Sality

By Contributors to Wikimedia projects

Published: 2012-01-13 · Archived: 2026-04-05 14:34:17 UTC

From Wikipedia, the free encyclopedia

Sality is the classification for a family of malicious software (malware) infecting Microsoft Windows system files. Sality was first discovered in 2003 and has advanced into a dynamic, enduring, full-featured form of malicious code. Systems infected with Sality may communicate over a peer-to-peer (P2P) network to form a botnet to relay spam, proxy communications, exfiltrate sensitive data, compromise web servers, and/or coordinate distributed computing tasks to process intensive tasks (e.g., password cracking). Since 2010, certain variants of Sality have also incorporated rootkit functions as part of an ongoing evolution of the malware family. Because of its continued development and capabilities, Sality is considered one of the most complex and formidable forms of malware to date.

The majority of Antivirus (A/V) vendors use the following naming conventions when referring to this family of malware:

- Sality
- SalLoad
- Kookoo
- SaliCode
- Kukacka

Sality is a family of polymorphic file infectors, which target Windows executable files with the extensions .EXE or .SCR.[1] Sality utilizes polymorphic and entry-point obscuring (EPO) techniques to infect files using the following methods: not changing the entry point address of the host, and replacing the original host code at the entry point of the executable with a variable stub to redirect execution to the polymorphic viral code, which has been inserted in the last section of the host file;[2][3] the stub decrypts and executes a secondary region, known as the loader; finally, the loader runs in a separate thread within the infected process to eventually load the Sality payload.[2]

Sality may execute a malicious payload that deletes files with certain extensions and/or beginning with specific strings, terminates security-related processes and services, searches a user's address book for e-mail addresses to send spam messages,[4] and contacts a remote host. Sality may also download additional executable files to install other malware, and for the purpose of propagating pay per install applications. Sality may contain Trojan components; some variants may have the ability to steal sensitive personal or financial data (i.e., information stealers),[5] generate and relay spam, relay traffic via HTTP proxies, infect websites, and achieve distributed computing tasks such as password cracking, as well as other capabilities.[2]

Sality's downloader mechanism downloads and executes additional malware as listed in the URLs received using the peer-to-peer component. The distributed malware may share the same “code signature” as the Sality payload, which may provide attribution to one group and/or indicate that they share a large portion of the code. The additional malware typically communicates with and reports to central command and control (C&C) servers located throughout the world. According to Symantec, the "combination of file infection mechanism and the fully decentralized peer-to-peer network [...] makes Sality one of the most effective and resilient malware in today's threat landscape."[2]

Two versions of the botnet are currently active: versions 3 and 4. The malware circulated on those botnets is digitally signed by the attackers to prevent a hostile takeover. In recent years, Sality has also included the use of rootkit techniques to maintain persistence on compromised systems and evade host-based detections, such as anti-virus software.[6]

The top countries affected by the botnet were India, Vietnam, and Morocco.[7]

Sality infects files in the affected computer. Most variants use a DLL that is dropped once on each computer. The DLL file is written to disk in two forms, for example:

- %SYSTEM%\wmdrtc32.dll
- %SYSTEM%\wmdrtc32.dl_

The DLL file contains the bulk of the virus code. The file with the extension ".dl_" is the compressed copy. Recent variants of Sality, such as Virus:Win32-Sality.AM, do not drop the DLL; instead, load it entirely in memory without writing it to disk. This variant, along with others, also drop a driver with a random file name in the folder %SYSTEM%\drivers. Other malware may also drop Sality in the computer. For example, a Sality variant detected as Virus:Win32-Sality.AU is dropped by Worm:Win32-Sality.AU.[1] Some Sality variants may also include a rootkit by creating a device named Device\amsint32 or \DosDevices\amsint32.[6]

Method of propagation

[edit]

Sality usually targets all files in drive C: that have .SCR or .EXE file extensions, beginning with the root folder. Infected files increase in size by a varying amount.

The virus also targets applications that run at each Windows start and frequently used applications, referenced by the following registry keys:

- HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run[1]

Sality avoids infecting particular files in order to remain hidden in the computer:

- Files protected by System File Checker (SFC)
- Files under the %SystemRoot% folder

- Executables of several antivirus/firewall products ignore files that contain certain substrings

Removable drives and network shares

[edit]

Some Sality variants can infect legitimate files, which are then moved to available removable drives and network shares by enumerating all network share folders and resources of the local computer and all files in drive C: (beginning with the root folder). It infects the files it finds by adding a new code section to the host and inserting its malicious code into the newly added section. If a legitimate file exists, the malware will copy the file to the Temporary Files folder and then infect the file. The resulting infected file is then moved to the root of all available removable drives and network shares as any of the following:

- *random file name*.pif
- *random file name*.exe
- *random file name*.cmd

The Sality variant also creates an "autorun.inf" file in the root of all these drives that points to the virus copy. When a drive is accessed from a computer supporting the AutoRun feature, the virus is then launched automatically.[1] Some Sality variants may also drop a file with a .tmp file extension to the discovered network shares and resources as well as drop a .LNK file to run the dropped virus.[8]

- Sality may inject code into running processes by installing a message hook[9]
- Sality commonly searches for and attempts to delete files related to antivirus updates and terminate security applications, such as antivirus and personal firewall programs; attempts to terminate security applications containing the same strings as the files it avoids infecting; and may also terminate security-related services and block access to security-related websites that contain certain substrings[1][2][3][8][10][11][12][13][14][15][16][17]
- Sality variants may modify the computer registry to lower Windows security, disable the use of the Windows Registry Editor and/or prevent the viewing of files with hidden attributes; Some Sality variants recursively delete all registry values and data under the registry subkeys for HKCU\System\CurrentControlSet\Control\SafeBoot and HKLM\System\CurrentControlSet\Control\SafeBoot to prevent the user from starting Windows in safe mode[1][4][8][10][11][18][19][20]
- Some Sality variants can steal sensitive information such as cached passwords and logged keystrokes, which were entered on the affected computer[1][13][15]
- Sality variants usually attempt to download and execute other files including pay per install executables using a preconfigured list of up to 1000 peers; the goal of the P2P network is to exchange lists of URLs to feed to the downloader functionality; the files are downloaded into the Windows Temporary Files folder and decrypted using one of several hardcoded passwords[1][2][3][5][9][10][11][12][13][14][15][16][18][20][21]
- Most of Sality's payload is executed in the context of other processes, which makes cleaning difficult and allows the malware to bypass some firewalls; to avoid multiple injections in the same process, a system-

wide mutex called `<process name>.exeM_<process ID>_` is created for every process in which code is injected, which would prevent more than one instance from running in memory at the same time.[1]

- Some variants of Win32-Sality drop a driver with a random file name in the folder %SYSTEM%\drivers to perform similar functions such as terminate security-related processes and block access to security-related websites, and may also disable any system service descriptor table (SSDT) hooks to prevent certain security software from working properly[1][2][3][10][11][12][18][20][22][23]
- Some Sality variants spread by moving to available removable/remote drives and network shares[1][2][3][8][9][11][12][20]
- Some Sality variants drop .LNK files, which automatically run the dropped virus[8]
- Some Sality variants may search a user's Outlook address book and Internet Explorer cached files for e-mail addresses to send spam messages, which then sends out spammed messages based on information it retrieves from a remote server[4]
- Sality may add a section to the configuration file %SystemRoot%\system.ini as an infection marker, contact remote hosts to confirm Internet connectivity, report a new infection to its author, receive configuration or other data, download and execute arbitrary files (including updates or additional malware), receive instruction from a remote attacker, and/or upload data taken from the affected computer; some Sality Variants may open a remote connection, allowing a remote attacker to download and execute arbitrary files on the infected computer[4][9][11][12][13][14][15][16][18][20][21]
- Computers infected with recent versions of Sality, such as Virus:Win32-Sality.AT, and Virus:Win32-Sality.AU, connect to other infected computers by joining a peer-to-peer (P2P) network to receive URLs pointing to additional malware components; the P2P protocol runs over UDP, all the messages exchanged on the P2P network are encrypted, and the local UDP port number used to connect to the network is generated as a function of the computer name[1]
- Sality may add a rootkit that includes a driver with capabilities such as terminating processes via NtTerminateProcess as well as blocking access to select anti-virus resources (e.g. anti-virus vendor web sites) by way of IP Filtering; the latter requires the driver to register a callback function, which will be used to determine if packets should be dropped or forwarded (e.g. drop packets if string contains the name of an anti-virus vendor from a comprised list)[6]

Microsoft has identified dozens of files which are all commonly associated with the malware.[1][4][8][9][10][11][12][13][14][15][16][17][21][22][23][24][25][26][27] Sality uses stealth measures to maintain persistence on a system; thus, users may need to boot to a trusted environment in order to remove it. Sality may also make configuration changes such as to the Windows Registry, which makes it difficult to download, install and/or update virus protection. Also, since many variants of Sality attempt to propagate to available removable/remote drives and network shares, it is important to ensure the recovery process thoroughly detects and removes the malware from any and all known/possible locations.

- Computer virus

1. ^ Jump up to: ***a*** ***b*** ***c*** ***d*** ***e*** ***f*** ***g*** ***h*** ***i*** ***j*** ***k*** ***l*** ***m*** *Microsoft Malware Protection Center (2010-08-07). "Win32-Sality". Microsoft. Archived from the original on 2013-09-17. Retrieved 2012-04-22.*

2. ^ Jump up to: *a b c d e f g h* Nicolas Falliere (2011-08-03). *"Sality: Story of a Peer-to-Peer Viral Network"* (PDF). Symantec. Archived from *the original* (PDF) on September 24, 2015. Retrieved 2012-01-12.
3. ^ Jump up to: *a b c d e* Angela Thigpen and Eric Chien (2010-05-20). *"W32.Sality"*. Symantec. Archived from *the original* on 2013-10-05. Retrieved 2012-04-22.
4. ^ Jump up to: *a b c d e* Microsoft Malware Protection Center (2009-05-29). *"Win32-Sality.A"*. Microsoft. Retrieved 2012-04-22.
5. ^ Jump up to: *a b* FireEye, Inc (2012-02-14). *"FireEye Advanced Threat Report - 2H 2011"* (PDF). FireEye. Archived from *the original* (PDF) on 2012-05-22. Retrieved 2012-04-22.
6. ^ Jump up to: *a b c* Artem I. Baranov (2013-01-15). *"Sality Rootkit Analysis"*. Archived from *the original* on 2013-08-10. Retrieved 2013-01-19.
7. ^ *"Kaspersky Threats — Sality"*. threats.kaspersky.com.
8. ^ Jump up to: *a b c d e f* Microsoft Malware Protection Center (2010-07-30). *"Worm:Win32-Sality.AU"*. Microsoft. Archived from *the original* on 2013-09-27. Retrieved 2012-04-22.
9. ^ Jump up to: *a b c d e* Microsoft Malware Protection Center (2010-04-28). *"Virus:Win32-Sality.G.dll"*. Microsoft. Retrieved 2012-04-22.
10. ^ Jump up to: *a b c d e* Microsoft Malware Protection Center (2010-06-28). *"Virus:Win32-Sality.AH"*. Microsoft. Retrieved 2012-04-22.
11. ^ Jump up to: *a b c d e f g* Microsoft Malware Protection Center (2010-08-27). *"Virus:Win32-Sality.gen!AT"*. Microsoft. Retrieved 2012-04-22.
12. ^ Jump up to: *a b c d e f* Microsoft Malware Protection Center (2010-10-21). *"Virus:Win32-Sality.gen!Q"*. Microsoft. Retrieved 2012-04-22.
13. ^ Jump up to: *a b c d e* Microsoft Malware Protection Center (2008-07-03). *"Virus:Win32-Sality.R"*. Microsoft. Archived from *the original* on 2014-04-04. Retrieved 2012-04-22.
14. ^ Jump up to: *a b c d* Microsoft Malware Protection Center (2008-07-07). *"Virus:Win32-Sality.T"*. Microsoft. Archived from *the original* on 2014-04-04. Retrieved 2012-04-22.
15. ^ Jump up to: *a b c d e* Microsoft Malware Protection Center (2008-07-07). *"Virus:Win32-Sality.AN"*. Microsoft. Retrieved 2012-04-22.
16. ^ Jump up to: *a b c d* Microsoft Malware Protection Center (2009-03-06). *"Virus:Win32-Sality.S"*. Microsoft. Retrieved 2012-04-22.
17. ^ Jump up to: *a b* Microsoft Malware Protection Center (2008-07-08). *"Virus:Win32-Sality"*. Microsoft. Archived from *the original* on 2012-01-01. Retrieved 2012-04-22.
18. ^ Jump up to: *a b c d* Microsoft Malware Protection Center (2010-07-30). *"Virus:Win32-Sality.AU"*. Microsoft. Archived from *the original* on 2013-09-27. Retrieved 2012-04-22.
19. ^ Microsoft Malware Protection Center (2010-07-30). *"TrojanDropper:Win32-Sality.AU"*. Microsoft. Retrieved 2012-04-22.
20. ^ Jump up to: *a b c d e* Microsoft Malware Protection Center (2010-04-26). *"Virus:Win32-Sality.AT"*. Microsoft. Archived from *the original* on 2014-01-30. Retrieved 2012-04-22.
21. ^ Jump up to: *a b c* Microsoft Malware Protection Center (2007-11-16). *"Virus:Win32-Sality.M"*. Microsoft. Archived from *the original* on 2014-04-05. Retrieved 2012-04-22.

22. ^ Jump up to: *a* *b* *Microsoft Malware Protection Center (2010-08-10). "Trojan:WinNT-Sality". Microsoft. Archived from the original on 2013-12-05. Retrieved 2012-04-22.*
23. ^ Jump up to: *a* *b* *Microsoft Malware Protection Center (2010-09-17). "WinNT-Sality". Microsoft. Retrieved 2012-04-22.*
24. ^ *Microsoft Malware Protection Center (2010-04-14). "Virus:Win32-Sality.G". Microsoft. Archived from the original on 2014-04-05. Retrieved 2012-04-22.*
25. ^ *Microsoft Malware Protection Center (2008-07-08). "Virus:Win32-Sality.AM". Microsoft. Archived from the original on 2013-12-09. Retrieved 2012-04-22.*
26. ^ *Microsoft Malware Protection Center (2009-06-17). "Virus:Win32-Sality.gen!P". Microsoft. Retrieved 2012-04-22.*
27. ^ *Microsoft Malware Protection Center (2009-09-02). "Virus:Win32-Sality.gen". Microsoft. Retrieved 2012-04-22.*
