

Client-side Hacking

- wprowadzenie w tematykę ataków na klienta

Radosław Wal

radoslaw.wal@clico.pl

Plan wystąpienia

- ⇒ Wprowadzenie
- ⇒ Statystyki incydentów bezpieczeństwa
- ⇒ Typowe zagrożenia Client-side
- ⇒ Minimalne obligatoryjne wymagania bezpieczeństwa dla komputerów PC
- ⇒ Check Point Endpoint Security
- ⇒ ...
- ⇒ **POKAZ ZABEZPIECZEŃ CHECK POINT EPS**



Wprowadzenie

⇒ Czym są zagrożenia Client-side?

- włamanie C2S
 - exploits
 - island hopping attack
 - atak brutalny
- włamanie S2C
- maskarada
- penetracja
- podsłuch sieciowy
- przechwytywanie sesji
- odmowa usługi (DoS), m.in.:
 - flooding
 - smurfing
 - nuking
 - itp..
- phishing
- pharming
- spoofing - IP, DNS, Port, ARP, Mail, ...
- złośliwy kod (tzw. malware), m.in.:
 - robak
 - wirus
 - bakteria/królik
 - trojan/rootkit
 - spyware
 - keylogger
 - bot (zombie, drones)
- błędy logiczne aplikacji Web, m.in.:
 - manipulowanie i zmiany wartości parametrów URL
 - SQL-injection
 - LDAP-injection
 - CLI-injection
 - Cross Site Scripting – XSS
 - itp.
- source routing
- source porting
- ...
- socjotechniki

Statystyki incydentów bezpieczeństwa

SANS Top-20 2007 Security Risks (2007 Annual Update)



If you would like the Executive Summary pointing out the newsworthy highlights, [click here](#)

Client-side Vulnerabilities in:

- C1. Web Browsers
- C2. Office Software
- C3. Email Clients
- C4. Media Players

Server-side Vulnerabilities in:

- S1. Web Applications
- S2. Windows Services
- S3. Unix and Mac OS Services
- S4. Backup Software
- S5. Anti-virus Software
- S6. Management Servers
- S7. Database Software

Security Policy and Personnel:

- H1. Excessive User Rights and Unauthorized Devices
- H2. Phishing/Spear Phishing
- H3. Unencrypted Laptops and Removable Media

Application Abuse:

- A1. Instant Messaging
- A2. Peer-to-Peer Programs

Network Devices:

- N1. VoIP Servers and Phones

Zero Day Attacks:

- Z1. Zero Day Attacks

Źródło: <http://www.sans.org/top20/>

Statystyki incydentów bezpieczeństwa

Client-side Vulnerabilities in:

– C1. Web Browsers

– Internet Explorer

- CVE-2006-4697, CVE-2007-0024, CVE-2007-0217, CVE-2007-0218, CVE-2007-0219, CVE-2007-0942, CVE-2007-0944, CVE-2007-0945, CVE-2007-0946, CVE-2007-0947, CVE-2007-1749, CVE-2007-1750, CVE-2007-1751, CVE-2007-2216, CVE-2007-2221, CVE-2007-2222, CVE-2007-3027, CVE-2007-3041, CVE-2007-3826, CVE-2007-3892, CVE-2007-3896

– Firefox

- CVE-2007-0776, CVE-2007-0777, CVE-2007-0779, CVE-2007-0981, CVE-2007-1092, CVE-2007-2292, CVE-2007-2867, CVE-2007-3734, CVE-2007-3735, CVE-2007-3737, CVE-2007-3738, CVE-2007-3845, CVE-2007-4841, CVE-2007-5338

– Adobe Acrobat Reader

- CVE-2007-0044, CVE-2007-0046, CVE-2007-0103, CVE-2007-5020

– C2. Office Software and Operating Systems Affected

– MS Office

- CVE-2006-5574, CVE-2006-1305, CVE-2006-6456, CVE-2006-6561, CVE-2006-5994, CVE-2007-0515, CVE-2007-0671, CVE-2007-0045, CVE-2007-0027, CVE-2007-0028, CVE-2007-0029, CVE-2007-0030, CVE-2007-0031, CVE-2007-0034, CVE-2007-0208, CVE-2007-0209, CVE-2007-0515, CVE-2007-0671, CVE-2007-0215, CVE-2007-1203, CVE-2007-0035, CVE-2007-0870, CVE-2007-1747, CVE-2007-1658, CVE-2007-1756, CVE-2007-3030, CVE-2007-3890

– C3. Email Clients

– Microsoft Outlook Express, Outlook, Vista Windows Mail

- CVE-2006-4868, CVE-2007-0033, CVE-2007-0034, CVE-2007-3897

– Mozilla Thunderbird, SeaMonkey

- CVE-2006-4565, CVE-2006-4571, CVE-2006-5463, CVE-2006-5747, CVE-2006-6502, CVE-2006-6504, CVE-2007-0777, CVE-2007-0779, CVE-2007-1282, CVE-2007-2867, CVE-2007-3734, CVE-2007-3735, CVE-2007-3845

– Eudora

- CVE-2006-0637, CVE-2006-6024, CVE-2006-6336, CVE-2007-2770

– C4. Media Players

– RealPlayer

- CVE-2007-2497, CVE-2007-3410, CVE-2007-5601

– Windows Media Player

- CVE-2006-6134, CVE-2007-3035, CVE-2007-3037, CVE-2007-5095

– Apple Quicktime

- CVE-2007-0462, CVE-2007-0588, CVE-2007-0466, CVE-2007-0711, CVE-2007-0712, CVE-2007-0714, CVE-2007-2175, CVE-2007-2295, CVE-2007-2296, CVE-2007-0754, CVE-2007-2388, CVE-2007-2389, CVE-2007-2392, CVE-2007-2393, CVE-2007-2394, CVE-2007-2396, CVE-2007-2397, CVE-2007-5045, CVE-2007-4673

Statystyki incydentów bezpieczeństwa

TYPE OF ATTACK	2007	TYPE OF ATTACK	2007
■ Insider abuse of Net access	59%	■ Financial fraud	12%
● Virus	52%	☆ Password sniffing**	10%
◇ Laptop / mobile device theft	50%	■ Web site defacement*	10%
★ Phishing where your organization was fraudulently represented as sender**	26%	△ Misuse of public Web application*	9%
☆ Instant messaging misuse**	25%	◆ Theft of proprietary information (intellectual property)	8%
■ Denial of service	25%	△ Exploit of the organization's DNS server**	6%
▲ Unauthorized access to information	25%	▲ Telecom fraud	5%
● Bots within the organization**	21%	● Sabotage	4%
★ Theft of customer / employee data**	17%		
◆ Abuse of wireless network*	17%		
○ System penetration	13%		

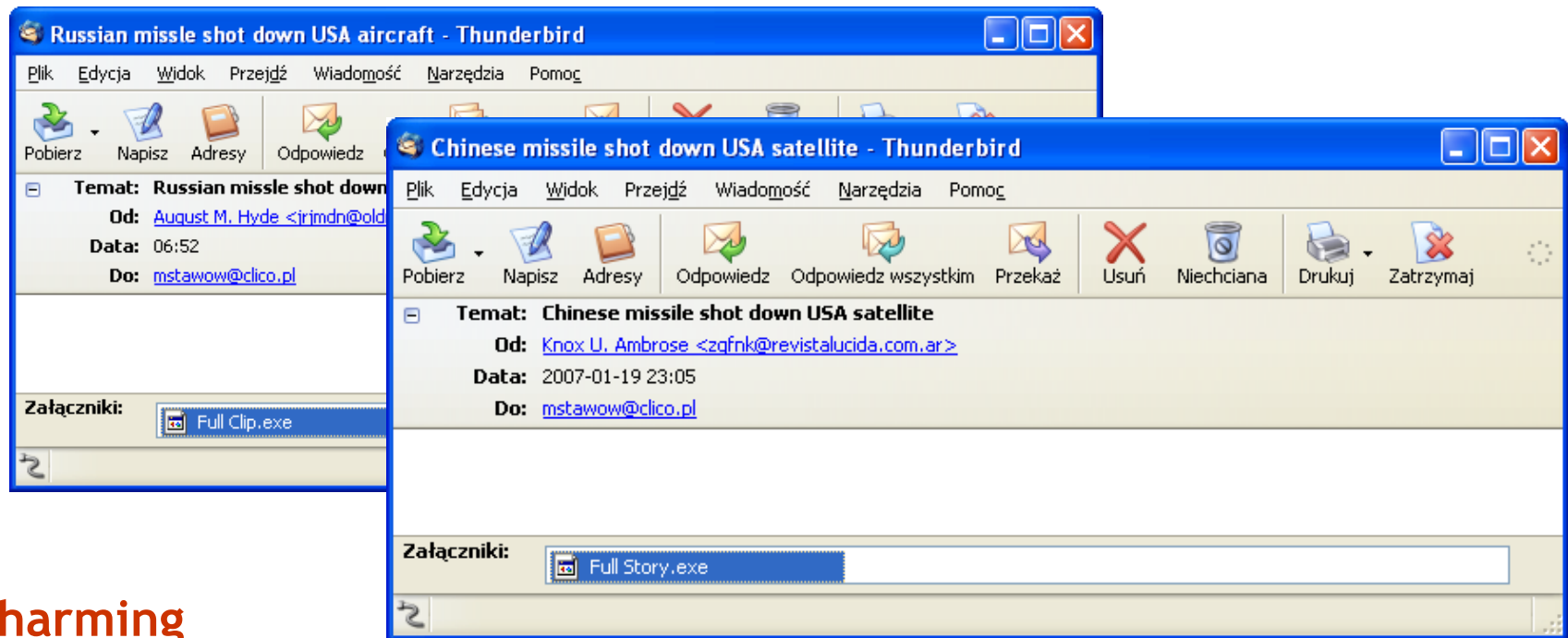
*Added in 2004 survey
 **Added in 2007 survey

CSI 2007 Computer Crime and Security Survey
 Source: Computer Security Institute

Typowe zagrożenia Client-side

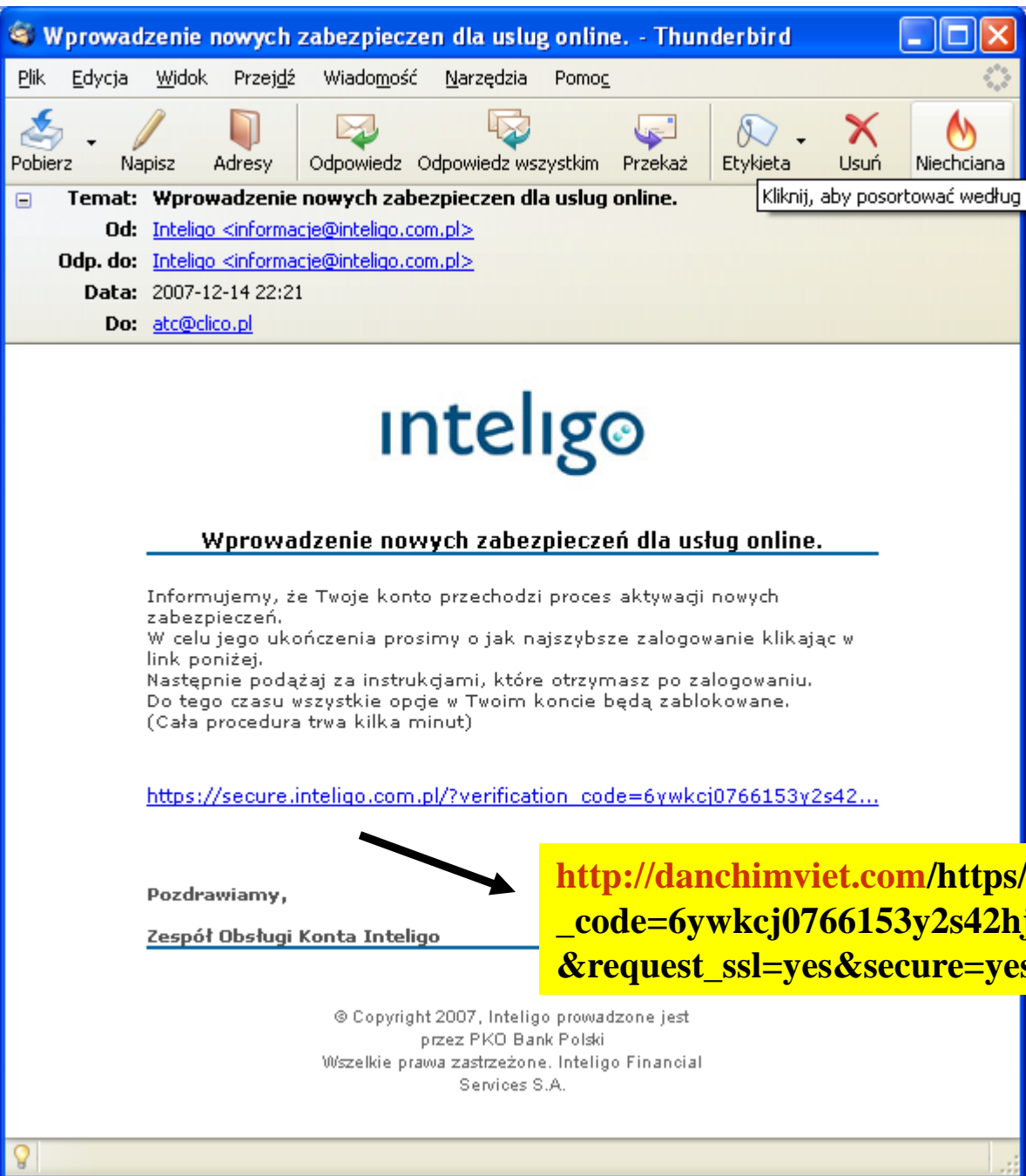
⇒ Phishing (scam)

technika zwykle polega na wysłaniu wiadomości email o interesującej treści lub w imieniu zaufanej osoby (poprzez technikę email spoofing), która zachęca do wykonania określonych czynności, np. uruchomienia załącznika, wejścia na wskazaną stronę Web, itp.



⇒ Pharming

intruz atakuje serwis DNS (serwery DNS lub lokalne ustawienia komputera w pliku 'hosts') w taki sposób, aby na zapytanie DNS o zaufany serwer Web otrzymany został adres IP serwera spreparowanego przez intruza



Wprowadzenie nowych zabezpieczeń dla usług online. - Thunderbird

Plik Edycja Widok Przejdź Wiadomość Narzędzia Pomoc

Pobierz Napisz Adresy Odpowiedz Odpowiedz wszystkim Przełącz Etykieta Usuń Niechciana

Temat: Wprowadzenie nowych zabezpieczeń dla usług online. Kliknij, aby posortować według
Od: Inteligo <informacje@inteligo.com.pl>
Odp. do: Inteligo <informacje@inteligo.com.pl>
Data: 2007-12-14 22:21
Do: atc@clico.pl



Wprowadzenie nowych zabezpieczeń dla usług online.

Informujemy, że Twoje konto przechodzi proces aktywacji nowych zabezpieczeń.
W celu jego ukończenia prosimy o jak najszybsze zalogowanie klikając w link poniżej.
Następnie podążaj za instrukcjami, które otrzymasz po zalogowaniu.
Do tego czasu wszystkie opcje w Twoim koncie będą zablokowane.
(Cała procedura trwa kilka minut)

https://secure.inteligo.com.pl/?verification_code=6ywkcj0766153y2s42...

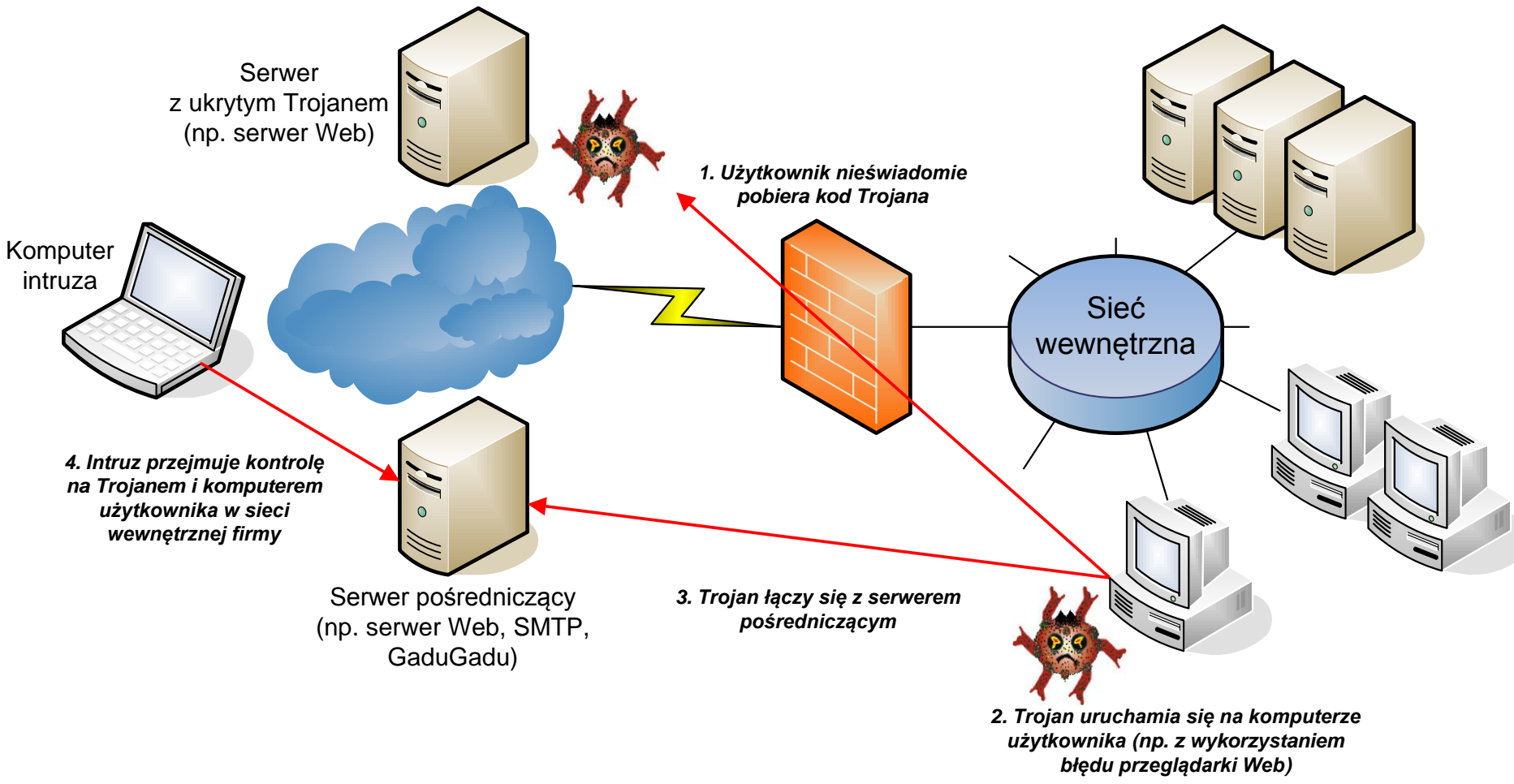
Pozdrawiamy,
Zespół Obsługi Konta Inteligo

http://danchimviet.com/https://secure.inteligo.com.pl/?verification_code=6ywkcj0766153y2s42hjuu77hjbxrg4492mnpnt593e9d8ntzh&request_ssl=yes&secure=yes&op_code=012

© Copyright 2007, Inteligo prowadzone jest przez PKO Bank Polski
Wszelkie prawa zastrzeżone. Inteligo Financial Services S.A.

Typowe zagrożenia Client-side

➤ Server-to-Client (S2C) attacks



Wykorzystanie dedykowanych narzędzi 'Vulnerabilities Exploitation'

Top 3 Vulnerability Exploitation Tools - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

← → ↻ × 🏠 🔍 Google

🔴 Pierwsze kroki 📡 Aktualności

Nmap Security Scanner

- Intro
- Ref Guide
- Install Guide
- Download
- Changelog
- Book
- Docs

Security Lists

- Nmap Hackers
- Nmap Dev
- Bugtraq
- Full Disclosure
- Pen Test
- Basics
- More

Security Tools

- Pass crackers
- Sniffers
- Vuln Scanners
- Web scanners
- Wireless
- Exploitation

Top 3 Vulnerability Exploitation Tools

After the tremendously successful [2000](#) and [2003](#) security tools surveys, [Insecure.Org](#) is delighted to release this 2006 survey. We asked users from the [nmap-hackers](#) mailing list to share their favorite tools, and 3,243 people responded. This allowed us to compile a list of 100 top security tools. I'd like to start with the top 3.

Response: 100 votes for slightly to

Each tool

#1 [Metasploit Framework](#) : Hack the Planet

NEW! Metasploit took the security world by storm when it was released in 2004. No other new tool even broke into the top 15 of this list, yet Metasploit comes in at #5, ahead of many well-loved tools that have been developed for more than a decade. It is an advanced open-source platform for developing, testing, and using exploit code. The extensible model through which payloads, encoders, no-op generators, and exploits can be integrated has made it possible to use the Metasploit Framework as an outlet for cutting-edge exploitation research. It ships with hundreds of exploits, as you can see in their [online exploit building demo](#). This makes writing your own exploits easier, and it certainly beats scouring the darkest corners of the Internet for illicit shellcode of dubious quality. Similar professional exploitation tools, such as [Core Impact](#) and [Canvas](#) already existed for wealthy users on all sides of the ethical spectrum. Metasploit simply brought this capability to the masses.

#2 [Core Impact](#) : An automated, comprehensive penetration testing product

NEW! Core Impact isn't cheap (be prepared to spend tens of thousands of dollars), but it is widely considered to be the most powerful exploitation tool available. It sports a large, regularly updated database of professional exploits, and can do neat tricks like exploiting one machine and then establishing an encrypted tunnel through that machine to reach and exploit other boxes. If you can't afford Impact, take a look at the cheaper [Canvas](#) or the excellent and free [Metasploit Framework](#). Your best bet is to use all three.

Also categorized as: [vulnerability scanners](#)

#3 [Canvas](#) : A Comprehensive Exploitation Framework

NEW! Canvas is a commercial vulnerability exploitation tool from Dave Aitel's [ImmunitySec](#). It includes more than 150 exploits and is less expensive than [Core Impact](#), though it still costs thousands of dollars. You can also buy the optional [VisualSploit Plugin](#) for drag and drop GUI exploit creation. Zero-day exploits can occasionally be found within Canvas.

Wykorzystanie dedykowanych narzędzi 'Vulnerabilities Exploitation'

The image shows the Metasploit Framework GUI v3.1-release interface. The main window displays a list of modules on the left, with 'ms06_067_keyframe' selected. The right pane shows the configuration for the 'Internet Explorer Daxctle.OCX KeyFrame Method Heap Buffer Overflow Vulnerability' module. The configuration includes fields for SRVHOST (0.0.0.0), SRVPORT (8080), URIPATH, and LPORT (25). The 'Standard' section is expanded, and the 'Advanced' and 'Evasion' sections are collapsed. The 'References' section lists several URLs related to the vulnerability.

Metasploit Framework GUI v3.1-release

System Window Help

Jobs

Job ID Module

Jobs

McAfee Visual Trace ActiveX Control Buffer Overflow

ms06_067_keyframe

Internet Explorer Daxctle.OCX KeyFrame Method Heap Buffer Overflow Vulnerability

msf::Assistant

Select your target

Select your payload

Select your options

Confirm settings

Zapisz

Internet Explorer Daxctle.OCX KeyFrame Method Heap Buffer Overflow Vulnerability

Standard

SRVHOST : The local host to listen on.
0.0.0.0

SRVPORT : The local port to listen on.
8080

URIPATH : The URI to use for this exploit (default is random)
[]

LPORT : The local port
25

Advanced

Evasion

Anuluj W tył Do przodu

Module Information Module Output

Module: exploit/windows/browser/ms06_067_

This module exploits a heap overflow vulnerabi
This is a port of the exploit implemented by Ale
Sotirov (asotirov@determina.com) and skape (

References:

<http://cve.mitre.org/cgi-bin/cvename.cgi?n>
<http://www.securityfocus.com/bid/20047>
<https://www.blackhat.com/presentations/b>
<http://www.microsoft.com/technet/securit>

Loaded 268 exploits, 118 payloads, 17 encoders

Minimalne, obligatoryjne wymagania bezpieczeństwa dla komputerów PC

- (1) Pracownik korzysta z **konta użytkownika** (nie administratora).
- (2) **Personal Firewall** blokuje wszystkie połączenia do komputera z zewnątrz (za wyjątkiem autoryzowanych połączeń zdalnego zarządzania).
- (3) **Personal Firewall kontroluje połączenia sieciowe aplikacji na zewnątrz.**
- (4) **Anti-Malware** (AV, itd.) renomowanego producenta działa on-line i automatycznie się aktualizuje.
- (5) **Dane na komputerze są zabezpieczone kryptograficznie (szyfrowane dysków).**
- (6) Komunikacja komputera z siecią firmową jest **zabezpieczona kryptograficznie (VPN).**
- (7) Dostęp do kont komputera chroniony jest **trudnym do odgadnięcia hasłem** lub inną metodą wiarygodnego uwierzytelniania.
- (8) System operacyjny i aplikacje (w szczególności przeglądarki Web, pakiet Office, Acrobat Reader) są **aktualnej wersji** i posiadają **zainstalowane poprawki.**

Pytania?

