# Wyciąg z ogólnej analizy ataków
# na witryny administracji państwowej RP w okresie 21-25 stycznia 2012r.

W dniach 21-25 stycznia 2012 miał miejsce szereg ataków na zasoby instytucji administracji państwowej, zorganizowanych w ramach akcji protestacyjnej przeciw podpisaniu przez Polskę porozumienia ACTA (Anti-Counterfeiting Trade Agreement, ACTA.

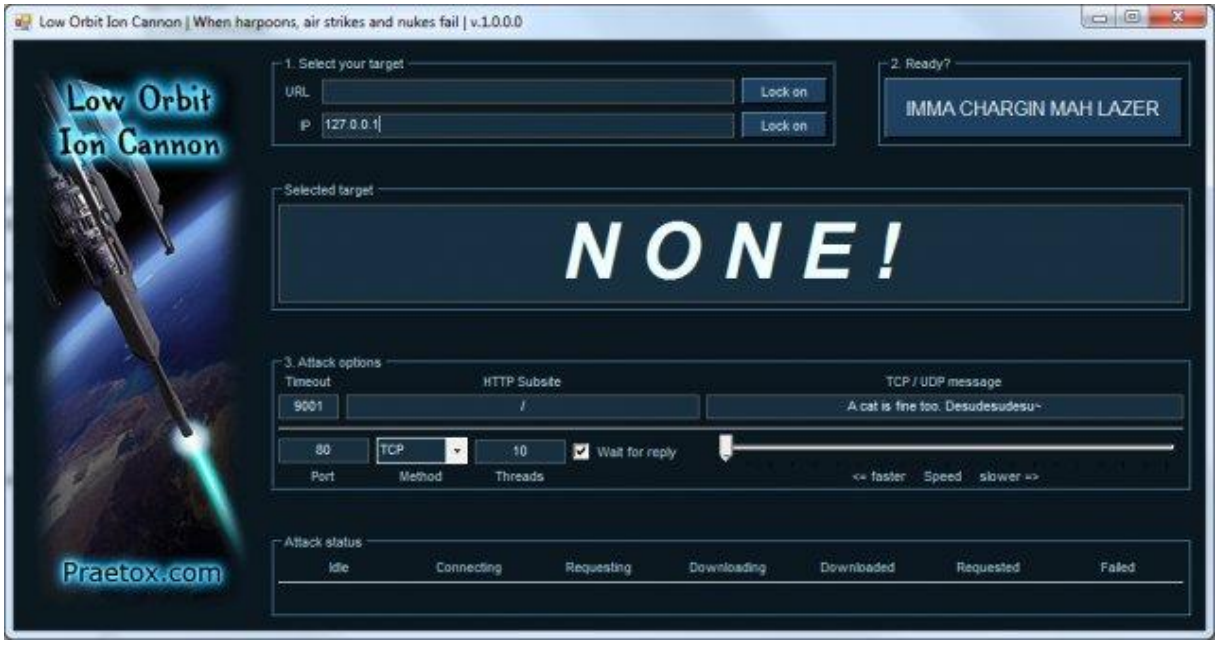
Przede wszystkim zaobserwowano ataki typu odmowa usług DDoS (Distributed Denial of Service) skierowane przeciwko serwerom WWW na których utrzymywane był strony ważniejszych instytucji administracji rządowej.

Ataki miały na celu wysycenie łącza internetowego a przez to spowodowanie niedostępności strony WWW.

Na podstawie analizy logów (analiza obejmuje żądania http, które przeszły przez inne systemy filtrowania i zostały „obsłużone" przez serwer WWW) stwierdzono wykorzystanie wielu różnych narzędzi w celu wygenerowania dużej ilości ruchu.

W pierwszej fazie ataku wykorzystano głownie narzędzie LOIC (Low Orbit Ion Cannon) zarówno w formie aplikacji WEB czyli dostępnej na stronach WWW jak i wersji możliwej do zainstalowania na poszczególnych komputerach.

Oprogramowanie to po raz pierwszy zostało wykorzystane w roku 2010 podczas ataku na instytucje finansowe Paypal, Mastercard, i Visa w odwecie za działania wymierzone przeciw firmom, które "nie sprzyjają" Wikileaeks.



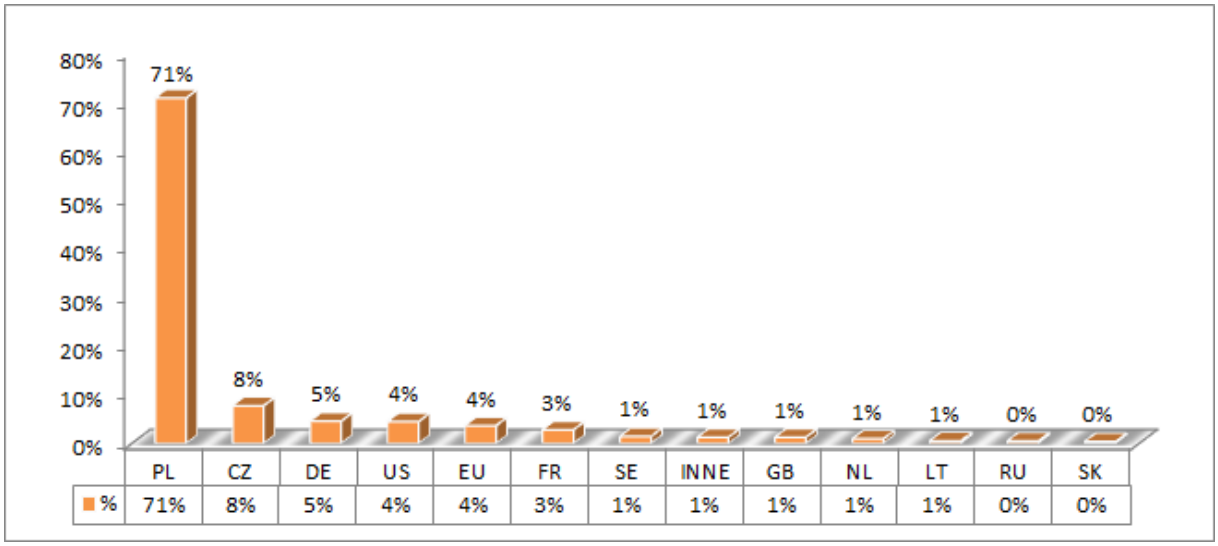

**Rysunek 1: Oprogramowanie LOIC**

LOIC ma możliwość generowania zapytań zarówno w formie HTTP jak i ruchu UDP. Ze względu na charakterystyczne żądania HTTP jakie generuje powyższe oprogramowania, na podstawie logów zidentyfikowano pierwszą dziesiątkę najczęstszych fragmentów zapytań stosowanych podczas ataków:

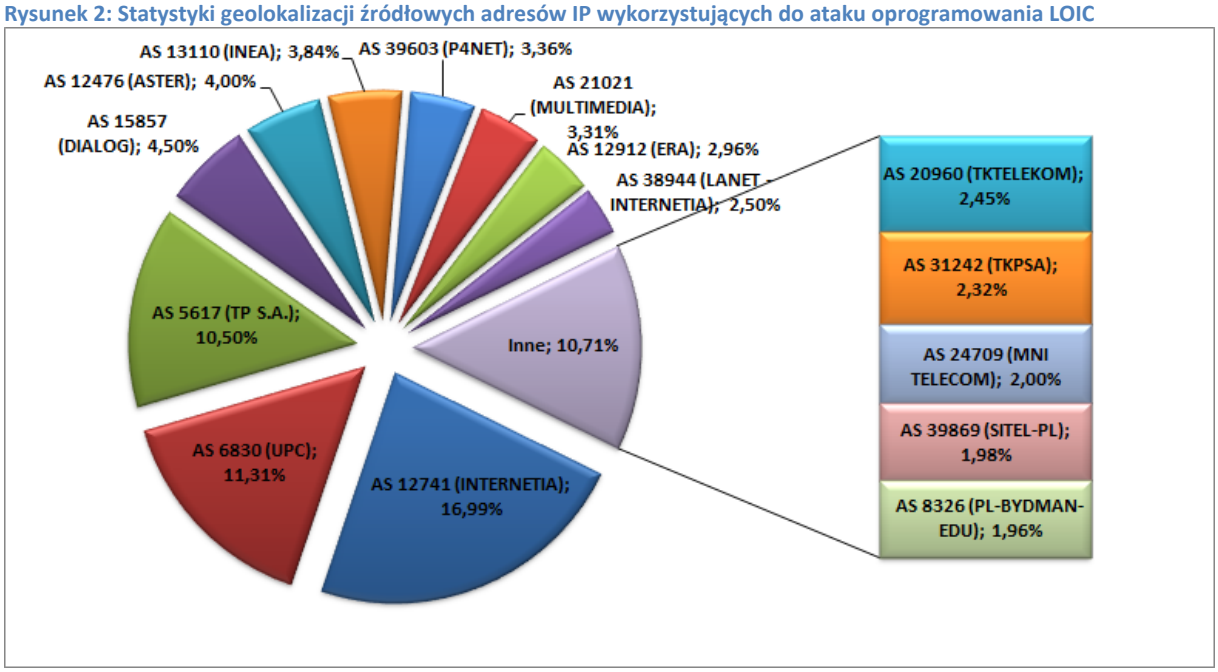
```
msg=STOP%20ACTA
msg=
msg=We%20Are%20Anonymous!
msg=STOP%20ACTA!
```

```
msg=We%20Are%20Legion
msg=we%20are%20anonymous
msg=Nie%20dla%20ACTA!
msg=STOP%2520ACTA
msg=NO%20ACTA
msg=516168466121864616815681641615 18
```

Przeprowadzone analizy źródeł ataków występujących w logach wskazują na 71% udział adresów IP z terenu Polski. Poniższy wykres przedstawia informacje o geolokalizacji źródłowych adresów IP wykorzystujących do ataku oprogramowanie LOIC.

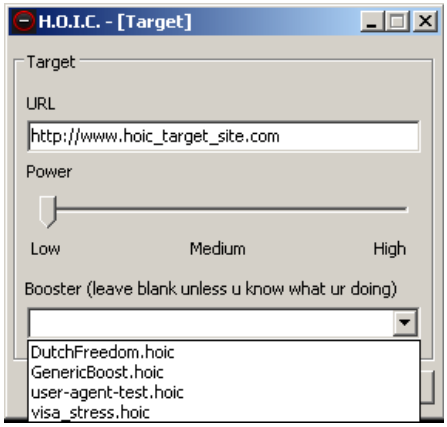



Rysunek 2: Statystyki geolokalizacji źródłowych adresów IP wykorzystujących do ataku oprogramowania LOIC

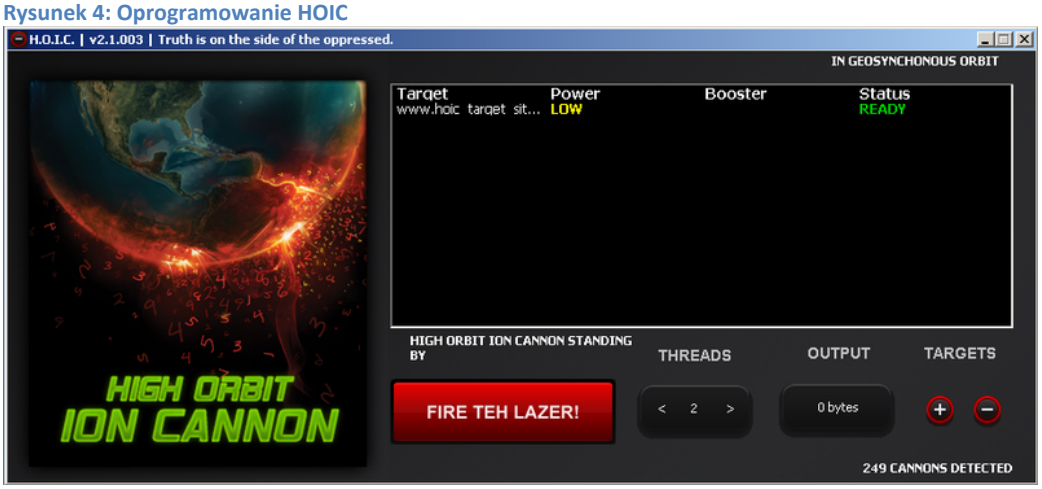



Rysunek 3: Rozkład ataków z terytorium Polski przy wykorzystaniu oprogramowania LOIC

Analiza logów pozwoliła również zidentyfikować wykorzystanie do ataku DDoS narzędzia HOIC (High Orbit Ion Cannon). Oprogramowanie powstało na platformę Windows i jego działanie jest zbliżone do działania jego poprzednika LOIC-a.




Rysunek 4: Oprogramowanie HOIC




Rysunek 5: Oprogramowanie HOIC

Różnica polega na możliwości wykorzystania do ataku tzw. „boosterów” – czyli plików konfiguracyjnych pozwalających na modyfikacje nagłówków wysyłanych zapytań HTTP oraz możliwości konfiguracji natężenia generowanego ruchu HTTP po przez uruchomienie zadanej ilości wątków. W wyniku podjętych działań przechwycono kilka plików konfiguracyjnych wykorzystywanych do ataków na polskie strony rządowe co pozwoliło na identyfikację zapytań w logach serwerów WWW.

Przykład pliku konfiguracyjnego:

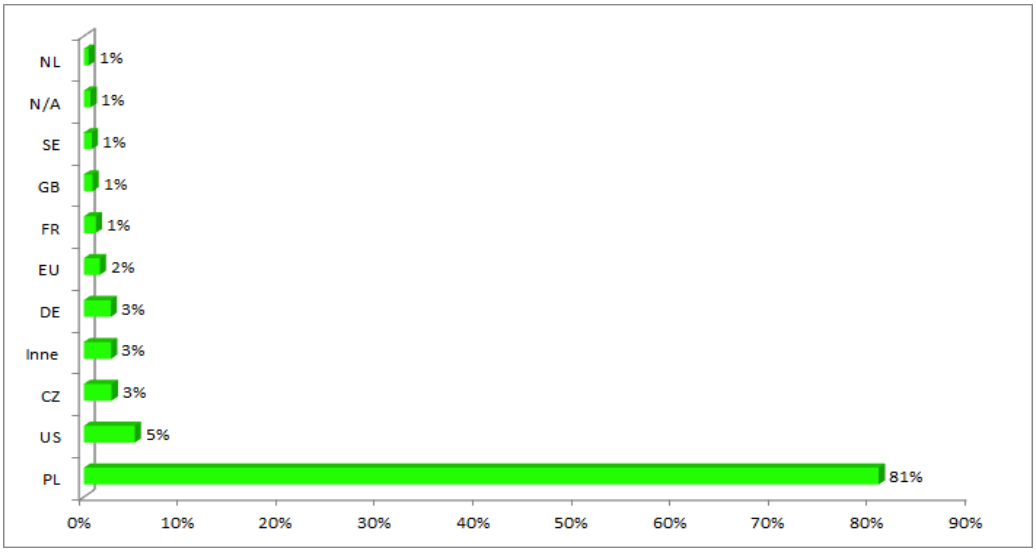
```
// populate rotating urls
randURLs.Append "http://www.xxxx.gov.pl/"
...
// rotate out url
URL =  randURLs(RndNumber(0, randURLs.UBound))

// populate list
useragents.Append "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)"
useragents.Append "Mozilla/4.0 (compatible; MSIE 5.0; Windows NT 5.1; .NET CLR 1.1.4322)"
useragents.Append "Googlebot/2.1 ( http://www.googlebot.com/bot.html) "
...

// Add random headers
randheaders.Append "Cache-Control: no-cache"
randheaders.Append "If-Modified-Since: Sat, 29 Oct 1994 11:59:59 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Sep 2002 10:34:27 GMT"
randheaders.Append "If-Modified-Since: Mon, 12 Aug 2004 12:54:49 GMT"
randheaders.Append "If-Modified-Since: Wed, 30 Jan 2000 01:21:09 GMT"
randheaders.Append "If-Modified-Since: Tue, 18 Aug 2006 08:49:15 GMT"
```

```
// generate random referer
Headers.Append "Referer: " + referers(RndNumber(0, referers.UBound))
// generate random user agent (DO NOT MODIFY THIS LINE)
Headers.Append "User-Agent: " + useragents(RndNumber(0, useragents.UBound))
// Generate random headers
Headers.Append randheaders(RndNumber(0, randheaders.UBound))
```

Kolejnym zaobserwowanym rodzajem ataków DDoS to atak przy wykorzystaniu narzędzi w postaci „hping", polegający na wysyłaniu dużej ilości pakietów TCP na port 80 z ustawiona flagą SYN czyli tzw. „SYN Flood". W przypadku dużej ilości zapytań HTTP dochodzi do wysycenia łącza, natomiast w przypadku ataku SY Flood następuje wysycenie zasobów sprzętowych serwera WWW.

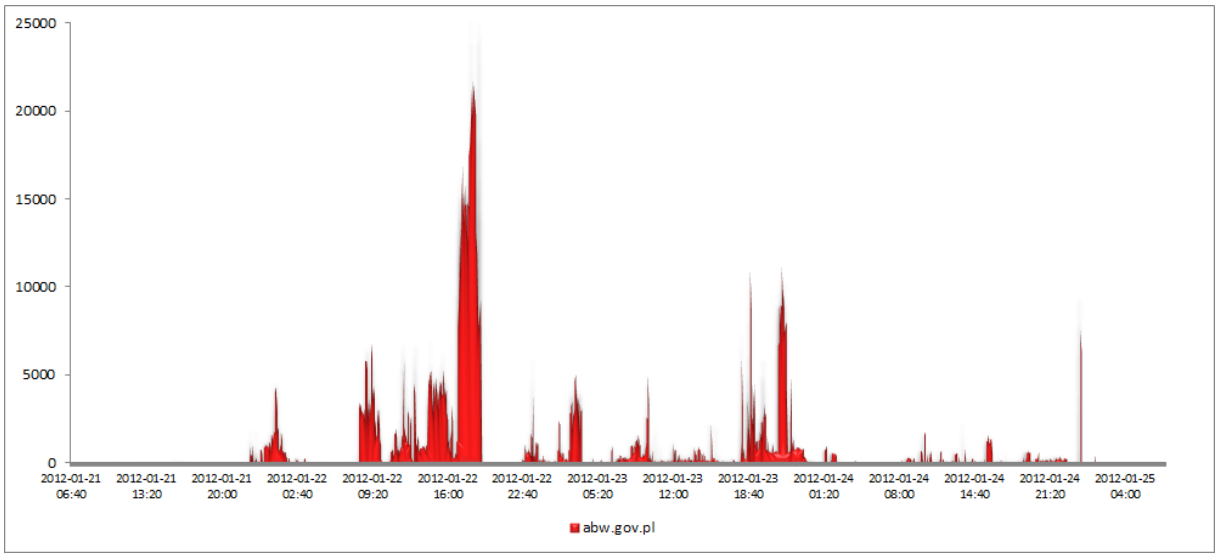
**Ogólne statystyki**

Poniżej przedstawiony został wykres rozkład całkowitego ruchu po względem geolokalizacji źródłowych adresów IP. Należy także dodać, że specyfika protokołu TCP/IP sprawia, iż nie można bezpośrednio łączyć źródła pochodzenia pakietów z rzeczywistą lokalizacją zleceniodawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący mogą wykorzystywać serwery pośredniczące (proxy) lub słabo zabezpieczone, bądź nieaktualizowane komputery, nad którymi wcześniej przejmują kontrolę.

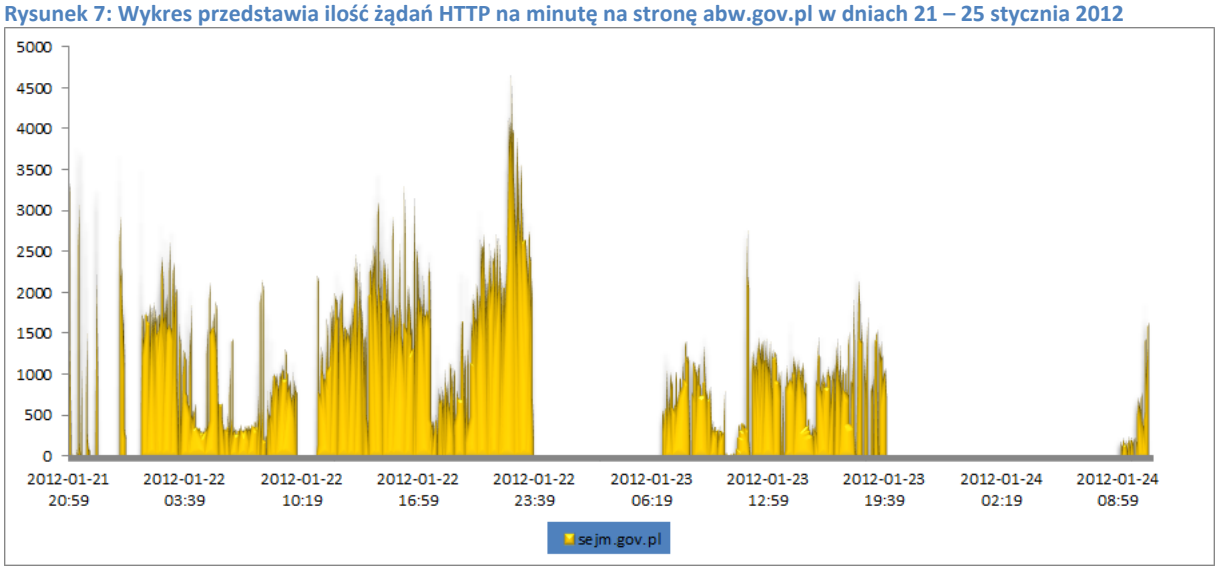



Rysunek 6: Rozkład całkowitego ruchu po względem geolokalizacji źródłowych adresów IP

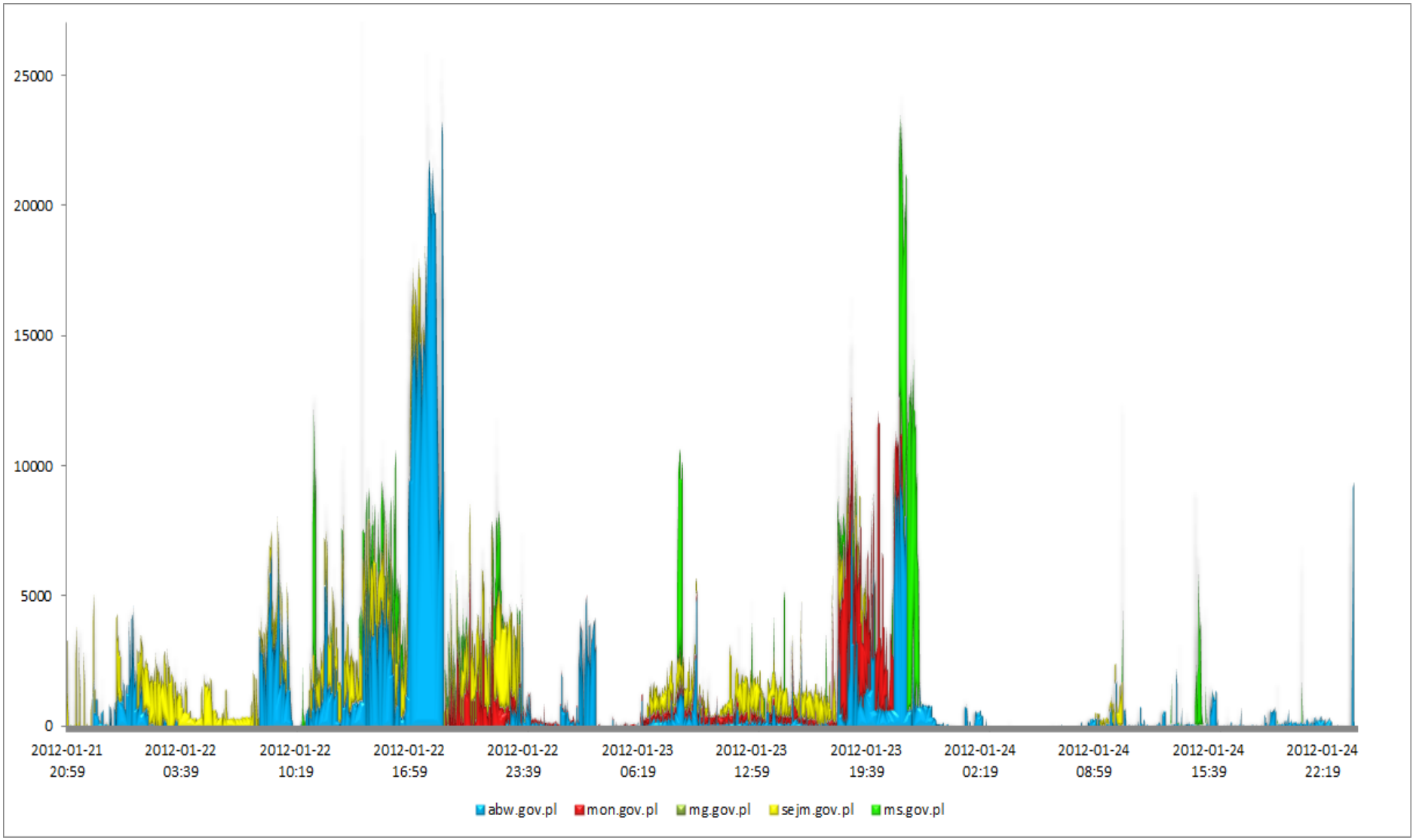
Poniższe wykresy przedstawiają nasilenie ruchu podczas ataku na wybrane strony z domen gov.pl.




**Rysunek 7: Wykres przedstawia ilość żądań HTTP na minutę na stronę abw.gov.pl w dniach 21 – 25 stycznia 2012**




**Rysunek 8: Wykres przedstawia ilość żądań HTTP na minutę na stronę sejm.gov.pl w dniach 21 – 25 stycznia 2012**




Rysunek 9: Przebieg ataków na poszczególne strony administracji rządowej (ilość żądań HTTP/min)