Subject: Big confesion to make.
Posted by jnz on Sun, 01 Apr 2007 21:30:49 GMT
View Forum Message <> Reply to Message

Blazer wrote on Sat, 03 February 2007 12:24Tonight I ran into one of the most extrme cheaters I have ever encountered. Here is a profile of this scum bag:

* Usually he impersonates moderators while cheating and kicks people who question him
* Apparently he often frequents the same servers, and knows who all of the mods are (so he can fake their name).
* He has used over 160 names (I got tired of counting) on the RenGuard network alone.
* He uses the *cheat name removed* bypass, which randomizes his serial hash and makes it appear that he is using RG.
* He has typical script-kiddie "how dare you challenge me" mentality (when I started to ban him he connected as another mod
name and gameover'd the server).
* Can easily and quickly change his IP address (can be kicked and rejoin with a new IP in less than 60 seconds)
* His ISP operates on at least two class A net blocks, so no only do usually the last 2 octets of his IP change, all 4 can as

well. I would distrust anyone from 88.x.x.x and 82.x.x.x
* From the looks of the logs, this guy has been doing this (cheating and using mods names) for a long time.

I discovered him because genlkozar was outside playing basketball, and I suddenly noticed that "he" was playing in the
n00bstories server. I immediately kick-banned him, and he quickly came back as a different moderators name, but was auto-banned
for having the same IP. He quickly came back with a new IP, as another moderators name. I banned this name as well and he
joined with yet another IP and another moderator name, and did a gameover on the server. I banned several more attempts from
him, including him connecting to the server with names like "Blazer" and "Kozar".

He also connected to n00bstories IRC as Cm2Play, probably to check out the game server channel:

```
[02:14:40] -ownage.n00bstories.com- *** Notice -- Client connecting at home.n00bstories.com: Cm2Play

(bad_ex_199@bzq-88-155-193-50.red.bezeqint.net)
[02:16:44] -ownage.n00bstories.com- *** Notice -- Client exiting at home.n00bstories.com:

Cm2Play!bad_ex_199@bzq-88-155-193-50.red.bezeqint.net (Quit: )
```

Here are some excepts from the IRC channel:

```
[01:50:43] [n00bsvr01]: Host: [BR] genlkozar is being KICK-BANNED by Blazer@IRC for: faking a
```

```
mod
[01:55:17] [n00bsvr01]: Player greb joined the game
[01:55:21] [n00bsvr01]: Host: [BR] greb has been BANNED on 02.03.2007 by Blazer@IRC for:
faking a mod
[01:55:21] [n00bsvr01]: Player greb left the game
[01:56:34] [n00bsvr01]: Player try_lee joined the game
[01:56:37] [n00bsvr01]: Host: [BR] try_lee has been BANNED on 02.03.2007 by Blazer@IRC for:
faking a mod
[01:56:37] [n00bsvr01]: Player try_lee left the game
[02:10:19] [@phpRenBot]: [39/40|50SFPS|Islands] Player Kozar joined the game, fighting for
team GDI (IP: 88.155.110.241)
[02:10:24] [@phpRenBot]: [39/40|50SFPS|Islands] Host: Kozar is being kicked by RenGuard for:
CHEATING
[02:11:11] [@phpRenBot]: [41/40|52SFPS|Islands] Player Cm2Play joined the game, fighting for
team GDI (IP: 88.155.195.113)
[02:11:24] [@phpRenBot]: [40/40|42SFPS|Islands] [Team] Cm2Play: !help
[02:11:19] [@phpRenBot]: [40/40|42SFPS|Islands] [Team] Cm2Play: !showmods
[02:11:20] [@phpRenBot]: [40/40|42SFPS|Islands] Host: InGame Moderators: &arnyswart
&Cm2Play
[02:11:33] [@phpRenBot]: [40/40|42SFPS|Islands] [Team] Cm2Play: !gameover
[02:11:33] [@phpRenBot]: [40/40|42SFPS|Islands] Host: Usage: !gameover NOW -CASE
SENSITIVE! TO AVOID ACCIDENTAL TRIGGERING
[02:11:44] [@phpRenBot]: [40/40|49SFPS|Islands] [Team] Cm2Play: !gameover NOW
[02:11:45] [@phpRenBot]: [40/40|49SFPS|Islands] [EVENT] The map has ended.
[02:11:55] [@phpRenBot]: [35/40|57SFPS|Islands] Cm2Play was kicked
[02:13:11] [@phpRenBot]: [34/40|59SFPS|City_Flying] Player sterps joined the game, fighting for
team Nod (IP: 88.155.195.113)
[02:13:12] [@phpRenBot]: [33/40|59SFPS|City_Flying] Player sterps left the game
[02:13:55] [@phpRenBot]: [35/40|56SFPS|City_Flying] Player Cm2Play joined the game, fighting
for team Nod (IP: 88.155.193.50)
[02:13:56] [@phpRenBot]: [34/40|56SFPS|City_Flying] Cm2Play was kicked
[02:15:44] [@phpRenBot]: [33/40|59SFPS|City_Flying] Player Blazer joined the game, fighting for
team Nod (IP: 88.154.8.203)
[02:16:09] [@phpRenBot]: [33/40|57SFPS|City_Flying] Host: Blazer is being kicked by RenGuard
for: RenGuard not running anymore.
[02:16:10] [@phpRenBot]: [32/40|57SFPS|City_Flying] Player Blazer left the game
[02:16:10] [@phpRenBot]: [32/40|57SFPS|City_Flying] Blazer was kicked
```

Names used on RenGuard (note many names are known server admins and mods that were exploited):

LGdirk
genlkozar
2020_Eagle_Eye
greb
try_lee
Cm2Play
blalbgfbgf

banzku
erikboxem
-=(MWV)==Sizzle06
theOne
bruupo
Muragoeth
Dot`
Knabber
remonbara
MHAH77
SteelMario
OR257
SP33D30
SSniper65
SaKo-
Xsmnti2131
E=P=E|RT~E|
ravesshaw
nonosocr1986

---

MoReS
mores01
XxshirlxX
=E=PRO=E=
alontavor
EagleEye
XsmntiSniper
xXxM3
poplkilrs
Poxi-Scout
nonosocr1986
1=ST=1
E=P=E<~SI~>
nawras1999
BlackDemon
`"`
BaCKTOYOU
E=P=E|RT~E|
Xsmnti
MassivePlayer
Wizard
=E=PRO=E=
$t4y=====3QUiLiBriUM
MassivePlayer-back&better-than-ever-
$eX0oN
nonosocr1986
cac33
justtokillyou

BlackDemonRooster
just-tokillyou
DeadHunter
Sermig
TrIxoNtro
remonbara
ropiy|
Blazer
ravesshaw
1231
Demon1211
dude`
striipp
striip|
Bo$$Wi$$aM
bosswj
OR257
BlackMan
DAM
bosswj
arabweeder
cac33
Èsosoma
©sosoma
sosoma
killernum1
Don'tMoveUDie
E=P=E<~SI-Ret.~>
|soap
Òsoap
soap.
ERetIclE
`babababaaaa
sway
Snip3rX55
trr...
```111
Snip3rX55
!
~!@#$^&*()
-BiO-Anubis_Orr
drkzigggo
lest
nonosocr1986
`lest
M0RES[SI]
soap
soap`
```

TriKo
Ba3sa
noooooob
DEATH
bambam
-=(MWV)=-Sizzle06
iMaStErMi
AM_New
TiX0S
E=P=E<~SI-Ret.~>
1=ST=1
Terrafire
alontavor
NaP
Sexy
LoL
DAMMIT
Becker
``!!
nonosocr1986
killer
dodokilll
dal11
Xsmnti#1
$aK0
Devile
Xsmnti
urdad2
urdad3
urdad4
bonbon
$eX0oN
kikik
Kill
VolMieR
maurice70
VolMieR
/!||.__.,||,_lL!_|.,..,_/
wachief
PRO_E-Ghost<~SI-E~>
zipzipsai
<~PRO~>E<~SI-E~>
B=M6=B
BlackHawkCat
cac32
IMaStErMI
VolMieR
ProE|RT~E|

raboy06
OR257
oren1944
PRO_E-Ghost<~SI~>
skd2000
[SNP]=MaStErM=
[SNP]=MaStErM=(L)
imbaguy
alontavor

Sample of known IPs (don' trust anything from 88.x.x.x, 82.x.x.x, or *.bezeqint.net
88.152.172.4
88.152.94.102
88.154.136.64
88.154.157.188
88.153.236.176
88.153.62.57
82.81.175.165
88.154.191.190
88.154.90.48
88.154.16.240
88.154.1.208
88.154.229.61
88.152.172.4
88.154.38.124
88.152.24.29

```
OrgName:    RIPE Network Coordination Centre
OrgID:      RIPE
Address:    P.O. Box 10096
City:       Amsterdam
StateProv:
PostalCode: 1001EB
Country:    NL
NetRange:   88.0.0.0 - 88.255.255.255
NetRange:   82.0.0.0 - 82.255.255.255
```

latest serial hash: 29d0b842e9a023fa25ac7eb936189d58 (probably random)

Sample Web Log Hits:

```
apathbeyond.com.log:88.155.14.216 - - [31/Jan/2007:06:11:42 -0600] "GET
/forum/style_emoticons/default/emot-q.gif HTTP/1.1" 200 803
"http://forums.relicnews.com/showthread.php?t=91416&page=40&pp=15" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
```

```
rengaurd.com.log:88.155.0.50 - - [28/Jan/2007:10:42:04 -0600] "GET
/_client_html/server_motd.php?id=1110020259&name=arabweeder HTTP/1.1" 200 5238 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"

rengaurd.com.log:88.155.180.151 - - [02/Feb/2007:10:16:32 -0600] "GET
/_client_html/server_motd.php?id=1190504956&name=SSniper65 HTTP/1.1" 200 3912 "-"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; MEGAUPLOAD 1.0)

rengaurd.com.log:88.155.110.241 - - [03/Feb/2007:10:08:34 +0100] "GET
/_client_html/server_motd.php?id=1385962457&name=egg098 HTTP/1.1" 200 5168 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; MEGAUPLOAD 1.0)"

rengaurd.com.log:88.155.110.241 - - [03/Feb/2007:03:09:31 -0600] "GET
/_client_html/server_motd.php?id=1385962457&name=Barry HTTP/1.1" 200 5172 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; MEGAUPLOAD 1.0)"

rengaurd.com.log:88.155.110.241 - - [03/Feb/2007:03:10:18 -0600] "GET
/_client_html/server_motd.php?id=1385962457&name=Kozar HTTP/1.1" 200 5172 "-" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; MEGAUPLOAD 1.0)"

rengaurd.com.log:88.155.195.113 - - [03/Feb/2007:03:11:17 -0600] "GET
/_client_html/images/banner_nod_kane.jpg HTTP/1.1" 304 - "
http://www.rengaurd.com/_client_html/server_motd.php?id=1385962457&name=Cm2P lay"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; MEGAUPLOAD 1.0)"

apathbeyond.com.log:88.155.14.216 - - [01/Feb/2007:12:29:09 -0600] "GET
/forum/style_emoticons/default/emot-q.gif HTTP/1.1" 200 803
"http://forums.relicnews.com/showthread.php?t=91416&page=41&pp=15" "Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
```

^^ was me