STUDIA INFORMATICA 2011
Volume 32 Number 3A (98)

Krzysztof LASOTA, Adam KOZAKIEWICZ
Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych
Naukowa i Akademicka Sieć Komputerowa

ANALIZA PODOBIEŃSTW ZŁOŚLIWYCH NAZW DOMENOWYCH

Streszczenie. W artykule przedstawiono wyniki badań, dotyczące podobieństw w konstrukcji złośliwych domen. Ich celem była weryfikacja postawionej tezy, iż pomiędzy złośliwymi nazwami domenowymi występują podobieństwa w budowie, znacząco różne od podobieństw występujących pomiędzy zwykłymi nazwami domenowymi.

Słowa kluczowe: złośliwe domeny, heurystyczne metody detekcji, detekcja phishingu

ANALYSIS OF SIMILARITIES IN MALICIOUS DOMAIN NAMES

Summary. The paper presents research results on similarities in structure of malicious domain names. The purpose of research was to verify the argument: Among malicious domain names the similarities in structure are significantly different from the similarities in structure among benign domain names.

Keywords: malicious domains, heuristic detection methods, phishing detection

1. Wprowadzenie

Ogromna liczba znanych niebezpieczeństw oraz ciągle pojawiające się nowe ataki wpływają na bezpieczeństwo użytkowników Internetu i ich maszyn. Rosnąca liczba ataków korzystających z infrastruktury sieci WWW, a co za tym idzie powszechne wykorzystanie systemu DNS, uświadamia potrzebę opracowania szybkich metod wspomagających proces detekcji niebezpiecznych incydentów, opartych na nazwach domenowych. Złożone systemy wyszukujące klienckie zagrożenia w sieci Internet, np.: klienckie honeypoty, ze względu na wysoki stopień skomplikowania, są stosunkowo powolne. Jednak szybsze systemy oparte są wyłącznie na sygnaturach, co skutkuje wykrywaniem tylko znanych wcześniej niebezpieczeństw.

Dotychczasowe badania dotyczące złośliwych nazw domenowych jedynie naświetliły statystyczne różnice występujące pomiędzy leksykalnymi własnościami zwykłych i złośliwych nazw domenowych. Ich główny nacisk został położony na analizę informacji kontekstowych, pobranych z publicznie dostępnych serwisów, a opartych na nazwach domenowych.

2. Istniejące rozwiązania

Podczas pracy koncepcyjnej zostało zbadanych wiele rozwiązań służących do detekcji zagrożeń w sieci Internet. Szczególną uwagę zwrócono na systemy umożliwiające detekcję zagrożeń sieciowych, korzystających z usługi translacji adresów: Google Safe Browsing [3], DNS Blackholing [2] oraz klienckie honeypoty [5, 6, 7].

Metody heurystyczne, mimo że nie zawsze wskazują poprawne wyniki, w dużym stopniu upraszczają proces detekcji. Heurystyki ograniczają zbiór danych wejściowych do ilości umożliwiającej efektywne przetwarzanie. Rodzinę metod heurystycznych, wykrywających niebezpieczne nazwy domenowe (głównie strony phishingowe) można podzielić na dwie grupy. Pierwsza, wykorzystuje dodatkowe informacje z publicznie dostępnych usług (DNS, WHOIS, geolokalizacja), a druga – własności leksykalne domeny. Prowadzone badania mają na celu stworzenie dodatkowej cechy: opartej na podobieństwie do złośliwych nazw domenowych i zawartej w drugim z wymienionych zbiorów. Inne własności wykorzystywane jako cechy leksykalne [10, 11] w metodach heurystycznych to przede wszystkim:

- długość nazwy mnemonicznej domeny – średnia długość złośliwej nazwy mnemonicznej jest krótsza od zwykłej nazwy domenowej,
- liczba kropek – statystycznie budowa złośliwej domeny jest bardziej złożona od zwykłej nazwy domenowej,
- wystąpienie słowa kluczowego – określa czy w nazwie domeny znajduje się określony podciąg znaków (wykorzystywane głównie do wykrywania phishingu),
- prawdopodobieństwo wystąpienia znaku – analogicznie do różnych języków, korzystających z identycznego alfabetu, również zbiory złośliwe mają różny rozkład prawdopodobieństwa występowania poszczególnych znaków względem nazw domenowych, korzystających z tego samego alfabetu,
- liczba różnych znaków w nazwie domeny – statystycznie liczba różnych znaków występujących w złośliwej nazwie mnemonicznej jest mniejsza niż w zwykłej.

3. Analizowane zbiory

Na potrzeby przeprowadzonych badań wykorzystano dwa publicznie dostępne zbiory danych. Pierwszy zbiór zawierał nazwy domen złośliwych, wykorzystywanych w projekcie DNS Blackholing [2]. Na początku października 2010 roku zawierał on około 10 tysięcy złośliwych wpisów i w dalszej części tekstu będzie oznaczany jako DNS-BH. Dodatkowe 5 tysięcy nazw domenowych z tego samego źródła, niewystępujących w zbiorze DNS-BH, a dodanych w późniejszym okresie oznaczono jako DNS-BH2.

Drugi zbiór zawierał dane zawarte w milionie najpopularniejszych adresów URL [1]. Wyodrębnione, unikalne nazwy mnemoniczne – w przytłaczającej większości niezłośliwe – miały na celu zobrazowanie tendencji w nazewnictwie stosowanym w dzisiejszej sieci. W październiku 2010 roku zbiór zawierał około 950 tysięcy niepowtarzalnych nazw mnemonicznych i w dalszej części tekstu będzie oznaczony jako Top-URL. Brakujące 50 tysięcy adresów to w dużej mierze adresy odwołujące się do hosta przez adres IP, jak również adresy różniące się tylko i wyłącznie ścieżką.

W celu zaprezentowania, w jaki sposób rozpatrywana jest nazwa domenowa, jak również na potrzeby przedstawienia terminologii używanej w dalszej części tekstu posłużono się przykładem: exam.ple.edu.pl. Domena składa się z domeny najwyższego poziomu TLD – pl, oraz 3 subdomen – exam, ple, edu. W związku z tym, że polityki rejestracji domen u operatorów różnią się pomiędzy sobą wprowadzono dwa dodatkowe pojęcia:

- domena właściwa – termin jest równoznaczny z subdomeną najwyższego poziomu, na którą ma wpływ osoba rejestrująca domenę, w przykładzie jest to subdomena ‘ple’;
- właściwe TLD – oprócz domeny najwyższego poziomu zawiera również wszystkie subdomeny zarezerwowane przez instytucję rejestrującą domeny w danym TLD, w przykładzie jest to ‘edu.pl’.

4. Wstępne analizy

Pierwsze badanie miało na celu sprawdzenie, jak mocno nazwy domenowe są do siebie podobne. Na podstawie ręcznej analizy zbiorów oraz znalezionych analogii w tworzeniu nazw domenowych przyjęto, iż domena X jest podobna do domeny Y, jeśli:

- obie są zarejestrowane poniżej tego samego właściwego TLD oraz odległość Levenshteina pomiędzy ich domenami właściwymi jest większa od zera oraz mniejsza niż część całkowita z pierwiastka liczby znaków porównywanej domeny X,
- domeny właściwe są tożsame, ale zostały zarejestrowane w innych właściwych TLD.

Tabela 1

Podobieństwa pomiędzy zbiorami nazw domenowych

Zbiór I	Liczba domen	Zbiór II	Liczba domen	Podobne
Top-URL	5000	Top-URL	1000000	52%
Top-URL	15000	Top-URL	15000	4%
DNS-BH	10000	DNS-BH	10000	16%

W tabeli 1 przedstawiono wyniki określające, jaki procent domen z pierwszego zbioru ma przynajmniej jedną domenę podobną w zbiorze drugim. W pierwszym wierszu przedstawiono średnie wyniki 5 tysięcy losowych domen, porównanych względem całego zbioru Top-URL. Drugi, prezentuje średni wynik dla 15 tysięcy losowych domen Top-URL, porównanych względem tego samego zbioru wylosowanych nazw. Ostatni wiersz zawiera wyniki dla zbioru DNS-BH, również porównanych względem siebie. Badania potwierdziły przypuszczenia, że podobieństwo jest bardzo ogólną własnością. Jednakże wyniki pokazują, że w przypadku małych zbiorów podobieństwo między złośliwymi domenami jest kilkakrotnie wyższe niż w przypadku zwykłych domen.

5. Zaproponowane analizy

Mając na uwadze wyniki otrzymane podczas wstępnych badań dotyczących występowania podobieństw w budowie niebezpiecznych nazw domenowych, jak również już wykorzystywane własności leksykalne nazwy domenowej zaproponowano przeprowadzenie następujących analiz.

1. Wystąpień znaków – oznaczona jako CharP; bierze ona pod uwagę wszystkie nazwy domenowe zawarte w analizowanym zbiorze i dla każdej z nich wylicza wystąpienia znaków pojedynczych, par oraz trójek występujących w domenie właściwej.
2. Miary niedopasowania – oznaczona jako MM; bazuje na wynikach otrzymanych podczas wstępnych analiz korelacji zbiorów. Analiza opiera się na odległości edycyjnej (Levenshteina – LEV, Damerau-Levenshteina – DAM), gdzie miara niedopasowania pomiędzy analizowanymi właściwymi domenami, zarejestrowanymi w tym samym, właściwym TLD, jest mniejsza niż zadana wartość graniczna. Na podstawie znalezionych podobieństw pomiędzy nazwami mnemonicznymi tworzone są tak zwane schematy podobieństwa, opisujące znalezioną własność. Dodatkowo, dla utworzonego schematu sprawdzane jest, czy w analizowanym zbiorze istnieje trzecia nazwa domenowa, która jest opisana przez ów schemat (LEV3, DAM3).

3. Wystąpień różnic – oznaczona jako CharD; badanie jest specyficznym połączeniem analizy miary niedopasowania oraz analizy wystąpień znaków. Ma ona na celu wyliczenie prawdopodobieństwa konkretnych działań na znakach – dostępnych przez poszczególne miary niedopasowania – dla podobnych konstrukcji nazw domenowych.

Wysunięte propozycje można podzielić na dwie grupy. Do pierwszej należy zaliczyć rozszerzenia już zdefiniowanych i wykorzystywanych własności leksykalnych (CharP). Druga zawiera własne propozycje analiz (MM, CharD), mogących wesprzeć metody wykrywania niebezpiecznych incydentów w sieci.

6. Wyniki zaproponowanych analiz

Rezultaty otrzymano na podstawie analizy zbiorów nazw domenowych, opisanych w rozdziale 3. We wszystkich przeprowadzonych badaniach wykorzystywany był cały zbiór DNS-BH. Dodatkowo, analiza CharP wykorzystywała 40 tysięcy najpopularniejszych nazw domenowych ze zbioru Top-URL, natomiast CharD zbiór o połowę mniejszy – 20 tysięcy.

Dodatkowo, na podstawie otrzymanych wyników zaprezentowano przykładowe metody, mogące wspomóc detekcję złośliwych nazw domenowych. Szczególną uwagę zwrócono na rezultaty otrzymane w dwóch przeprowadzonych analizach: wystąpienia znaków (CharP) oraz miary niedopasowania (MM).

6.1. Analiza wystąpień znaków

Najważniejszym wynikiem zaproponowanej analizy są prawdopodobieństwa wystąpień poszczególnych grup znaków. Uzyskane dane pozwoliły na wyliczenie charakterystyk dla wystąpień poszczególnych grup znaków. Charakterystyki uzyskano na podstawie różnic prawdopodobieństwa wystąpienia w zbiorach – zwykłym oraz złośliwym. Sposób przetrzymywania otrzymanych danych pozwala również łatwo wyliczyć charakterystyki wystąpień poszczególnych grup znaków, w zależności od rozpatrywanej długości domeny właściwej.

Zaproponowane sposoby detekcji wykorzystują różnice w prawdopodobieństwie wystąpienia tych samych znaków w zbiorach zwykłym i złośliwym. Analizowana domena jest uznawana za złośliwą w przypadku, kiedy suma wartości pochodzących z wybranej charakterystyki, odpowiadających wszystkim grupom znaków o określonej długości, występujących w danej domenie właściwej jest mniejsza od zera.

W tabeli 2 zaprezentowano wyniki detekcji złośliwych nazw domenowych w zbiorach – DNS-BH oraz Top-URL dla metod opartych na analizie wystąpień znaków. Nazwy metod detekcji mają odniesienia do wykorzystywanych charakterystyk: liczby znaków (1 – pojedynczy,

2 – para oraz 3 – trójka znaków) oraz informację o tym, czy wykorzystywana charakterystyka powstała na podstawie wszystkich przeanalizowanych domen czy na podstawie domen tej samej długości, co sprawdzana domena (L).

Tabela 2

Wyniki detekcji złośliwych nazw domenowych w zbiorach – DNS-BH oraz Top-URL dla metod opartych na analizie wystąpień znaków

Metoda detekcji	Domeny złośliwe		Metoda detekcji	Domeny złośliwe	
	DNS-BH	Top-URL		DNS-BH	Top-URL
CharP-1	9,2%	5,5%	CharP-1L	20,1%	10,9%
CharP-2	28,9%	13,5%	CharP-2L	49,9%	16,0%
CharP-3	54,0%	20,2%	CharP-3L	82,8%	15,4%
CharP-2+3	24,7%	5,8%	CharP-2L+3L	48,3%	6,2%

Porównując otrzymane wyniki można zauważyć, że zastosowanie różnych charakterystyk dla domen o różnej długości przynosi prawie dwukrotny wzrost wykrywalności złośliwych nazw mnemonicznych. Dodatkowo należy zwrócić uwagę na poziom niepoprawnych wskazań w zbiorze zwykłych domen, który również ulega zmianie. Mając na uwadze wciąż wysoki poziom niepoprawnych wskazań w zwykłym zbiorze danych, zaproponowano dwie kolejne metody detekcji – CharP-2+3 oraz CharP-2L+3L. Miały one obniżyć stopień złych wskazań poprzez nałożenie dodatkowego warunku mówiącego, że aby domena została uznana za złośliwą, obie metody składowe również mają uznać nazwę domenową za złośliwą.

Dodatkowym atutem prezentowanej metody jej szybkość klasyfikacji. Dla najwolniej działających przypadków (CharP-2L+3L oraz CharP-2+3) zaproponowana metoda potrafiła sklasyfikować około 50 nazw domenowych na sekundę, co jest zadowalającym wynikiem.

6.2. Analiza miary niedopasowania

Głównym, otrzymanym rezultatem przeprowadzonego badania są schematy opisujące znalezione podobieństwa w konstrukcji niebezpiecznych nazw mnemonicznych, opartych na odległościach Levenshteina (LEV, LEV3) oraz Damerau-Levenshteina (DAM, DAM3).

Kolejne iteracje badania przeprowadzono dla maksymalnej wartości granicznej miary niedopasowania, równej 1, 2 oraz 3. Uzależniono je również od minimalnej długości właściwych domen, dla których szukane było podobieństwo. Doprowadziły one do wyznaczenia metody detekcji charakteryzującej się niską stopą błędnych wskazań w zbiorze zwykłych nazw mnemonicznych.

W tabeli 3 znajdują się rezultaty dla zasugerowanej metody detekcji, opartej na analizie wyników analizy miary niedopasowania MM. Zaproponowane metody wykorzystują schematy prawdopodobieństwa, uzyskane w trzech iteracjach:

- LEV-1, DAM-1, LEV3-1, DAM3-1 – maksymalna wartość miary niedopasowania nie jest większa od 1,
- LEV-2-7, DAM-2-7, LEV3-2-7, DAM3-2-7 – maksymalna wartość miary niedopasowania nie jest większa od 2, dla właściwych domen nie krótszych niż 7 znaków,
- LEV-3-14, DAM-3-14, LEV3-3-14, DAM3-3-14 – maksymalna wartość niedopasowania nie jest większa od 3, dla właściwych domen nie krótszych niż 14 znaków.

Tabela 3

Wyniki detekcji złośliwych nazw domenowych zaproponowanych metod w dwóch zbiorach (DNS-BH2 oraz Top-URL)

Oznaczenia analiz	LEV-1+LEV-2-7+LEV-3-14 DAM-1+DAM-2-7+DAM-3-14	LEV3-1+LEV3-2-7+LEV3-3-14 DAM3-1+DAM3-2-7+DAM3-3-14
% domen z Top-URL	0,02	0,01
% domen z DNS-BH2	0,42	0,33

Kolejnym atutem prezentowanej metody jest jej szybkość klasyfikacji. Ze względu na rozróżnienie, czy wykorzystywany był wygenerowany zbiór schematów podobieństwa bez potwierdzenia (LEV-1+LEV-2-7+LEV-3-14, DAM-1+DAM-2-7+DAM-3-14) czy też z potwierdzeniem (LEV3-1+LEV3-2-7+LEV3-3-14, DAM3-1+DAM3-2-7+DAM3-3-14) metoda klasyfikowała około 227 nazw domenowych na sekundę, w pierwszym przypadku oraz aż 625 na sekundę w drugim, co jest wynikiem przynajmniej dobrym.

6.3. Analiza wystąpień różnic

Głównym wynikiem przeprowadzonych analiz są obliczone prawdopodobieństwa występowania działań dokonywanych na konkretnych znakach. W tabeli 4 zaprezentowano procentowy udział wykorzystywanych działań w wynikach analiz przeprowadzonych na obydwu zbiorach. Ponadto, dla poszczególnych działań dokonano rozróżnienia znaków, na jakich przeprowadzono dostępne działania. Wyszczególniony trzy grupy znaków – *litery*, *cyfry* oraz *inne*. Zbiór inne w przypadku dodania lub usunięcia znaku zawierał jedynie znak myślnika, natomiast w sytuacji, kiedy operacja zachodziła pomiędzy dwoma znakami (wymiana, zamiana), zbiór kumuluje wszystkie operacje zachodzące pomiędzy znakami nienależącymi do tego samego zbioru (np.: {a,1}, {-,6}). Jak widać pomiędzy zbiorami istnieje duże zróżnicowanie zarówno wykonywanych działań, jak i udziału zdefiniowanych zbiorów znaków w tych działaniach. W przypadku zbioru złośliwego aż 51% operacji było wykonanych wyłącznie na cyfrach, przy 9% w Top-URL.

Tabela 4
Udział wykorzystywanych działań na zbiorach znaków (Cyfry, Litery, Inne (-)) w wynikach analizy występowania różnic na zbiorach DNS-BH oraz Top-URL

Top-URL				
	+/-	Wymiana	Zamiana	Suma
Cyfry	4,27%	4,79%	0,09%	~9,15%
Litery	22,99%	58,29%	0,94%	~82,22%
Inne	0,51%	8,12%	0,00%	~8,63%
Suma	~27,78%	~71,20%	~1,03%	100%
DNS-BH				
	+/-	Wymiana	Zamiana	Suma
Cyfry	4,12%	47,24%	0,14%	~51,51%
Litery	1,32%	40,31%	0,50%	~42,13%
Inne	0,60%	5,62%	0,14%	~6,36%
Suma	~6,04%	~93,17%	~0,78%	100%

7. Podsumowanie

Przeprowadzone badania potwierdziły występowanie podobieństw w budowie złośliwych nazw domenowych. Zaproponowana, wstępna analiza wykazała, iż około 16% badanych złośliwych nazw domenowych można uznać za podobne do przynajmniej jednej innej domeny. Ponadto, rezultaty otrzymane przez dwie kolejne analizy – wystąpień znaków oraz wystąpień różnic – wykazały, iż konstrukcja domen złośliwych znacząco różni się od zwykłych. Pierwsza z nich, CharP, oparta została na prawdopodobieństwie grup znaków używanych do konstrukcji nazw domenowych. Druga (CharD) pozwoliła zaobserwować różnice w budowie podobnych nazw domenowych w zbiorach złośliwym i zwykłym.

Ponadto, na podstawie otrzymanych wyników analiz wystąpień znaków oraz miary niedopasowania zaproponowano przykładowe metody detekcji złośliwych nazw mnemonicznych. Nawet najwolniejsze z zaproponowanych metod – 50 domen/s w przypadku CharP oraz 227 dla MM – są i tak o co najmniej jeden rząd wielkości szybsze od złożonych systemów detekcji. Wydajniejsze, niskointeraktywne, klienckie honeypoty mogą się poszczycić wynikami rzędu 6,3 sekund na URL [13]. Ze względu na ogromną ilość wysyłanych wiadomości SPAM, a w związku z tym ogromnej liczby zawartych w nich różnych adresów URL do sprawdzenia, jak również z faktu krótkiego czasu życia złośliwych nazw domenowych zaproponowane metody doskonale nadają się na filtr danych wejściowych złożonych systemów

detekcji. Ponadto, dzięki bardzo dużej wydajności, a także umiarkowanej stopie błędów, wyniki miary niedopasowania mogą trafiać niezwłocznie do specjalistów z dziedziny bezpieczeństwa, w celu ręcznej, jeszcze dokładniejszej analizy niebezpiecznych incydentów. Użycie tych metod jako niezależnych automatycznych klasyfikatorów jest jednak niewskazane, choć może być stosowane, np. przez rejestratorów nazw mnemonicznych, w celu zwrócenia uwagi na podejrzane nowe nazwy domenowe.

Dodatkowo, wyniki analizy wystąpień różnic wskazały kierunek dalszych badań, które powinny zostać przeprowadzone, w celu uzyskania jeszcze dokładniejszych metod detekcji złośliwych nazw domenowych.

BIBLIOGRAFIA

1. Alexa, Top million sites, http://http://www.alexa.com/.
2. DNS Blackholing, http:// http://www.malwaredomains.com/.
3. Google Safe Browning, http://code.google.com/p/google-safe-browsing/.
4. Gusfield D.: Algorithms on strings, trees, and sequences: computer science and computational biology. Cambridge University Press, New York, 1997.
5. HoneySpider Network Project, http://www.honeyspider.net/.
6. The Honeynet Project, Capture-HPC, https://projects.honeynet.org/capturehpc.
7. Ikinci A., Holz T., Freiling F.: Monkey-Spider: Detecting Malicious Websites with Low-Interaction Honeyclients. University of Mannheim, 2008.
8. Kolari P., Finin T., Joshi A.: SVMs for the Blogosphere: Blog Identification and Splog Detection. Proceedings of the AAAI Spring Symposium on Computational Approaches to Analysing Weblogs, Stanford, 2006.
9. Lasota K., Kozakiewicz A.: Monitorowanie ruchu HTTP pod kątem występowania złośliwych adresów URL. KSTiT'2010, Wrocław – Przegląd Telekomunikacyjny, nr. 8/9/2010, s. 1325÷1332.
10. Ma J., Saul L. K., Savage S., Voelker G. M.: Beyond Blacklists: Learning to Detect Malicious Web Sites from Suspicious URLs. Proceedings of the SIGKDD Conference, Paris 2009.
11. McGrath D. K., Gupta M.: Behind Phishing: An Examination of Phisher Modi Operandi. Proc. of the USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET), San Francisco 2008.
12. Public Suffix List, http://publicsuffix.org/.
13. Seifert C., Welch I., Komisarczuk P.: HoneyC – The Low-Interaction Client Honeypot. 2006.

Recenzenci: Dr inż. Piotr Pikiewicz
Dr inż. Mirosław Skrzewski

Wpłynęło do Redakcji 11 marca 2011 r.

Abstract

The paper presents research results on similarities in structure of malicious domain names. The purpose of research was to verify the argument: Among malicious domain names the similarities in structure are significantly different from the similarities in structure among benign domain names.

The practical research part of the paper begins with presentation of the primary research results (Table 1) on which the analysis methods used to verify the thesis were developed. Paper presents three proposed methods: occurring of characters (CharP), measurement mismatch (MM) and occurring of differences (CharD). The results obtained with prototype tool were used to form new methods, potentially aiding the detection process of malicious domain names. The effectiveness of the methods was verified (Table 3 and Table 4) for potential practical application in more complex systems detecting malicious content on the Internet. In addition, results of the analysis CharD (Table 4) indicated the direction of further research that should be done to obtain more accurate methods for detection of malicious domain names.

Adresy

Krzysztof LASOTA: Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych, ul. Nowowiejska 15/19, 00-665 Warszawa, Polska, klasota@mion.elka.pw.edu.pl; Naukowa i Akademicka Sieć Komputerowa, ul. Wąwozowa 18, 02-796 Warszawa, Polska, krzysztof.lasota@nask.pl

Adam KOZAKIEWICZ: Politechnika Warszawska, Wydział Elektroniki i Technik Informacyjnych, ul. Nowowiejska 15/19, 00-665 Warszawa, Polska, akozakie@elka.pw.edu.pl; Naukowa i Akademicka Sieć Komputerowa, ul. Wąwozowa 18, 02-796 Warszawa, Polska, adam.kozakiewicz@nask.pl