SALITY

مجموعه گزارش‌های پلیدهای ابدی

شبکه گستر
امنیت شما | وظیفه ما

فهرست مطالب

چکیده مدیریتی

Sality بدافزاری از نوع ویروس[1] است که با چسباندن کد مخرب به فایل‌های اجرایی سالم، آنها را آلوده و تبدیل به ناقلی از خود می‌کند. ضمن اینکه با کپی فایل‌های آلوده بر روی حافظه‌های جداشدنی[2]، پوشه‌های اشتراکی و در برخی از نسخه‌ها سوءاستفاده از آسیب‌پذیری‌های امنیتی سیستم عامل، خود را به‌سرعت در سطح شبکه توزیع می‌کند.

این بدافزار بخش ابتدایی فایل‌های اجرایی را با کدی پیچیده جایگزین می‌کند تا در زمان اجرای فایل، کد مخرب فراخوانی شده و در عین حال عملکرد اصلی فایل نیز حفظ شود.

نخستین نسخه از بدافزار Sality در ۱۷ فروردین ۱۳۸۲ شناسایی شد و طی یک دهه پس از آن، نسخه‌های متعددی از این بدافزار مخرب با کدهایی پویا و با قابلیت‌های پیشرفته عرضه شد. از جمله این قابلیت‌ها می‌توان به توانایی فعالیت به‌عنوان درب‌پشتی[3]، جاسوس‌افزار[4] و روت‌کیت[5] اشاره کرد.

اگر چه چندین سال است که نسخه جدیدی از Sality ارائه نشده اما متأسفانه ایران در فهرست پنج کشوری است که این بدافزار در آنها بیشترین فعالیت را دارد.

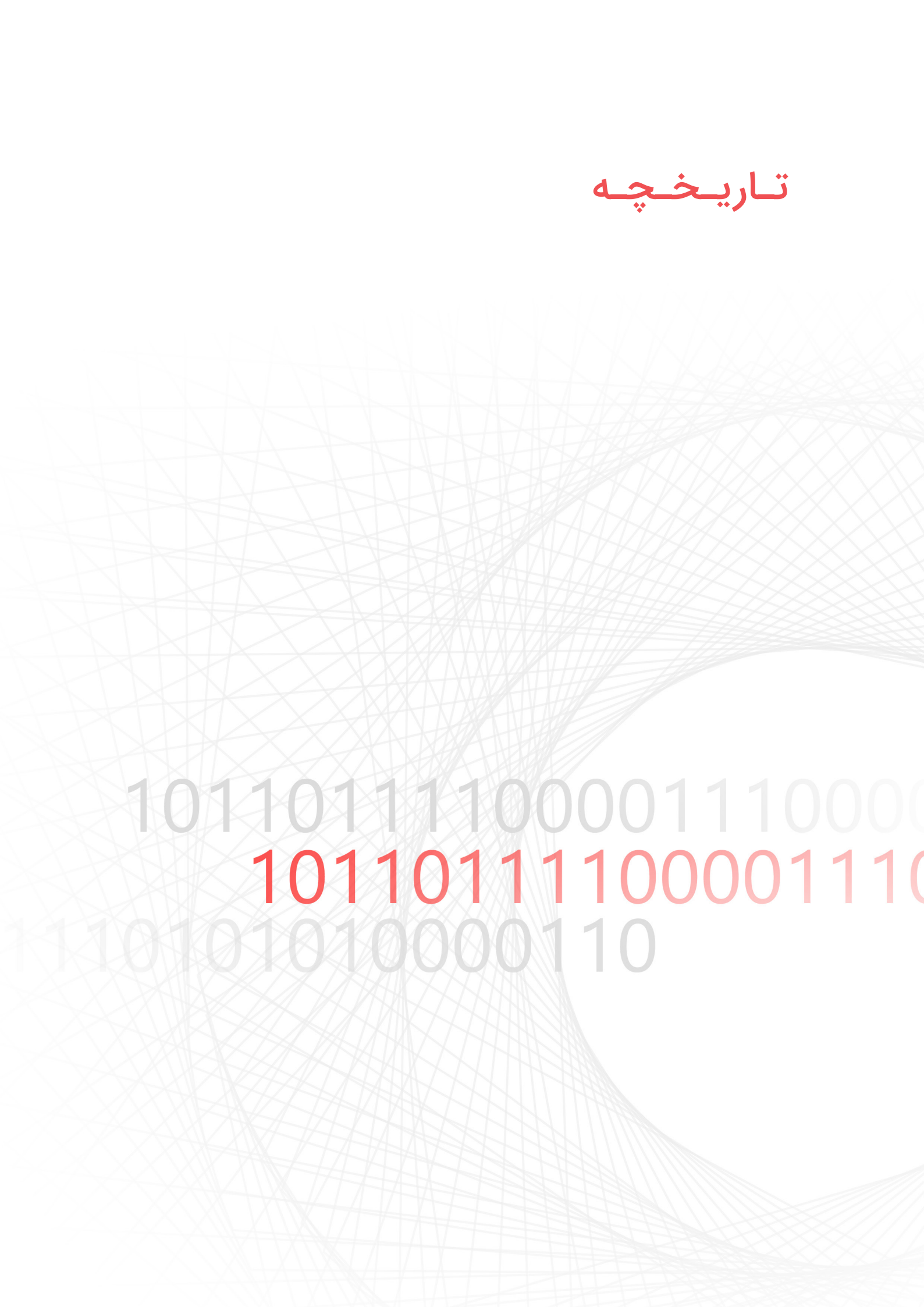
در این گزارش ضمن بررسی روش کار نسخه‌های متداول Sality به راه‌های مقابله با این بدافزار مخرب پیر پرداخته شده است.

India	26.30%
China	18.13%
Vietnam	7.05%
Indonesia	4.58%
Iran, Islamic Republic of	3.59%
Pakistan	3.47%
Thailand	3.47%
Philippines	3.34%
Egypt	2.35%
Turkey	1.98%

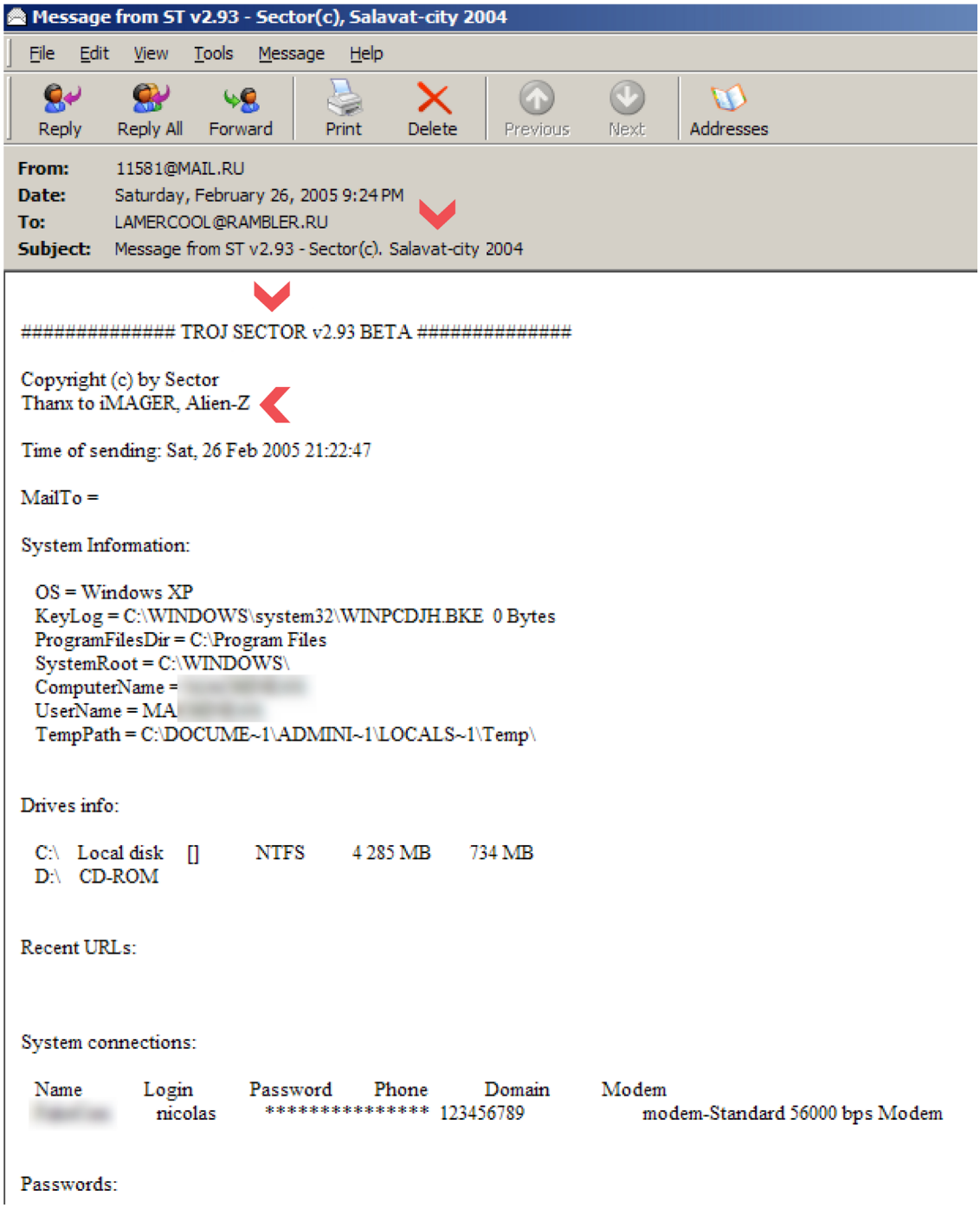
ایران در میان ده کشور با بیشترین آلودگی به بدافزار Sality - منبع: LookingGlass

[1] Virus
[2] Removable Storage
[3] Backdoor
[4] Spyware
[5] Rootkit

تاریخچه


10110111100001110000
1011011110000111
1110101010000110

در نسخه‌های نخستین Sality، اطلاعات جمع‌آوری شده از روی دستگاه قربانی نظیر کلیدهای فشرده شده توسط کاربر، رمزهای عبور ذخیره شده در محضرخانه[1] و تنظیمات Dial-up با استفاده از چندین سرور SMTP که همگی در روسیه قرار داشتند به مهاجمان ایمیل می‌شد. نمونه‌ای از این ایمیل‌ها در شکل زیر قابل مشاهده است.



Message from ST v2.93 - Sector(c), Salavat-city 2004

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: 11581@MAIL.RU
Date: Saturday, February 26, 2005 9:24 PM
To: LAMERCOOL@RAMBLER.RU
Subject: Message from ST v2.93 - Sector(c). Salavat-city 2004

############### TROJ SECTOR v2.93 BETA ###############

Copyright (c) by Sector
Thanx to iMAGER, Alien-Z

Time of sending: Sat, 26 Feb 2005 21:22:47

MailTo =

System Information:

OS = Windows XP
KeyLog = C:\WINDOWS\system32\WINPCDJH.BKE 0 Bytes
ProgramFilesDir = C:\Program Files
SystemRoot = C:\WINDOWS\
ComputerName =
UserName = MA
TempPath = C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\

Drives info:

C:\ Local disk [] NTFS 4 285 MB 734 MB
D:\ CD-ROM

Recent URLs:

System connections:

Name	Login	Password	Phone	Domain	Modem
	nicolas	**********	123456789		modem-Standard 56000 bps Modem

Passwords:

نمونه‌ای از ایمیل ارسالی به نویسندگان Sality که محتوای آن را اطلاعات سرقت شده از روی دستگاه آلوده به این بدافزار تشکیل می‌دهد

[1] Registry

کلمه Sality برگرفته شده از دو کلمه Salavat و City است که در عنوان این ایمیل‌ها به چشم می‌خورد. Salavat نام شهری در روسیه است.

وجود Sector، iMager و Alien-Z در ایمیل‌های مذکور موجب شده تا برخی از شرکت‌های ضدویروس از این کلمات نیز در نامگذاری این بدافزار استفاده کنند.

در برخی از نسخه‌های اولیه Sality، در روزهای دهم تا دوازدهم هر ماه در زمانی که دقیقه با ساعت برابر می‌شد پیامی مشابه تصویر زیر ظاهر می‌شد:

پیامی که در نسخه‌های اولیه Sality در شرایطی خاص بر روی دستگاه آلوده نمایان می‌شد

موضوعی که سبب گردید شرکت سوفوس این بدافزار را Kuku که در زبان روسی به معنای قایم موشک است نامگذاری کند.

همان‌طور که مشخص است در آن دوران نویسندگان این بدافزار ابایی از قرار دادن نشانه‌ها و سرنخ‌هایی که ملیت و نام گروه آنها را فاش کند نداشتند.

در فاصله بین سال‌های ۱۳۸۳ تا اواسط ۱۳۸۷ نویسندگان Sality تغییراتی بنیادی در این بدافزار اعمال کردند. از جمله می‌توان به چندشکلی شدن[۱] آن اشاره کرد که موجب دشوارتر شدن شناسایی توسط محصولات امنیتی شد. یا تفکیک کد اصلی مخرب[۲] با کد ویروس که از این طریق بدافزار قادر به اجرای هر گونه کد دیگری که از نشانی‌های زیر دریافت می‌کرد شد:

- www[.]h3ns1k.info
- www[.]g1ikdcvns3sdsal.info
- www[.]f5ds1jkkk4d.info

در این سال‌ها بتدریج Sality مجهز به قابلیت‌هایی به‌منظور مسدود و غیرفعال کردن تعدادی از محصولات دیواره آتش و ضدویروس شد.

بر خلاف نسخه‌های ابتدایی، نویسندگان از درج عناوین و عباراتی در کد که به‌نحوی ماهیت این گروه را افشا کند پرهیز می‌کردند. گر چه همچنان کلماتی نظیر kuku در کد آنها به چشم می‌خورند.

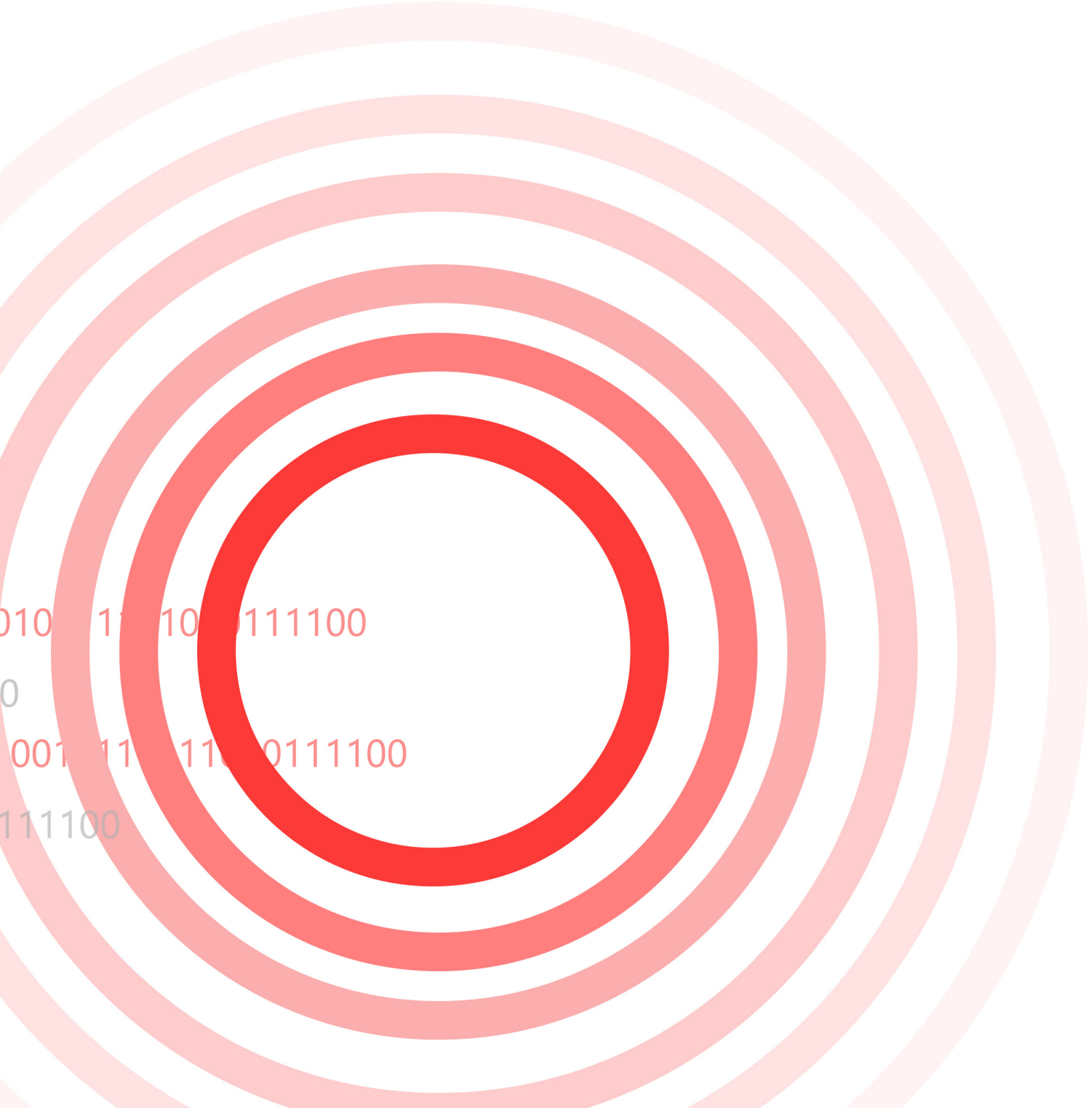
در حالی که تا پیش از آن نشانی‌های سرور فرماندهی[۳] در کد بدافزار تزریق شده بودند و محصولات امنیتی و نهادهای نظارتی به‌سادگی می‌توانستند با مسدودسازی دسترسی به این نشانی‌ها موجب توقف به‌روزرسانی Sality شوند از اواخر ۱۳۸۷ که می‌توان آن را نقطه عطفی در تاریخ این بدافزار دانست از روش‌های نقطه‌به‌نقطه و شبکه‌های مخرب برای دریافت کدهای جدید بهره گرفته شد. مکانیزمی که در عمل موجب بقای طولانی مدت این بدافزار گردید.

از سال ۱۳۸۹ برخی نسخه‌ها از Sality مجهز به قابلیت روت‌کیت شدند.

بخاطر تدام ارتقای آن، Sality به‌عنوان یکی از پیچیده‌ترین و توانمندترین بدافزارها شناخته می‌شود.

۱ Polymorphic
۲ Payload
۳ Command and Control - C&C

مـراحـل کـار



در اکثر نسخه‌ها به‌محض آلوده شدن یک دستگاه به Sality فایل مخرب اصلی با پسوندهای DLL و _DL در پوشه سیستمی Windows با نام‌هایی نظیر نمونه‌های زیر کپی می‌شود:

- %WinDir%\System32\wmdrtc32.dll
- %WinDir%\System32\wmdrtc32.dl_

فایل DLL شامل مجموعه کد بدافزار است. فایل با پسوند _DL نیز نسخه‌ای فشرده شده از همان مجموعه کد است.

در نسخه‌های جدیدتر Sality، بجای ذخیره فایل DLL بر روی دیسک، کد مخرب مستقیما در حافظه فراخوانی و اجرا می‌شود. بدین‌منظور یک راه‌انداز[1] با نامی تصادفی در مسیر %WinDir%\System32\drivers و عملکرد روت‌کیتی ایجاد می‌شود. روت‌کیت مذکور خود را راه‌انداز دستگاهی مجازی با یکی از نام‌های زیر معرفی می‌کند:

- Device\amsint32
- \DosDevices\amsint32

این روت‌کیت دو وظیفه برعهده دارد. اول، متوقف کردن پروسه‌ها در صورتی که تابع TerminateProcess() قادر به انجام آن نباشد. دوم، راه‌اندازی یک تابع بازخوانی[2] با نام IpFilter که کار آن پردازش بسته‌های شبکه‌ای است. Ipfltdrv.sys یک راه‌انداز استاندارد سیستم عامل Windows است که می‌تواند توسط سرویس IpFilterDriver شروع به کار کند. راه‌انداز قادر است تا یک تابع بازخوانی را در هر زمان که یک بسته IP وارد یا خارج می‌شود صدا کرده و در خصوص مسدوسازی بسته یا اجازه عبور دادن به آن تصمیم‌گیری کند. به‌عبارت دیگر، Sality از IpFilter به‌عنوان یک دیواره آتش ساده بهره می‌گیرد تا بدین‌ترتیب هر بسته IP که شامل کلماتی مطابق با فهرست زیر (محصولات امنیتی) است را مسدود کند:

- agnmitum.
- bitdefender.
- cureit.
- drweb.
- eset.com
- etrust.com
- ewido.
- f-secure.
- kaspersky
- mcafee.
- onlinescan.
- pandasoftware.
- sality-remov
- sophos.
- spywareguide.
- spywareinfo.
- symantec
- trendmicro.
- upload_virus
- virusinfo.
- virusscan.
- virustotal.
- windowsecurity.

همچنین از همین طریق قادر است بسته‌های مربوط به ارتباطات SMTP را از کار انداخته و عملات تبادلات ایمیلی را متوقف کند.

Sality فایل‌های EXE و SCR موجود بر روی سیستم را به خود آلوده می‌کند.

این بدافزار می‌تواند فایل‌های اجرایی ذخیره شده بر روی پوشه‌های اشتراکی قابل دسترس بر روی شبکه و درایوهای موسوم به Map شده را نیز آلوده کند.

ضمن اینکه کد مخرب را در فایل‌هایی که در مسیر زیر در محضرخانه به آنها اشاره شده تزریق می‌کند:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\ShellNoRoam\MUICache

مسیر مذکور به فایل‌هایی اشاره دارد که بیشترین اجرا را بر روی سیستم داشته‌اند.

فایل‌های EXE اشاره شده در مسیرهای زیر نیز از گزند Sality ایمن نیستند:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

[1] Driver
[2] Callback

به‌منظور جلوگیری از بروز اشکال در فرایند راه‌اندازی شدن دستگاه، Sality از دست‌درازی به فایل‌های EXE و SCR در هر مسیری که در آن یکی از کلمات زیر استفاده شده پرهیز می‌کند:

- WINDOWS
- SYSTEM
- SYSTEM32

همچنین برای کاهش حساسیت، Sality از آلوده کردن فایل‌های با هر یک از مشخصه‌های زیر خودداری می‌کند:

- فایل‌های حفاظت شده توسط بخش System File Checker – به اختصار SFC – در سیستم عامل Windows
- فایل‌های متعلق به برخی محصولات ضدویروس / دیواره آتش

چنانچه فایل شناسایی شده به یک نرم‌افزار امنیتی (فهرست زیر) تعلق داشته باشد بجای آلوده‌سازی، بخش نقطه شروع[1] آن با بایت‌های CC C3 CC C3 CC C3 CC C3 جایگزین می‌گردد تا از این طریق فایل دچار اشکال شود.

- AVPM.
- A2GUARD
- A2CMD.
- A2SERVICE.
- A2FREE
- AVAST
- ADVCHK.
- AGB.
- AKRNL.
- AHPROCMONSERVER.
- AIRDEFENSE
- ALERTSVC
- AVIRA
- AMON.
- TROJAN.
- AVZ.
- ANTIVIR
- APVXDWIN.
- ARMOR2NET.
- ASHAVAST.
- ASHDISP.
- ASHENHCD.
- ASHMAISV.
- ASHPOPWZ.
- ASHSERV.
- ASHSIMPL.
- ASHSKPCK.
- ASHWEBSV.
- ASWUPDSV.
- ASWSCAN
- AVCIMAN.
- AVCONSOL.
- AVENGINE.
- AVESVC.
- AVEVAL.
- AVEVL32.
- AVGAM
- AVGCC.AVGCHSVX.
- AVGCSRVX.
- AVGNSX.
- AVGCC32.
- AVGCTRL.
- AVGEMC.
- AVGFWSRV.
- AVGNT.
- AVCENTER
- AVGNTMGR
- AVGSERV.
- AVGTRAY.
- AVGUARD.
- AVGUPSVC.
- AVGWDSVC.
- AVINITNT.
- AVKSERV.
- AVKSERVICE.
- AVKWCTL.
- AVP.
- AVP32.
- AVPCC.
- AVAST
- AVSERVER.
- AVSCHED32.
- AVSYNMGR.
- AVWUPD32.
- AVWUPSRV.
- AVXMONITOR
- AVXQUAR.
- BDSWITCH.
- BLACKD.
- BLACKICE.
- CAFIX.
- BITDEFENDER
- CCEVTMGR.
- CFP.
- CFPCONFIG.
- CCSETMGR.
- CFIAUDIT.
- CLAMTRAY.
- CLAMWIN.
- CUREIT
- DEFWATCH.
- DRVIRUS.
- DRWADINS.
- DRWEB
- DEFENDERDAEMON
- DWEBLLIO
- DWEBIO
- ESCANH95.
- ESCANHNT.
- EWIDOCTRL.

[1] Entry-point

- EZANTIVIRUSREGISTRA-TIONCHECK.
- F-AGNT95.
- FAMEH32.
- FILEMON
- FIREWALL
- FORTICLIENT
- FORTITRAY.
- FORTISCAN
- FPAVSERVER.
- FPROTTRAY.
- FPWIN.
- FRESHCLAM.
- EKRN.
- FSAV32.
- FSAVGUI.
- FSBWSYS.
- F-SCHED.
- FSDFWD.
- FSGK32.
- FSGK32ST.
- FSGUIEXE.
- FSMA32.
- FSMB32.
- FSPEX.
- FSSM32.
- F-STOPW.
- GCASDTSERV.
- GCASSERV.
- GIANTANTISPYWARE
- GUARDGUI.
- GUARDNT.
- GUARDXSERVICE.
- GUARDXKICKOFF.
- HREGMON.
- HRRES.
- HSOCKPE.
- HUPDATE.
- IAMAPP.
- IAMSERV.
- ICLOAD95.
- ICLOADNT.
- ICMON.
- ICSSUPPNT.
- ICSUPP95.
- ICSUPPNT.
- IPTRAY.
- INETUPD.
- INOCIT.
- INORPC.
- INORT.
- INOTASK.
- INOUPTNG.
- IOMON98.
- ISAFE.
- ISATRAY.
- KAV.
- KAVMM.
- KAVPF.
- KAVPFW.
- KAVSTART.
- KAVSVC.
- KAVSVCUI.
- KMAILMON.
- MAMUTU
- MCAGENT.
- MCMNHDLR.
- MCREGWIZ.
- MCUPDATE.
- MCVSSHLD.
- MINILOG.
- MYAGTSVC.
- MYAGTTRY.
- NAVAPSVC.
- NAVAPW32.
- NAVLU32.
- NAVW32.
- NEOWATCHLOG.
- NEOWATCHTRAY.
- NISSERV
- NISUM.
- NMAIN.
- NOD32
- NORMIST.
- NOTSTART.
- NPAVTRAY.
- NPFMNTOR.
- NPFMSG.
- NPROTECT.
- NSCHED32.
- NSMDTR.
- NSSSERV.
- NSSTRAY.
- NTRTSCAN.
- NTOS.
- NTXCONFIG.
- NUPGRADE.
- NVCOD.
- NVCTE.
- NVCUT.
- NWSERVICE.
- OFCPFWSVC.
- OUTPOST
- ONLINENT.
- OPSSVC.
- OP_MON.
- PAVFIRES.
- PAVFNSVR.
- PAVKRE.
- PAVPROT.
- PAVPROXY.
- PAVPRSRV.
- PAVSRV51.
- PAVSS.
- PCCGUIDE.
- PCCIOMON.
- PCCNTMON.
- PCCPFW.
- PCCTLCOM.
- PCTAV.
- PERSFW.

- PERTSK.
- PERVAC.
- PESTPATROL
- PNMSRV.
- PREVSRV.
- PREVX
- PSIMSVC.
- QUHLPSVC.
- QHONLINE.
- QHONSVC.
- QHWSCSVC.
- QHSET.
- RFWMAIN.
- RTVSCAN.
- RTVSCN95.
- SALITY
- SAPISSVC.
- SCANWSCS.
- SAVADMINSERVICE.
- SAVMAIN.
- SAVPROGRESS.
- SAVSCAN.
- SCANNINGPROCESS.
- SDRA64.
- SDHELP.
- SHSTAT.
- SITECLI.
- SPBBCSVC.
- SPHINX.
- SPIDERCPL.
- SPIDERML.
- SPIDERNT.
- SPIDERUI.
- SPYBOTSD.
- SPYXX.
- SS3EDIT.
- STOPSIGNAV.
- SWAGENT.
- SWDOCTOR.
- SWNETSUP.
- SYMLCSVC.
- SYMPROXYSVC.
- SYMSPORT.
- SYMWSC.
- SYNMGR.
- TAUMON.
- TBMON.
- TMLISTEN.
- TMNTSRV.
- TMPROXY.
- TNBUTIL.
- TRJSCAN.
- VBA32ECM.
- VBA32IFS.
- VBA32LDR.
- VBA32PP3.
- VBSNTW.
- VCRMON.
- VPTRAY.
- VRFWSVC.
- VRMONNT.
- VRMONSVC.
- VRRW32.
- VSECOMR.
- VSHWIN32.
- VSMON.
- VSSERV.
- VSSTAT.
- WATCHDOG.
- WEBSCANX.
- WINSSNOTIFY.
- WRCTRL.
- XCOMMSVR.
- ZLCLIENT
- ZONEALARM

اگر فرایند جایگزینی با شکست روبرو شد Sality اقدام به حذف فایل می‌کند.

همچنین بدافزار با جستجویی بازگشتی[1] اقدام به حذف فایل‌های با هر یک از پسوندهای زیر که توسط بخش به‌روزرسانی برخی ضدویروس‌ها مورد استفاده قرار می‌گیرند می‌کند:

- .avc
- .key
- .trj
- .vdb

در بعضی نمونه‌ها، فراخوانی System Service Descriptor Table – به اختصار SSDT – که معمولا توسط محصولات ضدویروس انجام می‌شود غیرفعال می‌گردد.

[1] Recursive

از دیگر خرابکاری‌های Sality حذف سرویس‌های با هر یک از نام‌های زیر است:

- AVP
- 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 Web-Guard
- Avira AntiVir Premium Mail-Guard
- 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
- fsbwsys
- FSDFWD
- F-Secure Gatekeeper Handler Starter
- FSMA
- Google Online Services
- InoRPC
- InoRT
- InoTask
- ISSVC
- KPF4
- KLIF
- LavasoftFirewall
- LIVESRV
- McAfeeFramework
- McShield
- McTaskManager
- MpsSvc
- navapsvc
- NOD32krn
- NPFMntor
- NSCService
- Outpost Firewall main module
- OutpostFirewall
- PAVFIRES
- PAVFNSVR
- PavProt
- PavPrSrv
- PAVSRV
- PcCtlCom
- PersonalFirewal
- PREVSRV
- ProtoPort Firewall service
- PSIMSVC
- RapApp
- SharedAccess
- 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
- UmxAgent
- UmxCfg
- UmxLU
- UmxPol
- vsmon
- VSSERV
- WebrootDesktopFirewallData-Service
- WebrootFirewall
- wscsvc
- XCOMM

Sality ممکن است به‌نحوی به محضرخانه دست‌درازی کند که تنظیمات امنیتی Windows به‌شدت نزول یابد. برای این منظور تغییرات زیر در محضرخانه اعمال می‌شود.

- غیرفعال کردن بخش User Account Control:

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
EnableLUA = 0

- دست‌درازی به دیواره آتش برای مجاز تلقی شدن ارتباطات اینترنتی Sality:

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\Authorized-Applications\List
<Win32/Sality file name> = <Win32/Sality file name>:*:enabled:ipse

- متوقف کردن دیواره آتش:

HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
EnableFirewall = 0

- تغییر مسیر رویدادهای netsh:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Tracing\Microsoft\NAP\Netsh
LogSessionName = stdout

- غیرفعال کردن قابلیت مشاهده وضعیت ضدویروس نصب شده در بخش Microsoft Security Center:

HKLM\SOFTWARE\Microsoft\Security Center | HKLM\SOFTWARE\Microsoft\Security Center\Svc
AntiVirusOverride = 1

- غیرفعال کردن قابلیت نمایش هشدارهای امنیتی در بخش Microsoft Security Center:

HKLM\SOFTWARE\Microsoft\Security Center | HKLM\SOFTWARE\Microsoft\Security Center\Svc
FirewallDisableNotify | UacDisableNotify | UpdatesDisableNotify =1

- از کارانداختن بخش Windows Task Manager:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
DisableTaskMgr = 1

- خاموش کردن قابلیت Offline Mode در مرورگر Internet Explorer:

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
GlobalUserOffline = 0

- بازگردانی تنظیمات گزینه Show hidden files:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
Hidden = 2

- مسدود کردن Registry Editing Tools:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
DisableRegistryTools = 1

Sality تمامی مقادیر و داده‌های ذخیره شده در مسیرهای زیر در محضرخانه را حذف می‌کند تا از راه‌اندازی شدن Windows در حالت Safe Mode جلوگیری شود:

- HKCU\System\CurrentControlSet\Control\SafeBoot
- HKLM\System\CurrentControlSet\Control\SafeBoot

در بعضی نمونه‌ها، Sality با جستجوی فایل‌های موسوم به دفترچه نشانی‌ها[۱] نشانی‌های ایمیل را استخراج کرده و در ادامه اقدام به ارسال هرزنامه[۲] به آنها می‌کند.

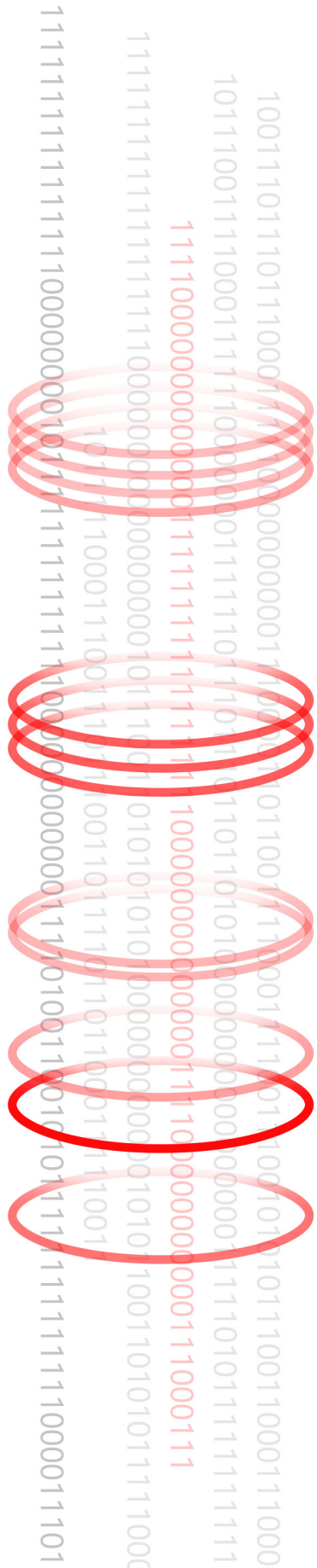
برخی نسخه‌های Sality نیز قادر به سرقت داده‌های حساسی همچون داده‌های شخصی، داده‌های مالی و به طور کلی کلیدهای فشرده شده توسط کاربر نیز هستند.

ارسال ترافیک در قالب پراکسی‌های HTTP، رخنه به سایت‌های تحت وب و مشارکت در عملیات توزیع شده نظیر کشف رمز عبور[۳] از دیگر قابلیت‌هایی است که مهاجمان در برخی نسخه‌های این بدافزار از آنها بهره گرفته‌اند.

اکثر کدهای Sality در بستر پروسه‌های دیگر اجرا می شوند که این موضوع ضمن دشوار کردن فرایند پاکسازی عبور آنها از سد دیواره‌های آتش را نیز تسهیل می‌کند.

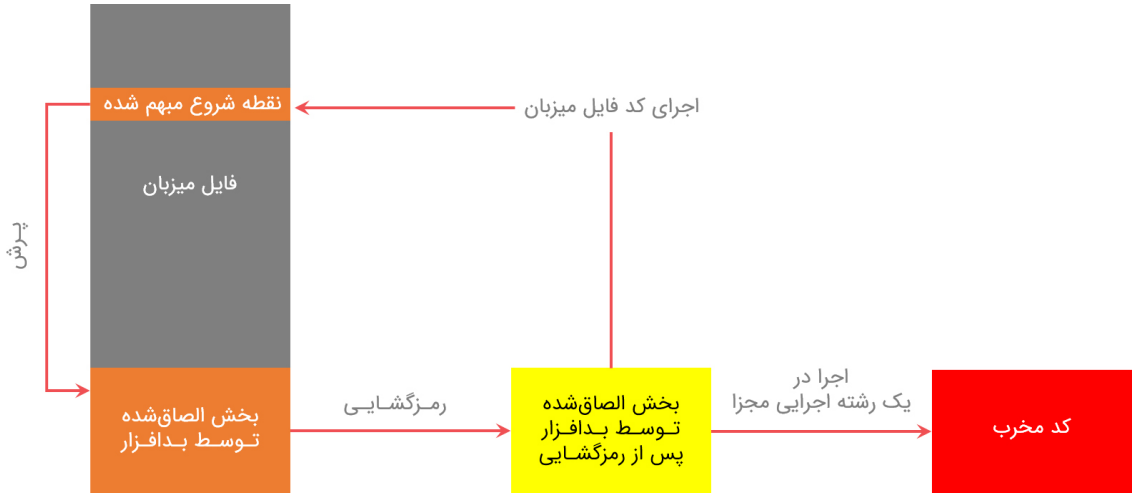
۱ Address Book
۲ Spam
۳ Password Cracking

دسـت‌درازی بـه فـایـل



آلوده‌سازی فایل‌های اجرایی سالم (فایل‌های میزبان) توسط Sality در مراحل زیر انجام می‌شود:

- کد مخرب به‌صورت رمزگذاری شده و چندشکلی به انتهای فایل افزوده می‌شود.
- اگرچه نشانی نقطه شروع کدهای فایل میزبان بدون تغییر باقی می‌ماند اما کد بخشی که نشانی به آن تعلق دارد توسط بدافزار جایگزین می‌شود.
- کد مذکور روند اجرا را به بخشی که در انتهای فایل اضافه شده منتقل می‌کند.
- کد پس از رمزگشایی شدن در یک رشته اجرایی[1] مجزا اجرا می‌شود. در صورتی که نمونه دیگری از Sality بر روی سیستم در حال اجرا باشد این کد اجرای خود را موقتا متوقف کرده و در انتظار می‌ماند.
- همزمان با مرحله قبل کدی که در مرحله دوم جایگزین شده بود بازگردانی شده و روند عادی اجرای فایل ادامه می‌یابد.

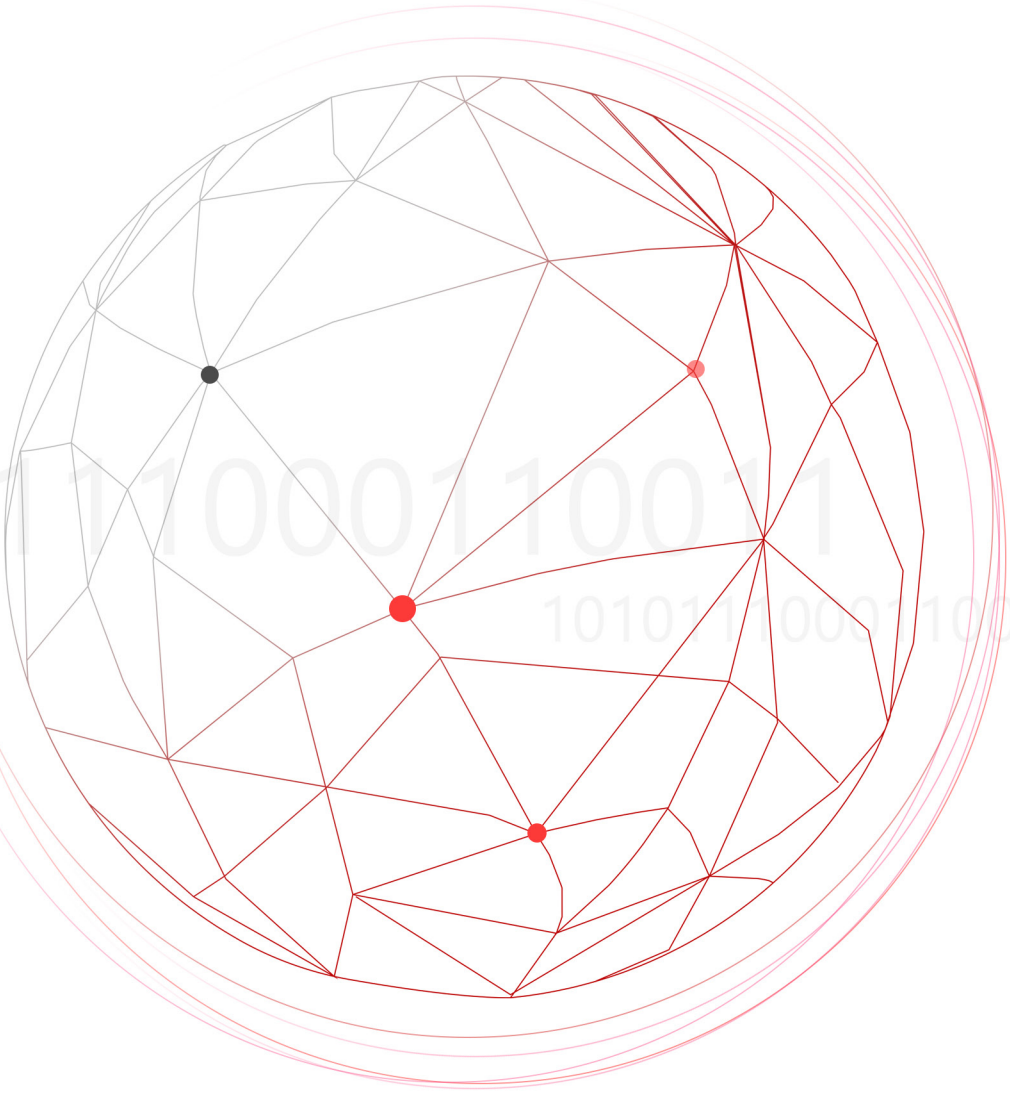


نحوه آلوده‌سازی فایلی سالم توسط Sality

روشی که توسط Sality در آدرس‌دهی مورد استفاده می‌گیرد نقطه شروع مبهم‌سازی شده[2] نام دارد که هدف آن مخفی‌سازی بخش مخرب فایل از دید محصولات امنیتی است. برخی بدافزارها نیز از این تکنیک برای به تأخیر انداختن اجرای کد مخرب - و نه اجرا به‌محض اجرای فایل سالم - بهره می‌گیرند.

[1] Thread
[2] Entry Point Obscuring

شبکه‌های مخرب



نویسندگان این بدافزار در مجموع اقدام به راه‌اندازی چهار شبکه مخرب[۱] که به شبکه‌های ۱، ۲، ۳ و ٤ معروف شده‌اند کردند. دو شبکه مخرب نخست عمر نسبتا کوتاهی داشتند؛ اما شبکه‌های ۳ و ٤ به‌ترتیب از سال‌های ۱۳۸۸ و ۱۳۸۹ فعال بوده و همچنان نیز دستگاه‌های تسخیر شده‌ای از آنها در حال فعالیت هستند.

پودمان ارتباطی این شبکه‌ها، نقطه‌به‌نقطه[۲] و در بستر UDP است.

استفاده از این پودمان ساده بوده و احتمالا توسط خود مهاجمان توسعه داده شده است.

بسته‌های تبادل شده در این ارتباطات با کلیدی با مقدار پویا توسط RC4 رمزگذاری شده‌اند.

هر فایل آلوده به Sality حاوی فهرستی یک‌هزارتایی از دستگاه‌های موسوم به جفت[۳] است. در Sality مکانیزمی نیز برای به‌روزرسانی فهرست جفت‌ها در نظر گرفته شده است.

بدافزار از روی دستگاهی که آن را به Sality آلوده کرده تلاش می‌کند تا به یکی از این جفت‌ها متصل شود. هدف از این کار تبادل نشانی‌های URL است که Sality باید با استفاده از آنها بدافزارها / کدهای مخرب مهاجمان را دریافت و سپس در ادامه آنها را اجرا کند.

Sality، این بدافزارها / کدهای مخرب را پس از دریافت در پوشه موسوم به Windows Temporary Files ذخیره کرده و در ادامه توسط یکی از رمزهای عبوری که در کد بدافزار تزریق شده رمزگشایی می‌کند. دو نمونه از این رمزهای عبور به‌شرح زیر است:

- GdiPlus.dll
- kukutrusted!.

نکته قابل توجه عدم وجود گواهینامه[٤] برای این فایل‌هاست. بنابراین هر کس قادر است تا با رمزگذاری فایلی اجرایی و قرار دادن آنها در این نشانی‌های URL موجب اجرای آن بر روی دستگاه‌های آلوده شده شود.

پودمان نقطه‌به‌نقطه در شبکه مخرب Sality از چند فرمان پشتیبانی می‌کند که بااهمیت‌ترین آنها به‌شرح زیر است:

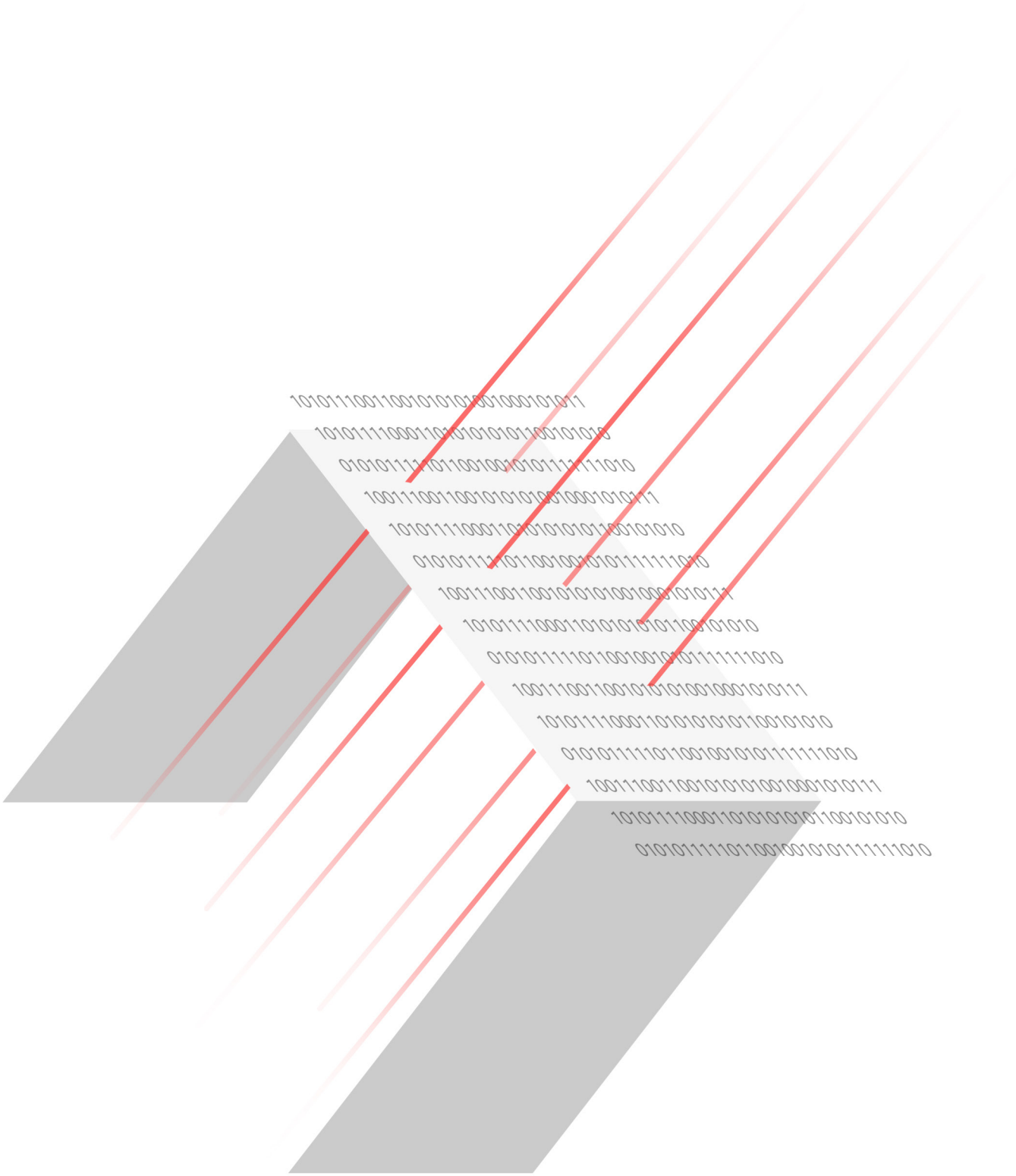
- درخواست از جفت برای ارسال فهرست نشانی‌های URL
- ارسال فهرست نشانی‌های URL به جفت
- درخواست از جفت برای ارسال نشانی IP و درگاه جفت دیگر در شبکه مخرب با هدف به‌روز نگاه داشتن فهرست جفت‌ها

هر فهرست نشانی‌های URL حاوی فراداده‌هایی[٥] همچون شماره توالی[٦] است. دستگاه آلوده تنها فهرست‌هایی را از جفت قبول می‌کند که شماره توالی آن بزرگ‌تر از شماره توالی فهرستی باشد که در حال حاضر در اختیار دارد. در غیر این صورت، این، دستگاه آلوده است که فهرست نشانی‌های URL خود را به جفت ارسال می‌کند.

در شبکه‌های مخرب ۱، ۲ و ۳ فهرست‌ها به‌صورت دیجیتالی با الگوریتم RSA با طول ۱۰۲٤ بیت امضا شده‌اند تا به این ترتیب فهرست‌های غیرمعتبر – از دید نویسندگان Sality – قابل تزریق به شبکه نبوده و یا شبکه به تسخیر مهاجمان دیگر در نیاید. در شبکه مخرب شماره ٤، رمزگذاری RSA با طول ۲۰٤۸ بیت به‌کار گرفته شده است.

۱ Botnet
۲ Peer-to-peer - P2P
۳ Peer
٤ Certificate
٥ Metadata
٦ Sequence

روش‌های انتشار



Sality از روش‌های مختلفی برای توزیع بر روی سیستم‌های دیگر استفاده می‌کند که در ادامه این بخش به آنها پرداخته شده است.

آلوده‌سازی فایل

همان‌طور که اشاره شد فایل‌های با هر یک از پسوندهای EXE و SCR از اهداف بدافزار Sality هستند. با توجه به افزوده شدن کد مخرب به فایل‌های آلوده شده عملا سایز آنها با نسخه اولیه تفاوت دارد. اندازه کد مخرب در نسخه‌های مختلف آن متفاوت می‌باشد. اجرای هر فایل حاوی کد مخرب بر روی سیستم‌های دیگر منجر به آلوده شدن آنها به Sality می‌گردد.

حافظه‌های جداشدنی و پوشه‌های اشتراکی

برخی نسخه‌ها از Sality قادر به آلوده‌سازی فایل‌های معتبر ذخیره شده بر روی حافظه های جداشدنی و پوشه های اشتراکی هستند. در صورت وجود فایلی معتبر در این مسیرها، بدافزار فایل را در پوشه‌ای موقت کپی کرده و در ادامه آن را آلوده می‌کند. سپس، فایل آلوده شده در ریشه تمامی حافظه‌های جداشدنی متصل به دستگاه و تمامی پوشه‌های اشتراکی با یکی از پسوندهای زیر کپی می‌شود:

- \<random file name>.pif
- \<random file name>.exe
- \<random file name>.cmd

در صورت عدم وجود فایل اجرایی معتبر، بدافزار نسخه‌ای آلوده شده از فایل‌های زیر را در مسیرهای مذکور کپی می‌کند:

- %SYSTEM%\NOTEPAD.EXE
- %SYSTEM%\WINMINE.EXE
- %SYSTEM%\TELNET.EXE

در ریشه این درایوها یک فایل autorun.inf که در آن به مسیر و فایل بدافزار اشاره شده کپی می‌شود. در نسخه‌های قدیمی Windows، هر زمان که یکی از این درایوها توسط کاربر مورد دسترسی قرار می‌گیرد، autorun.inf فایل اشاره شده در خود را به‌طور خودکار بر روی دستگاه اجرا می‌نماید.

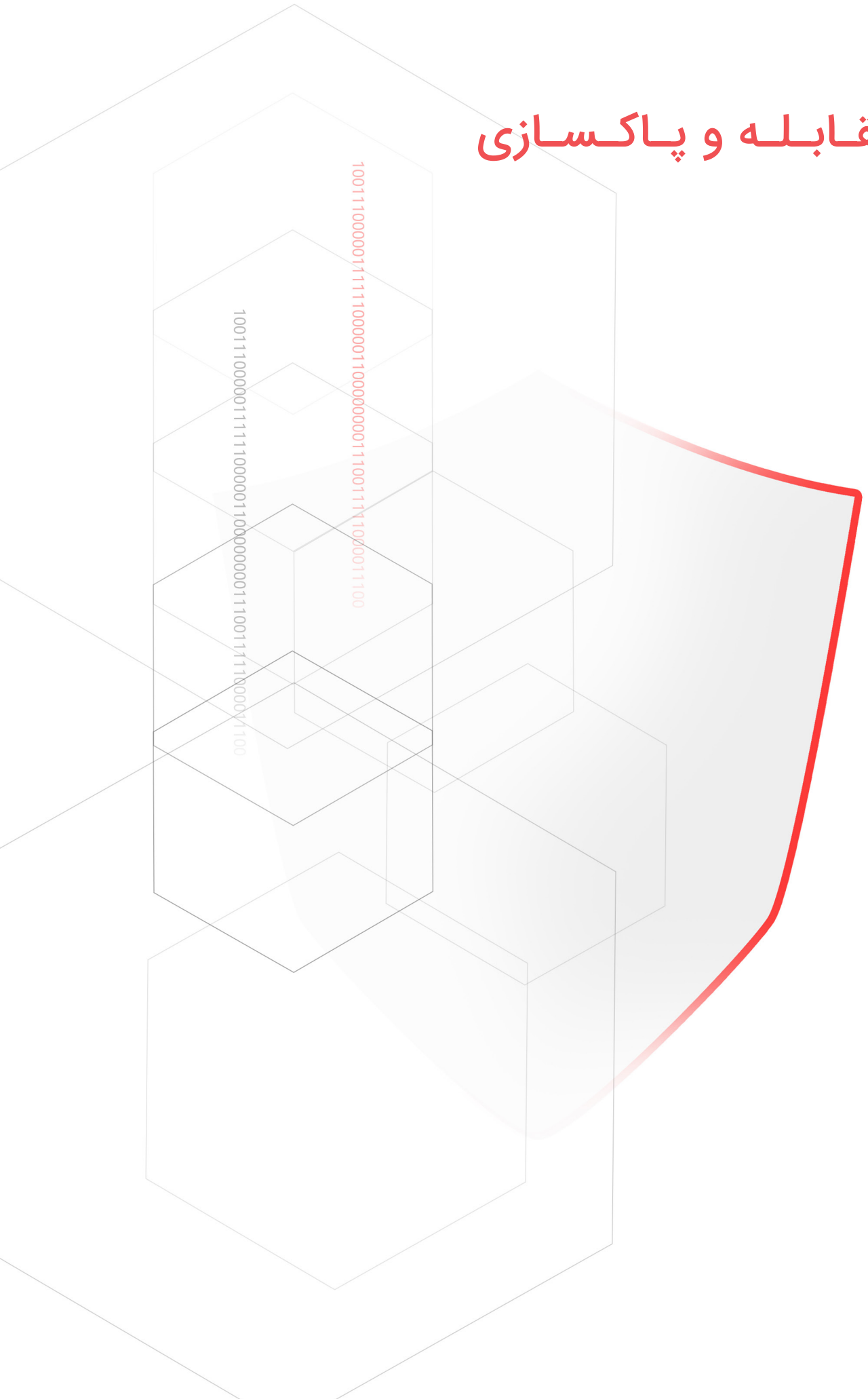
برخی از نسخه‌های Sality ممکن است فایلی با پسوند tmp را به همراه فایلی LNK که به فایل نخست اشاره دارد را نیز در پوشه‌های اشتراکی و منابع شناسایی شده کپی می‌کنند.

بهره‌جویی از آسیب‌پذیری‌های امنیتی

در نمونه‌هایی از Sality، مهاجمان از بهره‌جوها[1] برای سوءاستفاده از ضعف‌هایی نظیر آسیب‌پذیری حیاتی CVE-2010-2568 در سیستم عامل Windows برای انتشار بدافزار سود برده‌اند. از CVE-2010-2568 در چندین عملیات مخرب استفاده شده که مهمترین آن توسط ویروس Stuxnet است. در مرداد ۱۳۸۹، شرکت مایکروسافت این آسیب‌پذیری را در اصلاحیه MS10-046 ترمیم کرد.

[1] Exploit

مـقـابـلـه و پـاکـسـازی



اصلی ترین راهکار در مقابله با این بدافزار رعایت تمامی موارد زیر است:

- استفاده از ضدویروس قدرتمند و به‌روز
- نصب مستمر و به موقع اصلاحیه‌های امنیتی
- استفاده از رمزهای عبور پیچیده برای تمامی کاربران از جمله کاربران با سطح دسترسی Administrator
- حتی الامکان از ورود به دستگاه با نام کاربری با سطح دسترسی Administrator در سطح دامنه / گروه کاری[1] خودداری شود.
- بکارگیری محصولات موسوم به Device Control بر روی تمامی دستگاه‌ها
- محدودسازی سطوح دسترسی به پوشه‌های اشتراکی و پرهیز از به‌اشتراک‌گذاری فایل‌های اجرایی با سطح دسترسی نوشتن
- غیرفعال کردن قابلیت Autoplay در نسخه‌های قدیمی سیستم عامل Windows با استفاده از راهنمای زیر:
https://support.microsoft.com/en-us/help/967715/how-to-disable-the-autorun-functionality-in-windows

انجام عملیات پویش کامل[2] توسط یک ضدویروس قدرتمند و به‌روز موجب پاکسازی دستگاه از این بدافزار مخرب خواهد شد.

[1] Workgroup
[2] Full Scan

فهرست منابع

- https://community.mcafee.com/t5/Documents/Combating-Threats-W32-Sality-pdf/ta-p/549154?attachment-id=3181
- https://www.mcafee.com/enterprise/en-us/threat-intelligence.malwaretc.html?vid=269241
- https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Sality-H/detailed-analysis.aspx
- https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/sality-story-of-peer-to-peer-11-en.pdf
- https://map.lookingglasscyber.com/
- https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-046
- https://nvd.nist.gov/vuln/detail/CVE-2010-2568
- https://newsroom.shabakeh.net/45/w32sality.html
- https://newsroom.shabakeh.net/10/microsoft-security-updates-ms10-046.html
- https://newsroom.shabakeh.net/15290
- https://newsroom.shabakeh.net/17923
- https://newsroom.shabakeh.net/12847
- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Win32%2FSality
- https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Virus%3AWin32%2F-Sality.AH


آخرین اخبار امنیت فناوری اطلاعات
@SGnewsroom

شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید. در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید. از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه بوده است. ضدویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد. شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه در کشور بوده است. این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

ISO 9001:2008
Cert No 9150.C528

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی (ظفر)، شماره ۲۷۳

تلفن / دورنگار	۰۲۱-۴۲۰۵۲
رایانامه	info@shabakeh.net
تارنمای شرکت	www.shabakeh.net
خدمات پس از فروش و پشتیبانی	my.shabakeh.net
مرکز آموزش	events.shabakeh.net
اتاق خبر	newsroom.shabakeh.net