گزارش تحلیل بدافزار Dofoil

۱. 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.

۲. مشخصات فایل تحلیل شده

فایل تحلیل شده، یک فایل DLL ویندوز با مشخصات زیر است که از طریق Dropper اصلی در یکی از پروسه‌های اصلی ویندوز تزریق می‌شود:

MD5	C1E367461A2D2AF7317B9BF88A86800E
SHA1	DE8343F1426721524AA58A12F3AC1B2BEF3F7501
File Size	1,134,040 bytes
File Type	Win32 DLL
Magic Literal	PE32 executable for MS Windows (GUI) Intel 80386 32-bit

۳. فرآیند آلوده‌سازی

معمولاً آلوده شدن به این بدافزار از طریق هرزنامه‌ها اتفاق می‌افتد. هرزنامه‌هایی که برای کاربر ارسال می‌شود، معمولاً خود را از سوی شرکت Americal Airlines نشان می‌دهند و فایل‌های الصاقی به آن‌ها، اسامی مانند New_Password_IN46537.zip، Invoice_Copy.zip و یا Facebook_Password.zip دارند.

در صورتی که کاربر فایل الصاقی به این هرزنامه را باز کند، Dropper بدافزار Dofoil اجرا شده و DLL اصلی خود را در یکی از پروسه‌های اصلی ویندوز تزریق می‌نماید. این DLL با سرقت اطلاعات حساب‌های کاربری قربانی، آن‌ها را برای کارگزار کنترل و فرمان خود ارسال می‌کند و مجرمین و گردانندگان Dofoil از این اطلاعات سرقت شده برای ارسال هرزنامه‌های بیشتر و آلوده‌سازی سیستم‌های بیشتر استفاده می‌نمایند.

۴. شرح تحلیل

پس از آن‌که فرد قربانی فایل الصاق شده به هرزنامه دریافتی را اجرا نمود، Dropper بدافزار Dofoil شروع به کار می‌کند. کد اجرایی اصلی بدافزار در قالب یک فایل DLL رمزنگاری شده درون فایل Dropper ذخیره‌سازی شده است. پس از اجرا، Dropper ابتدا فایل DLL اصلی را رمزگشایی کرده و سپس یک نمونه جدید از پروسه svchost.exe بر روی سیستم ایجاد می‌نماید.

در مرحله بعد، با استفاده از عملیاتی که به اصطلاح Process Hollowing نامیده می‌شود، Dropper تمامی فضای حافظه پروسه‌ی svchost.exe ایجاد شده خود را پاک کرده و کد اجرایی DLL خود را به‌جای آن می‌نویسد. در نهایت نیز Dropper با فراخوان سیستم ResumeThread سبب می‌شود کد اجرایی خود در درون پروسه‌ای با نام svchost.exe شروع به اجرا کند که عملکرد اصلی بدافزار را به انجام می‌رساند.

عملکردهای اصلی بدافزار به سه دسته عمده تقسیم‌بندی می‌شوند که عبارتند از:

- تثبیت پایداری بر روی سیستم
- سرقت اطلاعات حساب‌های کاربری قربانی
- تشخیص محیط مجازی و تشخیص Debug
- اتصال به کارگزار کنترل و فرمان به منظور ارسال اطلاعات سرقت شده و دریافت فرامین

در ادامه موارد فوق با تفصیل بیشتر شرح داده خواهند شد.

۱. تثبیت پایداری بر روی سیستم

به منظور تثبیت پایداری بدافزار بر روی سیستم پس از راه‌اندازی مجدد، بدافزار یک نسخه از فایل Dropper خود را در مسیر Startup Folder ویندوز کپی می‌کند. Startup Folder مسیری در ویندوز است که فایل‌های موجود در آن به صورت خودکار توسط ویندوز در زمان راه‌اندازی سیستم اجرا می‌شوند. مسیر این فولدر در ویندوزهای 98، ME، 2000، XP و 2003 به شرح زیر است:

%USERPROFILE%\Start Menu\Programs\Startup

در نسخ جدیدتر ویندوز این فولدر در مسیر زیر قرار دارد:

%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

نام فایل کپی شده در نسخه‌های مختلف بدافزار متفاوت است. برخی از نام‌های مشاهده شده عبارتند از:

- Dxdiag.exe
- Lxdiag.exe
- Ctfmon.exe
- Gefreg.exe

بنابراین در صورتی که فایلی با یکی از نام‌های فوق در مسیر Startup Folder ویندوز وجود داشته باشد، احتمال آلوده بودن سیستم زیاد است. همچنین برخی دیگر از نسخه‌های این بدافزار فایل Dropper خود را با نام یکی از فایل‌های اصلی ویندوز مانند csrss.exe و یا smss.exe در مسیر %appdata% کپی می‌کنند. پس از آن یکی از کلیدهای زیر به منظور اجرای فایل‌های کپی شده پس از هربار راه‌اندازی مجدد ویندوز به رجیستری ویندوز اضافه می‌شوند:

- 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

توجه شود که در تمامی موارد فوق، مقدار تعیین شده برای کلید اضافه شده، مسیر فایل کپی شده در %appdata% می‌باشد که منجر به اجرا شدن فایل فوق پس از راه‌اندازی مجدد سیستم می‌شود.

برخی دیگر از نمونه مسیرها و نام‌فایل‌هایی که نمونه‌های دیگر مشاهده شده از بدافزار برای ذخیره‌سازی Dropper خود و یا سایر فایل‌های اجرایی بارگذاری شده استفاده می‌کنند عبارتند از:

- %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

بنابراین وجود هر یک از فایل‌های فوق بر روی سیستم می‌تواند نشانه‌ای از آلودگی سیستم باشد و بایستی مورد بررسی قرار گیرد.

۲. سرقت اطلاعات حساب‌های کاربری قربانی

عملکرد اصلی نمونه تحلیل شده، سرقت اطلاعات حساب‌های کاربری قربانی است. بدین صورت که بدافزار از مسیر پیش‌فرض نصب نرم‌افزارهایی آگاه است که قصد سرقت اطلاعات ذخیره شده در آن‌ها را دارد. بنابراین بدافزار با مراجعه به مسیر نصب این نرم‌افزارها، در صورتی که نرم‌افزار فوق بر روی سیستم نصب بود، با استفاده از مکانیزمی که برحسب هر نرم‌افزار متفاوت است، اقدام به سرقت اطلاعات حساب‌های کاربری ذخیره‌شده در آن نرم‌افزار می‌نماید.

همچنین این بدافزار با مانیتور کردن ارتباطات کاربر، در صورتی که کاربر به وب‌سایت یکی از اهداف بدافزار وارد شود، اطلاعات ورود کاربر به آن سایت را به سرقت می‌برد. نرم‌افزارهایی که این بدافزار اطلاعات آن‌ها را به سرقت می‌برد متنوع و وسیع بوده و انواع FTP Clientها و Mail Clientها و ... را شامل می‌شود.

در مورد نمونه تحلیل شده، نرم‌افزارها و وب‌سایت‌هایی که بدافزار افزار قصد سرقت اطلاعات آن‌ها را داشت عبارتند از:

- 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

همانگونه که مشاهده می‌شود، این لیست مجموعه وسیعی را شامل می‌شود. مجموعه اطلاعاتی که توسط این بدافزار قابل سرقت هستند عبارتند از:

- اطلاعات حساب‌کاربری سایت‌های FTP، ذخیره‌شده در یکی از کلاینت‌های ذکر شده
- اطلاعات حساب کاربری سایت‌های HTTP، ذخیره شده در یکی از کلاینت‌های ذکر شده
- اطلاعات حساب کاربری ایمیل
- اطلاعات حساب کاربری سرویس‌های چت

- اطلاعات حساب کاربری سرویس‌های Poker
- اطلاعات حساب‌کاربری دسترسی از راه‌دور RDP و VNC
- اطلاعات شماره تلفن‌ها و Dialup Connectionهای کاربر

با توجه به گسترده بودن اطلاعات قابل سرقت توسط این بدافزار و همچنین حساسیت بعضاً زیاد اطلاعاتی که توسط این بدافزار قابل سرقت هستند، می‌توان نتیجه گرفت که آلودگی به این بدافزار بسیار خطرناک بوده و در صورت کشف آلودگی نیاز است قربانی تمامی گذرواژه‌های حساب‌های ذکرشده فوق را سریعاً تغییر داده و نسبت به رفع هرچه سریع‌تر آلودگی اقدام نماید.

همچنین توجه شود که بدافزار بسیار هوشمند عمل نموده و به ازای هر نرم‌افزار و یا وب‌سایت، روش مجزا و منحصر به فردی برای سرقت اطلاعات دارد که این روش‌ها دائماً توسط توسعه‌دهندگان بدافزار به‌روزرسانی می‌شود. بنابراین به‌روزرسانی نرم‌افزارهای مربوطه الزاماً منجر به ایمن‌سازی کاربر نگردیده و رفع آلودگی به بدافزار بایستی هرچه سریع‌تر و با الویت بسیار بالا صورت پذیرد. به خصوص در مورد کاربرانی که مدیر شبکه هستند و اطلاعات دسترسی به کارگزاران مختلف را بر روی سیستم خود ذخیره دارند، آلودگی به این بدافزار می‌تواند تبعات جبران ناپذیری داشته باشد.

۳. تشخیص محیط مجازی و نیز تشخیص Debug

بدافزار Dofoil مکانیزم‌های مختلفی برای تشخیص اجرا در محیط مجازی و یا تشخیص Debug دارد. در صورتی که چنین شرایطی توسط بدافزار تشخیص داده شود، بدافزار عملکرد اصلی خود را انجام نداده و وارد یک حلقه بی‌نهایت می‌شود که به منظور گمراه کردن تحلیل‌گر طراحی شده است. شرایطی که توسط بدافزار بررسی می‌شوند عبارتند از:

- نام فایل و یا مسیر اجرای فایل حاوی کلمه Sample باشد.
- فایل sbiedll.dll که مربوط به ابزار Sandboxie است در پروسه بدافزار تزریق شده باشد.
- فایل dbghelp.dll که مربوط به ابزار WinDBG است در پروسه بدافزار تزریق شده باشد.
- شماره سریال دیسکی که درایو C: بر روی آن قرار دارد با یکی از مقادیر 0x70144646 و یا 0x0CD1A40 شروع شده باشد که مربوط به محیط‌های مجازی‌سازی است.
- کلید HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\Enum\0 در رجیستری حاوی یکی از مقادیر زیر باشد که نشان‌دهنده محیط مجازی سازی متناظر است:
  - Qemu: که نشان‌گر اجرا در محیط Qemu و یا KVM است.
  - VirtualBox: که نشان‌گر اجرا در محیط VirtualBox است
  - Vmware: که نشان‌گر اجرا در یکی از محیط‌های مجازی‌سازی VMWare است.
  - Xen: که نشان‌گر اجرا در محیط مجازی‌سازی Xen است.

- اطلاعات Uninstall در رجیستری ویندوز حاوی کلید AutoItv3CCleanerWIC باشد.

البته بایستی توجه داشت که این عملکرد باعث می‌شود بدافزار قادر به اجرا شدن بر روی کارگزارهای اجرا شده در محیط‌های مجازی نباشد و این نوع سرورها را از آلودگی به این بدافزار مصون می‌دارد. با توجه به عملکرد اصلی بدافزار که سرقت اطلاعات است، این امر نقطه ضعفی اساسی برای بدافزار و نقطه مثبت اساسی برای مدیران شبکه است.

۴. ارتباط با کارگزار کنترل و فرمان و اجرای فرامین

ارتباط بدافزار Dofoil با کارگزار کنترل و فرمان بسیار جالب است، به صورتی که ابتدا بدافزار به یک کارگزار نامربوط تعدادی بسته‌ی رمز شده ارسال می‌کند تا تحلیل‌گر را گمراه سازد. سپس با کارگزار اصلی ارتباط برقرار کرده و شروع به ارسال اطلاعات ارسال شده و دریافت دستورات می‌کند.

برای برقراری ارتباطات تقلبی، بدافزار با دسترسی به کلید زیر در رجیستری، لیست تمامی مقادیری که در کلیدهای HelpLink و URLInoAbout قرار دارند را استخراج می‌کند:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninst
all

پس از آن بدافزار به URLهای استخراج شده متصل شده و تعدادی بسته رمزنگاری شده برای آن‌ها ارسال می‌نماید. مسلماً از آن‌جایی که این کارگزارها، کارگزارهای اصلی بدافزار نیستند، جواب مناسبی از سوی آن‌ها دریافت نخواهد شد که می‌تواند منجر به تشخیص داده شدن این ارتباطات تقلبی شود.

در نمونه‌های مشاهده شده، برقراری ارتباط با کارگزار واقعی کنترل و فرمان بر روی یکی از نام‌های دامنه زیر صورت می‌پذیرد:

- 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

پس از برقراری ارتباط با کارگزار کنترل و فرمان، دو عملکرد اصلی توسط بدافزار صورت می‌گیرد:

الف) ارسال داده‌های سرقت شده (که پیش‌تر شرح داده‌هایی که قابل سرقت هستند بیان شد) برای کارگزار کنترل و فرمان

ب) بارگذاری و اجرای فایل‌های ارسالی از سوی کارگزار کنترل و فرمان: این عملکرد بدین صورت انجام می‌شود که یک فایل رمزنگاری شده از سوی کارگزار کنترل و فرمان برای بدافزار ارسال می‌شود. پس از رمزگشایی محتوای فایل، بدافزار ممکن است به یکی از سه روش زیر نسبت به اجرای فایل دریافتی اقدام نماید:

- محتوای دریافتی را درون یک فایل با نام تصادفی در مسیر %Temp% ویندوز ذخیره‌سازی کرده و سپس آن را اجرا نماید (در صورتی که فایل دریافتی Executable باشد).
- محتوای فایل را به صورت مستقیم در یکی از پروسه‌های در حال اجرا بر روی سیستم تزریق کرده و آن را اجرا نماید (در صورتی که فایل دریافتی DLL باشد).
- همچنین در صورتی که فایل دریافتی Executable باشد که نیاز باشد پس از هربار راه‌اندازی مجدد سیستم اجرا شود، بدافزار محتوای دریافتی را در یک فایل با نام تصادفی در Startup Folder ویندوز ذخیره سازی می‌نماید.

بررسی‌های انجام شده نشان می‌دهد که فایل‌های دانلود شده توسط بدافزار عمدتاً Agentهایی برای اجرای حملات DDoS و یا ارسال گسترده هرزنامه هستند.