Sakula Malware Family

secureworks.com/research/sakula-malware-family

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Thursday, July 30, 2015 *By: Dell SecureWorks Counter Threat Unit™ Threat Intelligence*

Summary

Dell SecureWorks Counter Threat Unit™ (CTU™) researchers analyzed multiple versions of a remote access trojan (RAT) named Sakula (also known as Sakurel and VIPER). The RAT, which according to compile timestamps first surfaced in November 2012, has been used in targeted intrusions through 2015. Sakula enables an adversary to run interactive commands as well as to download and execute additional components.

Sakula uses HTTP GET and POST communication for command and control (C2). Network communication is obfuscated with single-byte XOR encoding. Sakula also leverages single-byte XOR encoding to obfuscate various strings and files embedded in the resource section, which are subsequently used for User Account Control (UAC) bypass on both 32 and 64-bit systems. Most samples maintain persistence through a registry Run key, although some samples configure themselves as a service.

Analysis

CTU researchers performed detailed analysis on 346 Sakula samples, including the installer and all dropped files used by the malware to run. The earliest compilation timestamp is November 21, 2012. As of this publication, the most recent sample observed by CTU researchers was compiled on January 1, 2015. Some installers compiled in 2013 are configured to drop samples compiled in 2014, suggesting that the initial installer has been successful and that the adversary has a build process that permits them to easily re-use components. Multiple samples include their debug information, which yielded properties like LANG_NAME and SUBLANG_NAME (whose values are 'LANG_CHINESE' and 'SUBLANG_CHINESE_SIMPLIFIED', respectively).

Delivery

CTU researchers observed a copy of Sakula being delivered in a strategic web compromise (SWC) that exploited CVE-2014-0322, which was a zero-day vulnerability in Internet Explorer at the time of compromise. A subset of Sakula variants are digitally signed, allowing them to bypass security controls and providing users with a false sense of security that the software is legitimate. Table 1 lists the publisher names, thumbprints, and serial numbers used by Sakula to digitally sign its installer component.

Publisher	Thumbprint	Serial number
Career Credit Co	3203BA1693B76FCB68D33BE0B9E8F312EE97A9B9	01 A5 D9 59 95 19 B1 BA FC FA D0 E8 0B 6D 67 35
DTOPTOOLZ Co.	6E752358D18B8B401A764ABE1AB9D6D5B42332C8	47 D5 D5 37 2B CB 15 62 B4 C9 F4 C2 BD F1 35 87
MICRO DIGITAL INC.	3E49A89005AA19A9294F919ACE81169A33789638	31 06 2E 48 3E 01 06 B1 8C 98 2F 00 53 18 5C 36
NexG	554C8DDCDD782FA3102D750D94551EDC9B8A608F	5E 3D 76 DC 7E 27 3E 2F 31 3F C0 77 58 47 A2 A2
SJ SYSTEM	918BF759D590CC2D2240938C1A4310B49DB2ACC0	20 D0 EE 42 FC 90 1E 6B 3A 8F EF E8 C1 E6 08 7A
U-Tech IT service	AF7D3EC0D442C555E8E7337C571C2A72B32217D4	3A C1 0E 68 F1 CE 51 9E 84 DD CD 28 B1 1F A5 42

Table 1. Signature properties of certificates used to sign Sakula malware.

Some installers masqueraded as the following applications and used social engineering to convince users that the applications were required to do business:

- Adobe Self Extractor
- CITRIX Access Gateway Secure Input
- Juniper SSL VPN ActiveX Plugin

- Microsoft Hotfix
- Security Exchange Mail Exchange ActiveX Control

Figures 1 through 5 show the status windows that the Sakula installers display to victims.

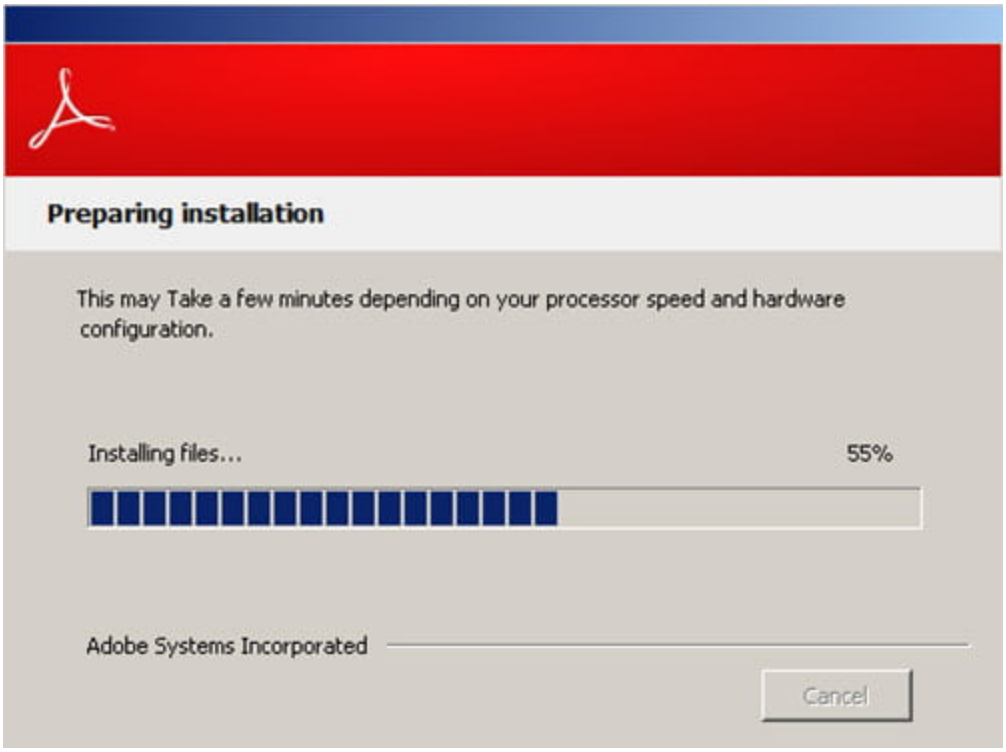

Figure 1. Screenshot of Sakula installer purporting to be installing Adobe software. (Source: Dell SecureWorks)

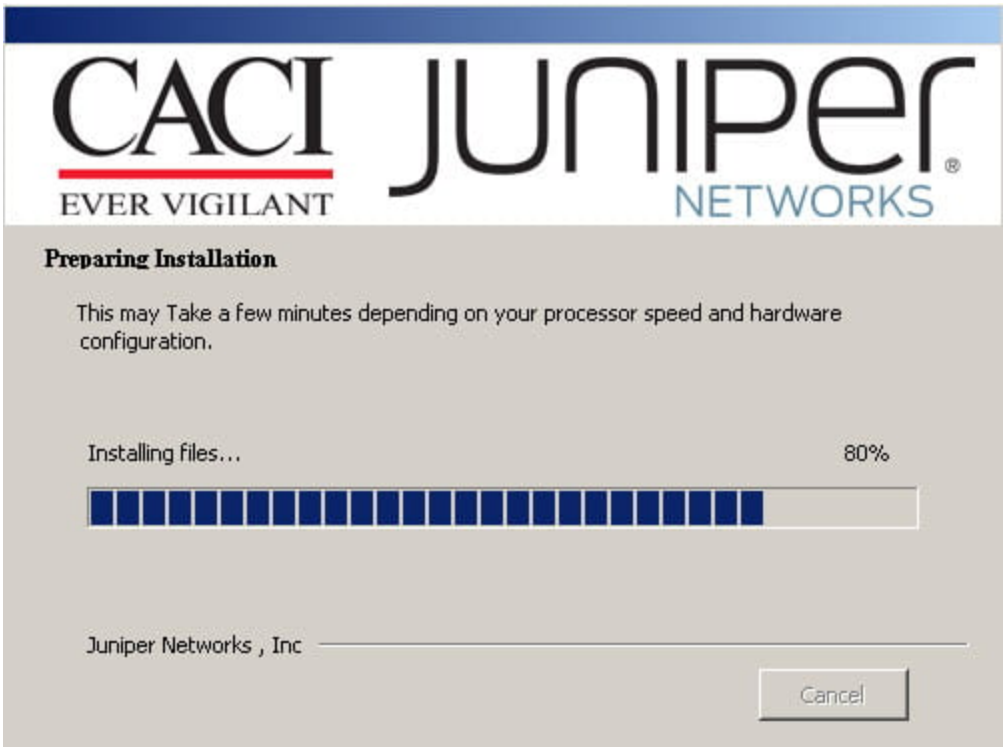

Figure 2. Screenshot of Sakula installer purporting to be installing Juniper software. (Source: Dell SecureWorks)

Figure 3. Screenshot of Sakula installer purporting to be installing Exchange software. (Source: Dell SecureWorks)

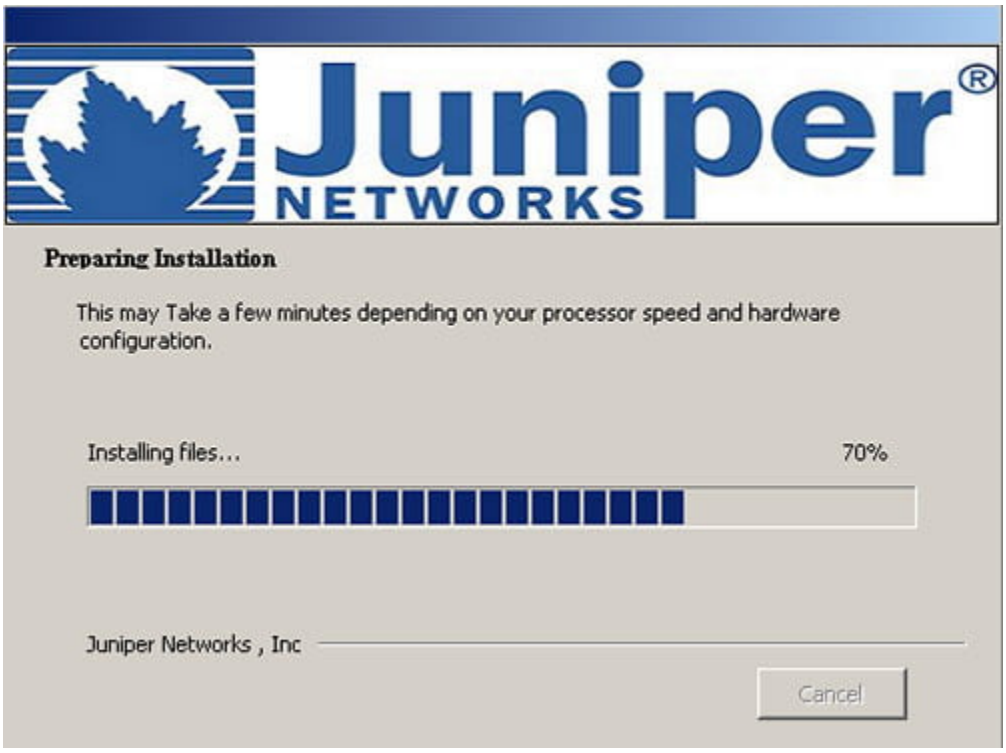

Figure 4. Screenshot of Sakula installer purporting to be installing Juniper software. (Source: Dell SecureWorks)

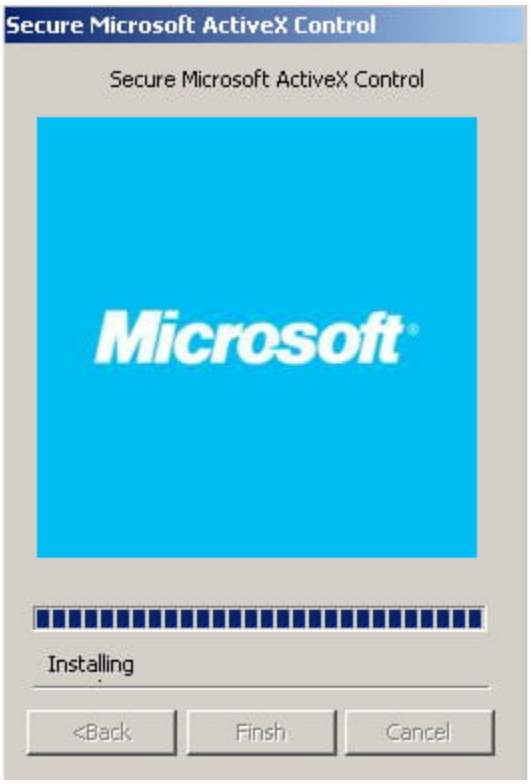

Figure 5. Screenshot of Sakula installer purporting to be installing a Microsoft ActiveX Control. (Source: Dell SecureWorks)

Installation

In most of the samples collected by the CTU research team, Sakula maintains persistence by setting the registry Run key (SOFTWARE\Microsoft\Windows\CurrentVersion\Run\) in either the HKLM or HKCU hive. The hive decision is based on the installer's ability to write to the %TEMP% directory. Through 2013, registry persistence was set using standard Windows APIs. In the samples compiled in 2014, the adversary switched to adding the Run key by invoking cmd.exe:

```
cmd.exe /c reg add %s\Software\Microsoft\Windows\CurrentVersion\Run /v "%s" /t REG_SZ
/d "%s"
```

The registry value and filename vary by sample. CTU researchers extracted the following parameters:

Values:

- MicroMedia
- JuniperACX
- MicroSoftMedia
- CCPUpdate
- SenseSvc

Filenames:

- MediaCenter.exe
- AdobeUpdate.exe
- JuniperSafeACX.exe
- MicroPlayerUpdate.exe
- CitrixReciever.exe
- SensrSvc.exe
- SensrSvc2013.exe
- MicroSoftSecurityLogin.ocx
- Utmm.ocx
- Sweep.exe
- pdfforie.exe
- shiape.exe

In the cases where Sakula does not use a registry key for persistence, it attempts to set itself up as a service (see Table 2). It invokes itself by calling WinExec with the "net start %s" argument (without quotes), where "%s" is the service name.

Service name	Service description	Filename and location

AppleService	Apple Application Service.	C:\WINDOWS\system32\AppleService.exe
Office Auto Update	Microsoft Office Auto Update.	C:\WINDOWS\system32\Sweep.exe

Table 2. Properties used by Sakula when setting itself up as a service.

Other than the service setup, the resident file location is fairly consistent across all samples. Most Sakula samples install their components within a directory under %TEMP%. The actual value of the environment variable is identified by an API call to ExpandEnvironmentStringsA. Three of the analyzed samples placed files in %APPDATA%, while the remaining Sakula samples placed files in a directory under %ALLUSERSPROFILE%. A small number of samples did not use an additional subdirectory. CTU researchers discovered Sakula files being installed under the following directory paths:

- %TEMP%\MicroMedia\
- %TEMP%\JuniperACX\
- %TEMP%\MicroMedia\
- %TEMP%\MicroSoftMedia\
- %ALLUSERSPROFILE%\MicroMediaCCP\
- %TEMP%\
- %ALLUSERSPROFILE%\
- %APPDATA%\

The 2014 samples maintain persistence with the same SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ registry key, but Sakula leverages DLL side-loading, which involves running a legitimate, typically digitally signed, program that loads a malicious DLL. The legitimate application is a digitally signed sample of Kaspersky Anti-Virus (AV) 6.0 for Windows Workstations. When the Kaspersky application is run, it loads a file named msi.dll, which is located within the same directory. The msi.dll file is configured to read and XOR-decode setup.msi, also located in the same directory, and run it in memory. The XOR-decode process, which skips zeroes, uses the single-byte key 0x88.

The 2015 sample differs from the 2014 samples in the files used and how the persistence mechanism is executed. Instead of the Kaspersky application, the 2015 sample uses a legitimately signed file from McAfee's Outlook Scan About Box application. Sakula names this file either MicroWhoknow.dll or Emabout.dll. There are two additional files within the same directory. The first, shutil.dll, is loaded by MicroWhoknow.dll or Emabout.dll and is configured to read and XOR-decrypt Thumbs.db using the same XOR key value as setup.msi. The other is the registry key used for persistence, which uses VBScript to call cmd.exe to run a DLL via the rundll32 application, passing the Plugupdate export within the MicroWhoKnow.dll as its entry point:

```
HKU\Software\Microsoft\Windows\CurrentVersion\Run\MicroWhoknow: "mshta
vbscript:CreateObject("WScript.Shell").Run("cmd /c cd
C:\Users\user\AppData\Local\Temp\MicroWhoknow && rundll32 MicroWhoknow.dll
Plugupdate",0)(window.close)"
```

Multiple samples contain UAC bypass code for both 32 and 64-bit systems. The UAC bypass code is stored as 'DAT' in the file's resource section. The two DLLs are stored in separate items, identified as 101 and 102. The files are single-byte XOR-encoded with the value 0x24. The decode process skips hex bytes identical to the XOR key and zeroes. Based on whether the compromised system is 32-bit or 64-bit, the appropriate file is written and run using cmd.exe calling rundll32 on the DLL with the PlayWin32 or PlayWin64 export.

Persistence for the UAC bypass DLL file is maintained via a SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ registry key in the HKLM or HKCU hive, with the value "CCPUpdate". Other Sakula variants temporarily write the files to disk and execute each time the main Sakula application is called. In these cases, the temporary file is written to the %TEMP% directory, and the filename is a combination of numbers generated from a call to GetTickCount and the '.dat' extension (e.g., 2225260.dat). In some instances, the filename is prefaced with the word "Center" (e.g., Center509671.dat).

In a small group of Sakula samples from 2013, the install process also modified the hosts file to point some of the victim's subdomains to various IP addresses within the victim's own organization. The malware also registered a file as a command component within the registry.

In the Sakula samples where the install process performed cleanup, the malware invoked cmd.exe. This process was instantiated by first performing a ping request to localhost to ensure the install process completed before the temporary file was deleted:

```
C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 & del /q %TEMP%\Center73946.dat
```

On a subset of samples compiled in 2014, Sakula invoked the default web browser, which loaded a hard-coded URL. This action occurred after the seemingly legitimate application (discussed in the Delivery section) finished installing. Of the following URLs hard-coded within the malware, only the first three appeared to be under the adversary's control:

- http:// www . qzbwcq . com/cookie.html
- http:// sharepoint-vaeit . com/login.php?ref
- http:// extcitrix . we11point . com/vpn/index.php?ref=1
- https:// portal . caci . com/
- https:// webmail . mfa . gov . mn/
- http:// cabinet . gov . mn/mfa-gov/Success.html
- http:// www . bisononthevinayerd . org/BisonOntheVineyard.pdf

Capabilities

Sakula obfuscates many of its strings using single-byte XOR obfuscation. Samples with a 2012 compile timestamp use a key value of either 0x88 or 0x56. Samples compiled in 2013 and 2014 use a key value of 0x56, while the lone 2015 sample uses 0x57.

Core functionality across all Sakula samples is fairly consistent. While there are some minor differences among the samples, Sakula typically implements eight commands (see Table 3).

Case	Description
1	Invoke a remote shell via named pipe with optional command
2	Download and execute (randomly named file in %TEMP%)
3	Upload a file by path
4	Call WinExec on file
5	Update C2 OR C2 beacon interval
6	Uninstall and exit
7	Get information about self (PID/filename)
8	Invoke a remote shell OR sleep

Table 3. Command functionality available in Sakula samples analyzed by CTU researchers.

The "OR" in Table 3 indicates that the feature for that case varied by sample. For Case 2, the randomly named file is generated each time the command is used. It is sourced from a call to GetTickCount and is appended with ".exe". Case 8 was observed in samples compiled in mid-2013, with the Sleep command introduced in the only 2015 sample identified as of this publication.

Command and control

Sakula uses HTTP GET and POST for command and control, with most samples configured with only one C2 server. The network communications are encoded with the single-byte XOR keys listed in Table 4.

XOR key value	Observed sample year (based on compile time)
0x59	2012 and 2013
0x56	2013 and 2014

0x66	2014
0x5C	2014
0x7C	2015

Table 4. Single-byte XOR keys used to decode network traffic.

The URI patterns used to communicate with the C2 server are fairly consistent across all samples regardless of compile time. Table 5 lists a breakdown of format by HTTP method in the analyzed Sakula samples.

HTTP method	URI request format
POST	/check.asp?imageid=%s&type=%d
POST	/newimage.asp?imageid=%s&type=%d&resid=%d
POST	/news/view.asp?cookie=%s&type=%d&vid=%d
POST	/script.asp?imageid=%s&type=%d&resid=%d&nmsg=up
POST	/update.asp?cstring=%s&tom=%d&id=%d
POST	/view.asp?cookie=%s&type=%d&vid=%d
GET	/news/photo/%s.jpg?vid=%d
GET	/photo/%s.jpg
GET	/photo/%s.jpg?id=%d
GET	/photo/%s.jpg?resid=%d
GET	/script.asp?resid=%d&nmsg=del&photoid=%s
GET	/view.asp?cstring=%s&tom=0&id=%d
GET	/viewphoto.asp?photoid=%s
GET	/viewphoto.asp?resid=%d&photoid=%s
GET	/x0x/%s.jpg?id=%d

Table 5. Sakula URI formats by HTTP method. URIs using %s insert a string of characters, and %d insert digits.

Sakula uses hard-coded User-Agents in its C2 communications but did not mimic standard browser User-Agents until 2014:

- iexplorer
- Mozilla/4.0+(compatible;+MSIE+8.0;+Windows+NT+5.1;+SV1)
- Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)

Conclusion

The Sakula RAT has been in use since 2012 with very few changes to the code base, which indicates that it is effective in targeted intrusions. Simplistic in nature, the small command set for Sakula allows its operator to actively control a compromised system, download and execute additional components, and hide in plain sight with single-byte XOR-encoded HTTP GET and POST C2 communications.

Threat indicators

The threat indicators in Table 6 can be used to detect activity related to Sakula. The IP addresses and domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
104.128.233.4	IP address	Sakula C2 server
115.47.35.117	IP address	Sakula C2 server
180.210.206.246	IP address	Sakula C2 server
23.27.112.143	IP address	Sakula C2 server
secure.devpia.com	Domain name	Sakula C2 server
login.qzbwcq.com	Domain name	Sakula C2 server
oa.ameteksen.com	Domain name	Sakula C2 server
sinmoung.com	Domain name	Sakula C2 server

extcitrix.we11point.com	Domain name	Sakula decoy page
sharepoint-vaeit.com	Domain name	Sakula decoy page
citrix.vipreclod.com	Domain name	Sakula C2 server
update.microsoft.co.kr	Domain name	Sakula C2 server
web.vipreclod.com	Domain name	Sakula C2 server
www.huchin.com	Domain name	Sakula C2 server
www.northpoleroute.com	Domain name	Sakula C2 server
www.polarroute.com	Domain name	Sakula C2 server
www.qzbwcq.com	Domain name	Sakula decoy page
www.savmpet.com	Domain name	Sakula C2 server
www.we11point.com	Domain name	Sakula C2 server
iexplorer	User-Agent	Hard-coded Sakula User-Agent
Mozilla/4.0+(compatible;+MSIE+8.0; +Windows+NT+5.1;+SV1)	User-Agent	Hard-coded Sakula User-Agent
/check.asp?imageid=%s&type=%d	URI	Sakula hard-coded POST request format

/newimage.asp?imageid=%s&type=%d&resid=%d	URI	Sakula hard-coded POST request format
/news/view.asp?cookie=%s&type=%d&vid=%d	URI	Sakula hard-coded POST request format
/script.asp?imageid=%s&type=%d&resid=%d&nmsg=up	URI	Sakula hard-coded POST request format
/update.asp?cstring=%s&tom=%d&id=%d	URI	Sakula hard-coded POST request format
/view.asp?cookie=%s&type=%d&vid=%d	URI	Sakula hard-coded POST request format
/news/photo/%s.jpg?vid=%d	URI	Sakula hard-coded GET request format
/photo/%s.jpg	URI	Sakula hard-coded GET request format
/photo/%s.jpg?id=%d	URI	Sakula hard-coded GET request format

/photo/%s.jpg?resid=%d	URI	Sakula hard-coded GET request format
/script.asp?resid=%d&nmsg=del&photoid=%s	URI	Sakula hard-coded GET request format
/viewphoto.asp?photoid=%s	URI	Sakula hard-coded GET request format
/view.asp?cstring=%s&tom=0&id=%d	URI	Sakula hard-coded GET request format
/viewphoto.asp?resid=%d&photoid=%s	URI	Sakula hard-coded GET request format
/x0x/%s.jpg?id=%d	URI	Sakula hard-coded GET request format
Career Credit Co	Publisher name	Used to digitally sign Sakula malware
DTOPTOOLZ Co.	Publisher name	Used to digitally sign Sakula malware

MICRO DIGITAL INC.	Publisher name	Used to digitally sign Sakula malware
NexG	Publisher name	Used to digitally sign Sakula malware
SJ SYSTEM	Publisher name	Used to digitally sign Sakula malware
U-Tech IT service	Publisher name	Used to digitally sign Sakula malware
HKU\Software\Microsoft\Windows\CurrentVersion\Run\MicroWhoknow: "mshta vbscript:CreateObject("WScript.Shell").Run("cmd /c cd C:\Users\user\AppData\Local\Temp\MicroWhoknow && rundll32 MicroWhoknow.dll Plugupdate",0)(window.close)"	Registry key	Used by Sakula to maintain persistence
%TEMP%\MicroMedia\	Path	Sakula malware installation path
%TEMP%\JuniperACX\	Path	Sakula malware installation path
%TEMP%\MicroMedia\	Path	Sakula malware installation path
%TEMP%\MicroSoftMedia\	Path	Sakula malware installation path

%ALLUSERSPROFILE%\MicroMediaCCP\	Path	Sakula malware installation path
031832adb059c8a30bf06e3036813a05	MD5 hash	Sakula malware
034b2d2c7b1b6812d242771fbc382183	MD5 hash	Sakula malware
04f17c37259533e301b01a8c64e476e6	MD5 hash	Sakula malware
065aa01311ca8f3e0016d8ae546d30a4	MD5 hash	Sakula malware
07af666d2117296a7814c86839ee2ae0	MD5 hash	Sakula malware
07b62497e41898c22e5d5351607aac8e	MD5 hash	Sakula installer
0a8a4cfa745b6350bea1b47f5754595e	MD5 hash	Sakula malware
0ae8ace203031f32e9b1ac5696c0c070	MD5 hash	Sakula malware
0b6a0ca44e47609910d978ffb1ee49c6	MD5 hash	Sakula malware
0c693b4ee77c1ebb646334ce28331d5c	MD5 hash	Sakula malware
0db52e612d904f4d4212beee4bd5c35c	MD5 hash	Sakula malware
0e5d1b941dcb597eb9b7dc1f0694c65f	MD5 hash	Sakula malware
0f218e73da96af2939e75ebea7c958dc	MD5 hash	Sakula malware
0ff96f4dbfe8aa9c49b489218d862cd7	MD5 hash	Sakula malware
1098e66986134d71d4a8dd07301640b1	MD5 hash	Sakula malware

11587f16f3129cad17222498eadc84f2	MD5 hash	XOR-encoded UAC bypass code for Sakula
124089995494be38d866de08c12f99ef	MD5 hash	Sakula malware
1240fbbabd76110a8fc29803e0c3ccfb	MD5 hash	Sakula malware
127cd711193603b4725094dac1bd26f6	MD5 hash	Sakula malware
1377e513f872a062c6377d1e240225a8	MD5 hash	Sakula malware
13e99782f29efa20a2753ac00d1c05a0	MD5 hash	Sakula malware
15ccb0918411b859bab268195957c731	MD5 hash	Sakula malware
1893cf1d00980926f87c294c786892d2	MD5 hash	Sakula malware
191696982f3f21a6ac31bf3549c94108	MD5 hash	Sakula malware
194f79e5f043efecb5707ebc4f9d0573	MD5 hash	Sakula malware
1a6c43b693bb49dad5fe1637b02da2c6	MD5 hash	Sakula malware
1ab782431ed9948bf68196e1aa27cbc9	MD5 hash	Sakula malware
1affacbe9e5889d2e1b7045a828c7252	MD5 hash	Sakula malware
1d016bb286980fd356cab21cdfcb49f4	MD5 hash	Sakula installer
1d80af301994f9b6bf3fa2389ff125da	MD5 hash	XOR-encoded UAC bypass code for Sakula

1de5db7cef81645f3f0e7aabdb7551a8	MD5 hash	Sakula malware
205c9b07c449a9c270aabe923123c0c1	MD5 hash	Sakula malware
230d4212692c867219aba739c57f0792	MD5 hash	Sakula malware
230d8a7a60a07df28a291b13ddf3351f	MD5 hash	Sakula installer
2567d2bbcce5c8e7dcabcd2c1db2a98a	MD5 hash	Sakula malware
259ea5f6f3f1209de99d6eb27a301cb7	MD5 hash	Sakula malware
2798fa07d5708f7be69ba525e5452d13	MD5 hash	Sakula malware
28771cb939b989e2ab898408ccaf5504	MD5 hash	Sakula malware
2d619b2c648d095fa2fb2e0864dbc7c9	MD5 hash	Sakula malware
2ffea14b33b78f2e2c92aead708a487a	MD5 hash	Sakula malware
34db8fb5635c7f0f76a07808b35c8e55	MD5 hash	Sakula malware
352411e5288b2c6ea5571a2838c8f7f3	MD5 hash	Sakula malware
360273db9ac67e1531257323324d9f62	MD5 hash	Sakula malware
3759833848a8cd424bf973d66e983e91	MD5 hash	Sakula malware
379d4a0f24bb56569d6139946b7ccf88	MD5 hash	Sakula malware
388a7ae6963fd4da3ec0a4371738f4e0	MD5 hash	Sakula malware
391c01bdbeb5975c85cee0099adb132c	MD5 hash	Sakula malware

3b70ab484857b6e96e62e239c937dea6	MD5 hash	Sakula malware
3cd598e8e2fd033134d8784251eff59e	MD5 hash	Sakula malware
3ce08f804c5986856a85e16a4e211334	MD5 hash	Sakula malware
3d2c2fdd4104978762b89804ba771e63	MD5 hash	Sakula installer
3e0016d728b979b7f8fd77a2738047eb	MD5 hash	Sakula malware
3f0ba1cd12bab7ba5875d1b02e45dfcf	MD5 hash	Sakula installer
3fc6405499c25964dfe5d37ee0613a59	MD5 hash	Sakula malware
41093a982526c6dc7dbcf4f63814d428	MD5 hash	Sakula malware
419ce8f53d5585abd144e9e76113639d	MD5 hash	Sakula malware
4297e98e6d7ea326dee3d13e53aa8d70	MD5 hash	Sakula malware
42d3e38db9f1d26f82ef47f0a0ec0499	MD5 hash	Sakula malware
4315274a5eda74cd81a5ec44980876e8	MD5 hash	Sakula malware
442f10bfc2a02831b6a733d6c01b0c59	MD5 hash	Sakula malware
45468c2450e6451cf63d2b9b2b70c632	MD5 hash	Sakula malware
49c5da72aafabcc0b6896fec637ed167	MD5 hash	Sakula installer
4a6f45ff62e9ab9fe48f1b91b31d110e	MD5 hash	Sakula malware
4a7b4635af040cba1851b2f57254ba5e	MD5 hash	Sakula installer

4c15781cb47d4a7604788e188fc722de	MD5 hash	Sakula malware
4dc526eb9d04f022df9fa2518854bbb4	MD5 hash	Sakula malware
4e239b731a0f1dbf26b503d5e2a81514	MD5 hash	Sakula malware
4ea3afbed7a0c7d0013f454060243fba	MD5 hash	Sakula installer
4f545dff49f81d08736a782751450f71	MD5 hash	Sakula installer
51ee4ef7f326e90d391ee9d1c5238b34	MD5 hash	Decoded UAC bypass DLL file for Sakula
5382efbecccf8227c7adc443e229542f	MD5 hash	Sakula malware
5482deee917c374bab43dd83a4a6c722	MD5 hash	Sakula malware
586c418bf947a0ef73afd2a7009c4439	MD5 hash	Sakula malware
5acc539355258122f8cdc7f5c13368e1	MD5 hash	Sakula installer
5b27234b7f28316303351ea8bcfaa740	MD5 hash	Sakula malware
5d04457e3d4026a82ac3ec9b1c0819ec	MD5 hash	Sakula malware
5d54c0756fbe33aae5dc8a4484a7aee5	MD5 hash	Decoded UAC bypass DLL file for Sakula
5dbdc2839e3f5c2dd35f3def42002663	MD5 hash	Sakula malware
5e1c170d96b0faea3a1281d182c29e02	MD5 hash	Sakula malware

606b9759de1aa61a76cf4afa4ccf8601	MD5 hash	Sakula malware
61fe6f4cb2c54511f0804b1417ab3bd2	MD5 hash	Sakula malware
63ae83244a8d7ca1eef4e834eb0eb07f	MD5 hash	Sakula malware
63c0978e2fa715a3cad6fb3068f70961	MD5 hash	Sakula malware
64201ec97467910e74f40140c4aaa5ce	MD5 hash	Sakula malware
67112866e800b9dce2892cf827444d60	MD5 hash	Sakula malware
67fceab90a142e1e286bca0922dbffd3	MD5 hash	Sakula malware
68e13422b9a5d280f4a19235d8bf7da5	MD5 hash	Sakula malware
69314300da7a4a0e95be545b804565dd	MD5 hash	Sakula installer
6a2ea24ed959ef96d270af5cdc2f70a7	MD5 hash	Sakula malware
6bd7fb8f4565866ff032f236f0a29ee2	MD5 hash	Sakula malware
6ccb6d1b964f115f8c7215c6ab67b1cc	MD5 hash	Sakula malware
740561c8d5d2c658d2134d5107802a9d	MD5 hash	Sakula installer
74eb66027ac6fa5a59632383e09915e2	MD5 hash	Sakula malware
7b2677c7215fab4e42f4507eb01c4326	MD5 hash	XOR-encoded Sakula malware
81d74b0e9560f2bf780f12893d885f41	MD5 hash	Sakula malware
848fcb062218ae3162d07665874429a7	MD5 hash	Sakula malware

8506064925a774a8d11d9fac374eb86a	MD5 hash	Sakula malware
8542cf0d32b7c711d92089a7d442333e	MD5 hash	Sakula malware
888876810fa9f85a82645bf5d16468e8	MD5 hash	Sakula installer
8a45ea989807636cc685b81effc60d96	MD5 hash	Sakula malware
8ee244ad6b6f2b814d34d26dae880f12	MD5 hash	Sakula malware
8f523f7fc73e52d54bb4e94dc44768b0	MD5 hash	Sakula malware
91569c57fc342161c479603f3b527c1d	MD5 hash	Sakula malware
928579b6fd1162c3831075a7a78e3f47	MD5 hash	Sakula malware
96fab28f1539f3909a255436bc269062	MD5 hash	Sakula malware
98721c78dfbf8a45d152a888c804427c	MD5 hash	Sakula installer
9a63f72911b385a0c17427444c968ed0	MD5 hash	Sakula installer
9e45ad7f3f3354ff99b979b9dfe54248	MD5 hash	Sakula malware
9f38fbcc039e0b42e56eb79315a39ee9	MD5 hash	Sakula malware
a00a19c85c42cb49ad48c0be349daec0	MD5 hash	Sakula malware
a00e275feb97b55776c186579d17a218	MD5 hash	Sakula malware
a034a674b439d9b3d3ad1718bc0c6bb0	MD5 hash	Sakula malware
a05fb3920fe3842623f55df712914916	MD5 hash	Sakula malware

a068bf4b31738a08ed06924c7bf37223	MD5 hash	Sakula malware
a104ab14c9a1d425a0e959f046c97f29	MD5 hash	Sakula malware
a2030658767635894abdb3742db5e279	MD5 hash	Sakula malware
a225ee8669c52540b5056fd848f1e267	MD5 hash	Sakula malware
a2bdb2aaf4d8eacbbb634476f553455b	MD5 hash	Sakula malware
a33c6daba951f7c9a30d69b5e1e58af9	MD5 hash	Sakula malware
a39729153ceaeaf9b3aded9a28d0e4dc	MD5 hash	Sakula malware
a53782f0790258d7ae1c9330b4106976	MD5 hash	Sakula malware
a548d3dedd85683930d9732ed0316ec0	MD5 hash	Sakula malware
a700db7a97eceea15d5f43d1376a6f09	MD5 hash	Sakula malware
a759b73716bdc406b9a20ebef394bc6d	MD5 hash	Sakula malware
a7e467e16834e80a5713e0d6bb73def5	MD5 hash	Sakula malware
a932a0d01962773e2a8f4a516c5d0515	MD5 hash	Sakula installer
ab557f2197647aa3fb7be3de8770a109	MD5 hash	Sakula malware
aca2756917024c859d1f13ca1cdcb843	MD5 hash	Sakula malware
ae6f33f6cdc25dc4bda24b2bccff79fe	MD5 hash	Sakula malware
aec367555524a71efcc60f45e476c678	MD5 hash	Sakula malware

b011a616da408875bd0d39cebf11dd1d	MD5 hash	Sakula malware
b297c84e2cdeacdbae86cbf707fc7540	MD5 hash	Sakula malware
b2d900e2803dd0bcd5e85b64e24c7910	MD5 hash	Sakula malware
b42417f49dd3aa2d31449fdf06769ca0	MD5 hash	Sakula malware
b4958424c5db8b0eca61ce836b81d192	MD5 hash	Sakula malware
b4e24a4edba2d2644877cfc933973228	MD5 hash	Sakula malware
b6d9a58bacb8a92e428f7d70532cb33e	MD5 hash	Sakula malware
b79be0503606ee3e2ce243e497265dbb	MD5 hash	Sakula malware
b7bd80dd344af7649b4fd6e9b7b5fd5c	MD5 hash	Sakula malware
b7e3f853e98ea9db74bf3429803f7a4b	MD5 hash	Sakula malware
b8006fde97a095b2c86f8b0a06b7d24f	MD5 hash	Sakula malware
b83fed01e49300d45afadc61a5e5cf50	MD5 hash	Sakula malware
bb4bb0d7a794f31129cdb55025ea847b	MD5 hash	Sakula malware
bc74a557e91597d8b37ed357c367643e	MD5 hash	Sakula malware
bc99d3f41dfca74f2b40ce4d4f959af0	MD5 hash	Sakula command component
bccaa2ea0cf2c8ef597c84726c5417d0	MD5 hash	Sakula malware
bddb68ea6c732613bc4a31503eac3297	MD5 hash	Sakula malware

beb174ca92c75c8ef4dc4ee24afeabeb	MD5 hash	Sakula malware
bf29d2c64db69170ae01ebb4eabe9bd3	MD5 hash	Sakula installer
c0e37ffac09a426c5a74167d0e714177	MD5 hash	Sakula malware
c1f09f902a24b5132be481d477b92e5e	MD5 hash	Sakula malware
c2b7bf8a30ac6672d9eb81582bd32a4a	MD5 hash	Sakula malware
c35300af4a2b23c1a7d6435c6d4cb987	MD5 hash	Sakula malware
c384e7f567abd9ea50f647715a28661a	MD5 hash	Sakula installer
c43d74b85001f622aad61e9da5744b52	MD5 hash	Sakula malware
c4f541ab592c8fca4d66235eb2b8eeb2	MD5 hash	Sakula malware
c50612ebe76bfd7bc61174c581fb2a95	MD5 hash	Sakula installer
c5e90ead14dc49449fa37a2869a45842	MD5 hash	Sakula malware
c71b09dfffd870af2c38a8135762e84d	MD5 hash	Sakula installer
c72fb5b8de6ee95ff509b161fe9828f3	MD5 hash	Sakula malware
c823946a7490b8fc5ee29be583f39d23	MD5 hash	Sakula malware
c83500ea6e0c9844ad2e21badb64bb23	MD5 hash	Sakula malware
c869c75ed1998294af3c676bdbd56851	MD5 hash	Sakula installer
c8fa5701a43cd817b30327e44dc70369	MD5 hash	Sakula malware

ca9e06c0679586d2ff3ff7e3416c8b87	MD5 hash	Sakula malware
cb56b1fc08451d1f56481a29bd1047e9	MD5 hash	Sakula malware
cc15a9109b41297f65a7349920f42c09	MD5 hash	Sakula malware
ce09e671c124f1111fe5f2bde1267a63	MD5 hash	Sakula malware
cec76eec323613641dce1a261ca9a850	MD5 hash	Sakula malware
d00b3169f45e74bb22a1cd684341b14a	MD5 hash	Sakula malware
d690ba5dbb873c469cfdaf44fe2bd67f	MD5 hash	Sakula malware
d76be14a5e3a6ec45150ad2582f5c1a8	MD5 hash	Sakula installer
d86a4148bd34d78b808fdee7f936f1af	MD5 hash	Sakula malware
d87ce47e24ee426d8ac271873b041d50	MD5 hash	Sakula malware
d8b496c4837b80952c52e1375c31648c	MD5 hash	Sakula malware
dba4e180ed355a4ad63ceaf57447b2b7	MD5 hash	Sakula installer
dda9f3b2d5e70e70be1be7e4195b7016	MD5 hash	Sakula malware
df689186b50384026382d5179841abec	MD5 hash	Sakula malware
e2c32ed6b9cd40cb87569b769db669b7	MD5 hash	Sakula malware
e595292b1cdaea69ef365097a36195ad	MD5 hash	Sakula malware
e604176c2638fdf015d6a346803ed6f3	MD5 hash	Sakula malware

e66164b4967cf7b3cdb3c1c510abe957	MD5 hash	Sakula malware
e7113c872386edd441e7030d185238ca	MD5 hash	Sakula malware
e9115f553ac156542dcd38042f45ec68	MD5 hash	Sakula malware
e9181ef132fec9e560822551a093bb5c	MD5 hash	Sakula malware
f0082c886bc04fafe4a2615d75c2eaeb	MD5 hash	Sakula malware
f06b0ee07daa7f914dec27f98a6d8850	MD5 hash	Sakula malware
f2d59757a9795531796df91097d5fa2b	MD5 hash	Sakula malware
f47afcbc291cbc108112c110de77dbb1	MD5 hash	Sakula malware
f583a1fdb3c8be409e2118795ad916ba	MD5 hash	Sakula malware
f60f94d257ad5d781595b6c909844422	MD5 hash	Sakula malware
fbb2db8a78645f0a2e0f34316f119144	MD5 hash	Sakula malware
fbd85dad36fe13d46eaca7d7f2d50b0b	MD5 hash	Sakula malware
fc52814e8eb48aca6b87fa43656cbf42	MD5 hash	Sakula malware
fe74dc43af839146f64ec7bea752c4f0	MD5 hash	Sakula malware
fedf54586ebd00684e20712ad7eb9189	MD5 hash	Sakula malware
019a5f531f324d5528ccc09faa617f42	MD5 hash	Sakula malware
01c45a203526978a7d8d0457594fafbf	MD5 hash	Sakula malware

023ef99bc3c84b8df3f837454c0e1629	MD5 hash	Sakula malware
0334b1043c62d48525a29aeb95afcb09	MD5 hash	Sakula malware
04e8510007eea6bb009ab3b053f039db	MD5 hash	Sakula malware
05cd4bfeac3ad6144b5f5023277afa45	MD5 hash	Sakula malware
06ec79f67ad8ede9a3bd0810d88e3539	MD5 hash	Sakula malware
07b678ed364b23688b02a13727166a45	MD5 hash	Sakula malware
0a2c6265a65a25e9bef80f55cdd62229	MD5 hash	Sakula malware
0d0f5c0416247bb1dd6e0e2be1114b67	MD5 hash	Sakula malware
1077a39788e88dbf07c0b6ef3f143fd4	MD5 hash	Sakula malware
116dbfd8f5b6c5a5522d3b83a3821268	MD5 hash	Sakula malware
121320414d091508ac397044495d0d9c	MD5 hash	Sakula malware
1371181a6e6852f52374b4515aaa026a	MD5 hash	Sakula malware
1472fffe307ad13669420021f9a2c722	MD5 hash	Sakula malware
1856a6a28621f241698e4e4287cba7c9	MD5 hash	Sakula malware
1b826fa3fd70a529623ed1267944cee5	MD5 hash	Sakula malware
1bb0fb051cf5ba8772ad8a21616f1edb	MD5 hash	Sakula malware
1ff57a7aa2aa92698356f6c157290a28	MD5 hash	Sakula malware

21131bce815f2cb1bc0eb1fbf00b3c25	MD5 hash	Sakula malware
21ee6c85f431c2aa085b91ac0c86d27f	MD5 hash	Sakula malware
23169a0a2eee3d12fde0f3efd2cd55f1	MD5 hash	Sakula malware
231d0bfe48388082f5769f3deef5bcab	MD5 hash	Sakula malware
2414d83e97cb4c442b5594c6fbafe045	MD5 hash	Sakula malware
260349f5343244c439b211d9f9ff53cf	MD5 hash	Sakula malware
276f06196001dcfa97a035509f0cd0aa	MD5 hash	Sakula malware
29bd6cfc21250dfa348597a21a4a012b	MD5 hash	Sakula malware
2adc305f890f51bd97edbece913abc33	MD5 hash	Sakula malware
2ca3f59590a5aeab648f292bf19f4a5e	MD5 hash	Sakula malware
2f23af251b8535e24614c11d706197c3	MD5 hash	Sakula malware
2ff61b170821191c99d8b75bd01726f2	MD5 hash	Sakula malware
33be8e41a8c3a9203829615ae26a5b6e	MD5 hash	Sakula malware
34b7aa103deefbe906df59106683cc97	MD5 hash	Sakula malware
3859b0ea4596d8f47677497d09bcc894	MD5 hash	Sakula malware
3a1df1ec3ef499bb59f07845e7621155	MD5 hash	Sakula malware
3edbc66089be594233391d4f34ec1f94	MD5 hash	Sakula malware

3ff30fce107a01d3d17a9768abe6e086	MD5 hash	Sakula malware
416e598fb1ed9a7b6ce815a224015cb8	MD5 hash	Sakula malware
416e831d583665352fe16fe9232d36cf	MD5 hash	Sakula malware
421bff8f5dd218727283a2914424eccc	MD5 hash	Sakula malware
43e6a46d8789e1563e94ff17eff486d7	MD5 hash	Sakula malware
470e8dd406407b50483ce40de46660af	MD5 hash	Sakula malware
488c55d9a13c7fa8ee1aa0c15a43ab1e	MD5 hash	Sakula malware
492c59bddbcbe7cbd2f932655181fb08	MD5 hash	Sakula malware
4d8482da8730a886e4d21c5bfb7cd30e	MD5 hash	Sakula malware
4e239b731a0f1dbf26b503d5e2a81514	MD5 hash	Sakula malware
501db97a6b60512612909cfe959fbcd0	MD5 hash	Sakula malware
5496cff5e3bf46448c74fbe728763325	MD5 hash	Sakula malware
55daa4271973bb71ad4548225675e389	MD5 hash	Sakula malware
567a33e09af45123678042e620f31769	MD5 hash	Sakula malware
5a843bc0b9f4525b1ee512e1eba95641	MD5 hash	Sakula malware
5a894c18c5cc153f80699145edd1c206	MD5 hash	Sakula malware
5b76c68f9ca61bfd8a5bcbf2817a1437	MD5 hash	Sakula malware

5bb780344a601f4eff9ce0c55daf4361	MD5 hash	Sakula malware
5eea7686abeba0affa7efce4da31f277	MD5 hash	Sakula malware
5ff5916c9f7c593d1d589c97c571b45a	MD5 hash	Sakula malware
617eda7bcba4e3d5acc17663bbc964b3	MD5 hash	Sakula malware
62d4777dd8953743d26510f00b74f444	MD5 hash	Sakula malware
62e82c46647d2d2fe946791b61b72a4d	MD5 hash	Sakula malware
638304bf859e7be2f0fa39a655fdaffc	MD5 hash	Sakula malware
63f171705b28a05c84b67750b7e0ebf7	MD5 hash	Sakula malware
69374e5bcb38a82ef60c97ec0569ded3	MD5 hash	Sakula malware
6a273afa0f22d83f97d9fd2dc7dce367	MD5 hash	Sakula malware
6a7b2feed82d8d1746ac78df5a429bce	MD5 hash	Sakula malware
6bdf4e5b35b4cc5d3d519edc67086d7f	MD5 hash	Sakula malware
6c3523020a2ba0b7045060707d8833ea	MD5 hash	Sakula malware
6c4d61fedd83970cf48ef7fdd2a9871b	MD5 hash	Sakula malware
6d308fc42618812073481df1cd0452a7	MD5 hash	Sakula malware
71bbd661a61e0fee1f248f303af06f3f	MD5 hash	Sakula malware
7248d4b73d68cfc023d8d156c63f6b74	MD5 hash	Sakula malware

77a25486d425825986d2c6306a61f637	MD5 hash	Sakula malware
7d2c9936bff1e716b8758376cd09505d	MD5 hash	Sakula malware
7ee7a9446d7cf886223274d809d375d6	MD5 hash	Sakula malware
80eb86542ce7ad99acc53a9f85b01885	MD5 hash	Sakula malware
836a618341c6149e7c83e99755a7fd5f	MD5 hash	Sakula malware
895dc0a3adfafce2a74d733ff2a8754e	MD5 hash	Sakula malware
8b3de46ecb113cd1ee2d9ec46527358f	MD5 hash	Sakula malware
8b52cd1df70ef315bce38223ac7f4ec3	MD5 hash	Sakula malware
8feb7d6eae0ab9c1900fb6d0b236201b	MD5 hash	Sakula malware
90bc832fbaa6bbd7e4251c39473e5a4b	MD5 hash	Sakula malware
930af711a1579f3e1326cdb6d0005398	MD5 hash	Sakula malware
9526e4abcacc4e4a55fa1b2fc2313123	MD5 hash	Sakula malware
97479fa13d9b96da33cdb49749fc2baf	MD5 hash	Sakula malware
97a6e9e93bc591baf588bada61559d6a	MD5 hash	Sakula malware
97fc2d9b514f3183ae7c800408e5c453	MD5 hash	Sakula malware
985e819294cdc3b5561c5befa4bcbc5b	MD5 hash	Sakula malware
9c4db94cc3bdb9b5864bde553bff1224	MD5 hash	Sakula malware

9cee5c49dcaad59ea0eea6e7b67c304c	MD5 hash	Sakula malware
a006d31515bb2a54b5c3ddda8d66f24b	MD5 hash	Sakula malware
a05bc6c5f63880b565941ac5c5933bfe	MD5 hash	Sakula malware
a1a15a9e82880e8fc881668c70126315	MD5 hash	Sakula malware
a39c424e6df5d10b74aa72fb3a120c0c	MD5 hash	Sakula malware
a4856f40fd013b6144db8fe19625434b	MD5 hash	Sakula malware
a554e8867a076768e57e923a249f7a09	MD5 hash	Sakula malware
a81569d86c4a7bce2c446f169816a7ff	MD5 hash	Sakula malware
a90e38c3214eeba99aa46ad5e3ec34ff	MD5 hash	Sakula malware
a91ba2ab82553f43440ed24a9afeef82	MD5 hash	Sakula malware
ab357c26a2ed7379b62dd1cc869690b7	MD5 hash	Sakula malware
ab8badbf16a0cd7013197977f8b667e9	MD5 hash	Sakula malware
ab91b9e35d2b1e56285c042eef95d324	MD5 hash	Sakula malware
ae55d7b5c3d3bc7ed338d40ada25902f	MD5 hash	Sakula malware
aeed29398ceb645213cf639a9f80367c	MD5 hash	Sakula malware
af114e711259964b1db0235e9b39a476	MD5 hash	Sakula malware
af661cb478510d1d00dfdf1f2de4e817	MD5 hash	Sakula malware

b31e97c9740d8e95e56a5957777830d7	MD5 hash	Sakula malware
b38c4766ec0c5fb9b9e70af0b7414e78	MD5 hash	Sakula malware
b6b3e7b18384bb632602662a7f559bcd	MD5 hash	Sakula malware
b8346b4a5f8b4a6d79814f9824940504	MD5 hash	Sakula malware
ba5415f34927a356d4aaffb4bd7fe907	MD5 hash	Sakula malware
bb57362757182b928d66d4963104ffe8	MD5 hash	Sakula malware
bd48ca50da3b76aa497f28d842954c12	MD5 hash	Sakula malware
bdb6a8a95e5af85d8b36d73ba33ec691	MD5 hash	Sakula malware
bf35690e72a3fbd66ff721bd14a6599e	MD5 hash	Sakula malware
c5933a7ca469e98f7799c3ab52a1bc3c	MD5 hash	Sakula malware
c66b335fb606b542206b5a321beb2a76	MD5 hash	Sakula malware
c6d1954b58a17bd203e7b6be9d5047d8	MD5 hash	Sakula malware
c6eab24761a223e6c6f1a9d15ecca08a	MD5 hash	Sakula malware
cd1c95aa6f45101735d444aeb447225c	MD5 hash	Sakula malware
cfd1eb4ccdeea554d8cffa17021ffbfa	MD5 hash	Sakula malware
d1f0ff695021aed31ada3397ad1f491e	MD5 hash	Sakula malware
d2a27b9acb8dc9a9adbde76d2a10a189	MD5 hash	Sakula malware

d3cb441f03e8370155381d74c2b7d827	MD5 hash	Sakula malware
d57075de72308ed72d8f7e1af9ce8431	MD5 hash	Sakula malware
d5d6881b4bef3544d9067b71af3287eb	MD5 hash	Sakula malware
d7351f6937379dbbeedc83d37a86e794	MD5 hash	Sakula malware
d810b773e694279ece31106c26fb2869	MD5 hash	Sakula malware
d82230d1ac02405d16530f849abdde0b	MD5 hash	Sakula malware
d875a70c4b07dcc18770870c9c1d2abd	MD5 hash	Sakula malware
dc7469f6b18cfce712156e3988d238d2	MD5 hash	Sakula malware
df15e0f3169f65080ee7d783c061cda3	MD5 hash	Sakula malware
dfea1e69d2f5d84a1b6c6b67b01b7ff8	MD5 hash	Sakula malware
e0b6a8e23e0d586663e74f1e1d755ae0	MD5 hash	Sakula malware
e13bf40bbdbba86d638c04e0d72de268	MD5 hash	Sakula malware
e1b53ff413915e03245807b2eba504eb	MD5 hash	Sakula malware
e1ccd9f1696e4bf943fa2816356a443b	MD5 hash	Sakula malware
e36028a1bf428bb5a0993dc445deb5b8	MD5 hash	Sakula malware
e7139a2e1e28efd6c303dc28f676ffe3	MD5 hash	Sakula malware
e804f5d88ceb937b6ce0c900260793d3	MD5 hash	Sakula malware

ec85830342217b5d03f6bd26a703ce1a	MD5 hash	Sakula malware
ef855c88842821a15a80bbee00024817	MD5 hash	Sakula malware
ef94e4b0bd689972df09e19a3ed0653e	MD5 hash	Sakula malware
f1eb2a68d5d438e93a22b2126c812f4d	MD5 hash	Sakula malware
f349ee3706c815a79a60d2534284935d	MD5 hash	Sakula malware
f4862b793f89b9ca59da6ac38dff0e2d	MD5 hash	Sakula malware
f5b9862f2d508c57b81fbaaad91030f4	MD5 hash	Sakula malware
f8dbcfe4f826aa27724ccfd6b080b26d	MD5 hash	Sakula malware
f918fc73484f2a1684de53040ec816d2	MD5 hash	Sakula malware
f942344daf85bf211b4a27a1c947843c	MD5 hash	Sakula malware
f9b71e959f79d25bad195f59f5ae502e	MD5 hash	Sakula malware
faed2bcd842e81c180a6ac9dde78f8d5	MD5 hash	Sakula malware
fcad5bdeb3eb2eaa6e1c2bb9d9eb2cc0	MD5 hash	Sakula malware
fd69439c6e2bac79e490b9572b6c91ad	MD5 hash	Sakula malware
ff1d5c6a476a56eb7ca4e38b57761a4e	MD5 hash	Sakula malware

Table 6. Threat indicators for Sakula.