SonicALERT: CVE 2014-0322 Malware - Sakurel (Feb 21, 2014)

Back to SonicALERT

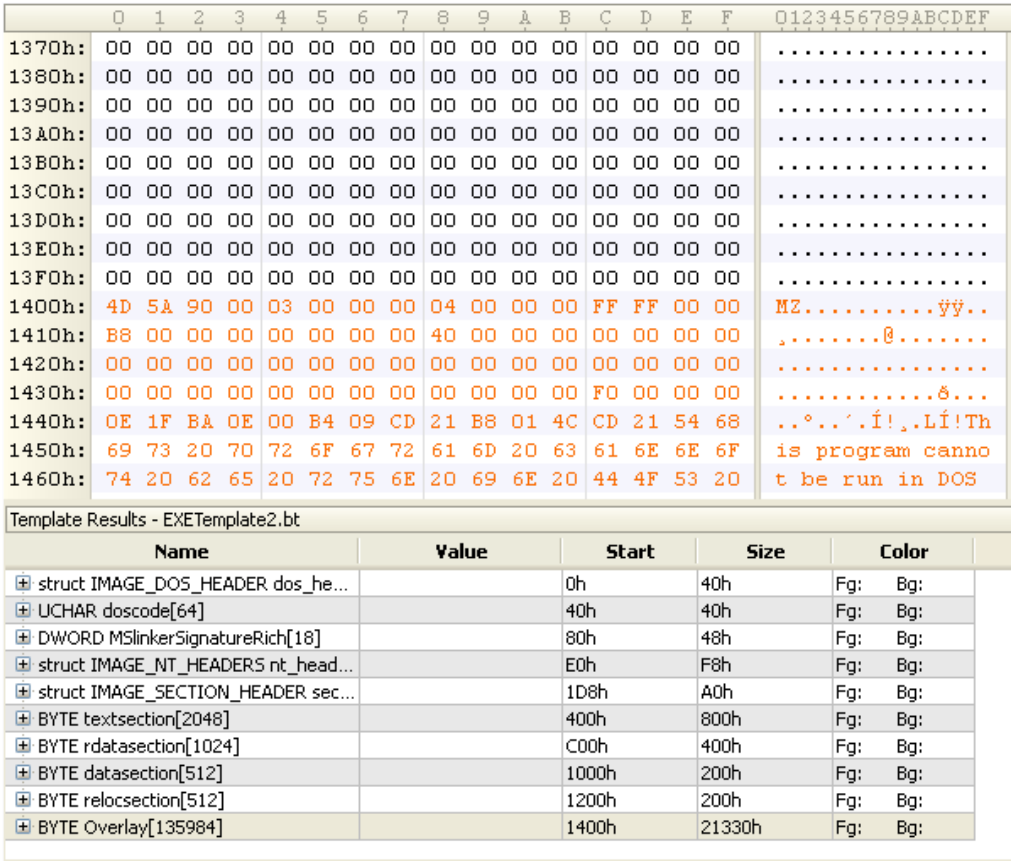
CVE 2014-0322 Malware - Sakurel (Feb 21, 2014)

Description

The Dell SonicWall Threats Research Team has spotted the latest malware being served in the recent CVE 2014-0322 attack. We have already shared our analysis on the exploit behavior so we will now discuss the behavior of the malware payload, Sakurel.

This malware has many features and contains multiple levels of embedded files. The malware ultimately seeks to steal information and provide a backdoor to the infected system, and uses different modules to accomplish its tasks.

The file that gets dropped after exploitation, 'stream.exe', has fairly basic dropper behavior. The file contains an XOR-encoded binary which gets decoded and executed in memory.



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
1370h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
1380h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
1390h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
13A0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
13B0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
13C0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
13D0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
13E0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
13F0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
1400h:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
1410h:	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.......
1420h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
1430h:	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00	............ð...
1440h:	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..´.Í!¸.LÍ!Th
1450h:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
1460h:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS

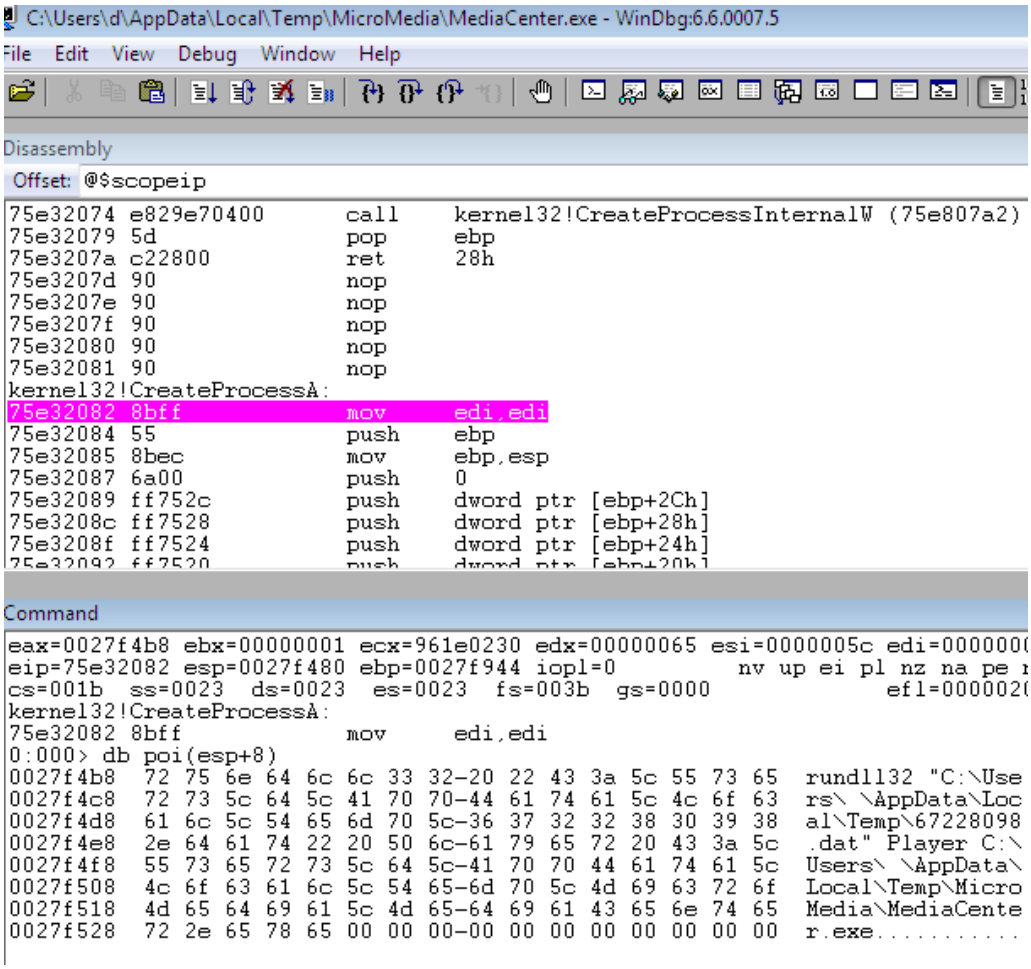
Template Results - EXETemplate2.bt

Name	Value	Start	Size	Color
struct IMAGE_DOS_HEADER dos_he...		0h	40h	Fg: Bg:
UCHAR doscode[64]		40h	40h	Fg: Bg:
DWORD MSlinkerSignatureRich[18]		80h	48h	Fg: Bg:
struct IMAGE_NT_HEADERS nt_head...		E0h	F8h	Fg: Bg:
struct IMAGE_SECTION_HEADER sec...		1D8h	A0h	Fg: Bg:
BYTE textsection[2048]		400h	800h	Fg: Bg:
BYTE rdatasection[1024]		C00h	400h	Fg: Bg:
BYTE datasection[512]		1000h	200h	Fg: Bg:
BYTE relocsection[512]		1200h	200h	Fg: Bg:
BYTE Overlay[135984]		1400h	21330h	Fg: Bg:

The decoded malware contains additional embedded modules, including one that provides for privilege escalation if the current user is not an administrator.

```
call    ds:IsUserAnAdmin
test    eax, eax
jz      short loc_100011B1
xor     eax, eax
inc     eax
jmp     loc_10001373
```

After checking if the current process is running as an administrator, the escalation module is extracted and dropped with a .dat extension, then executed via 'rundll32'.



This DLL contains a well-known technique for escalating user privileges via the 'sysprep' tool. This uses a UAC bypass which affects 32-bit versions Windows 7 and Windows 8.

```
.text:10001139                push    offset aSysprep ; "\\sysprep\\"
.text:1000113E                push    esi             ; lpString1
.text:1000113F                call    ds:lstrcatW
.text:10001145                push    esi             ; lpString2
.text:10001146                mov     edi, offset word_10003438
.text:1000114B                push    edi             ; lpString1
.text:1000114C                call    ds:lstrcpyW
.text:10001152                push    offset aSysprep_exe ; "sysprep.exe "

.text:1000120F                push    eax             ; ppv
.text:10001210                push    offset riid     ; riid
.text:10001215                push    edx             ; pBindOptions
.text:10001216                push    offset pszName  ; "Elevation:Administrator!new:{3ad05575-8"...
.text:1000121B                mov     dword_10003024, edx
.text:10001221                mov     dword ptr [edx], 24h
.text:10001227                mov     dword ptr [edx+14h], 4
.text:1000122E                call    ds:CoGetObject
```

Once the malware has administrator privileges, it extracts an OCX file from its resources and moves a copy of its original dropped incarnation into "MicroMedia" underneath "%APPDATA%\Local\Temp" and creates the following registry key to execute when the system boots up:

> **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\MicroMedia:**
> ***%APPDATA%\Local\Temp\MicroMedia\MediaCenter.exe***

Once the malware has acquired sufficient access and achieved peristence on the machine, the Windows 'hosts' file is modified to redirect a number of domains to IP addresses controlled by the attackers. These strings from the binary show the domains the attackers are redirecting:

```
aDriversEtcHost db '\drivers\etc\hosts',0 ; DATA XREF: sub_100026A7+38↑o
                align 10h
aCsg_secure_sne db 'csg.secure.snecma.fr          217.108.170.94',0Dh,0Ah
                                                  ; DATA XREF: sub_100026A7+66↑o
                db 'ctx.secure.snecma.fr          217.108.170.81',0Dh,0Ah
                db 'fdm.secure.snecma.fr          217.108.170.23',0Dh,0Ah
                db 'qa.fdm.secure.snecma.fr       217.108.170.27',0Dh,0Ah
                db 'qa.indigo.secure.snecma.fr    217.108.170.98',0Dh,0Ah
                db 'pi.secure.snecma.fr           217.108.170.96',0Dh,0Ah
                db 'qa.secure.snecma.fr           217.108.170.88',0Dh,0Ah
                db 'qasd.secure.snecma.fr         217.108.170.87',0Dh,0Ah
                db 'sd.secure.snecma.fr           217.108.170.199',0Dh,0Ah
                db 'int.tcua.secure.snecma.fr     217.108.170.18',0Dh,0Ah
                db 'qa.tcua.secure.snecma.fr      217.108.170.13',0Dh,0Ah
                db 'secure.snecma.fr              217.108.170.196',0Dh,0Ah,0
```

The following strings, which include command and control domains and paths, are encoded in the binary with the XOR key 0x56:

```
50 F2 00 10 08 50 01 10 6F 61 2E 61 6D 65 74 65  Pò...P..oa.amete  00 00 00 00 66 23 00 00 00 00 00 00 6F 61 2E 61  ....f#......oa.a
6B 73 65 6E 2E 63 6F 6D 3A 38 30 00 00 00 00 00  ksen.com:80.....  6D 65 74 65 6B 73 65 6E 2E 63 6F 6D 3A 34 34 33  meteksen.com:443
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 2F 70 68 6F 74 6F  ........../photo  00 00 00 00 00 00 00 00 00 00 00 00 00 00 2F 70  ................/p
2F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  /...............  68 6F 74 6F 2F 00 00 00 00 00 00 00 00 00 00 00  hoto/...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 73 63 72 69  ............scri  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
70 74 2E 61 73 70 00 00 00 00 00 00 00 00 00 00  pt.asp..........  73 63 72 69 70 74 2E 61 73 70 00 00 00 00 00 00  script.asp......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 2F 73  ................/s  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
63 72 69 70 74 2E 61 73 70 00 00 00 00 00 00 00  cript.asp.......  00 00 2F 73 63 72 69 70 74 2E 61 73 70 00 00 00  ../script.asp...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
69 6D 61 67 65 69 64 00 00 00 00 00 00 00 00 00  imageid.........  00 00 00 00 69 6D 61 67 65 69 64 00 00 00 00 00  ....imageid.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 4D 65 64 69 61 43 65 6E 74 65 72 2E 65 78  ..MediaCenter.ex  00 00 00 00 00 00 4D 65 64 69 61 43 65 6E 74 65  ......MediaCente
65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  e...............  72 2E 65 78 65 00 00 00 00 00 00 00 00 00 00 00  r.exe...........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 4D 69 63 72 6F 4D 65 64 69 61 00 00  ....MicroMedia..  00 00 00 00 00 00 00 00 4D 69 63 72 6F 4D 65 64  ........MicroMed
```

Overall the main motive of this malware is to steal user credentials from the targeted domains. The malware also provides full backdoor access to the system via the command and control structure. We will continue to monitor this threat and provide updates on its capabilities.

Dell SonicWALL Gateway AntiVirus provides protection against this threat via the following signature:

> **GAV: Sakurel.EX (Trojan)**

Back to top

Back to SonicALERT