گزارش فنی تحلیل بدافزار Dofoil با هدف ارسال هرزنامه جهت انجام حملات سرویس توزیع شده (DDOS)

معرفی بدافزار

Dofoil بدافزاری است که عمدتاً برای ارسال هرزنامه، انجام حملات منع سرویس توزیع شده و نیز سرقت اطلاعات ورود مورد استفاده قرار می‌گیرد. این بدافزار معمولاً از طریق فایل‌های الصاق شده به هرزنامه‌ها انتشار می‌یابد. پس از نصب بر روی سیستم، این بدافزار ابتدا دسترسی کاربر به Registry Editor ویندوز را محدود کرده و سپس با اتصال به کارگزارهای کنترل و فرمان خود، دستورات دریافتی را اجرا می‌نماید.

عملکرد اصلی این بدافزار، سرقت اطلاعات کاربر و ارسال آن برای کارگزار کنترل و فرمان است و از آنجا که گسترده و نوع اطلاعات قابل سرقت توسط این بدافزار بسیار گسترده و حساس است، آلودگی به این بدافزار بسیار خطرناک بوده و نیازمند رفع سریع آلودگی و تغییر تمامی گذرواژه‌های کاربر است. اطلاعاتی که توسط این بدافزار قابل سرقت است، شامل تمامی اطاعات ذخیره شده در نرم‌افزارهای زیر و یا نام‌کاربری/گذرواژه ورود به وب‌سایت‌های زیر است:

- Miranda ICQ DB
- Windows Live Mail
- PocoMail
- IncredMail
- Mail.Ru
- Mozilla Thunderbird
- SeaMonkey
- Apple Safari
- Mozilla Firefox
- Internet Explorer
- Opera
- PacificPoker
- PartyPoker
- CakePoker
- TitanPoker
- Gmail
- PokerStarts
- FullTiltPoker
- FlashGet
- JetCar
- Internet Download Accelator
- Download Master
- TotalPhones
- Advanced Dialer
- PySoft Autoconnect
- Flexiblesoft Dialer Lite
- MuxaSoft Dialer
- Trillian

- Abstract Software JAJC
- QIP Online
- Pandion
- AIM Pro
- Pidgin
- Sipphone Gizmo Project
- Excite Private Messenger
- Paltalk
- Windows Live Messenger
- Myspace IM
- Google Talk
- IM2
- Odigo
- GAIM
- AOL Instant Messenger
- Yahoo! Messenger
- MSN Messenger
- Mirabilis ICQ
- CISCO VPN Client
- Camfrog Client
- FreeCall
- PC Remote Control
- Remote Desktop Connection
- WinVNC3
- FTPCON
- South River Technologies WebDrive
- WinSCP
- LeapFTP
- FreeFTP
- DirectFTP
- Day Zero G FTP Uploader
- SoftX FTP Client
- NCH Software Fling
- NCH Software Classic FTP
- ExpanDrive
- BitKinex
- Cryer WebSitePublisher
- FTPRush
- UltraFXP
- VanDyke SecureFX
- Frigate3
- FTP Explorer
- FTPWare CoreFTP
- CoffeeCup
- Sota FFFTP
- TurboFTP
- SmartFTP
- BulletProof FTP Client

- FTP Commander
- FileZilla
- FlashFXP
- CuteFTP
- Ipswitch WS_FTP
- Total Commander
- FAR Manager FTP

نحوه شناسایی سیستم آلوده از طریق لاگ‌های شبکه

برای تشخیص بدافزار Dofoil از طریق لاگ شبکه، دو راه وجود دارد:

راه اول: تمامی میزبان‌هایی که نام‌های دامنه زیر را Resolve کرده‌اند و با آدرس‌های IP متناظر آن‌ها در ارتباط بوده‌اند، احتمالاً آلوده‌اند:

- 01eqyc.com
- 0bv2ga.com
- 123getos.tk
- 3b3estudio.com
- addimgs.com
- aman-shhhids.com
- anub.net
- averaph.com
- bgnt.net
- blpk.net
- bzsx.net
- carsero.com
- demorollz.com
- derj.net
- domialepof.ru
- elit333.net
- feelingmoney.com
- fkhfgfg.tk
- gme.cz.cc
- goodtraff.com
- goodyeartiresisgood.in
- helplinuxnow.tk
- hithere.vv.cc
- hmbpcomanyweb431.com
- hxlb.net
- in-in.in
- interviewbuy.ru
- kaza.cz.cc
- linuxhelpnow.tk
- mailaccaunt1.co.cc
- mailsystem256.co.cc

- megasexf<obfuscated>k.com
- mialedot.ru
- mialepromo.ru
- miminoprost.net
- minakala.com
- msantispam-srv2.com
- myldrpanel.com
- news-banner-net.com
- oemsoftbox.com
- passportu.cn
- phe-phe.com
- plyx.net
- polidoli200.com
- popirosa.tk
- porohh.net
- profmiale.ru
- pytt.net
- sacv.net
- sancan.in
- searchgood.net
- searchnew.net
- ssn-much.com
- suhont.com
- summer-ciprys.com
- system16286.in
- systemupdatewins.in
- teonflex1.tk
- thedomonisterioster.info
- traffic-send-poli.in
- tynv.net
- ventoushd.net
- www.capodeicapi.eu
- www.helplinuxnow.org
- xyxyxy.ru
- yostat100.ru
- zastolbis.ru
- zdesestvareznezahodi.com
- znakomie10.ru

راه دوم (تشخیص کاربرانی که هرزنامه‌های مرتبط با این بدافزار را دریافت نموده‌اند): تمامی کاربرانی که هرزنامه‌ای دریافت نموده‌اند که فایل الصاق شده دارای یکی از نام‌های زیر باشد، در معرض آلودگی قرار دارند:

- New_Password_IN46537.zip
- Invoice_Copy.zip
- Facebook_Password.zip

نحوه بررسی وجود آلودگی

۱. وجود یکی از فایل‌های زیر بر روی سیستم (برای ویندوزهای Vista و جدیدتر):

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Dxdiag.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Lxdiag.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Ctfmon.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Gefreg.exe

۲. وجود یکی از فایل‌های زیر بر روی سیستم (برای ویندوزهای قدیمی‌تر از Vista):

- %USERPROFILE%\Start Menu\Programs\Startup\dxdiag.exe
- %USERPROFILE%\Start Menu\Programs\Startup\lxdiag.exe
- %USERPROFILE%\Start Menu\Programs\Startup\ctfmon.exe
- %USERPROFILE%\Start Menu\Programs\Startup\gefreg.exe

۳. وجود یکی از فایل‌های زیر بر روی سیستم (برای تمامی نسخ ویندوز):

- %SystemDrive%\Documents and Settings\garciaju\Application Data\2EC795.exe
- %USERPROFILE%\Application Data\90434F.exe
- %TEMP%\oskb.exe
- %LOCALAPPDATA%\NetMailTmp.bin
- %APPDATA%\E6CB3B\E6CB3B.exe
- %SystemDrive%\Documents and Settings\hrad.e_aldosuky\Application Data\E3BB7F.exe
- %SystemDrive%\Documents and Settings\Chief\Application Data\9CB732.exe
- %USERPROFILE%\Application Data\16F747.exe
- %TEMP%\Rar$EX46.552\eCalendar 6.5\eCalendar.exe
- %PROGRAMFILES(x86)%\WinApps\msmsgs.exe
- %APPDATA%\61B329\61B329.exe
- %APPDATA%\9A9D63.exe
- %USERPROFILE%\Application Data\E602DF.exe
- D:\Program Files\WirelessNetView 1.38\WirelessNetView.exe
- %USERPROFILE%\Documenti\Downloads\Office.2010.RTM.PreAttivato.ITA.x32-x64.-ATTIVAZION\mini-KMS_Activator_v1.2_Office2010_VL_ENG.exe
- 503186.exe
- AA3DA6.exe

۴. وجود یکی از کلیدهای زیر در رجیستری ویندوز که مقدار مشکوکی داشته باشد:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Microsoft
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\adobe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Classes
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\EPL SHEET

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\FlySky
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Intel
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ Local AppWizard-Generated Applications
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Netscape
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ODBC

۵. وجود دسترسی به نام‌های دامنه ذکر شده

نحوه پاک‌سازی سیستم

۱. حذف فایل‌های زیر از روی سیستم برای ویندوزهای Vista و جدیدتر:

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Dxdiag.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Lxdiag.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Ctfmon.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Gefreg.exe

۲. حذف فایل‌های زیر از روی سیستم برای ویندوزهای قدیمی‌تر از Vista:

- %USERPROFILE%\Start Menu\Programs\Startup\dxdiag.exe
- %USERPROFILE%\Start Menu\Programs\Startup\lxdiag.exe
- %USERPROFILE%\Start Menu\Programs\Startup\ctfmon.exe
- %USERPROFILE%\Start Menu\Programs\Startup\gefreg.exe

۳. حذف فایل‌های زیر از روی سیستم برای تمامی نسخ ویندوز:

- %SystemDrive%\Documents and Settings\garciaju\Application Data\2EC795.exe
- %USERPROFILE%\Application Data\90434F.exe
- %TEMP%\oskb.exe
- %LOCALAPPDATA%\NetMailTmp.bin
- %APPDATA%\E6CB3B\E6CB3B.exe
- %SystemDrive%\Documents and Settings\hrad.e_aldosuky\Application Data\E3BB7F.exe
- %SystemDrive%\Documents and Settings\Chief\Application Data\9CB732.exe
- %USERPROFILE%\Application Data\16F747.exe
- %TEMP%\Rar$EX46.552\eCalendar 6.5\eCalendar.exe
- %PROGRAMFILES(x86)%\WinApps\msmsgs.exe
- %APPDATA%\61B329\61B329.exe
- %APPDATA%\9A9D63.exe
- %USERPROFILE%\Application Data\E602DF.exe
- D:\Program Files\WirelessNetView 1.38\WirelessNetView.exe
- %USERPROFILE%\Documenti\Downloads\Office.2010.RTM.PreAttivato.ITA.x32-x64. -ATTIVAZION\mini-KMS_Activator_v1.2_Office2010_VL_ENG.exe
- 503186.exe

- AA3DA6.exe

۴. حذف کلیدهای زیر در رجیستری ویندوز که مقدار مشکوکی داشته باشد:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Microsoft
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\adobe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Classes
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\EPL SHEET
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\FlySky
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Intel
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ Local AppWizard-Generated Applications
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Netscape
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ODBC

۵. مسدودسازی دسترسی به نام‌های دامنه ذکر شده

۶. راه‌اندازی مجدد سیستم

نحوه اطمینان یافتن از پاک بودن سیستم

۱. نبود هیچ یک از فایل‌های زیر بر روی سیستم برای ویندوزهای Vista و جدیدتر:

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Dxdiag.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Lxdiag.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Ctfmon.exe
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Gefreg.exe
-

۲. نبود هیچ‌یک از فایل‌های زیر بر روی سیستم برای ویندوزهای قدیمی‌تر از Vista:

- %USERPROFILE%\Start Menu\Programs\Startup\dxdiag.exe
- %USERPROFILE%\Start Menu\Programs\Startup\lxdiag.exe
- %USERPROFILE%\Start Menu\Programs\Startup\ctfmon.exe
- %USERPROFILE%\Start Menu\Programs\Startup\gefreg.exe

۳. نبود هیچ‌یک از فایل‌های زیر بر روی سیستم برای تمامی نسخ ویندوز:

- %SystemDrive%\Documents and Settings\garciaju\Application Data\2EC795.exe
- %USERPROFILE%\Application Data\90434F.exe
- %TEMP%\oskb.exe

- %LOCALAPPDATA%\NetMailTmp.bin
- %APPDATA%\E6CB3B\E6CB3B.exe
- %SystemDrive%\Documents and Settings\hrad.e_aldosuky\Application Data\E3BB7F.exe
- %SystemDrive%\Documents and Settings\Chief\Application Data\9CB732.exe
- %USERPROFILE%\Application Data\16F747.exe
- %TEMP%\Rar$EX46.552\eCalendar 6.5\eCalendar.exe
- %PROGRAMFILES(x86)%\WinApps\msmsgs.exe
- %APPDATA%\61B329\61B329.exe
- %APPDATA%\9A9D63.exe
- %USERPROFILE%\Application Data\E602DF.exe
- D:\Program Files\WirelessNetView 1.38\WirelessNetView.exe
- %USERPROFILE%\Documenti\Downloads\Office.2010.RTM.PreAttivato.ITA.x32- x64. - ATTIVAZION\mini-KMS_Activator_v1.2_Office2010_VL_ENG.exe
- 503186.exe
- AA3DA6.exe

۴. نبود کلیدهای زیر در رجیستری ویندوز که مقدار مشکوکی داشته باشد:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Microsoft
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Policies
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\adobe
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Classes
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\EPL SHEET
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\FlySky
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Intel
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ Local AppWizard-Generated Applications
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\Netscape
- HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ODBC

۵. نبود دسترسی به نام‌های دامنه ذکر شده

توصیه‌های امنیتی برای پیش‌گیری

۱. خودداری از باز نمودن ایمیل‌های ناشناس
۲. خودداری از باز نمودن فایل‌های الصاق شده به ایمیل‌های ناشناس
۳. عدم استفاده از کرک‌های نامعتبر برای نرم‌افزارها
۴. مسدودسازی دسترسی به نام‌های دامنه ذکر شده
۵. استفاده از یک کاربر با دسترسی محدود برای انجام امور روزانه
۶. عدم ذخیرسازی گذرواژه‌های حساس بر روی نرم‌افزارها