



# Ochrona danych – wszystko, co powinieneś wiedzieć, ale boisz się zapytać

Michał Ceklarz



# IBM globalny zasięg

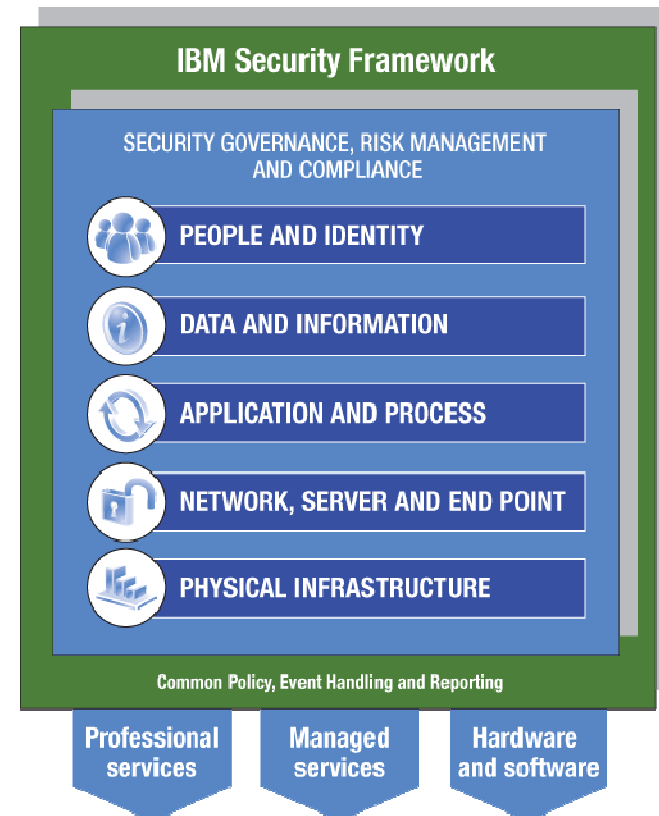


**TIVOLI SUMMER ACADEMY** IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security | 1



# IBM: Kompleksowe podejście do bezpieczeństwa

- Jedyne dostawca rozwiązań bezpieczeństwa typu *end-to-end*
- 15,000 badaczy, developerów i innych pracowników związanych z bezpieczeństwem
- 3,000+ patentów związanych z bezpieczeństwem
- 200+ klientów będących publiczną referencją i ponad 50+ opublikowanych case study
- 40+ doświadczeń w zabezpieczaniu środowisk zSeries





# Rozwiązanie punktowe ?

***„Pudełka” to nie  
bezpieczeństwo !***

***... Bezpieczeństwo to coś zupełnie  
innego !***

***Zrozumienie zagrożenia jest  
kluczem do ochrony***





## Leo why..?





# Identyfikacja i ocena zagrożenia

- Cz



ia



## Wnioski z raportu za 2009r.

### Application and Process

- Odkryto 6,601 nowych podatności w całym 2009, to o **11%** mniej niż w 2008,
- **49%** podatności dotyczyło aplikacji Web.
- **52%** podatności nie miało poprawki producenta w 2009r.

### Data and Information

- Znacznie więcej podatności związanych z PDF niż z dokumentami Office.
- Coraz więcej automatycznych narzędzi do tworzenia wrogich kodów.
- W US hostowanych jest najwięcej stron ze złośliwymi linkami.

### Network, Server, and End Point

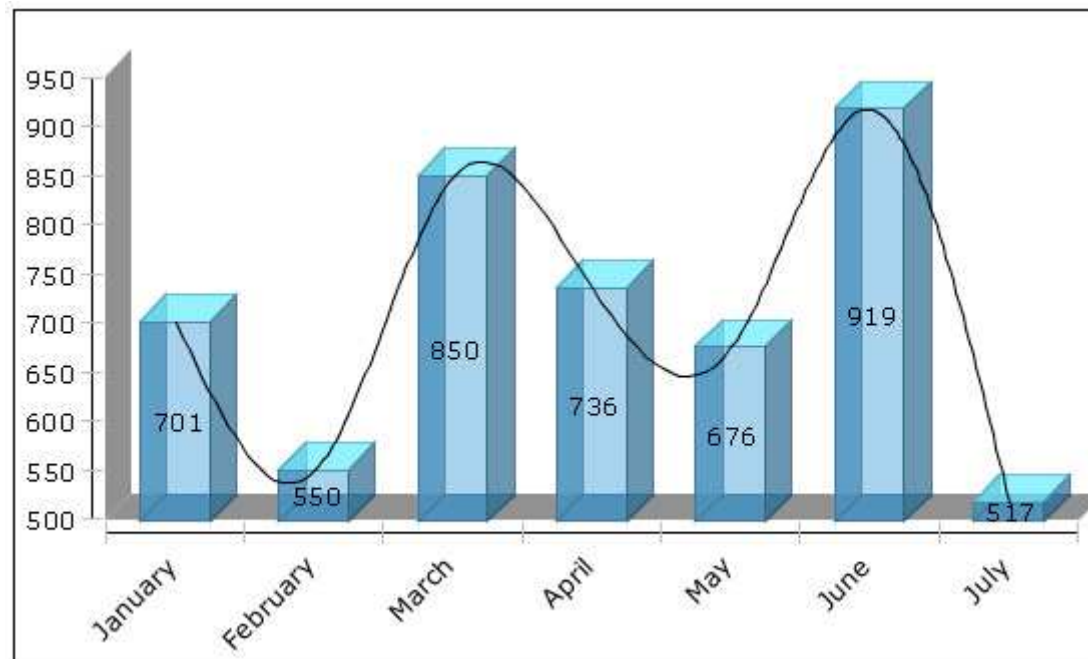
- 7.5% treści w internecie jest uważanych za nie do zaakceptowania z powodów społecznych.
- Ilość wrogich linków zwiększyła się o **345%** w porównaniu z 2008.

### People and Identity

- Większość SPAM'u (**80%**) jest klasyfikowana jako URL spam.
- Coraz więcej SPAMU powołuje się na znane i wzbudzające zaufanie domeny.
- **60.9%** phishing jest skupionych na instytucjach finansowych, **20.4%** dotyczy organizacji „rządowych”



## Tylko w 2010 wykryto 4383 nowych podatności





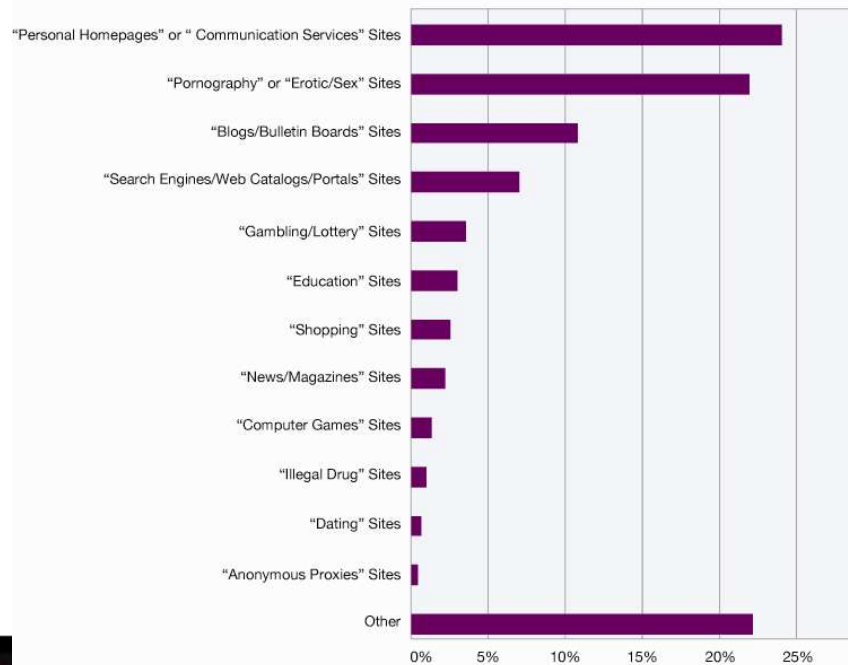


Created using **Wink**

# „Dobre strony” serwują złośliwe linki

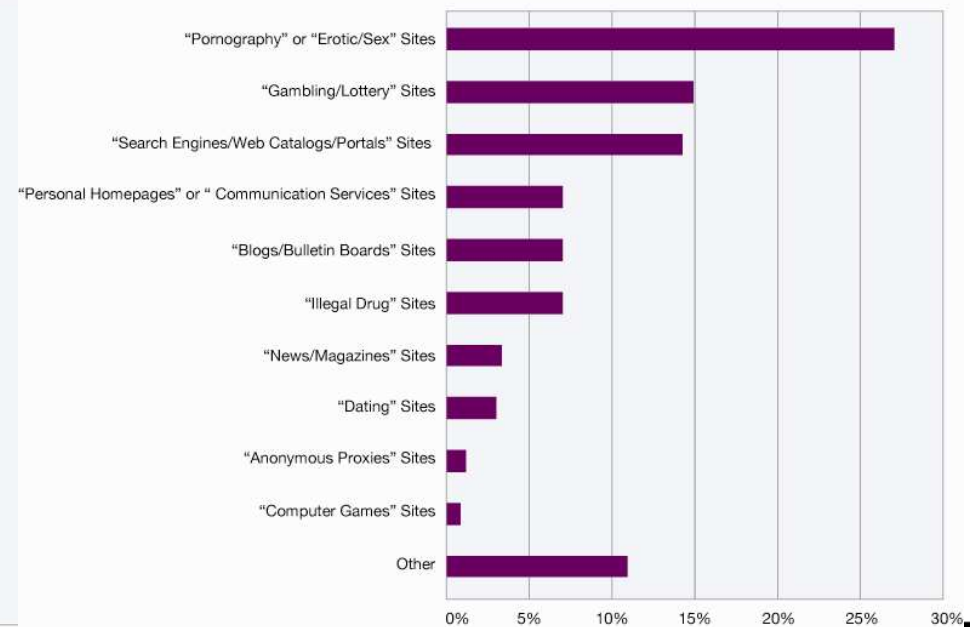
- Prawie połowa strony użytkowników „domowych” (często umieszczone na serwerach dostawców internetowych) posiadają odnośniki do niebezpiecznych stron
- Ponad 10 takich linków posiadają strony z pornografią **28%** i hazardem **14%**

Top Web Site Categories Containing at Least One Malicious Link  
2009 H2



Source: IBM X-Force®

Top Web Site Categories Containing 10 or More Malicious Links  
2009 H2



Source: IBM X-Force®



## Każdy administrator IT powie:

- ... u mnie działa

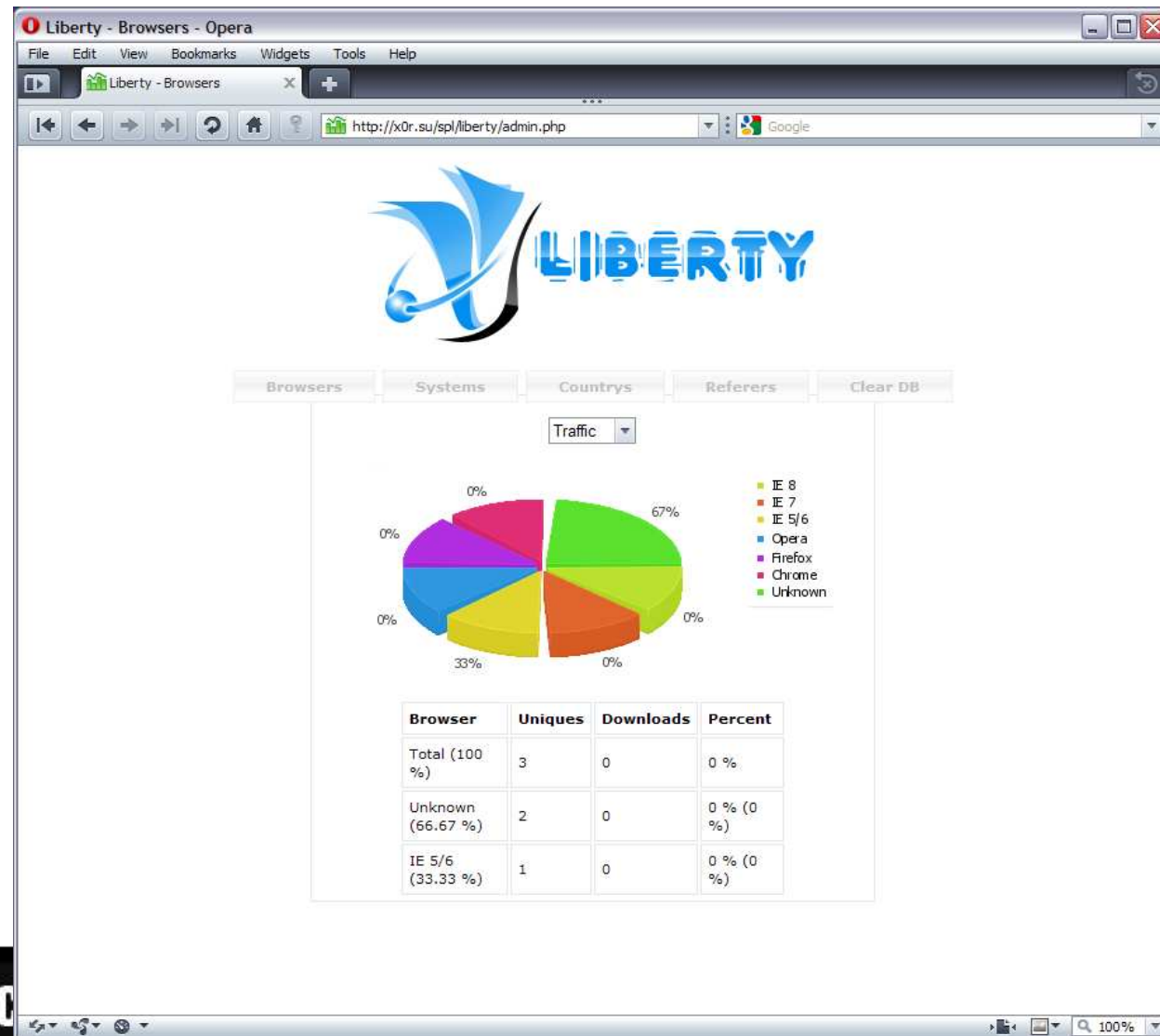




# Pytanie czy systemy zabezpieczające mu w tym pomagają...

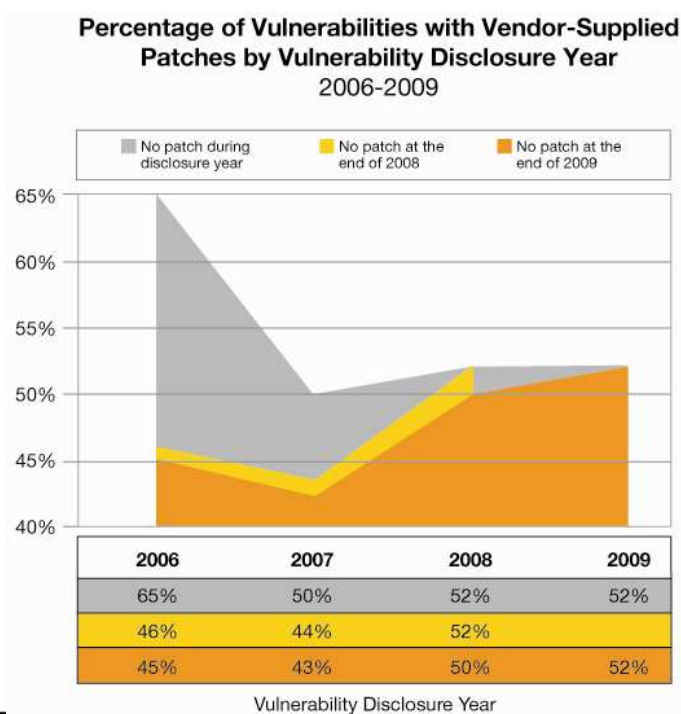


# Celem ataków jest popularne oprogramowanie



# W dalszym ciągu nie ma poprawek dla luk wrytych w poprzednich latach

- Ponad połowa (**52%**) podatności odkrytych w 2009 nie ma łatki bezpieczeństwa.
  - **45%** z 2006, **43%** z 2007 i **50%** z 2008 podatności w dalszym ciągu nie jest załatwana (stan na koniec 2009).



Source: IBM X-Force®

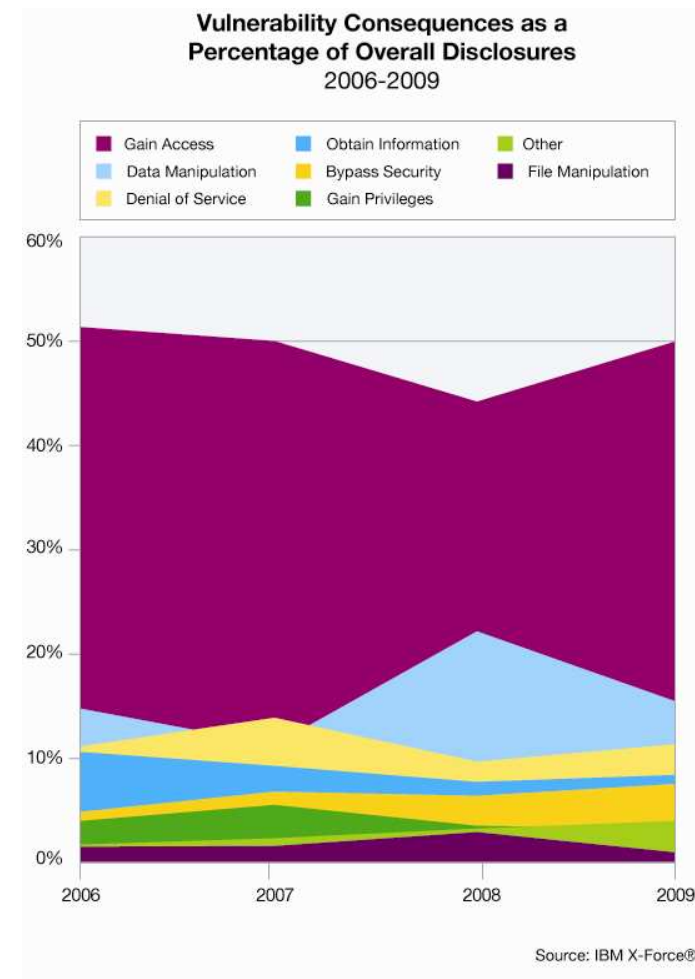
Vendor	Percent of 2009 Disclosures with No Patch	Percent of Critical & High 2009 Disclosures with No Patch
<b>All Vendors–2009 Average</b>	<b>52%</b>	<b>60%</b>
Linux	50%	53%
Oracle	40%	38%
Novell	27%	31%
IBM	25%	27%
Google	47%	25%
Apple	14%	22%
Microsoft	29%	15%
Sun	7%	8%
Symantec	18%	7%
HP	16%	5%
Adobe	4%	4%
Cisco	11%	1%
Opera	47%	0%
GNU	33%	0%
Mozilla	15%	0%
Rim	14%	0%

Table 4: Best and Worst Patchers, 2009



## W 2009 atakujący chciał uzyskać dostęp i zmienić informacje

- “Uzyskanie dostępu” to w dalszym ciągu najczęstsza konsekwencja udanego ataku.
- “Data Manipulation” to w dalszym ciągu duże zagrożenie.





# Zeus Crimeview

Member slots filled: 3 / 30

[Q] What is  
[A] is a mix between the ZeuS Trojan and MalKit. A browser attack to a computer and start logging all outgoing connections.

[Q] How much does it cost?  
[A] Hosting for costs \$50 for 3 months. This includes the following:

- Fully set up ZeuS Trojan with configured FUD binary.
- Log all information via internet explorer
- Log all FTP connections
- Steal banking data
- Steal credit cards
- Phish US, UK and RU banks
- Host file override
- All other ZeuS Trojan features
- Fully set up MalKit with stats viewer inter graded.
- 10 IE 4/5/6/7 exploits
- 2 Firefox exploits
- 1 Opera exploit
- Admin area to view statistics

[Q] Can i see a demo?  
[A] Yes you can, there is a demo set up [here](#) (Comming soon)

Methods of payment:

- Moneybookers.com
- LibertyReserve.com
- WesternUnion
- Alertpay.com

**Zeus :: Logs search**

**Information:**  
We also host Profile:  
This includes GMT date:  
GMT time:

**Statistics:**  
Summary

**Botnet:**  
Online bots  
Remote commands

**Logs:**  
→ Search  
Search with template  
Uploaded files  
Logout

Hosting for costs \$50 for 3 months.  
This includes the following:

- # Fully set up ZeuS Trojan with configured FUD binary.
- # Log all information via internet explorer
- # Log all FTP connections
- # Steal banking data
- # Steal credit cards
- # Phish US, UK and RU banks
- # Host file override
- # All other ZeuS Trojan features
- # Fully set up MalKit with stats viewer inter graded.
- # 10 IE 4/5/6/7 exploits
- # 2 Firefox exploits
- # 1 Opera exploit“

We also host normal ZeuS clients for \$10/month.  
This includes a fully set up zeus panel/configured binary

**MassInfect**  
explorer, FireFox, Opera - 2008

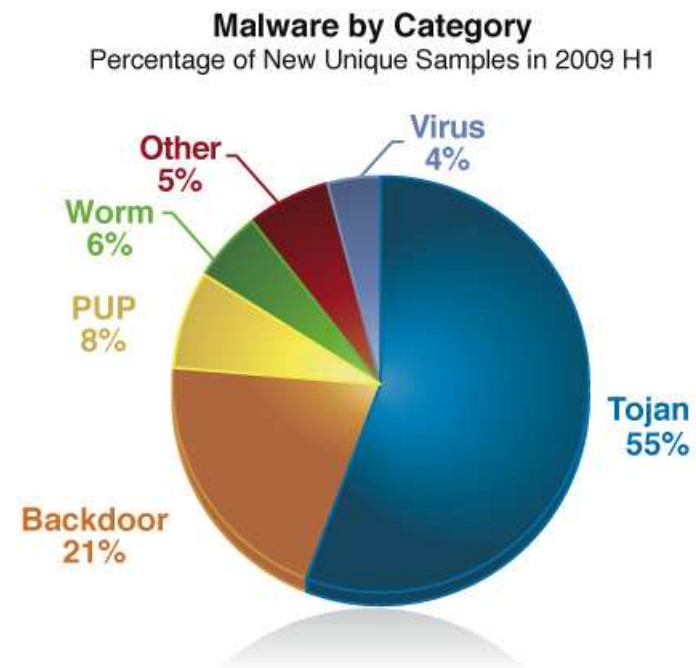
Hits	Infects
23	0
7	0
3	0
3	0
2	0
1	0
1	0
1	0
1	0
1	0
28	0
11	0
5	0
21	0

Search type: Any  
 Case  
 Exclu  
 Don  
 Reset  
 Output: Normal  
 (slow)  
 Search



# Większość wrogich kodów to Trojany

- Udział Trojanów zwiększył się o dziewięć procent (w 2008r – 46%)
- Duża część wrogich kodów generowanych jest za pomocą publicznie dostępnych narzędzi
- Poziom zaawansowania wrogich kodów w 2009 był na niespotykanie wysokim poziomie
  - **Techniki propagacji, mutacji i ukrywania ataku świadczą o podtekście finansowych działania wrogich kodów**



source: IBM X-Force®



#### Bronze Edition

- This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version)
- 1 month replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail
- Supports only Windows 95/98/ME/NT/2000/XP
- Realtime Screen viewing(controlling is disabled)

**Price : 99\$** (United State Dollar)



#### Silver Edition

- 4 months (maximum 3 times) replacement warranty if it gets dedected by any antivirus
- 7/24 online support via e-mail and instant messengers
- Supports 95/98/ME/NT/2000/XP/Vista
- Webcam streaming is available with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies chngements on clipboard and save them

**Price : 179\$** (United State Dollar)



#### Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets dedected by any antivirus (you can choose 6 months or 9 months)
- 7/24 online support via e-mail and instant messengers
- Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
- Remote Shell (Managing with Ms-Dos Commands)
- Webcam - audio streaming and msn sniffer
- Controlling remote computer via keyboard and mouse
- Notifies chngements on clipboard and save them
- Technical support after installing software
- Viewing pictures without any download(Thumbnail Viewer)

**Price : 249\$** (United State Dollar)



# Automatyczne SQL Injection z wyszukiwarką

- Komercyjne narzędzia do SQL Injection są automatycznie aktualizowane

```
<Scan_Google> [milw0rm] Joomla Component Expose <= RC
  Vulnerability - http://www.milw0rm.com/exploits/4194
<Scan_Google> [milw0rm] QuickEStore <= 8.2 (insertord
  Vulnerability - http://www.milw0rm.com/exploits/4193
<Scan_Google> [milw0rm] Vivvo CMS <= 3.4 (index.php)
  Exploit - http://www.milw0rm.com/exploits/4192
<Scan_Google> [milw0rm] Pictures Rating (index.php ns
  Vulnerability - http://www.milw0rm.com/exploits/4191
<Scan_Google> [milw0rm] Data Dynamics ActiveBar Activ
  Insecure Methods - http://www.milw0rm.com/exploits/4
<Scan_Google> [milw0rm] Expert Advisor (index.php id
  Vulnerability - http://www.milw0rm.com/exploits/4189
<Scan_Google> [milw0rm] Flash Player/Plugin Video fil
  Execution POC - http://www.milw0rm.com/exploits/4188
<h3x8z5o1> !scan phpBB Module SupaNav 1.0.0
<Scan_Google> [Scan] Started: phpBB - Dork: Module SupaNav 1.0.0 Engine: Google
<Scan_Google> [Scan] Google Found: 150 Sites!
<Scan_Google> [Scan] Cleaned results: 2 Sites!
<Scan_Google> [Scan] Exploiting started!
<Scan_Google> [Scan] Scan Finished Module SupaNav 1.0.0
<h3x8z5o1> !scan Flash Player/Plugin Video file parsing Remote Code Execution POC
<Scan_Google> [Scan] Started: Flash - Dork: Player/Plugin Video file parsing Remote
  Code Execution POC Engine: Google
<Scan_Google> [Scan] Google Found: 2679 Sites!
<Scan_Google> [Scan] Cleaned results: 492 Sites!
<Scan_Google> [Scan] Exploiting started!
```

```
<B-Scan> [Vuln] Exploiting 1080 on 1242 sites
<A-Scan> [Vuln] Exploiting 3090 on 5468 sites
<haaaaaweee> !string
<A-Scan> [String] agenda.php3?rootagenda= allinurl:/phpmyagenda/
<B-Scan> [String] components/com_extended_registration/registration_detailed.
  inc.php?mosConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Vuln] Exploiting 3120 on 5468 sites
<haaaaaweee> !a components/com_extended_registration/registration_detailed.inc.php?mo
  sConfig_absolute_path= inurl:com_extended_registration
<A-Scan> [Dork] inurl:com_extended_registration
<A-Scan> [Bug] components/com_extended_registration/registration_detailed.inc.php?mos
  Config_absolute_path=
<A-Scan> [Scan] Scanning started now!
<A-Scan> [Google] Started : inurl:com_extended_registration -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<A-Scan> [Acco] Started : inurl:com_extended_registration -
  components/com_extended_registration/registration_detailed.inc.php?mosConfig_absolu
  te_path=
<B-Scan> [Vuln] Exploiting 840 on 2106 sites
<B-Scan> [Vuln] Exploiting 1110 on 1242 sites
<A-Scan> [Vuln] Exploiting 3150 on 5468 sites
<B-Scan> [Vuln] Exploiting 1140 on 1242 sites
<B-Scan> [Vuln] Exploiting 1170 on 1242 sites
<B-Scan> [Vuln] Exploiting 1200 on 1242 sites
```

- Najpierw wyszukanie podatnych celów, a następnie przeprowadzenie ataku



# Narzędzi oparte o subskrypcje

- Automatyczny atak typu SQL Injection
  - Wspecyfikowanie payload (default `http://www.2117966 [dot] net/fckjip.js` )
  - Sprawdzenie na stronie w Chinach czy jest ważna subskrypcja
  - Wyszukanie za pomocą Google podatnych stron `inurl:".asp" inurl:"a="`
  - Rozpoczęcie ataku

```
CLI
?? ???? asdf ??
http://www.google.com/search?num=100&hl=en&lr=&newwindow=1&as_qdr=all&q=inurl%3A%22.asp%22+inurl%3A%22
http://www.google.com/search?q=inurl%3A%22.asp%22+inurl%3A%22&num=100&hl=en&lr=&newwindow=1&as_qdr=all&start=200
http://www.simttester.com/page/news/showpubnews.asp?title=A+Quick+Look+at+Enhanced+Performance+Profiles+(EPP)+Me
http://investing.businessweek.com/research/common/symbollookup/symbollookup.asp?letterIn=A
http://search.banesandnoble.com/bookssearch/results.asp?wrda=new+earth&src=tc
http://www.recruitireland.com/careercentre/news/anmvviewer.asp?a=1512&z=2&isasp=inews.asp&subcat=
http://www.robertmundell.net/books/main.asp?Title=A%20Theory%20of%20Optimum%20Currency%20Areas
http://www.sethbarnes.com/index.asp?filename=theres-a-worldwide-war-between-good-evil
http://www.ins.state.pa.us/ins/cwp/view.asp?a=1331&q=542979
http://www.aegis.com/nl/topics/glossary/a.asp?page=A
http://www.niscar.res.in/InformationResources/info.asp?a=topframe.htm&b=leftcon.asp&c=nsi/nsi.htm&d=test
http://www.moneyminded.com.au/words/default.asp?letter=A
http://www.online-medical-dictionary.org/a.asp?q=a
http://keywords.msu.edu/a-z/directory.asp?list=a
http://www.banking.state.pa.us/banking/cwp/view.asp?a=1350&q=546528
http://www.sickkids.ca/HumanResources/section.asp?s=Find+a+Career&slD=13
http://www.vegastowers.com/raf.asp?BT ag=a
http://www.atstacticalgear.com/istar.asp?a=29&manufacturer=ATS
http://www.acronymfinder.com/af-query.asp?acronym=Hep+A
http://www.watermelon.org/index.asp?a=dsp&hype=recipe&pid=18
http://www.ecml.at/help/alpha.asp?abc=A
http://www.nhra.com/apcm/APCMviewer.asp?a=17520&z=8
http://www.xigla.com/absolutem/xaabsolutem/animviewer.asp?a=1&z=1
http://www.law-dictionary.org/a.asp?q=a
http://www.maplemusic.com/artist_listing.asp?id1=a
http://www.tafe.wa.gov.au/Dynamic/DynamicPge.asp?a=10029,0,Std
http://www.mg.co.za/Content/13_f.asp?a=18&o=10298
http://www.dk21.com/SCRIPTING/RUNDLL32/REGGUIDE.ASP?P=A
ALL MEMO1'S URL FINISHED! ^ _ ^ SEE LOG
```

Courtesy: <http://isc.sans.org/diary.html?storyid=4294>

# Przykład narzędzi automatycznych

地址: http://w URL: http://localhost/sqlinject/news.asp?id=1

网页 图片

总体输出 基本信息 探测设置 HEAD Cookies 浏览

另存为... 保存 复制  同时输出到表格 在浏览器中打开当前注入点

• 远程服务器列表:  
服务器名: MTJ-S4\GSQL  
服务器产品: SQL Server  
数据源: MTJ-S4\GSQL  
位置:  
提供者文本:  
服务器网络名: MTJ-S4\GSQL

• 登录用户列表:  
用户名:  
密码HASH: 0x  
安全编号: 0x  
X状态: ...

用户名: testDB.admin

用户名 密码HASH 安全编号 X状态

公用 SQL Server Access MySQL Oracle

用户名 密码HASH 安全编号 X状态

信息回显方式: 基于我的SQLServer服务器转发 设置我的MS SQL服务器 取记录数失败时强制读取的最大记录数: 5

基本信息 命令行 GetWebShell 获取数据库内容 数据库插马 文件读写 杂项工具

where: id=1 SQL: select top 3 id,username,password from TestDB..admin order by id

top: 3  逆序排列 当前库: TestDB 排序: id

id	username	password
1	testUserzjs	123456
25	test	password
26	ff	aa

TestDB

- t\_t
- admin
  - id
  - username
  - password
  - privilege
  - telephone
  - address
- pass\_kr
- news
  - id
  - title

服务器名 服务器产品 数据源 位置 提供者文2 服务器网

服务器名	服务器产品	数据源	位置	提供者文2	服务器网
MTJ-S4\GS	SQL Server	MTJ-S4\GSQL			MTJ-S4\GS

用户名 密码HASH 安全编号 X状态

获取基本信息完毕?

http://www. 完整URL

http://www. 安全漏洞

http://www. 扫描页面

http://www. 错误

http://www. msdb

http://www. temp

http://www. Test

http://www. com/zfbz/zfnr.asp?id=78 515 5 XoR 8=3 + XoR 8=8 XOR 数字型 未探测 中国铁通东莞分公司-



## Tak działają niektóre systemy...

*technologia zorientowana na exploity:*





**Korzystaj ze sprawdzonych rozwiązań...  
...czasem dobry pomysł może spalić na  
panewce**





**Michał Ceklarz**

*IBM Internet Security Systems*

*Michal.Ceklarz@pl.ibm.com*

**Pytania?**