



# **Ataki na serwery Domain Name System (DNS Cache Poisoning)**

Jacek Gawrych  
semestr 9

Teleinformatyka i Zarządzanie w Telekomunikacji

[jgawrych@elka.pw.edu.pl](mailto:jgawrych@elka.pw.edu.pl)

# Plan prezentacji

- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?
- Pytania

# Phishing -> Pharming



## •Phishing -> Pharming

- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Phishing – termin powstały ok. 10 lat temu
- Pierwsze przypadki – America Online (AOL)
- Pharming – dużo poważniejsza forma phishingu
- Główne przejawy przy podrabianiu serwisów WWW związanych z płatnościami elektronicznymi

# Atak na DNS – spojrzenie ze strony klienta



•Phishing -> Pharming

•Atak na DNS –  
spojrzenie ze strony  
klienta

•Co można osiągnąć  
zatruciem serwera  
DNS?

•Atak na DNS –  
spojrzenie ze strony  
atakującego

•Podatność  
istniejącego  
oprogramowania DNS

•Jak się bronić?

•Polecenie połączenia z maszyną na podstawie nazwy domenowej (np. [www.mbank.com.pl](http://www.mbank.com.pl))

•Skierowanie do usługi bliźniaczo podobnej, jednak zarządzanej przez zupełnie inny podmiot

•Wyrządzenie szkody klientowi

# Co można osiągnąć zatruciem serwera DNS?



## •WWW

- Kradzież danych podczas płatności
- Skompromitowanie instytucji
- Przejęcie klientów instytucji
- Zmylenie użytkowników poszukujących informacji w sieci

## •FTP

- Przejęcie danych wysyłanych do serwera
- Pobranie zainfekowanego oprogramowania
- Pobranie zainfekowanych aktualizacji oprogramowania

•Phishing -> Pharming

•Atak na DNS –  
spojrzenie ze strony  
klienta

•Co można osiągnąć  
zatruciem serwera  
DNS?

•Atak na DNS –  
spojrzenie ze strony  
atakującego

•Podatność  
istniejącego  
oprogramowania DNS

•Jak się bronić?

# Atak na DNS – spojrzenie ze strony atakującego



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Protokół DNS
- Słabość protokołu DNS
- Wykorzystanie słabości
  - Atak klasyczny
  - Zmodyfikowany atak klasyczny
  - Atak dnia narodzin

# Protokół DNS



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Początki – plik hosts.txt
- Obecnie – rozproszona baza danych
- Resolver – klient DNS
- Przechowywanie odpowiedzi w Cache
- Najczęściej – żądanie od najbliższego serwera DNS rozwiązania podanego adresu domenowego na adres IP -> najbliższy serwer DNS zdobywa żądane informacje i zwraca klientowi

# Protokół DNS



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Oparty na UDP
- Format zapytania: adres źródłowy, port źródłowy, adres docelowy, port docelowy (53), żądany adres do rozwiązania, 16-bitowy znacznik żądania (1-65535)
- Format odpowiedzi: adresy/porty docelowe/źródłowe, rozwiązany adres, ten sam znacznik, dodatkowe informacje (czas aktualności odpowiedzi, inne serwery)

# Słabość protokołu DNS



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Znacznik TYLKO 16-bitowy!!!
- Można podać sfałszowaną odpowiedź, zatruwając tym jego pamięć Cache serwera bądź resolvera

# Atak klasyczny



- Phishing -> Pharming

- Atak na DNS –  
spojrzenie ze strony  
klienta

- Co można osiągnąć  
zatruciem serwera  
DNS?

- Atak na DNS –  
spojrzenie ze strony  
atakującego

- Podatność  
istniejącego  
oprogramowania DNS

- Jak się bronić?

- Wysłanie 1 zapytania klient-serwer
- Podrobienie odpowiedzi serwer-serwer poprzez podanie serii pakietów zawierających sfałszowaną odpowiedź, różniących się tylko znacznikiem
- Prawdopodobieństwo sukcesu:  
 $P = n / 65535$  (n – liczba różnych pakietów)
- Przy 65535 pakietach 100-bajtowych przesyłanych jest ok. 50 Mb, co w sieciach 100 Mbit/s może zająć ok. 1 SEKUNDĘ

# Zmodyfikowany atak klasyczny



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Przesyłanie w pętli do serwera/resolvera pakietów podrabiających odpowiedź DNS i oczekiwanie aż zastąpią te oczekiwane
- Wystarcza znacznie mniejsza liczba pakietów (np. 1000 a nie ponad 60000)
- Potrafi być skuteczniejszy niż atak klasyczny

# Atak dnia narodzin



•Phishing -> Pharming

•Atak na DNS –  
spojrzenie ze strony  
klienta

•Co można osiągnąć  
zatruciem serwera  
DNS?

•Atak na DNS –  
spojrzenie ze strony  
atakującego

•Podatność  
istniejącego  
oprogramowania DNS

•Jak się bronić?

•U podstaw paradoks dnia narodzin

•Wysłanie wielu zapytań klient-serwer i  
takiej samej liczby odpowiedzi serwer-  
serwer

$$P = 1 - \left(1 - \frac{1}{65535}\right)^{\frac{n(n-1)}{2}}$$

• $P > 1/2$  przy  $n = 302$

•Przy  $n = 700$   $P = 0,97608$  (dla takiego  $n$   
przy ataku klasycznym  $P = 0,01068$ )

# Podatność istniejącego oprogramowania DNS



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- BIND 8 i BIND 9
- djbdns
- Resolvery Windows 2000 i Windows XP

# BIND 8 i BIND 9



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Berkeley Internet Name Domain
- Akceptują każdą odpowiedź wysłaną na port 53
- BIND 9 kolejkuje zapytania, w przeciwieństwie do BIND 8 (atak dnia narodzin niemal niemożliwy, za to osiągnane są rezultaty przy zmodyfikowanym ataku klasycznym)

# djbdns

- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Serwer autorstwa Dana J. Bernsteina, twórcy serwera pocztowego qmail
- Niepodatny na przytoczone techniki
- Generuje losowo numery portów, z których pochodzą zapytania i akceptuje odpowiedzi przychodzące tylko na te porty (inaczej niż BIND)
- Zabrania stosowania serwerów DNS Cache i autorytatywnego DNS na tym samym IP

# Resolvery firmy Microsoft



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

## •Windows 2000

- Losowo generowane numery ID
- 5 zapytań dla 1 informacji
- Numer portu zwiększany o 2

## •Windows XP

- Od momentu restartu DNS, pierwsze żądanie DNS zawsze z portu 1170 o ID=1, potem przy każdym kolejnym pytaniu ID zwiększane o 1

# Jak się bronić?



- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?

- Nie korzystać z usług DNS, przynajmniej przy istotnych działaniach
- Nie Cache'ować odpowiedzi
- Nie używać podatnego oprogramowania
- DNSSEC – uwierzytelnienie w oparciu o PKI, niestety niekompatybilny z DNS, już zaimplementowany w BIND

# Podsumowanie

- Phishing -> Pharming
- Atak na DNS – spojrzenie ze strony klienta
- Co można osiągnąć zatruciem serwera DNS?
- Atak na DNS – spojrzenie ze strony atakującego
- Podatność istniejącego oprogramowania DNS
- Jak się bronić?



**Pytania**