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 بدافزار SwiftSlicer

## گزارش فنی

| | |
|---|---|
| شناسه سند | MaherReportsTemplate_14011128 |
| نوع سند | گزارش فنی |
| شماره نگارش | ۰,۱ |
| تاریخ نگارش | ۱۴۰۱/۱۱/۲۸ |
| طبقه‌بندی سند | عادی |

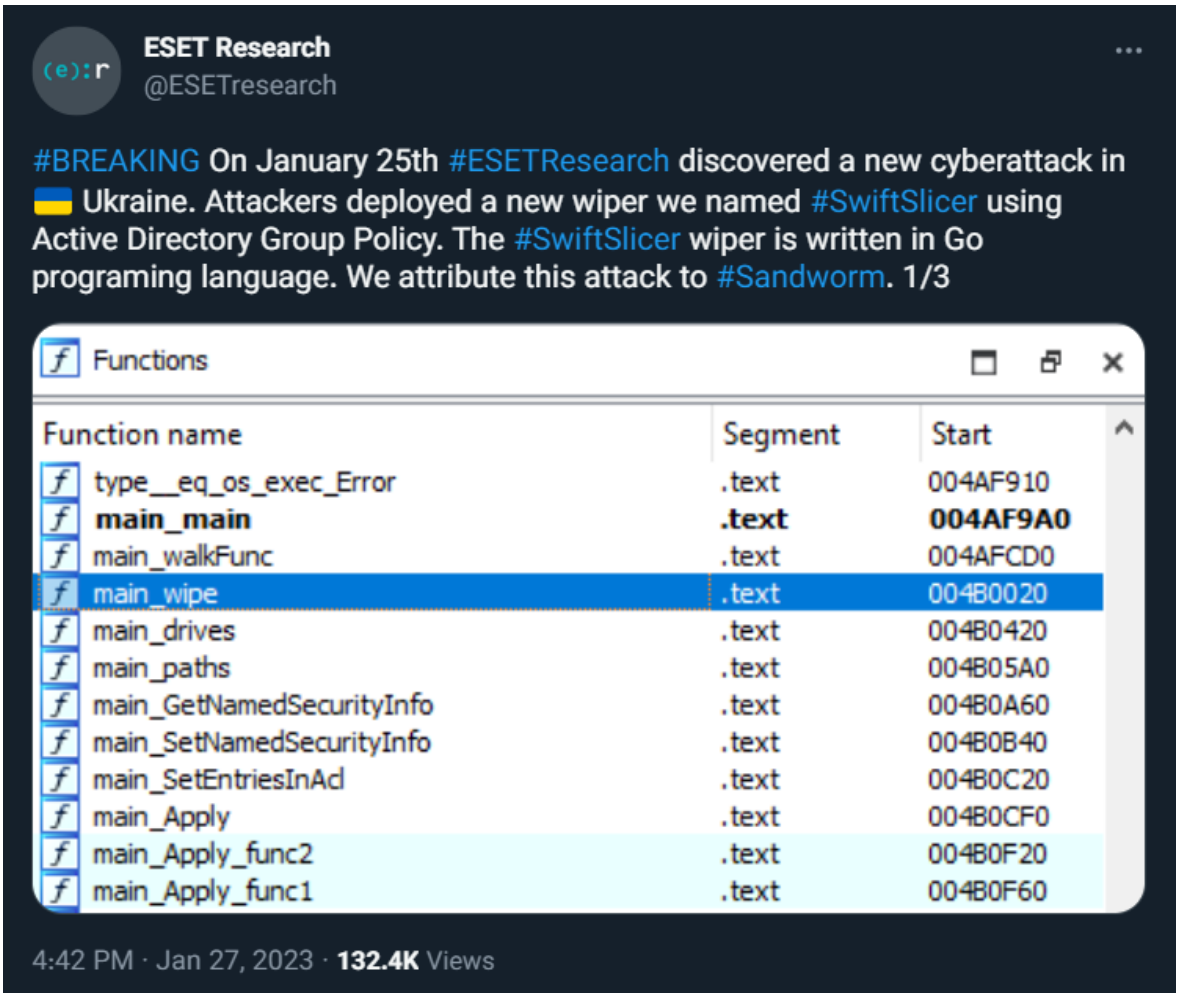

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک ۲۶۷

(۰۲۱) ۸۸۱۱۵۷۲۴ (۰۲۱) ۸۸۱۱۵۷۲۴ cert.ir

# فهرست مطالب

# ۱ مقدمه

در ۲۵ ژانویه ۲۰۲۳ (۵ بهمن ۱۴۰۱) بدافزار SwiftSlicer که از نوع بدافزارهای Wiper یا به عبارت دیگر پاک‌کننده دیتاها می‌باشد در زیرساخت شبکه یک سازمان اکراینی مشاهده شد. طبق مشاهدات صورت گرفته، این بدافزار برای فعالیت خود احتیاجی به اتصال به اینترنت ندارد. اما برای شروع فعالیت خود نیاز به دسترسی مدیر سیستم (Administrator) دارد. این بدافزار همچنین از طریق Active Directory سایر رایانه‌های ویندوزی در شبکه را نیز مورد حمله قرار می‌دهد. طبق اعلام شرکت ESET که برای اولین بار این بدافزار را مشاهده و آنالیز کرده، بدافزار SwiftSlicer، کاری از گروه ارتش سایبری روسیه به نام Sandworm می‌باشد.




# ۲ مشخصات فایل اجرایی

| | |
|---|---|
| نام فایل | 1db93ee81050da0ba413543f9fbc388499a466792f9a54ea6f1bbdb712ba9690.exe |

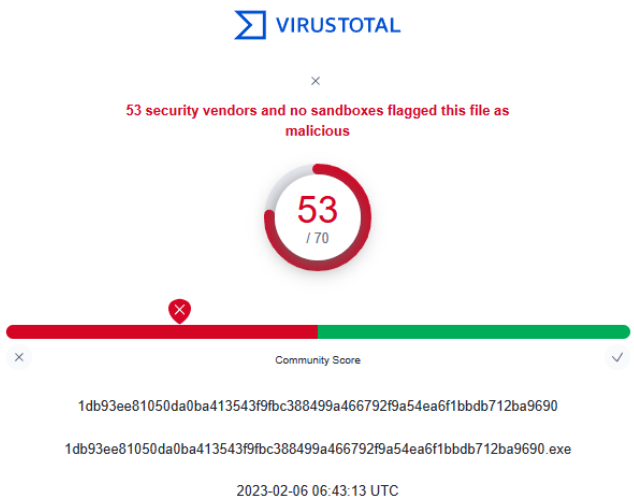
| | |
|---|---|
| **MD5** | FEE7C379F3A555C5C821E872EC384A91 |
| **SHA-1** | 7346E2E29FADDD63AE5C610C07ACAB46B2B1B176 |
| **SHA-256** | 1DB93EE81050DA0BA413543F9FBC388499A466792F9A54EA6F1BBDB712BA9690 |
| **نوع فایل** | Win32 EXE |
| **اندازه فایل** | 1.53 MB (1602560 bytes) |

# ۳ شجره‌نامه

براساس شواهد موجود، بدافزار SwiftSlicer از ابتدا توسط گروه Sandworm ابداء شده و پیشینه‌ای برای آن تشخیص داده نشده است. همچنین موتورهای ضدبدافزار نیز آن‌را زیرمجموعه گروهی خاص قرار نمی‌دهند.

# ۴ میزان تهدید فایل بدافزار

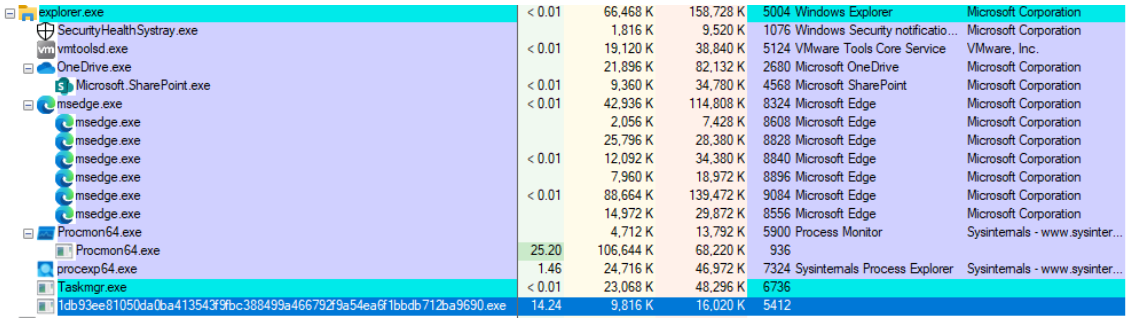
درحال حاضر ۵۳ مورد از ۷۰ ضد بدافزار سامانه VirusTotal بدافزار پاک‌کننده SwiftSlicer را به عنوان یک برنامه مخرب شناسایی می‌کنند:



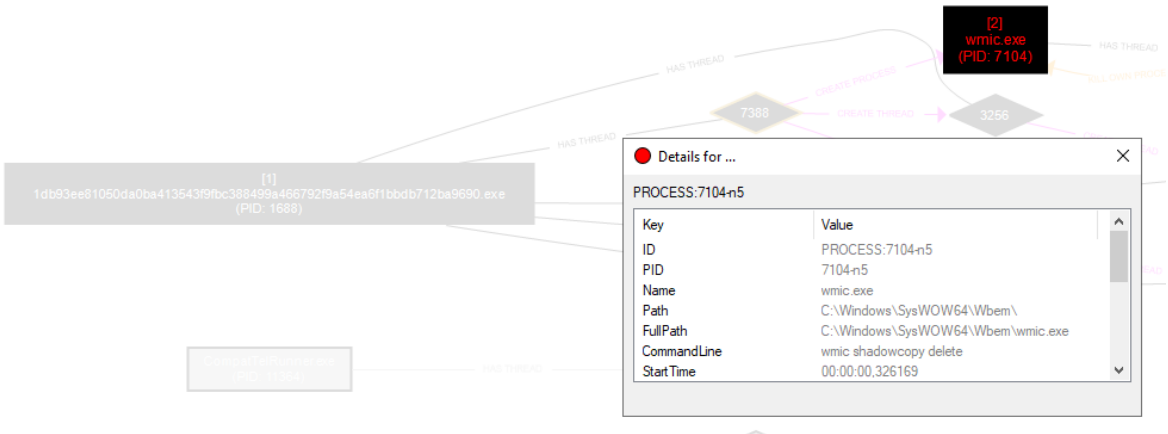
# ۵ تحلیل پویا

## ۵-۱ آناتومی حمله

پس از اجرای بدافزار SwiftSlicer در محیط آزمایشگاهی، مشاهده شد که این بدافزار هم بر روی ماشین مجازی و هم فیزیکی اجرا می‌شود و رفتار زیر را نشان می‌دهد. همانطور که اشاره شد بدافزار مذکور برای اجرا می‌بایست دسترسی ادمین داشته باشد، در غیر این صورت شروع به فعالیت نمی‌کند.

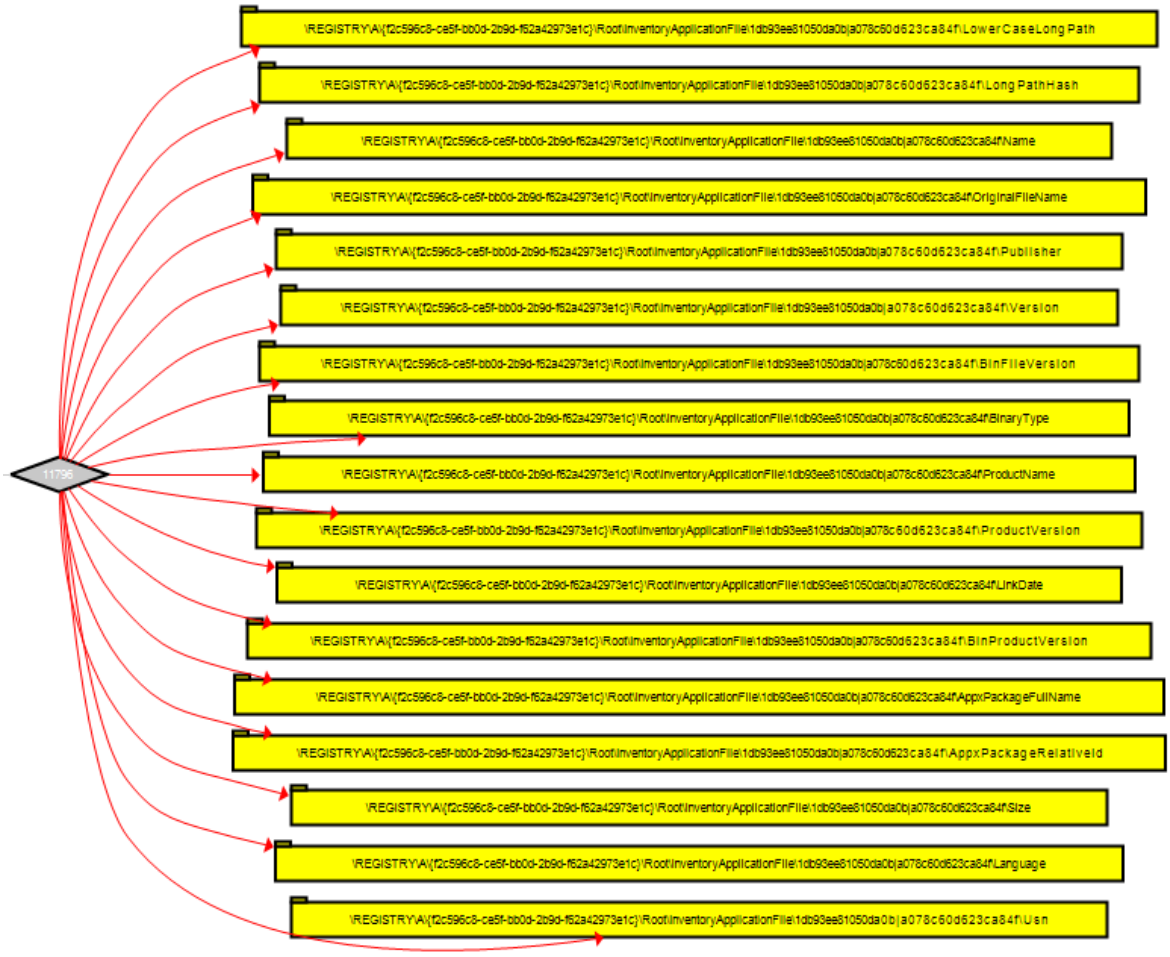



بدافزار SwiftSlicer در ابتدای اجرا، اطلاعات درون فضای VSS ویندوز را با دستور vmic shadowcopy delete پاک می‌کند تا از بازیابی احتمالی جلوگیری کند.



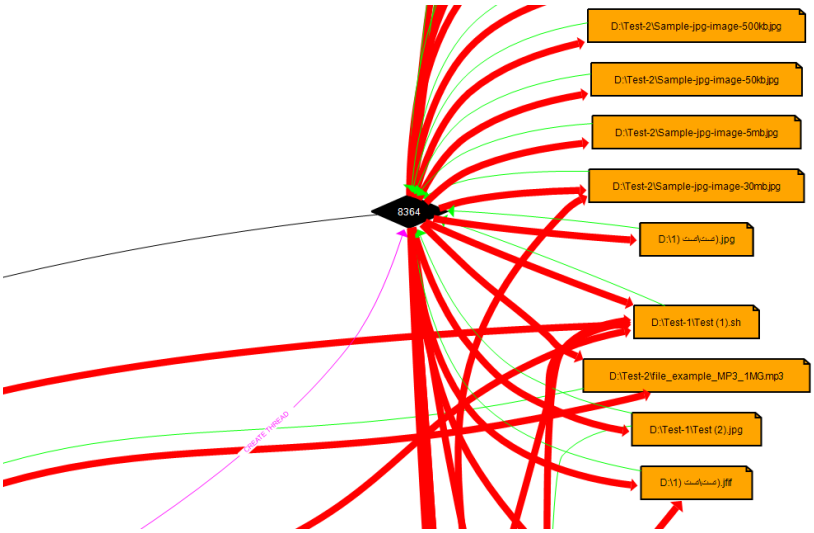

| i | Time | Event |
|---|---|---|
| > | 2/15/23 7:17:46.000 AM | 02/15/2023 10:47:46 AM<br>... 22 lines omitted ...<br>Company: Microsoft Corporation<br>OriginalFileName: wmic.exe<br>CommandLine: wmic shadowcopy delete<br>CurrentDirectory: C:\Users\Apa\Downloads\<br>Show all 38 lines<br>host = DESKTOP-BNVF8GS source = WinEventLog:Microsoft-Windows-Sysmon/Operational<br>sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational |

بررسی‌های انجام شده در محیط آزمایشگاهی نشان می‌دهد که SwiftSlicer با فایل‌ها سر و کار دارد بنابراین با یک‌سری کلیدهای رجیستری مرتبط با آن ارتباط برقرار می‌کند:

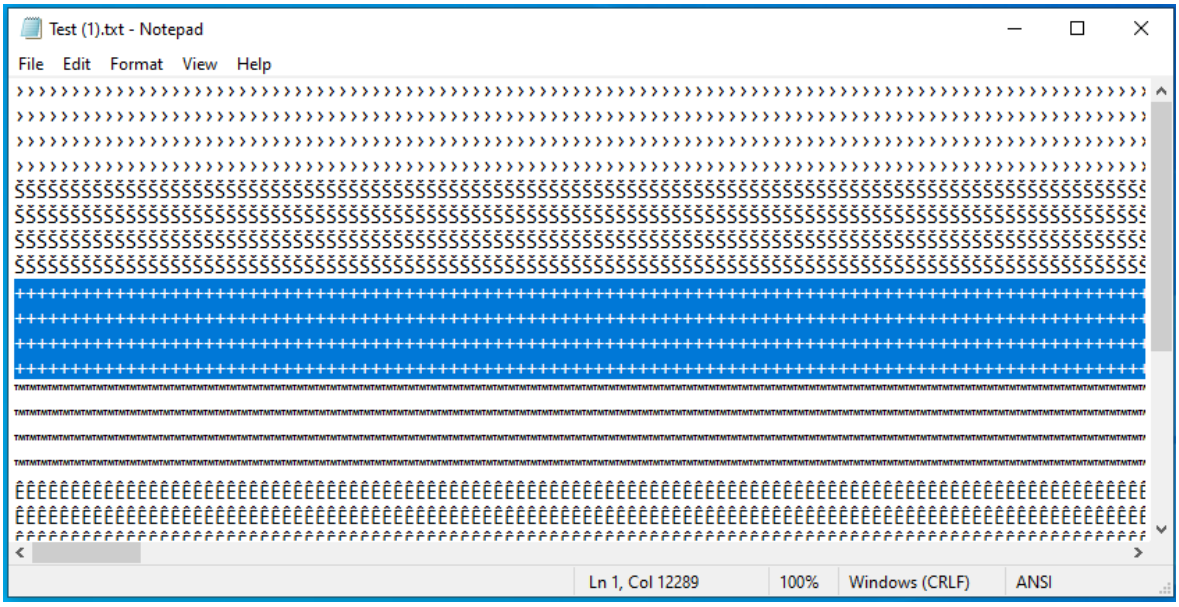



تمام کلیدهای استفاده شده رجیستری از مسیر ...\Root\InventoryApplicationFile\... می‌باشند که نشان از وجود دسترسی ادمین در استفاده از کلیدها می‌باشد.

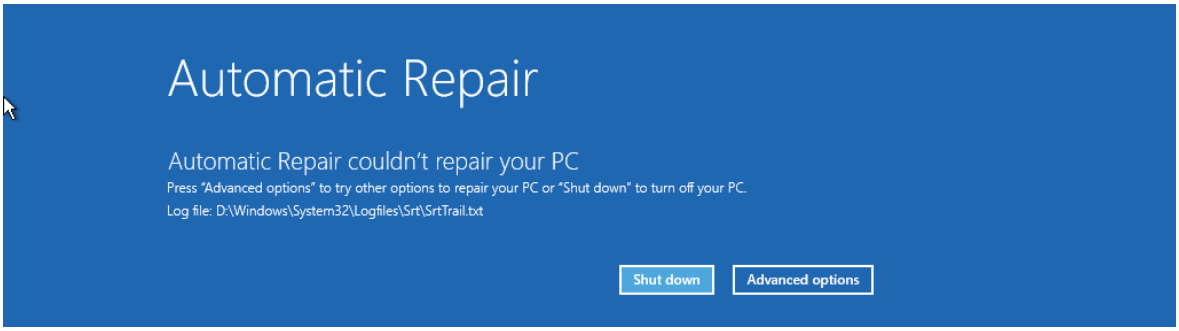
پس از آن نیز به صورت کلی فعالیت این بدافزار بسیار ساده بوده و بخش اصلی و عمده فعالیتش برای رونویسی داده‌ها با کاراکتری به طول ۴۰۹۶ بایت و مقداری تصادفی می‌باشد. بدافزار برای این کار ابتدا از دیسک اول سیستم شروع کرده و به ترتیب دیسک‌ها را با نوشتن اطلاعات روی داده‌های موجود تخریب می‌کند:



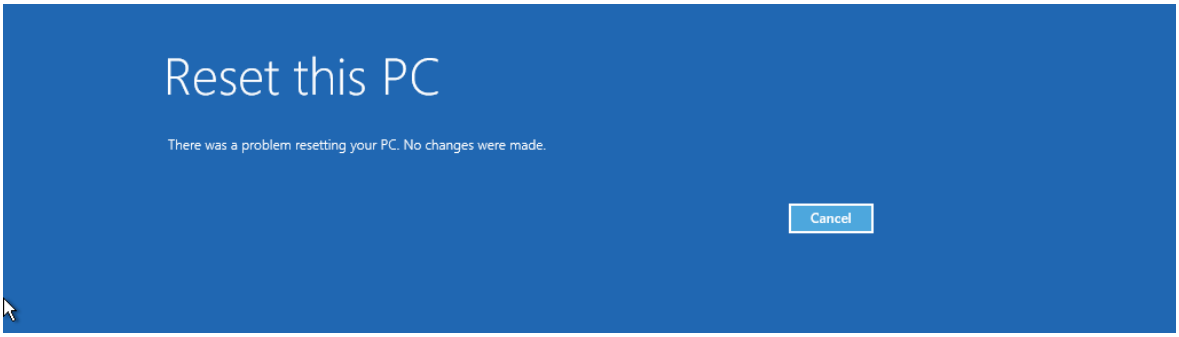

محتویات یک فایل متنی پس از حمله بدافزار بدین گونه تغییر و نمایش داده می‌شود:




پس از حمله SwiftSlicer به سیستم قربانی، بتدریج سرویس‌های مختلف ویندوز با رونویسی داده‌های نامربوط از کار افتاده و در نهایت سیستم ری‌استارت شده و توانایی بوت شدن را از دست می‌دهد:



هنگامی که ویندوز پیغام ناتوانی در تعمیر PC را نمایش می‌دهد دیگر حتی قابلیت Reset را نیز از دست داده و ساختار کل سیستم تخریب شده است:




## ۵-۲ روش انتشار

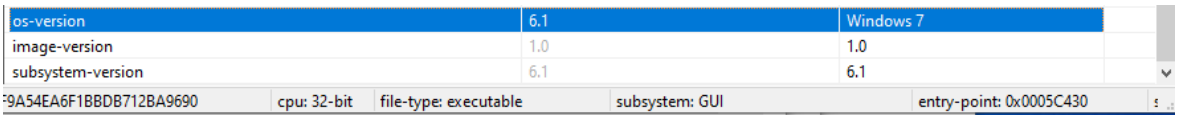
هدف اصلی بدافزار SwiftSlicer حمله به شرکت‌ها، سازمان‌ها و ارگان‌های کشور اکراین می‌باشد تا سیستم‌های آن‌ها را از کار انداخته و همچنین اطلاعات موجود ذخیره شده برروی آن‌ها را از بین ببرد. گروه روسی سازنده این بدافزار هیچی خط‌مشی‌ای برای این بدافزار درنظر نگرفته و به نظر می‌رسد هدف آن‌ها تنها آسیب رساندن به قربانیان در عین سادگی و سرعت تمام است. در حال حاضر، جزئیاتی از روش انتشار این بدافزار منتشر نشده اما بر اساس منابع جهانی، به نظر می‌رسد بدافزار مذکور از طریق هرزنامه‌ها و ایمیل‌های فیشینگ منتشر می گردد.

## ۵-۳ روش مقابله

بدافزار SwiftSlicer در صورت فعال بودن لایه‌ی محافظتی Windows Defender یا ضد بدافزارهای دیگر قابل تشخیص می‌باشد و از اجرای آن جلوگیری به عمل خواهد آمد. همچنین در شبکه‌های سازمانی با اعمال محدودیت عدم دسترسی ادمین بر روی سیستم کاربران، تا حد زیادی می‌توان از اجرای بدافزار جلوگیری کرد.

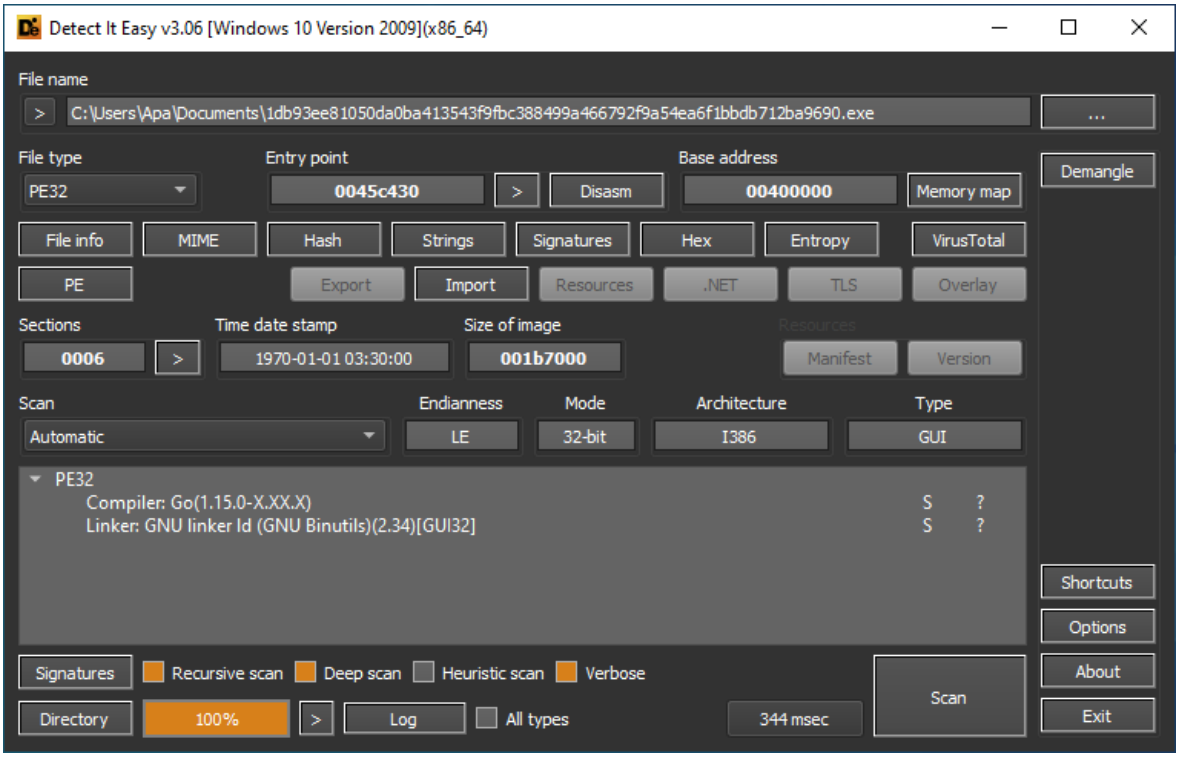
# ۶ تحلیل ایستا

بررسی‌های اولیه بر روی نمونه تست شده بدافزار SwiftSlicer نشان می‌دهد که بدافزار مذکور بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از ۷ به بعد، اجرا خواهد شد.




## ۶-۱ تحلیل کد

طبق بررسی‌های صورت گرفته، کد بدافزار SwiftSlicer توسط زبان برنامه‌نویسی Go نوشته شده است و بصورت پکیج Executable در آمده است:




با عملیات مهندسی معکوس می‌توانیم به برخی از توابع این برنامه دست یابیم.

```
94  v20[0] = (int)"shadowcopy";
95  v20[1] = 10;
96  v20[2] = (int)"deleteefence";
97  v20[3] = 6;
98  v12 = os_exec_Command((int)"wmic", 4, (int)v20, 2, 2);
99  os_exec__Cmd_Run(v12);
```

در قطعه کد بالا، بدافزار با استفاده از ابزار WMIC موجود در خود ویندوز و از طریق رابط خط فرمان، فضای VSS ویندوز را را حذف می‌کند.

در ادامه، SwiftSlicer مجوزهای زیر را در سیستم قربانی تنظیم می‌کند:

```
v21[0] = (int)"SeTakeOwnershipPrivilegeUS Eastern Standard Time"; ۱
v21[1] = 24;
v21[2] = (int)"SeSecurityPrivilege"; ۲
v21[3] = 19;
v21[4] = (int)"SeRestorePrivilege"; ۳
v21[5] = 18;
v21[6] = (int)"SeBackupPrivilege"; ۵
v21[7] = 17;
v21[8] = (int)"SeShutdownPrivilege"; ۶
v21[9] = 19;
v10 = main_enableDisableProcessPrivilege((int)v21, 5, 5, 2);
```

| | |
|---|---|
| ۱ | مجوز گرفتن برای برای هر فایل و فولدری بدون وجود دسترسی مناسب |
| ۲ | مجوز تغییر تنظیمات امنیتی هر فایل و فولدری |
| ۳ | مجوز بازیابی فایل‌ها و فولدرهایی که توسط سیستم پشتیبان‌گیری شده است |
| ٤ | مجوز برای پشتیبان‌گیری از فایل‌ها و فولدرها |
| ٥ | مجوز برای خاموش کردن سیستم |

دستورات زیر برای پیدا کردن و ذخیره لیست دیسک‌ها و درایوهای سیستم قربانی استفاده می‌شود:

```
16  LogicalDriveStrings = main_GetLogicalDriveStrings(0, 0);
17  result = LogicalDriveStrings;
18  if ( !v4 )
19  {
20    v11 = LogicalDriveStrings;
21    v5 = runtime_makeslice((int)&dword_4C0CE0, LogicalDriveStrings, LogicalDriveStrings);
22    if ( !v11 )
23      runtime_panicIndex(v1, v2);
24    main_GetLogicalDriveStrings(v11, v5);
25    v6 = unicode_utf16_Decode(v5, v11, v11);
26    v8 = runtime_slicerunetostring(0, v6, v7, v10);
27    v9 = strings_TrimRight(v8, v10, (int)asc_4CFD9F, 1);
28    return strings_genSplit(v9, v10, (int)asc_4CFD9F, 1, 0, -1);
29  }
```

(تابع GetLogicalDriveStrings نام درایوهای موجود در سیستم را برمی‌گرداند.)

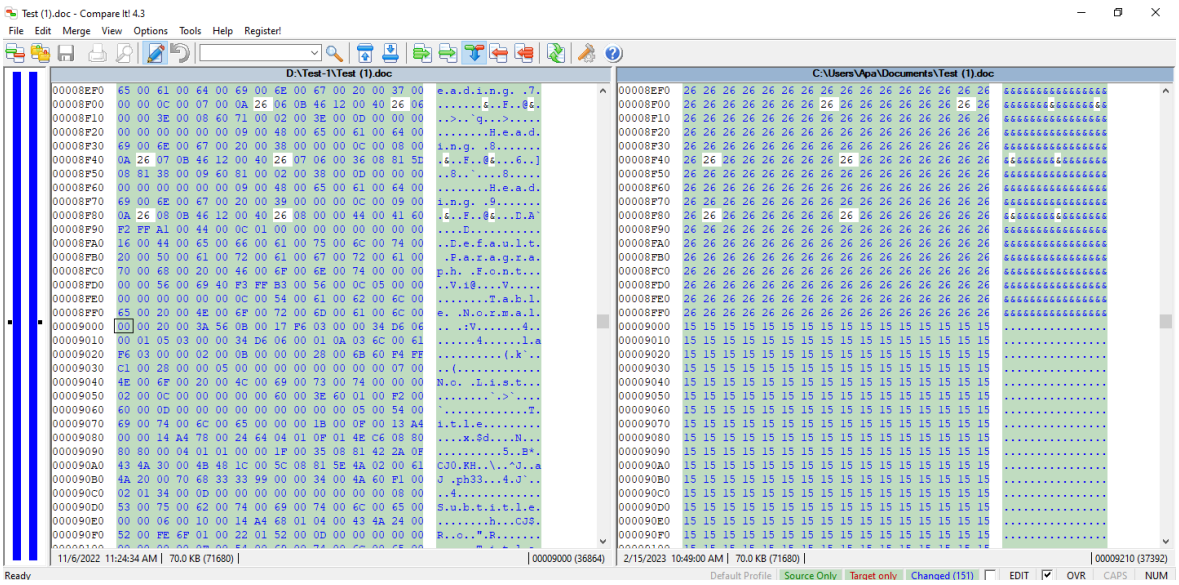
و همینطور مجموعه دستورات زیر نیز برای بررسی مسیرهای سیستمی در درایوهای موجود استفاده می‌شود:

```
60  main_GetSystemDirectory();
61  result = v29;
62  if ( !v35 )
63  {
64    v44 = v32;
65    v51 = v29;
66    v36 = path_filepath_volumeNameLen(v29, v32);
67    if ( v36 > v44 )
68      runtime_panicSliceAlen(v30, v33);
69    v54 = (int)"\b";
70    v55 = runtime_convTstring(v51, v36);
71    v50 = fmt_Sprintf((int)"%s\\", 3, (int)&v54, 1, 1);
72    main_drives();
```

```
95  v40 = fmt_Sprintf((int)"%s\\drivers", 10, (int)&v54, 1, 1);
122 v41 = fmt_Sprintf((int)"%sWindows\\NTDS", 14, (int)&v54, 1, 1);
```

قطعه کدهای بالا نشان می‌دهد که به صورت خاص بدافزار به مسیر C:\Windows\ حمله می‌کند و در درون این مسیر نیز نگاه ویژه‌تری به دو مسیر C:\Windows\System32\drivers و C:\Windows\NTDS برای تخریب دارد. (تابع GetSystemDirectory محتویات پوشه‌ی C:\Windows را برمی‌گرداند.)

پس از بررسی چند نمونه فایل سالم با نمونه رونویسی‌شده با کاراکتر تصادفی مشخص گردید که تمام پسوندهای فایل‌ها توسط این بدافزار مورد حمله قرار می‌گیرند و از ابتدای هر فایل شروع شده و هر ۴۰۹۶ بایت یک بلوک کاراکتر تصادفی را برروی فایل قربانی می‌نویسد:




## ۲-۶ تحلیل ترافیک شبکه

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

# ۷ شناسه‌های تهدید (IOCs)

Samples:

| |
|---|
| *MD5: fee7c379f3a555c5c821e872ec384a91* |

Detection names:

| |
|---|
| *Kaspersky: Trojan.Win32.DelShad.kiw* |
| *Bitdefender: Generic.Trojan.Wiper.B.ADD137E4* |
| *ESET: A Variant Of WinGo/KillFiles.C* |
| *Windows Defender: DoS:Win32/LeopardBlade.A!dha* |

# ۸ شناسایی (Detection)

- با توجه به اینکه بدافزار SwiftSlicer 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 بدافزار SwiftSlicer در فاصله زمانی کوتاهی، فایل‌های زیادی را در سیستم قربانی حذف می‌کند، این رفتار را که معمولاً در Wiperها مشاهده می‌شود می‌توان به عنوان یک رفتار مشکوک در سیستم‌عامل در نظر گرفت که با کوئری زیر در اسپلانک قابل شناسایی است:

```
index="sysmon" EventCode=23 (TargetFilename="*.exe" OR TargetFilename="*.sys" OR TargetFilename="*.dll")
 |stats values(TargetFilename) AS deleted_files min(_time) AS firstTime max(_time) AS lastTime count by ComputerName, User, EventCode, Image
 |where (count >= 100)
 |convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
 |convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```