LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

Garnkiem miodu w zombie

Detekcja, analiza, dns-blackholing sieci botnet.

Borys Łącki – Patryk Dawidziuk

http://www.logicaltrust.net

Pingwinaria - 2009

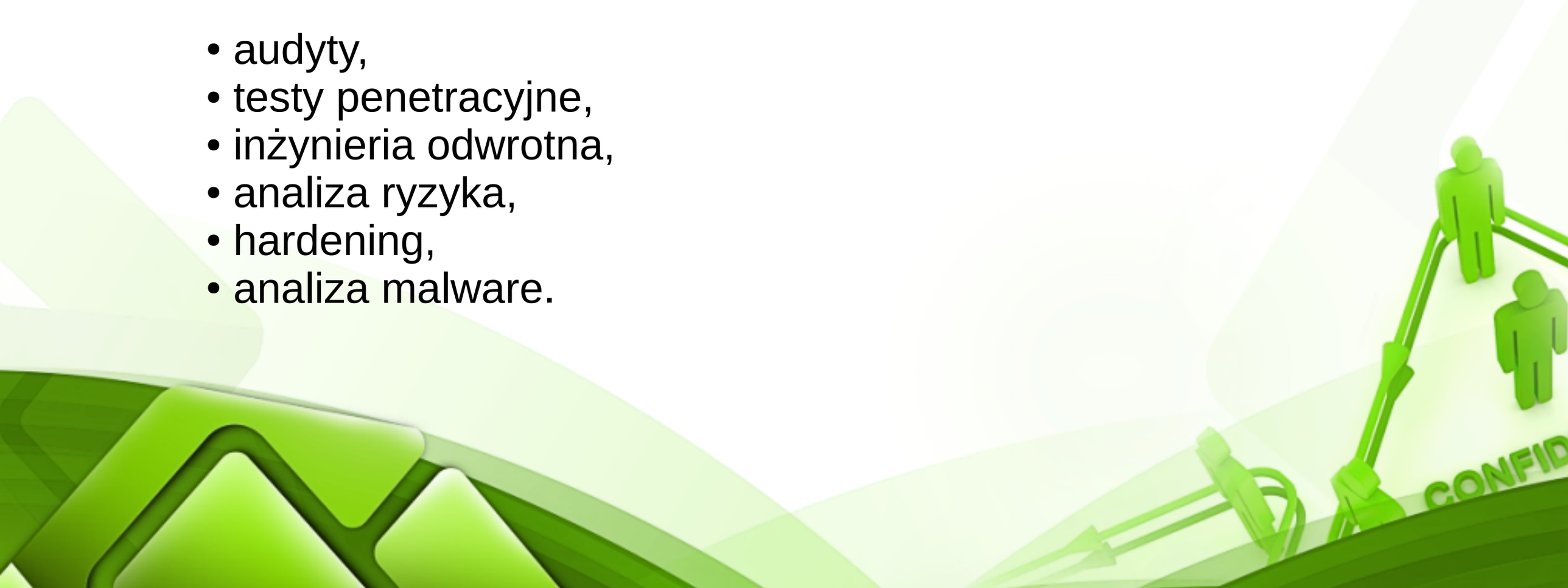
LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

LogicalTrust

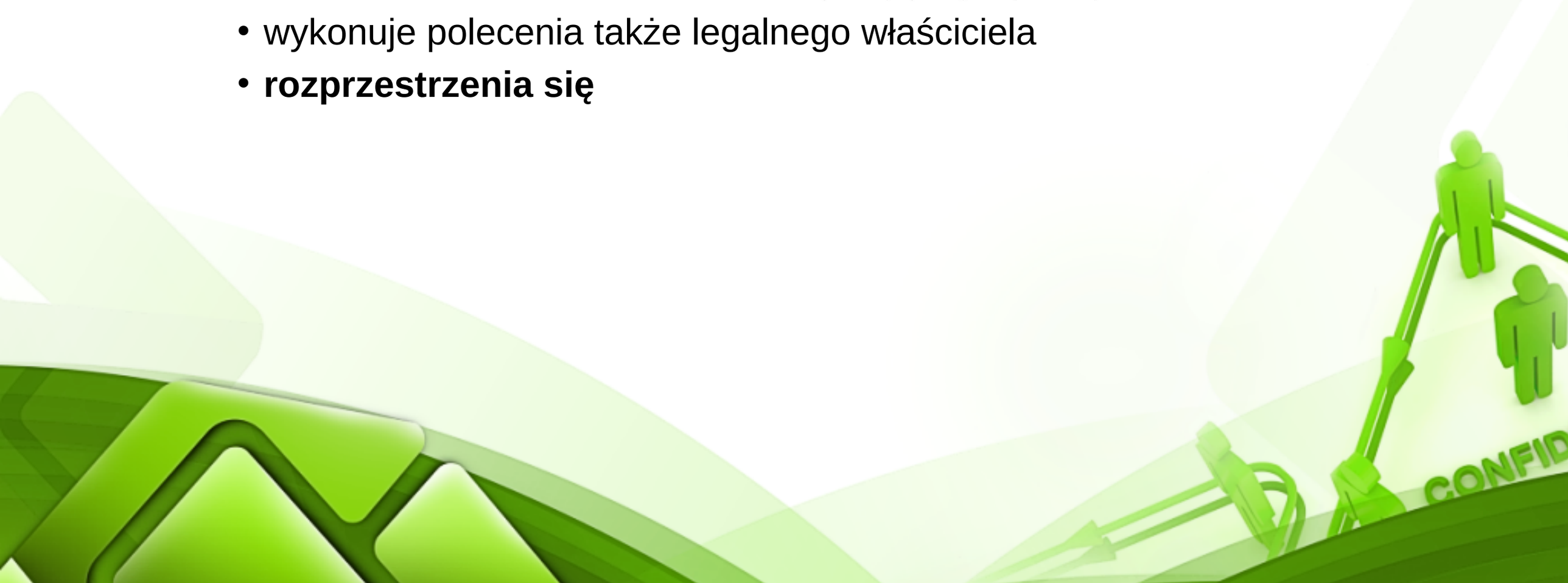
departament bezpieczeństwa IT Business Consulting Experts Sp. z o.o. świadczący usługi
w wybranych obszarach bezpieczeństwa IT.

- audyty,
- testy penetracyjne,
- inżynieria odwrotna,
- analiza ryzyka,
- hardening,
- analiza malware.



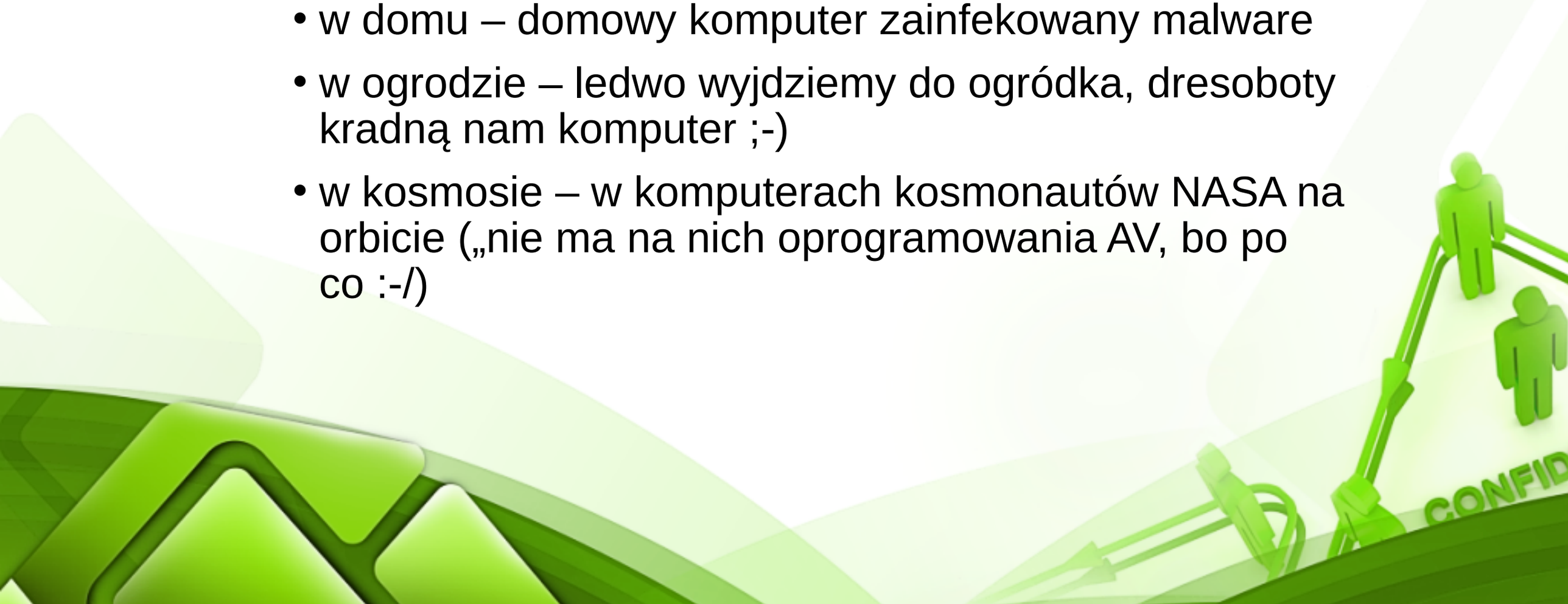
Podstawy teoretyczne

- co to jest botnet – informacje ogólne
  - armia komputerów zainfekowana trojanami (botami)
    - słucha rozkazów od serwera zarządzającego (C&C)
    - wykonuje polecenia także legalnego właściciela
    - **rozprzestrzenia się**



Podstawy teoretyczne

- botnet wystepuje w domu, w ogrodzie i w kosmosie
  - w domu – domowy komputer zainfekowany malware
  - w ogrodzie – ledwo wyjdziemy do ogródka, dresoboty kradną nam komputer ;-)
  - w kosmosie – w komputerach kosmonautów NASA na orbicie („nie ma na nich oprogramowania AV, bo po co :-/)



LogicalTrust
www.logicaltrust.net

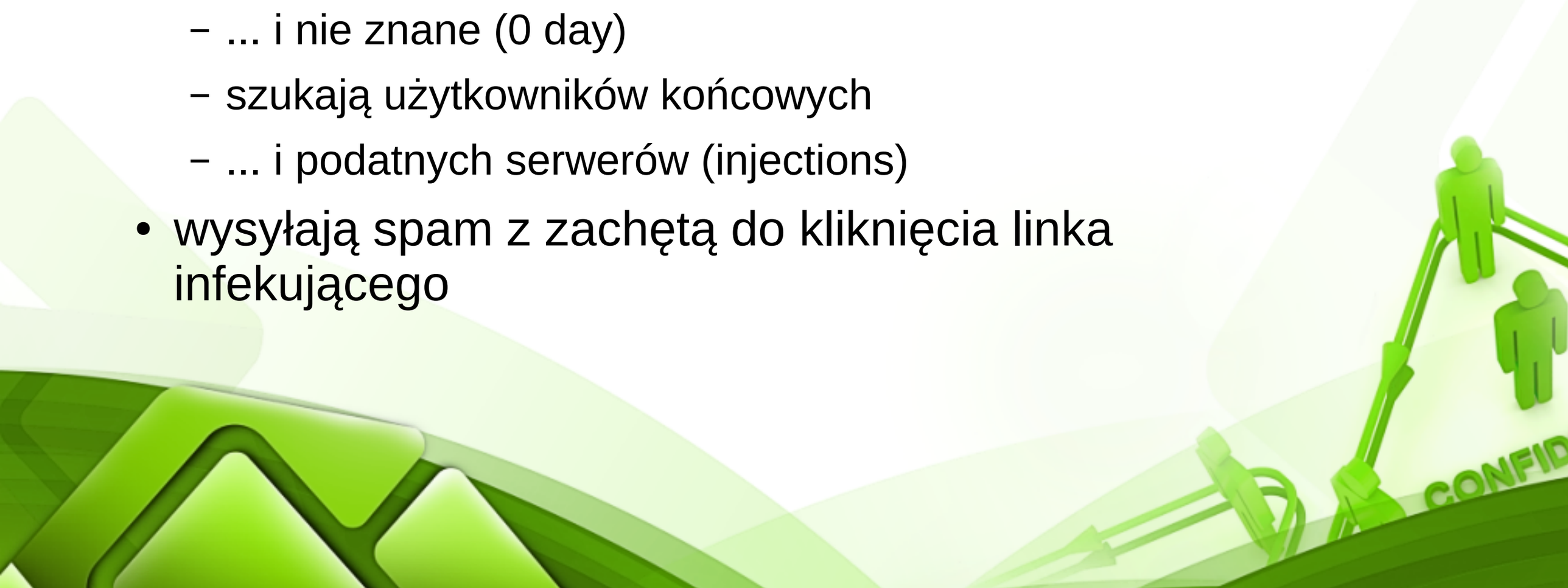
IT BCE BUSINESS CONSULTING EXPERTS

Podstawy teoretyczne

„poznacie ich po owocach (...)” Mat. 7:16

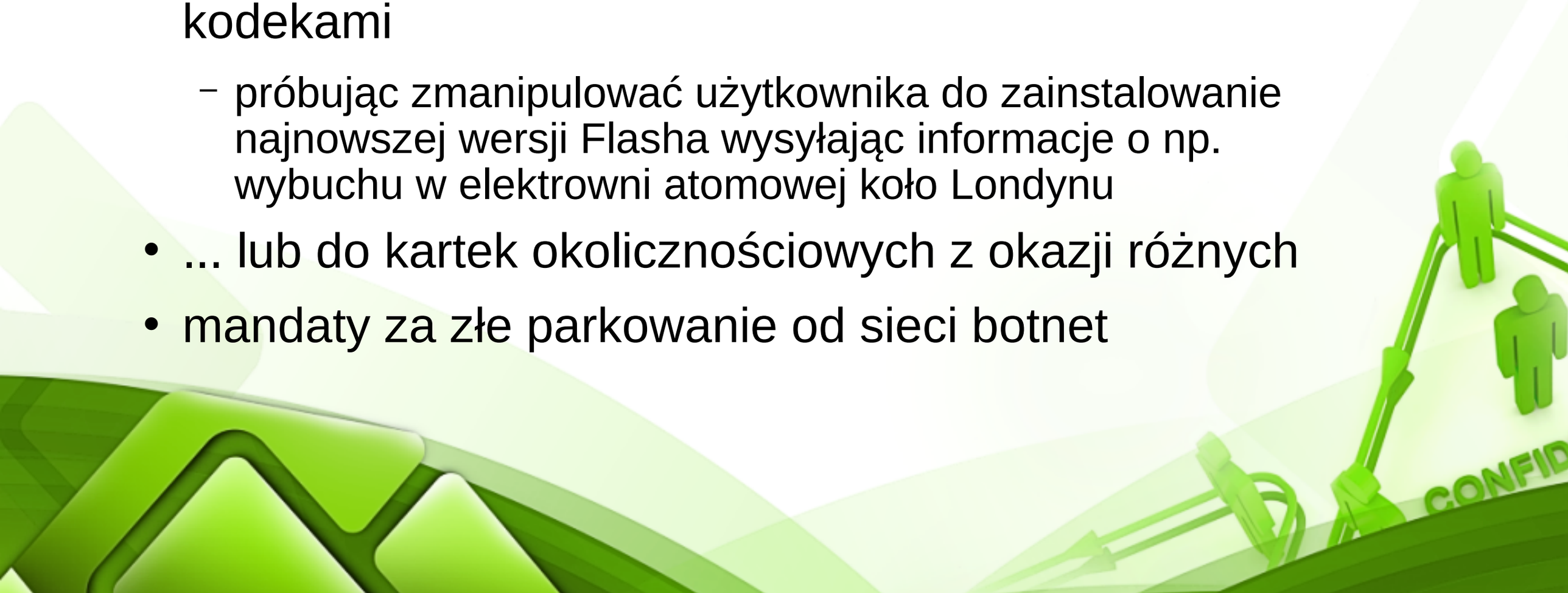
Podstawy teoretyczne

- boty skanują adresy IP w poszukiwaniu podatności na ataki
  - wykorzystują luki znane
  - ... i nie znane (0 day)
  - szukają użytkowników końcowych
  - ... i podatnych serwerów (injections)
- wysyłają spam z zachętą do kliknięcia linka infekującego



Podstawy teoretyczne

- coraz rzadziej wysyłają maile ze złośliwymi załącznikami
- coraz częściej wysyłają linki do stron z fałszywymi kodekami
  - próbując zmanipulować użytkownika do zainstalowanie najnowszej wersji Flasha wysyłając informacje o np. wybuchu w elektrowni atomowej koło Londynu
- ... lub do kartek okolicznościowych z okazji różnych
- mandaty za złe parkowanie od sieci botnet

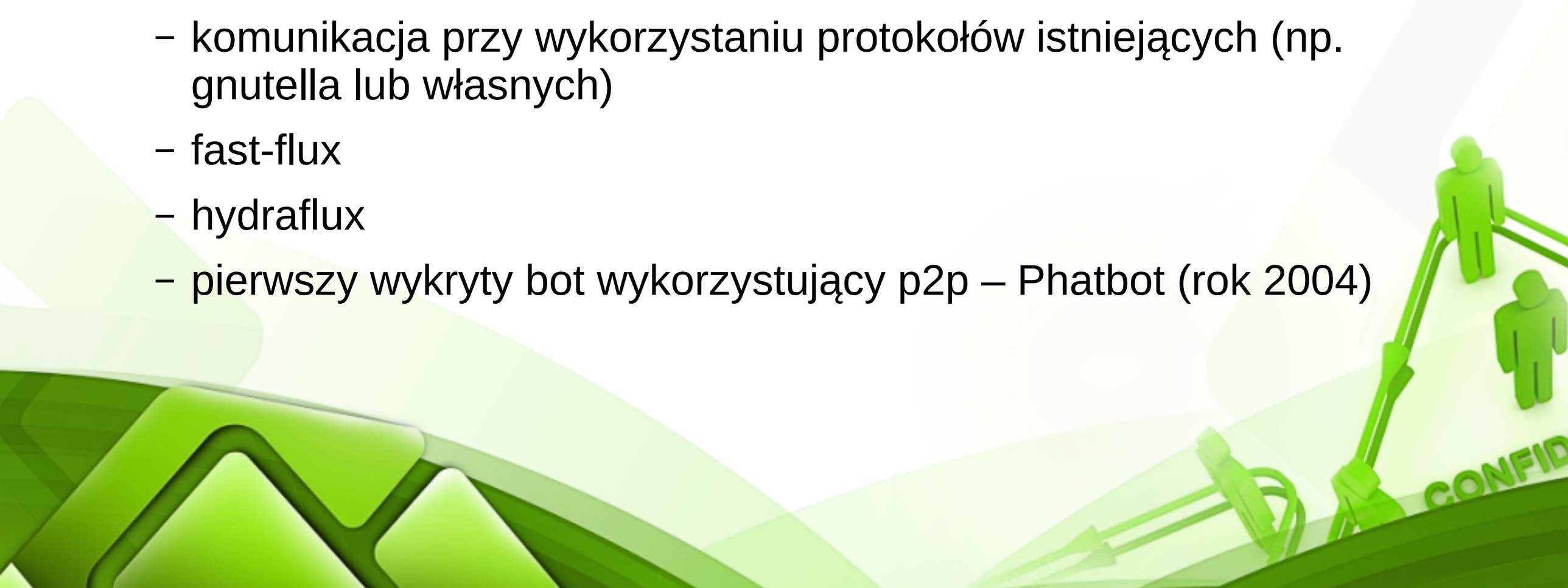


Topologie sieci botnet

- scentralizowana – boty łączą się do centrum zarządzania (serwer Command and Control, C&C) i słuchają rozkazów
  - komunikacja przy wykorzystaniu protokołów http oraz irc

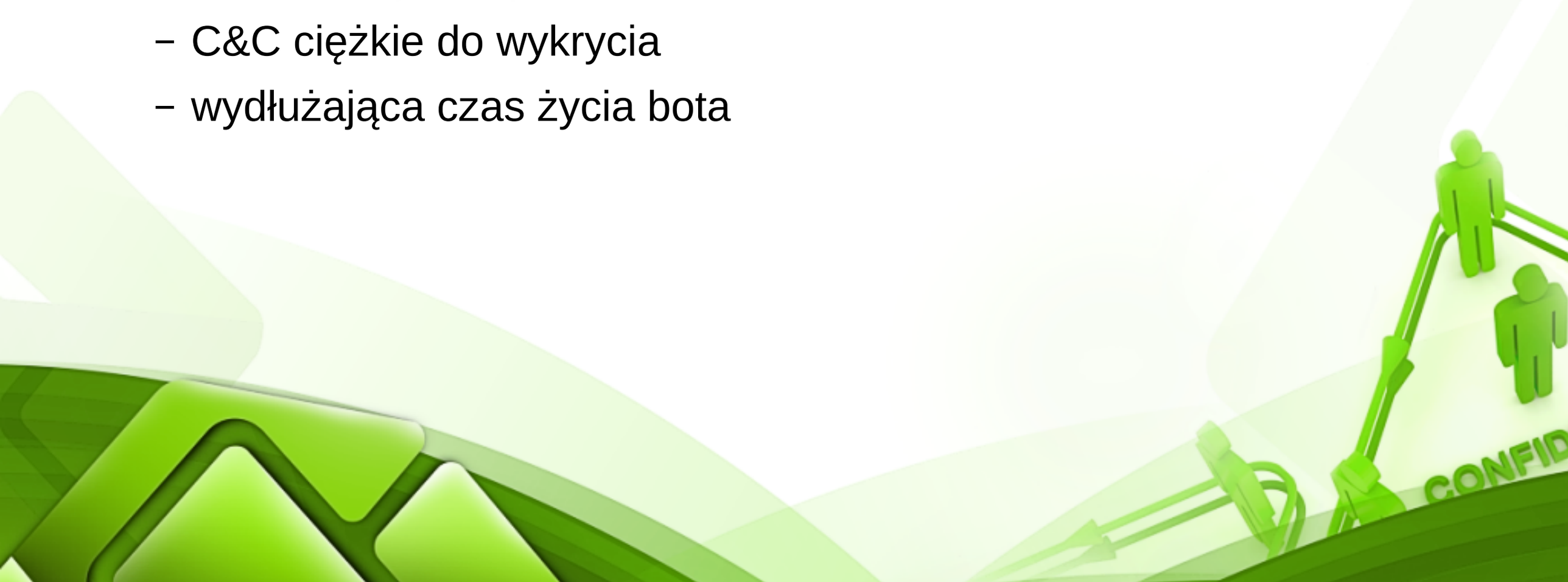
Topologie sieci botnet

- peer-to-peer (p2p) – boty łączą się do wykrytych innych pośredników w sieci – w efekcie docierają do centrum zarządzania
  - komunikacja przy wykorzystaniu protokołów istniejących (np. gnutella lub własnych)
  - fast-flux
  - hydraflux
  - pierwszy wykryty bot wykorzystujący p2p – Phatbot (rok 2004)



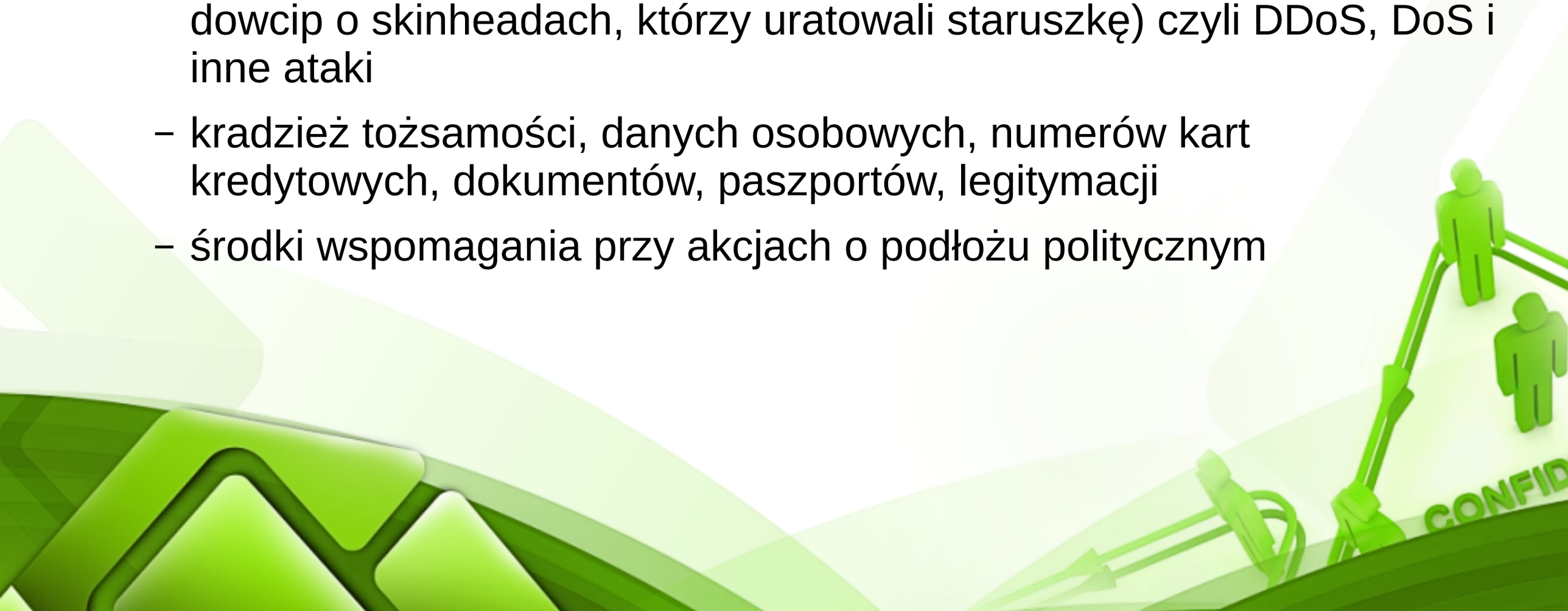
Topologie sieci botnet

- przypadkowa (random) – jest to topologia przyszłości, którą badacze postrzegają jako następny krok w ewolucji botnetów
  - komunikacja w oparciu o ... ?
  - C&C ciężkie do wykrycia
  - wydłużająca czas życia bota



Podstawy teoretyczne

- zalety posiadania botnetu
  - spam, phishing, fraud
  - terroryzm (“podobno macie problem z dostępem do sieci”, patrz dowcip o skinheadach, którzy uratowali staruszkę) czyli DDoS, DoS i inne ataki
  - kradzież tożsamości, danych osobowych, numerów kart kredytowych, dokumentów, paszportów, legitymacji
  - środki wspomagania przy akcjach o podłożu politycznym

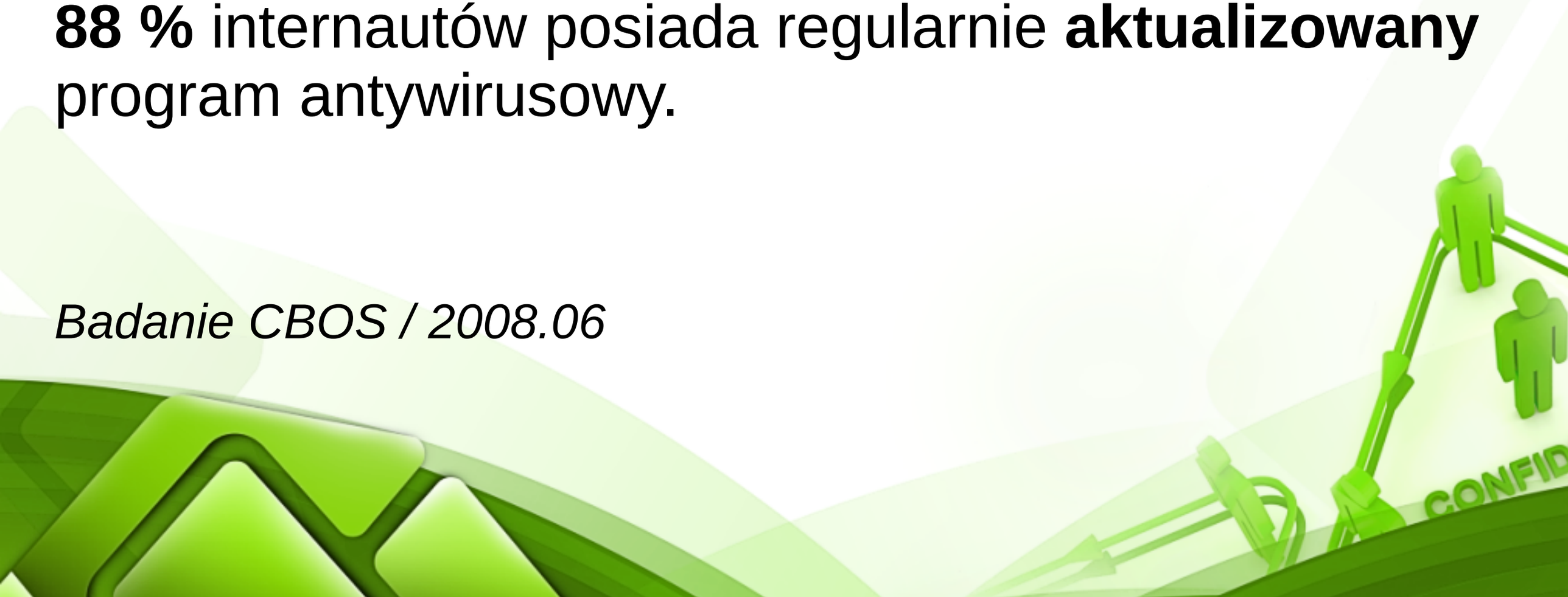


Bezpieczeństwo użytkowników

„Spokojnie, jesteśmy bezpieczni. Mamy antywirusa...”

88 % internautów posiada regularnie **aktualizowany** program antywirusowy.

Badanie CBOS / 2008.06



Bezpieczeństwo użytkowników, NOT!

LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

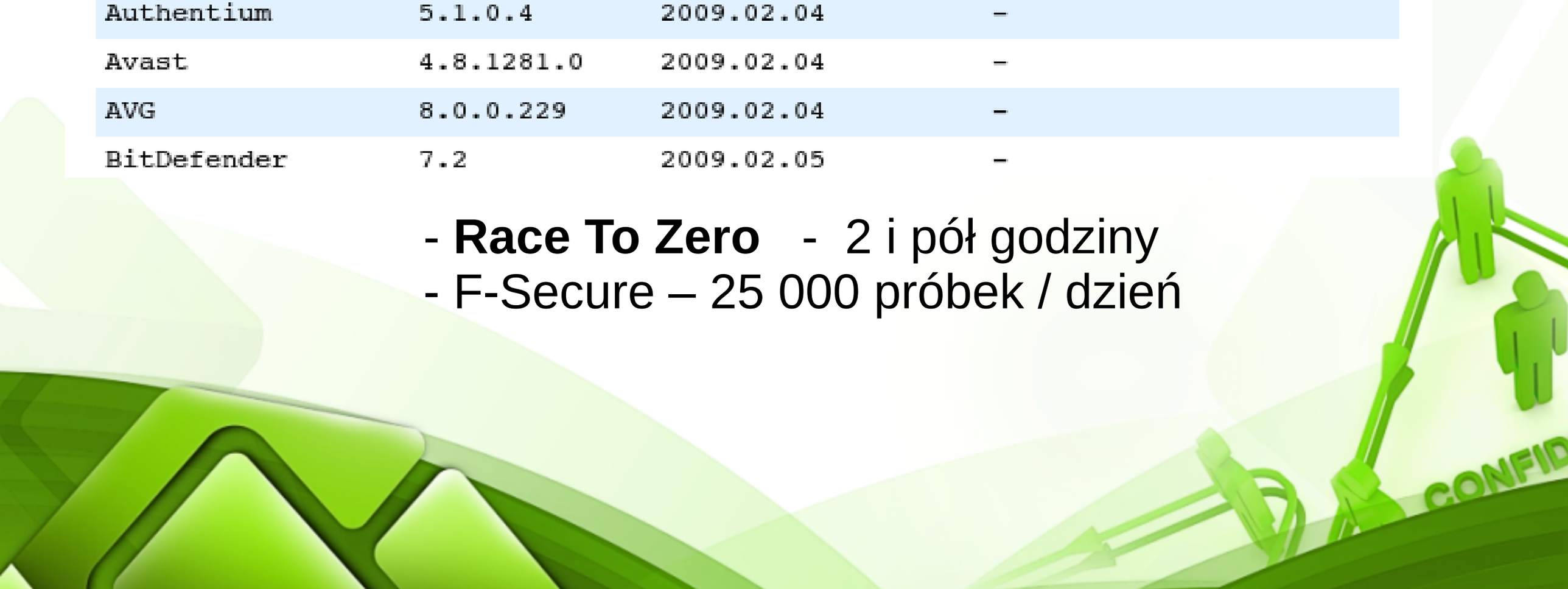
Plik **services.exe** otrzymany **2009.02.05 10:57:20 (CET)**
Obecny status: **zakończono**
Wynik: **9/39 (23.08%)**

Zwięzły

Drukuj wyniki

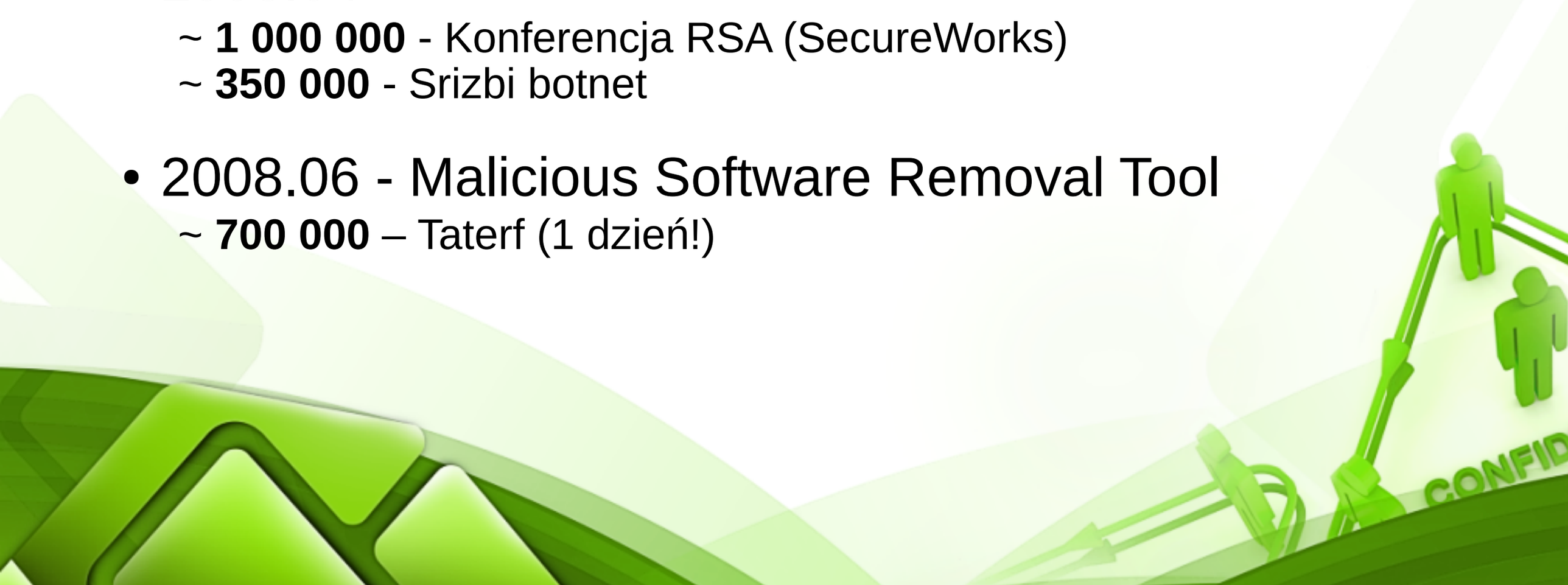
Antywirus	Wersja	Ostatnia aktualizacja	Wynik
a-squared	4.0.0.93	2009.02.05	Virus.Win32.PePatch!IK
AhnLab-V3	5.0.0.2	2009.02.05	-
AntiVir	7.9.0.74	2009.02.05	-
Authentium	5.1.0.4	2009.02.04	-
Avast	4.8.1281.0	2009.02.04	-
AVG	8.0.0.229	2009.02.04	-
BitDefender	7.2	2009.02.05	-

- **Race To Zero** - 2 i pół godziny
- F-Secure – 25 000 próbek / dzień

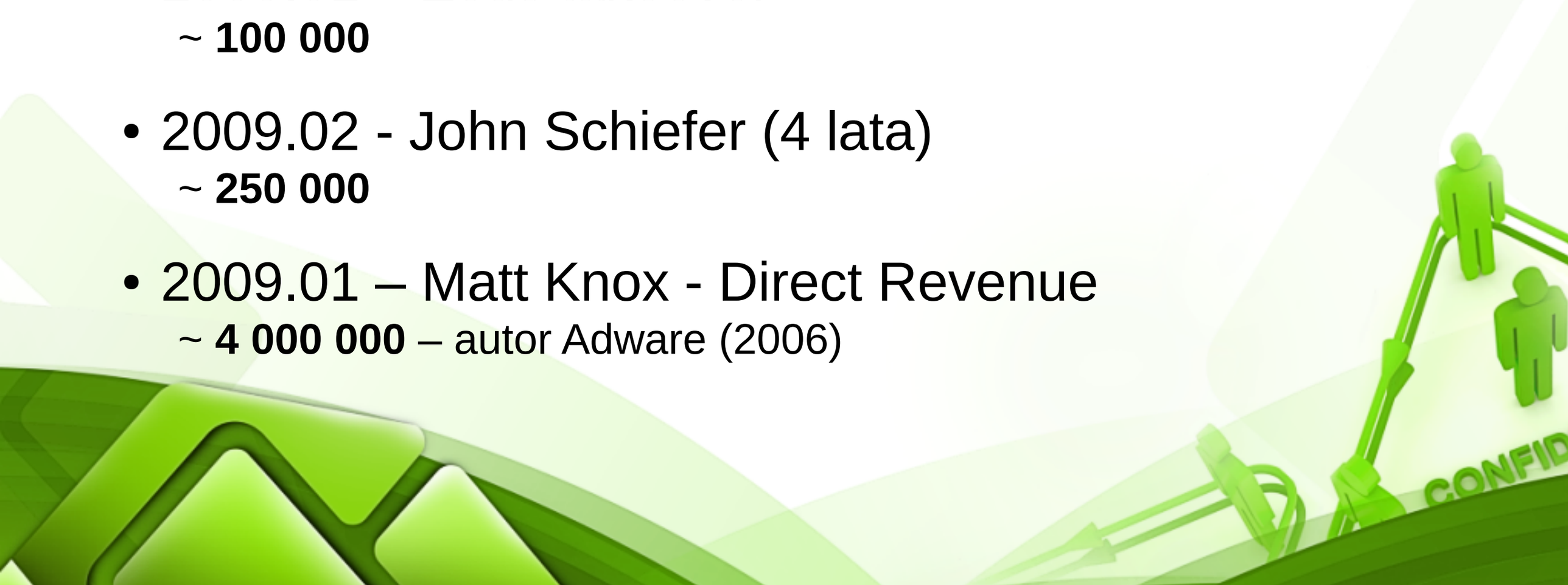


Fakty

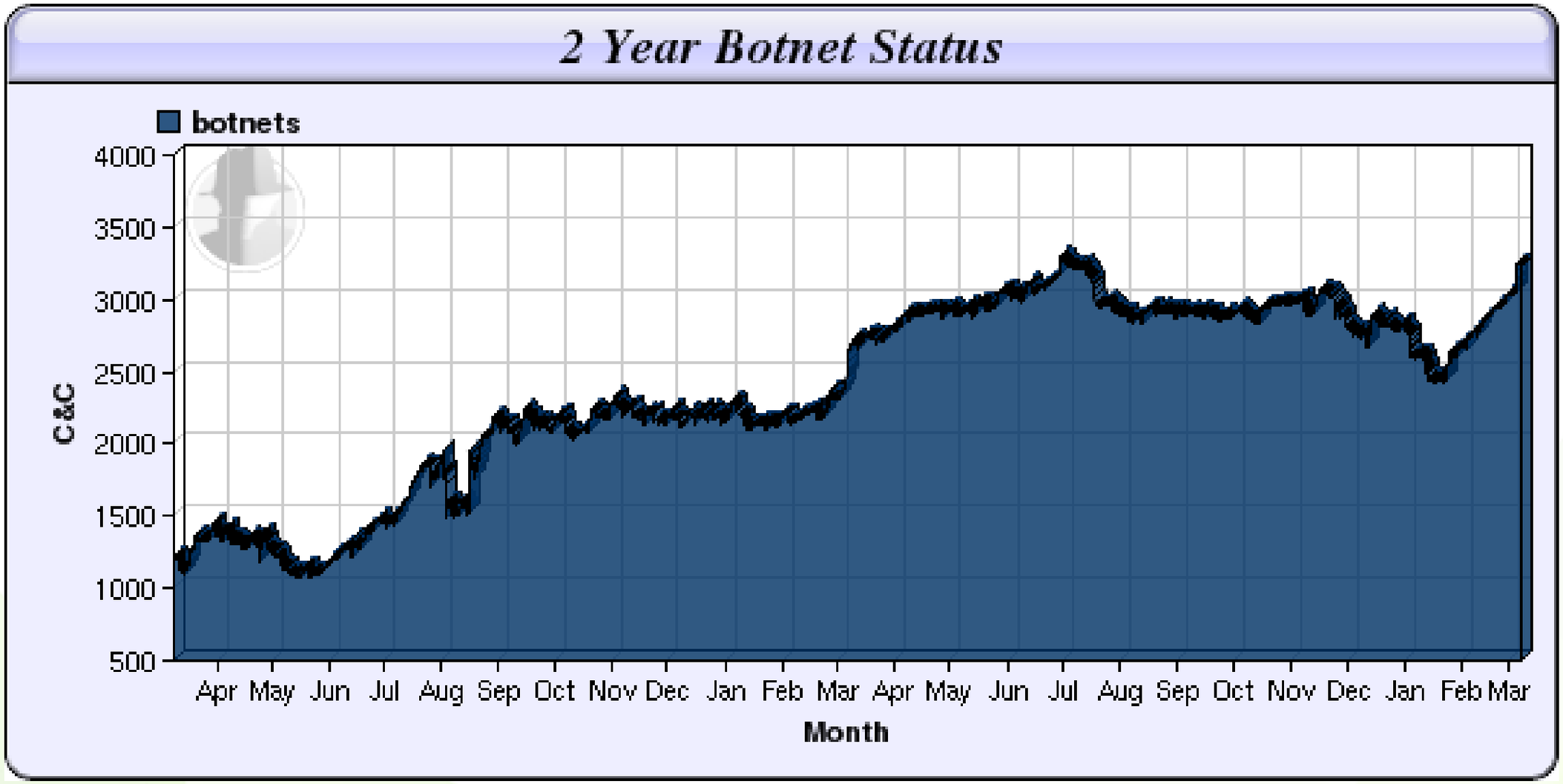
- 2007.11 – Owen Thor Walker (18 latek)
  ~ **1 300 000**
- 2008.03 – Kraken/Bobax botnet
  ~ **400 000** zainfekowanych maszyn
- 2008.04
  ~ **1 000 000** - Konferencja RSA (SecureWorks)
  ~ **350 000** - Srizbi botnet
- 2008.06 - Malicious Software Removal Tool
  ~ **700 000** – Taterf (1 dzień!)



- 2008.08 - Holandia
  ~ **100 000**
- 2008.12 - Malicious Software Removal Tool
  ~ **400 000** – Antivirus 2009
- 2009.01 – Zeus takeover
  ~ **100 000**
- 2009.02 - John Schiefer (4 lata)
  ~ **250 000**
- 2009.01 – Matt Knox - Direct Revenue
  ~ **4 000 000** – autor Adware (2006)

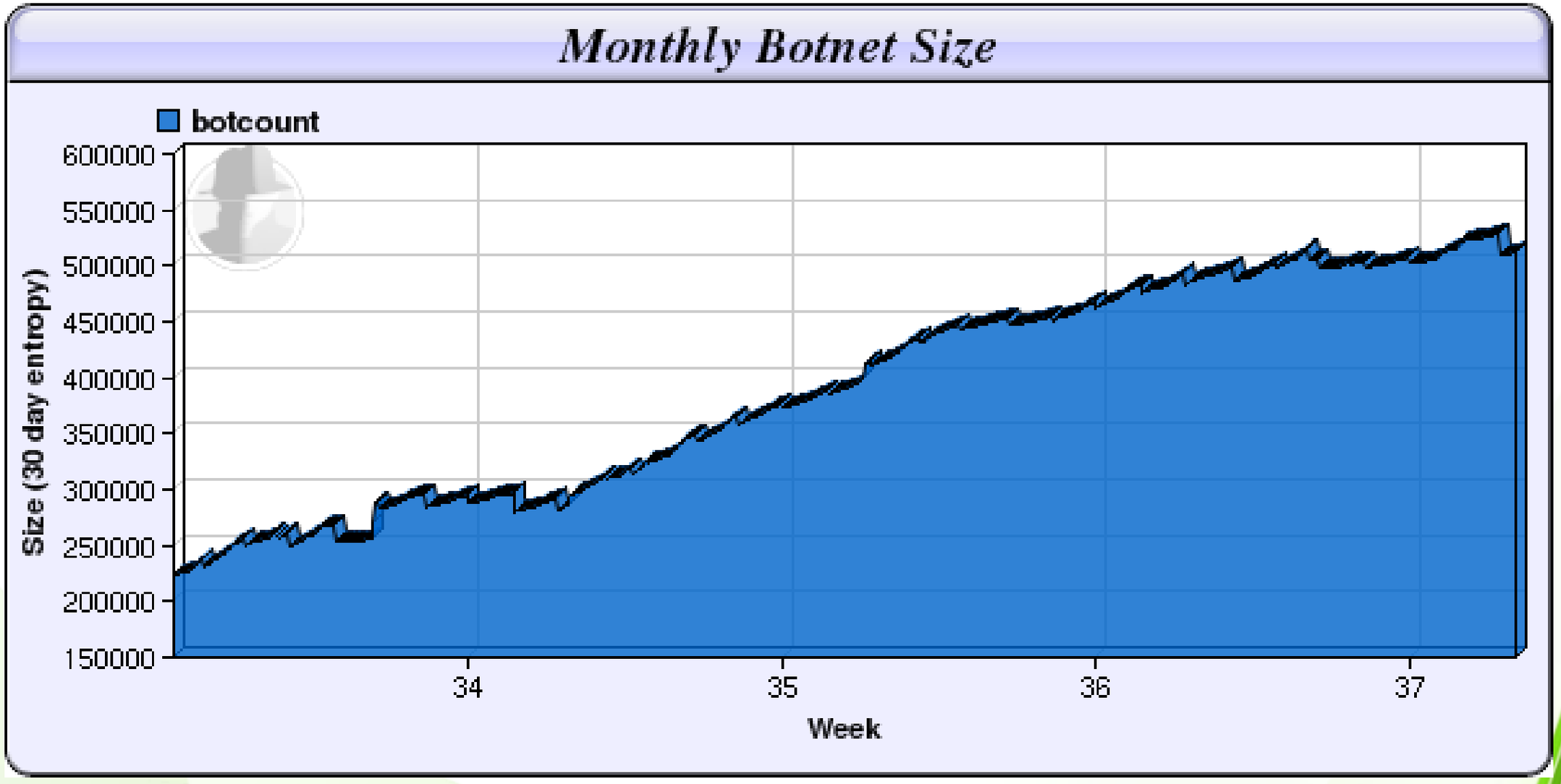


Fakty

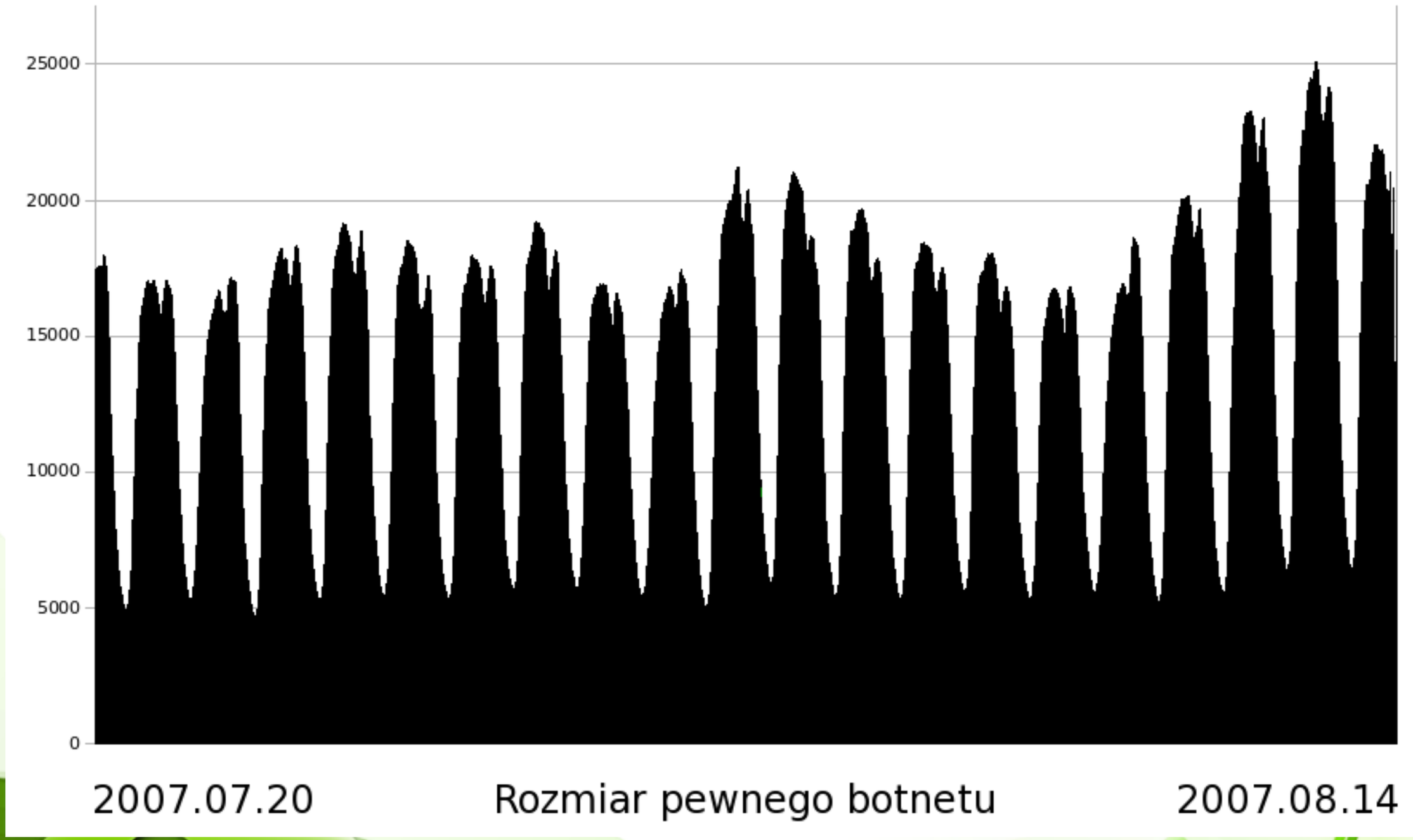


Źródło: www.shadowserver.org

Fakty



Źródło: www.shadowserver.org


25000
20000
15000
10000
5000
0
2007.07.20
Rozmiar pewnego botnetu
2007.08.14

LogicalTrust IT Security Solutions

SPAM

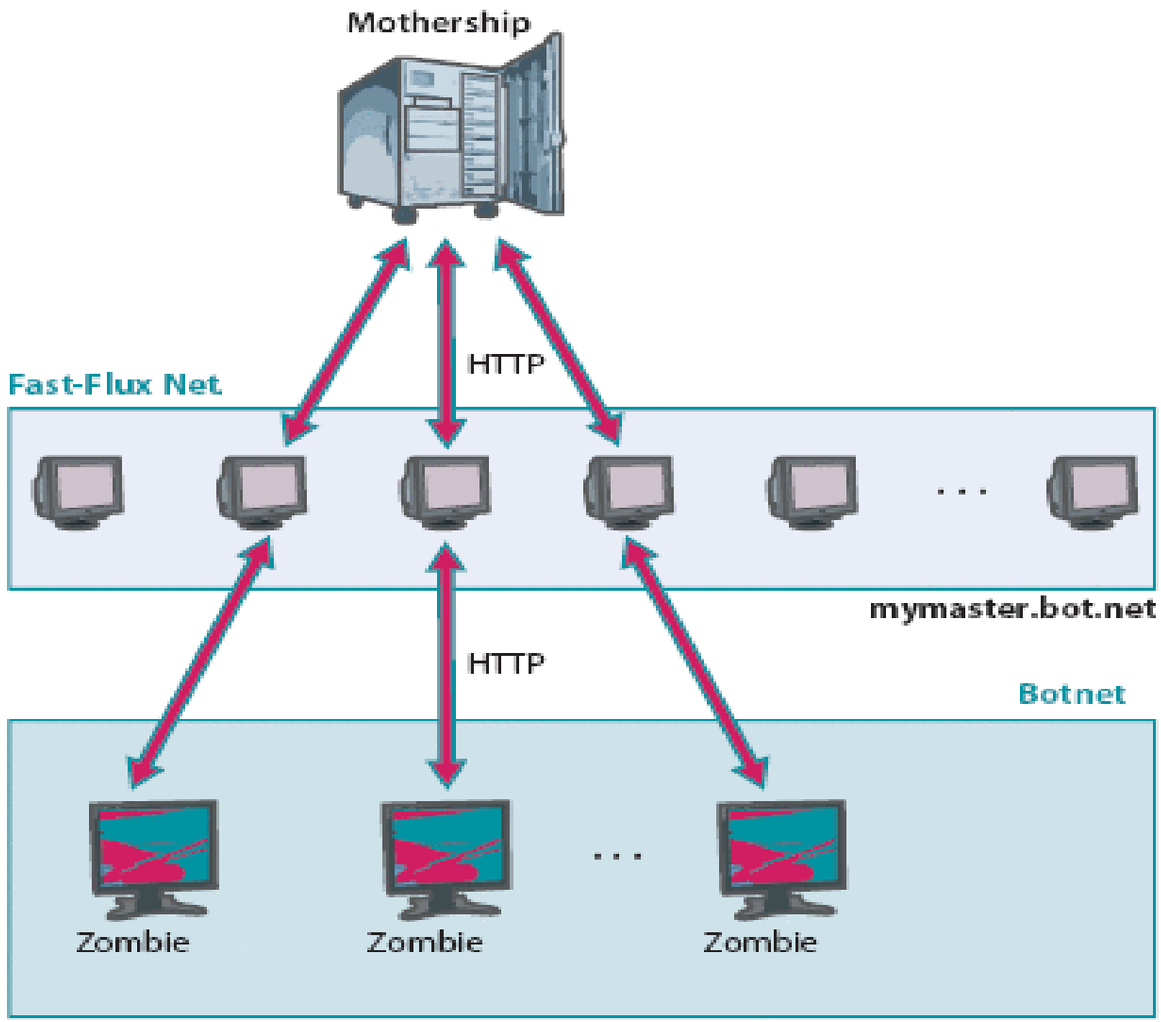
Upload: 256 Kb/s = 32 KB/s
1 spam = 11 KB
Średnia ilość botów: 13.862

32*13.862*3.600=159.690.240 KB /h = 156 GB /h
159.690.240/11=14.517.294 wiadomości typu spam /h

348.415.056 wiadomości typu spam / dziennie

Fakty

- FastFlux
- Hydra



+ P2P

Źródło: http://www.heise-online.pl

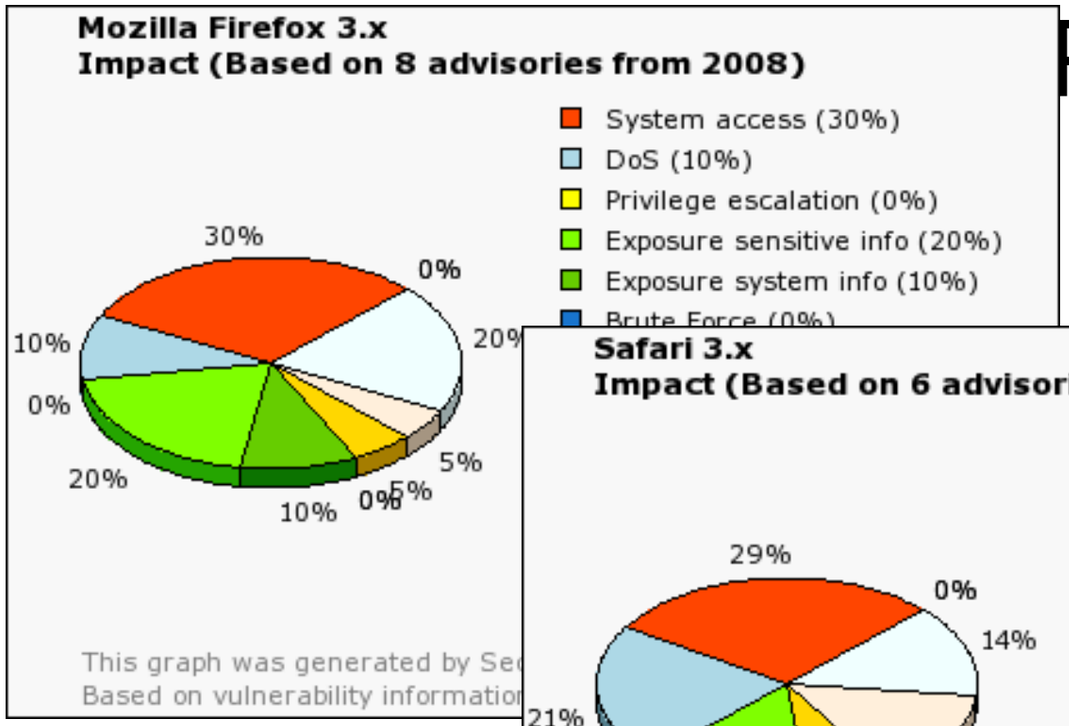
LogicalTrust
www.logicaltrust.net

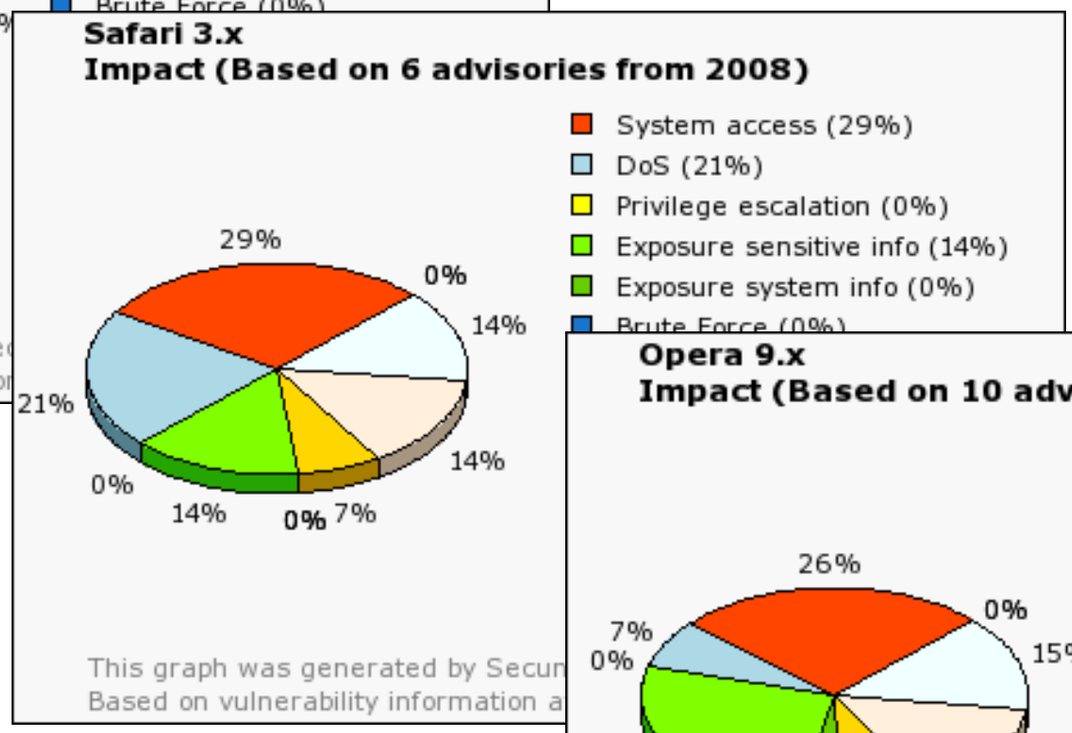
IT BCE BUSINESS CONSULTING EXPERTS

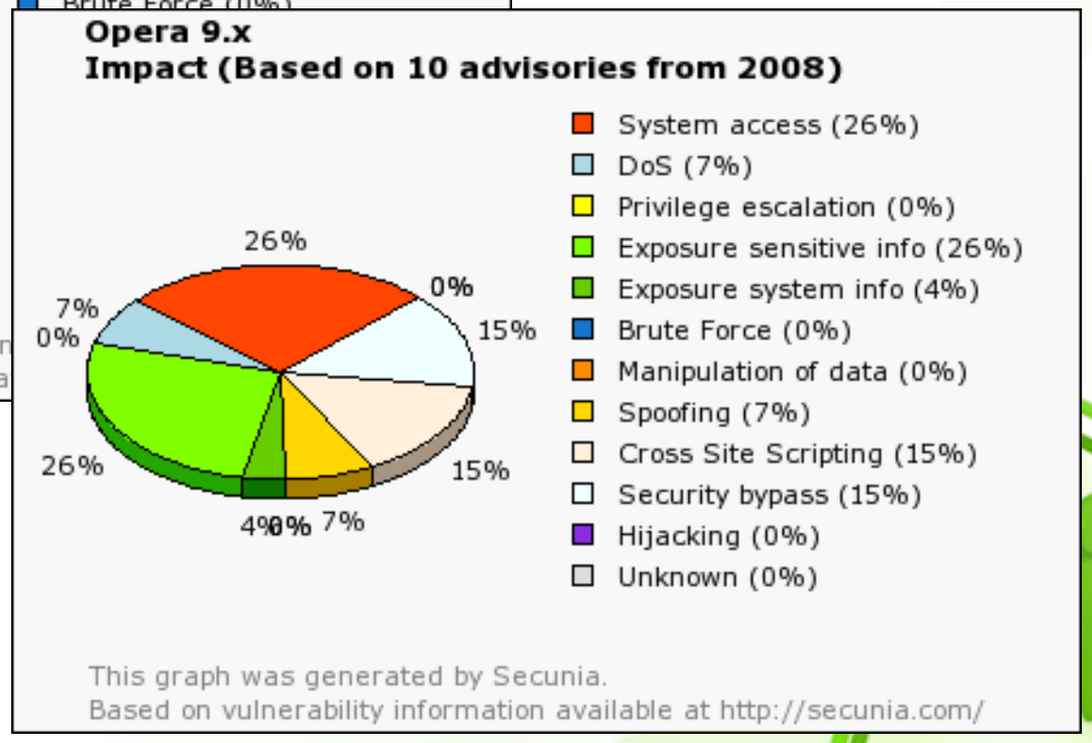
Fakty - WWW

„Alternatywy 4”

Fakty - WWW







- URL Handler Crash
- “SaveAs” stack-based overflow
- Automatic File Download
- Malicious link DoS
- Inspect Element DoS

Fakty - WWW

- **2008.03**

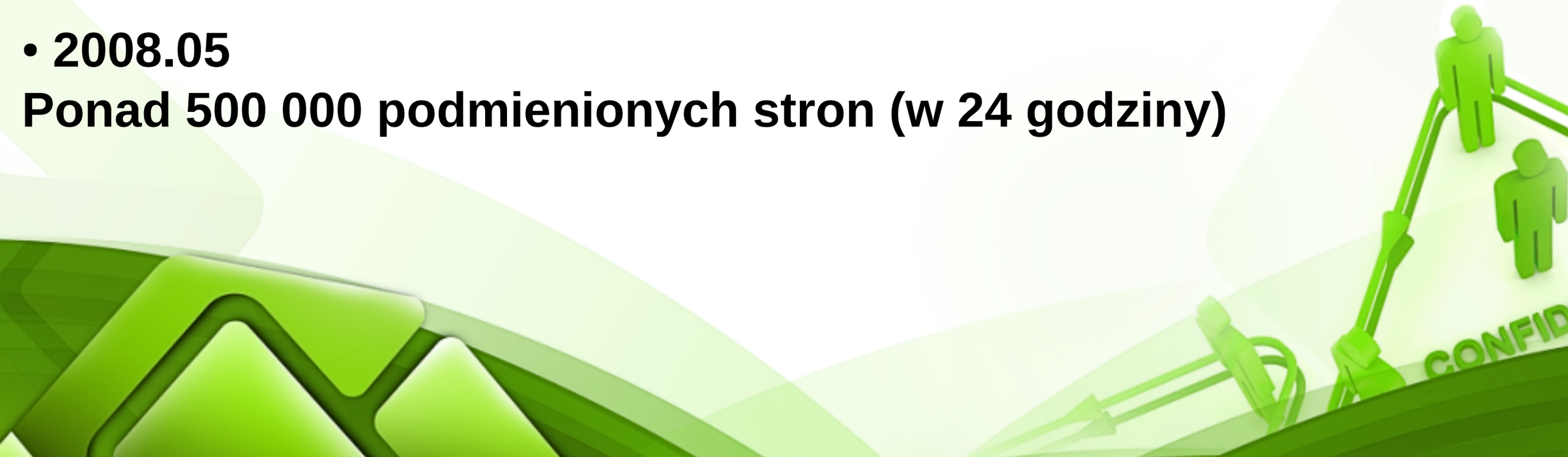
> 100 000 wyników wyszukiwarki Google zarażonych
(TV.com, News.com, ZDNetAsia.com)

- **2008.04**

Niebezpieczna reklama Flash w serwisie USATODAY.com

- **2008.05**

Ponad 500 000 podmienionych stron (w 24 godziny)



LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

„Botnet FastFluxowy każdy z nas ma... Mam i ja...”

Narzędzia

- **cuteQQ** - multi rootkit (400 – 3000 Juanów | 120 – 900 zł)
- **Zeus** - multigenerator
- **MPack, Adrenaline** - Malware Kit [PHP]
- **DreamSystem** - zarządzanie sieciami botnet [WWW]
- **Xrumer** – Forum Spam

„Best price my friend, best price...” 50 – 1000 $

- Icepack, Firepack, Neosploit, Pinch, Tornado, Ultra Lite Pack, G-Pack, Exploit Multipackage, Death-Pack, Apophis, DoS 5.0, BlackEnergy , Fishing Bait, Limbo 2, MicroJoiner, My Poly Sploits, PhpSpy, Ring 0, Shark 2, Turkojan 4.0, WOW Loader, Zunker.....

Narzędzia


Site:
ajcjobs.com
Login:
Password:
Search string:
Date (mm/dd/yy):
Job Location:
-- All --
Parse pages:
10000
Target email:
ajcjobs.com
aol
careerbuilder.com-proxy
careerbuilder.com-socks
careermag.com
hotjobs.
jobcontr
jobvertis
militaryhi
monster
newmor
newmor
seek.cor
Pinch 2 PRO builder
File About Build 2.60
Default
create
load
pinch 2 pro
SMTP HTTP FILE
Protocol
SMTP HTTP FILE
Status check str:
_ret_ok_1
BD
etc
Kill
IRC-bot
Values
KEY System
DLL ssmc.dll
EXE svchost.exe
SVC ServiceName
DIS ServiceDiscript
after:
time
12:12
when online
Bypass Windows Firewall (SP2)
UPX MEW
COMPILE
暗黑网马者 [Vip2008 Standard VerSion 3]
暗黑工作组
官方公告
其它功能
购买咨询QQ:784378237 (仅此一位,提防被骗)
会员验证
机器码
注册码
验 证
用 户
密 码
购 买
功能选项
智能性分析
延时性运行
智能化统计
破主动防御
破瑞星卡卡
破杀软拦截
破 IE 拦截
破 IE 监控
禁源码查看
禁右键点击
配置地址
木马地址:
存放地址:
http://请输入您网马的存放地址/
统计地址:
智能化检测
智能化除错
生成选项
Ms Access
Ms06014
Ms07004
Ms07055
Ms08011
Realplay11
Yahoo Exp
Google Exp
暴风影音
联众0day
迅雷网马
Realplayer
生成模式
.Gif模式
.Htm模式
服务状态
当前使用帐号:
会员开通日期:
当前使用版本:Vip2008 Standard VerSion 3.45
其它
关于程序
官方主站
官方论坛
在线更新
代码加密
挂马代码
暗黑网马者 [Vip2008 Standard VerSion 3] CopyRight (C) 2008 www.CuteQq.cn All Rights Reserved .

LogicalTrust

www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

Adware $

Czarny rynek $$$

```
<cUrl> 4,0[5,4]4,5[1,5]5,1[0,1 ...:::SELLING >>> HACKED HOST [((cPANEL + FTP))] (12
$)-//-PHP MAiLER 2 INBOX (8$)-//-c99/r57 SHELLS (9$)-//-EMAIL SPIDER GOLD V9 [((FUL
L VERSiON))] (30$)-//-PRIV8 PHP GOOGLE RFi SCANNER [((SCRIPT))] (26$)-//-PERL RFi S
CANNER [((SCRiPT))] (28$)-//-ANY WEB SCRiPT/TEMPLATE (55$)-//-MAILING LIST US/UK/IN
DIA (1mb 10$)-//-ALSO DESIGNING CUSTOM SCAM PAGEz (26$) !!! RiPPERS/TIME WASTERS/LO
NG TALKERS ---> DIE !! ONLY SERiOUS
<\2Legit> 9,1I Am 8,1Western1,8Union9,1 Confirmer Cashing Out Male Cvv2's With Dob
+ Ssn And Full Infos Also Need Paypal Drop Wtih Atm Debit Card For Instant Cashout
Msg Me For Deal.
<Geezer> 0,4 I am selling:- Declined Fullz + Fresh socks4/5 (any country) + All Sca
m Pages(BOA/PayPal/Aol/Hotmail/Yahoo) and others + DDsoHTTP with serial key - I acc
ept E-Gold == I need US unspammed fresh leads + CPanel
d luxmarket/#ccpower has requisite people for bulk cc orders, Needs direct supplier
s. your share is 50%
<Droper> contact me for any cashout in US,UK and Canada,through transfer and Billpa
y also pick up Wu&MG anyname,and i have drop for merchandise, need a good spammer f
or long term deal
<uznt> 4,1I have photos of these items: CCs(visa, mastercard), Drive licences(UK, m
ale, female), Passports(UK, male, female), student cards. Also have photos of China
, Mongolia, Russia, Vietnam Visas(documents, not cards). PM me
```

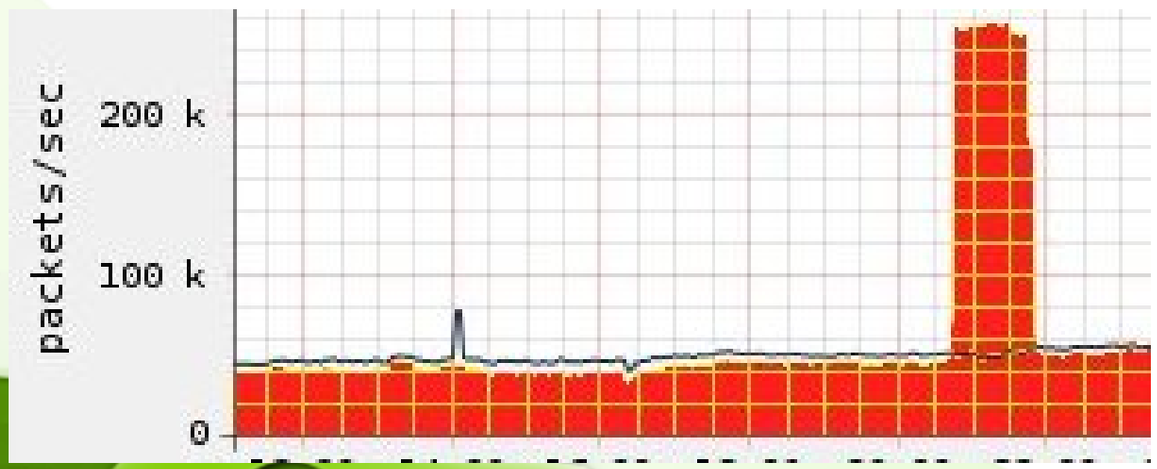
Czarny rynek $$$

2004 – Forrester - **20 %**
2008 – Marshal - **29 %**

... uczestników badania przyznało, że dokonało zakupów ze spamu

SPAM

1.000.000 wiadomości E-mail	5 – 10 $
10.000.000 wiadomości dziennie	600 $
1.000.000 wiadomości ICQ	150 $
1 wiadomość SMS	0.2 $



DDoS

1 godzina	10 $ - 20$
1 dzień	100 $
> 1 dzień	> 200 $
10 minut	free

LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

Czarny rynek $$$

BOTNET

400 000 maszyn 300 - 700 $

ADRESY E-mail

1.000.000	100 $
3.000.000	200 $
5.000.000	300 $
8.000.000	500 $
16.000.000	900 $
32.000.000	1500 $

ICQ 1 numer 1 - 10 $

FTP 1 konto 1 $

CAPTCHA

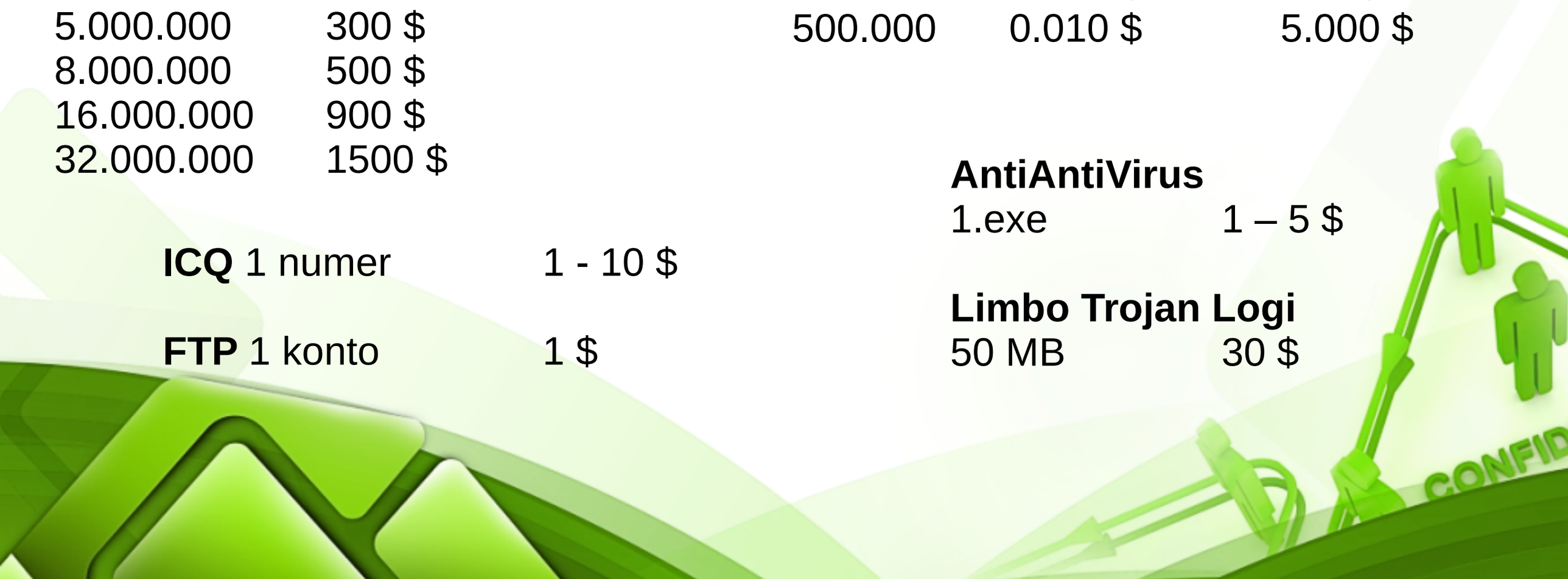
500	0.025 $	12.50 $
5.000	0.020 $	100 $
50.000	0.015 $	750 $
500.000	0.010 $	5.000 $

AntiAntiVirus

1.exe 1 – 5 $

Limbo Trojan Logi

50 MB 30 $



Zarobki $$$

DDoS:

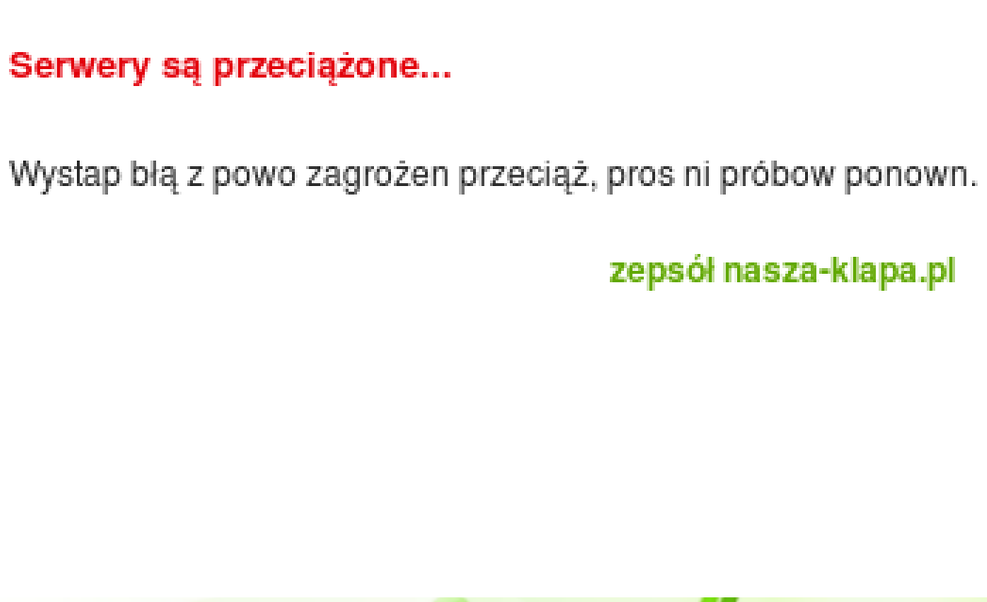
„Czy strona twojej firmy jest nadal niedostępna? Występuje problem z twoją stroną i oferujemy Wam rozwiązanie tego problemu. Koszt naprawy wynosi 480 000 jenów (~ 10 000 zł). Jeśli nie uiścicie opłaty, możecie spodziewać się dalszych problemów.”

Straty na poziomie 50 milionów jenów dziennie (1 mln zł) – tydzień!

(Atak o sile 6 GB/s)

- 2008.03

> 30.000 (PC i Mac) Wygenerowało ruch na poziomie **10 Gb/s**.



Zarobki $$$

Król wysyłania spamu - Scott Richter

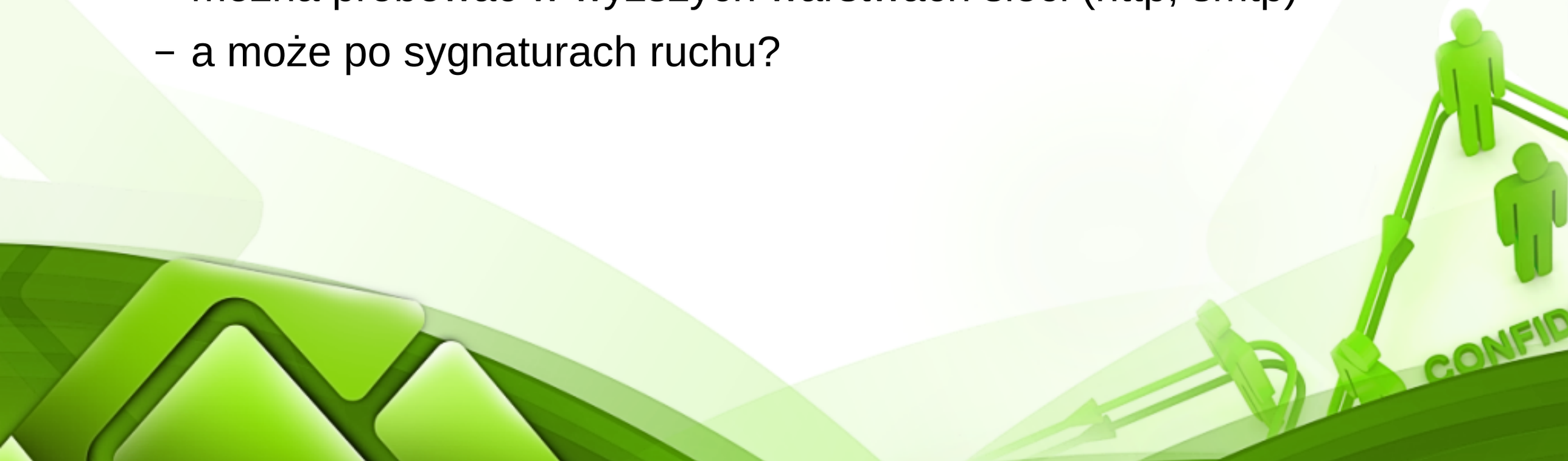
- 2004 – 50.000 $ grzywny na rzecz stanu - > Nowy Jork
- 2006 - zapłacił już 6.000.000 $ -> Microsoft
- 2008 – **6.000.000 $** -> MySpace

150 000 000 $ - przychody MyCanadianPharmacy.com
Pat Peterson (Cisco Systems)

- Wywiady [1 osoba !!!]
  - **Phisher:** 30.000 osób / 3000 - 4000 dolarów / dzień
  - **Spamer:** 10.000 - 15.000 dolarów / dzień

Detekcja

- sposoby wykrywania wrogiej działalności w sieci
  - boty skanują sieć, lokalną i każdą inną, w poszukiwaniu nowych ofiar
  - wykrycie (w dowolny sposób) skanowania sieci, najczęściej oznacza towarzystwo
  - można próbować w wyższych warstwach sieci (http, smtp)
  - a może po sygnaturach ruchu?



Detekcja

- wykrycie dużej ilości wysyłanego spamu także oznacza „towarzystwo” (spamdetector.sh !)

15:50:12.015918 IP xxx.xxx.xxx.xxx.57393 > 89.111.176.249.25

15:50:12.060454 IP xxx.xxx.xxx.xxx.56817 > 217.10.192.250.25

15:50:12.078871 IP xxx.xxx.xxx.xxx.57687 > 217.23.155.56.25

15:50:12.179452 IP xxx.xxx.xxx.xxx.57016 > 81.1.214.103.25

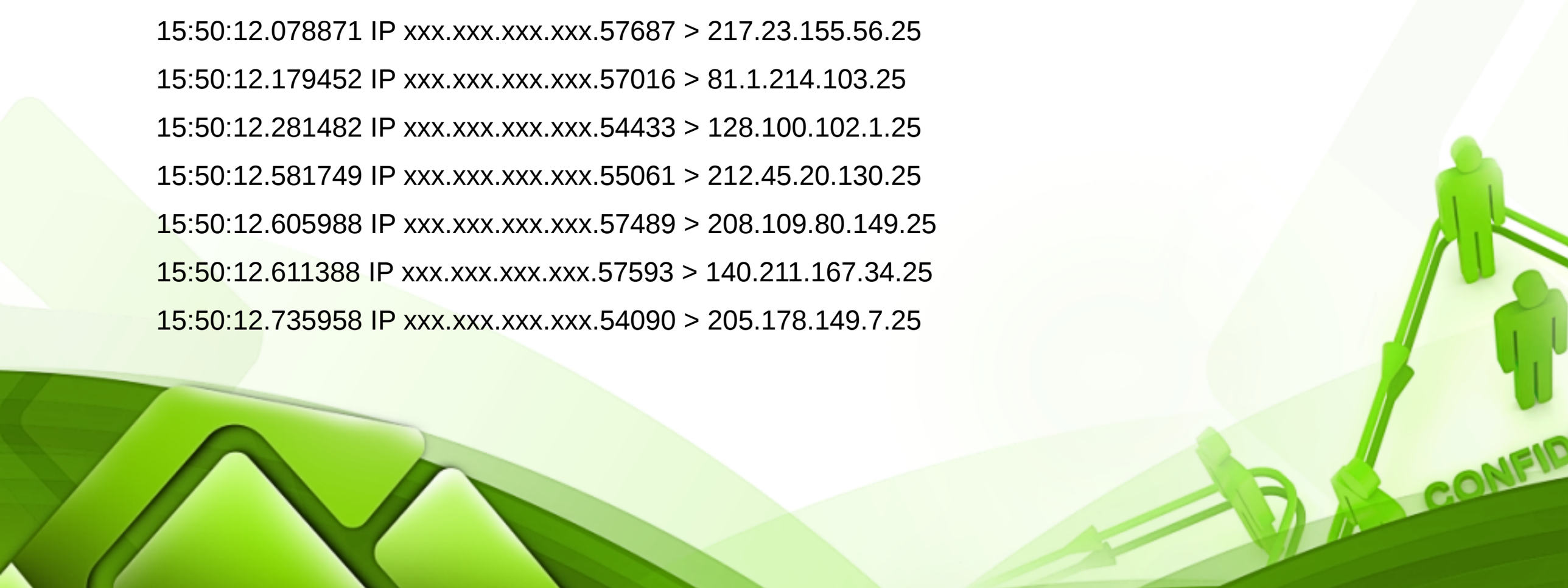
15:50:12.281482 IP xxx.xxx.xxx.xxx.54433 > 128.100.102.1.25

15:50:12.581749 IP xxx.xxx.xxx.xxx.55061 > 212.45.20.130.25

15:50:12.605988 IP xxx.xxx.xxx.xxx.57489 > 208.109.80.149.25

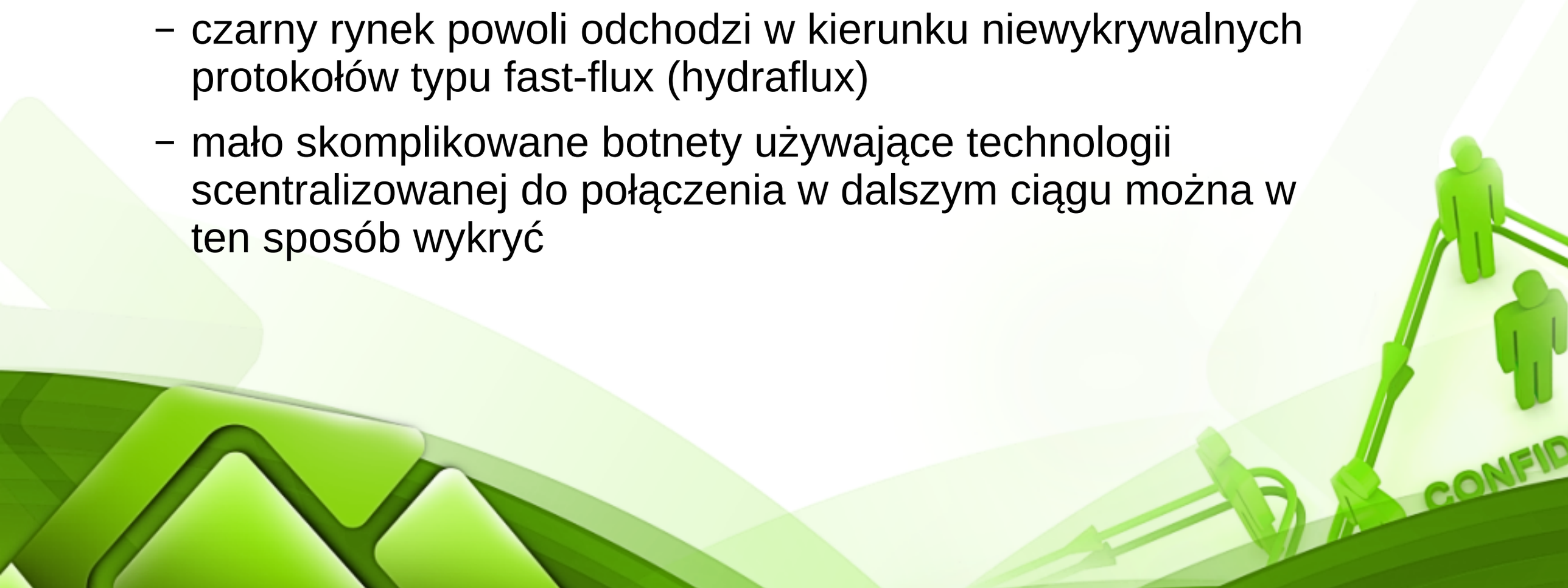
15:50:12.611388 IP xxx.xxx.xxx.xxx.57593 > 140.211.167.34.25

15:50:12.735958 IP xxx.xxx.xxx.xxx.54090 > 205.178.149.7.25



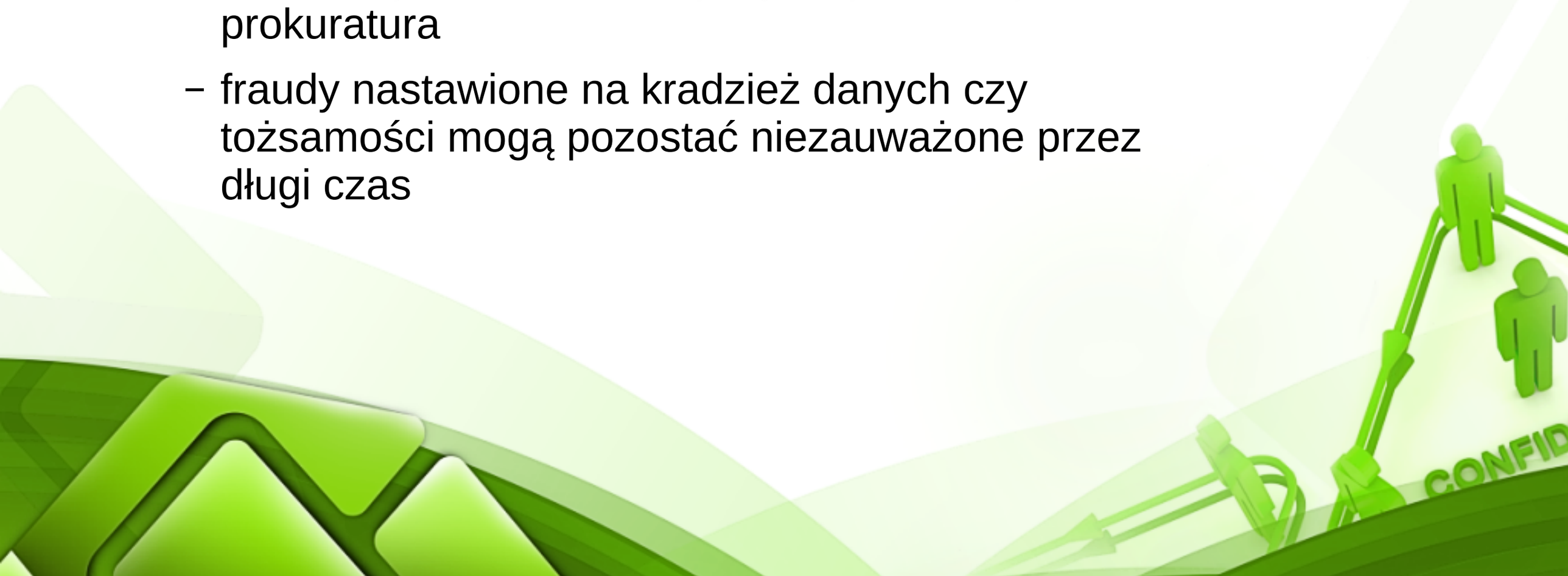
Detekcja

- analiza ruchu na porty IRCa
  - była skuteczna dekadę temu
  - czarny rynek powoli odchodzi w kierunku niewykrywalnych protokołów typu fast-flux (hydraflux)
  - mało skomplikowane botnety używające technologii scentralizowanej do połączenia w dalszym ciągu można w ten sposób wykryć



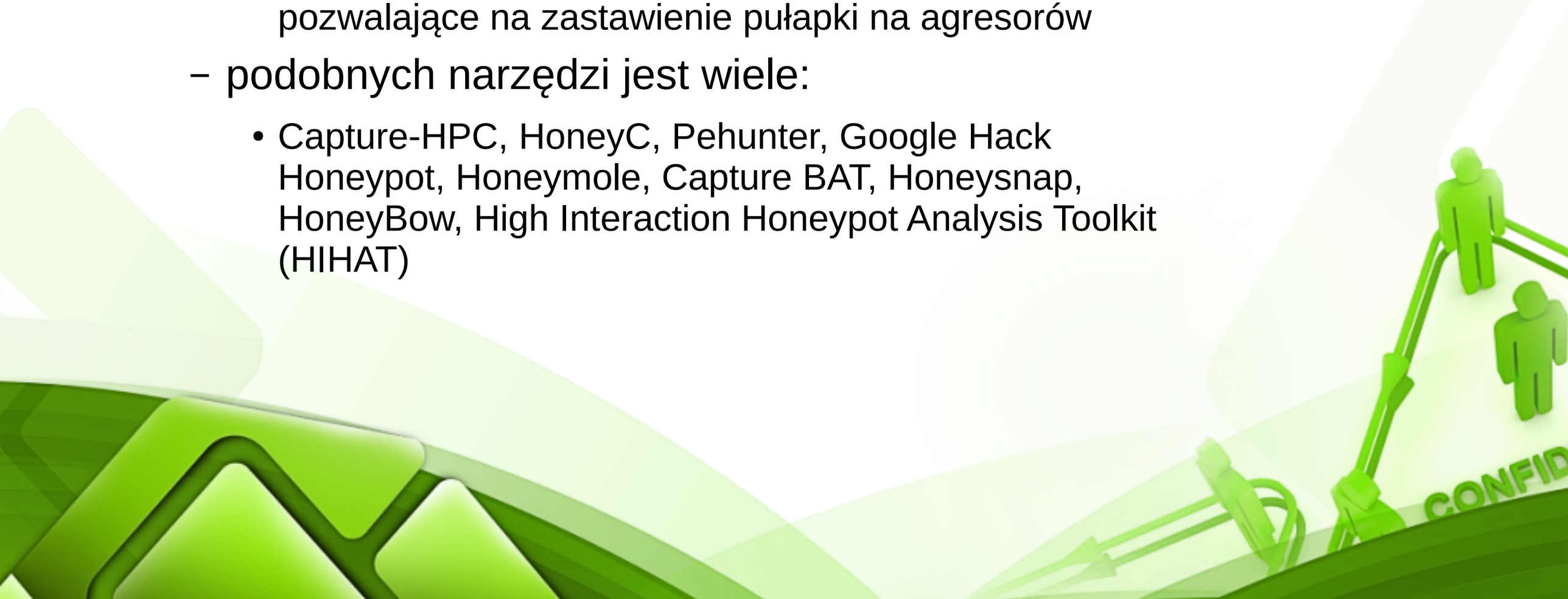
Detekcja

- Fraudy
  - przeważnie są wykrywane po fakcie
  - o masowych fraudach najczęściej informuje prokuratura
  - fraudy nastawione na kradzież danych czy tożsamości mogą pozostać niezauważone przez długi czas



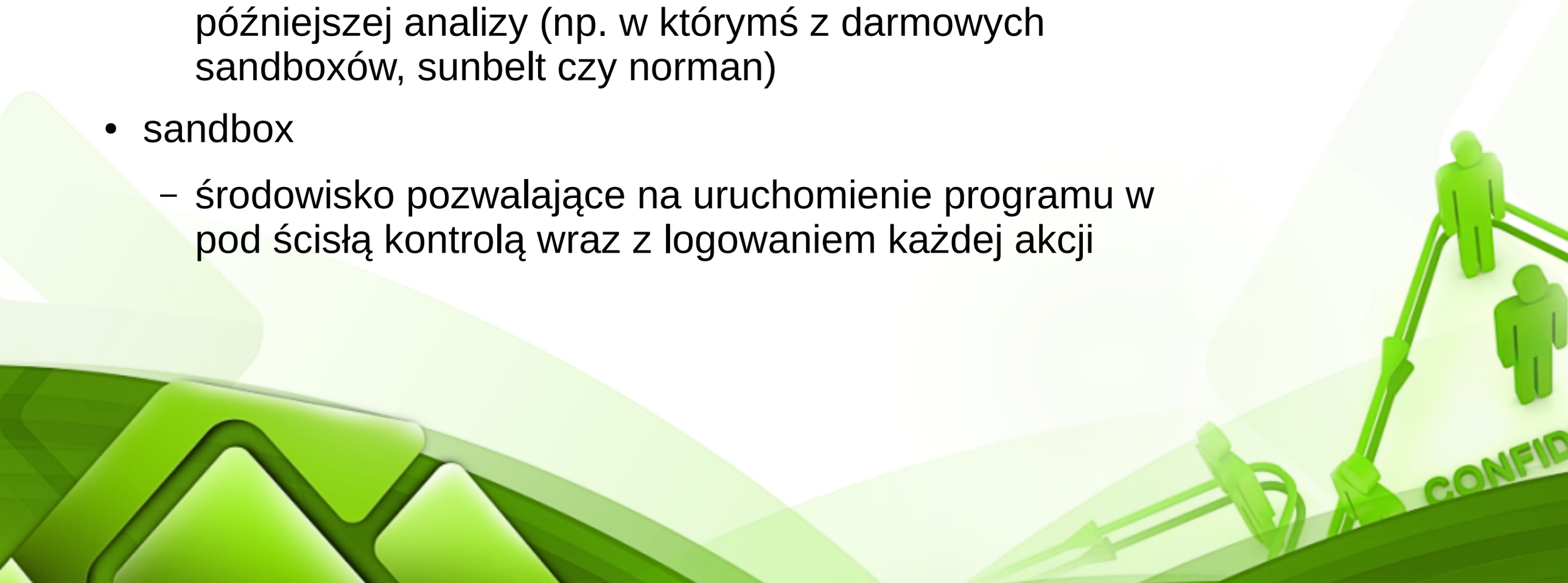
Nepenthes

- co to jest
  - HoneyPot (z ang. garnek miodu)
    - oprogramowanie udające prawdziwy system operacyjny, pozwalające na zastawienie pułapki na agresorów
  - podobnych narzędzi jest wiele:
    - Capture-HPC, HoneyC, Pehunter, Google Hack Honeypot, Honeymole, Capture BAT, Honeysnap, HoneyBow, High Interaction Honeypot Analysis Toolkit (HIHAT)



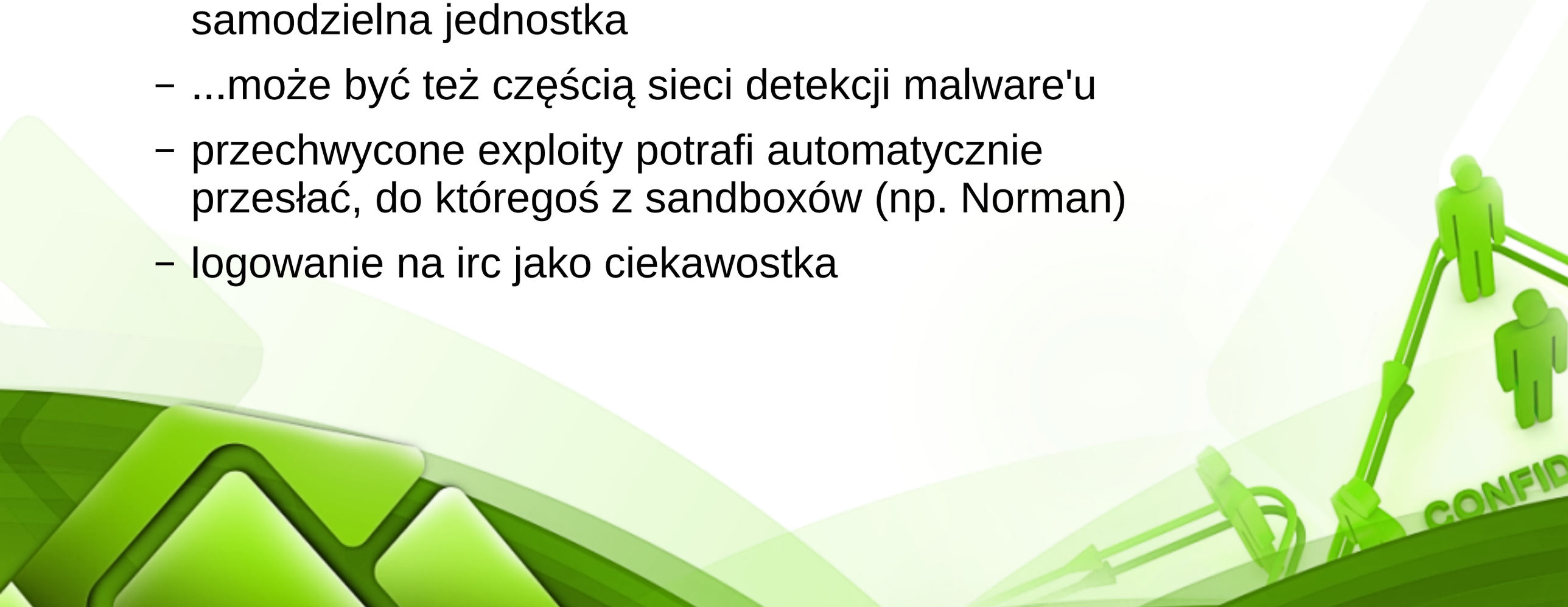
Nepenthes

- podstawy działania
  - nasłuchuje na portach emulując znane luki w wiodącym systemie operacyjnym
  - zaatakowany, potrafi przechwycić exploita w celu jego późniejszej analizy (np. w którymś z darmowych sandboxów, sunbelt czy norman)
- sandbox
  - środowisko pozwalające na uruchomienie programu w pod ścisłą kontrolą wraz z logowaniem każdej akcji



Nepenthes

- możliwości
  - pojedynczy nepenthes może działać jako samodzielna jednostka
  - ...może być też częścią sieci detekcji malware'u
  - przechwycone exploity potrafi automatycznie przesłać, do któregoś z sandboxów (np. Norman)
  - logowanie na irc jako ciekawostka



Nepenthes

- przykładowe analizy pochodzące z exploitów przesłanych do sandboxa

Nepenthes

nic nie wykryto

nepenthes-744f7bb406891c512b0c19ae4a5d7489-msnmsgr.exe : Not detected by Sandbox
(Signature: NO_VIRUS)

[General information]

* File length: 152576 bytes.

* MD5 hash: 744f7bb406891c512b0c19ae4a5d7489.

[Process/window information]

* Terminates AV software.

Nepenthes

anti debug/emulation code present – zabezpieczone przed podglądaniem

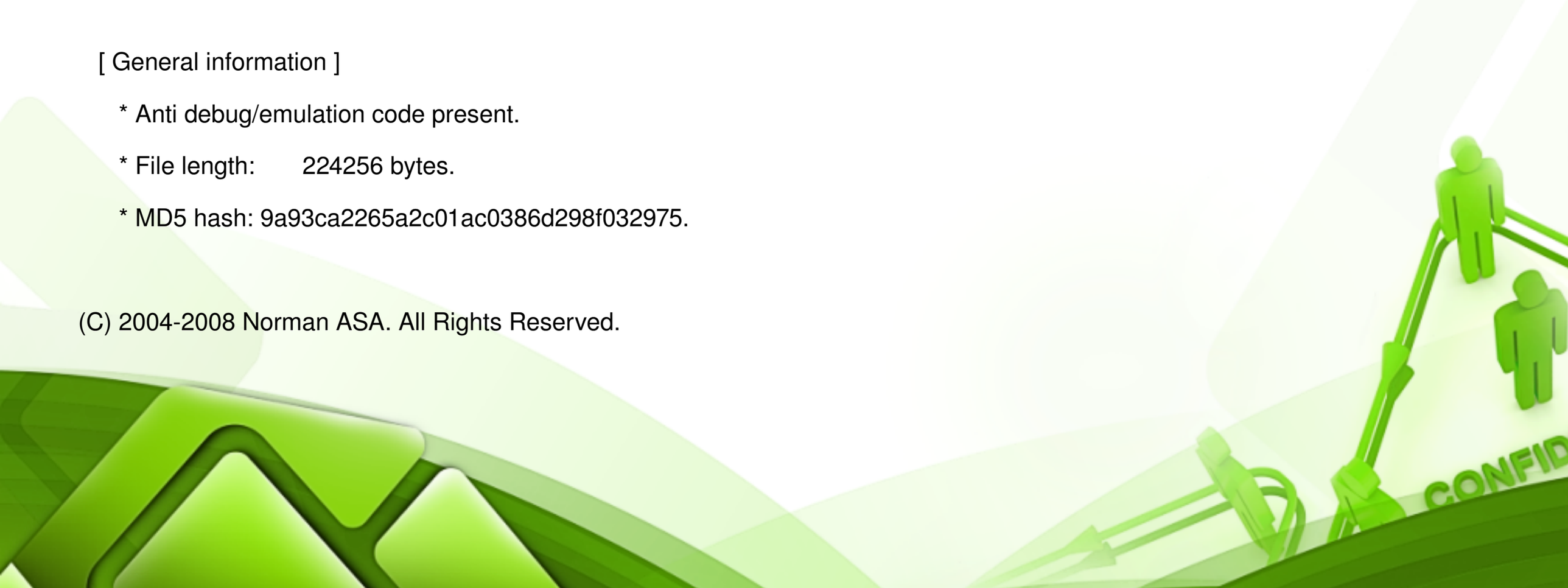
nepenthes-9a93ca2265a2c01ac0386d298f032975-xhost.exe : Not detected by Sandbox (Signature: NO_VIRUS)

[General information]

* Anti debug/emulation code present.

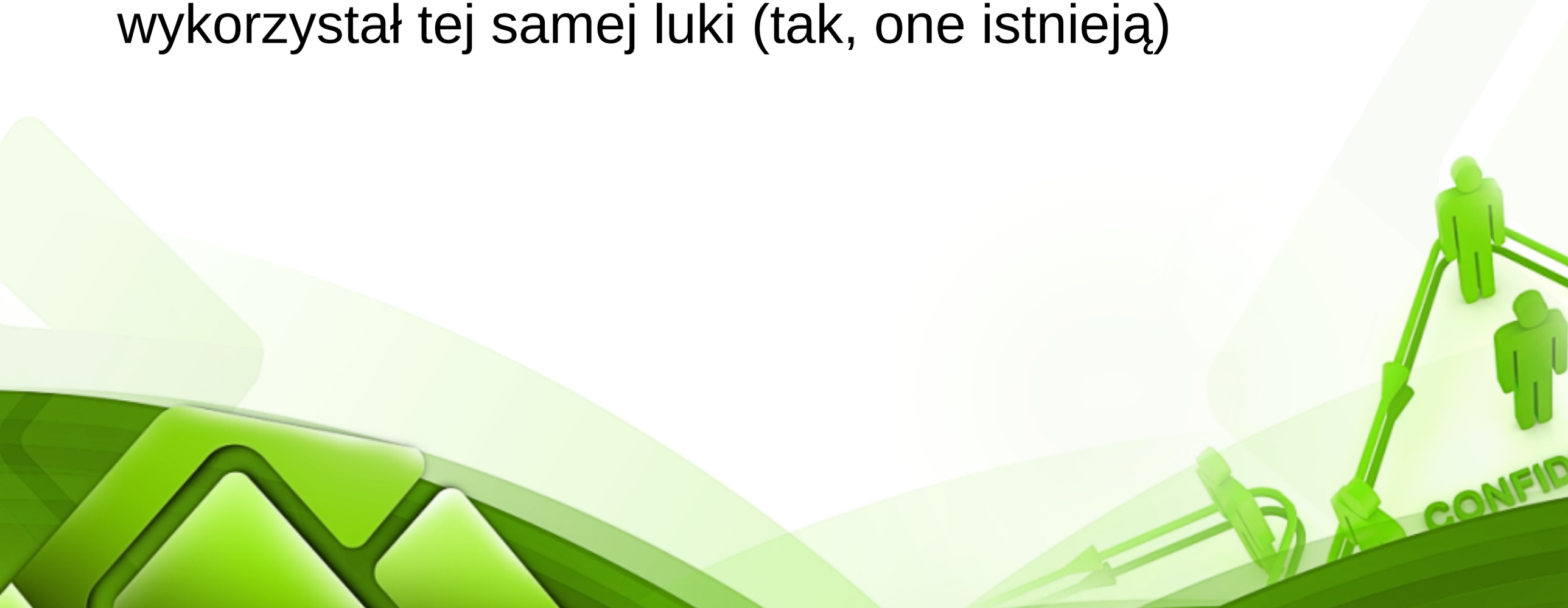
* File length: 224256 bytes.

* MD5 hash: 9a93ca2265a2c01ac0386d298f032975.



Nepenthes

- boty patchujące system, żeby nikt inny nie wykorzystał tej samej luki (tak, one istnieją)



Nepenthes

[Network services]

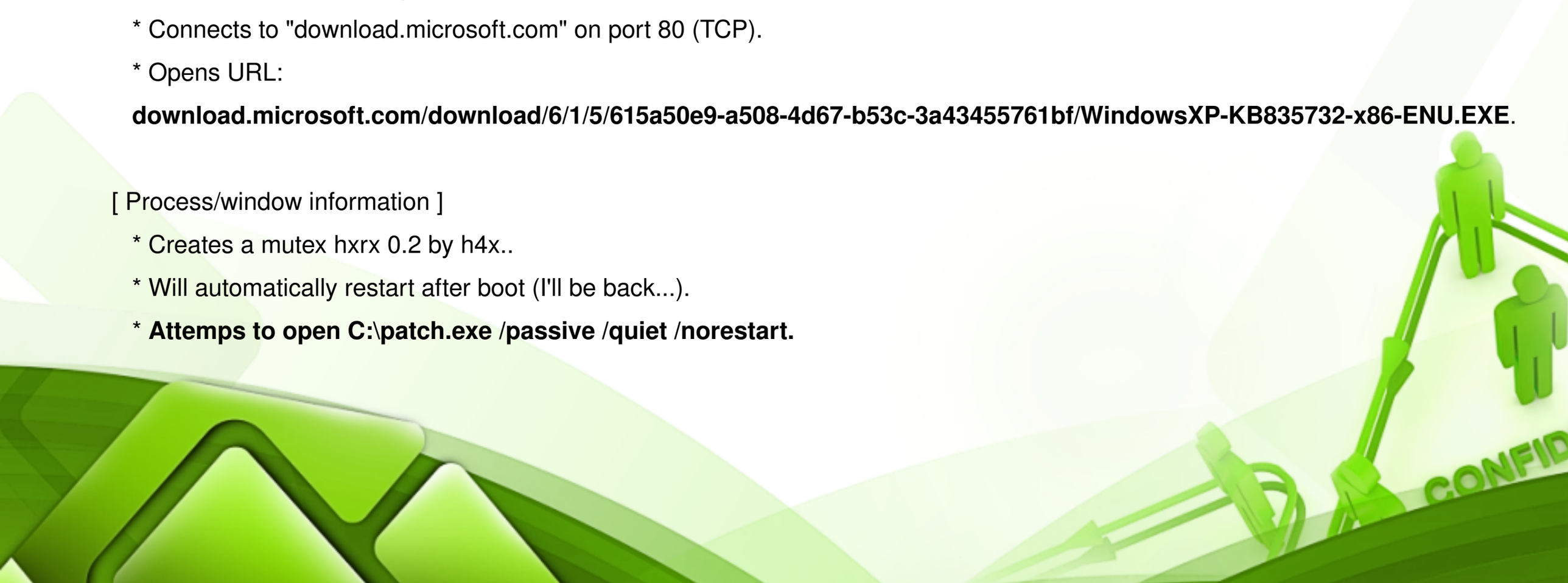
* Attempts to delete share named "Admin$" on local system.
* Attempts to delete share named "C$" on local system.
* **Downloads file from**

http://download.microsoft.com/download/6/1/5/615a50e9-a508-4d67-b53c-3a43455761bf/WindowsXP-KB835732-x86-ENU
as C:\WINDOWS\TEMP\patch.exe.

* Connects to "download.microsoft.com" on port 80 (TCP).
* Opens URL:
download.microsoft.com/download/6/1/5/615a50e9-a508-4d67-b53c-3a43455761bf/WindowsXP-KB835732-x86-ENU.EXE.

[Process/window information]

* Creates a mutex hxrx 0.2 by h4x..
* Will automatically restart after boot (I'll be back...).
* **Attemps to open C:\patch.exe /passive /quiet /norestart.**



Nepenthes

Przykład botnetu standardowego:

CWSandbox Malware Analysis Report

Scan Summary | File Changes | Registry Changes | Network Activity | Technical Details

Submission Details

Date	03.04.2008 16:29:47
Sandbox Version	2.0.33
File Name	nepenthes9e36bd4fd7162c7f13987097f265fe11WinTcpipi.exe

Summary Findings

Total Number of Processes	2
Termination Reason	NormalTermination
Start Time	00:00.765
Stop Time	00:02.171
Start Reason	AnalysisTarget

Scanner Results

Scan Engine	Version	Signature Version	Result	More Info
ClamAV			OK	

Analysis HighLights

Spawned Processes	Found 1 Processes. (View Activity by Process)
Filesystem Changes	View File Changes
Registry Changes	View Registry Changes
Network Activity	View Network Activity

Nepenthes

... i jego aktwności sieciowych

CWSandbox Sunbelt MALWARE ANALYSIS REPORT

Scan Summary | File Changes | Registry Changes | Network Activity | Technical Details

Network Activity

Connections

DNS Lookup

Host Name	IP Address
scorti1.dns2go.com	67.19.50.66

Opened listening TCP connection on port: 113

- C&C Server: 67.19.50.66:7000
- Server Password:
- Username: vmlzydbzz
- Nickname: DEU|XP|SP2|00|69170138
- Channel: #Virus# (Password: ss88ss.)
- Channeltopic: :.ABOSAL7 -a -s

Nepenthes

Przykładowa analiza jest dostępna w linkach

LogicalTrust
www.logicaltrust.net

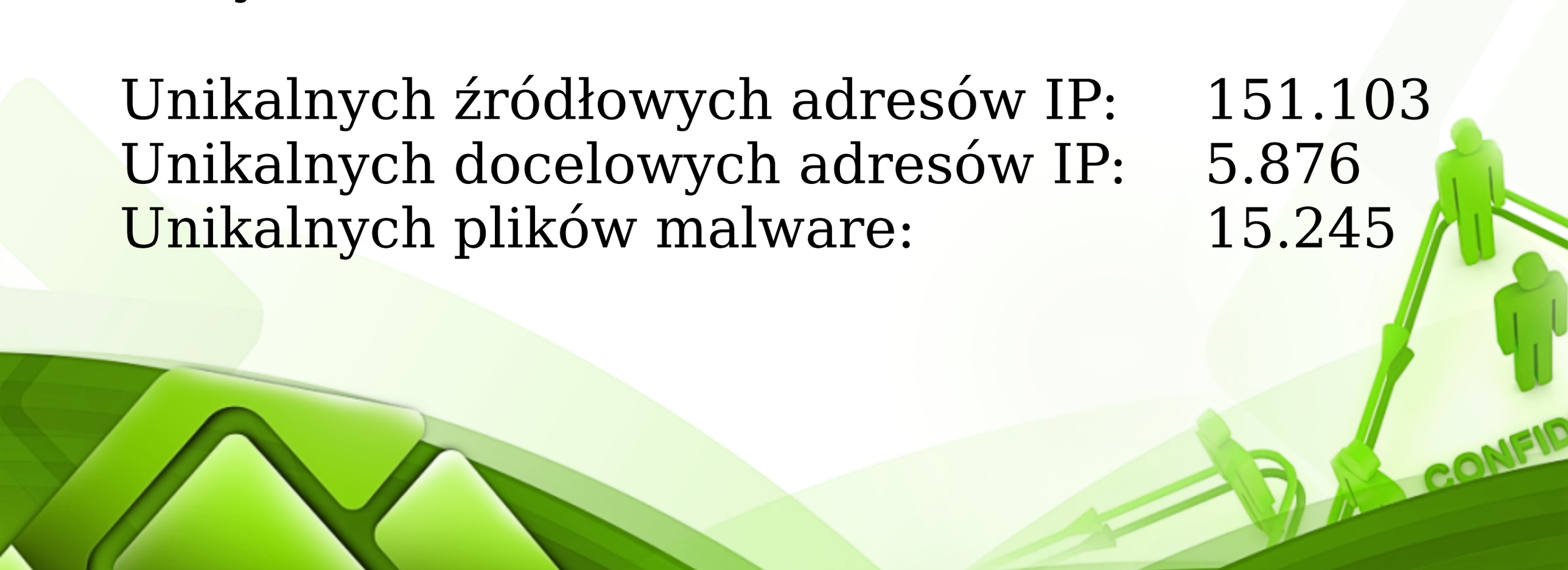
IT BCE BUSINESS CONSULTING EXPERTS

Statystyki

Data pierwszego ataku: 2007-02-16 18:34:23
Data ostatniego ataku: 2009-03-07 19:12:31

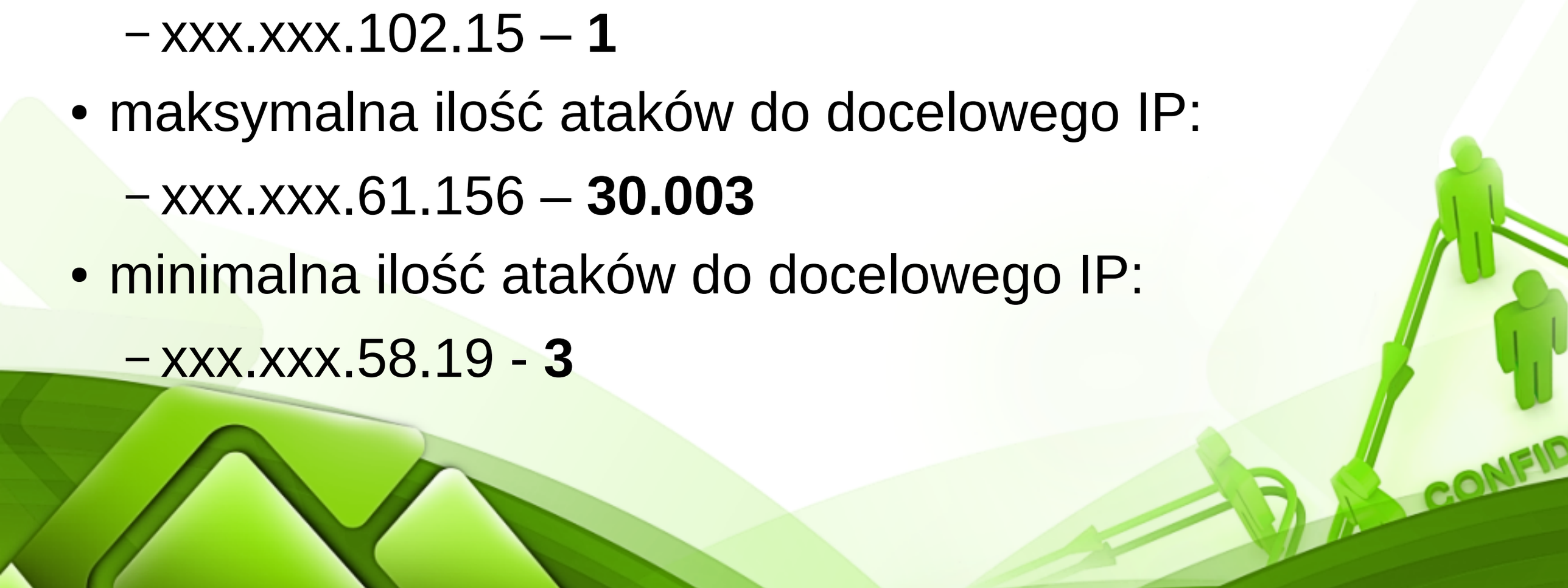
Wszystkich ataków: **3.713.717**

Unikalnych źródłowych adresów IP: 151.103
Unikalnych docelowych adresów IP: 5.876
Unikalnych plików malware: 15.245



Statystyki

- maksymalna ilość ataków ze źródłowego IP:
  - xxx.xxx.28.115 – **198.099**
- minimalna ilość ataków ze źródłowego IP:
  - xxx.xxx.102.15 – **1**
- maksymalna ilość ataków do docelowego IP:
  - xxx.xxx.61.156 – **30.003**
- minimalna ilość ataków do docelowego IP:
  - xxx.xxx.58.19 - **3**

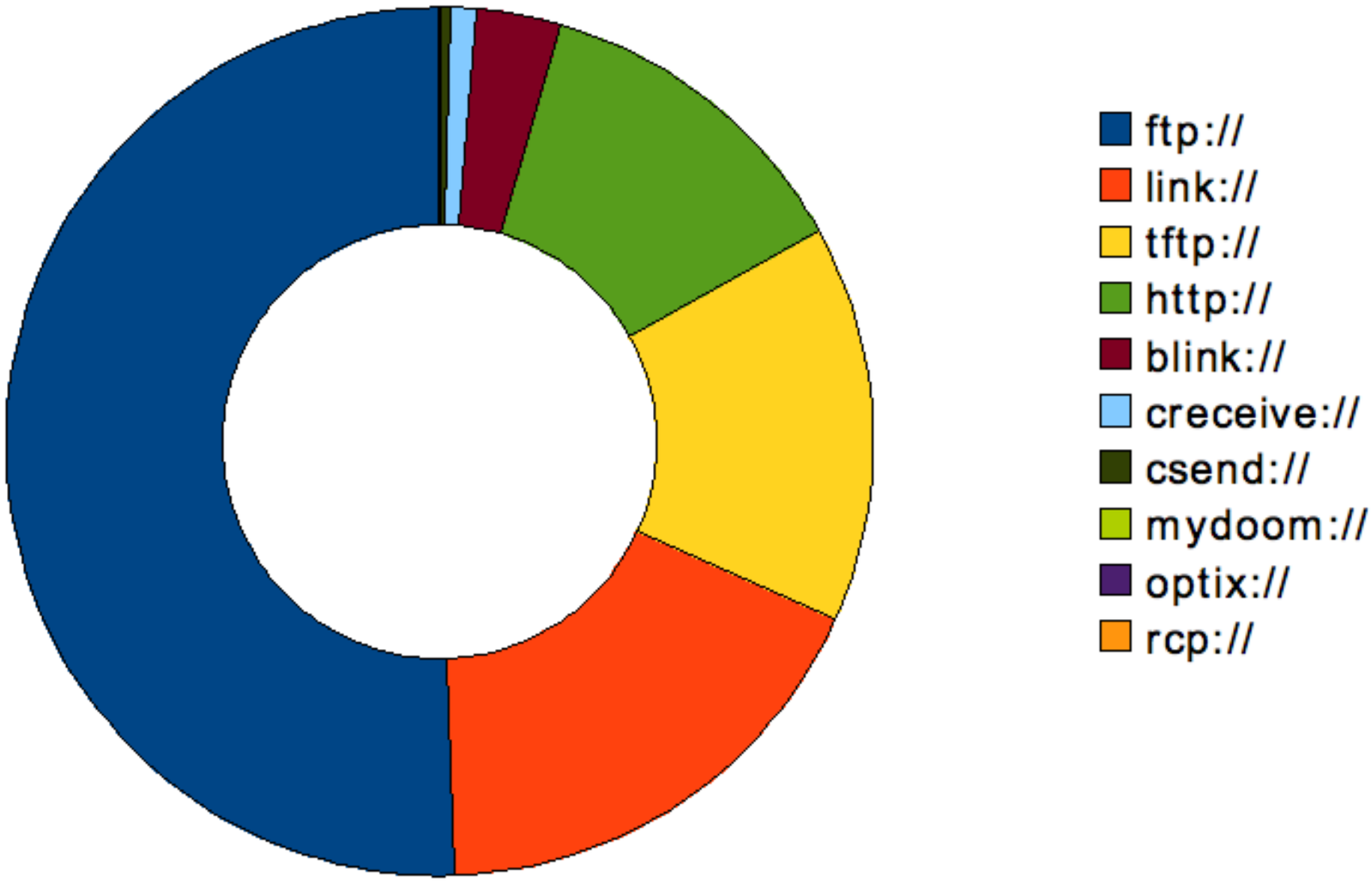


Statystyki

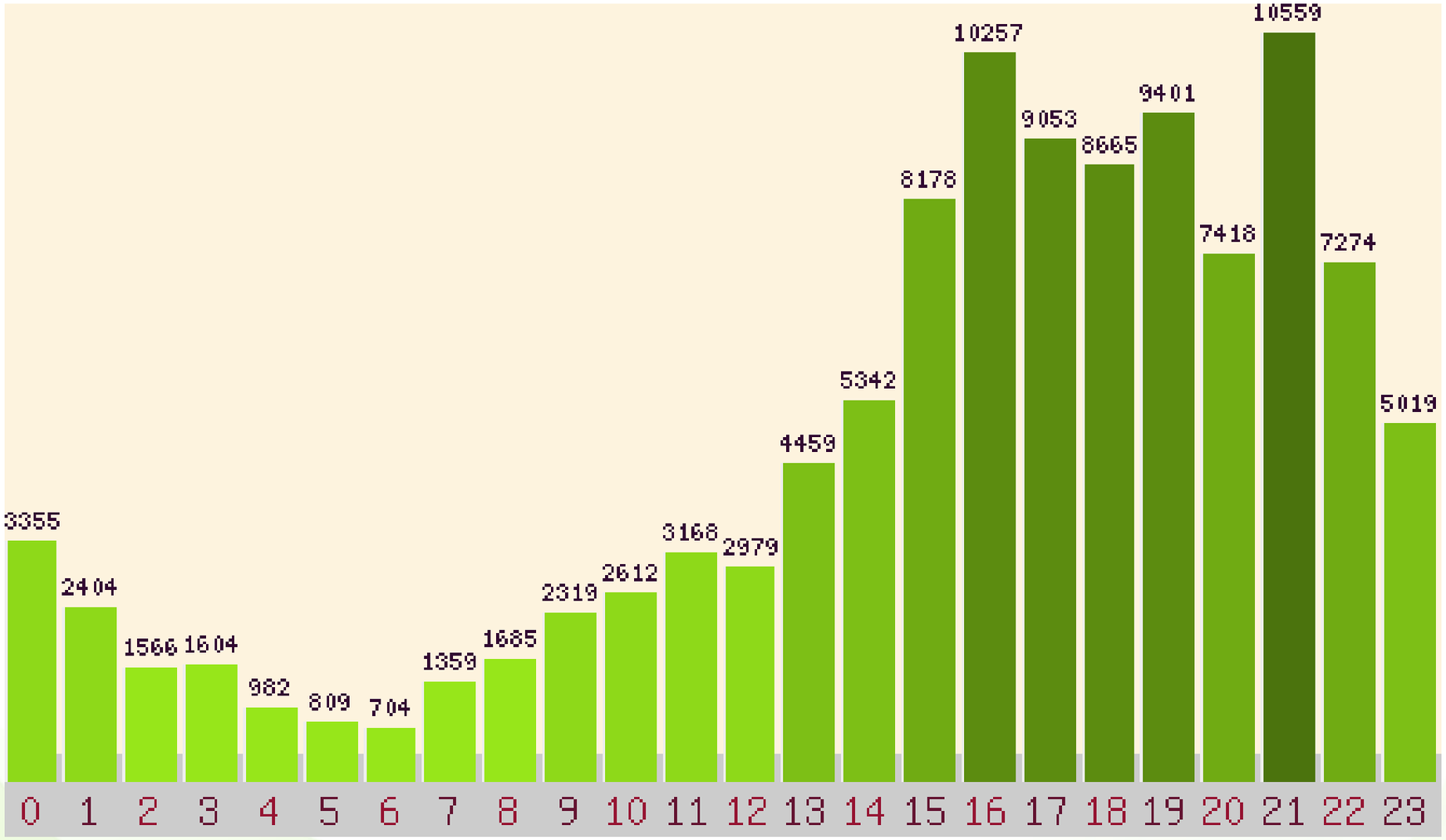
Maksymalna ilość ataków dla malware:
b65a426bee4440171ad6ed7143cc93ba (md5) **339.364**

Ataków na minutę: **3,43**
Ataków na godzinę: **206,28**
Ataków na dzień: **4950,73**

Statystyki

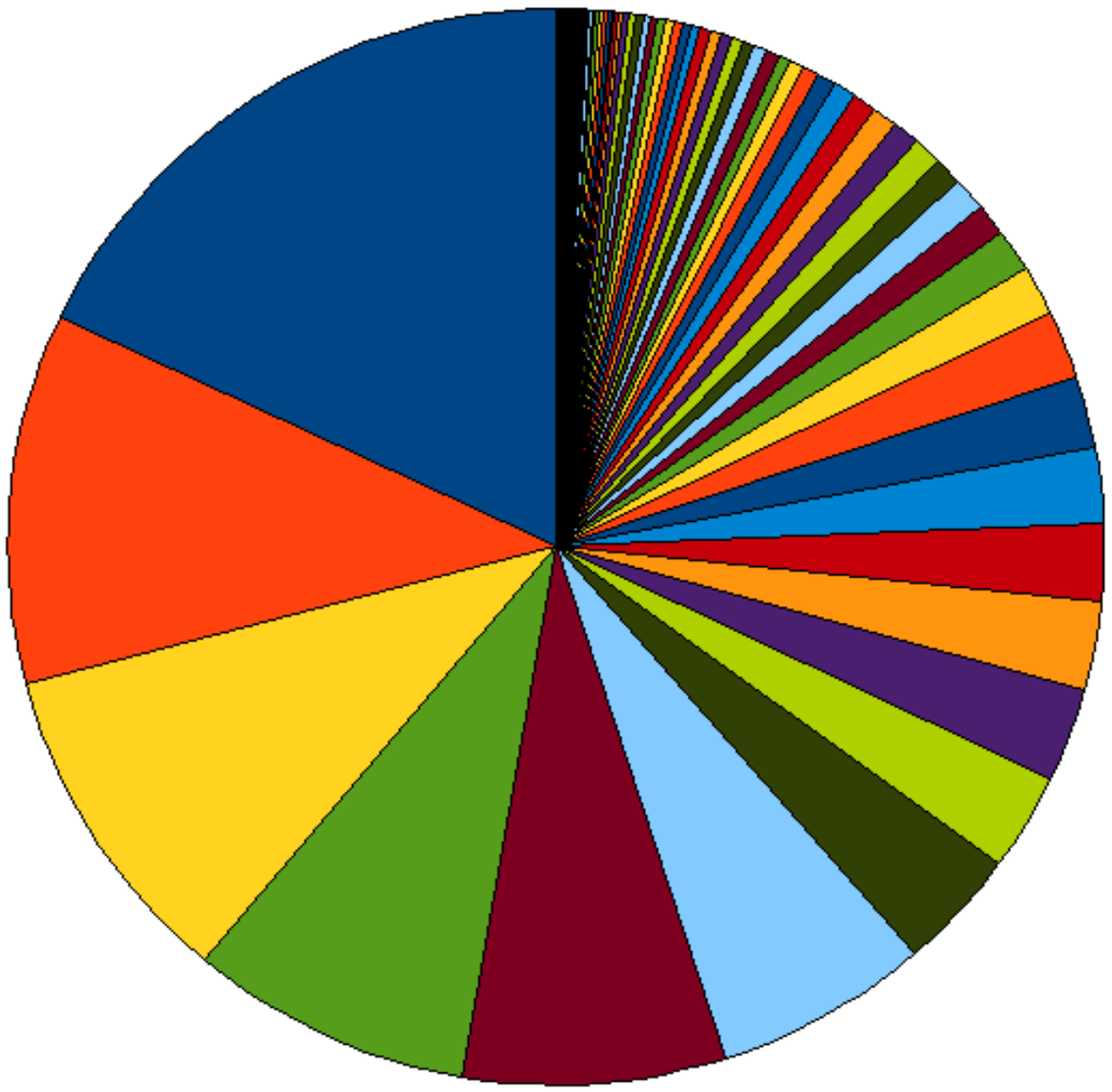


Statystyki



Ilość ataków na godzinę - 2009.01

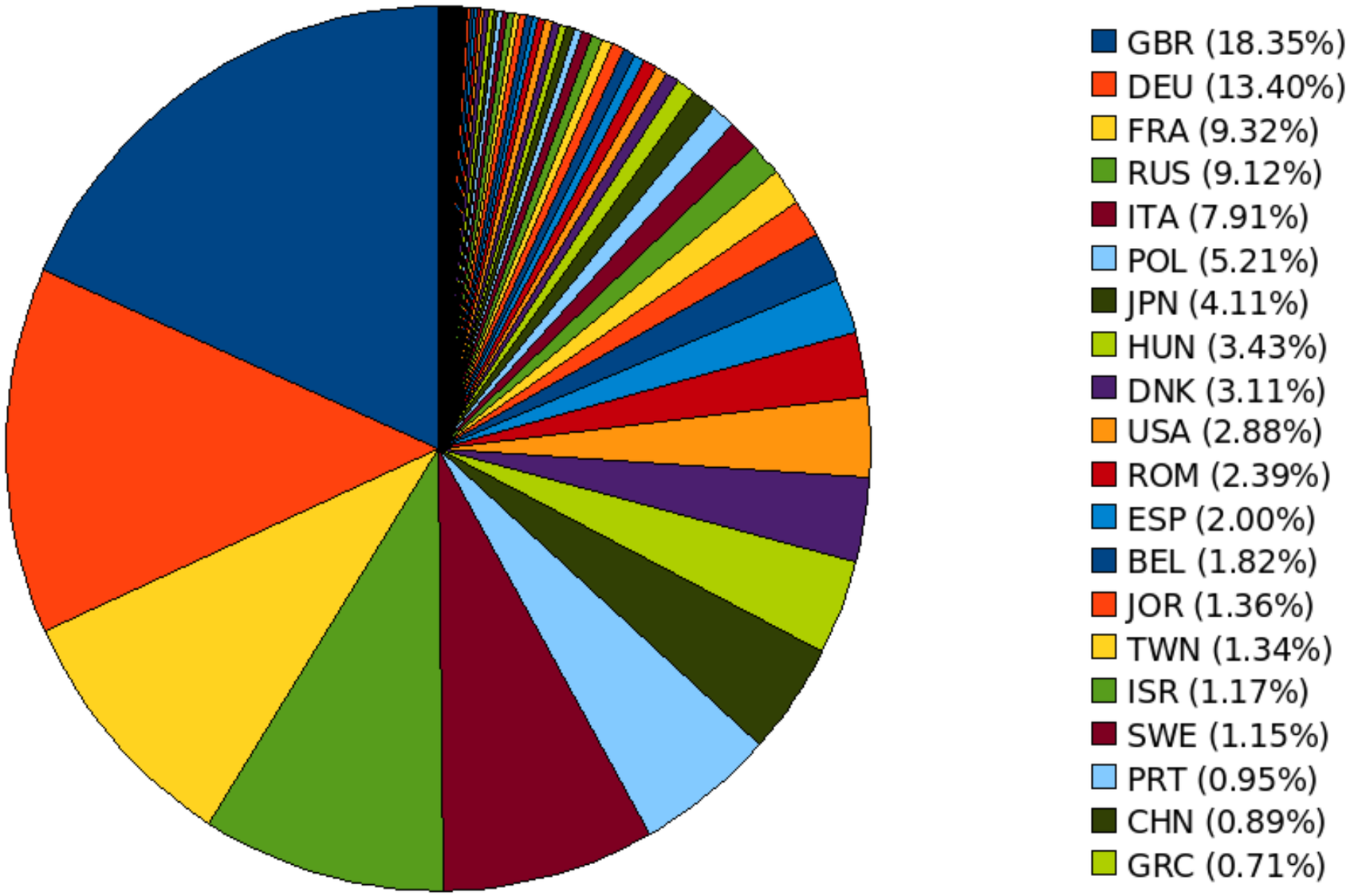
Statystyki



Źródło ataku

137 krajów !

Statystyki



Malware URL

LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

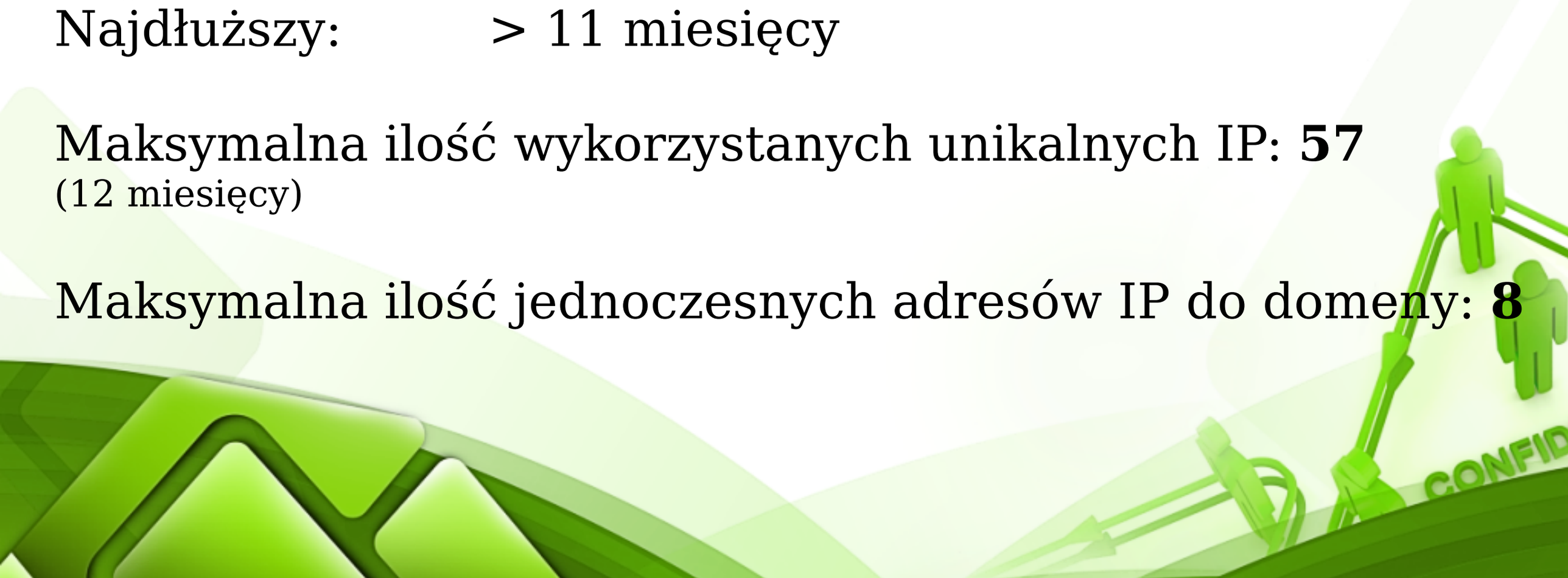
Statystyki

492 domen
24 miesięce

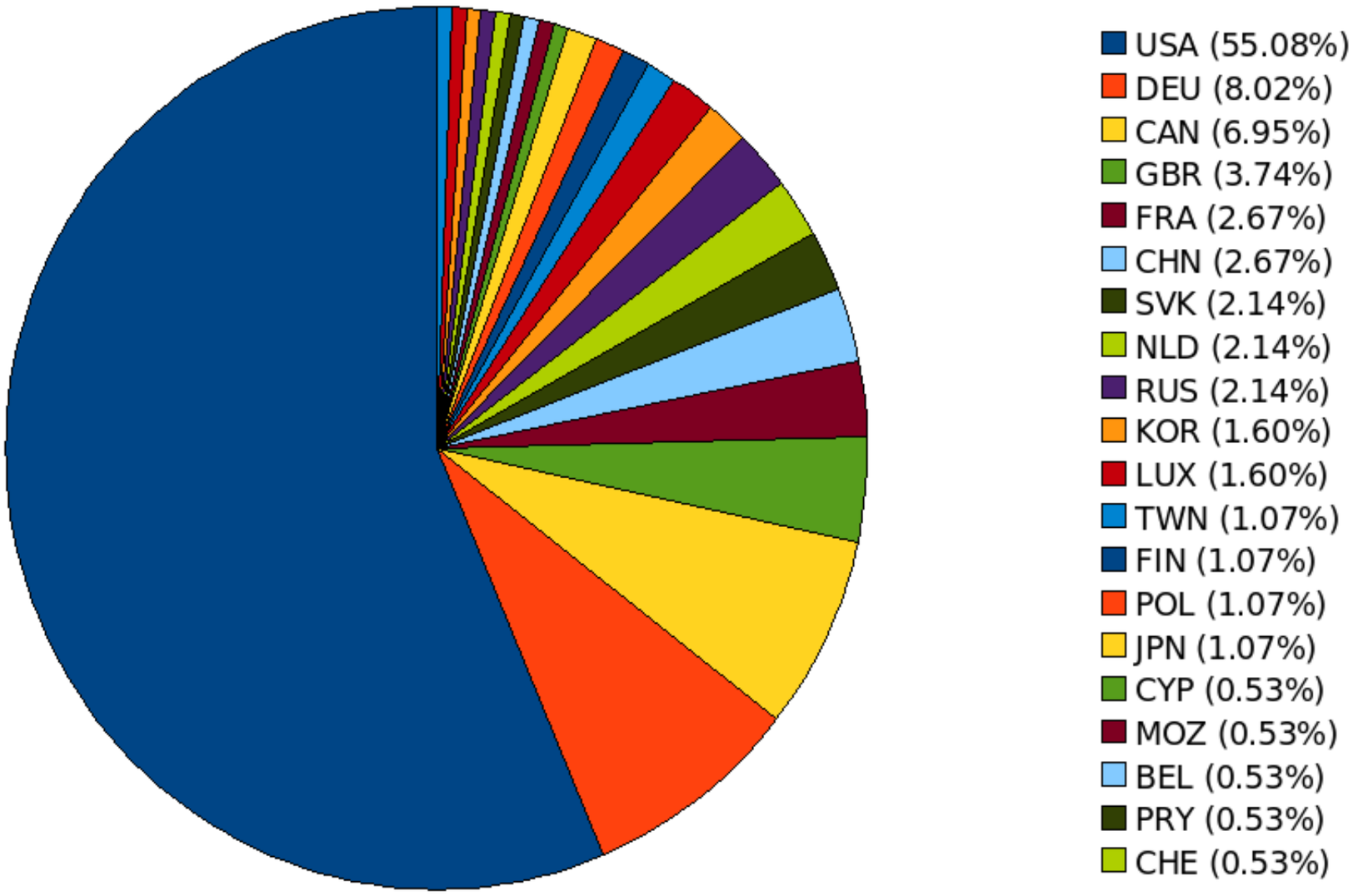
Czas stałego dowiązania domeny do IP:
Najkrótszy: < 1 dzień
Najdłuższy: > 11 miesięcy

Maksymalna ilość wykorzystanych unikalnych IP: **57**
(12 miesięcy)

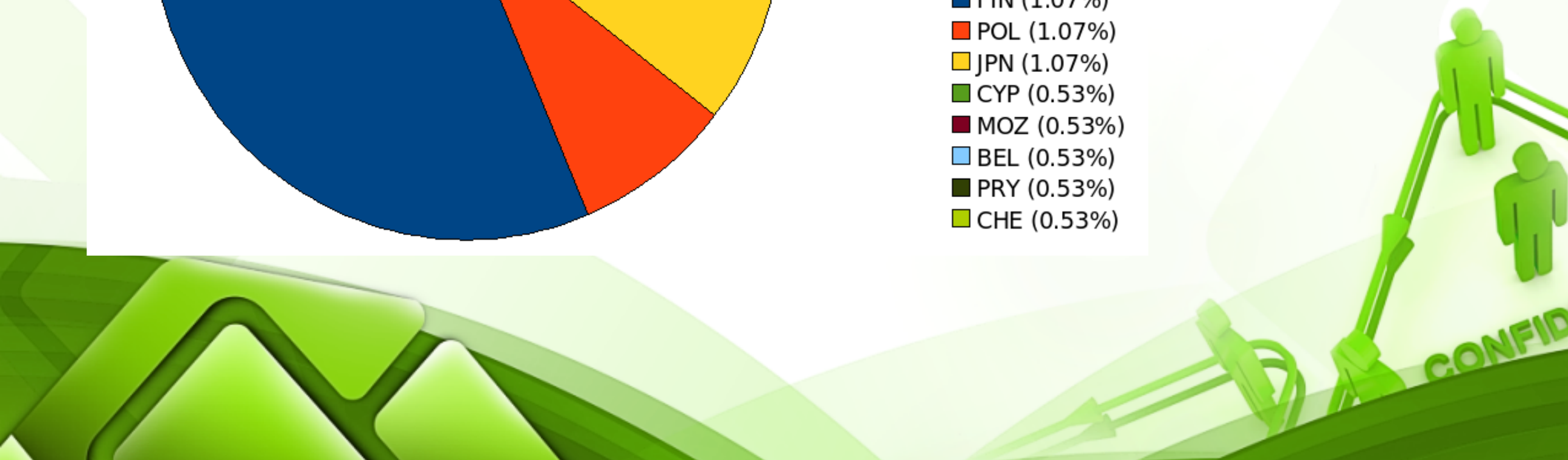
Maksymalna ilość jednoczesnych adresów IP do domeny: **8**



Statystyki

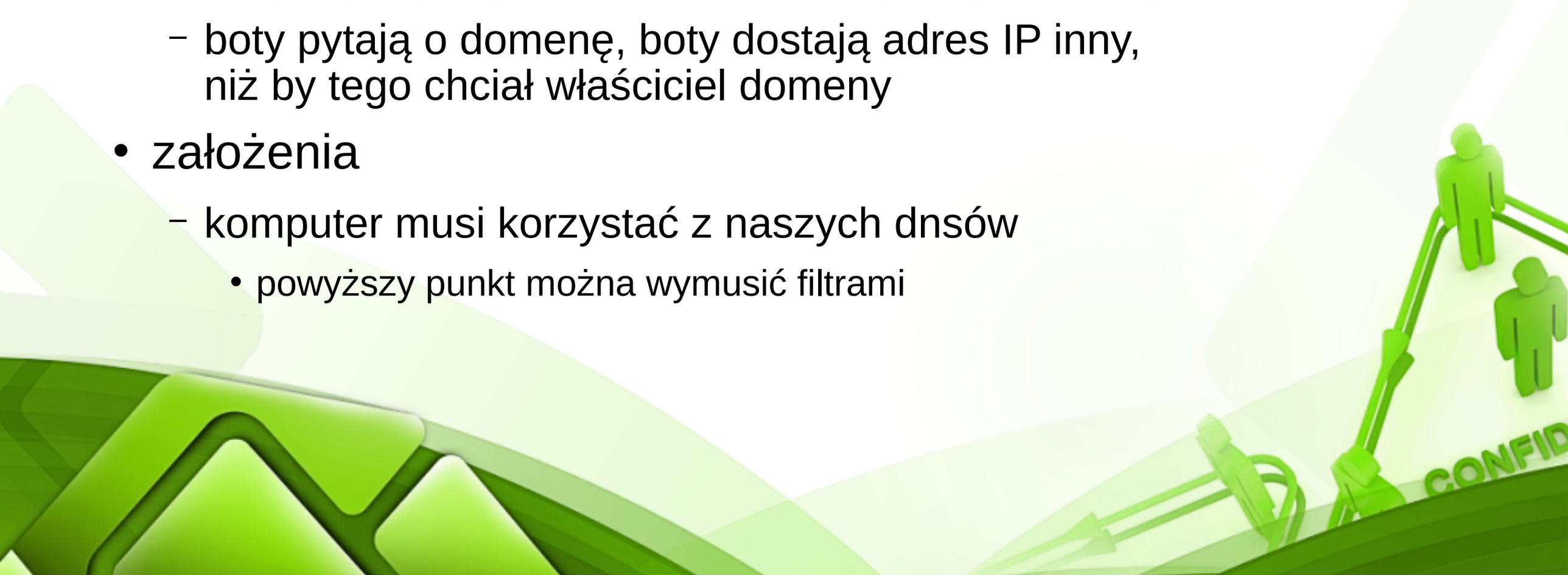


C & C



DNS blackholing

- teoria działania
  - konfiguracja serwera DNS tak, żeby działał jako master dla konkretnej domeny
  - udajemy legalny serwer DNS obsługujący domenę
  - boty pytają o domenę, boty dostają adres IP inny, niż by tego chciał właściciel domeny
- założenia
  - komputer musi korzystać z naszych dnsów
    - powyższy punkt można wymusić filtrami

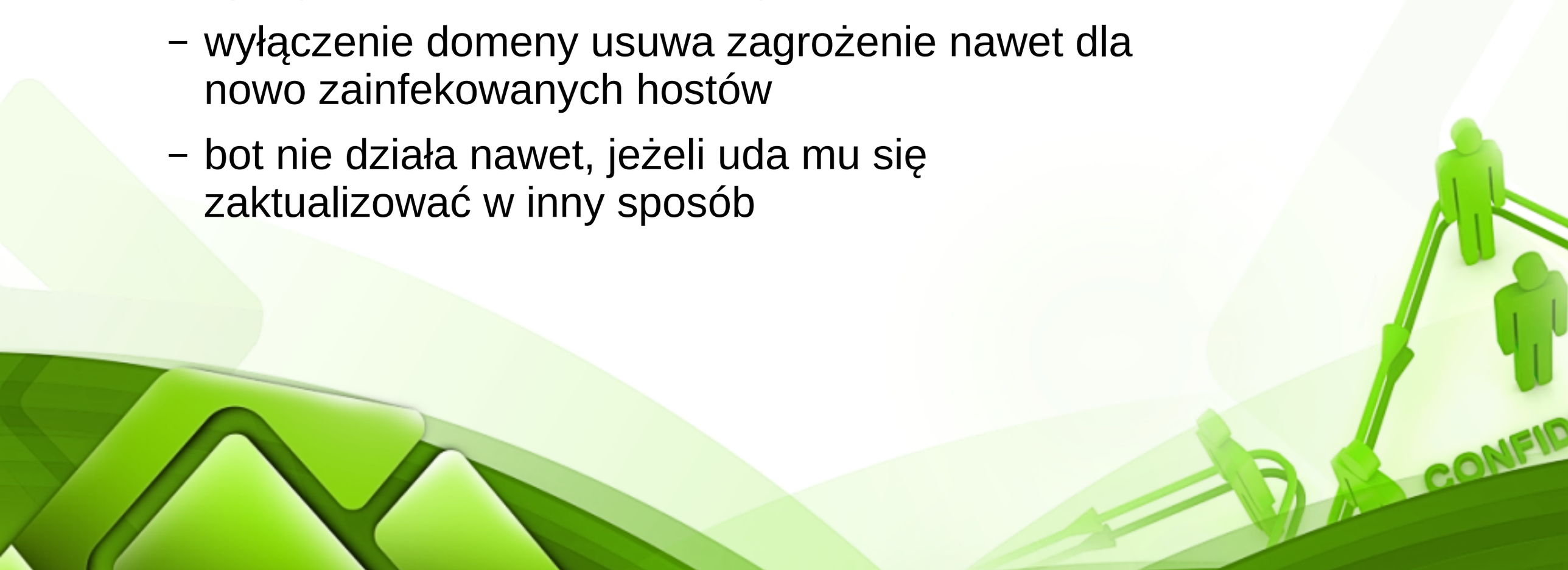


DNS blackholing

- możliwości wykorzystania
  - przekierowanie blackholowanych domen na dowolny adres IP w celu dalszej analizy
  - dezaktywacja bota bez ingerencji w komputer klienta (kwestia etyczna)

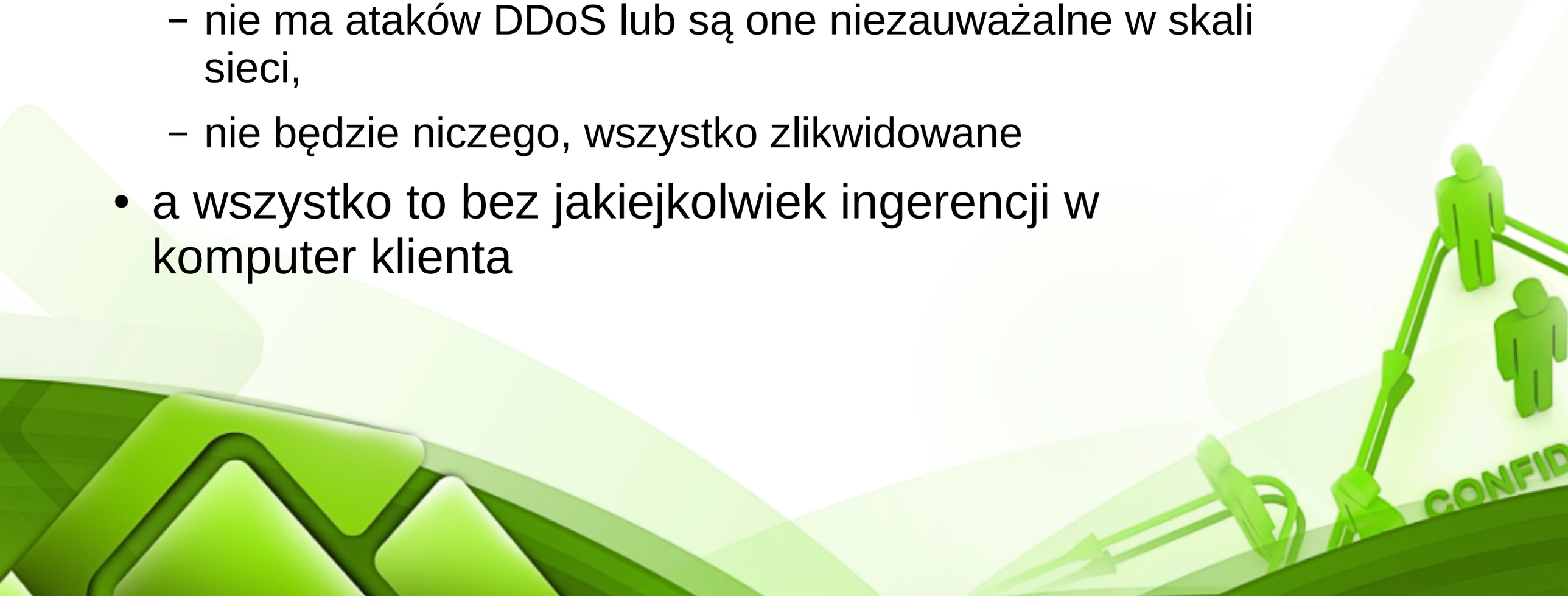
DNS blackholing

- skuteczniejszy od firewalli
  - adresy IP serwerów C&C w ramach domeny zmieniają się często
  - oprogramowanie AV nie nadąża za botami
  - wyłączenie domeny usuwa zagrożenie nawet dla nowo zainfekowanych hostów
  - bot nie działa nawet, jeżeli uda mu się zaktualizować w inny sposób



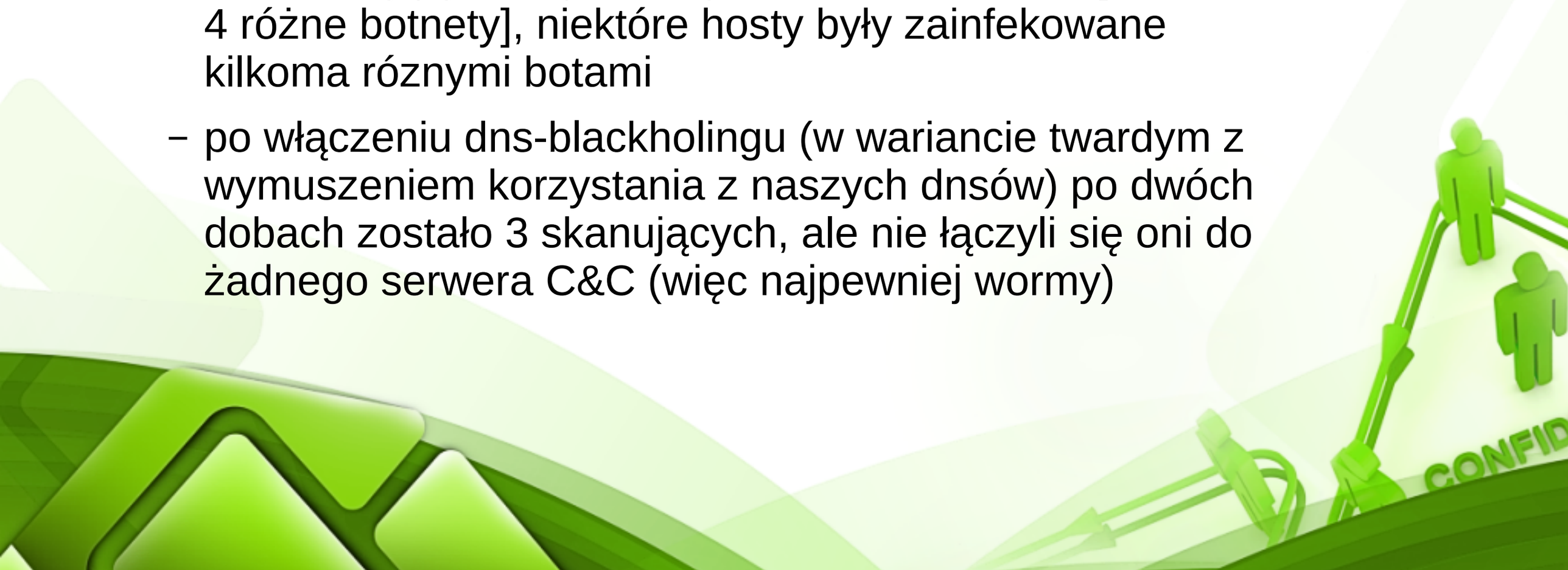
DNS blackholing

- pozytywne efekty wdrożenia
  - boty nie działają bez głowy
  - nie ma spamu
  - nie ma ataków DDoS lub są one niezauważalne w skali sieci,
  - nie będzie niczego, wszystko zlikwidowane
- a wszystko to bez jakiejkolwiek ingerencji w komputer klienta



DNS blackholing

- skuteczność z życia wzięta
  - przejęta sieć na 1.2k userów
  - od 150 do 200 osób zainfekowanych (skanujących i komunikujących się z różnymi serwerami C&C [w sumie 4 różne botnety], niektóre hosty były zainfekowane kilkoma róznymi botami
  - po włączeniu dns-blackholingu (w wariancie twardym z wymuszeniem korzystania z naszych dnsów) po dwóch dobach zostało 3 skanujących, ale nie łączyli się oni do żadnego serwera C&C (więc najpewniej wormy)



LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

Konfiguracja - przykłady

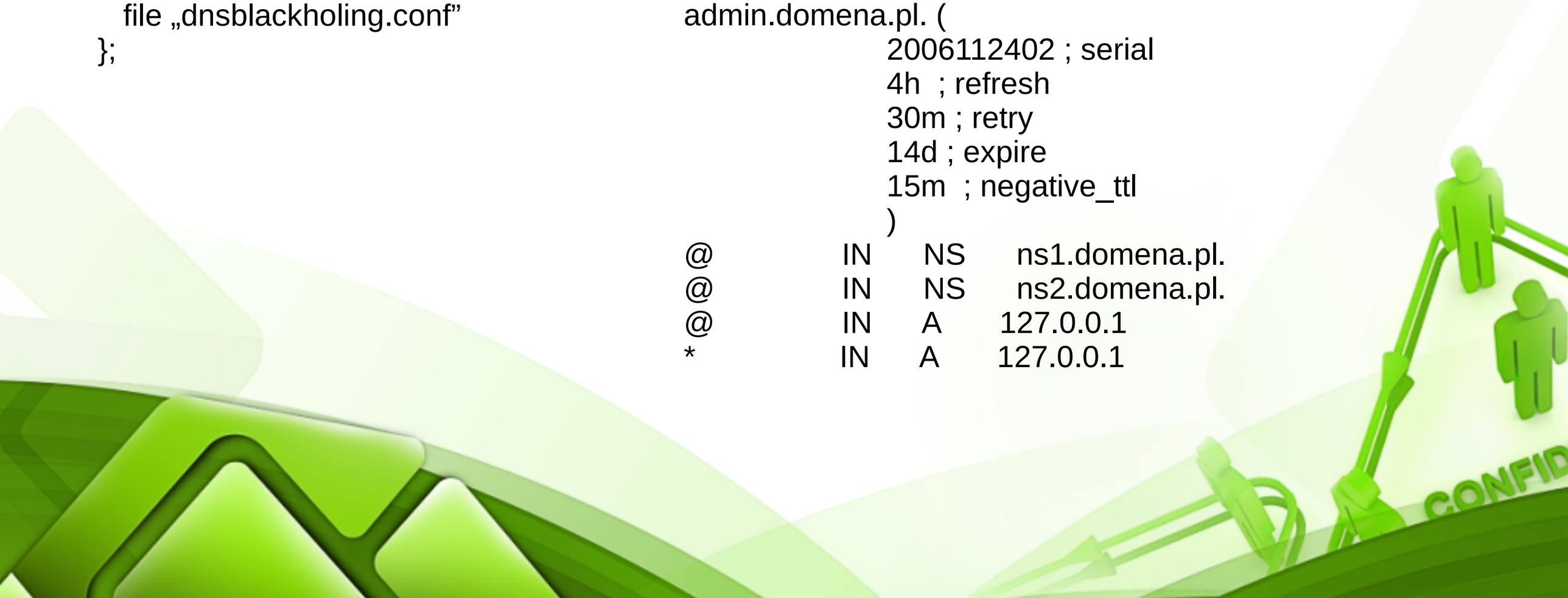
Bind 9

/etc/bind/named.conf – główny konfig

```
zone "powiekszswojinteres.pl" IN {
   type master;
   file „dnsblackholing.conf”
};
```

dnsblackholing.conf – plik domeny

```
$TTL 15m
@           IN     SOA    ns1.domena.pl.
admin.domena.pl. (
                   2006112402 ; serial
                   4h  ; refresh
                   30m ; retry
                   14d ; expire
                   15m  ; negative_ttl
                   )
@          IN     NS     ns1.domena.pl.
@          IN     NS     ns2.domena.pl.
@          IN     A      127.0.0.1
*          IN     A      127.0.0.1
```



Nepenthes

konfiguracja pod bazę PostgreSQL

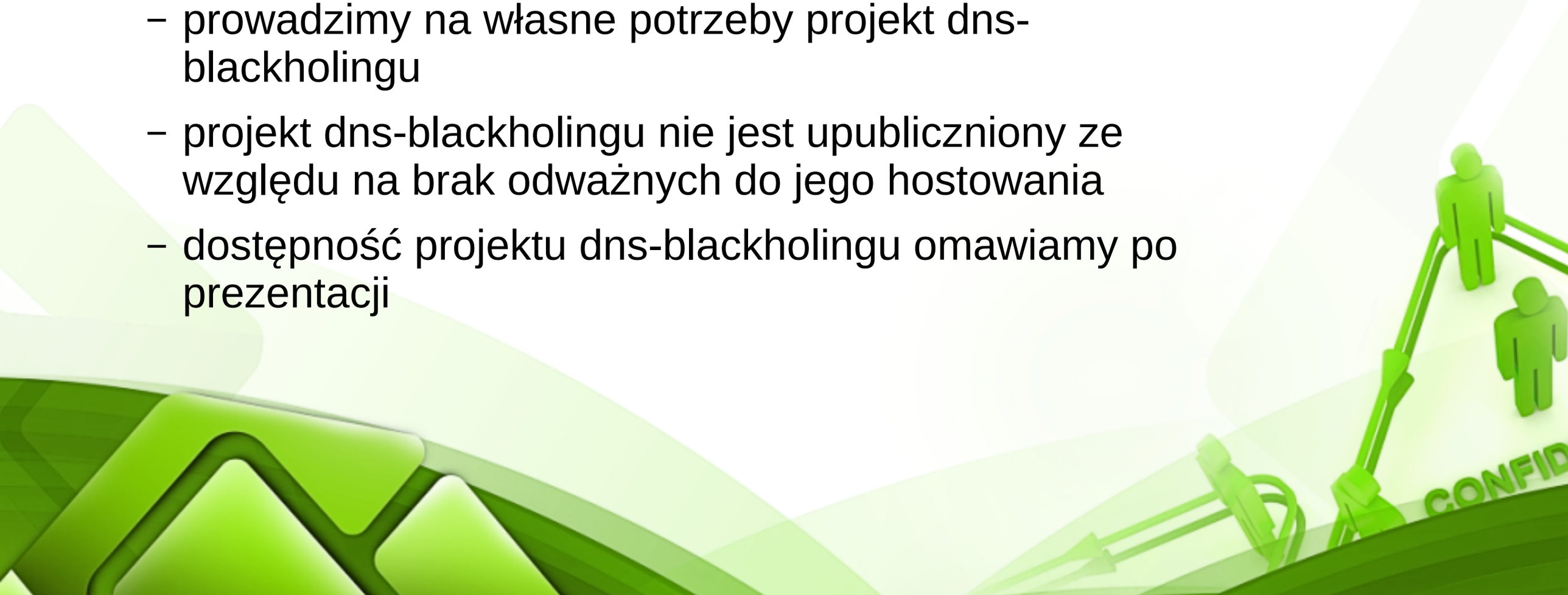
submit-postgres
{
server "1.2.3.4"; // use ips,domains/hostnames won't work!
user "user"; // db user
pass "hasłord"; // db pass
db "mwcollect"; // which database to use
options ""; // not sure if options already work
spooldir "/var/spool/nepenthes/submitpostgres/";
};

wysyłanie wyników do Sandboxa Normana

submit-norman
{
	// this is the adress where norman sandbox reports will be sent
	email "dsfsdfsdfsfs@no-mail.pl";
	urls ("http://www.norman.com/microsites/nsic/Submit/Special/45773/",
		"http://luigi.informatik.uni-mannheim.de/submit.php?action=verify"); };

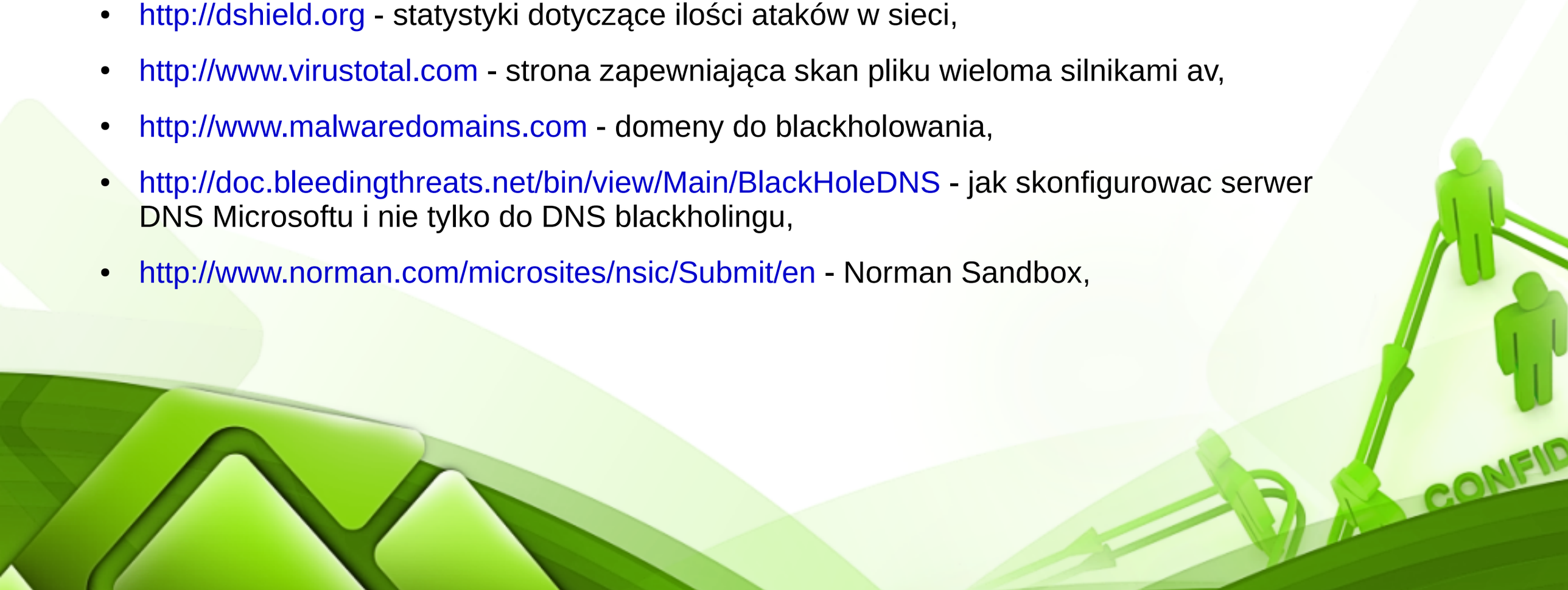
Pytania

- Często Zadawane Pytania - odpowiedzi
  - nie posiadamy własnego botnetu
  - prowadzimy na własne potrzeby projekt dns-blackholingu
  - projekt dns-blackholingu nie jest upubliczniony ze względu na brak odważnych do jego hostowania
  - dostępność projektu dns-blackholingu omawiamy po prezentacji



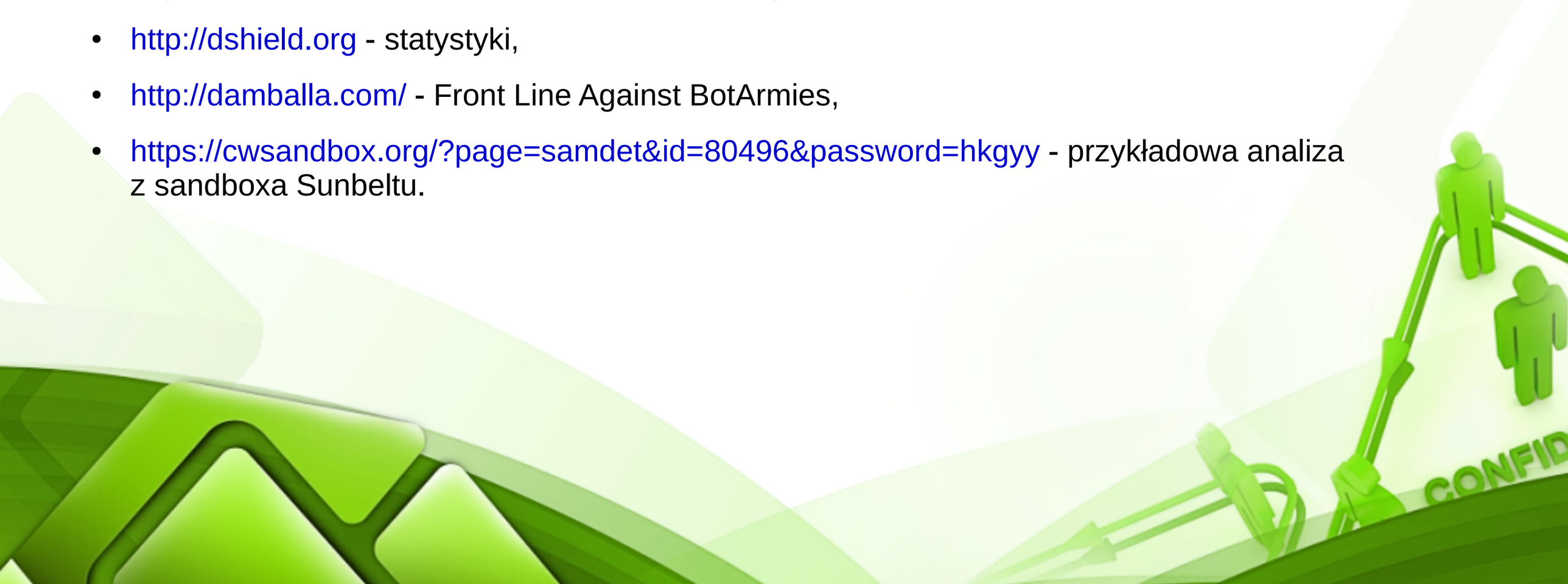
Linki

- http://bothunters.pl - Blog tropicieli botów,
- http://nepenthes.mwcollect.org - HomePage Nepenthesa,
- http://www.honeynet.org - strona projektu 'Honeynet',
- http://www.mwcollect.org - statystyki z ataków,
- http://honeynet.org/tools/index.html - alternatywne narzędzia do łapania malware'u,
- http://dshield.org - statystyki dotyczące ilości ataków w sieci,
- http://www.virustotal.com - strona zapewniająca skan pliku wieloma silnikami av,
- http://www.malwaredomains.com - domeny do blackholowania,
- http://doc.bleedingthreats.net/bin/view/Main/BlackHoleDNS - jak skonfigurowac serwer DNS Microsoftu i nie tylko do DNS blackholingu,
- http://www.norman.com/microsites/nsic/Submit/en - Norman Sandbox,



Linki

- http://ircproxy.packetconsulting.pl - ircproxy do badania konwersacji irca,
- http://kaneda.bohater.net/files/spamdetector.sh - spamdetector,
- http://www.spywareguide.com/ - Spyware Guide,
- http://research.sunbelt-software.com/Submit.aspx - Sunbelt Sandbox,
- http://dshield.org - statystyki,
- http://damballa.com/ - Front Line Against BotArmies,
- https://cwsandbox.org/?page=samdet&id=80496&password=hkgyy - przykładowa analiza z sandboxa Sunbeltu.



Zdjęcia

- http://www.hyscience.com/archives/Lane-Iran_Nuclear_Po.jpg
- http://flickr.com/photos/angelillo182/170068133/
- http://files.myopera.com/Numen/blog/browsers-logos.png
- http://flickr.com/photos/jnatividad/2566951902/
- http://flickr.com/photos/laloyd/801634032/
- http://flickr.com/photos/edglazar/460186475/
- http://flickr.com/photos/seanrayford/482058734/

LogicalTrust
www.logicaltrust.net

IT BCE BUSINESS CONSULTING EXPERTS

Dziękujemy za uwagę

Logicaltrust – IT Security Solutions

IT BCE sp. z o.o.

Borys Łącki - b.lacki@itbce.com
Patryk Dawidziuk - p.dawidziuk@itbce.com