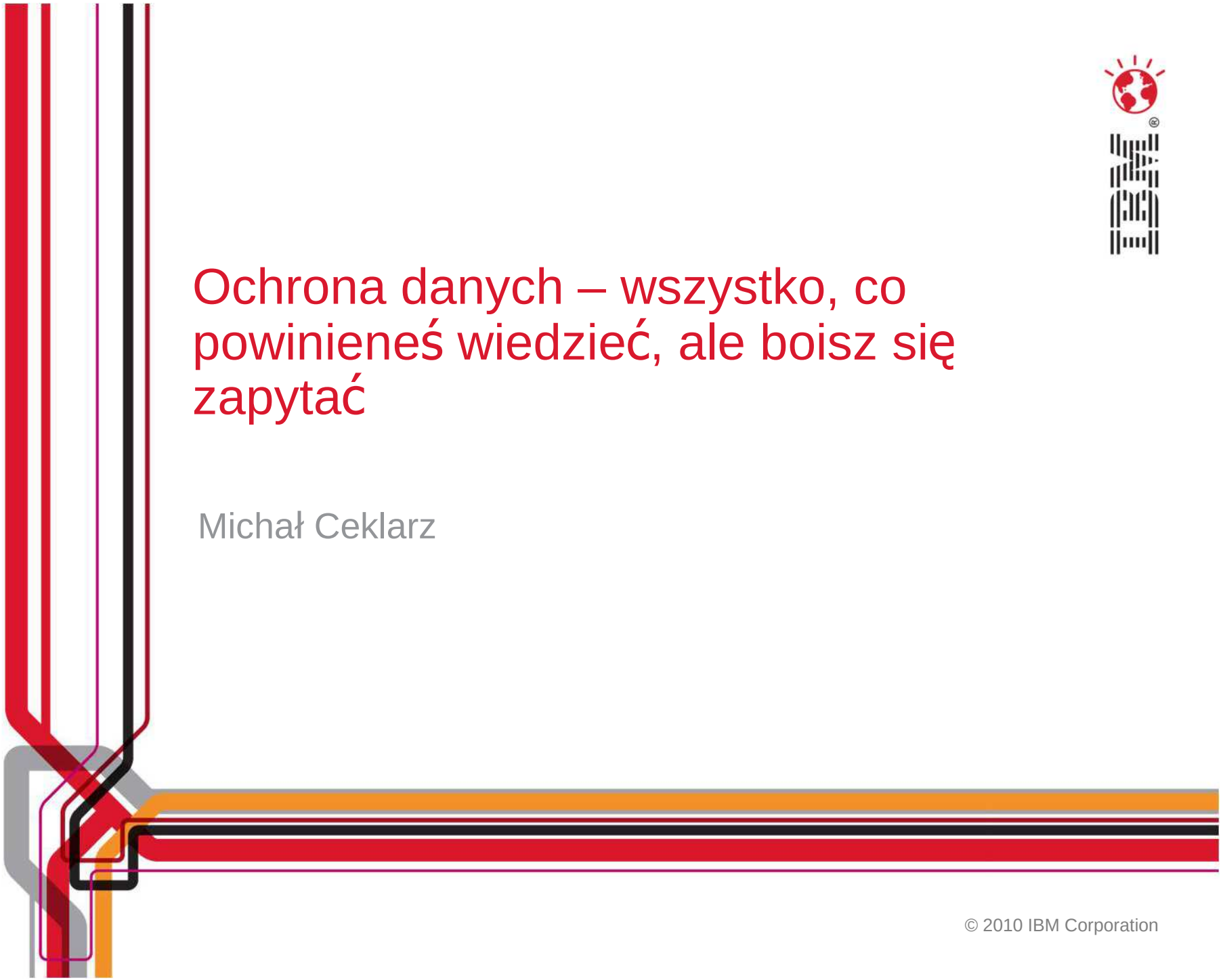


Ochrona danych – wszystko, co powinieneś wiedzieć, ale boisz się zapytać

Michał Ceklarz

IBM globalny zasięg

8 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 20,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 4 Billion+ Events Per Day

IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

IBM: Kompleksowe podejście do bezpieczeństwa

- Jedyny 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

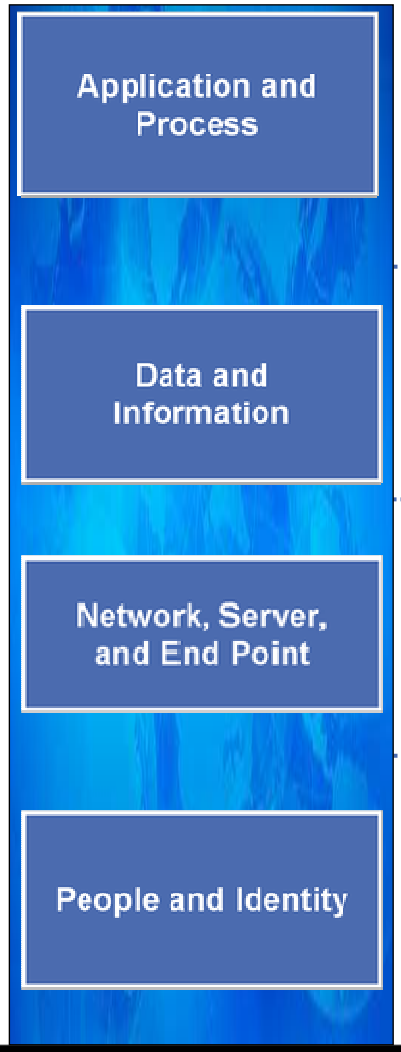
Leo why..?

Identyfi

- Cza

ia

Wnioski z raportu za 2009r.



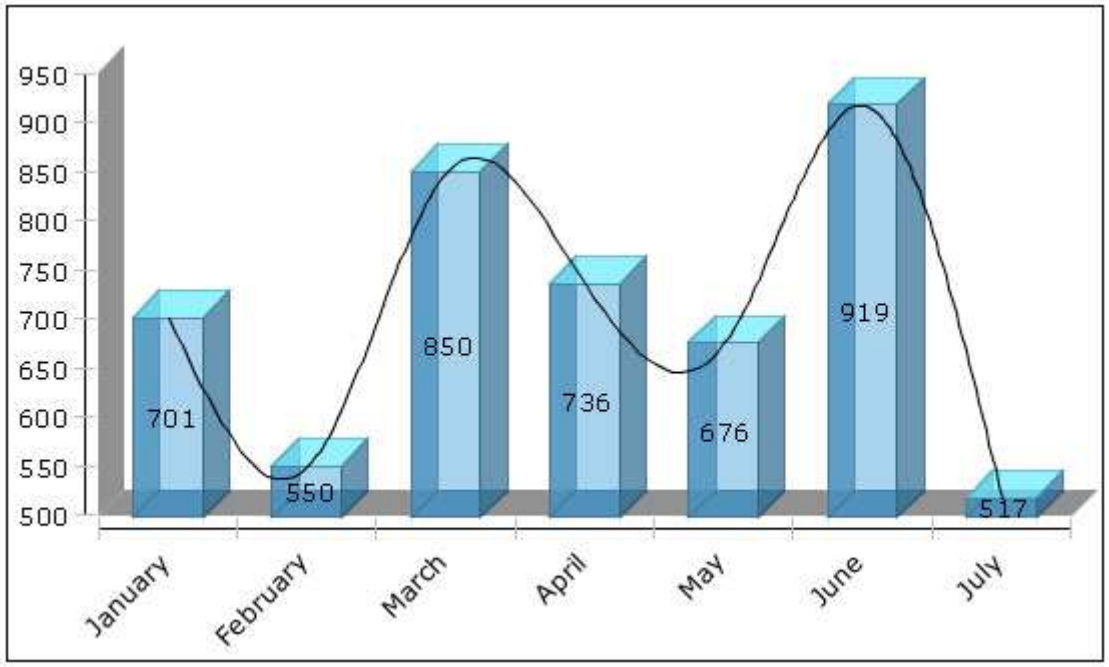
- Odkryto 6,601 nowych podatności w całym 2009, to o **11%** mniej niż w 2008,
- **49%** podatności dotyczyło aplikacji Web.
- **52%** podatności nie miało poprawki producenta w 2009r.

- 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.

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

- 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"

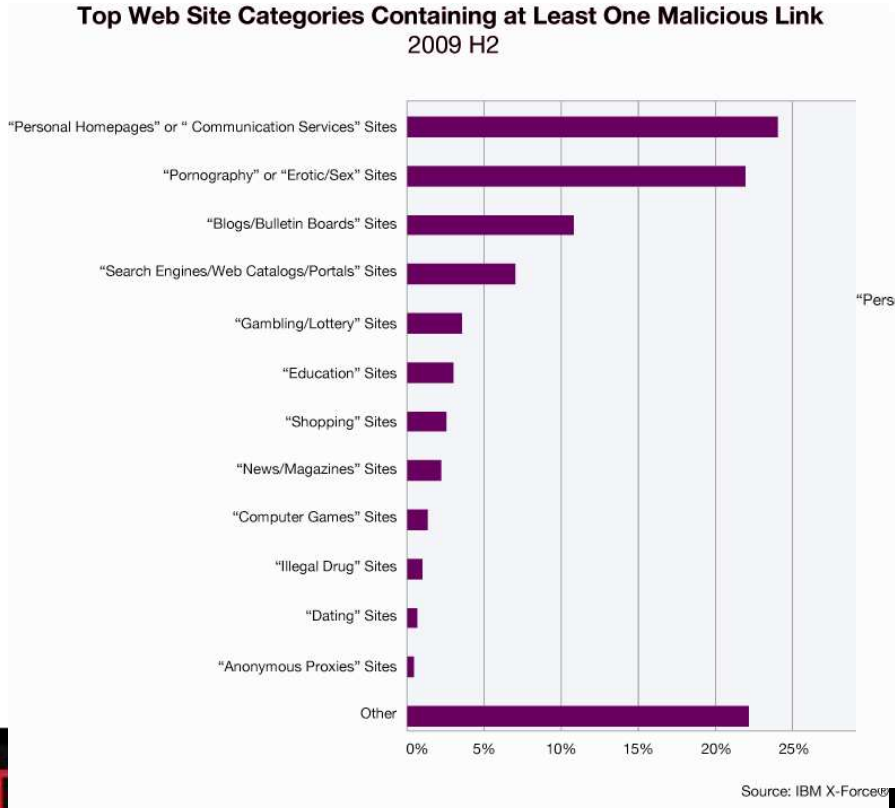
Tylko w 2010 wykryto 4383 nowych podatności

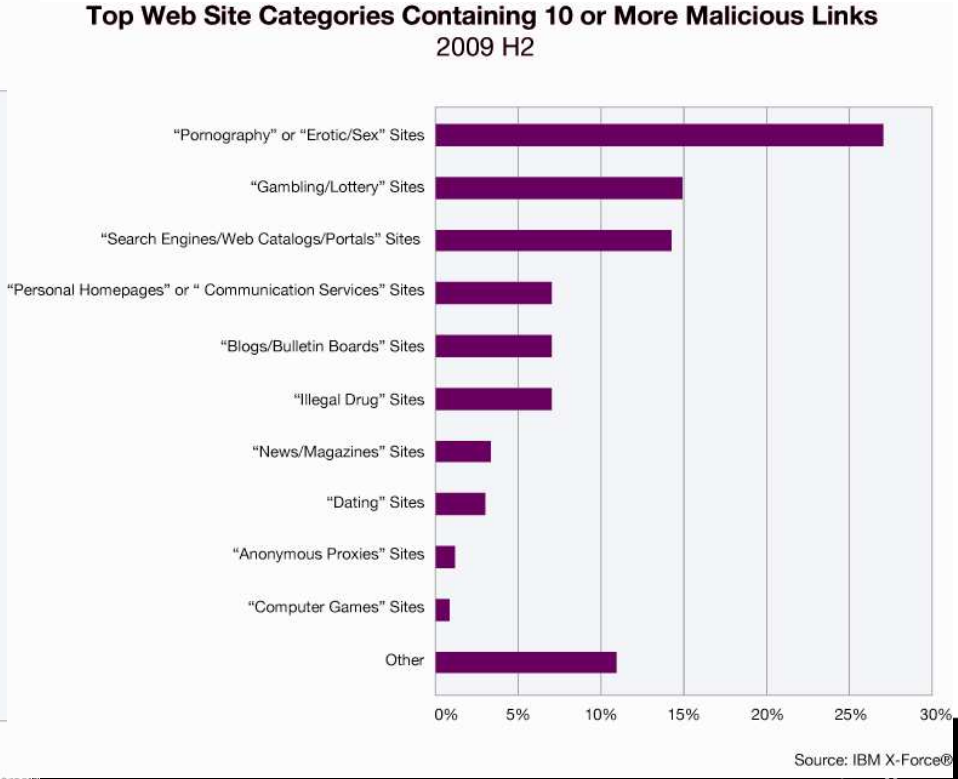


Created using **Wink**

„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%**



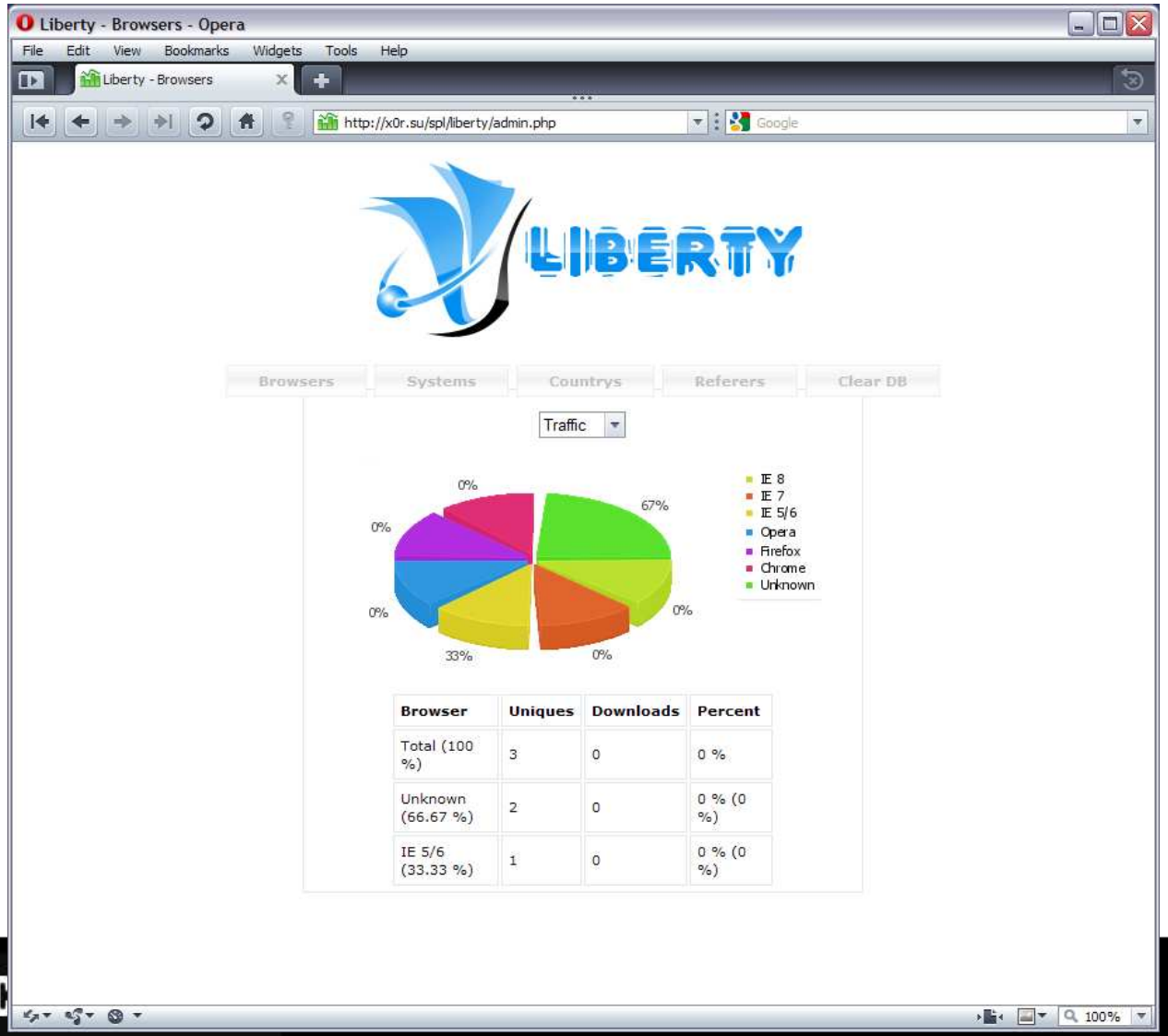


Każdy administrator IT powie:

- … u mnie działa

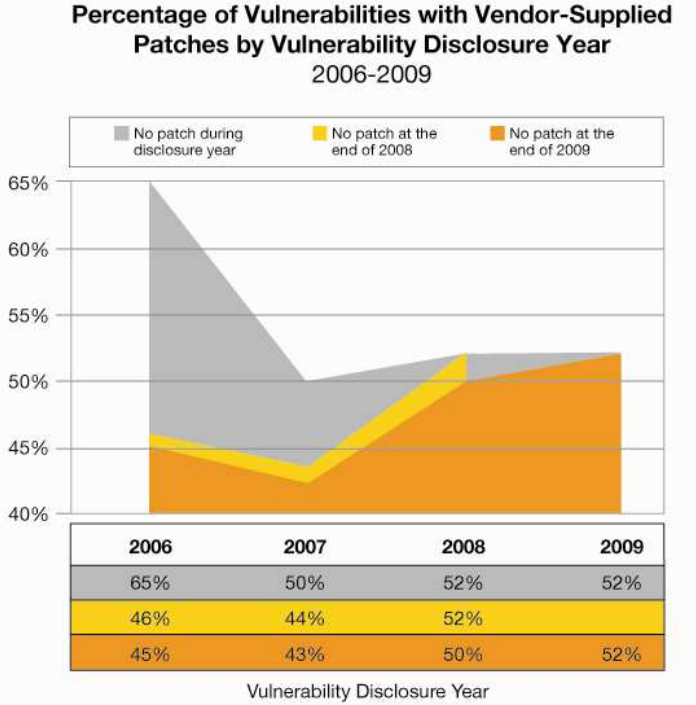
Pytanie czy systemy zabezpieczające mu w tym pomagają…

Celem ataków jest popularne oprogramowanie



W dalszym ciągu nie ma poprawek dla luk wyrytych 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 załatana (stan na koniec 2009).

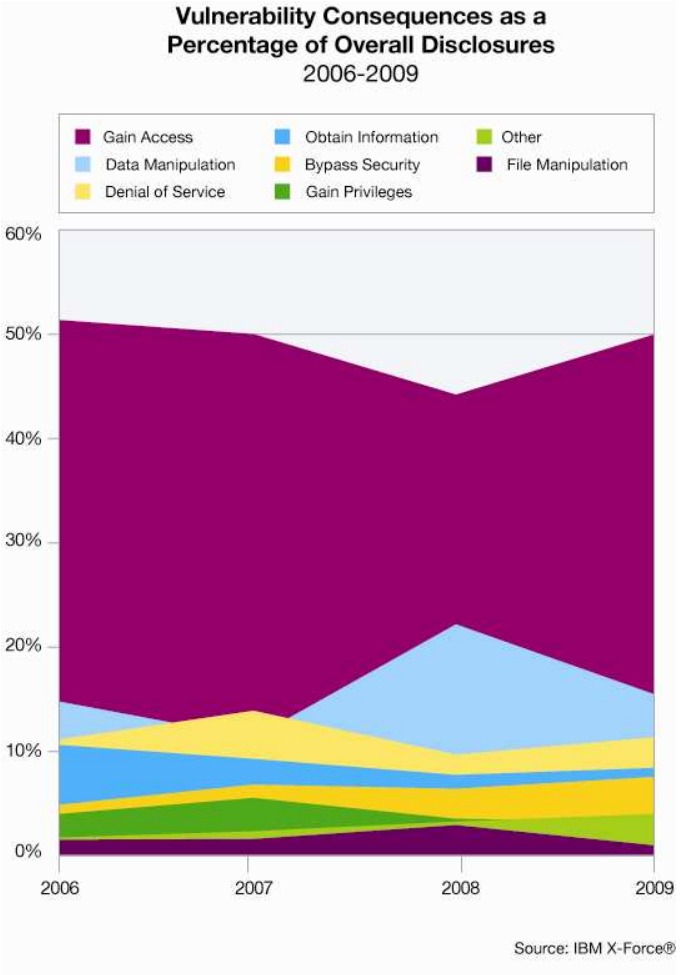


Vendor	Percent of 2009 Disclosures with No Patch	Percent of Critical & High 2009 Disclosures with No Patch
All Vendors– 2009 Average	52%	60%
Linux	50%	53%
Oracle	40%	38%
Novell	27%	31%
IBM	25%	27%
Google	47%	25%
Apple	14%	22%
Microsoft	29%	15%
Sun	7%	8%
Symantec	18%	7%
HP	16%	5%
Adobe	4%	4%
Cisco	11%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

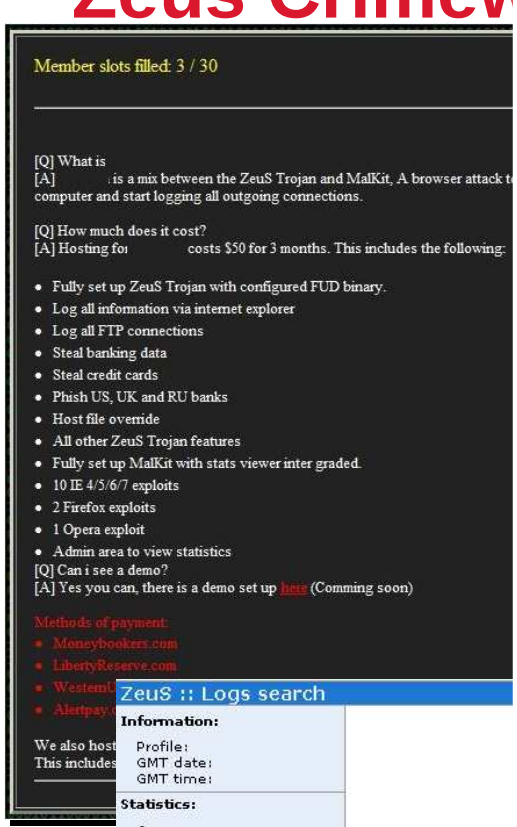


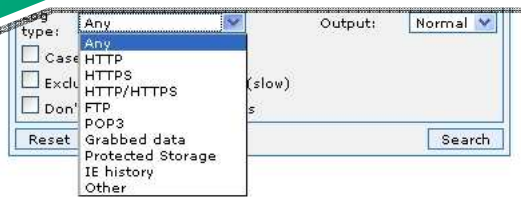
Zeus Crimew

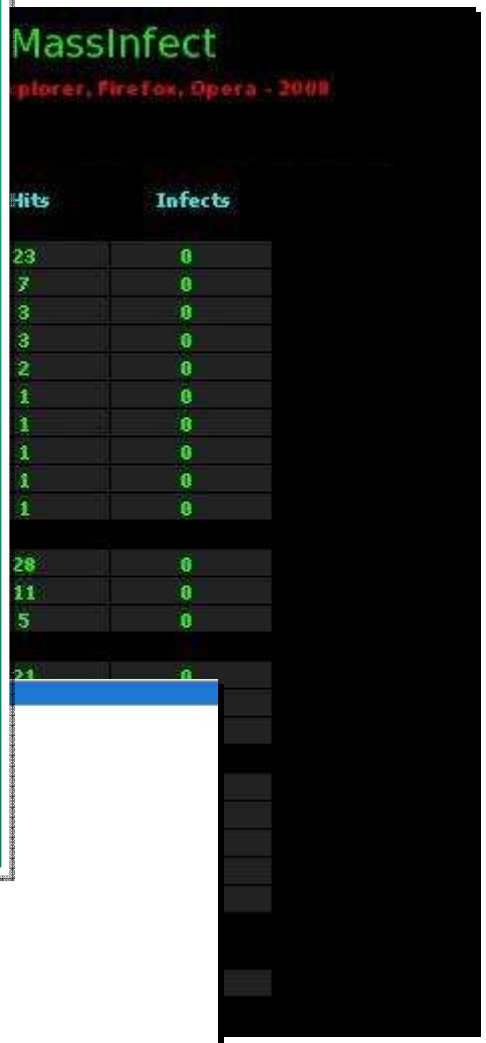
Hosting for costs **$50 for 3 months.**
This includes the following:

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

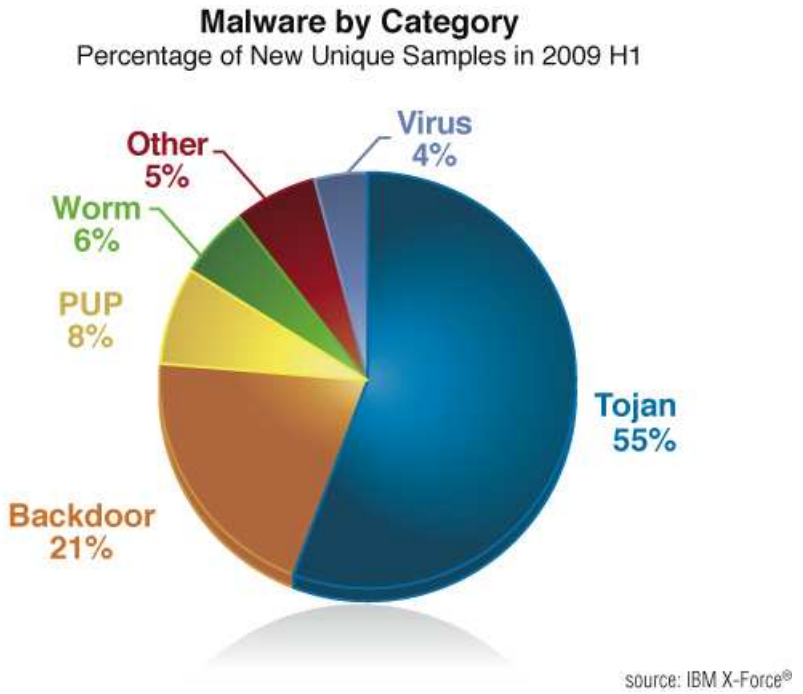






Większość wrogich kodów to Trojany

- 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**



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 avaliable with this version
- Realtime Screen viewing(controlling is disabled)
- Notifies changements 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 changements 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

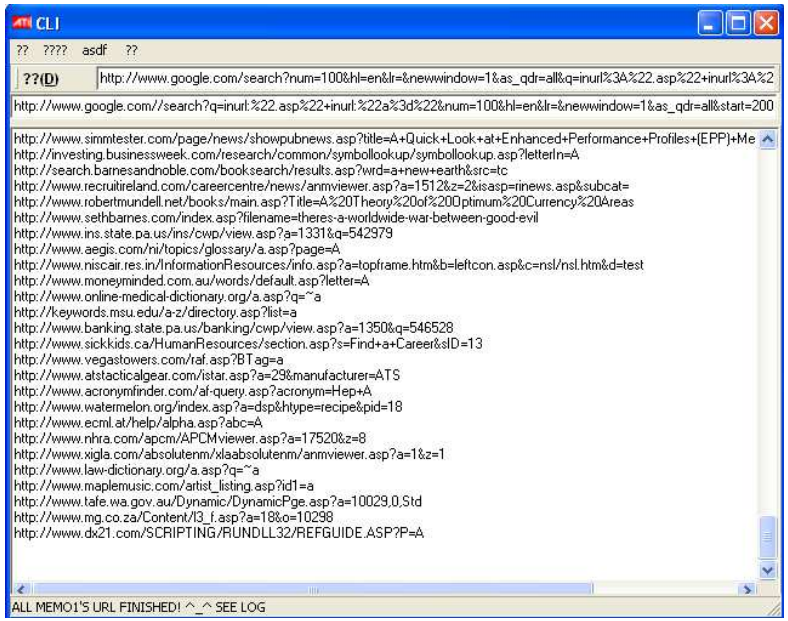
```
<Scan_Google> [milw0rm]  Joomla Component Expose <= RC
  Vulnerability - http://www.milw0rm.com/exploits/4194
<Scan_Google> [milw0rm]  QuickEStore <= 8.2 (insertorc
  Vulnerability - http://www.milw0rm.com/exploits/4193
<Scan_Google> [milw0rm]  Vivvo CMS <= 3.4 (index.php)
  Exploit - http://www.milw0rm.com/exploits/4192
<Scan_Google> [milw0rm]  Pictures Rating (index.php ms
  Vulnerbility - 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 Advisior (index.php ic
  Vulnerbility - 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] Exploting 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] Exploting 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**

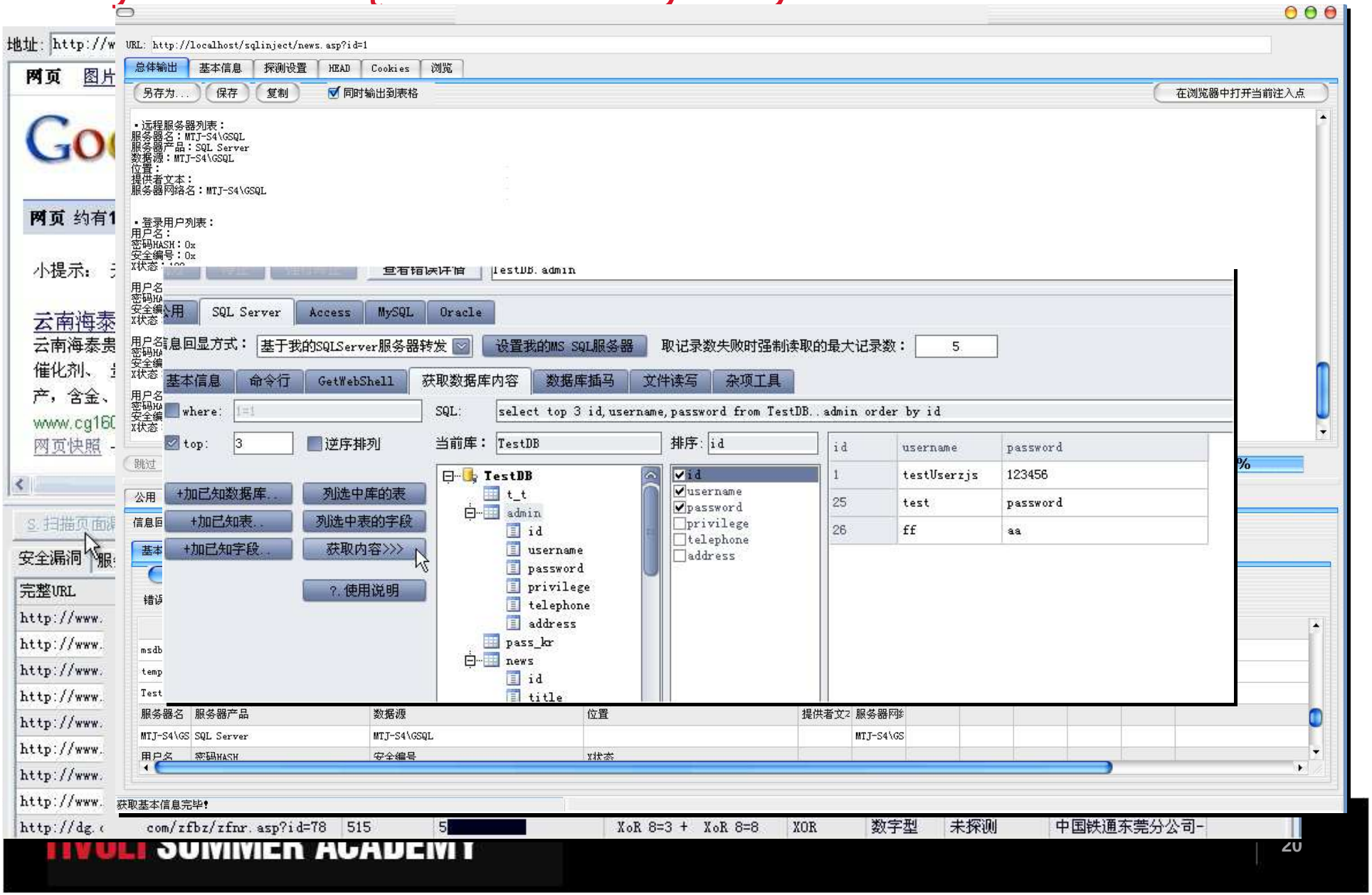
Narzędzi oparte o subskrypcje

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



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

Przykład narzędzi automatycznych



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?