Mac.BackDoor.Systemd.1

vms.drweb.com/virus/

SHA1:

```
3cb1cfa072dbd28f02bd4a6162ba0a69f06f33f0
```

Trojan backdoor for macOS. Once launched, it sends the following string to the console:

```
This file is corrupted and connot be opened
```

It is executed as a daemon called systemd. In order to conceal its file, the Trojan marks it with flags uchg, schg and hidden. It can use the following arguments for the launch:

argument	value
d	daemon
r	launch
u	update

Then the Trojan creates file with SH commands and a PLIST file in order to register itself in the autorun.

```
#!/bin/sh
. /etc/rc.common
StartService (){
    ConsoleMessage "Start system Service"
    “File path" d
}
StopService (){
    return 0
}
RestartService (){
    return 0
}
RunService "$1"
```

A file with the following content is created:

```
{
    Description     = "Start systemd";
    Provides        = ("system");
    Requires        = ("Network");
    OrderPreference = "None";
}
```

Also a PLIST file is created:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
      <plist version="1.0">
      <dict>
               <key>Disabled</key>
               <false/>
               <key>UserName</key>
               <string>root</string>
               <key>Label</key>
               <string>
               com.appule.sysetmd
               </string>
               <key>KeepAlive</key>
               <dict>
                   <key>NetworkState</key>
                   <true/>
               </dict>
               <key>ProgramArguments</key>
                   <array>
                       <string>
                       File path
                       </string>
                       <string>d</string>
                  </array>
               <key>RunAtLoad</key>
               <true/>
               <key>StartInterval</key>
               <integer>5</integer>
      </dict>
      </plist>
```

The Trojan stores configuration information in its own file and encrypts it with the 3DES algorithm. Example of the decrypted configuration is as follows:

```
01 02 00 00-00 30 31 02-32 00 00 00-31 32 39 2E  ☺☻   01☻2   ***.
32 33 32 2E-31 39 35 2E-32 32 36 2C-34 33 2E 32  ***.***.226,**.2
34 37 2E 32-36 2E 33 37-2C 78 69 73-66 69 77 70  **.**.37,xis****
65 69 64 73-73 64 77 65-61 64 2E 63-6F 6D 03 05  *****wead.com♥♣
00 00 00 31-30 34 34 33-04 02 01 00-00 00 04 BC     10443♦☻☺    ♦╝
8E 12 99 9C-83 58 E6 0C-52 0C 3E DE-00 CA F2 0E  O↕ЩЬГХц♀R♀>▌╩Є♫
A4 1D ED 65-BF 47 3A CB-F9 26 3E B9-D9 3F 08 4C  д↔эе┐G:╦·&>╣╜?◘L
57 E8 C4 F6-05 3D 27 98-74 29 5D 1C-A8 44 ED 87  Wш─Ў♣='Шt)]∟иDэЗ
F4 86 98 5F-4B A8 13 BA-5A FE 8F 90-FF C0 41 F0  ЇЖШ_Ки‼╟Z■ПР ╰АЁ
CC D9 60 4D-F5 C3 42 29-19 88 95 72-10 64 6F 00  ╠╛`Mї├B)↓ИXr►do
22 8E 49 1C-28 CE DC AC-AA 1B 61 A3-97 2F 76 00  "OI∟(╬▄мк←агЧ/v
7E 1C ED 05-7D FC A3 96-A9 8A E4 57-6F 10 3A 2F  ~∟э♣}№гЦйКфWo►:/
56 3B EA EB-1E CE 41 93-61 B2 FC 09-10 30 4F 00  V;ъы▲╬АУa▒№○►0O
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 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 00-01 00 01 05                ☺ ☺♣
10 00 00 00-62 31 65 31-35 64 38 61-36 63 36 34  ►   b1e15d8a6c64
34 39 30 33-08 80 00 00-00 82 76 EE-86 35 91 59  4903◘A   ВvюЖ5СY
EF 72 28 0F-6A AB 99 33-4B 18 22 3F-AA 66 69 78  яr(☼jлЩ3К↑"?кfix
79 25 65 5D-15 B5 00 7A-B8 5A 79 F6-CF E1 71 C3  y%e]§╡ z╕ZyЎ╧cq├
EB F9 D4 95-2E 2B E9 C8-C5 81 3E 65-FB 19 EA 79  ы·╘X.+щ╙┼Б>e√↓ъy
A1 38 B4 06-0B AF A5 02-6C 19 65 BA-5C 2C 51 BE  б8┤♠♂пе☻l↓e╟\,Q╛
05 11 4C 8C-24 54 E5 2A-BC 4A 74 01-1C F3 51 6A  ♣◄LM$Tx*╝Jt☺∟єQj
1D 91 2E A1-05 02 5C 58-AA 5F F2 C7-A3 F5 08 3D  ↔С.б♣☻\Хк_Є╠гї◘=
BE 3E 3C 8F-09 DB FE DD-B3 8C D5 9B-23 8B 11 AA  ╛><П○▉■▌│М╒Ы#Л◄к
CA C5 48 8A-C7 A5 D1 F6-1B 00 00 00-00 00 00 07  ╩┼НК╟е╤Ў←       •
```

Depending on the Trojan configuration, it establishes a connection with the command and control server itself or waits for an incoming connection request. Once connected, the backdoor executes the commands it receives and periodically sends the following information to cybercriminals:

- Name and version of the operating system;
- User name;
- Availability of root privileges;
- MAC addresses of all available network interfaces;
- IP addresses of all available network interfaces;
- External IP address;
- CPU type;
- RAM amount;
- Data about the malware version and its configuration.

Information, which is shared between the Trojan and the C&C server, is encrypted with the 3DES algorithm. The backdoor can execute the following commands:

command	Parameter	Value
0x200	file manager	execute commands of the file manager
	1 - list dir (ls -la *)	receive a list of the contents of a specified directory
	2 - read file	read a file
	3 - write file	write to a file, it also can write data to a file for an update
	4 - list file (ls -la file)	get the contents of a file
	5 - chmod/chown/rename	execute CHMOD, CHOWN and RENAME commands
	6 - delete file	delete a file
	7 - mkdir	create a directory
0x300		execute a command in the bash shell
0x400		update the Trojan
0x500		reinstall the Trojan
0x800		change the command and control server’s IP address
0x900		install a plug-in

News about the Trojan