

بسمه تعالی



وزارت ارتباطات و فناوری اطلاعات  
سازمان فناوری اطلاعات ایران  
معاونت امنیت فضای تولید و تبادل اطلاعات



مرکز مدیریت امداد و هماهنگی  
عملیات رخدادهای رایانه ای

## تحلیل فنی باج افزار DarkBit

### گزارش فنی

شناسه سند ..... MaherReports\_14020105  
نوع سند ..... گزارش فنی  
شماره نگارش ..... ۰,۱  
تاریخ نگارش ..... ۱۴۰۱/۱۲/۲۹  
طبقه بندی سند ..... **عادی**

تهران، خیابان شهید بهشتی - بین بزرگراه شهید مدرس و خیابان احمد قصیر - پلاک ۲۶۷

cert.ir



(۰۲۱) ۸۸۱۱۵۷۲۴



(۰۲۱) ۸۸۱۱۵۷۲۴





۱	مقدمه	۱
۱	مشخصات فایل اجرایی	۲
۱	شجره نامه	۳
۱	میزان تهدید فایل باج افزار	۴
۲	تحلیل پویا	۵
۲	۱-۵ آناتومی حمله	۵-۱
۶	۲-۵ روش مقابله	۵-۲
۶	ایستا	۶
۶	۱-۶ تحلیل کد	۶-۱
۹	۲-۶ تحلیل ترافیک شبکه	۶-۲
۹	شناسه های تهدید (IOCs)	۷
۱۰	شناسایی (Detection)	۸

## ۱ مقدمه

باج افزار DarkBit که اولین حمله خود را در اواخر بهمن ماه سال گذشته در یکی از دانشگاه ها انجام داده است، برای فعالیت خود احتیاجی به اتصال به اینترنت ندارد و چه با دسترسی مدیر سیستم (Administrator) و چه بدون آن، اطلاعات سیستم را رمزنگاری می کند. الگوریتم رمزنگاری این باج افزار از نوع AES-256 می باشد.

## ۲ مشخصات فایل اجرایی

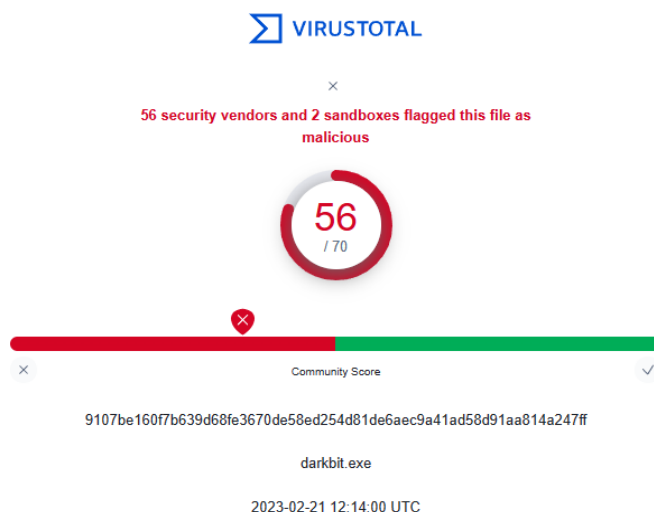
9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff.exe	نام فایل
9880fae6551d1e9ee921f39751a6f3c0	MD5
30466ccd4ec7bcafb370510855da2cd631f74b7a	SHA-1
9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff	SHA-256
Win32 EXE (PE64)	نوع فایل
5.14 MB (5385216 bytes)	اندازه فایل

## ۳ شجره نامه

طبق مشاهدات صورت گرفته، باج افزار DarkBit منتسب به یک گروه شناخته شده یا گونه ای خاص نیست و در نامش از ترکیب نام باج افزارهای پرآوازه ای مانند LockBit و DarkSide استفاده شده است. سمپل مورد استفاده در این گزارش، اولین و تنها مورد از مشاهده این باج افزار تا زمان نوشتن این تحلیل می باشد.

## ۴ میزان تهدید فایل باج افزار

در حال حاضر ۵۶ مورد از ۷۰ ضد بد افزار سامانه VirusTotal باج افزار DarkBit را به عنوان یک برنامه مخرب شناسایی می کنند:



## ۵ تحلیل پویا

### ۱-۵ آناتومی حمله

پس از اجرای باج‌افزار DarkBit در محیط آزمایشگاهی، مشاهده شد که این باج‌افزار هم بر روی ماشین مجازی و هم فیزیکی اجرا می‌شود و رفتارهای زیر را نشان می‌دهد.

explorer.exe	0.37	78,412 K	174,608 K	6936	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		2,048 K	13,612 K	8720	Windows Security notificatio...	Microsoft Corporation
vmtoolsd.exe	< 0.01	21,596 K	39,808 K	8716	VMware Tools Core Service	VMware, Inc.
OneDrive.exe		21,080 K	79,080 K	9176	Microsoft OneDrive	Microsoft Corporation
procexp64.exe	0.75	22,732 K	46,968 K	7720	Sysinternals Process Explorer	Sysinternals - www.sysinter...
Procmon64.exe		4,760 K	14,236 K	3940	Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe	8.24	71,160 K	43,704 K	6736		
Taskmgr.exe	< 0.01	23,656 K	49,016 K	10060		
9107be160f7b639d68fe367...	21.71	22,832 K	15,520 K	6884		
conhost.exe	< 0.01	7,096 K	19,816 K	9688	Console Window Host	Microsoft Corporation

باج‌افزار به عنوان زیر پراسسی از explorer.exe اجرا می‌شود و از لحظه اجرا تا انتها، روند اجرای خود را در محیط CMD به نمایش می‌گذارد:

```

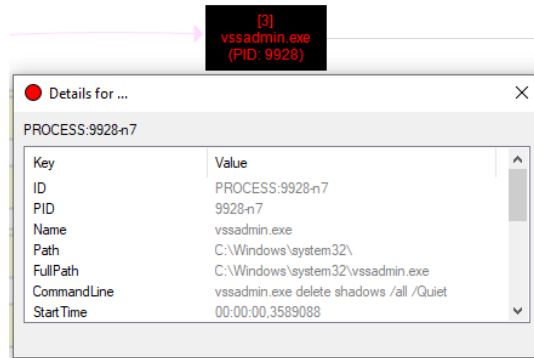
C:\Users\Apa\Downloads\9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff.exe
Encryption will run on all files in 10
Vssadmin delete vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Encryption will run on all files in 9
Encryption will run on all files in 8
Encryption will run on all files in 7
Encryption will run on all files in 6
Encryption will run on all files in 5
Encryption will run on all files in 4
Encryption will run on all files in 3
Encryption will run on all files in 2
Encryption will run on all files in 1
Running with 4 Worker threads
Running with 4 Worker threads
EOF
2023/02/21 10:03:29 EOF
Failed to Rename C:\users\Apa\AppData\Local\Comms\UnistoreDB\tmp.edb to C:\users\Apa\AppData\Local\Comms\UnistoreDB\6mVnK20c1676961205.Darkbit
2023/02/21 10:03:32 rename C:\users\Apa\AppData\Local\Comms\UnistoreDB\tmp.edb C:\users\Apa\AppData\Local\Comms\UnistoreDB\6mVnK20c1676961205.Darkbit: The system cannot find the file specified.
Encrypted 8006 files in 1 mins
2023/02/21 10:04:28 open D:\System Volume Information: Access is denied.
Encrypted 15552 files in 2 mins
Encrypted 18985 files in 3 mins
2023/02/21 10:06:20 CreateFile C:\users\Apa\AppData\Local\Microsoft\Edge\User Data\lockfile: The system cannot find the file specified.

```

این اطلاعات شامل شمارش معکوس شروع فرآیند در ۱۰ ثانیه، خطاهای موجود، تعداد رشته‌های فعال در فرآیند و همچنین آمار تعداد فایل‌های رمز شده در واحد دقیقه می‌باشد.

باج‌افزار DarkBit در ابتدای اجرا قبل از شروع عملیات رمزنگاری، اطلاعات درون فضای VSS ویندوز را با دستور `vssadmin.exe delete shadows /all /Quiet` پاک می‌کند تا از بازیابی احتمالی جلوگیری کند.



```
Image: C:\Windows\System32\vssadmin.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: Command Line Interface for Microsoft® Volume Shadow Copy Service
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: VSSADMIN.EXE
CommandLine: vssadmin.exe delete shadows /all /Quiet
```

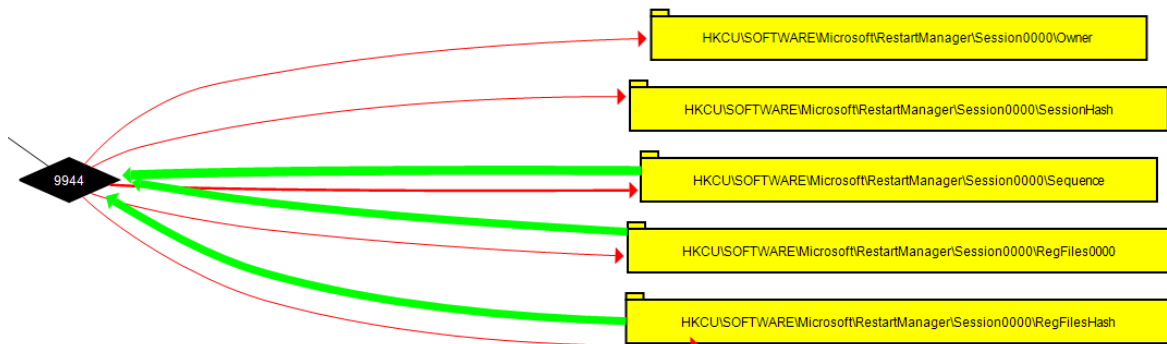
با این حال باج افزار مذکور برای اجرای کامل می بایست دسترسی ادمین داشته باشد، در غیر این صورت نمی تواند فضای shadowcopy را دستکاری کند:

```
C:\Users\Apa\Downloads\9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff.exe
Encryption will run on all files in 10
Vssadmin delete vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2013 Microsoft Corp.

Error: You don't have the correct permissions to run this command. Please run this utility f
window that has elevated administrator privileges.

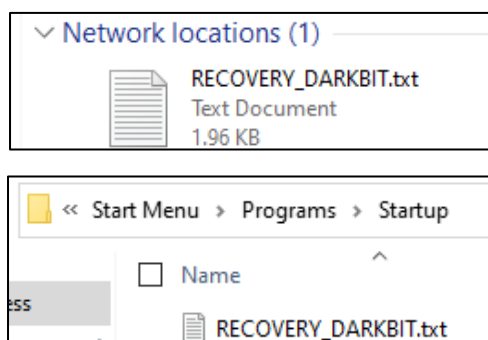
vssadmin exit status 2
Encryption will run on all files in 9
Encryption will run on all files in 8
```

بررسی انجام شده بر روی فعالیت های کلید رجیستری این سمپل نشان می دهد که DarkBit با کلیدهای رجیستری RestartManager برای از کار انداختن یک سری برنامه ها ارتباط برقرار می کند:



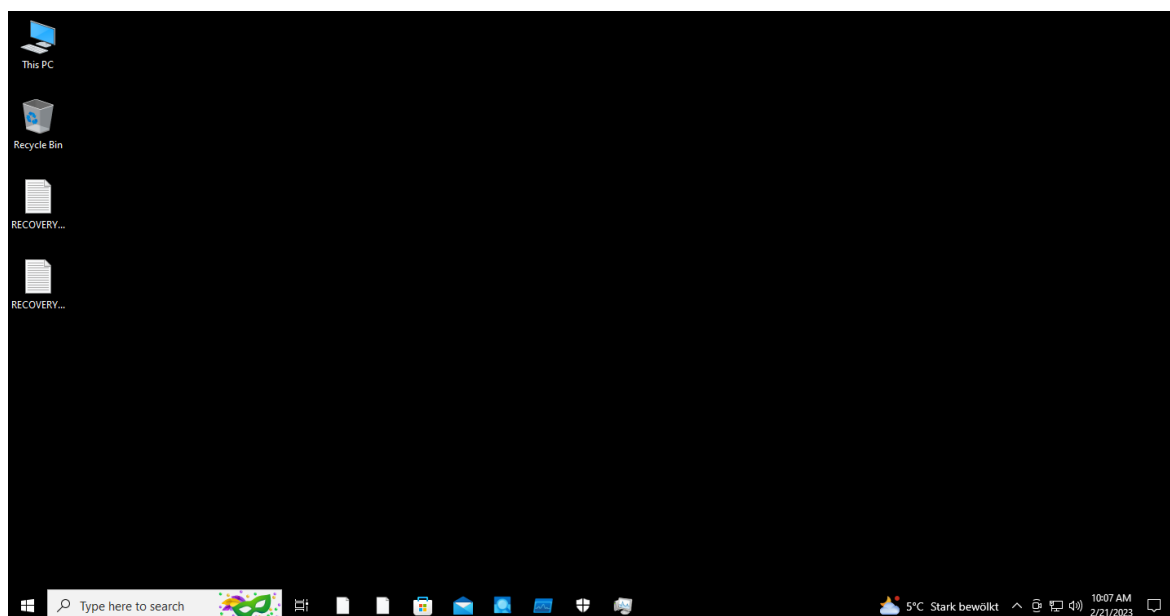
بلافاصله پس از اجرا، باج افزار، پیغام باج خواهی خود تحت عنوان RECOVERY\_DARKBIT.txt را در پوشه Startup قرار می دهد تا با هر بار روشن شدن سیستم، این پیغام برای کاربر به نمایش درآید. همچنین یک

نسخه از این پیغام در تمام مسیرهای به اشتراک گذاشته شده در شبکه و یا رسانه‌های قابل حمله از جمله DVD Writer کپی می‌شود.



در متن باج‌افزار DarkBit اشاره شده است که شبکه مورد نظر به‌طور کامل هک شده است و همه‌ی اطلاعات آن به سرورهای مهاجم منتقل شده است. همچنین در متن بیان شده است که فایل‌ها با درجه نظامی الگوریتم AES-256 رمزنگاری شده‌اند. بنابراین بدون داشتن کلید، شروع به بازیابی نکنید تا از آسیب دائمی به فایل‌ها جلوگیری شود، باید به آنها برای عملیات بازیابی اعتماد کنیم و در نهایت باج درخواستی را به مقدار ۸۰ بیت‌کوین (80 BTC) بپردازیم؛ پس از پرداخت نیز کلید رمزگشایی ارسال می‌شود. در انتهای پیغام باج‌خواهی نیز اشاره شده که بعد از ۴۸ ساعت ۳۰٪ به مبلغ باج افزوده می‌شود و همچنین پس از ۵ روز اطلاعات برای فروش گذاشته می‌شود.

باج‌افزار DarkBit پس از حمله به سیستم قربانی، تصویر صفحه دسکتاپ را به صورت زیر تغییر می‌دهد. (اگر با دسترسی ادمین اجرا نشود روی دسکتاپ تنها یک فایل متنی مربوط به باج قرار می‌گیرد.)



علاوه بر این، باج افزار برخی از برنامه‌های در حال اجرا را از ادامه باز می‌دارد (مانند Wireshark) و همین‌طور برخی دیگر از برنامه‌های درون سیستم را نیز ناقص می‌کند تا اجرای آن‌ها به مشکل خورد؛ همچنین فایل‌های Shortcut موجود در استارت و تسک‌بار را نیز از بین می‌برد.

باج افزار DarkBit پس از اتمام اجرا فایل اجرایی خود را پاک نمی‌کند:

Name	Date modified	Type	Size
▼ Last week (7)			
OGlylyjL1676962064.Darkbit	2/21/2023 10:17 AM	DARKBIT File	6,849 KB
8tVdJvPW1676962064.Darkbit	2/21/2023 10:17 AM	DARKBIT File	15,223 KB
9107be160f7b639d68fe3670de58ed254...	2/21/2023 6:30 AM	Application	5,259 KB
b7vkKvJp1676962064.Darkbit	2/21/2023 10:17 AM	DARKBIT File	888 KB
hJ9wlZhc1676962064.Darkbit	2/21/2023 10:17 AM	DARKBIT File	2,030 KB
RECOVERY_DARKBIT.txt	2/21/2023 10:17 AM	Text Document	2 KB
VxFtfI881676962064.Darkbit	2/21/2023 10:17 AM	DARKBIT File	716 KB

فایل‌هایی که با این باج افزار رمزگذاری می‌شوند با الگوی "8-char-random-string"8-number'.Darkbit نام گذاری می‌شوند:

Name	Date modified	Type	Size
JHPLEGLF1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	1,070,886 KB
jq9NX7uo1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	5,470 KB
kKiaf2Ok1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	1,413 KB
KlhB7Pfw1677322261.Darkbit	2/25/2023 2:21 PM	DARKBIT File	15,435 KB
LDoqjc01677322261.Darkbit	2/25/2023 2:21 PM	DARKBIT File	9,937 KB
LPsLx9s51677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	143,758 KB
LUygAMXK1677322261.Darkbit	2/25/2023 2:21 PM	DARKBIT File	5,270 KB
N4HhKvQC1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	31 KB
O8yHd8EK1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	227 KB
OK21VSWC1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	258,718 KB
QCzUtPHx1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	71 KB
RECOVERY_DARKBIT.txt	2/25/2023 2:20 PM	Text Document	2 KB
SwrwtBgT1677322260.Darkbit	2/25/2023 2:21 PM	DARKBIT File	75 KB
tIivDwFr1677322261.Darkbit	2/25/2023 2:21 PM	DARKBIT File	3,073 KB
Test (1).bin	10/23/2022 10:41 AM	BIN File	1,035 KB
Test (1).com	10/23/2022 10:41 AM	MS-DOS Applicati...	1,035 KB
Test (1).Darkbit	10/23/2022 10:41 AM	DARKBIT File	1,035 KB
Test (1).exe	6/16/2019 4:25 AM	Application	129 KB
Test (1).msi	10/23/2022 10:41 AM	Windows Installer ...	1,035 KB
Test (1).theme	10/23/2022 10:41 AM	Windows Theme F...	1,035 KB
Test (3).exe	10/23/2022 10:41 AM	Application	1,035 KB
Test (4).exe	11/6/2022 12:26 PM	Application	76,842 KB
Test (5).exe	10/23/2022 10:42 AM	Application	101,581 KB
Test (5).idx	10/23/2022 10:41 AM	IDX File	1,035 KB
WRdmlL901677322261.Darkbit	2/25/2023 2:21 PM	DARKBIT File	3,593 KB
yPjP6B8r1677322261.Darkbit	2/25/2023 2:21 PM	DARKBIT File	3,402 KB
Zq6PIRzX1677322261.Darkbit	2/25/2023 2:21 PM	DARKBIT File	6,100 KB

در انتهای اجرا باج افزار موردنظر در فعالیت سیستم‌های امنیتی ویندوز مانند Defender و Event Viewer اختلالی ایجاد نمی‌کند.

## ۲-۵ روش مقابله

باچافزار DarkBit هم‌اکنون در صورت فعال بودن لایه‌ی محافظتی Windows Defender یا ضد باچافزارهای دیگر قابل تشخیص می‌باشد و از اجرای آن جلوگیری به عمل خواهد آمد. همچنین در شبکه‌های سازمانی با اعمال سطوح دسترسی مناسب برای کاربران دامین، می‌توان از اجرای باچافزار جلوگیری کرد.

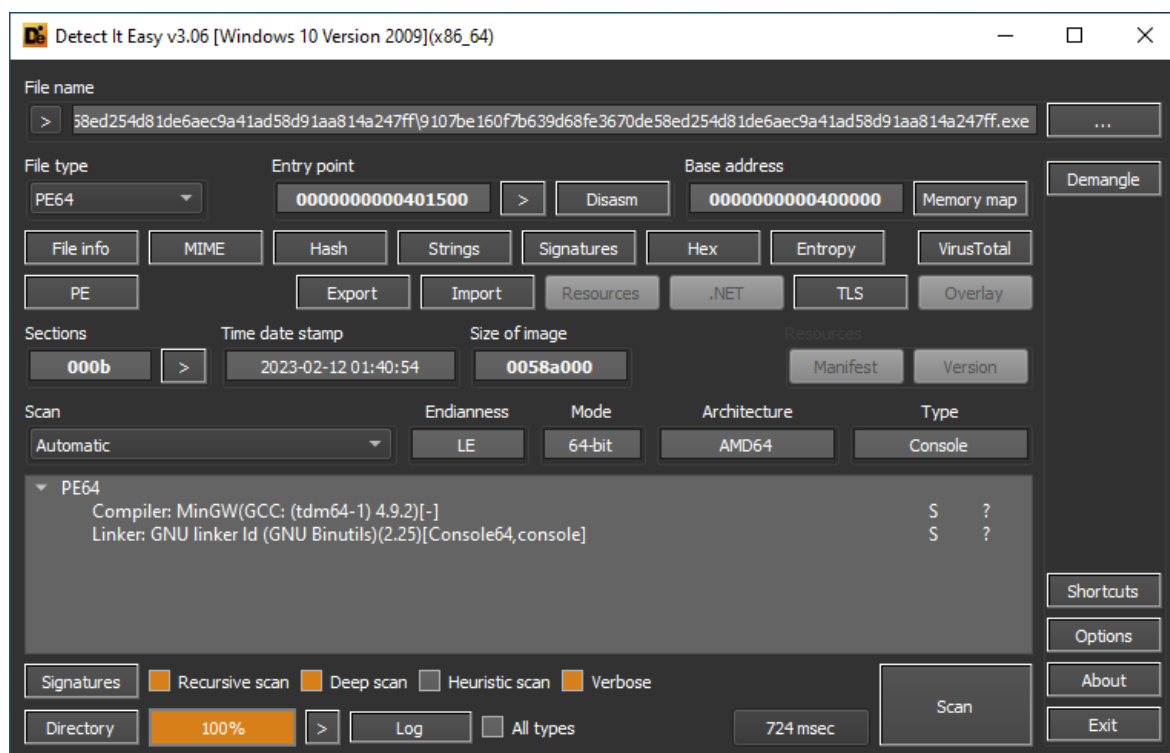
## ۶ ایستا

بررسی‌ها بر روی نمونه تست شده باچافزار DarkBit نشان می‌دهد که باچافزار مذکور بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از ۷ به بعد به شرط ۶۴ بیتی بودن، اجرا خواهد شد.

os-version	6.1	Windows 7
cpu	64-bit	

## ۱-۶ تحلیل کد

طبق بررسی‌های صورت گرفته، کد باچافزار DarkBit توسط زبان برنامه‌نویسی C/C++ نوشته شده است و بصورت پکیج Portable Executable در آمده است:



که با ابزار و عملیات مهندسی معکوس می‌توانیم به برخی از توابع این برنامه دست یابیم. کد این برنامه به میزان زیادی درهم‌سازی شده است و اطلاعات زیادی از آن کسب نمی‌شود.

در این بخش فایل Rstrtmgr.dll که مربوط به Restart Manager است بارگذاری می‌شود و برخی از توابع آن برای به‌کارگیری در برنامه فراخوانی می‌شوند:



```

● 27 | LibraryA = LoadLibraryA("Rstrtmgr.dll");
● 28 | v2 = LibraryA;
● 29 | if ( !LibraryA )
● 30 |     return 0i64;
● 31 | ProcAddress = GetProcAddress(LibraryA, "RmStartSession"); ۱
● 32 | if ( !ProcAddress )
● 33 |     return 0i64;
● 34 | v4 = GetProcAddress(v2, "RmRegisterResources"); ۲
● 35 | if ( !v4 )
● 36 |     return 0i64;
● 37 | v5 = GetProcAddress(v2, "RmGetList"); ۳
● 38 | if ( !v5 )
● 39 |     return 0i64;
● 40 | v6 = GetProcAddress(v2, "RmShutdown"); ۴
● 41 | if ( !v6 )
● 42 |     return 0i64;
● 43 | v7 = GetProcAddress(v2, "RmEndSession"); ۵

```

۱	یک Session جدید در Restart Manager ایجاد می کند
۲	تعیین می کند که چه برنامه یا سرویسی باید خاموش یا راه اندازی دوباره شود
۳	لیست برنامه هایی که توسط Restart Manager رجیستر شده اند را برمی گرداند
۴	دستور خاموش شدن برنامه را صادر می کند
۵	Session فعال Restart Manager را می بندد

در این بخش نیز اطلاعاتی از سیستم دریافت می کند تا آمار نسبت به زمان فایل های رمز شده را بدست آورد:

```

● 35 | strcpy(v29, "GetSystemTimeAsFileTime"); ۱
● 36 | v6 = sub_42C8E0(0x18ui64, 0x656D6954656C69i64, a3, a4);
● 37 | if ( dword_976970 )
● 38 |     v6 = sub_457E60(v8);
● 39 | else
● 40 |     qword_91E788 = v6;
● 41 | if ( !v6 )
● 42 | {
● 43 | LABEL_27:
● 44 |     sub_432080(v8, v7);
● 45 |     goto LABEL_28;
● 46 | }
● 47 | strcpy(v28, "QueryPerformanceCounter"); ۲
● 48 | v10 = sub_42C8E0(0x18ui64, 0x7265507972657551i64, 0x7265746E756F43i64, v9);
● 49 | if ( dword_976970 )
● 50 |     sub_457E60(v11);
● 51 | else
● 52 |     qword_91E7A8 = v10;
● 53 | strcpy(v30, "QueryPerformanceFrequency"); ۳
● 54 | v14 = sub_42C8E0(0x1Aui64, 0x79636E65757165i64, v12, v13);
● 55 | if ( dword_976970 )
● 56 |     v14 = sub_457E60(v16);
● 57 | else
● 58 |     qword_91E7B0 = v14;

```

۱	تاریخ و ساعت فعلی سیستم را برمی گرداند
۲	مقدار فعلی شمارنده عملکرد را بازیابی می کند که می تواند برای اندازه گیری بازه زمانی استفاده شود
۳	فرکانس شمارنده عملکرد را بازیابی می کند که به کمک قبلی برای اندازه گیری زمان استفاده می شود

پس از اینکه فایل PE برنامه را بصورت ASCII جستجو می‌کنیم به چند فایل json برخوردیم که از آن‌ها برای کنترل عملکرد باج‌افزار استفاده می‌شود. پس از استخراج محتویات فایل‌های کانفیگ json به نتایج زیر می‌رسیم:

```

"limits": [
  {
    "limitMB": 25,
    "parts": 1,
    "eachPart": -1
  },
  {
    "limitMB": 1000,
    "parts": 2,
    "eachPart": 12000
  },
  {
    "limitMB": 4000,
    "parts": 3,
    "eachPart": 10000
  },
  {
    "limitMB": 7000,
    "parts": 2,
    "eachPart": 20000
  },
  {
    "limitMB": 11000,
    "parts": 3,
    "eachPart": 30000
  },
  {
    "limitMB": 51000,
    "parts": 5,
    "eachPart": 30000
  },
  {
    "limitMB": 1000000,
    "parts": 3,
    "eachPart": 1000000
  },
  {
    "limitMB": 5000000,
    "parts": 5,
    "eachPart": 1000000
  },
  {
    "limitMB": 6000000,
    "parts": 20,
    "eachPart": 10000000
  }
],

```

درون فایل limits شروط قطعه قطعه کردن فایل‌ها برای رمزگذاری آمده است که limitMB حجم تا آن فایل هدف، parts مقسوم‌علیه تقسیم فایل در حجم آن و eachPart تعداد بایت از اول هر قطعه برای رمزنگاری است.

```

"extensions": {
  "msilog": 1,
  "log": 1,
  "ldf": 1,
  "lock": 1,
  "theme": 1,
  "msi": 1,
  "sys": 1,
  "wpv": 1,
  "cpl": 1,
  "adv": 1,
  "msc": 1,
  "scr": 1,
  "key": 1,
  "ico": 1,
  "dll": 1,
  "hta": 1,
  "deskthemepack": 1,
  "nomedia": 1,
  "msu": 1,
  "rtp": 1,
  "msp": 1,
  "idx": 1,
  "ani": 1,
  "386": 1,
  "diagcfg": 1,
  "bin": 1,
  "mod": 1,
  "ics": 1,
  "com": 1,
  "hlp": 1,
  "spl": 1,
  "nls": 1,
  "cab": 1,
  "diagpkg": 1,
  "icl": 1,
  "ocx": 1,
  "rom": 1,
  "prf": 1,
  "themepack": 1,
  "msstyles": 1,
  "icns": 1,
  "mpa": 1,
  "drv": 1,
  "cur": 1,
  "diagcab": 1,
  "exe": 1,
  "cmd": 1,
  "shs": 1,
  "Darkbit": 1
},

```

محتویات extensions نیز لیست سفید پسوندهای فایل‌های هدف را نشان می‌دهد (حساس به بزرگ کوچک بودن حرف نمی‌باشد) که مقدار 1 جلوی هر key به معنای نادیده گرفتن فایل‌هایی با این پسوندها برای رمزنگاری است.

```

"names": {
  "thumbs.db": 1,
  "desktop.ini": 1,
  "darkbit.jpg": 1,
  "recovery_darkbit.txt": 1,
  "system volume information": 1
},

```

محتویات names نیز نام فایل‌هایی که باج‌افزار باید در لیست سفید قرار دهد را نشان می‌دهد (حساس به بزرگ کوچک بودن حرف نمی‌باشد) که اینجا هم مقدار 1 جلوی هر key به معنای نادیده گرفتن فایل است. پس از بررسی چند نمونه فایل سالم با نمونه رمزنگاری شده مشخص شد که پس از عملیات رمزنگاری مقدراری به اندازه ۳۰۳ الی ۳۳۵ بایت به آخر هر فایل اضافه می‌شود که شامل اطلاعاتی از فایل رمز شده می‌باشد و با تبدیل مقادیر Hex آن‌ها به ASCII متن DARKBIT\_ENCRYPTED\_FILES نمایش داده می‌شود:

00000000	00 01	02 03	04 05	06 07	08 09	0a 0b	0c 0d	0e 0f	
000117f0	00 00	00 00	00 00	00 00	00 00	00 00	00 00	00 00	.....
00011800	44 41	52 4b	42 49	54 5f	45 4e	43 52	59 50	54 45	DARKBIT_ENCRYPTE
00011810	44 5f	46 49	4c 45	53 7c	ad 86	b4 4d	12 9b	3e 7f	D_FILES .†M.>>.
00011820	4b 2c	8d 2d	e8 1a	44 14	44 41	52 4b	42 49	54 2b	K,-.è.D.DARKBIT+
00011830	21 e4	ef 7d	3b 1e	25 98	8e aa	b4 35	07 84	62 d7	!äi};.%Zª 5.,,bx
00011840	d6 ae	22 b4	ec c8	d7 d7	78 fa	7b 9c	db 78	fb c1	0ª" 'iExxxú{æ0xúA
00011850	25 7d	11 56	e4 0a	8f cc	1f 52	a8 00	7c d6	bb be	%}.Vä..I.R". 0»%
00011860	26 19	35 1c	71 c8	09 46	82 7f	d4 4c	1c 3a	74 c5	&.5.qÈ.F,.0L.:tA
00011870	56 69	df d3	e7 97	ef 57	53 02	78 ac	62 f0	e5 6d	ViB0ç-iWS.x-bðàm
00011880	24 27	ef e0	a4 e6	c5 a7	99 71	70 76	44 19	6e 5b	\$'iàªæA\$™qpV.D.n[
00011890	d4 85	0c b4	be 80	c7 6d	f2 49	c3 93	98 4e	06 9a	O... %€ÇmòIA""N.š
000118a0	3f df	2d bf	c2 01	d1 83	bb 45	1d 21	3a 21	7b ac	?B-زA.Nf»E.!!:[-
000118b0	eb ca	0b 1c	54 5d	0e 4d	14 bb	bc 51	b6 cc	dc 8d	èÈ..T].M.»%Q¶IU.
000118c0	24 9e	a4 1f	6f 75	a7 e2	6e 67	3e bd	44 eb	f7 0e	\$žª.oušàng>%Dè±.
000118d0	b7 12	a4 8f	44 5c	64 2c	15 8b	d7 e0	ae bf	c6 85	.ª.D\d,..<xàªžÈ...
000118e0	6d 39	c4 08	ee e1	df 77	dd ac	30 be	a3 64	9f 8a	m9A.îáBwY-0%fdYS
000118f0	d4 c8	23 9c	0f b6	24 01	ad 20	e2 0c	7e f7	6c 44	0È#e.¶\$. . â.~÷ D
00011900	d1 1c	5f 44	b7 ec	7f 41	5b 37	0a c9	9f 49	b3 8a	N._D.ì.A[7.EYIªS
00011910	02 79	8f 0b	b4 6c	3e d9	2c d0	21 ef	aa 2d	f3 71	.y.. 'l>U,ð!iª-óq
00011920	22 bb	1c b5	e0 e0	82 fb	10 f6	fc a9	58 bd	dd ..	"»..µàà,ù.òuèX%Y.
00011930	.. ..	.. ..	.. ..	.. ..	.. ..	.. ..	.. ..	.. ..	.....

## ۲-۶ تحلیل ترافیک شبکه

پس از بررسی ترافیک شبکه ضبط شده پس از اجرای باج‌افزار DarkBit و همچنین بررسی نتایج سندباکس‌های آنلاین، هیچ‌گونه ارتباط شبکه‌ای در مورد باج‌افزار مشاهده نشد و این سمپل کاملاً آفلاین فعالیت می‌کند.

## ۷ شناسه‌های تهدید (IOCs)

Samples:

SHA256: 9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff

Ransom Note:

recovery\_darkbit.txt

Detection names:

Kaspersky: Trojan-Ransom.Win64.Darkbit.a

Bitdefender: Trojan.GenericKD.65491228

ESET: WinGo/Filecoder.DarkBit.A

Windows Defender: Ransom:Win64/DarkBit

## ۸ شناسایی (Detection)

با توجه به اینکه باج‌افزار DarkBit بلافاصله پس از اجرا، فضای VSS ویندوز را حذف می‌کند، با استفاده از کوئری زیر در اسپلانک می‌توان هر گونه فعالیت مرتبط با Shadow Copy را شناسایی کرد:

```
((EventCode="4688" OR EventCode="1") (CommandLine="*vssadmin* *delete* *shadows*" OR CommandLine="*wmic* *shadowcopy* *delete*" OR CommandLine="*vssadmin* *resize* *shadowstorage*")) OR (EventCode="5857" ProviderName="MSVSS__PROVIDER") OR (EventCode="5858" Operation="*Win32_ShadowCopy*")
```

از آنجایی که باج‌افزار DarkBit در مسیرهای حساس سیستمی فعالیت می‌کند و از طریق رابط خط فرمان، فایل‌هایی (Processes) را نیز در این مسیرها می‌سازد، این رفتار را می‌توان به عنوان یک رفتار مشکوک در سیستم عامل در نظر گرفت که با کوئری زیر در اسپلانک قابل شناسایی است:

```
index="sysmon" AND (CommandLine="vssadmin.exe delete shadows*" OR CommandLine="vssadmin delete shadows*" OR CommandLine="vssadmin create shadow /for=C:*" OR CommandLine="copy \\?\GLOBALROOT\Device\*\windows\ntds\ntds.dit*" OR CommandLine="copy \\?\GLOBALROOT\Device\*\config\SAM*" OR CommandLine="copy \\?\GLOBALROOT\Device\*\config\SYSTEM*" OR CommandLine="type \\?\GLOBALROOT\Device\*\config\SAM*" OR CommandLine="type \\?\GLOBALROOT\Device\*\config\SYSTEM*" OR CommandLine="type \\?\GLOBALROOT\Device\*\windows\ntds\ntds.dit*" OR CommandLine="reg SAVE HKLM\SYSTEM *" OR CommandLine="reg SAVE HKLM\SAM *" OR CommandLine="*sekurlsa:" OR CommandLine="net localgroup administrators */add" OR CommandLine="net group \Domain Admins\" * /ADD /DOMAIN" OR CommandLine="certutil.exe *-urlcache* http*" OR CommandLine="certutil.exe *-urlcache* ftp*" OR CommandLine="netsh advfirewall firewall *\AppData\*" OR CommandLine="attrib +S +H +R *\AppData\*" OR CommandLine="schtasks* /create *\AppData\*" OR CommandLine="schtasks* /sc minute*" OR CommandLine="*\Regasm.exe *\AppData\*" OR CommandLine="*\Regasm *\AppData\*" OR CommandLine="*\bitsadmin* /transfer*" OR CommandLine="*\certutil.exe * -decode *" OR CommandLine="*\certutil.exe * -decodehex *" OR CommandLine="*\certutil.exe -ping *" OR CommandLine="icacls */grant Everyone:F/T/C/Q" OR CommandLine="* wmic shadowcopy delete *" OR CommandLine="* wmic shadowcopy call create Volume=*" OR CommandLine="* wbadmin.exe delete catalog -quiet*" OR CommandLine="*\wscript.exe *.jse" OR CommandLine="*\wscript.exe *.js" OR CommandLine="*\wscript.exe *.vba" OR CommandLine="*\wscript.exe *.vbe" OR CommandLine="*\cscript.exe *.jse" OR CommandLine="*\cscript.exe *.js" OR CommandLine="*\cscript.exe *.vba" OR CommandLine="*\cscript.exe *.vbe" OR CommandLine="*\fodhelper.exe" OR CommandLine="*waitfor*/s*" OR CommandLine="*waitfor*/si persist*" OR CommandLine="*remote*/s*" OR CommandLine="*remote*/c*" OR CommandLine="*remote*/q*" OR CommandLine="*AddInProcess*" OR CommandLine="*/stext *" OR CommandLine="*/scomma *" OR CommandLine="*/stab *" OR CommandLine="*/stabular *" OR CommandLine="*/shtml *" OR CommandLine="*/sverhtml *" OR CommandLine="*/sxml *")
```

(by Florian Roth at SOC Prime Threat Detection Marketplace)