بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

مرکز ماهر

مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای

تحلیل فنی باج‌افزار DarkBit

گزارش فنی

شناسه سند	MaherReports_14020105
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۴۰۱/۱۲/۲۹
طبقه‌بندی سند	عادی

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

(۰۲۱) ۸۸۱۱۵۷۲۴

(۰۲۱) ۸۸۱۱۵۷۲۴

cert.ir

فهرست مطالب

۱ مقدمه

باج‌افزار DarkBit که اولین حمله خود را در اواخر بهمن ماه سال گذشته در یکی از دانشگاه‌ها 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 می‌کند. الگوریتم رمزنگاری این باج‌افزار از نوع AES-256 می‌باشد.

۲ مشخصات فایل اجرایی

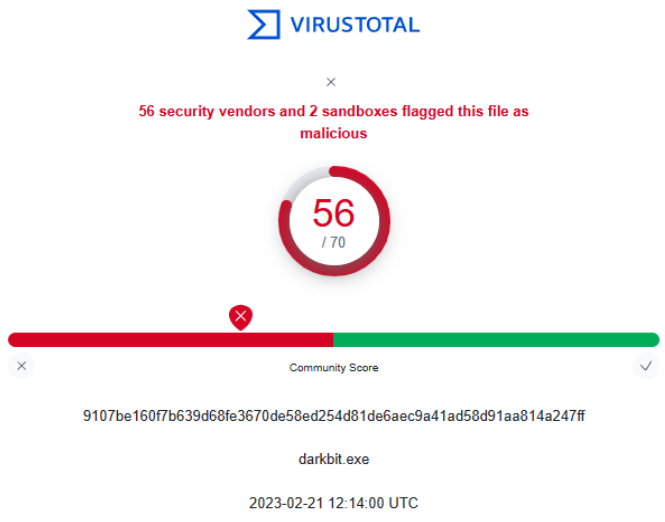
نام فایل	9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff.exe
MD5	9880fae6551d1e9ee921f39751a6f3c0
SHA-1	30466ccd4ec7bcafb370510855da2cd631f74b7a
SHA-256	9107be160f7b639d68fe3670de58ed254d81de6aec9a41ad58d91aa814a247ff
نوع فایل	Win32 EXE (PE64)
اندازه فایل	5.14 MB (5385216 bytes)

۳ شجره‌نامه

طبق مشاهدات صورت گرفته، باج‌افزار DarkBit منتسب به یک گروه شناخته شده یا گونه‌ای خاص نیست و در نامش از ترکیب نام باج‌افزارهای پرآوازه‌ای مانند LockBit و DarkSide استفاده شده است. سمپل مورد استفاده در این گزارش، اولین و تنها مورد از مشاهده این باج‌افزار تا زمان نوشتن این تحلیل می‌باشد.

۴ میزان تهدید فایل باج‌افزار

درحال حاضر ۵۶ مورد از ۷۰ ضد بدافزار سامانه VirusTotal باج‌افزار DarkBit را به عنوان یک برنامه مخرب شناسایی می‌کنند:



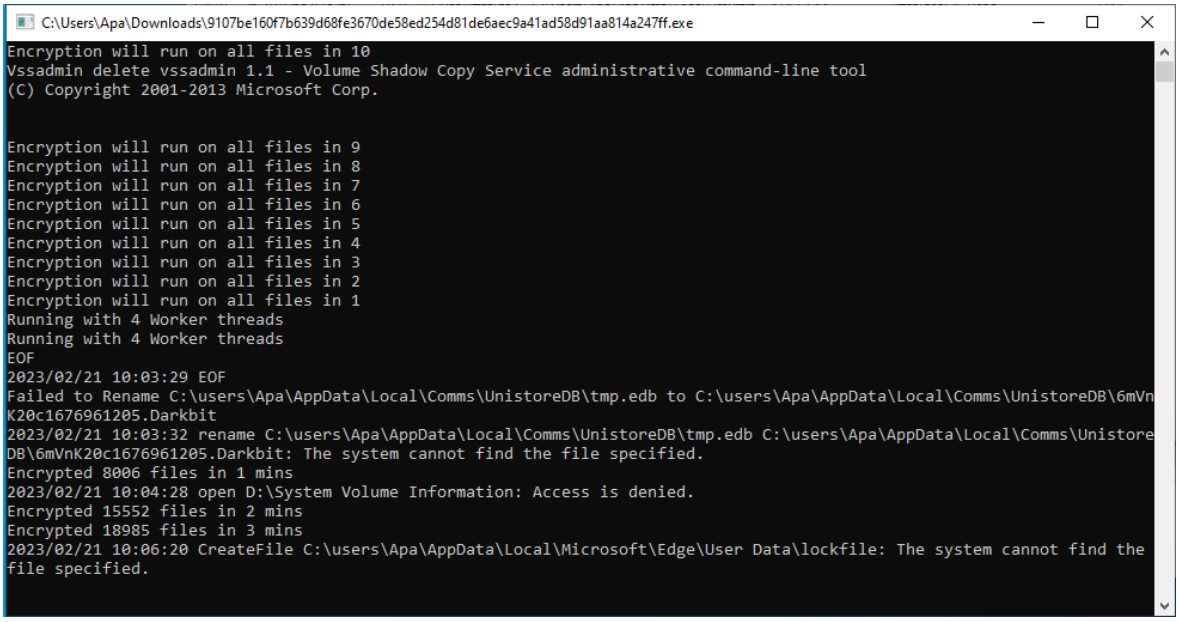
۵ تحلیل پویا

۵-۱ 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.

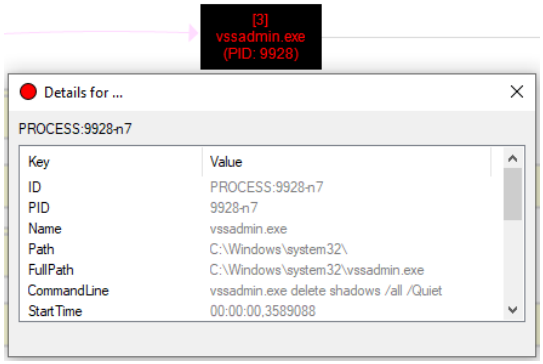
explorer.exe	0.37	78,412 K	174,608 K	6936 Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		2,048 K	13,612 K	8720 Windows Security notificatio...	Microsoft Corporation
vmtoolsd.exe	< 0.01	21,596 K	39,808 K	8716 VMware Tools Core Service	VMware, Inc.
OneDrive.exe		21,080 K	79,080 K	9176 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:



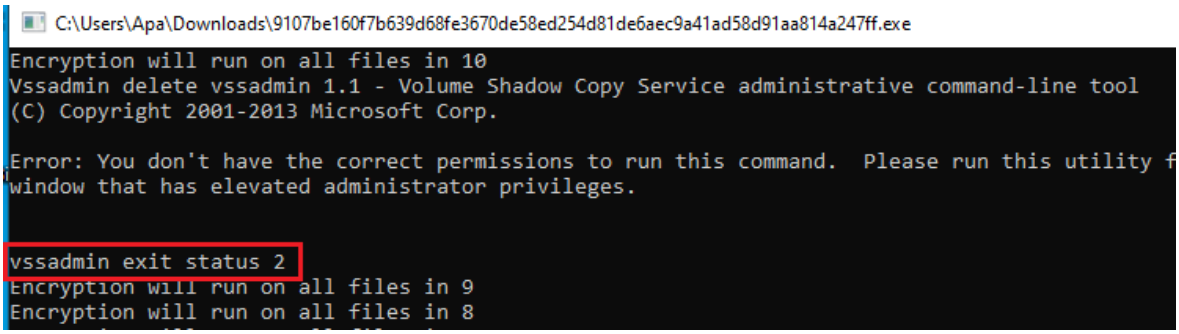
این اطلاعات شامل شمارش معکوس شروع فرآیند در ۱۰ ثانیه، خطاهای موجود، تعداد رشته‌های فعال در فرآیند و همچنین آمار تعداد فایل‌های رمز شده در واحد دقیقه می‌باشد.

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.

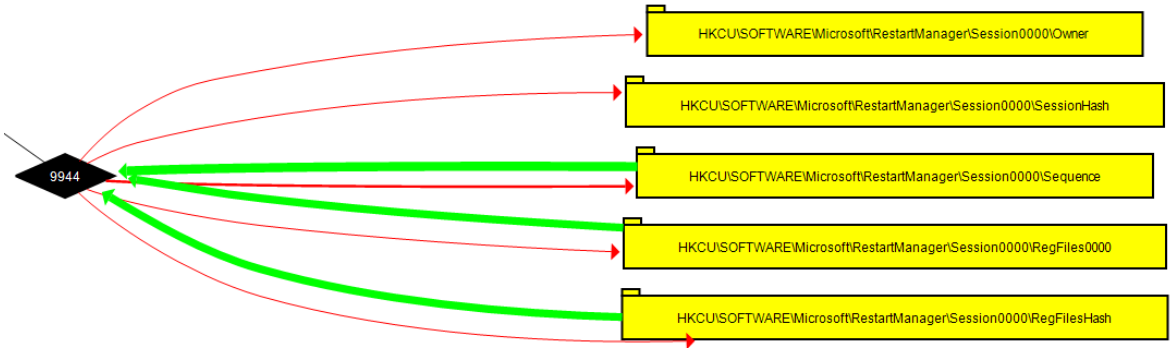



```
Image: C:\Windows\System32\vssadmin.exe
FileVersion: 10.0.19041.1 (WinBuild.160101.0800)
Description: Command Line Interface for Microsoft® Volume Shadow Copy Service
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: VSSADMIN.EXE
CommandLine: vssadmin.exe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

با این حال باج‌افزار مذکور برای اجرای کامل می‌بایست دسترسی ادمین داشته باشد، در غیر این صورت نمی‌تواند فضای shadowcopy را دستکاری کند:

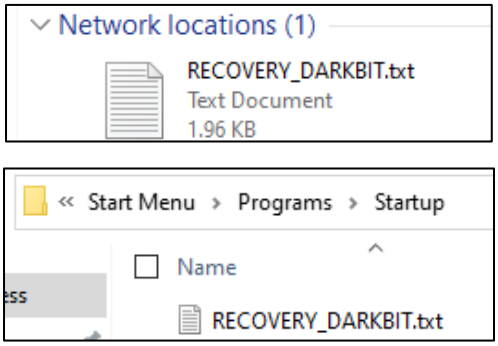


بررسی انجام شده بر روی فعالیت‌های کلید رجیستری این سمپل نشان می‌دهد که DarkBit با کلیدهای رجیستری RestartManager برای از کار انداختن یک‌سری برنامه‌ها ارتباط برقرار می‌کند:



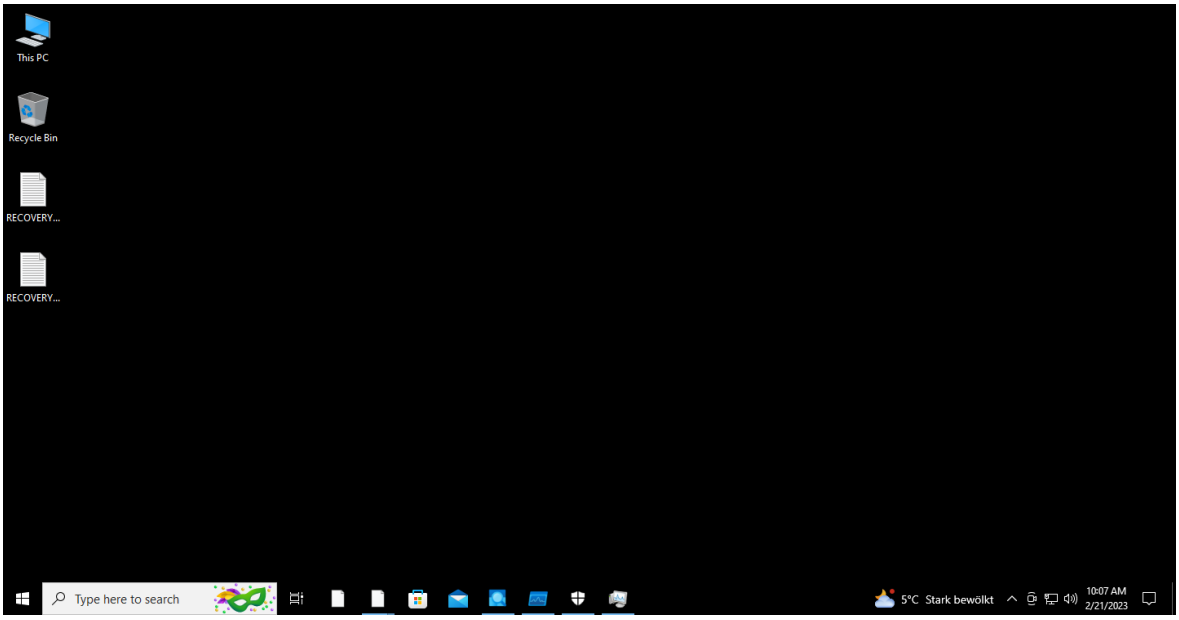
بلافاصله پس از اجرا، باج‌افزار، پیغام باج‌خواهی خود تحت عنوان RECOVERY_DARKBIT.txt را در پوشه Startup قرار می‌دهد تا با هر بار روشن شدن سیستم، این پیغام برای کاربر به نمایش درآید. همچنین یک

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



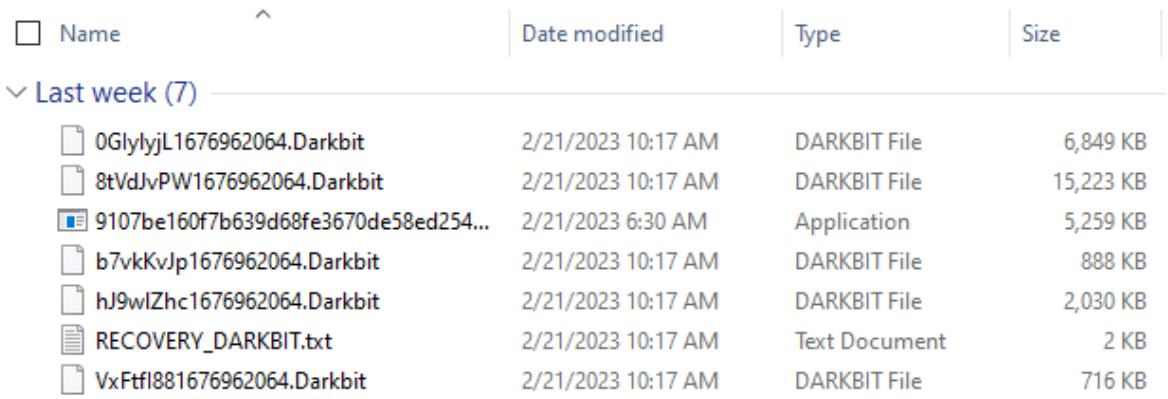
در متن باجِ باج‌افزار DarkBit اشاره شده است که شبکه مورد نظر به‌طور کامل هک شده است و همه‌ی اطلاعات آن به سرورهای مهاجم منتقل شده است. همچنین در متن بیان شده است که فایل‌ها با درجه نظامی الگوریتم AES-256 رمزنگاری شده‌اند. بنابراین بدون داشتن کلید، شروع به بازیابی نکنید تا از آسیب دائمی به فایل‌ها جلوگیری 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.)

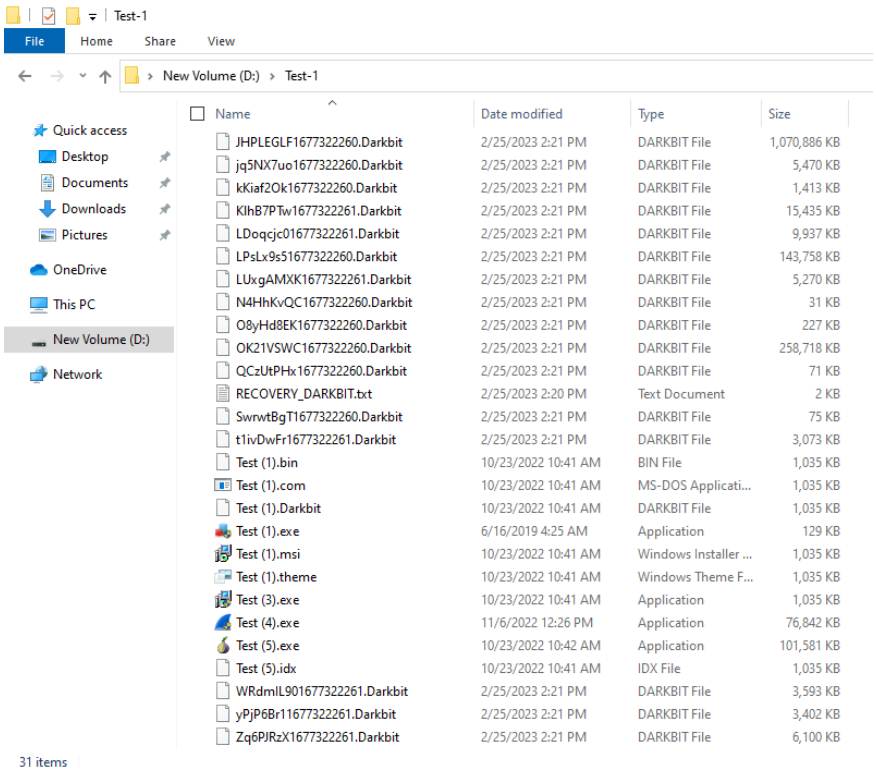


علاوه بر این، باج‌افزار برخی از برنامه‌های درحال اجرا را از ادامه باز می‌دارد (مانند Wireshark) و همین‌طور برخی دیگر از برنامه‌های درون سیستم را نیز ناقص می‌کند تا اجرای آن‌ها به مشکل خورد؛ همچنین فایل‌های Shortcut موجود در استارت و تسک‌بار را نیز از بین می‌برد.

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



فایل‌هایی که با این باج‌افزار رمزگذاری می‌شوند با الگوی "’8-char-random-string’’8-number’.Darkbit" نام‌گذاری می‌شوند:



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

۲-۵ روش مقابله

باج‌افزار DarkBit هم‌اکنون در صورت فعال بودن لایه‌ی محافظتی Windows Defender یا ضد باج‌افزارهای 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 باج‌افزار جلوگیری کرد.

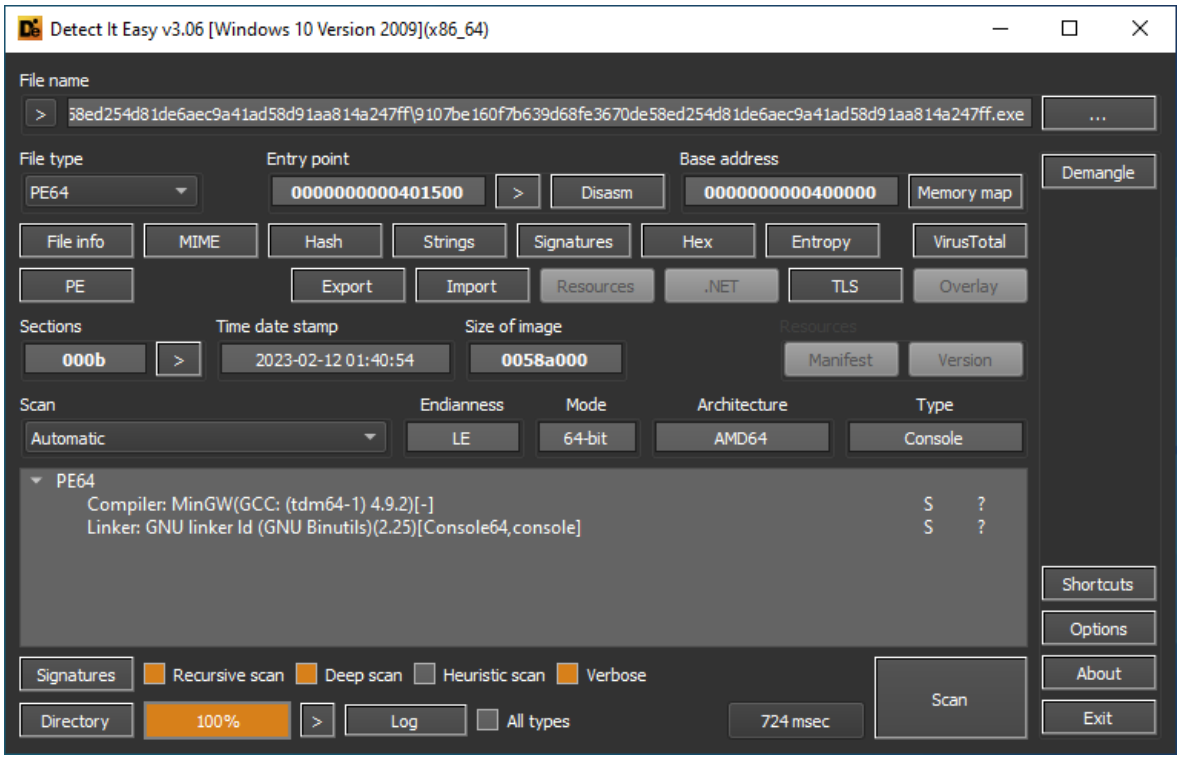
۶ ایستا

بررسی‌ها بر روی نمونه تست شده باج‌افزار DarkBit نشان می‌دهد که باج‌افزار 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 باج‌افزار 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 می‌کند
۲	تعیین می‌کند که چه برنامه یا سرویسی باید خاموش یا راه‌اندازی دوباره شود
۳	لیست برنامه‌هایی که توسط Restart Manager رجیستر شده اند را برمی‌گرداند
٤	دستور خاموش شدن برنامه را صادر می‌کند
۵	Session فعال Restart Manager را می‌بندد

در این بخش نیز اطلاعاتی از سیستم دریافت می‌کند تا آمار نسبت به زمان فایل‌های رمزشده 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  {
43LABEL_27:
44    sub_432080(v8, v7);
45    goto LABEL_28;
46  }
47  strcpy(v28, "QueryPerformanceCounter");   ۲
48  v10 = sub_42C8E0(0x18ui64, 0x726550797265751i64, 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 برمی‌گرداند
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 اندازه‌گیری زمان استفاده می‌شود

پس از اینکه فایل PE برنامه را بصورت ASCII جستجو می‌کنیم به چند فایل json برخورده که از آن‌ها برای کنترل عملکرد باج‌افزار استفاده می‌شود. پس‌از استخراج محتویات فایل‌های کانفیگ json به‌نتایج 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 فایلlimits شروط قطعه قطعه کردن فایل‌ها برای رمزگذاری آمده است که limitMB حجم تا آن فایلِ هدف، parts مقسوم‌علیه تقسیم فایل در حجم آن و eachPart تعداد بایت از اول هرقطعه برای رمزنگاری است.

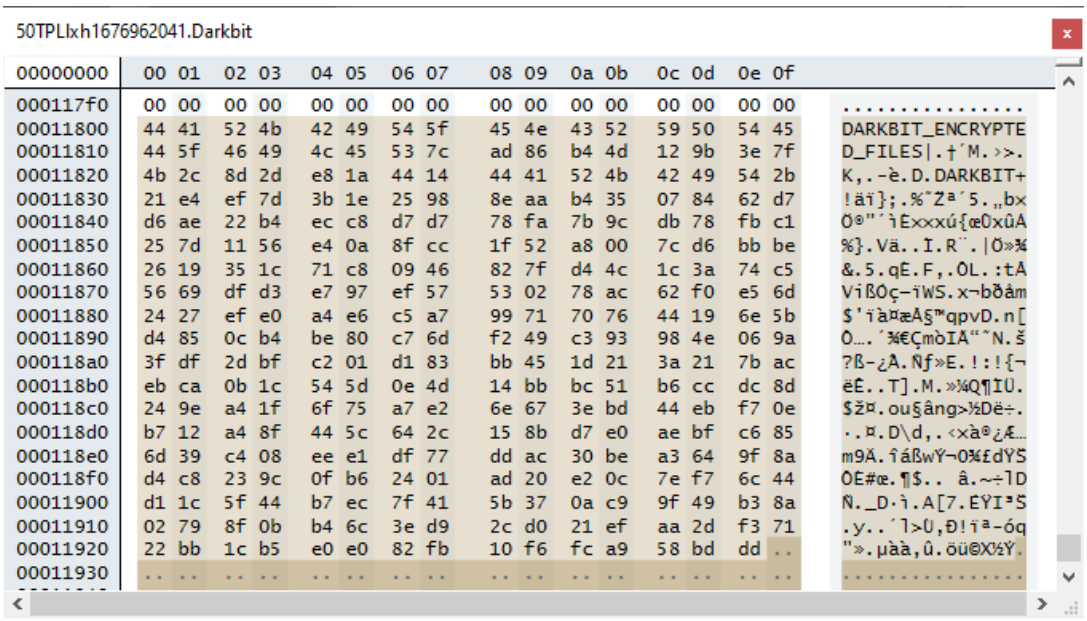

```
"extensions": {
    "msilog": 1,
    "log": 1,
    "ldf": 1,
    "lock": 1,
    "theme": 1,
    "msi": 1,
    "sys": 1,
    "wpx": 1,
    "cpl": 1,
    "adv": 1,
    "msc": 1,
    "scr": 1,
    "key": 1,
    "ico": 1,
    "dll": 1,
    "hta": 1,
    "deskthemepack": 1,
    "nomedia": 1,
    "msu": 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 مقداری به اندازه ۳۰۳ الی ۳۳۵ بایت به آخر هر فایل اضافه می‌شود که شامل اطلاعاتی از فایل رمزشده می‌باشد و با تبدیل مقادیر Hex آن‌ها به ASCII متن DARKBIT_ENCRYPTED_FILES نمایش داده می‌شود:



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 سیستم‌عامل 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)