Find out about Virus.Win32.Sality.ag template

Viruses like these often have a mechanism to replicate the resources on the infected computer, unlike worms, unused viruses and exploit network services to replicate and spread themselves to other computers ..

Viruses like these often have a mechanism to manually replicate the resources on the infected computer, unlike worms, unused viruses and exploit network services to replicate themselves. and spread to other computers . A complete copy of the virus will automatically 'crawl' the computers if the infected object is identified in one of the following ways - for several reasons or reasons that are not related to the functioning. of that virus. Eg:

- When infecting one or more accessible drives, the virus will infiltrate one or more fixed files on the system.

- They can copy themselves to mobile storage devices

- When the user sends 1 or more emails with infected files

Virus.Win32.Sality.ag (by Kaspersky's naming method) is also known in the following forms:

- *Trojan.Win32.Vilsel.vyz (also according to Kaspersky Lab)*
- *W32 / Sality.aa (Panda)*
- *Virus: Win32 / Sality.AT (MS (OneCare))*
- *Win32 / Sality.NBA virus (Nod32)*
- *Win32.Sality.3 (BitDef7)*
- *Win32.Sality.BK (VirusBuster)*
- *W32 / Sality.AG (AVIRA)*
- *W32 / Sality.BD (Norman)*
- *Virus.Win32.Sality.ag [AVP] (FSecure)*
- *PE_SALITY.BA (TrendMicro)*
- *Virus.Win32.Sality.at (v) (Sunbelt)*
- *Win32.Sality.BK (VirusBusterBeta)*

This virus sample was discovered on April 7, 2010 at 08:21 GMT, operating the next day - April 8, 2010 at 09:40 GMT, the analysis information was officially announced on the same day - April 8, 2010 at 13:13 GMT.

Detailed technical analysis

Malicious programs like these often infect and "execute" executable files on infected computers. They also have the function of automatically downloading and activating additional malicious programs on the victim's computer without their knowledge. And essentially, they are Windows PE EXE files, written in C ++ language.

When enabled, these programs automatically 'extract' one or more files from themselves and save them in Windows system folders with different names:

% System% drivers.sys

with is often random Latin character string, such as INDSNN. These files are usually kernel mode drivers of 5157 bytes. And according to Kaspersky Anti-Virus they are classified into *Virus.Win32.Sality.ag* class.

The drivers are decompressed, installed and activated into a Windows service called amsint32.

Infection process

In essence, they are created to infect all Windows executable files with the * .EXE and * .SCR extensions. But only files containing those sections in the PE header section are infected: TEXT, UPX and CODE.

When successfully infected with the PE file, the virus will inherit the final sections in the file and copy the body to the end of the section. After that, they will spread everywhere on the hard drive and continue to find more files to infect. And when these infected files are activated, they will immediately copy the original file's body to a temporary folder created with the following name:

% Temp% __ Rar.exe

To make sure they activate automatically when the system starts, they will copy themselves to all logical partitions with random names and extensions in the following list: * .exe, * .pif and * .cmd. Also, they create hidden files in the root of these drives:: autorun.inf - here the code, the command to activate the malicious files are stored. Or when users open Windows Explorer, these viruses will also be activated.

Payload method

Once operational, they will create unified identification parameters called Ap1mutx7 to mark their presence in the system. And then, they will continue to download data from the following addresses:

*http:///*******nc.sa.funpic.de/images/logos.gif*
*http:///www.*********ccorini.com/images/logos.gif*
*http:///www.********gelsmagazine.com/images/logos.gif*
*http:///www.********ukanadolu.com/images/logos.gif*
*http:///******vdar.com/logos_s.gif*
*http:///www.****r-adv.com/gallery/Fusion/images/logos.gif*
*http:///********67.154/testo5/*
*http:///*********stnet777.info/home.gif*
*http:///*******stnet888.info/home.gif*
*http:///**********net987.info/home.gif*
*http:///www.**********wieluoi.info/*
*http:///**********et777888.info/*
*http:///********7638dfqwieuoi888.info/*

These files will be saved in the% Temp% folder and automatically activated. At this point, the following templates will be downloaded to the system from the links listed above:

- *Backdoor.Win32.Mazben.ah*
- *Backdoor.Win32.Mazben.ax*
- *Trojan.Win32.Agent.didu*

The above templates are created primarily for spam and spam. In addition to the task of downloading other malicious malware, these viruses can also modify Windows system parameters, such as:

- Lock the operation of Task Manager, refuse to edit the Registry by changing the following key:

[HKÑUSoftwareMicrosoftWindowsCurrentVersionPoliciessystem]
"DisableRegistryTools" = dword: 00000001
"DisableTaskMgr" = dword: 00000001

- Change Windows Security Center settings by intervening and Registry in the following way:

[HKLMSOFTWAREMicrosoftSecurity Center]
"AntiVirusOverride" = dword: 00000001
"FirewallOverride" = dword: 00000001
"UacDisableNotify" = dword: 00000001

[HKLMSOFTWAREMicrosoftSecurity CenterSvc]
"AntiVirusDisableNotify" = dword: 00000001
"AntiVirusOverride" = dword: 00000001
"FirewallDisableNotify" = dword: 00000001
"FirewallOverride" = dword: 00000001
"UacDisableNotify" = dword: 00000001
"UpdatesDisableNotify" = dword: 00000001

- Hidden files cannot be displayed by adding the following parameters to the Registry:

[HKCUSoftwareMicrosoftWindowsCurrentVersionExplorer
Advanced]
"Hidden" = dword: 00000002

Changing options in the default browser always activates online mode:
[HKCUSoftwareMicrosoftWindowsCurrentVersionInternet Settings]
"GlobalUserOffline" = dword: 00000000
Turn off the UAC (User Account Control) function by changing the EnableLUA parameter in the Registry to 0:
[HKLMSoftwareMicrosoftWindowsCurrentVersionpoliciessystem]
"EnableLUA" = dword: 00000000

- Self-assigning themselves to the Windows firewall's secure application list to gain access to the Internet and the system network:

[HKLMSystemCurrentControlSetServicesSharedAccess
ParametersFirewallPolicyStandardProfileAuthorizedApplicationsList]
""
*= ": *: Enabled: ipsec"*

- Create a registry key to store data:

HKCUSoftware

Here is the custom value.

- Continue, they will search for the file:

% WinDir% system.ini

and assign the following record values ??to the file:

[MCIDRV_VER]
DEVICEMB = 509102504668 (any arbitrary number)

- At the same time, they delete the following keys to make the computer unable to boot in Safe Mode:

HKLMSystemCurrentControlSetControlSafeBoot
HKCUSystemCurrentControlSetControlSafeBoot

- Delete all * .exe and * .rar files in the temporary directory of all user accounts: *% Temp%*

- Continue to find and delete files with the format: * .VDB, * .KEY, * .AVC and * .drw
on the other hand, they use previously decomposed drives to block all requests to connect to domains that contain the following strings:

upload_virus
sality-remov
virusinfo.
cureit.
drweb.
onlinescan.
spywareinfo.
ewido.
virusscan.
windowsecurity. S
pywareguide. bitdefender.
pandasoftware.

agnmitum.
virustotal.
sophos.
trendmicro.
etrust.com
symantec.
mcafee.
f-secure.
eset.com
kaspersky

- Disconnect and delete the following services:

Agnitum Client Security Service
ALG Amon monitor
aswUpdSv
aswMon2
aswRdr
aswSP
aswTdi
aswFsBlk
acssrv
AV Engine
avast! iAVS4
Control Service
avast! Antivirus
avast! Mail Scanner
avast! Web Scanner
avast! Asynchronous Virus Monitor
avast! Self Protection
AVG E-mail Scanner
Avira AntiVir Premium Guard
Avira AntiVir Premium WebGuard
Avira AntiVir Premium MailGuard
avp1
BackWeb Plug-in - 4476822
bdss
BGLiveSvc
BlackICE
CAISafe
ccEvtMgr
ccProxy
ccSetMgr
COMODO Firewall Pro Sandbox Driver
cmdGuard
cmdAgent
Eset Service
Eset HTTP Server
Eset Personal Firewall

F-Prot Antivirus Update Monitor
fsbwsysFSDFWD
F-Secure Gatekeeper Handler Starter
FSMA
Google Online Services
InoRPC
InoRT
InoTask
ISSVC
KPF4
KLIF
LavasoftFirewall
LIVESRV
McAfeeFramework
McShield
McTaskManager
navapsvc
NOD32krn
NPFMntor
NSCService
Outpost Firewall main module
OutpostFirewall
PAVFIRES
PAVFNSVR
PavProt PavPrSrv
PAVSRV
PcCtlCom PersonalFirewal
PREVSRV
ProtoPort Firewall service
PSIMSVC
RapApp
SmcService
SNDSrvc
SPBBCSvc
SpIDer FS Monitor for Windows NT
SpIDer Guard File System Monitor
SPIDERNT
Symantec Core LC
Symantec Password Validation
Symantec AntiVirus Definition Watcher
SavRoam
Symantec AntiVirus
Tmntsrv
TmPfw
tmproxy
tcpsr
UmxAgent
UmxCfg
UmxLU

UmxPol
vsmon
VSSERV
WebrootDesktopFirewallDataService
WebrootFirewall
XCOMM
AVP

- At the same time, they can also prevent scanning and identification processes of security programs or popular support tools today.

Ways to prevent and remove viruses

If the computer you are using does not have a strong security program, or does not update the database for the application, the risk of being affected is very high. Use the following tips to keep your system safe:

- Use Kaspersky products here or here, and always update Kaspersky completely. However, users can almost never delete all infected files, because they 'stick' to most executable files (* .exe) of Windows, so use them. Add Sality Killer tool.

- Restore previously edited Registry keys:

[HKLMSoftwareMicrosoftWindowsCurrentVersionpoliciessystem]
"EnableLUA" = dword: 00000000

[HKLMSOFTWAREMicrosoftSecurity Center]
"AntiVirusOverride" = dword: 00000000
"FirewallOverride" = dword: 00000001
"UacDisableNotify" = dword: 00000001

[HKLMSOFTWAREMicrosoftSecurity CenterSvc]
"AntiVirusDisableNotify" = dword: 00000000
"AntiVirusOverride" = dword: 00000000
"FirewallDisableNotify" = dword: 00000000
"FirewallOverride" = dword: 00000000
"UacDisableNotify" = dword: 00000000
"UpdatesDisableNotify" = dword: 00000000

[HKCUSoftwareMicrosoftWindowsCurrentVersionExplorerAdvanced] "Hidden" = dword: 00000002

- Delete the following keys in the Registry:

[HKÑUSoftwareMicrosoftWindowsCurrentVersionPoliciessystem]
"DisableRegistryTools"
"DisableTaskMgr"

[HKCUSoftwareMicrosoftWindowsCurrentVersion

Internet Settings] "GlobalUserOffline"

- Delete all files in the temporary folder including Temp and% Temp%

- Only use the security software of reputable firms, encourage you to buy the official license of the application - to ensure benefits and receive direct support from the manufacturer. You can refer to the security program here.

Good luck!