniane zainteresowanym partnerom. Z zebranych danych wynika, że próby połączenia z C&C dokonywane są średnio z około 270 tysięcy unikalnych adresów IP dziennie, co stanowi przybliżone górne oszacowanie wielkości botnetu w momencie przejęcia domen. Blisko połowa zarażonych maszyn znajduje się w jednym z trzech krajów: Egipt, Pakistan lub Indie. Polska znajduje się dopiero na 19 miejscu pod względem skali infekcji. Niniejszy raport przedstawia chronologię działań podjętych przez NASK, sposób zbierania danych, oraz wyniki, wskazujące między innymi na mechanizmy zarażania ofiar oraz powiązania z innymi rodzajami przestępczej działalności, np. sprzedaż fałszywego oprogramowania antywirusowego.

2 Wstęp

2.1 Czym jest Virut?

Virut to złośliwe oprogramowanie, służące do przejmowania kontroli nad komputerem bez wiedzy i zgody jego użytkownika. Po uruchomieniu, Virut nawiązuje połączenie do serwera IRC znajdującego się pod kontrolą atakującego. Serwer ten, w wiadomościach prywatnych, przekazuje polecenia pobrania i uruchomienia plików wykonywalnych ze wskazanych adresów URL. W ten sposób, z wykorzystaniem Viruta, można na zainfekowanym komputerze wykonać zdalnie dowolne polecenia i instalować dodatkowe programy modyfikujące zachowanie systemu. Virut wykorzystywany jest między innymi do doklejania reklam do wyświetlanych przez użytkownika treści, ale sieć złożona z zarażonych maszyn (tzw. botnet) Viruta była wynajmowana także do rozsyłania spamu, czy ataków DDoS.

Serwery IRC, służące do zarządzania botnetem, umieszczane były przede wszystkim w domenach z końcówką `.pl` (między innymi `ircgalaxy.pl`, `zief.pl`), a także `.ru` oraz `.at`. W celu podniesienia niezawodności, każda zarażona maszyna dysponowała krótką zadaną listą domen, z którymi próbowała nawiązywać połączenie. Ostatnie odmiany Viruta wykorzystują także mechanizm DGA (ang. *Domain Generation Algorithm*), co pozwala dodatkowo na przekierowanie C&C w razie awarii do specjalnie zarejestrowanej domeny `.com`.

Virut rozprzestrzenia się przede wszystkim infekując pliki wykonywalne w zarażonym

systemie. Oznacza to, że największe ryzyko zainfekowania występuje przy korzystaniu z urządzeń przenośnych takich jak pendrive czy dzielonych zasobów sieciowych, a także przy pobieraniu plików z niezweryfikowanych źródeł, np. torrentów czy stron z crackami. Nowsze wersje Viruta modyfikują także pliki HTML znalezione na zarażonym komputerze, doklejając do nich kod powodujący infekcję Virutem z wykorzystaniem metody *drive-by-download*, tj. przez lukę w przeglądarce lub jej rozszerzeniu podczas przeglądania tak zmodyfikowanej strony. Virut bywał także łączony z innym złośliwym oprogramowaniem, umożliwiającym mu rozprzestrzenianie się na zasadach robaka internetowego, najczęściej przez atak na usługi RPC, w wyniku którego pobierany i uruchamiany był kod Viruta.

2.2 Przejęcie domen botnetu Virut

Opisane w tym dokumencie działania, zmierzające do unieszkodliwienia botnetu Virut, zostały zainicjowane przez NASK. Głównym celem było usunięcie domen służących do zarządzania botnetem i rozpowszechniania złośliwego oprogramowania z Rejestru `.pl`. Działania były poprzedzone szczegółową analizą prawną oraz techniczną. Pierwszym bezpośrednim krokiem działań było zebranie jak najbardziej aktualnych dowodów dotyczących podejrzanych domen, ponieważ sytuacja ulegała dynamicznym zmianom. Z prośbą o pomoc w tym zakresie zwrócono się również do międzynarodowej społeczności, prosząc o przekazywanie informacji o złośliwym oprogramowaniu skojarzonym z niektórymi z przedmiotowych domen. W tym momencie nie przekazywano na zewnątrz informacji o planie działań. W odpowiedzi wsparcie otrzymano od firm Spamhaus oraz VirusTotal.

W oparciu o własne analizy botnetu, zespół CERT Polska zbudował tzw. *sinkhole*, czyli serwer emulujący zachowanie infrastruktury C&C (z ang. *Command and Control*) służącej do zarządzania botnetem. Plan zakładał sinkhole'owanie wszystkich nazw domenowych znajdujących się w domenie `.pl` przez zmianę ich serwerów nazw na adresy kontrolowane przez CERT Polska. Sposób ten umożliwia przekierowanie ruchu z wszystkich zainfekowanych maszyn i uniemożliwienie ich komunikacji z rzeczywistą infrastrukturą C&C, znajdującą się wciąż w rękach cyberprzestępców. Wieczorem 17 stycznia 2013 r. NASK przejął pierwszą partię domen (23 domeny) i przekierował je na ustanowiony sinkhole. Dopiero wtedy informacje o operacji zostały przekazane na zewnątrz - w pierwszej kolejności podmiotom, które przekazały dane operacyjne.

W drugą część operacji, polegającą na przejęciu kolejnych 15 domen, była zaangażowana także firma Home.pl, jako rejestrator, za pośrednictwem którego były one utrzymywane. Przekierowanie ruchu odbyło się 18 stycznia 2013 r., natomiast transfer zakończył się 21 stycznia 2013 r. W tym czasie Spamhaus poinformował zespoły CERT w Austrii i Rosji o domenach w tych krajach, które także wykorzystywane były do zarządzania Virutem. Operację zakończono 6 lutego 2013 r. transferem ostatniej partii 5 domen do NASK od innego partnera, Consulting Service. Łącznie przejęto i przekierowano na sinkhole 43 domeny służące do zarządzania botnetem Virut. Decydującym czynnikiem umożliwiającym przeprowadzenie operacji była zmiana polityki rejestru .pl w zakresie domen, które są rejestrowane w celu zarządzania złośliwym oprogramowaniem i rozpowszechniania go.

3 Sinkhole

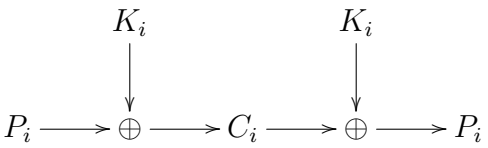
Poniżej przedstawiamy informacje dotyczące konfiguracji serwera `sinkhole.cert.pl` (o adresie IP `148.81.111.111`). Na serwer ten przekierowywany jest cały ruch skierowany na domeny botnetu Virut, które zostały przejęte. Dane otrzymywane od zainfekowanych komputerów są gromadzone i przetwarzane przez zespół CERT Polska.

3.1 Komunikacja

Komputery zainfekowane botnetem Virut łączą się z sinkhole za pomocą różnych adresów DNS w trzech domenach najwyższego poziomu: `.pl`, `.at` oraz `.ru`. Zaobserwowaliśmy ruch związany z botnetem tylko na dwa porty protokołu TCP: 80 oraz 65520. Boty komunikują się albo tekstem jawnym albo za pomocą prostego szyfru strumieniowego.

3.2 Połączenia szyfrowane

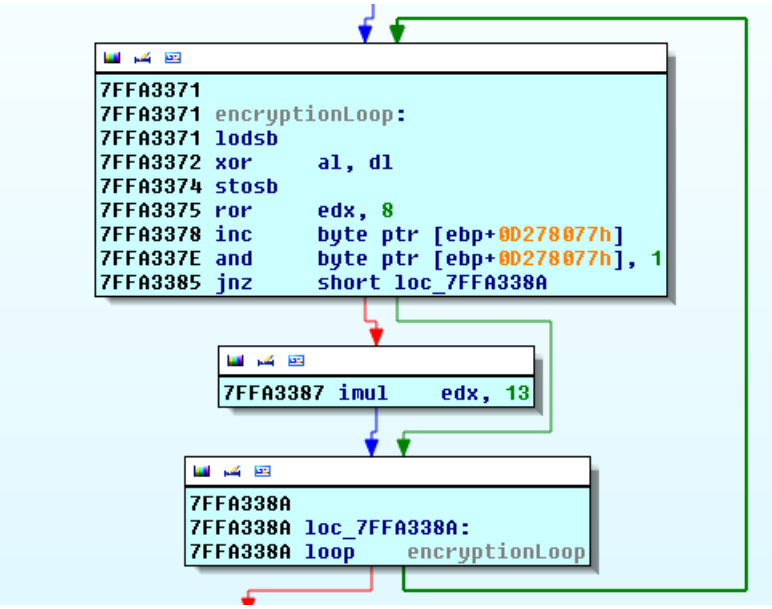
Szyfr wykorzystywany przez botnet Virut jest podobny do szyfru Vernama. Schemat działania szyfru przestawiony jest na rysunku 1. Przez $C\,[1\ldots n]$ oznaczamy tekst zaszyfrowany (z ang. *ciphertext*), przez $P\,[1\ldots n]$ oznaczamy tekst jawny (z ang. *plaintext*), natomiast przez $K\,[1\ldots n]$ oznaczamy strumień klucza (z ang. *keystream*).



Rysunek 1: Schemat działania szyfru Vernama

Szyfr Vernama zakłada, że obie strony komunikacji wymieniły ze sobą odpowiednio dużą część wygenerowanego losowo strumienia klucza. W szyfrowaniu zastosowanym w Virucie strumień klucza generowany jest w sposób pseudolosowy na podstawie 4-bajtowej liczby $S = (S_4S_3S_2S_1)$ wylosowanej przez bota. Algorytm generowania wszystkich bajtów strumienia klucza jest przedstawiony poniżej. Wszystkie zmienne są czterobajtowymi liczbami bez znaku.

$$K_i \leftarrow S_1$$
$$K_{i+1} \leftarrow S_2$$
$$S \leftarrow (S_2 S_1 S_4 S_3)$$
$$S \leftarrow 13 \cdot S$$



Rysunek 2: Pętla generująca strumień klucza

Pierwsze cztery bajty tekstu jawnego przesyłanego przez bota to `NICK`. W takiej sytuacji, ponieważ pierwsze cztery bajty strumienia klucza są przekształceniem liniowym liczby S, możliwy jest atak za pomocą tekstu jawnego, aby uzyskać S. Co ciekawe, bot nigdy nie wymienia z serwerem losowo wygenerowanej wartości początkowej, co pozwala przypuszczać, że prawdziwy C&C botnetu również używał opisanego tutaj ataku, aby ją poznać.

Odpowiedzi z serwera muszą być zaszyfrowane za pomocą tego samego algorytmu z tym samym kluczem początkowym S. Wsteczna kompatybilność serwera szyfrującego dane zagwarantowana jest przez fakt, że dane niezaszyfrowane można traktować tak samo jak dane zaszyfrowane kluczem początkowym $S = 0$.

3.3 Przesyłane dane

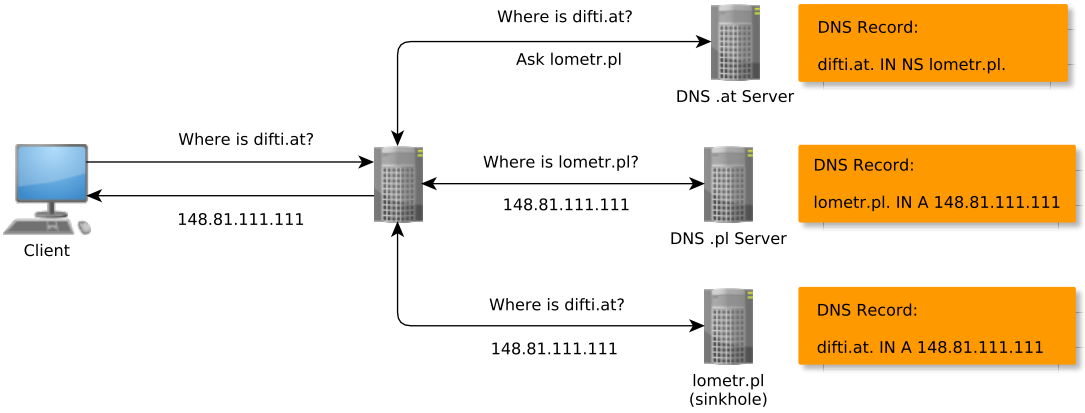
Zainfekowane maszyny, w zależności od wersji, przesyłają, po połączeniu do serwera C&C, następujące informacje (jak widać na rysunku 3):

- wersja systemu operacyjnego,
- *Volume Serial Number* (razem z sumą kontrolną), czyli numer seryjny przypisywany partycji po sformatowaniu. Nie ma on związku z numerem seryjnym przypisanym przez producenta. Użytkownik może również, za pomocą różnych narzędzi, zmienić ten numer na dowolny inny.
- Informacje na temat dodatków typu *Service Pack*.

Rysunek 3: Zrzut ruchu sieciowego

W dalszej części raportu przedstawiamy informacje, które udało nam się uzyskać dzięki tym danym. Na ich podstawie, w połączeniu z adresami IP maszyn łączących się z serwerem sinkhole, byliśmy w stanie ustalić, że zachowanie każdego bota jest w pewnym aspektach stałe. Zainfekowana maszyna próbuje zawsze dołączyć do tego samego kanału oraz przesyła wiadomości w pewnym stałym formacie. Łącząc to z numerem portu, na który bot próbuje się połączyć oraz rodzajem komunikacji (szyfrowana bądź nie) ustaliliśmy, że istniało kilkadziesiąt różnych odmian złośliwego oprogramowania. Maszyny z najbardziej rozpowszechnioną wersją łączyły się z ponad półtora miliona różnych adresów IP (w okresie od 18 stycznia do 6 lutego), co stanowiło ponad połowę wszystkich połączeń. Niektóre z wersji mają rozkład geograficzny inny niż rozkład geograficzny całości botnetu, co może świadczyć o próbie wprowadzenia pewnej regionalizacji względem kanału, na który bot się łączy. W najpopularniejszej wersji jednak bot nie łączy się do żadnego kanału.

3.4 Przejęcie domeny serwera nazw lometr.pl



Rysunek 4: Schemat zapytań o domeny .at, .ru

Domeny, które zostały przez nas zaobserwowane jako związane z botnetem Virut, miały przeważnie ustawiony rekord `NS` na `*.lometr.pl` lub `*.zief.pl`. W związku z tym, w momencie gdy `zief.pl` oraz `lometr.pl` zostały przejęte przez NASK, serwer sinkhole zaczął otrzymywać zapytania o inne, nie przejęte, domeny, takie jak na przykład `difti.at`. Doprowadziło to do możliwości przejęcia ruchu również na domeny nie znajdujące się

w rejestrze `.pl`. Na rysunku 4 przedstawiono schemat zapytania o domenę `difti.at`. Statystyki zawarte w tym raporcie dotyczą również domen `.ru` oraz `.at`, które zostały przejęte w ten sposób.

3.5 Algorytm generowania nazw domen (DGA)

Istnieją wersje botów systemu Virut, które zostały wyposażone w algorytm generowania nazw domenowych (z ang. *Domain Generation Algorithm* – w skrócie DGA). Algorytm ten jest odpowiedzialny za wygenerowanie nazw domen, z którymi bot spróbuje się połączyć w przypadku gdyby zapisane w nim na stałe serwery C&C uznał za skompromitowane. W laboratorium CERT Polska przeprowadzono analizę DGA na podstawie próbki bota.

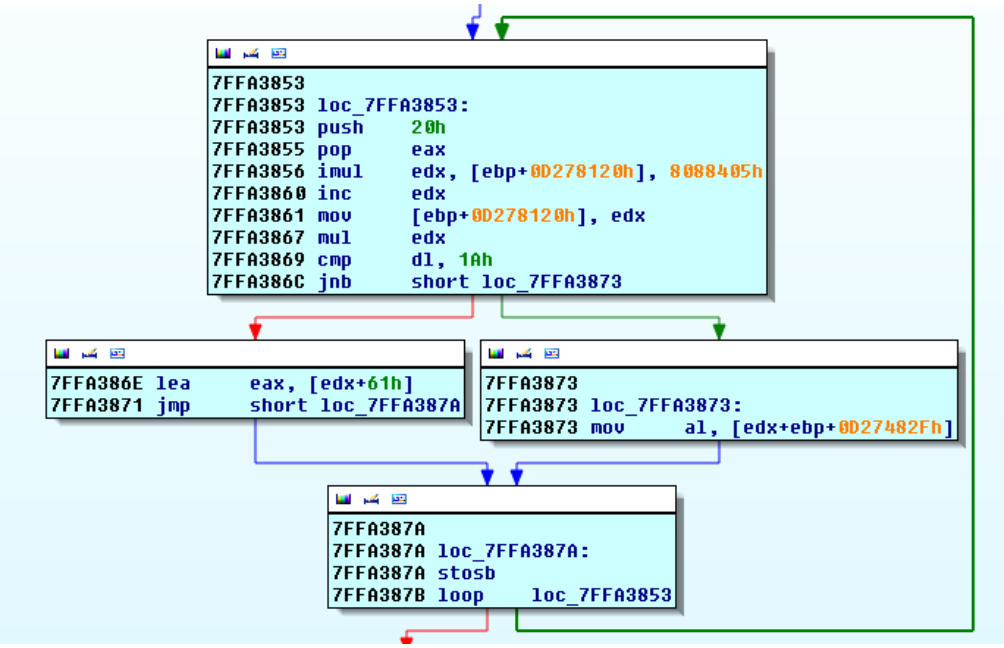
Na początku program pobiera datę (dzień, miesiąc i czterocyfrowy rok) z zainfekowanej maszyny. Następnie tylko na podstawie tej liczby generuje 100 adresów DNS, wszystkie o długości sześciu znaków i zlokalizowane w domenie `.com`. Poniżej (rysunek 5) zaprezentowany jest pseudokod, za pomocą którego następuje generowanie nazw domenowych. Przez *year* oznaczono czterocyfrowy rok, *month* – miesiąc, a przez *day* dzień. Rezultat jest zapisywany w, na początku pustej, tablicy $domain\,[1 \ldots 100]$. Funkcja $\mathrm{shr}\,(number, places)$ wykonuje przesunięcie bitowe liczby *number* o *places* miejsc w prawo. Wszystkie zmienne są czterobajtowymi liczbami bez znaku (z wyjątkiem rzutowania na 64-bitowy typ `long` w linii 11).

```
1:  seed ← year * 10000 + month * 100 + day
2:  for i ← 1 ... 366 do                          ▷ Tworzenie początkowej wartości pseudoloswej
3:      seed ← seed · 0x8088405 + 1
4:  end for
5:  for j ← 1 ... 100 do                                                  ▷ Główna pętla
6:      for i ← 1 ... 594 do                      ▷ Tworzenie wartości pseudolowej dla domeny
7:          seed ← seed · 0x8088405 + 1
8:      end for
9:      for i ← 1 ... 6 do                                  ▷ Tworzenie nazwy domeny
10:         seed ← seed · 0x8088405 + 1
11:         index ← shr ((long) 0x20 · seed, 32)
12:         domain[j] ← domain[j] + character [index]
13:     end for
14:     domain[j] ← domain[j] + ".com"                ▷ Dodawanie końcówki domenowej
15: end for
```

Rysunek 5: Kod generujący nazwy domenowe

Tablica znaków *character*, do której jest odwołanie w 12 linii jest zdefiniowana następująco: $character\,[1 \ldots 31] = (a, \ldots, z, a, e, i, o, u, y)$. Po połączeniu się na port 443 z wygenerowaną domeną klient oczekuje od serwera podpisanej elektronicznie wiadomości zawierającej nazwę domeny, do której się podłączył. Pseudokod, który prezentujemy

na rysunku 5 został uproszczony względem kodu prezentowanego na rysunku 6, który znajdował się w analizowanej próbce.



Rysunek 6: Główna pętla algorytmu DGA

3.6 Uwierzytelnianie serwerów C&C

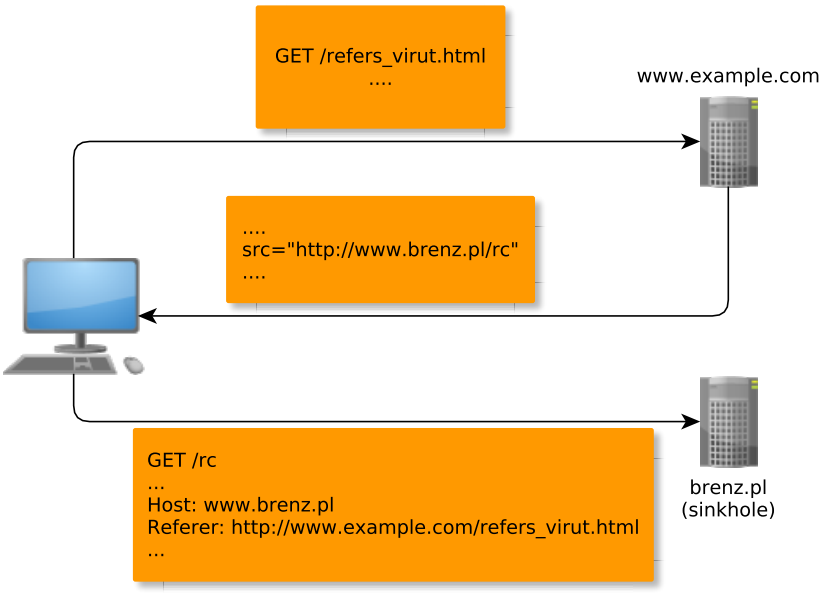
Analizoawana przez CERT Polska próbka bota Virut wymagała wiadomości uwierzytelniających od serwera C&C. Początkowo lista serwerów C&C, z którymi łączy się bot jest zapisana na stałe. Codziennie jednak generowane są nazwy domenowe zgodne z algorytmem DGA. Aby taka domena znalazła się na liście serwerów C&C, serwer musi w ciągu 20 sekund przesłać podpisany (za pomocą 2048 bitowego klucza RSA) skrót (obliczony funkcją SHA-256) domeny, do której klient się połączył.

Gdy bot próbuje się połączyć z serwerem C&C, serwer ma 30 sekund na przeprowadzenie następującej procedury uwierzytelniającej. C&C przesyła do klienta obecną datę (dzień, miesiąc i rok) oraz, tak samo jak poprzednio, podpisany cyfrowo skrót adresu IP serwera oraz tej samej daty. Klient weryfikuje, czy podpis jest zgodny z kluczem publicznym. Następnie następuje weryfikacja daty. Jeśli data na zainfekowanym komputerze różni się od daty na serwerze (np. kiedy obie maszyny są w różnych strefach czasowych) to klient informuje o tym za pomocą wiadomości `DSTAMP`. Wiadomość ta zawiera datę, którą klient chciałby, aby serwer podpisał.

Udało nam się ustalić, na podstawie zgromadzonych danych, że nie wszystkie wersje botów wymagają takich wiadomości.

3.7 Ruch na porcie 80 nie związany z C&C

Od momentu przejęcia domen zaobserwowaliśmy ruch na porcie 80, który nie był związany z komunikatami IRC wysyłanymi do serwera C&C. Na przejętych domenach było również utrzymywane *exploit-pack*, które infekowały maszyny wysyłające do nich żądania HTTP. Żądania te zawierały pełne nagłówki HTTP, dzięki czemu możliwe było stworzenie statystyk dotyczących zarówno infekujących jak i infekowanych hostów. Na rysunku 7 znajduje się schemat prezentujący stronę `http://www.example.com/refers_virut.html` i nagłówki HTTP wysyłane przez klienta. Gdy komputer użytkownika próbuje się skontaktować ze stroną `http://www.example.com/refers_virut.html` wysyła żądanie HTTP zaczynające się od `GET /refers_virut.html` do serwera `www.example.com`. Jeśli w odpowiedzi otrzyma plik HTML, który zawiera odwołanie do zasobu `http://www.brenz.pl/rc` to wyśle do serwera `www.brenz.pl` żądanie `GET /rc` z nagłówkiem `Host: www.brenz.pl` (ponieważ żądanie jest kierowane do `www.brenz.pl`) oraz z nagłówkiem `Referer` ustawionym na `http://www.example.com/refers_virut.html` (ponieważ na tej stronie znalazło się odwołanie). To właśnie żądanie zostanie przechwycone i zalogowane przez serwer sinkhole. Należy też zauważyć, że odwołanie może wymagać wykonania akcji przez użytkownika (kiedy jest to np. hiperłącze) lub nie (kiedy jest to np. załączony plik z kodem JavaScript).



Rysunek 7: Użytkownik wchodzący na http://www.example.com/refers_virut.html

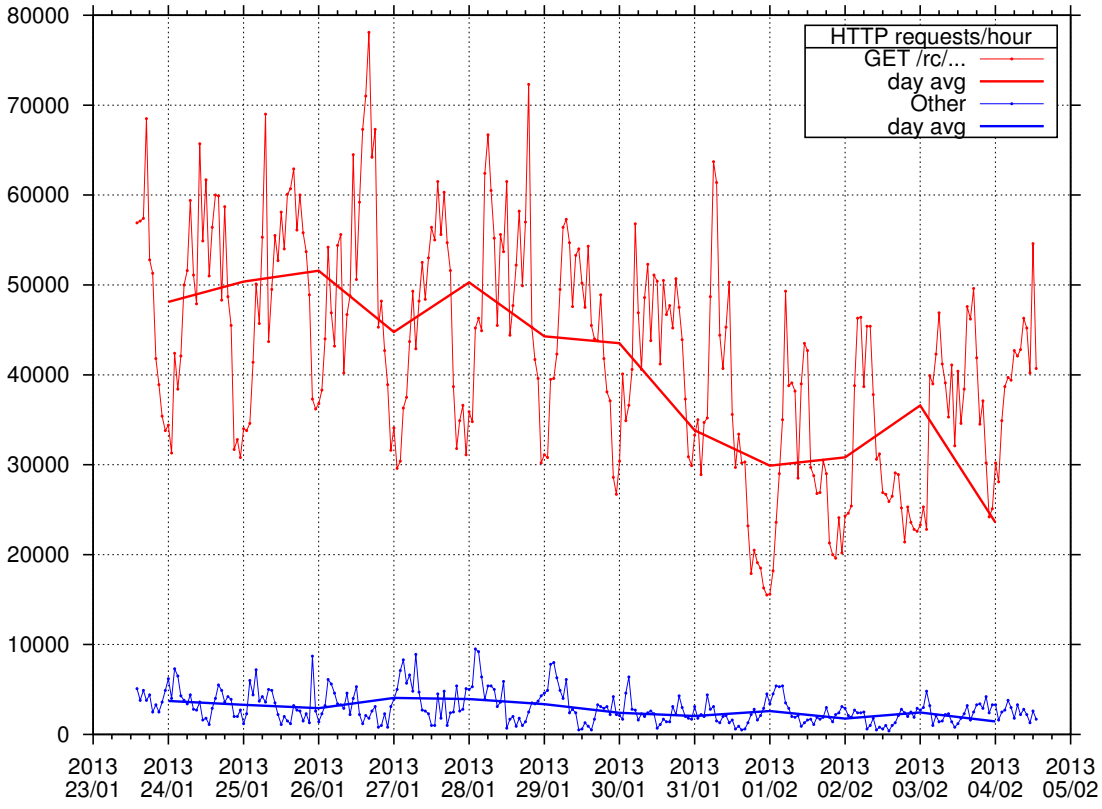
Tabela 2 prezentuje zawartość nagłówka `Host` wysyłanego do serwera HTTP, natomiast tabela 1 prezentuje zawartość 10 najpopularniejszych domen drugiego poziomu z nagłówka `Referer`. Wśród tych domen `whtbk.com` występowało w ponad 27% przypadków. Wśród wartości nagłówków `Referer` pojawiały się również popularne strony ineternetowe takie jak `facebook.com`, `qq.com` czy `youtube.com`.

	Referer	Liczba połączeń
1.	whtbk.com	36 458
2.	localhost	943
3.	qqwutai.cn	498
4.	net76.net	397
5.	carlhattley.com	352
6.	hostzi.com	350
7.	07kino.com	270
8.	facebook.com	209
9.	brenz.pl	202
10.	pytiaozao.com	201

Tabela 1: Nagłówek `Referer`

	Host	Liczba połączeń
1.	brenz.pl	117 682
2.	jl.chura.pl	50 492
3.	trenz.pl	35 639
4.	zief.pl	18 847

Tabela 2: Nagłówek `Host`



Rysunek 8: Liczba żądań HTTP w czasie

Oprócz żądań o *exploit-pack* na port 80 trafiały również żądania HTTP o strony internetowe, które były powiązane z botnetem Virut. Jedną z takich stron była znana już wcześniej `exerevenue.com`, które oferowało instalację oprogramowania na komputerach

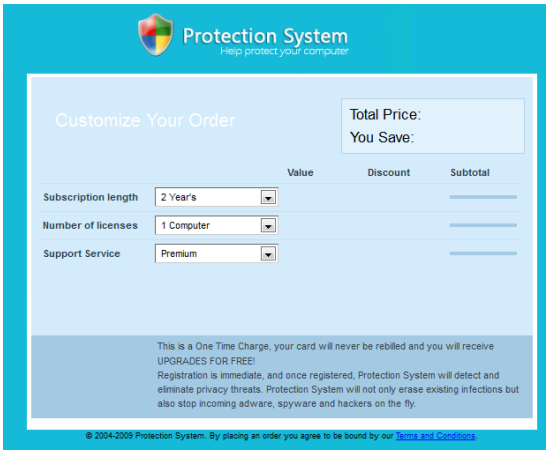
zainfekowanych botnetem. Drugą ciekawą stroną była `protsystem.com`, która zawierała oprogramowanie typu *FakeAV*. Jest to rodzaj złośliwego oprogramowania, które udaje testową wersję programu antywirusowego i obiecuje usunięcie zagrożeń z komputera, o ile wpłacimy pewną kwotę na konto przestępców w zamian za *pełną wersję*.

Wersja strony głównej `protsystem.com` zarchiwizowana w serwisie `web.archive.org` w dniach 4 września 2009 roku oraz 3 lipca 2011 roku jest zaprezentowana na rysunku 9, natomiast na rysunku 10 zaprezentowana jest podstrona służąca do zakupu fałszywego antywirusa. 41 825 zapytań DNS wysłanych do serwera sinkhole w czasie od 18 stycznia do 14 lutego dotyczyło domen `.com`, przy czym zdecydowana większość to zapytania o adresy dwóch wymienionych tu witryn. Szczegółowy rozkład przedstawia tabela 3.

Domena	Liczba zapytań	Udział procentowy
www.protsystem.com	22 665	54,19%
www.exerevenue.com	9 771	23,38%
exerevenue.com	4 990	11,93%
protsystem.com	3 945	9,43%
Inne	454	1,07%

Tabela 3: Zapytania DNS o domeny `.com`

Rysunek 9: Strona główna witryny `protsystem.com`



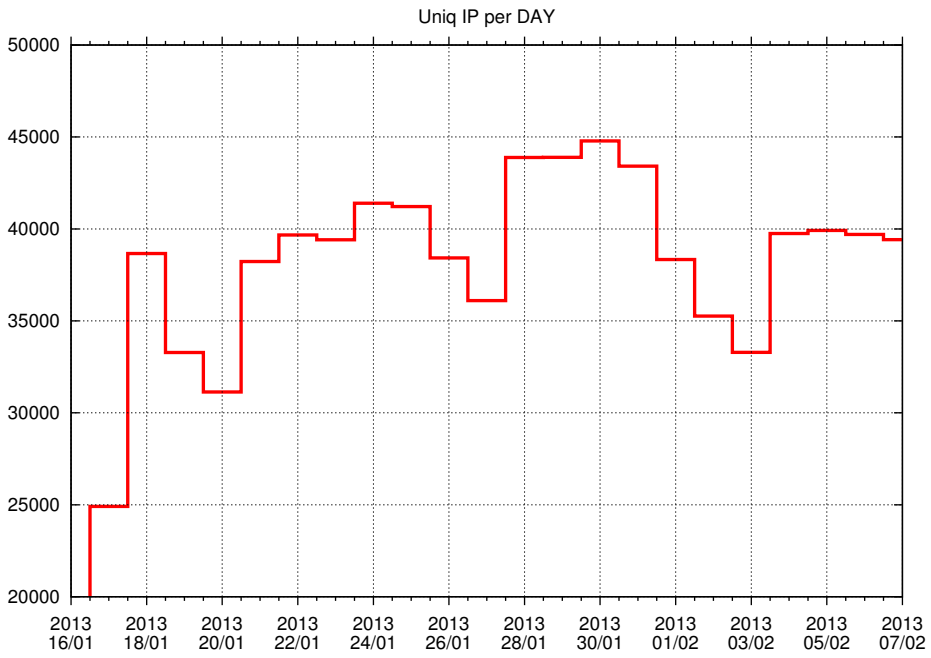
Rysunek 10: Strona zachęcająca do kupna fałszywego antywirusa

4 Statystyki

Poniżej prezentujemy statystyki podsumowujące działanie sinkhole. Są to zarówno statystyki dotyczące liczby nawiązywanych połączeń, rozmieszczenia geograficznego, systemów autonomicznych oraz kwerend DNS.

4.1 Kwerendy DNS

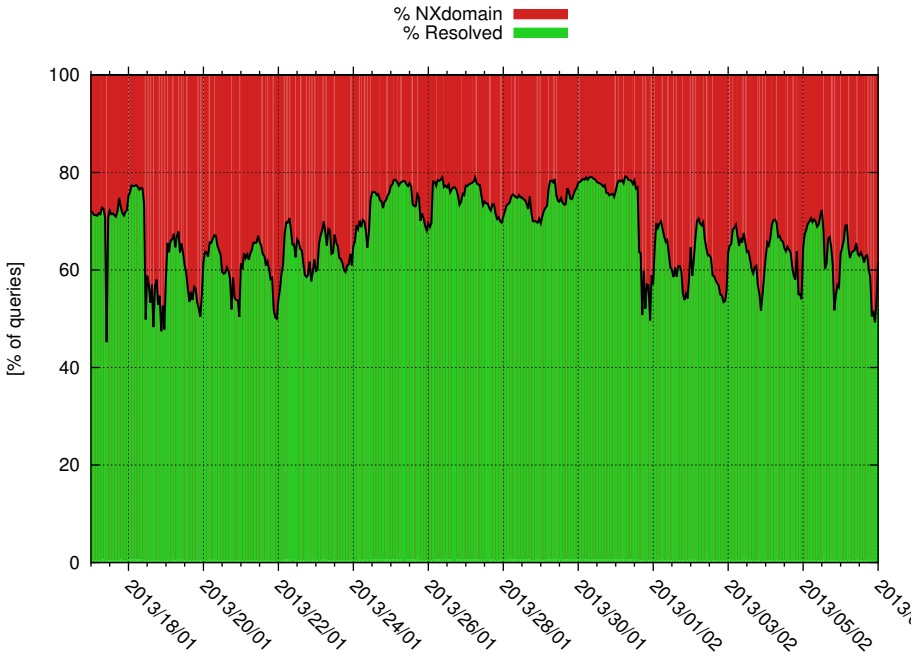
W odróżnieniu od adresów łączących się z usługami na serwerze sinkhole, adresy znalezione w logach DNS mówią jedynie o serwerach DNS-Resolver wykorzystywanych przez zainfekowane komputery. Niemożliwe jednak, na podstawie tych danych, jest ustalenie ile różnych zapytań wyszło od maszyn użytkowników. Ilość unikalnych adresów IP, odpowiadających serwerom DNS-Resolver, na dzień przedstawiona jest na wykresie 11. Oscyluje ona w okolicach 35 do 40 tysięcy.



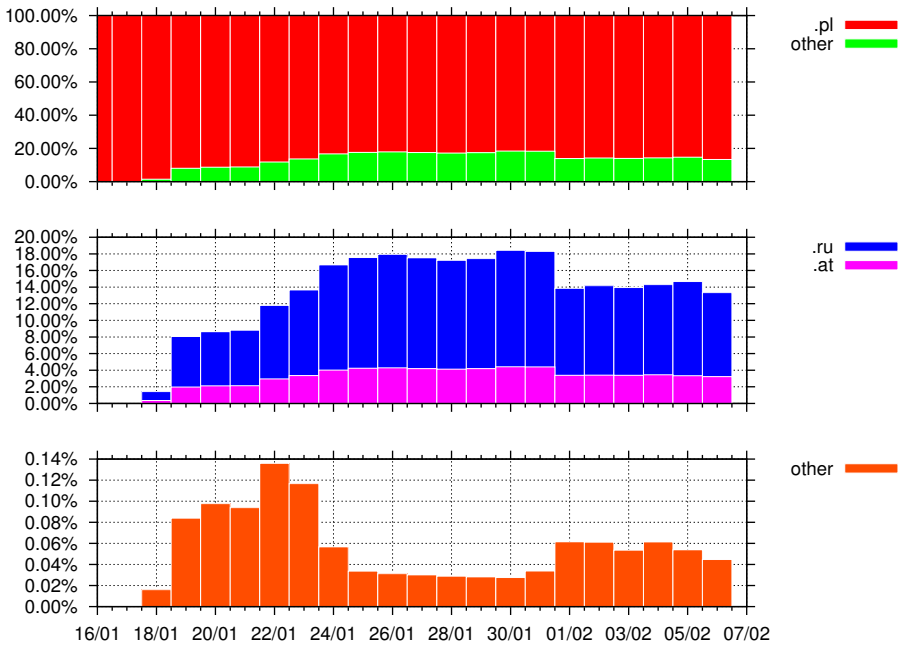
Rysunek 11: Liczba unikalnych adresów IP odpytujących serwer DNS w czasie

Serwer DNS maszyny sinkhole ustawiony był tak, aby odpowiadać jedynie na zapytania o rekordy typu A (zapytanie o adres IPv4) oraz NS (zapytanie o adres serwera nazw). Zapytania o inne typy rekordów kończyły się odpowiedzią z ustawionym kodem błędu `NXDOMAIN`. Jak widać na wykresie 12 zapytania o rekord A i NS stanowiły znaczą część zapytań.

Jak widać na wykresie 13, spośród wszystkich zapytań, ponad 80% stanowiły kwerendy dotyczące domeny `.pl`. Na drugim i trzecim miejscu znajdują się domeny `.at` i `.ru`. Inne domeny TLD stanowią miej niż 1.5‰ wszystkich zapytań.



Rysunek 12: Stosunek odpowiedzi na zapytania o rekordy DNS



Rysunek 13: Zapytania DNS z podziałem na domeny najwyższego poziomu

4.2 Połączenia z C&C

Od 19 stycznia do 5 lutego 2013 zaobserwowaliśmy 3 211 135 unikalnych adresów IP jakie nawiązały połączenie z sinkholem. Połączenia nawiązane zostały z 218 krajów. Znacząco przeważały połączenia na port TCP/80 – zaobserwowaliśmy 2 657 571 unikalnych adresów IP. Adresy z Polski stanowiły 0,67% całości, przy czym również przeważały połączenia na port TCP/80 z 15 407 unikalnymi adresami IP. Połączenia z dziesięciu najwyżej sklasyfikowanych krajów (tabela 4) stanowiły ponad 78% wszystkich połączeń. Dziennie średnio 270 785 unikalnych adresów IP nawiązało połączenie z sinkholem, co pozwala na oszacowanie wielkości botnetu.

	Kraj	**Liczba adresów IP**	**Udział procentowy**
1.	Egipt	580 611	18,08%
2.	Pakistan	487 292	15,18%
3.	Indie	428 565	13,35%
4.	Wietnam	266 350	8,29%
5.	Iran	229 726	7,15%
6.	Indonezja	167 794	5,23%
7.	Chiny	124 449	3,88%
8.	Algieria	92 766	2,89%
9.	Tajlandia	82 887	2,58%
10.	Rosja	48 968	1,52%
		⋮	
19.	Polska	21 569	0,67%

Tabela 4: Zaobserwowane unikalne adresy IP

Na wykresie (rysunek 15) przedstawiona jest liczba unikalnych adresów IP jakie nawiązały połączenie z sinkholem w danym dniu. Zauważalna jest tendencja wzrostowa. Połączenia nawiązywane na porcie 80 przeważały i średnio były nawiązywane z 220 598 unikalnych adresów IP dziennie. Natomiast połączeń na porcie 65520 było znacznie mniej (średnio 56 020 unikalnych adresów IP dziennie). W sumie odnotowaliśmy 2 657 571 połączeń z unikalnych adresów IP na port 80 oraz 748 238 na port 65520.

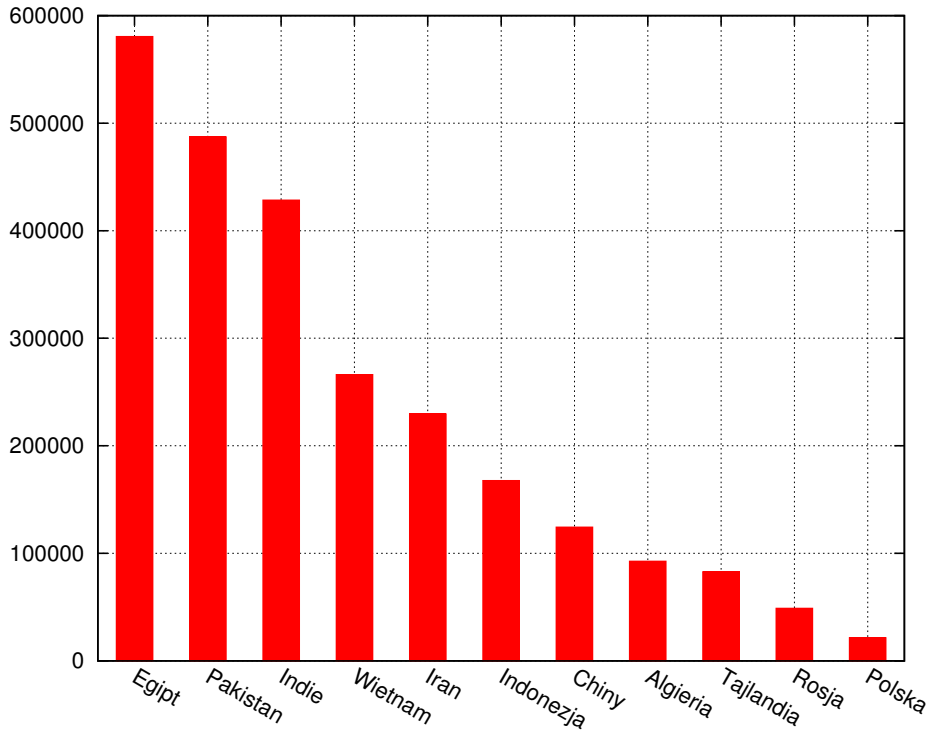
Zgodnie z zaprezentowanym podziałem połączeń na państwa, najwięcej połączeń nawiązywanych jest od operatorów internetowych z Egiptu i Pakistanu. Największy polski operator uplasował się na 73 miejscu z 5 289 zainfekowanymi adresami IP. Dziennie notowaliśmy średnio 1 647 połączeń z adresów IP z Polski. Połączenia pochodziły z 268 różnych systemów autonomicznych.

	Kraj	Liczba adresów IP
1.	Egipt	553 593
2.	Indie	379 076
3.	Pakistan	284 987
4.	Wietnam	222 695
5.	Iran	212 842
6.	Indonezja	144 063
7.	Chiny	108 520
8.	Algieria	88 906
9.	Tajlandia	77 578
10.	Rosja	38 208
	⋮	
20.	Polska	15 407

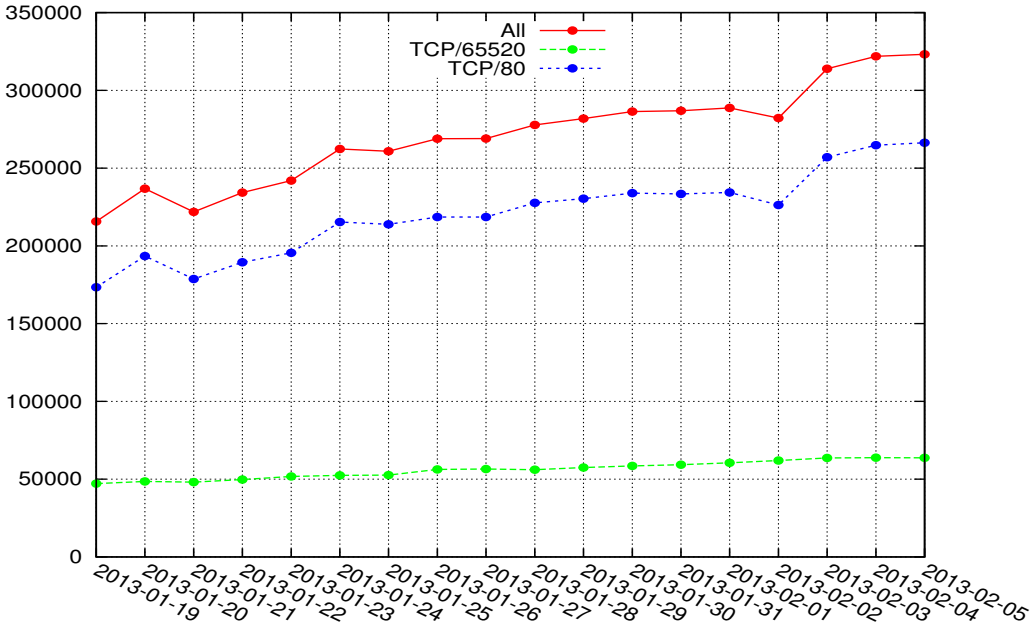
Tabela 5: Połączenia na port TCP/80

	Kraj	Liczba adresów IP
1.	Pakistan	294 025
2.	Egipt	57 150
3.	Indie	55 132
4.	Wietnam	52 110
5.	Indonezja	34 926
6.	Iran	22 510
7.	RPA	18 351
8.	Rosja	17 648
9.	Chiny	16 604
10.	Turcja	9 083
	⋮	
18.	Polska	6 254

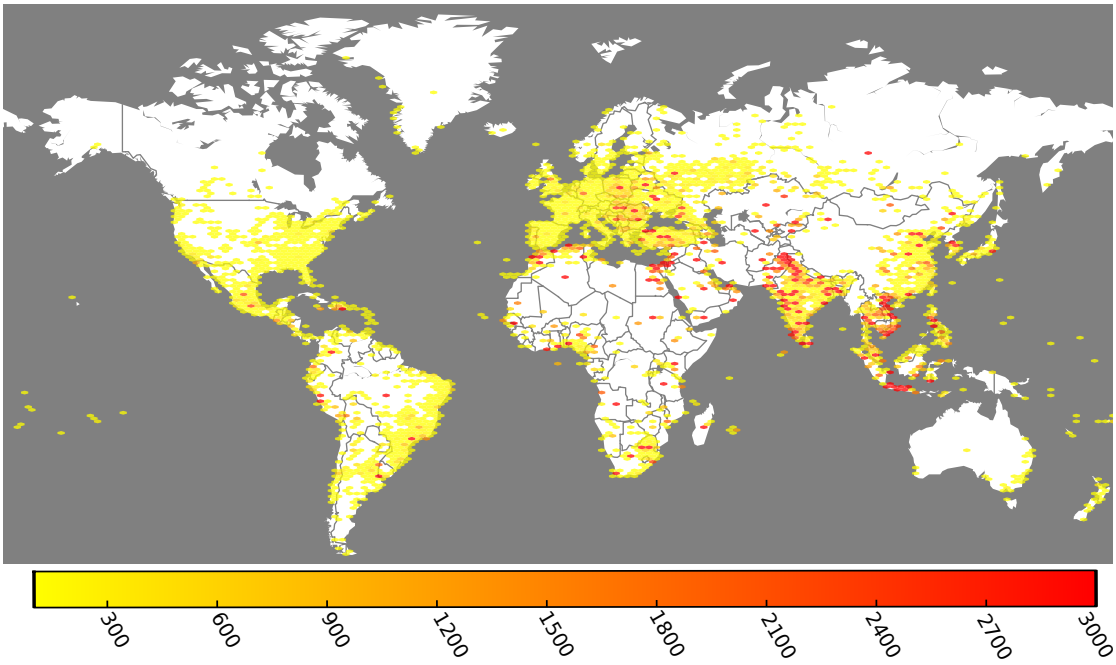
Tabela 6: Połączenia na port TCP/65520



Rysunek 14: Rozkład zainfekowanych adresów IP w podziale na kraje



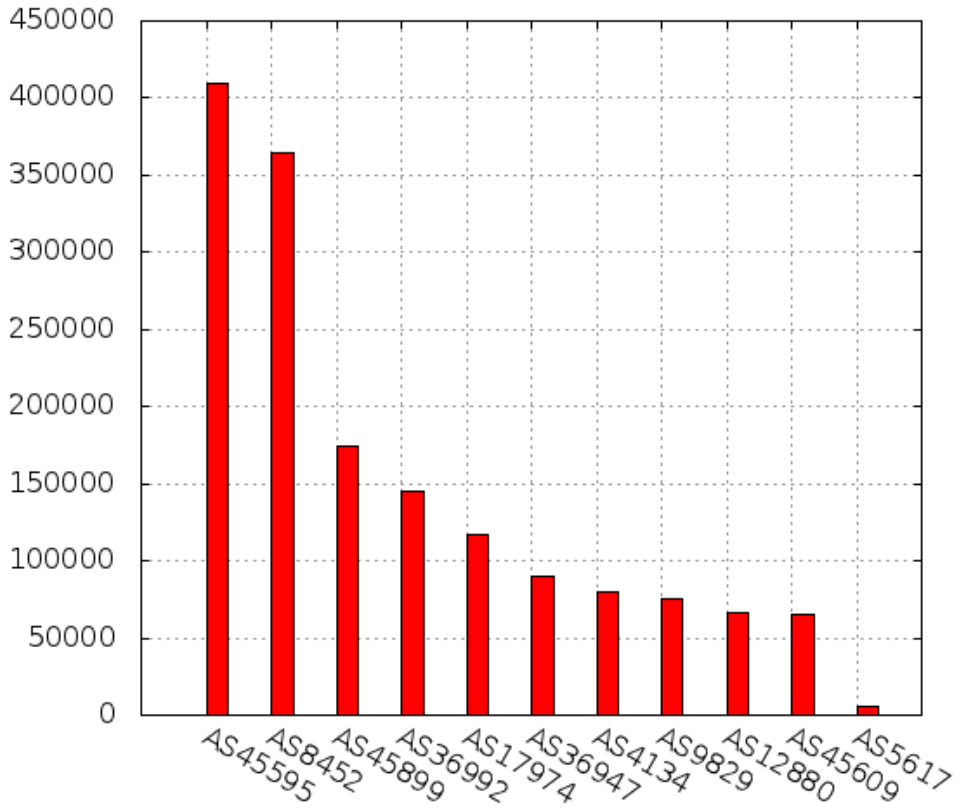
Rysunek 15: Liczba połączeń z unikalnych adresów IP na dzień



Rysunek 16: Rozmieszczenie geograficzne zainfekowanych adresów IP

	Liczba połączeń	ASN	Nazwa	Kraj
1.	410 010	AS45595	Pakistan Telecom Company Limited	Pakistan
2.	364 096	AS8452	TE Data	Egipt
3.	174 002	AS45899	VNPT Corp	Wietnam
4.	145 312	AS36992	ETISALAT MISR	Egipt
5.	117 390	AS17974	PT Telekomunikasi Indonesia	Indonezja
6.	89 606	AS36947	ALGTEL-AS	Algieria
7.	79 752	AS4134	Chinanet	Chiny
8.	75 604	AS9829	National Internet Backbone	Indie
9.	66 169	AS12880	Information Technology Company (ITC)	Iran
10.	65 404	AS45609	Bharti Airtel Ltd. AS for GPRS Service	Indie
		⋮		
73.	5 958	AS5617	Telekomunikacja Polska S.A.	Polska

Tabela 7: Autonomiczne sieci z największą liczbą połączeń z unikalnych adresów IP



Rysunek 17: Autonomiczne sieci z największą liczbą połączeń

	Liczba adresów IP	ASN	Nazwa
1	5 958	AS5617	Telekomunikacja Polska S.A.
2	4 117	AS43447	PTK Centertel Sp. z o.o.
3	3 074	AS8374	Polkomtel Sp. z o.o.
4	2 325	AS39603	P4 Sp. z o.o.
5	1 985	AS12912	Polska Telefonia Cyfrowa S.A.
6	1 342	AS12741	Netia SA
7	1 335	AS15855	Aero 2 sp. z o.o.
8	243	AS21021	Multimedia Polska S.A.
9	132	AS6830	UPC Broadband Holding B.V.
10	89	AS29314	VECTRA S.A.

Tabela 8: Lista polskich sieci z największą liczbą połączeń

Dzięki informacjom przesyłanym przez boty na temat zainfekowanych maszyn byliśmy w stanie ustalić wersję systemu operacyjnego zarażonego komputera. Zaobserwowaliśmy 25 różnych przesyłanych wersji systemów, ale nie wszystkie odpowiadały rzeczywistym wersjom systemów z rodziny Windows. Udało nam się zidentyfikować 8 różnych wersji systemu Windows, które Virut był w stanie zainfekować. Najczęściej spotykanym, zgodnie z oczekiwaniami, okazał się Windows XP z ponad 76% udziale. Kolejnym często spotykanym systemem był Windows 7 (ponad 21%). Pozostałe systemy stanowiły jedynie 3%. Wyniki prezentowane w tabeli 9 nie zawsze wskazują jednoznacznie na wersję systemu. Wynika to z faktu, iż wiele wersji systemu Windows, ze względu na chęć zachowania pomiędzy nimi kompatybilności, ma to samo oznaczenie wersji, ale inną nazwę. Na przykład wersja `020601` może oznaczać zarówno Windows 7 jak i Windows Server 2008 R2. Warto też zauważyć, iż niektóre wersje Viruta nie wysyłały wersji systemu operacyjnego.

Wersja systemu operacyjnego	Liczba wystąpień
Windows XP	2 470 890
Windows 7 / Server 2008 R2	701 637
Windows Vista / Server 2008	20 792
Windows XP 64bit / Server 2003	6 038
Windows 8	3 987
Windows 2000	2 403
Windows 98	1 794
Windows ME	106
Brak	28 439
Inne	38

Tabela 9: Zaobserwowane systemy operacyjne

A Lista domen i adresów IP

Poniżej znajduje się lista domen, które zidentyfikowaliśmy jako związane z botnetem Virut.

A.1 Domeny .pl

1. adle.pl
2. asyr.pl
3. bigex.pl
4. brans.pl
5. brenz.pl
6. bton.pl
7. cfan.pl
8. chura.pl
9. civix.pl
10. deps.pl
11. ghura.pl
12. hamb.pl
13. idet.pl
14. idon.pl
15. ircgalaxy.pl
16. ixie.pl
17. kerit.pl
18. kilme.pl
19. konter.pl
20. lifty.pl
21. lometr.pl
22. meiu.pl
23. merts.pl
24. mugu.pl
25. nels.pl
26. nigim.pl
27. play9.pl
28. ragom.pl
29. remp.pl
30. runk.pl
31. sizi.pl
32. strup.pl
33. sums.pl
34. tanz.pl
35. timid.pl
36. traum.pl
37. trenz.pl
38. tymis.pl
39. valc.pl
40. vand.pl
41. vasli.pl
42. volke.pl
43. zief.pl

A.2 Domeny .ru

1. alr4.ru
2. bzug.ru
3. cawt.ru
4. dbut.ru
5. gbil.ru
6. gimbs.ru
7. ijol.ru
8. ilgo.ru
9. ilopa.ru
10. ketor.ru
11. libis.ru
12. lilke.ru
13. limag.ru
14. linug.ru
15. migtu.ru
16. mlix.ru
17. pamip.ru
18. qnx1.ru
19. rdek.ru
20. rolmi.ru
21. rulm.ru
22. tasb.ru
23. tim4.ru
24. varpo.ru
25. vilq.ru
26. wict.ru
27. xalx.ru
28. xdix.ru
29. xitr.ru
30. ziten.ru

A.3 Domeny .at

1. amfib.at
2. difti.at
3. egab.at
4. ikepa.at
5. kamfo.at
6. maft.at
7. mampo.at
8. sox4.at

A.4 Inne domeny i adresy IP

Poza wymienionymi powyżej, zaobserwowaliśmy jeszcze jedną domenę związaną z botnetem Virut: `adxhost.org`. Wszystkie te domeny powiązane były z adresem IP `60.27.58.4` bądź z adresem IP z klasy `81.177.170.0/24`.