20th Annual FIRST Conference

Cyber Fraud Trends - Authentication

Ralph Thomas - iDefense Malcode Intelligence
rthomas@idefense.com, +1.571.723.1978

June, 2008

Cyber Fraud Disruptors

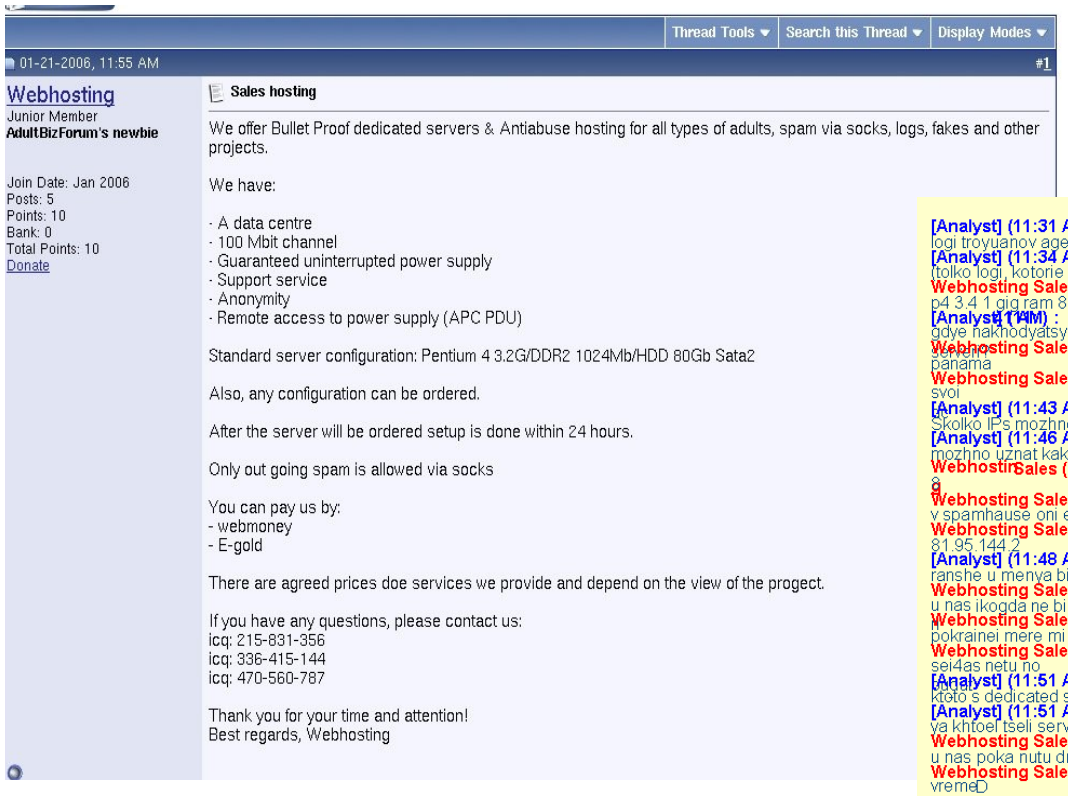
- Anti-virus
  - Stopped static malware
  - Packers and scrambling is now common practice
- Windows XP SP2 Firewall
  - Enabled by default
  - Stopped malware from coming to the computer
  - Start of drive-by installs via browser exploitation (get the victim to go to the malware)
- Windows Vista Firewall
  - Outbound filtering enabled by default (incl. phishing filters)
  - Limit drive-by installations
  - Limit malware from phoning home
  - *Essential for attackers to maintain untainted/volatile hosting*
    --> Bulletproof Hosting
- 2FA Deployment
  - *Underground economy changes*
    --> Adjusted Behaviour

Cyber Fraud Disruptors

- Essential for attackers to maintain untainted/volatile hosting
  --> **Bulletproof Hosting**
- Underground economy changes
  --> Adjusted Behaviour

Bulletproof Hosting

- The Truth About RBN
  - All public customers on one network
  - Not secretive at all, heavily spammed ads on many forums



Thread Tools ▾ | Search this Thread ▾ | Display Modes ▾

01-21-2006, 11:55 AM #1

Webhosting
Junior Member
AdultBizForum's newbie

Join Date: Jan 2006
Posts: 5
Points: 10
Bank: 0
Total Points: 10
Donate

Sales hosting

We offer Bullet Proof dedicated servers & Antiabuse hosting for all types of adults, spam via socks, logs, fakes and other projects.

We have:

- A data centre
- 100 Mbit channel
- Guaranteed uninterrupted power supply
- Support service
- Anonymity
- Remote access to power supply (APC PDU)

Standard server configuration: Pentium 4 3.2G/DDR2 1024Mb/HDD 80Gb Sata2

Also, any configuration can be ordered.

After the server will be ordered setup is done within 24 hours.

Only out going spam is allowed via socks

You can pay us by:
- webmoney
- E-gold

There are agreed prices doe services we provide and depend on the view of the progect.

If you have any questions, please contact us:
icq: 215-831-356
icq: 336-415-144
icq: 470-560-787

Thank you for your time and attention!
Best regards, Webhosting

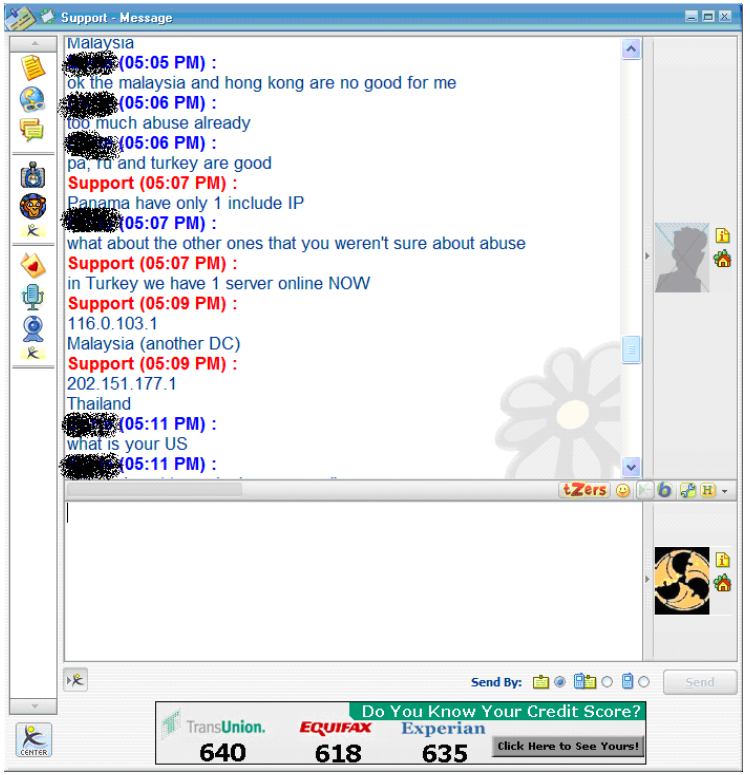
[Analyst] (11:31 AM) :
logi troyuanov agentdq
[Analyst] (11:34 AM) :
(tolko logi, kotorie ya instraliriyu iz drugovo mesta)
Webhosting Sales (11:38 AM) :
p4 3.4 1 gig ram 80 sata2 600$ month
[Analyst] (11:40 AM) :
gdye nakhodyatsya
Webhosting Sales (11:41 AM) :
panama
Webhosting Sales (11:41 AM) :
svoi
[Analyst] (11:43 AM) :
Skolko IPs mozhno est?
[Analyst] (11:46 AM) :
mozhno uznat kakie IP nomeri zaranee, i test ikh portiv blocklists?
Webhosting Sales (11:46 AM) :
8
Webhosting Sales (11:46 AM) :
v spamhause oni estr
Webhosting Sales (11:46 AM) :
81.95.144.2
[Analyst] (11:48 AM) :
ranshe u menya bil VPS na 81.95.x i u menya bil problemi. U vas eshe IP ranges?
Webhosting Sales (11:49 AM) :
u nas ikogda ne bilo VPS
Webhosting Sales (11:50 AM) :
pokrainei mere mi ne prodavali vps ludam
Webhosting Sales (11:50 AM) :
sei4as netu no
[Analyst] (11:51 AM) :
ktoto s dedicated server pordoval menye
[Analyst] (11:51 AM) :
ya khtoel tseli server, no mozhet
Webhosting Sales (11:52 AM) :
u nas poka nutu drugih
Webhosting Sales (11:52 AM) :
vremeD
n

Bulletproof Hosting

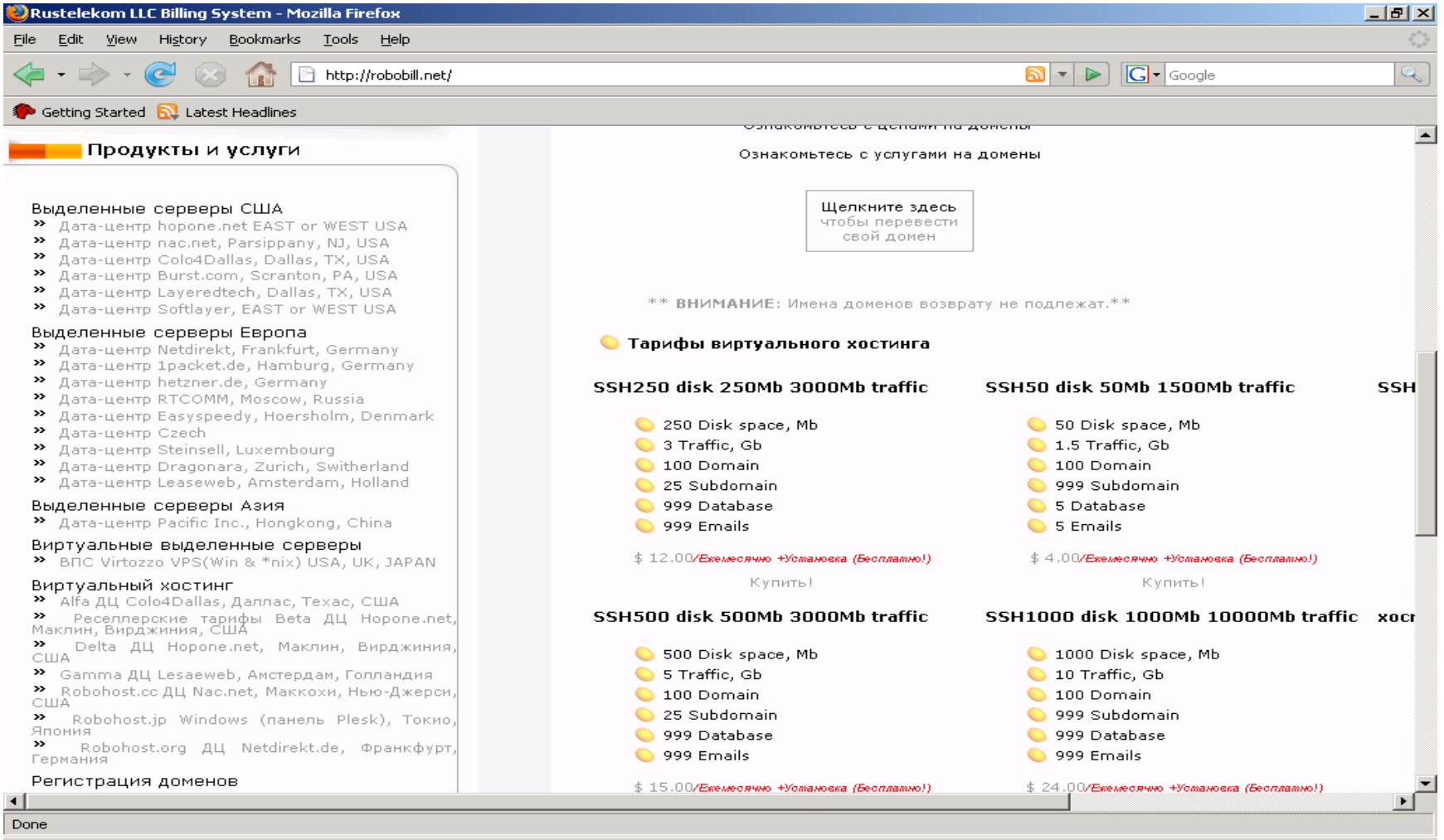
- The Post-RBN Era
  - Most popular providers existed well before the fall of RBN
  - Competitors to RBN, no proven connections to leadership
  - Common customers is NOT evidence of common leadership
    - McColo
    - AbdAllah
    - RentaBL

Bulletproof Hosting - AbdAllah

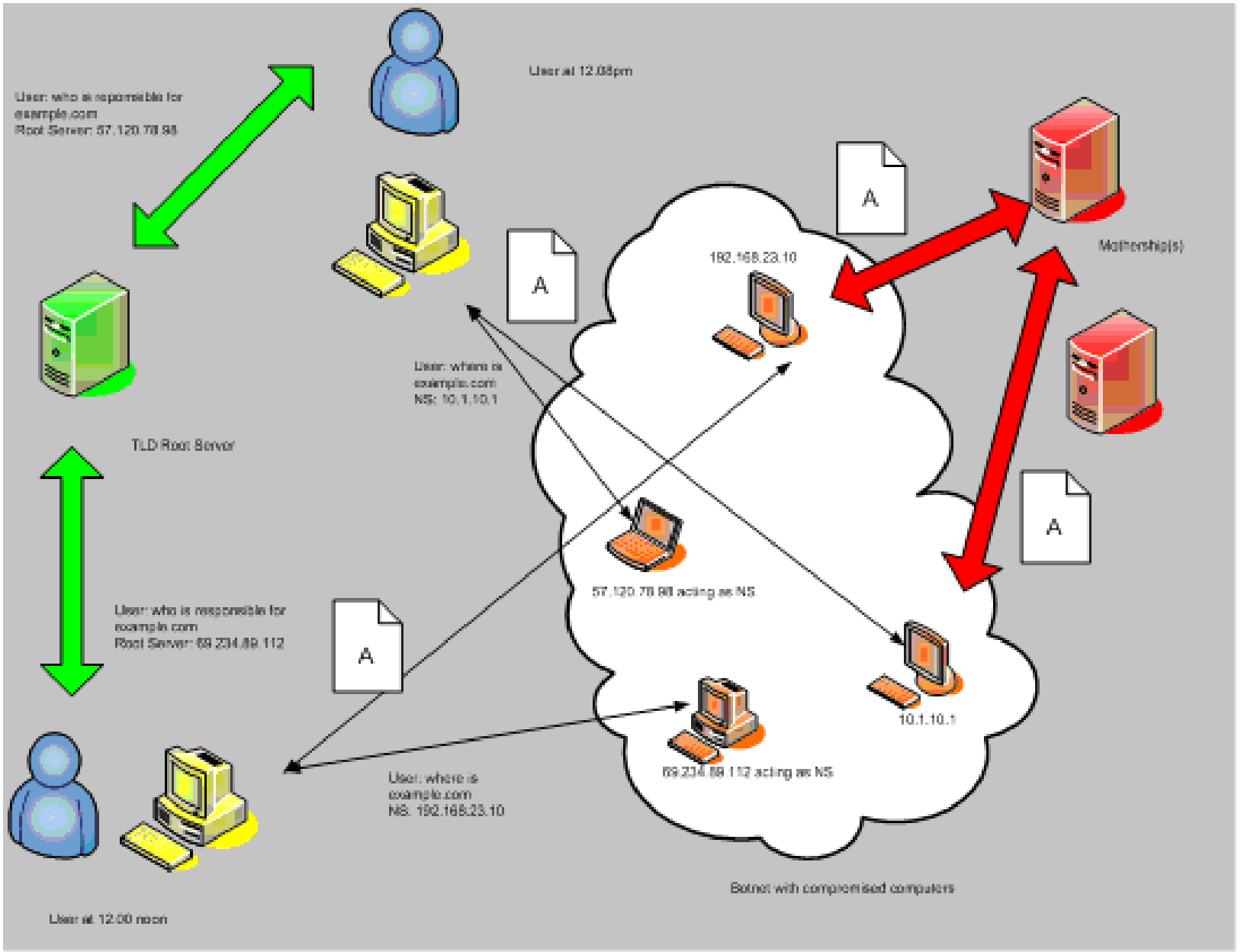
- Reseller of a coalition of bulletproof hosts
- Controls one network, resells the rest



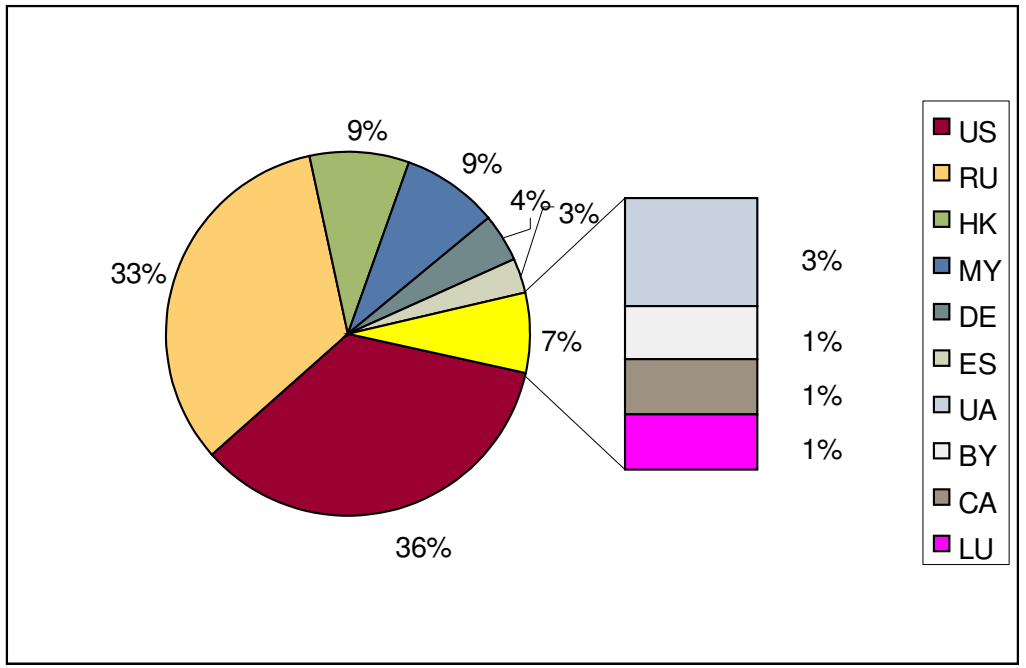
Bulletproof Hosting

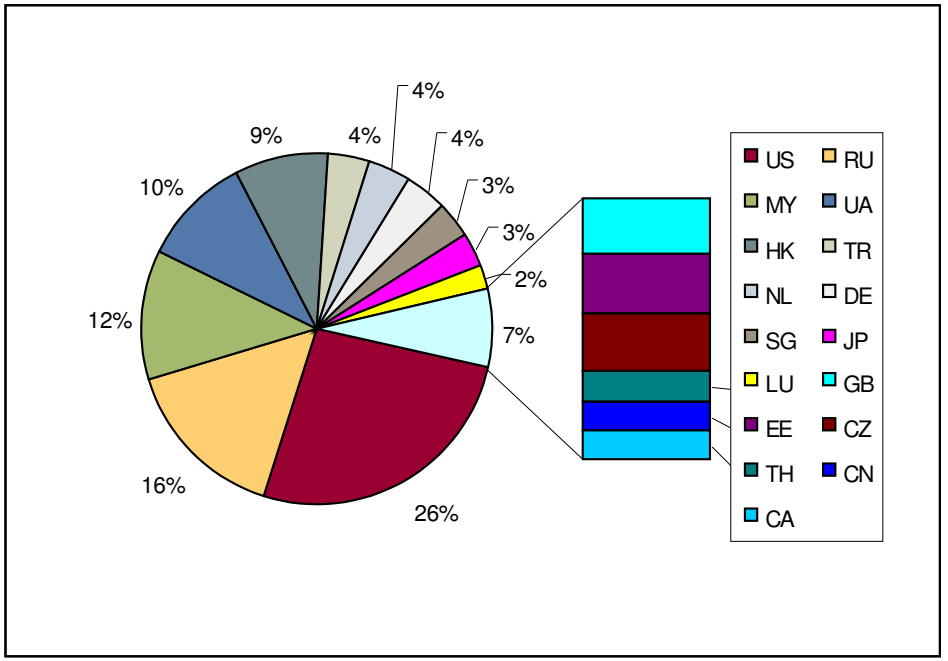


"Bulletproof Hosting" - Fastflux



Bulletproof Hosting





Cyber Fraud Disruptors

- Essential for attackers to maintain untainted/volatile hosting
  --> Bulletproof Hosting
- Underground economy changes
  --> **Adjusted Behaviour**

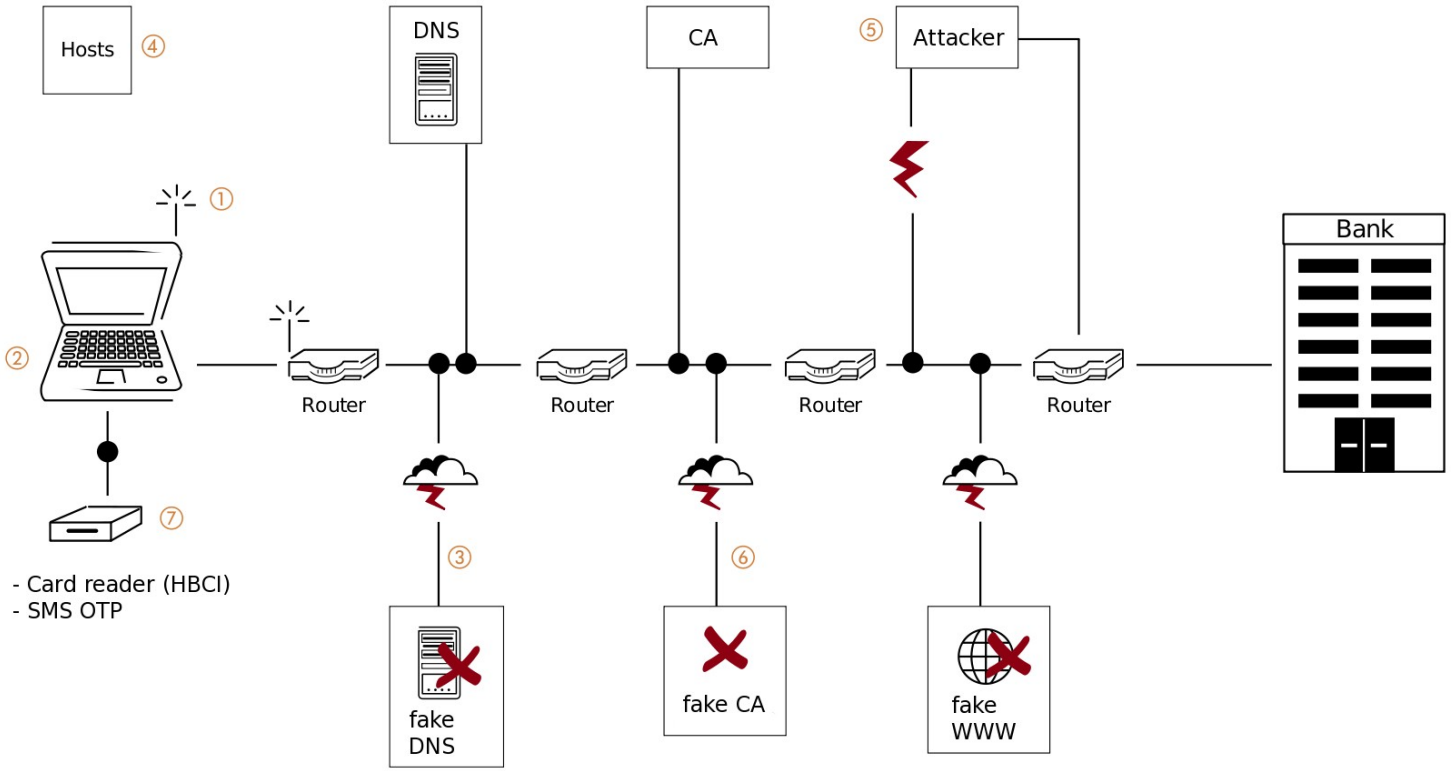
Adjusted Behavior

- Fraud is more difficult/complex
  - give up! **(not going to happen anytime soon)**
  - keep current tactics and change targets
    - go for the smaller fish, drastic increase of phishing attacks against smaller institutions, which are now faced with a 'new' problem
  - stay with current targets and adjust tactics
    - due to 2FA, stolen credentials are stale
    - move from phishing/pharming to malware
- All internet users are affected
  - financial (e-banking, e-brokerage)
  - e-commerce, e-recruitment, communication (e-mail, IM, blogs/forums/groups, ...)
  - persistent environments, social networks, and gaming

Ambush: e-Consumers Under Attack

1) WLAN: Invite for eavesdropping
2) Fake User: I am not me
3) Detour into the bandit's camp: DNS spoof
4) Deceptive Guidepost: The hosts file

1) Trojans: Bogus Software
2) With counterfeit passport into the vault
3) Enter PIN: The crooks read along



Ambush: e-Consumers Under Attack

- Phishing & Pharming
  - Lure victims via social engineering and tempering with DNS to fraudulent webpage designed to steal personal identifiable information (PII)
- Man-in-the-middle (MITM)
  - Fraudulent webpage designed to instantly defraud victims in order to circumvent temporary 2FA means
- Malware
  - Hostile software installed on the victim's computer designed to steal PII or to perform MITM. This compromises the consumer's communication endpoint.

Strong Authentication

- Many choices for client-side authentication
  - Smart card
  - USB Token
  - Virtual Token
  - OTP Token
  - Scratch Pad
  - Certificate
  - Biometrics
  - Phone/Cell/SMS
  - etc.
- Mutual (2-way) authentication
- Account vs. Transaction Authentication
- Implementation is key
  - e.g. cell phone as OTP Token vs. mTAN
  - e.g. OTP token timeout at BR bank
  - e.g. weakness in business process: change phone number

Strong Authentication

Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.	TAN	Nr.
1	687716	31	842387	61	723733	91	012518	121
2	163690	32	559269	62	164612	92	001711	122
3	908192	33	900620	63	491715	93	686908	123
4	603268	34	950912	64	858265	94	549263	124
5	637410	35	131290	65	500439	95	837088	125
6	632961	36	734080	66	832015	96	426360	126
7	028567	37	872269	67	[illegible]	97	553098	127
8	179016	38	301940	68	212578	98	784526	128
9	888375	39	038797	69	784722	99	475780	129
10	606687	40	780513	70	115323	100	884085	130
11	051256	41	807036	71	040492	101	563935	131
12	647111	42	085357	72	637365	102	475779	132
13	529030	43	508000	73	470604	103	867445	133
14	844281	44	781571	74	217050	104	049606	134
15	714599	45	484862	75	790635	105	361909	135
16	930386	46	489429	76	336037	106	376870	136
17	415784	47	372715	77	449721	107	990906	137
18	662879	48	270335	78	345867	108	984350	138
19	516339	49	253155	79	078398	109	199615	139
20	720656	50	943781	80	674680	110	748216	140
21	007656	51	024151	81	073888	111	583864	141
22	182770	52	324678	82	251299	112	360451	142
23	256019	53	797344	83	209347	113	249027	143
24	090062	54	914072	84	837084	114	265513	144
25	792450	55	922216	85	513496	115	149817	145
26	432141	56	007464	86	659760	116	653549	146
27	926541	57	689751	87	287030	117	551854	147
28	895181	58	858066	88	693494	118	537888	148
29	289812	59	602244	89	441575	119	746229	149
30	782360	60	989895	90	315754	120	605609	150

Q + A

Ralph Thomas - iDefense Malcode Intelligence
rthomas@idefense.com, +1.571.723.1978

May 28, 2008