

<http://handlers.sans.org/pbueno/ma5.html>

MALWARE ANALYSIS - PART 5

MD5 of the available file: ecd45b584f7a1e50bb044646f4abb0be
Name of the file: cretzu.exe-orig-ecd45b584f7a1e50bb044646f4abb0be

MD5 of the zip file with password [infected]= ecd45b584f7a1e50bb044646f4f3113t
<http://handlers.sans.org/pbueno/cretzu.exe.zip>

1. Is this file packed? If so, which packer?

Yes, it was first packed with UPX; running strings against the cretzu.exe file shows the header of the UPX packer: "UPX0 UPX1"

testing cretzu.exe-orig-ecd45b584f7a1e50bb044646f4abb0be [OK]

MD5 of the packed file=ecd45b584f7a1e50bb044646f4abb0be
MD5 of the unpacked file=74e52f90026f6d2c39f73649b9854221
Size of the packed file=849,319
Size of the unpacked file=894,375

Using the upx packer you can verify the file as an upx file and uncompress it.

Doing the same against the uncompressed file shows it is compressed with rar "WinRAR SFX", using rar to test the file shows all files that are going to be found later on the infected system:

Testing archive cretzu.upx.exe

□[0;1;37;47m; [> owned by mad ! <]

Testing	aliases.ini
Testing	control.ini
Testing	mirco.ico
Testing	mirco.ini
Testing	moo.dll
Testing	nicks.txt
Testing	perform.ini
Testing	popups.ini
Testing	radmin.txt
Testing	remote.ini
Testing	run.exe
Testing	script.ini
Testing	servers.ini
Testing	sup.bat
Testing	sup.reg
Testing	svchost.exe
Testing	users.ini

Plus! It will give the nickname "mad" probably the owner/writer of the malware.

2. Without running the file, is it possible to identify what this malware can and will do?

Yes, we can see information on the strings output regarding IRC, "GETPASSWORD1", This could be a BOT with any type of key logging capabilities. Sending this file to on-line virus engines, <http://virusscan.jotti.org> and <http://www.virustotal.com> the result was:

```
Dropper/PSW.Zapchast.57
Backdoor.IRC.Zapchast
Backdoor.Cloner.ae
Win32/IRCFlood.Fizz!Dropper
Trojan.IRCBot-93
```

Nice, they have detected also the UPX format:

Packers detected: UPX

The most interesting thing was to see the results of the antivirus engines against the uncompressed file:

```
SecurityPrivacyRisk/Moo.A riskware
Trojan/Starter.A.7
IRC/Cloner.ae1 script-virus
Trojan.Zapchas.F
Trojan.Mirc.Fizz.3147.A
Backdoor.Irc.Lambot.G
Trojan.Starter.C
Backdoor.IRC.Cloner.AE
Backdoor.IRC.Zapchast
IRC/Cloner.N@troj
```

The results were much more detailed.

We need to consider this file to have any type of backdoor capability.

3. Now, using any methods available to you, which changes, if any, will this malware do in the system, among new files and registry entries...?

Sending the uncompressed file to <http://sandbox.norman.no> it returned to me this:

```
[ Process/window information ]
* Attempts to NULL C:\WINDOWS\system32\drivers\sup.bat NULL.
```

When executing the creatzu file those file appears on the system:

```
nicks.txt on c:\windows\system32\drivers
this is a list of irc nicknames
the file name can be obtained on the strings output also, nicks.txt
```

```
run.exe on c:\windows\system32\drivers
visual basic file, makes reference to rcd.exe
```

```
remote.ini on c:\windows\system32\drivers
configuration file for irc
```

```
radmin.txt on c:\windows\system32\drivers
```

script.ini on c:\windows\system32\drivers
script file to connect to irc and start scans

sub.bat on c:\windows\system32\drivers
bat file to make registration of the key sup.reg

Keys added to the registry. Located on the file sup.reg on
c:\windows\system32\drivers

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"svchost.exe"="C:\\WINNT\\system32\\drivers\\svchost.exe"
"system32"="C:\\WINDOWS\\system32\\drivers\\svchost.exe"
```

Since those keys are visible to normal shell is possible that this malware don't have rootkit technology

```
c:\reg query HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

The file svchost.exe listed on the key are located at
c:\windows\system32\drivers and has a mirc icon.
Executing this file without any parameter it will appears minimized on the taskbar but without any icon, using the mouse you can access the properties and realize this is the mirc binary

Browsing on this mirc binary we can find the following channels listed: #Creatu #Cretu and #Cretzu

Information from svchost.exe running:

```
Full name: juliana (from the file nicks.txt)
Email address: MAD
NickName: Of6iJv6aF (random generated using script.ini)
Alternative: Jz6tNc6iR
UserID: cacat
Quit Message: mad is my master !
Service Name: svchost
By default configuration this bot try to connect to undernet servers
Finger attempts will be logged and store on
c:\windows\sysste32\drivers\finger.txt
```

moo.dll

This file is used to collect information about the system, like processor type, and other resource information. This can be done on the IRC channel and is also referred on the scrypt.ini file.

Here is a sample of information can be collect on an IRC channel:

Now talking in #quiz5_malware

```
<super_> [2gfx][Matrox Graphics Millennium II PCI]
[2moo.dll error][Motherboard Monitor 5 is not loaded]
<super_> [2Network Interfaces][#1(NVIDIA nForce Networking Controller - Eacfilt
Miniport (100Mb/s) 18.67MB In, 1.34MB Out) #2(VMware Virtual Ethernet Adapter
```

```
for VMnet1 (100Mb/s) 0.03MB In, 0.03MB Out) #3(VMware Virtual Ethernet Adapter
for VMnet8 (100Mb/s) 0.03MB In, 0.03MB Out)]
<super_> □2os□[Windows XP Professional, Service Pack 2 (5.1 - 2600)] □2uptime□[-
3h 7m 46s] □2cpu□[1-AMD , 2209MHz (0% Load)] □2mem□[Usage: 640/1023MB
(62.56%) [|||||----]]
□2moo.dll error□[Could not get RAS info on this OS]
<super_> □2screen□[1024x768 32bit 60Hz]
<super_> □2uptime□[Windows XP Professional, Service Pack 2 (5.1 - 2600) uptime -
3h 8m 9s]
```

```
The file svchost.exe is the original mirc 6.03 binary:
\b766003f431cad186bd115f5761592d1 svchost.exe
\b766003f431cad186bd115f5761592d1 *c:\Program Files\mIRC\mirc.exe
```

4. Now, what is the purpose of this malware?

It's a Bot, with a backdoor and scripts to make scans.

5. When will this malware be triggered/start?

When the system will be restarted, since we have the "patch Thursday" we now at least the system can/will be reboot once per month.

6. Can you explain the netstat output?

```
TCP 192.168.0.53:1036 195.47.220.2:6667 ESTABLISHED
This shows the bot connected to one of the undernet servers
```

```
TCP 192.168.0.53:1088 xxx.80.0.50:4899 SYN_SENT
TCP 192.168.0.53:1089 xxx.80.0.51:4899 SYN_SENT
TCP 192.168.0.53:1090 xxx.80.0.52:4899 SYN_SENT
TCP 192.168.0.53:1091 xxx.80.0.53:4899 SYN_SENT
TCP 192.168.0.53:1092 xxx.80.0.54:4899 SYN_SENT
TCP 192.168.0.53:1093 xxx.80.0.55:4899 SYN_SENT
TCP 192.168.0.53:1094 xxx.80.0.56:4899 SYN_SENT
TCP 192.168.0.53:1095 xxx.80.0.57:4899 SYN_SENT
TCP 192.168.0.53:1096 xxx.80.0.58:4899 SYN_SENT
TCP 192.168.0.53:1097 xxx.80.0.59:4899 SYN_SENT
```

Those lines show the infect system, aka zombie, scanning the xxx.80.0.* network against the port 4899. This is the port of the backdoor of Radmin.

7. What about the TaskManager screenshot? What useful information can you get?

The process running under username "malware" they are the same founded on the infected system, svchost.exe 4,492K. We can also see the tools running on the system to make the analysis, process explorer from sysinternals (procexp.exe) and also tcpview to see information about connections.

8. About the creztu file, please explain each of the files that it contains :)

The creztu file was first packed with rar and then with UPX. The first creztu file has several files, all related to the bot and irc.

All files were placed on C:\WINDOWS\system32\drivers\

aliases.ini -> mirc aliases configuration file
control.ini -> mirc control configuration file
mirc.ico -> mirc icon
mirc.ini -> mirc main configuration file
moo.dll -> module to collect information about the system
nicks.txt -> nicknames to be used
perform.ini -> mirc file
popups.ini -> mirc file
radmin.txt ->
remote.ini -> information on the remote backdoor on port 31337, password muie
run.exe -> Trojan starter.a
script.ini -> script file, make the nicknames, scan and collect info
servers.ini -> list of IRC server of undernet
sup.bat -> script to registry the sup.reg keys
sup.reg -> keys with the process name to be initialized on the system
svchost.exe -> mirc binary
users.ini -> list of usernames (@Cr3tu @CretuDeLaCta @CretuJmen)

Bonus Questions:

9. Which other information about the channel can you provide?

We have the channels names:

#Creatu #Cretu and #Cretzu

10. How would you call this Malware and describe what this category of malware do.

This is a bot, a program to control an infected system remotely using IRC servers and channels as communication methods. Systems infected with this kind of malicious program are normally called zombies by the mass media. The infect systems can be used to make scans, ping systems (dos) and can be controlled remotely.

11. Please explain the logs above.

```
PING :Lelystad.NL.EU.UnderNet.Org :`5mui`lei!shoby17---@68-112-234-  
6.dhcp.oxfr.ma.charter.com QUIT :Read error: Connection reset by peer  
:angelique!~cacat@172.206.142.94 JOIN #Creatu :Jo_m46!~cacat@ip68-9-84-  
60.ri.ri.cox.net JOIN #Creatu :Nht_Boy!~shashank@107.67.63.81.cust.bluewin.ch  
QUIT :Read error: Connection reset by peer :angelique!~cacat@172.206.142.94 NICK  
:PatruOchi :mari37!phillip@81-235-146-201-no33.tbcn.telia.com JOIN #Creatu
```

```
:|paritul|!mitul_@cpe-67-11-255-16.satx.res.rr.com QUIT :Ping timeout  
:SHOGHUN!cacat@ACCE8E5E.ipt.aol.com JOIN #Creat
```

Those are logs of users connecting to undernet IRC servers. We can see the usernames used, ips used and channel #Creat