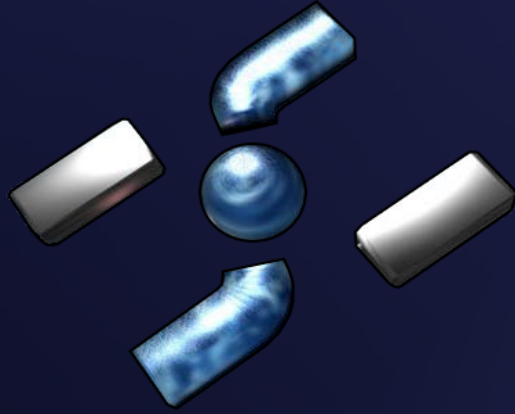


Hispace

Bankery versus użytkownicy

Przegląd popularnych trojanów bankowych

by Gynvael Coldwind



Hispace
<http://hispasec.com>



Vexillum
<http://vexillum.org>

Zagrożenia w bankowości internetowej

phishing i SE

Zagrożenia w bankowości internetowej

phishing i SE
MITM

Zagrożenia w bankowości internetowej

phishing i SE

MITM

słabe hasła

Zagrożenia w bankowości internetowej

phishing i SE

MITM

słabe hasła

malware

Twórcy i wektor ataku

Kto tworzy bankery ?

Twórcy i wektor ataku

Skąd się biorą na Twoim komputerze ?

MPack by Dream Coders Team

wejście na stronę

=

uruchomienie exploitu

=

banker wkracza do akcji

MPack by Dream Coders Team

Wersja v.85 zawierała:

MS06-014 (MDAC)

MS06-006 for Firefox 1.5.x & Opera 7.x (WMP)

unnamed 0day for Win2000 (ms06-044 - MMC)

XML overflow for XP\2k3 with delayed execution

WebViewFolderIcon overflow

WinZip ActiveX overflow

QuickTime overflow

ANI overflow

M-Pack by Dream Coders Team










M-Pack v0.90 stats

Attacked hosts (total - uniq)	
IE XP ALL	114721 - 96104
QuickTime	2175 - 2048
Win2000	7033 - 6260
Firefox	12885 - 12514
Opera7	1271 - 1264

Traffic (total - uniq)	
Total traff	159073 - 129089
Exploited	44804 - 35574
Loads count	17408 - 15968
Loader's response	38.85% - 44.89%
Efficiency 10.94% - 12.37%	

Browser stats (total)	
MSIE	4 0%
Opera	1 0%

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
 RU - Russian federation	112793 70.9%	12653 72.7%	11.22%
 UA - Ukraine	16666 10.5%	1670 9.6%	10.02%
 IT - Italy	7045 4.4%	593 3.4%	8.42%
 GE - Georgia	5775 3.6%	673 3.9%	11.65%
 BY - Belarus	5419 3.4%	657 3.8%	12.12%
 KZ - Kazakstan	3098 1.9%	376 2.2%	12.14%
 US - United states	1117 0.7%	50 0.3%	4.48%
 AZ - Azerbaijan	1060 0.7%	128 0.7%	12.08%
 MD - Moldova, republic of	683	101	14.70%

Delephant

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	Win-Trojan/Banker.4270080.B
AntiVir	-	-	TR/Spy.Banker.Gen
Authentium	-	-	W32/D_Banker!Generic
Avast	-	-	Win32:Banker-ERW
AVG	-	-	PSW.Banker4.AFLP
BitDefender	-	-	Trojan.Crypt.Delf.F
CAT-QuickHeal	-	-	-
ClamAV	-	-	-
DrWeb	-	-	Trojan.PWS.Banker.22474
eSafe	-	-	Suspicious File
eTrust-Vet	-	-	-
Ewido	-	-	Logger.Banker.nkj
F-Prot	-	-	W32/D_Banker!Generic
Fortinet	-	-	Banker.CG!tr.pws
GData	-	-	Trojan-Spy.Win32.Banker.nkj
Ikarus	-	-	Trojan-Spy.Win32.Banker.JU
K7AntiVirus	-	-	Trojan-Spy.Win32.Banker.nkj
Kaspersky	-	-	Trojan-Spy.Win32.Banker.nkj
McAfee	-	-	PWS-Banker.gen.cg
Microsoft	-	-	TrojanSpy:Win32/Bancos.gen!A
NOD32v2	-	-	probably a variant of Win32/Spy.Banker
Norman	-	-	W32/Banker.DBZO
Panda	-	-	Trj/Banker.FWD
PCTools	-	-	-
Rising	-	-	-
Sophos	-	-	Mal/Banspy-F
Sunbelt	-	-	Trojan-Spy.Win32.Banker.nkj
TheHacker	-	-	Trojan/Spy.Banker.nkj
TrendMicro	-	-	-
VBA32	-	-	Trojan-Spy.Win32.Banker.nkj
ViRobot	-	-	-
VirusBuster	-	-	-
Webwasher-Gateway	-	-	Trojan.Spy.Banker.Gen

Delephant

stworzony w Delphi

Delephant

stworzony w Delphi
spakowany waży 4 MB

Delephant = Delphi + elephant

stworzony w Delphi

spakowany waży 4 MB

...a rozpakowany 16 MB

Delephant

stworzony w Delphi
spakowany waży 4 MB
...a rozpakowany 16 MB
zawiera wiele obrazków

Delephant

Teclado Virtual Bankline

Atenção: digite a sua senha eletrônica no teclado abaixo:

0 ou 8 2 ou 7 5 ou 6 1 ou 9 3 ou 4

clique aqui clique aqui clique aqui clique aqui clique aqui

LIMPAR OK

Senha eletrônica: usada para acesso ao Bankline
Senha do cartão: usada para acesso ao Caixa Eletrônico

Para a mãe que é mestre-cuca, o **Crediário Automático Itaú** é a cozinha completa que ela sempre quis.

➔ Saiba Mais ➔ Contrate já

Dinheiro extra em sua conta corrente para você gastar como quiser.

Seu cartão de Segurança Itaú

Oscódigos que você deve digitar tem 4 dígitos e está na posição do seu **Cartão de Segurança Itaú**.

Verifique se você está com o seu **Cartão de Segurança Itaú**,

Nº	Codigo	Nº	Codigo	Nº	Codigo	Nº	Codigo
01	XXXX	11	XXXX	21	XXXX	31	XXXX
02	XXXX	12	XXXX	22	XXXX	32	XXXX
03	XXXX	13	XXXX	23	XXXX	33	XXXX
04	XXXX	14	XXXX	24	XXXX	34	XXXX
05	XXXX	15	XXXX	25	XXXX	35	XXXX
06	XXXX	16	XXXX	26	XXXX	36	XXXX
07	XXXX	17	XXXX	27	XXXX	37	XXXX
08	XXXX	18	XXXX	28	XXXX	38	XXXX
09	XXXX	19	XXXX	29	XXXX	39	XXXX
10	XXXX	20	XXXX	30	XXXX	40	XXXX

Digite apenas o número que fica do lado esquerdo do seu cartão magnético, acima do seu nome.

Consulte a [imagem do cartão](#) com a localização desse número.

Senha do Cartão: 6 Dígitos

Informe sua data de nascimento

ENTRAR >

? Em caso de dúvida, ligue para:
Grande São Paulo e localidades com DDD 11: 3019 1213 | Demais localidades: 0800 12 1314

NOVO PROCEDIMENTO DE ACESSO

Chave de Segurança Bradesco

Atenção
Cartão Chave de Segurança Bradesco

Para sua segurança, você deve informar somente desta vez, todos os números das chaves do seu cartão de Segurança Bradesco!

Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave	Nº Chave
01	11	21	31	41	51	61	
02	12	22	32	42	52	62	
03	13	23	33	43	53	63	
04	14	24	34	44	54	64	
05	15	25	35	45	55	65	
06	16	26	36	46	56	66	
07	17	27	37	47	57	67	
08	18	28	38	48	58	68	
09	19	29	39	49	59	69	
10	20	30	40	50	60	70	

REF:

CONFIRMAR

Importante:
Observe atentamente o número de referência do seu cartão.
Em caso de perda, roubo/furto ou extravio entre em contato com o **Fone Fácil Bradesco** ou sua **Agência**.

Tela 701

Delephant



Delephant

szuka znanego tytułu okna

Delephant

**szuka znanego tytułu okna
wstawia swoje okno w okno IE**

Delephant

szuka znanego tytułu okna
wstawia swoje okno w okno IE
wyświetla „stronę” banku

Delephant

szuka znanego tytułu okna
wstawia swoje okno w okno IE
wyświetla „stronę” banku
wysyła wprowadzone dane

Delephant w akcji

Projeto Fronteiras - Sinivem - INFOSEG - Windows Internet Explorer

https://www2.infoseg.gov.br/sinivem/

Live Search

Plik Edycja Widok Ulubione Narzędzia Pomoc

Projeto Fronteiras - Sinivem - INFOSEG

Ministério da Justiça

REDE INFOSEG
Secretaria Nacional de Segurança Pública - SENASP

SINIVEM
Sistema Nacional de Identificação de Veículos em Movimento
Projeto Fronteiras

Página Principal

ATENÇÃO! Sua senha é pessoal e intransferível. Mantenha-a sempre em segredo. Os usuários estão sujeitos ao [Código Penal Brasileiro](#).

CPF:

Senha: < OK Limpar

4	5	6	7	8	9	0	1	2	3
q	w	e	r	t	y	u	i	o	p
a	s	d	f	g	h	j	k	l	ç
z	x	c	v	b	n	m			

Caps - Contraste +

Gotowe

Internet | Tryb chroniony: włączony

100%

Delephant w akcji

Projeto Fronteiras - Sinivem - INFOSEG - Windows Internet Explorer

https://www2.infoseg.gov.br/sinivem/

Live Search

Plik Edycja Widok Ulubione Narzędzia Pomoc

Projeto Fronteiras - Sinivem - INFOSEG

Ministério da Justiça

REDE INFOSEG
Secretaria Nacional de Segurança Pública - SENASP

Quinta-feira, 22 de Novembro de 19107

[Página Principal](#)

ATENÇÃO! Sua senha é pessoal e intransferível. Mantenha-a sempre em segredo. Os usuários estão sujeitos ao Código Penal Brasileiro.

CPF:

Senha: < OK Limpar

7	8	9	0	1	2	3	4	5	6
q	w	e	r	t	y	u	i	o	p
a	s	d	f	g	h	j	k	l	ç
z	x	c	v	b	n	m			

Caps - Contraste +

Gotowe

Internet | Tryb chroniony: włączony

100%

Delephant w akcji

Projeto Fronteiras - Sinivem - INFOSEG - Windows Internet Explorer

https://www2.infoseg.gov.br/sinivem/

Live Search

Plik Edycja Widok Ulubione Narzędzia Pomoc

Projeto Fronteiras - Sinivem - INFOSEG

Ministério da Justiça

REDE INFOSEG
Secretaria Nacional de Segurança Pública - SENASP

Quinta-feira, 22 de Novembro de 19107

Página Principal

ATENÇÃO: Sua senha é pessoal e intransferível. Mantenha-a sempre em segredo. Os usuários estão sujeitos ao [Código Penal Brasileiro](#).

CPF:

Senha: < OK Limpar

7	8	9	0	1	2	3	4	5	6
q	w	e	r	t	y	u	i	o	p
a	s	d	f	g	h	j	k	l	ç
z		x	c	v	b	n	m		

Caps - Contraste +

Gotowe

Internet | Tryb chroniony: włączony


100%

Delephant w akcji

Projeto Fronteiras - Sinivem - INFOSEG - Windows Internet Explorer.txt - Notatnik

Plik Edycja Format Widok Pomoc

Ministério da Justiça

 **REDE INFOSEG**
Secretaria Nacional de Segurança Pública - SENASP

Quinta-feira, 22 de Novembro de 19107

[Página Principal](#)

ATENÇÃO! Sua senha é pessoal e intransferível. Mantenha-a sempre em segredo. Os usuários estão sujeitos ao [Código Penal Brasileiro](#).

CPF:

Senha: < OK Limpar

7	8	9	0	1	2	3	4	5	6
q	w	e	r	t	y	u	i	o	p
a	s	d	f	g	h	j	k	l	ç
z	x	c	v	b	n	m			

Caps - Contraste +

© 2004 - REDE INFOSEG - Esplanada dos Ministérios Edifício Anexo II, Andar Térreo, Infoseg, CEP - 70.064-900, Brasília - DF, Fone (61) 3429-9393

Delephant - podsumowanie

bardzo duży
łatwy do zauważenia
łatwy do usunięcia
...ale i tak skuteczny

Flash Faker

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	TR/Crypt.CFI.Gen
Authentium	-	-	-
Avast	-	-	Win32:Trojan-gen {Other}
AVG	-	-	-
BitDefender	-	-	-
CAT-QuickHeal	-	-	Backdoor.Agent.rex
ClamAV	-	-	-
DrWeb	-	-	-
eSafe	-	-	Suspicious File
eTrust-Vet	-	-	-
Ewido	-	-	-
F-Prot	-	-	-
F-Secure	-	-	Backdoor.Win32.Agent.rex
Fortinet	-	-	PossibleThreat
GData	-	-	Backdoor.Win32.Agent.rex
Ikarus	-	-	Backdoor.Win32.Agent.rex
K7AntiVirus	-	-	-
Kaspersky	-	-	Backdoor.Win32.Agent.rex
McAfee	-	-	-
Microsoft	-	-	PWS:Win32/Yessim.gen
NOD32v2	-	-	-
Norman	-	-	W32/Agent.HBLC
Panda	-	-	-
PCTools	-	-	-
Prevx1	-	-	Suspicious
Rising	-	-	-
Sophos	-	-	Mal/Emogen-N
Sunbelt	-	-	-
Symantec	-	-	Infostealer
TheHacker	-	-	-
TrendMicro	-	-	BKDR_AGENT.AORT
VBA32	-	-	suspected of Embedded.Trojan-Clicker.Win32.Agent.bbt
ViRobot	-	-	-
VirusBuster	-	-	-
Webwasher-Gateway	-	-	Trojan.Crypt.CFI.Gen

Flash Faker

zajmuje około 250KB

Flash Faker

zajmuje około 250KB

ściąga archiwum rar 3MB

Flash Faker

zajmuje około 250KB

ściąga archiwum rar 3MB

rozpakowuje z niego

fałszywe www banków etc

Flash Faker

zajmuje około 250KB

ściąga archiwum rar 3MB

rozpakowuje z niego

fałszywe www banków etc

podmienia strony w IE

Flash Faker

filmik :)

Flash Faker - podsumowanie

nieduży
łatwy do zauważenia
łatwy do usunięcia
...również skuteczny

Audio Video – zaczyna się robić ciekawie

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	TR/Crypt.XPACK.Gen
Authentium	-	-	-
Avast	-	-	Win32:Zbot-ANH
AVG	-	-	Pakes
BitDefender	-	-	Trojan.Generic.694885
CAT-QuickHeal	-	-	-
ClamAV	-	-	Trojan.Zbot-1988
DrWeb	-	-	modification of Trojan.Packed.424
eSafe	-	-	-
eTrust-Vet	-	-	-
Ewido	-	-	Logger.Zbot.djp
F-Prot	-	-	W32/Zbot.J3.gen!Eldorado
F-Secure	-	-	Trojan-Spy.Win32.Zbot.erk
Fortinet	-	-	W32/Cryp_Pai.5
GData	-	-	Trojan-Spy.Win32.Zbot.erk
Ikarus	-	-	Trojan-Spy.Win32.Zbot.anp
K7AntiVirus	-	-	Trojan-Spy.Win32.Zbot.erk
Kaspersky	-	-	Trojan-Spy.Win32.Zbot.erk
McAfee	-	-	-
Microsoft	-	-	VirTool:Win32/Obfuscator.BL
NOD32v2	-	-	a variant of Win32/Spy.Agent.PZ
Norman	-	-	W32/AntiVirus2008.HK
Panda	-	-	Trj/Sinowal.DW
PCTools	-	-	-
Prevx1	-	-	-
Rising	-	-	Trojan.Spy.Win32.Zbot.erk
Sophos	-	-	Mal/Packer
Sunbelt	-	-	Trojan-Spy.Win32.Zbot.erk
Symantec	-	-	-
TheHacker	-	-	-
TrendMicro	-	-	Cryp_Pai-5
VBA32	-	-	-
ViRobot	-	-	-
VirusBuster	-	-	-
Webwasher-Gateway	-	-	Trojan.Crypt.XPACK.Gen

Audio Video – zaczyna się robić ciekawie

zajmuje około 50KB

Audio Video – zaczyna się robić ciekawie

zajmuje około 50KB

ukrywa katalog z danymi i .exe

Audio Video – zaczyna się robić ciekawie

zajmuje około 50KB

ukrywa katalog z danymi i .exe

config w zew. pliku (zaszyfr.)

Audio Video – zaczyna się robić ciekawie

zajmuje około 50KB

ukrywa katalog z danymi i .exe

config w zew. pliku (zaszyfr.)

hookuje API sieciowe


Audio Video – zaczyna się robić ciekawie

filmik :)

Audio Video – Zeus

Zeus :: Bots

Information:

Profile: 
GMT date: 28.01.2008
GMT time: 23:26:56

Statistics:

Summary

Botnet:

→ Online bots
Remote commands

Logs:

Search
Search with template
Uploaded files

System:

Profiles
Profile
Options
Logout

Filter			
Countries:	<input type="text"/>	CompID's:	<input type="text"/>
Botnets:	<input type="text"/>	IP's:	<input type="text"/>
Type:			<input type="button" value="Outside NAT"/> <input type="button" value="Apply"/>


[Forward >>](#)

Result:									
#	CompID	Ver/Botnet	IP	Country	Socks	Proxy	Screenshot	Online time	Speed
1		1.0.2.11/nnn5		--			View	01:25:10	0.931
2		1.0.2.11/nnn5		--			View	00:20:58	0.656
3		1.0.2.11/nnn5		--			View	26:41:26	0.766
4		1.0.2.11/nnn5		--			View	01:01:36	0.651
5		1.0.2.11/nnn5		FR			View	07:03:39	2.922
6		1.0.2.11/nnn5		--			View	02:42:05	0.521
7		1.0.2.11/nnn5		TR			View	02:42:18	0.828
8		1.0.2.11/nnn5		EG			View	02:44:32	1.36
9		1.0.2.11/nnn5		PL			View	04:22:31	0.719
10		1.0.2.11/nnn5		PL			View	10:01:48	0.672
11		1.0.2.11/nnn5		MA			View	01:02:46	0.772
12		1.0.2.11/nnn5		BR			View	00:02:53	1.25
13		1.0.2.11/nnn5		PL			View	01:43:22	0.625
14		1.0.2.11/nnn5		PL			View	03:43:01	0.941
15		1.0.2.11/nnn5		UK			View	00:43:55	6.049
16		1.0.2.11/nnn5		--			View	00:23:43	0.719
17		1.0.2.11/nnn5		--			View	04:04:41	0.797
18		1.0.2.11/nnn5		TW			View	20:24:15	0.515
19		1.0.2.11/nnn5		MA			View	01:24:08	0.797
20		1.0.2.11/nnn5		US			View	07:31:51	0.531
21		1.0.2.11/nnn5		GE			View	00:24:35	0.735
22		1.0.2.11/nnn5		--			View	01:45:32	5.328
23		1.0.2.11/nnn5		RO			View	02:05:29	0.672
24		1.0.2.11/nnn5		PL			View	26:07:48	0.875
25		1.0.2.11/nnn5		CA			View	19:31:48	3.563
26		1.0.2.11/nnn5		GE			View	04:27:48	0.75

Audio Video – Zeus

Zeus :: Statistics

Information:

Profile: 
 GMT date: 04.02.2008
 GMT time: 10:48:53

Statistics:

→ Summary

Botnet:

Online bots
 Remote commands

Logs:

Search
 Search with template
 Uploaded files

System:

Profiles
 Profile
 Options

 Logout

Information

Total logs in database:	3001608
Time of first install:	21:47:11 16.10.2007
Total bots:	11205
Total active bots in 24 hours:	618

Botnet: Any >>

Installs (8131)	Reset	Online bots (167)	Reset
--	1274	US	33
US	999	--	27
TR	681	RU	15
RU	497	FR	10
DE	496	PL	8
IN	281	TR	7
AU	250	IN	6
PL	240	AU	5
UK	196	DE	5
CN	188	UK	4
FR	185	UA	3
MA	153	CN	3
IT	134	ES	3
BR	125	CA	3
ES	124	CZ	2
MX	124	BE	2
AR	105	VN	2
PE	102	BG	2
CA	101	TH	2
EG	94	IL	2
UA	86	AR	2
ID	86	SE	2
BE	69	HK	1
RO	65	SK	1
JP	65	BA	1
CZ	65	PH	1
NL	58	BY	1
IR	57	MA	1

Audio Video – podsumowanie

mały

trudny do wykrycia (rootkit r3)

„obsługuje” sporo banków

zaszyfrowane co się da

...jest bardzo skuteczny

XMLC – a jak się wabi Twój pies?

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	TR/Agent.acqe
Authentium	-	-	-
Avast	-	-	-
AVG	-	-	-
BitDefender	-	-	-
CAT-QuickHeal	-	-	Trojan.Agent.acqe
ClamAV	-	-	-
DrWeb	-	-	-
eSafe	-	-	-
eTrust-Vet	-	-	-
Ewido	-	-	Trojan.Agent.yei
F-Prot	-	-	-
F-Secure	-	-	Trojan.Win32.Agent.acqe
Fortinet	-	-	PossibleThreat
GData	-	-	Trojan.Win32.Agent.acqe
Ikarus	-	-	Trojan.Win32.BHO.f
K7AntiVirus	-	-	Trojan.Win32.Agent.acqe
Kaspersky	-	-	Trojan.Win32.Agent.acqe
McAfee	-	-	-
Microsoft	-	-	Trojan:Win32/Meredrop
NOD32v2	-	-	-
Norman	-	-	W32/Malware.DUDC
Panda	-	-	-
PCTools	-	-	-
Prevx1	-	-	Cloaked Malware
Rising	-	-	-
Sophos	-	-	-
Sunbelt	-	-	Trojan.Win32.Agent.acqe
Symantec	-	-	-
TheHacker	-	-	-
TrendMicro	-	-	-
VBA32	-	-	-
ViRobot	-	-	-
VirusBuster	-	-	Trojan.Agent.EXQS
Webwasher-Gateway	-	-	Trojan.Agent.acqe

XMLC – a jak się wabi Twój pies?

zajmuje około 70KB

XMLC – a jak się wabi Twój pies?

zajmuje około 70KB

jego config jest w XML

XMLC – a jak się wabi Twój pies?

zajmuje około 70KB

jego config jest w XML

działa jako BHO

XMLC – a jak się wabi Twój pies?

zajmuje około 70KB

jego config jest w XML

działa jako BHO

wstawia dodatkowe pola

XMLC – a jak się wabi Twój pies?

filmik :)

XMLC – a jak się wabi Twój pies?

```
<inject
url="cbonline"
before="name=password> </TD></TR>"
what="<TR>
<TD><FONT class=userinfo>&nbsp;
What is your favourite meal or restaurant?&nbsp;
</FONT></TD><TD align=left><INPUT tabIndex=1
type=password value=" name=pswdmword>
  </TD></TR>
[...]"
check="pswd">
</inject>
```

XMLC – a jak się wabi Twój pies?

Stats

Fakes

Settings

Autotransfers

Logs

Task

System

E-Gold

Sparkasse

Postbank

Accounts

Drops

Transfers

Powered by DMAPi

postbank: 0

Account Number	Info	Sum
Delete Selected		

XMLC – a jak się wabi Twój pies?

Stats

Fakes

Settings

Autotransfers

Logs

Task

System

Bot id:

Database

Users

Form Grabber

Screenshots

Tan Grabber

Other

Powered by D.M.A.P.I

причинам не работает
настройку убедитесь ч
граббером, т.е. его логи у
фильтра, вам нужно указ
(*) любое поле формы где вводится TAN (кроме поля самого TANa), и либо
порядковый номер поля, либо имя поля содержащего TAN

Login Data Filters

Tan Grabbing Filters

Powered by D.M.A.P.I

ах, где по каким-то
е чем добавлять
не ловится TAN
для создания нового
//, допустима маска

URL	Keyword	Tan field
<input type="checkbox"/> https://www.vr-networld-ebanking.de	DestinationBankname	Schmetterling
<input type="checkbox"/> https://www.dresdner-privat.de*ueberweisungs	apache	!3
<input type="checkbox"/> https://*gfs.nb.se	skrapkod1	!1
<input type="checkbox"/> https://*netbanking.ch	oneTimePwd	!5
<input type="checkbox"/> https://*finanzportal.fiducia.de	tan	!21
<input type="checkbox"/> https://eplusgiro.plusgirot.se	ENGANGS_KOD	!3
<input type="checkbox"/> https://eplusgiro.plusgirot.se	ENGANG	!9
<input type="checkbox"/> https://*gfs.nb.se	skrapkod1	!3
<input type="checkbox"/> https://icabanken.ica.se	Input1	!4
<input type="checkbox"/> https://*hembanken.danskebank.se	txiPassord	!24
<input type="checkbox"/> https://*hembanken.danskebank.se	gsLogon	!1
<input type="checkbox"/> https://postbanken.no	password	!2
<input type="checkbox"/> https://nettbankdrift.edb.com	otpassword	!3
<input type="checkbox"/> https://www.otpbankdirekt.hu	smsAzonosito	!2
<input type="checkbox"/> https://www.alpha.gr	OTP	!10
<input type="checkbox"/> https://internetbank.budapestbank.hu	codepart	!2
<input type="checkbox"/> https://www*1*.*handelsbanken.fi	PassWd	!2
<input type="checkbox"/> https://www*1.handelsbanken.fi	MPwd	!3
<input type="checkbox"/> https://www*.skandiabanken.se	onetimepin	!6
<input type="checkbox"/> https://activa.caixagalicia.es/*		ononCoor
<input type="checkbox"/> https://finanzportal.fiducia.de/eb*	ignore_txtVorlage	!13

Delete Selected

XMLC – podsumowanie

**mały
łatwy do znalezienia, jeśli się
o nim wie
„obsługuje” sporo banków
zaszyfrowane co się da
automatyczne transfery
...jest bardzo skuteczny**

MDCOCO

Antivirus	Version	Last Update	Result
AhnLab-V3	2008.9.12.2	2008.09.12	Win-Trojan/Banker.589824.J
AntiVir	7.8.1.28	2008.09.12	TR/Spy.Banker.ipz
Authentium	5.1.0.4	2008.09.12	W32/Banker.CFCL
Avast	4.8.1195.0	2008.09.11	Win32:Trojan-gen {Other}
AVG	8.0.0.161	2008.09.12	PSW.Banker4.TGO
BitDefender	7.2	2008.09.11	Generic.Banker.Delf.92144319
CAT-QuickHeal	9.50	2008.09.12	TrojanSpy.Banker.ipz
ClamAV	0.93.1	2008.09.12	-
DrWeb	4.44.0.09170	2008.09.12	Trojan.PWS.Banker.18049
eSafe	7.0.17.0	2008.09.11	Suspicious File
eTrust-Vet	31.6.6086	2008.09.12	-
Ewido	4.0	2008.09.11	-
F-Prot	4.4.4.56	2008.09.12	W32/Banker.CFCL
F-Secure	8.0.14332.0	2008.09.12	Trojan-Spy.Win32.Banker.ipz
Fortinet	3.113.0.0	2008.09.12	Spy/Banker
GData	19	2008.09.12	Trojan-Spy.Win32.Banker.ipz
Ikarus	T3.1.1.34.0	2008.09.12	Trojan-Spy.Win32.Banker.ipz
K7AntiVirus	7.10.452	2008.09.11	Trojan-Spy.Win32.Banker.CKIL
Kaspersky	7.0.0.125	2008.09.12	Trojan-Spy.Win32.Banker.ipz
McAfee	5382	2008.09.11	-
Microsoft	1.3903	2008.09.12	TrojanSpy:Win32/Brajur.A
NOD32v2	3437	2008.09.12	a variant of Win32/Spy.Banker.NXF
Norman	5.80.02	2008.09.12	W32/Banker.CKIL
Panda	9.0.0.4	2008.09.11	Trj/Banker.KPQ
PCTools	4.4.2.0	2008.09.11	TrojanSpy.Banker.AWOH
Prevx1	V2	2008.09.12	Suspicious
Rising	20.61.42.00	2008.09.12	-
Sophos	4.33.0	2008.09.12	Mal/Generic-A
Sunbelt	3.1.1628.1	2008.09.11	Trojan.Banker.Delf
Symantec	10	2008.09.12	Infostealer.Bancos
TheHacker	6.3.0.9.077	2008.09.10	Trojan/Spy.Banker.ipz
TrendMicro	8.700.0.1004	2008.09.12	-
VBA32	3.12.8.5	2008.09.10	Trojan-Spy.Win32.Banker.ipz
ViRobot	2008.9.11.1373	2008.09.11	-
VirusBuster	4.5.11.0	2008.09.11	TrojanSpy.Banker.AWOH
Webwasher-Gateway	6.6.2	2008.09.12	Trojan.Spy.Banker.ipz

MDCOCO

krótko, bo pewnie czas się kończy ;>

najpierw było logowanie

MDCOCO

krótko, bo pewnie czas się kończy ;>

**najpierw było logowanie
pojawiły się keyloggery**

MDCOCO

krótko, bo pewnie czas się kończy ;>

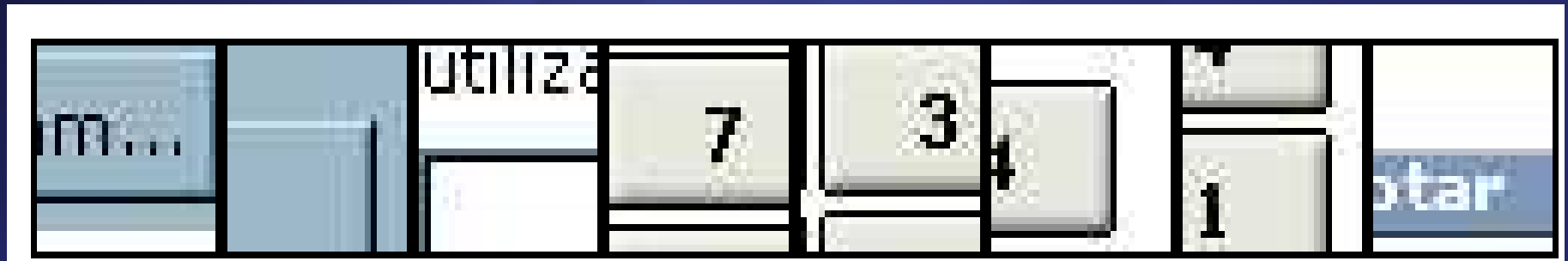
**najpierw było logowanie
pojawiły się keyloggery
stworzono wirtualne klawiatury**



MDCOCO

krótko, bo pewnie czas się kończy ;>

**najpierw było logowanie
pojawiły się keyloggery
stworzono wirtualne klawiatury
pojawiły się screen capture**



MDCOCO

krótko, bo pewnie czas się kończy ;>

najpierw było logowanie

pojawiły się keyloggery

stworzono wirtualne klawiatury

pojawiły się screen capture

stworzono maskowanie

MDCOCO

krótko, bo pewnie czas się kończy ;>

najpierw było logowanie

pojawiły się keyloggery

stworzono wirtualne klawiatury

pojawiły się screen capture

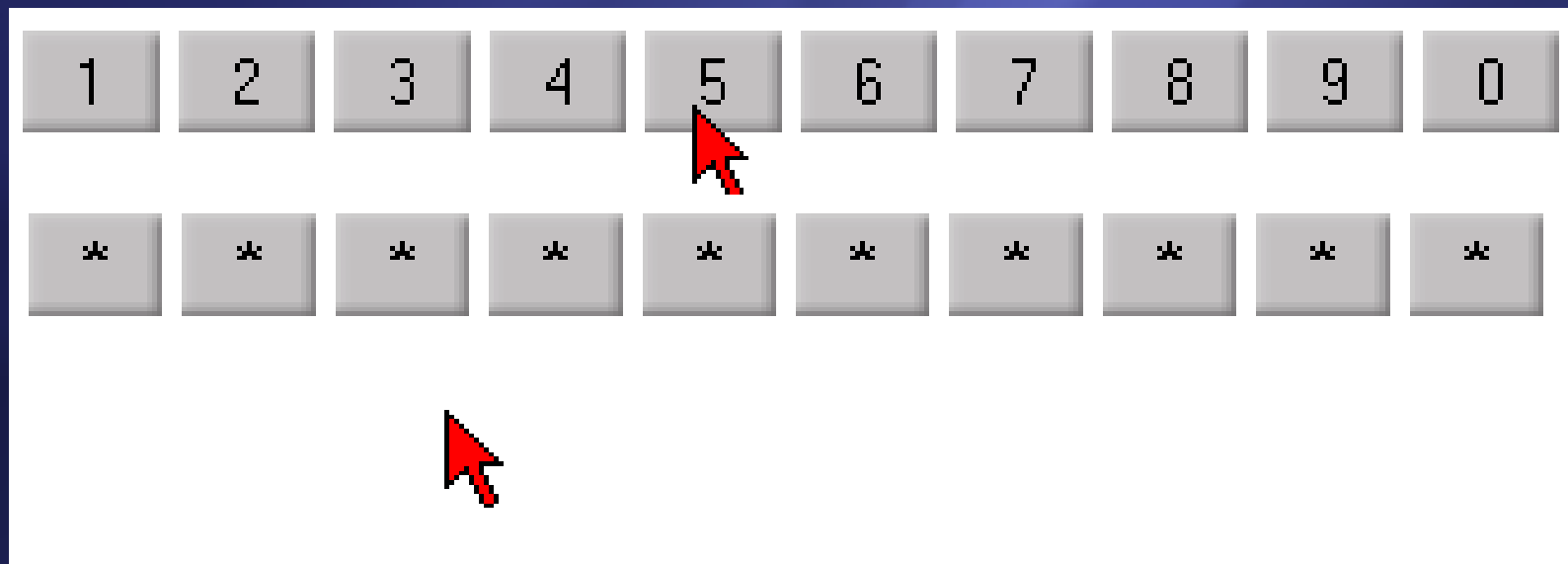
stworzono maskowanie

pojawił się MDCOCO

MDCOCO

krótko, bo pewnie czas się kończy ;>

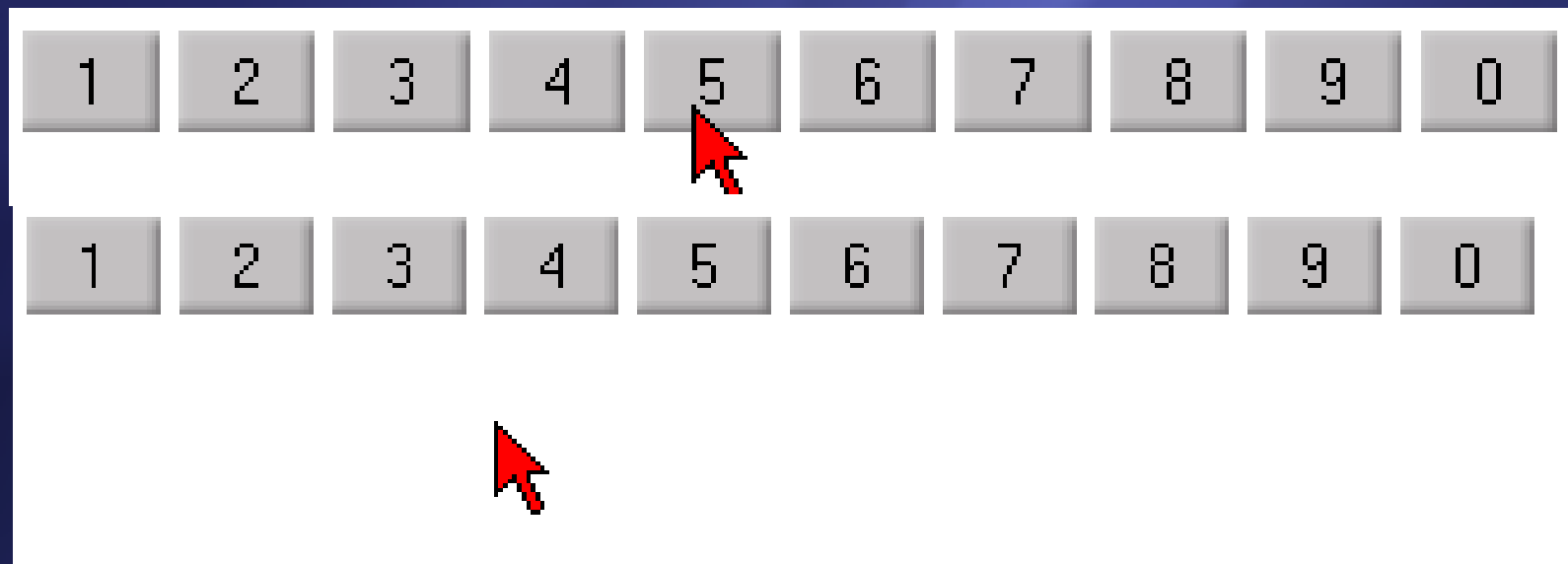
maskowanie



MDCOCO

krótko, bo pewnie czas się kończy ;>

maskowanie + MDCOCO



MDCOCO

krótko, bo pewnie czas się kończy ;>

Bez paniki :)

Sinowal i MBR Sinowal

all of your cash are belong to us

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	TR/PWS.Sinowal.Gen
Authentium	-	-	W32/Backdoor2.CDUL
Avast	-	-	Win32:Sinowal-DG
AVG	-	-	Generic11.FMA
BitDefender	-	-	Backdoor.Sinowal.D
CAT-QuickHeal	-	-	Backdoor.Sinowal.le
ClamAV	-	-	-
DrWeb	-	-	Trojan.Packed.585
eSafe	-	-	-
eTrust-Vet	-	-	-
Ewido	-	-	-
F-Prot	-	-	W32/Backdoor2.CDUL
F-Secure	-	-	Backdoor.Win32.Sinowal.le
Fortinet	-	-	W32/Sinowa.A!tr.bdr
GData	-	-	Backdoor.Win32.Sinowal.le
Ikarus	-	-	PWS.Win32.Sinowal.L
K7AntiVirus	-	-	Backdoor.Win32.Sinowal.le
Kaspersky	-	-	Backdoor.Win32.Sinowal.le
McAfee	-	-	New Win32.g4
Microsoft	-	-	PWS:Win32/Sinowal.gen!L
NOD32v2	-	-	a variant of Win32/Mebrook.Q
Norman	-	-	W32/Sinowal.gen8
Panda	-	-	-
PCTools	-	-	-
Prevx1	-	-	-
Rising	-	-	-
Sophos	-	-	Mal/Sinowa-A
Sunbelt	-	-	Backdoor.Win32.Sinowal.le
TheHacker	-	-	-
TrendMicro	-	-	-
VBA32	-	-	Backdoor.Win32.Sinowal.le
ViRobot	-	-	Backdoor.Win32.Sinowal.282944
VirusBuster	-	-	-
Webwasher-Gateway	-	-	Trojan.PWS.Sinowal.Gen

Sinowal i MBR Sinowal
all of your cash are belong to us

stara wersja:

DLL inject do wszystkich proc.

hookowanie API

nowa wersja:

zintegrowany rootkit MBR

Sinowal i MBR Sinowal

all of your cash are belong to us

Antivirus	Version	Last Update	Result
AhnLab-V3	-	-	-
AntiVir	-	-	TR/PWS.Sinowal.Gen
Authentium	-	-	W32/Backdoor2.CDUL
Avast	-	-	Win32:Sinowal-DG
AVG	-	-	Generic11.FMA
BitDefender	-	-	Backdoor.Sinowal.D
CAT-QuickHeal	-	-	Backdoor.Sinowal.le
ClamAV	-	-	-
DrWeb	-	-	Trojan.Packed.585
eSafe	-	-	-
eTrust-Vet	-	-	-
Ewido	-	-	-
F-Prot	-	-	W32/Backdoor2.CDUL
F-Secure	-	-	Backdoor.Win32.Sinowal.le
Fortinet	-	-	W32/Sinowa.A!tr.bdr
GData	-	-	Backdoor.Win32.Sinowal.le
Ikarus	-	-	PWS.Win32.Sinowal.L
K7AntiVirus	-	-	Backdoor.Win32.Sinowal.le
Kaspersky	-	-	Backdoor.Win32.Sinowal.le
McAfee	-	-	New Win32.g4
Microsoft	-	-	PWS:Win32/Sinowal.gen!L
NOD32v2	-	-	a variant of Win32/Mebrook.Q
Norman	-	-	W32/Sinowal.gen8
Panda	-	-	-
PCTools	-	-	-
Prevx1	-	-	-
Rising	-	-	-
Sophos	-	-	Mal/Sinowa-A
Sunbelt	-	-	Backdoor.Win32.Sinowal.le
TheHacker	-	-	-
TrendMicro	-	-	-
VBA32	-	-	Backdoor.Win32.Sinowal.le
ViRobot	-	-	Backdoor.Win32.Sinowal.282944
VirusBuster	-	-	-
Webwasher-Gateway	-	-	Trojan.PWS.Sinowal.Gen

Podsumowanie

Nie dać się zarazić :)
Inaczej jest game over...

Pytania i kontakt

Czy są jakieś pytania ? :)

e-mail

michael@hispasec.com

gynvael@coldwind.pl

WWW

<http://hispasec.com>

<http://gynvael.coldwind.pl>