

Wykrywanie i analiza złośliwych stron WWW

Łukasz Juszczyszyn
CERT Polska/NASK
lukasz.juszczyszyn@cert.pl

Agenda

atak → analiza → obrona

techniki i
mechanizmy
ataków

narzędzia,
problemy

sposoby
obrony

Atak

Źródło ataków

- Strony internetowy
 - tworzenie szkodliwych
 - wykorzystanie legalnych

Techniki ataków

- JavaScript/VBScript/HTML
- Wtyczki do przeglądarki
 - Flash
 - Dokumenty PDF
 - RealPlayer
 - ActiveX,
 - Java
- Fastflux

JavaScript/VBScript/HTML

- Tworzenie obiektów ActiveX
- Przekierowania
- Pobieranie *malwaru* z innych serwerów
 - XMLHttpRequest
- Pływające ramki
- Przepełnienia bufora
- Zaciemnienie kodu

Animacje Flash

- Przekierowania
- Błędy w odtwarzaczu (*flash player*)
- Osadzony HTML i kod JavaScript

Dokumenty PDF

- Błędy w czytnikach
 - interpreter języka
- Złożoność formatu
- Osadzony kod JavaScript
 - Shellcode
- Kompresja, kodowanie, szyfrowanie

FastFlux

Sieć skompromitowanych komputerów udostępniających publiczne rekordy DNS

- dla jednej domeny zwracane jest wiele adresów IP
- bardzo częste zmiany adresów
- dystrybucja nielegalnych treści

Analiza

Narzędzia do analizy

- Honeypoty klienckie
 - HSN, Capture, SHELIA, PhoneyC, HoneyC, ...
- Analiza „ręczna”
 - Przeglądarka
 - Narzędzia
 - JavaScript, Flash, PDF

Honeypot

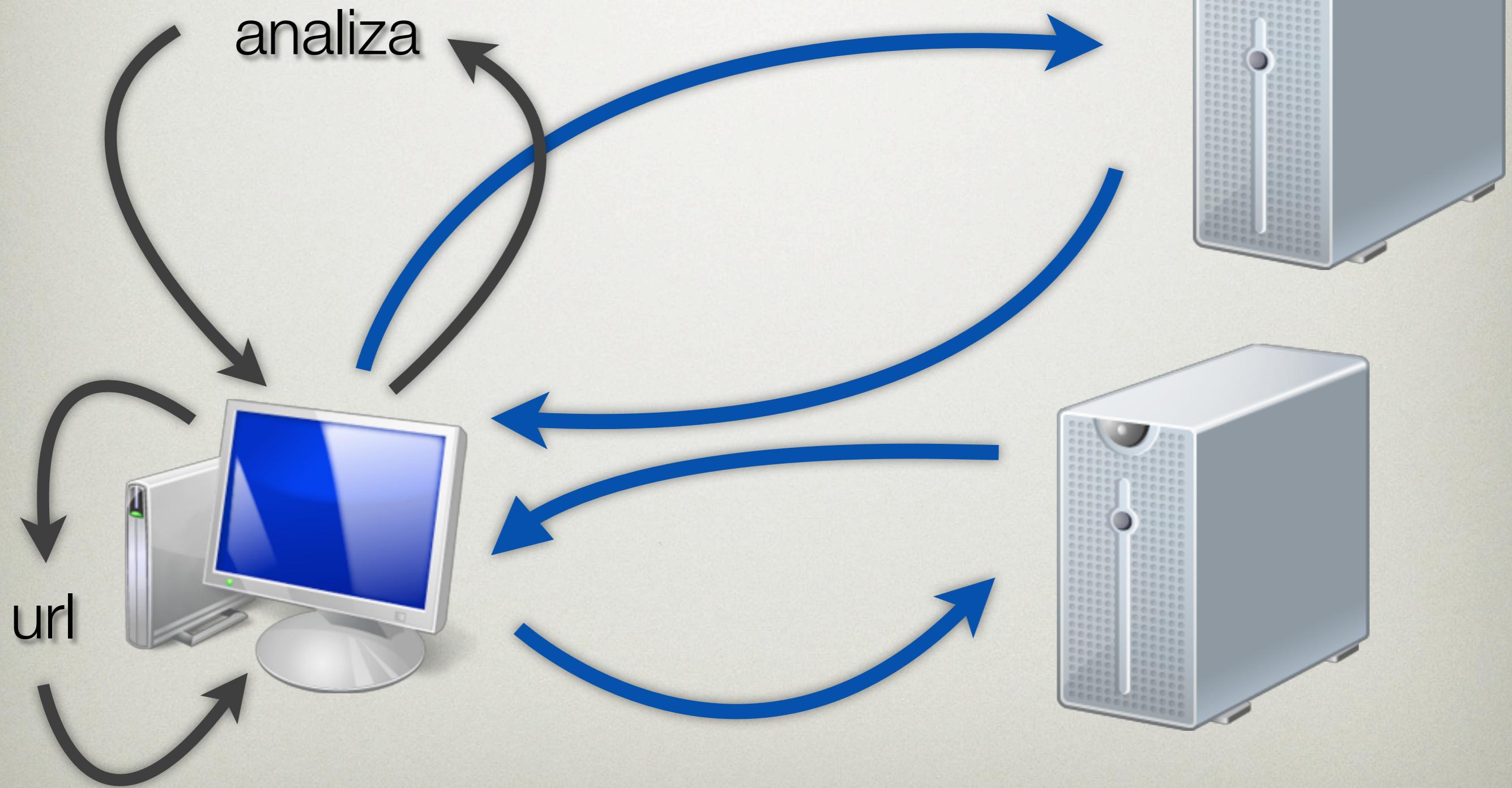
System przygotowany na atak

- zbiera oraz analizuje informacje
- **identyfikacja, zrozumienie oraz ochrona przed incydentami**

Honeypot kliencki

- ataki na podatności klienta
 - przeglądarka, **wtyczki**, OS
- **wyszukuje** złośliwe serwery
- nisko- oraz wysokointeraktywne

Honeypot kliencki



Honeypot niskointeraktywny

- Część aplikacji lub systemu
- Emulacja przeglądarki internetowej, *web crawler*
- Analiza statyczna
 - sygnatury
- Szybki, łatwy we wdrożeniu i utrzymaniu
- Nie wykrywa złożonych ataków

Honeypot wysokointeratywny

- Cały system
 - rzeczywista przeglądarka internetowa
- Pozwala na przeprowadzenie całego ataku
- Wykrywa nieznane ataki
- Wolniejsze działanie, duże obciążenie systemu, złożona konfiguracja

Honeypot hybrydowy

- HoneySpider Network
 - Centrum
 - Moduł niskointeraktywny
 - Moduł wysokointeraktywny

Analiza ręczna

- Przeglądarka internetowa
 - „naturalne” środowisko
 - <textarea>
 - Firebug
- Interpreter JavaScript
 - SpiderMonkey, Rhino
 - tagi HTML, niepożądane funkcje
 - `document.write()` → `print()`

Analiza - narzędzia

- Malzilla
 - *Malware hunting tool*
- wepawet
 - analiza Flash, JavaScript, PDF
- jsunpack
 - wydobywa JavaScript z PDF, Flash
- Firebug
 - dodatek do Firefoksa

Analiza - narzędzia

- pdftk
 - Operacje na PDF-ach
- pdf-parser.py, pdfid.py
 - Struktura PDF
- swftools
 - Analiza Flasha
- flare, flasm
 - Dekompilacja ActionScript
 - Deasemblacja ActionScript

Trudności w analizie

- Zaciemniony kod JavaScript
- VBScript w JavaScript
- DOM przeglądarki
- Utrudnienia twórców
 - Wykrywanie „nieprzeglądarki”
- Zamknięte standardy
- Wydajność narzędzi

Zaciemnianie kodu

```
// Hello World
x1 = unescape('%48%65%6c%6c%6f%20%57%6f%72%6c%64');
x2 = '\x48\x65\x6c\x6c\x6f\x20\x57\x6f\x72\x6c\x64';
x3 = unescape('%48%65%6c' + '%6c%6f' + '%20%57%6f%72%6c%64');
x4 = unescape('%u0048%u0065%u006c%u006c%u006f%u0020%u0057%u006f%u0072%u006c%u0064');
x5 = unescape('%48%65%6c%6c%6f') + unescape('%u0020%u0057%u006f%u0072%u006c%u0064');

var p="%";
p+="u00";
var x6 =
unescape(
'rtyui48rtyui65rtyui6crtysi6frtyui20rtyui57rtyui6frtyui72rtyui6crtysi64'
.replace(/rtyui/ig, p));

var _0xdead=[ "\x48\x62", "\x66\x65\x62", "\x24\x42", "\x62\x65\x65\x66"];
var _0xbeef=[ "\x48\x65\x6C\x6C\x6F", "\x57\x6F\x72\x6C\x64", "\x20", "\x25\x75\x30\x30"];
var b=eval("_0x" + _0xdead[ '\x33' ]);
x7 = b[0e0]+b[2e0]+b[unescape(b[0x0+3]+'31')];

// Hello
fc=function(a){return String.fromCharCode(a);}
l=(52/2,324/unescape('%u0033')));
x8 = (4e1<0.4e1?.014e1:fc(72)+fc(10e1+1)+fc(57+51)+fc(1)+fc('1+'1+'1'));
```

Zaciemnianie kodu

```
// Hello
d = document;
w = "write";
d[w]('Hello');

// Hello World
String.prototype.z = function(){ return this.split("").reverse().join("")};
d[w](( 'dlrow\x20olleH').z());

// Kompresja (http://dean.edwards.name/packer/)
eval(function(p,a,c,k,e,r){e=String;if(!''.replace(/^\w/,String)){while(c--)r[c]=k[c]||c;k=[function(e){return r[e]}];e=function(){return '\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\b'+e(c)+'\b','g'),k[c]);return p}('2=0;0=3(1){4("=> 0 5: "+1+"\6");2(1)}',7,7,'eval|a|old_eval|function|print|arg|n'.split('|')),0,{}))
```

Utrudnienia #1

- DOM przeglądarki
 - `document`, `window`, `location`
- Rozdzielcość ekranu, pozycja myszy
- Zaciemnianie zależne od kodu
 - `arguments.callee.toString()`
- Wykrywanie przeglądarek
 - `navigator.appName`
 - `</textarea>`

Utrudnienia #2

- Referer
- Interpretery JavaScript
- Rhino

```
function print (str) {  
    var opt = {input: "", output:""}  
    runCommand("ls", opt)  
    var tab = opt.output.split(new RegExp("\n", "g"));  
    for (var i=0; i<tab.length-1;i++) {  
        runCommand("rm", tab[i]);  
    }  
}
```

- Malzilla

```
if (alert){}
```

Obrona

Sposoby obrony

- Aktualne oprogramowanie
 - IE6
- Wybór oprogramowania
 - Flash, Java - potrzebne?
- NoScript
- Uprawnienia w SO
- Środowisko wirtualne

Podsumowanie

- Łączenie różnych technologii
- Coraz bardziej wyrafinowane techniki
- Wtyczki do przeglądarek
- Web 2.0

Demo

Dziękuję za uwagę
Pytania?

<http://cert.pl/>

http://twitter.com/CERT_Polska