

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

Archived: 2026-04-02 11:05:16 UTC

Dell SonicWALL Security Center

[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	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
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	FO	00	00	00	.....&...																
1440h:	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..'!¡,LI!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'.

```

C:\Users\d\AppData\Local\Temp\MicroMedia\MediaCenter.exe - WinDbg:6.6.0007.5
File Edit View Debug Window Help
Disassembly
Offset: @$scopeip
75e32074 e829e70400 call kernel32!CreateProcessInternalW (75e807a2)
75e32079 5d pop ebp
75e3207a c22800 ret 28h
75e3207d 90 nop
75e3207e 90 nop
75e3207f 90 nop
75e32080 90 nop
75e32081 90 nop
kernel32!CreateProcessA:
75e32082 8bff mov edi,edi
75e32084 55 push ebp
75e32085 8bec mov ebp,esp
75e32087 6a00 push 0
75e32089 ff752c push dword ptr [ebp+2Ch]
75e3208c ff7528 push dword ptr [ebp+28h]
75e3208f ff7524 push dword ptr [ebp+24h]
75e32092 ff7520 push dword ptr [ebp+20h]
Command
eax=0027f4b8 ebx=00000001 ecx=961e0230 edx=00000065 esi=0000005c edi=00000000
eip=75e32082 esp=0027f480 ebp=0027f944 iopl=0         nv up ei pl nz na pe r
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000020
kernel32!CreateProcessA:
75e32082 8bff mov edi,edi
0:000> db poi(esp+8)
0027f4b8 72 75 6e 64 6c 6c 33 32-20 22 43 3a 5c 55 73 65  rundll32 "C:\Use
0027f4c8 72 73 5c 64 5c 41 70 70-44 61 74 61 5c 4c 6f 63  rs\ \AppData\Loc
0027f4d8 61 6c 5c 54 65 6d 70 5c-36 37 32 32 38 30 39 38  al\Temp\67228098
0027f4e8 2e 64 61 74 22 20 50 6c-61 79 65 72 20 43 3a 5c  .dat" Player C:\
0027f4f8 55 73 65 72 73 5c 64 5c-41 70 70 44 61 74 61 5c  Users\ \AppData\
0027f508 4c 6f 63 61 6c 5c 54 65-6d 70 5c 4d 69 63 72 6f  Local\Temp\Micro
0027f518 4d 65 64 69 61 5c 4d 65-64 69 61 43 65 6e 74 65  Media\MediaCente
0027f528 72 2e 65 78 65 00 00 00-00 00 00 00 00 00 00 00  r.exe.....

```

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:10001148          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:10001218          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 persistence 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	Pö...P...oa.amete	00 00 00 00 66 23 00 00 00 00 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	...../photo	(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 00 00 00 00 00 00	...../p
2F 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...../photo	68 6F 74 6F 2F 00 00 00 00 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	.....scri	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	.....scri	00 00 00 00 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	pt.asp.....	73 63 72 69 70 74 2E 61 73 70 00 00 00 00 00 00 00 00 00 00	script.asp.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	...../s	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	cript.asp.....	00 00 2F 73 63 72 69 70 74 2E 61 73 70 00 00 00 00 00 00 00 00	.../script.asp...
00 00 00 00 00 00 00 00 00 00 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	.....imageid.....
69 6D 61 67 65 69 64 00 00 00 00 00 00 00 00	.....MediaCenter.ex	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....MediaCente
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....MicroMedia..	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....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

Source: <https://web.archive.org/web/20151001235506/https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=654>