

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 Nevada

### گزارش فنی

شناسه سند ..... MaherReports\_14020118  
نوع سند ..... گزارش فنی  
شماره نگارش ..... ۰,۱  
تاریخ نگارش ..... ۱۴۰۲/۰۱/۱۸  
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
۲	شجره نامه	۳
۲	میزان تهدید فایل باج افزار	۴
۳	تحلیل پویا	۵
۳	۱-۵ آناتومی حمله	
۸	۲-۵ روش انتشار	
۸	۳-۵ روش مقابله	
۸	تحلیل ایستا	۶
۸	۱-۶ تحلیل کد	
۱۳	۲-۶ تحلیل ترافیک شبکه	
۱۳	۷ شناسه های تهدید (IOCs)	

## ۱ مقدمه

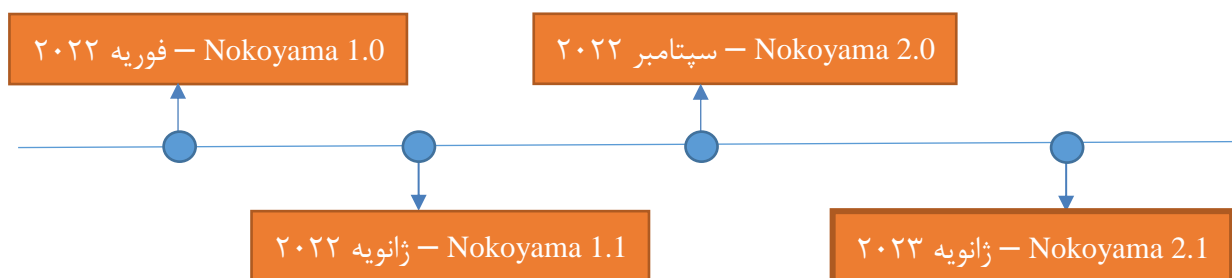
در ابتدای فوریه ۲۰۲۳ (میان بهمن ۱۴۰۱) باج افزار Nevada در حملاتی در سطح اینترنت دیده شد. نمونه تحلیل شده در این گزارش، اولین انتشار از باج افزار Nevada پس از فعال سازی سیستم RaaS خود در دسامبر ۲۰۲۲ بوده است و در ژانویه ۲۰۲۳ ساخت آن به اتمام رسیده است. طبق بررسی های صورت گرفته، باج افزار Nevada گونه ای از خانواده باج افزار Nekoyawa است. این باج افزار برای فعالیت خود احتیاجی به اتصال به اینترنت ندارد و چه با دسترسی مدیر سیستم (Administrator) و چه بدون آن، اطلاعات سیستم را رمزگذاری می کند. الگوریتم رمزنگاری این باج افزار از نوع X25519 بعلاوه Salsa20 می باشد. طبق نتایج بدست آمده نشان می دهد که ظاهراً هدف باج افزار Nevada یک یا چند گروه خاص نمی باشد.

## ۲ مشخصات فایل اجرایی

855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808.exe	نام فایل
99549bcea63af5f81b01decf427519af	MD5
c7fcbaedf6b077b3d9bfc4720c3860a5d848bcb4	SHA-1
855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808	SHA-256
Win32 EXE (PE64)	نوع فایل
506.00 KB (518144 bytes)	اندازه فایل

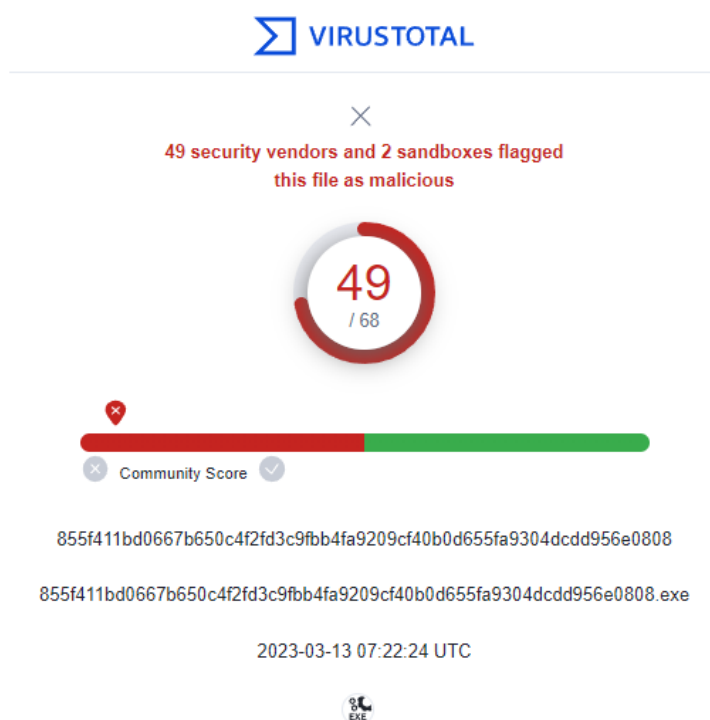
## ۳ شجره نامه

طبق بررسی‌های صورت گرفته، به نظر می‌رسد باج‌افزار Nevada آپدیتی از گروه Nokoyawa است و شاید حتی بتوان آن را Nokoyama 2.1 نامید. خانواده Nokoyama از نوع RaaS می‌باشد. نمونه مورد استفاده در این گزارش، اولین و تنها مورد از مشاهده این باج‌افزار تا زمان نوشتن این تحلیل می‌باشد.



## ۴ میزان تهدید فایل باج‌افزار

در حال حاضر ۴۹ مورد از ۶۸ ضد بدافزار سامانه VirusTotal باج‌افزار Nevada را به عنوان یک برنامه مخرب شناسایی می‌کنند:



## ۵ تحلیل پویا

### ۱-۵ آناتومی حمله

پس از اجرای باج افزار Nevada در محیط آزمایشگاهی، مشاهده شد که این باج افزار هم بر روی ماشین مجازی و هم فیزیکی اجرا می شود و رفتارهای زیر را نشان می دهد.

explorer.exe	< 0.01	67,196 K	142,652 K	6704	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		2,040 K	9,136 K	9980	Windows Security notificatio...	Microsoft Corporation
vmtoolsd.exe	< 0.01	23,816 K	33,192 K	9840	VMware Tools Core Service	VMware, Inc.
OneDrive.exe		21,920 K	51,712 K	10212	Microsoft OneDrive	Microsoft Corporation
procexp64.exe	1.10	25,152 K	49,080 K	8940	Sysinternals Process Explorer	Sysinternals - www.sysinter...
855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcd956e0808.exe	17.28	4,296 K	7,232 K	9312		
conhost.exe	0.37	7,156 K	18,364 K	8956	Console Window Host	Microsoft Corporation

باج افزار به عنوان زیر پراسسی از explorer.exe اجرا می شود و از لحظه اجرا تا انتها، روند اجرای خود را در محیط CMD به نمایش می گذارد:

```

C:\Users\Apa\Downloads\855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcd956e0808.exe
Created thread: 0
Created thread: 2
Total threads: 8
Created thread: 1
Created thread: 3
Created thread: 4
Created thread: 5
Created thread: 6
Created thread: 7
C:\ working drive
D:\ working drive
C:\readme.txt
C:\$Recycle.Bin\readme.txt
C:\$Recycle.Bin\S-1-5-18\readme.txt
C:\$Recycle.Bin\S-1-5-21-1153584407-1743598643-1221634055-1000\readme.txt
C:\$Recycle.Bin\S-1-5-21-1153584407-1743598643-1221634055-1001\readme.txt
C:\$WinREAgent\readme.txt
C:\$WinREAgent\Scratch\readme.txt
C:\Documents and Settings\readme.txt
Failed to read directory: permission denied
C:\PerfLogs\readme.txt
C:\Recovery\readme.txt
C:\Recovery\OEM\readme.txt
C:\Users\readme.txt
C:\Users\All Users\readme.txt
C:\Users\All Users\Aomei\readme.txt
C:\Users\All Users\AomeiBR\readme.txt
C:\Users\All Users\AomeiBR\cb\readme.txt
C:\Users\All Users\AomeiBR\cb\cache\readme.txt
C:\Users\All Users\AomeiBR\cb\config\readme.txt

```

این اطلاعات شامل ساخت و تعداد رشته های فعال در فرآیند، درایوهایی که قرار است فایل های درون آنها رمزنگاری شوند، قرار دادن فایل readme.txt در دایرکتوری ها و خطاهای موجود می باشد.

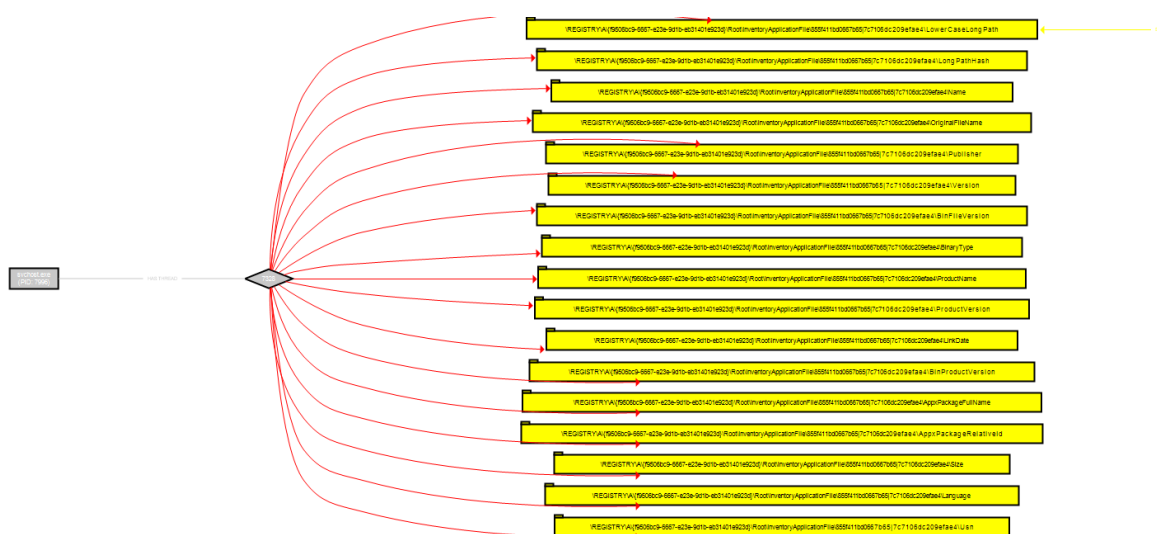
طبق نتایج بدست آمده در محیط آزمایشگاهی، این نمونه از باج افزار Nevada اطلاعات درون فضای VSS ویندوز را دست کاری نمی کند. با این حال باج افزار مذکور برای اجرای کامل می بایست دسترسی ادمین داشته باشد، در غیر این صورت نمی تواند در برخی دایرکتوری ها به طور کامل عملیات خود را پیاده سازی کند:

```

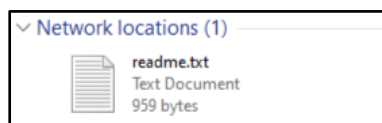
C:\readme.txt
Failed to create ransom note
C:\$Recycle.Bin\readme.txt
Failed to create ransom note
C:\$Recycle.Bin\S-1-5-21-1153584407-1743598643-1221634055-1001\readme.txt
C:\$WinREAgent\readme.txt
Failed to create ransom note
C:\$WinREAgent\Scratch\readme.txt
Failed to create ransom note
C:\Documents and Settings\readme.txt
Failed to create ransom note
Failed to read directory: permission denied

```

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



باج‌افزار در هنگام اجرا پس از عبور از هر دایرکتوری پیغام باج‌خواهی خود تحت عنوان readme.txt را در آن قرار می‌دهد و همچنین یک نسخه از این فایل نیز در شبکه به اشتراک گذاشته می‌شود.



متن درون فایل readme.txt بدین گونه است:

```

readme.txt - Notepad
File Edit Format View Help
Greetings! Your files were stolen and encrypted.

You have two ways:

    -> Pay a ransom and save your reputation.
    -> Wait for a miracle and lose precious time.

We advise you not to wait.

After 2 days of your silence we will make a call your superiors and notificated them about what's happened.

After another 2 days all your competitors will be informed about your decision.

Finally, after 3 days we will post your critical data on our TOR-website.

If you are going to recover your files from backups and forget this like a nightmare, we are hurry to inform you - you can't prevent a leak.

Recommendations:

    -> Don't delete/rename encrypted files
    -> Don't use any public "decryptor", they contain viruses.

You have to download TOR browser.

To contact with us your can use the following link:

    http://nevcorps5cvivjf6i2gm4uia7cxng5ploqny2rgrinctazjlnqr2yiyd.onion/63bb5b5ff541280c4bc116f2

The cat is out of the bag.
Ln 1, Col 1      100% Windows (CRLF) UTF-8

```

در متن باج باج افزار Nevada به موارد زیر اشاره شده است:

فایل های شما دزدیده و رمز گذاری شده اند و دو راه پیشنهاد می دهد که یکی پرداخت باج و حفظ شهرت است و دیگری صبر برای معجزه و از دست دادن تایم با ارزش است.

آن ها توصیه می کنند که صبر کردن را انتخاب نکنید چون بعد از ۲ روز اگر شما گزارشی ندهید خودمان با سرپرست تان تماس می گیریم و شرح حال می کنیم؛ بعد از ۲ روز دیگر نیز همه ی رقبای شما از تصمیم شما باخبر خواهند شد؛ در نهایت بعد از ۳ روز اطلاعات حیاطی شما را در وبسایت TOR خودمان منتشر می کنیم.

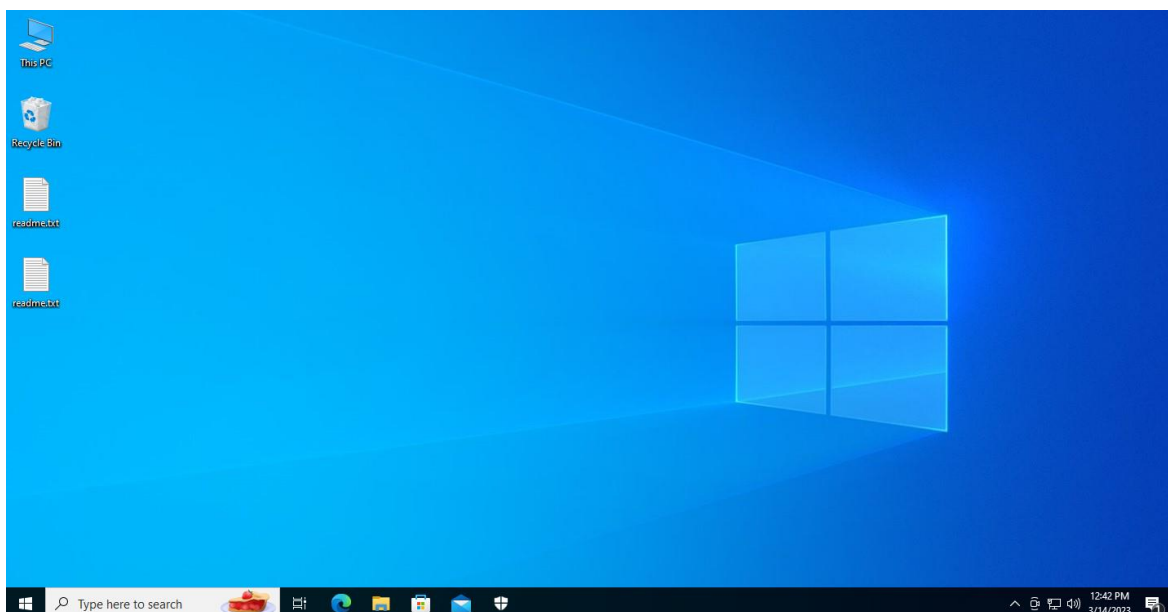
همچنین تهدید می کنند که اگر می خواهید فایل های خود را از طریق پشتیبان گیری ها بازیابی کنید، آن را فراموش کنید چون که با این کار از انتشار آنها جلوگیری نمی شود.

دو توصیه دیگر هم ارائه می دهند که "فایل ها را پاک نکنید یا تغییر نام ندهید" و "از رمزگشاهای عمومی استفاده نکنید که حاوی ویروس می باشند" می باشد.

سازندگان باج افزار Nevada، راه ارتباطی قربانیان که از طریق لینکی در TOR می باشد را نیز در متن پیغام باج خواهی قرار داده اند.

جمله آخر نیز ضرب المثلی است به معنی "ماجرا لو رفته است" می باشد.

باچ‌افزار Nevada پس از حمله به سیستم قربانی، تغییری در صفحه دسکتاپ را ایجاد نمی‌کند. (فقط اگر با دسترسی ادمین اجرا نشود روی دسکتاپ تنها یک فایل متنی مربوط به باچ قرار می‌گیرد.)



باچ‌افزار Nevada پس از اتمام اجرا، فایل اجرایی خود را پاک نمی‌کند:

Name	Date modified	Type	Size
▼ Today (10)			
<input checked="" type="checkbox"/> 855f411bd0667b650c4f2fd3c9fbb4fa92...	3/4/2023 8:50 AM	Application	506 KB
<input type="checkbox"/> 855f411bd0667b650c4f2fd3c9fbb4fa92...	3/4/2023 4:15 PM	NEVADA File	249 KB
<input checked="" type="checkbox"/> acc31048e00d1a0f4cd5569d5d4db539...	3/4/2023 8:49 AM	Application	506 KB
<input type="checkbox"/> acc31048e00d1a0f4cd5569d5d4db539...	3/4/2023 4:15 PM	NEVADA File	247 KB
<input type="checkbox"/> BlackCat.rar.NEVADA	3/4/2023 4:15 PM	NEVADA File	15,223 KB
<input type="checkbox"/> DarkBit.zip.NEVADA	3/4/2023 4:15 PM	NEVADA File	2,030 KB
<input type="checkbox"/> Makop.rar.NEVADA	3/4/2023 4:15 PM	NEVADA File	6,849 KB
<input type="checkbox"/> Phobos.rar.NEVADA	3/4/2023 4:15 PM	NEVADA File	888 KB
<input type="checkbox"/> readme.txt	3/4/2023 4:15 PM	Text Document	1 KB
<input type="checkbox"/> SwiftSlicer.zip.NEVADA	3/4/2023 4:15 PM	NEVADA File	716 KB

فایل‌هایی که با این باچ‌افزار رمزگذاری می‌شوند با الگوی "own-filename.extention.NEVADA" نام‌گذاری می‌شوند که به عبارتی تنها NEVADA. به انتهای فایل اضافه می‌شود:



Name	Date modified	Type	Size
readme.txt	3/4/2023 12:34 PM	Text Document	1 KB
Test (1).deb.NEVADA	3/4/2023 12:34 PM	NEVADA File	226 KB
Test (1).doc.NEVADA	3/4/2023 12:34 PM	NEVADA File	71 KB
Test (1).exe	6/16/2019 4:25 AM	Application	129 KB
Test (1).jfif.NEVADA	3/4/2023 12:34 PM	NEVADA File	1,461 KB
Test (1).jpg.NEVADA	3/4/2023 12:34 PM	NEVADA File	1,413 KB
Test (1).mkv.NEVADA	3/4/2023 12:34 PM	NEVADA File	1,070,886 KB
Test (1).mp4.NEVADA	3/4/2023 12:34 PM	NEVADA File	143,758 KB
Test (1).pdf.NEVADA	3/4/2023 12:34 PM	NEVADA File	955 KB
Test (1).rar.NEVADA	3/4/2023 12:34 PM	NEVADA File	888 KB
Test (1).sh.NEVADA	3/4/2023 12:34 PM	NEVADA File	258,718 KB
Test (1).txt.NEVADA	3/4/2023 12:34 PM	NEVADA File	31 KB
Test (1).xls.NEVADA	3/4/2023 12:34 PM	NEVADA File	75 KB
Test (1).zip.NEVADA	3/4/2023 12:34 PM	NEVADA File	5,470 KB
Test (2).jpg.NEVADA	3/4/2023 12:34 PM	NEVADA File	3,402 KB
Test (2).txt.NEVADA	3/4/2023 12:34 PM	NEVADA File	301 KB
Test (3).exe	10/23/2022 10:41 AM	Application	1,035 KB
Test (3).jpg.NEVADA	3/4/2023 12:34 PM	NEVADA File	3,593 KB
Test (3).txt.NEVADA	3/4/2023 12:34 PM	NEVADA File	3,073 KB
Test (4).exe	11/6/2022 12:26 PM	Application	76,842 KB
Test (4).jpg.NEVADA	3/4/2023 12:34 PM	NEVADA File	5,269 KB
Test (5).exe	10/23/2022 10:42 AM	Application	101,581 KB
Test (5).jpg.NEVADA	3/4/2023 12:34 PM	NEVADA File	6,099 KB
Test (6).jpg.NEVADA	3/4/2023 12:34 PM	NEVADA File	9,937 KB
Test (7).jpg.NEVADA	3/4/2023 12:34 PM	NEVADA File	15,435 KB

بررسی‌ها نشان می‌دهد، فایل‌های با پسوندهای زیر توسط باج‌افزار NEVADA رمزگذاری نمی‌شوند:

پوشه‌ها	پسوندها
Windows	exe
Program Files	ini
Program Files (x86)	dll
AppData	url
Programdata	lnk
System volume information	scr

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

## ۲-۵ روش انتشار

هدف باج‌افزار Nevada از حمله، ایجاد بیشترین آلودگی و قربانی است و خط‌مشی خاصی ندارد. این باج‌افزار به‌نظر می‌رسد که از طریق ایمیل‌های فیشینگ منتشر می‌شود و یا بصورت ماکرو در اسناد آفیس قرار داده می‌شود که در صورت غیرفعال بودن آنتی‌ویروس و اجرای مستقیم یا فعال‌سازی ماکروها در اسناد اجرا می‌شود.

## ۳-۵ روش مقابله

باج‌افزار Nevada هم‌اکنون در صورت فعال بودن لایه‌ی محافظتی Windows Defender یا بیشتر ضد بدافزارهای 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، با محدودسازی فایل‌های اجرایی که می‌توان از اجرای باج‌افزار بصورت ناخواسته جلوگیری کرد.

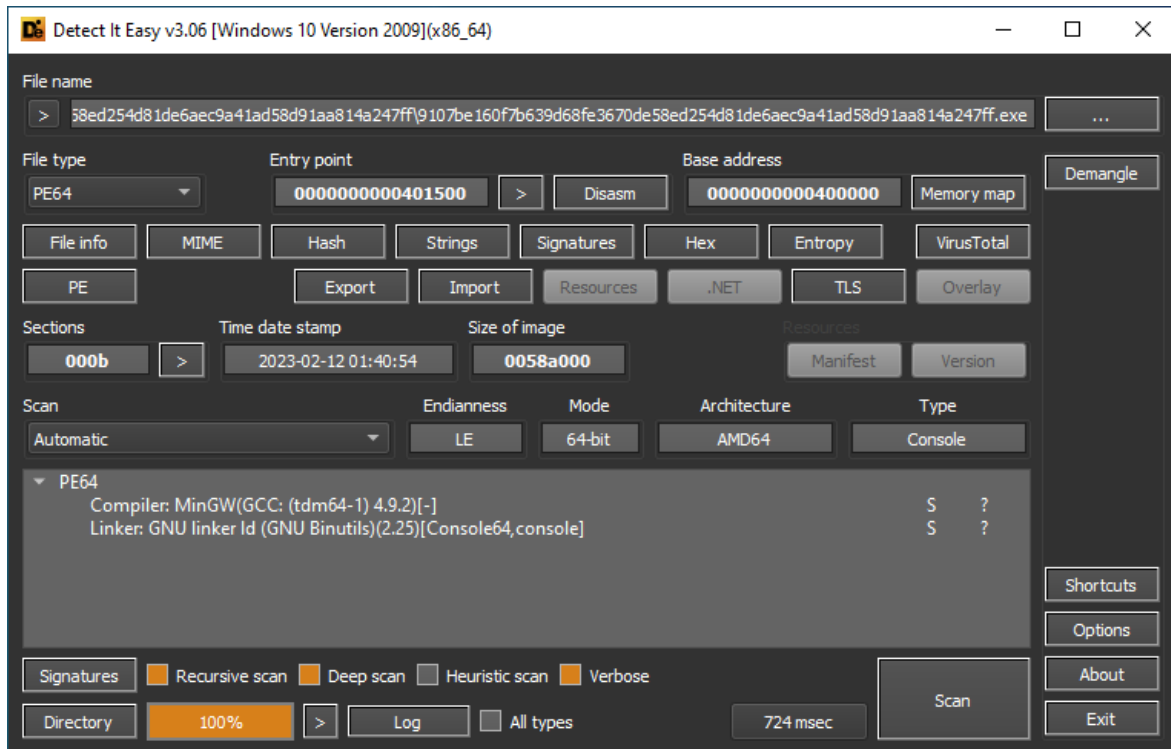
## ۶ تحلیل ایستا

بررسی‌ها بر روی نمونه تست شده باج‌افزار Nevada نشان می‌دهد که باج‌افزار مذکور بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از ۷ یا ویندوز سرور ۲۰۰۸ به بعد به شرط ۶۴ بیتی بودن، اجرا خواهد شد.

os-version	6.0	Windows Server 2008
image-version	0.0	0.0
subsystem-version	6.0	6.0
machine	0x8664	Amd64

## ۱-۶ تحلیل کد

طبق بررسی‌های صورت گرفته، کد باج‌افزار Nevada 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 مبهم‌سازی (Obfuscate) 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
۴	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 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 برمی‌گرداند
۲	مقدار فعلی شمارنده عملکرد را بازیابی می‌کند که می‌تواند برای اندازه‌گیری بازه زمانی استفاده شود
۳	فرکانس شمارنده عملکرد را بازیابی می‌کند که به کمک قبلی برای اندازه‌گیری زمان استفاده می‌شود

پس از اینکه فایل PE برنامه را بصورت ASCII جستجو می‌کنیم به چند فایل json برمی‌خوریم 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 مگابایتِ فایلِ 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,
  "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.

```

"hostnames": [
  "TD-EF-DC.ef.technion.ac.il",
  "td-ef-main.ef.technion.ac.il",
  "td-ef-mainc.ef.technion.ac.il",
  "T-BM-DC2.bm.technion.ac.il",
  "T-BM-DC3.bm.technion.ac.il",
  "TD-SI-DC.si.technion.ac.il",
  "td-si-dc2.si.technion.ac.il",
  "td-st-dc.st.technion.ac.il",
  "TD-ST-DC2.st.technion.ac.il",
  "TD-AE-aeneid.ae.technion.ac.il",
  "td-ae-aeolus.ae.technion.ac.il",
  "TD-ME-DC01.me.technion.ac.il",
  "TD-ME-DC2.me.technion.ac.il",
  "TDSAPDC.sap.technion.ac.il",
  "tdsapdc2.sap.technion.ac.il",
  "Tech-Med-BK2019.medicine.technion.ac.il",
  "Tech-Med-DC2019.medicine.technion.ac.il",
  "Staff-DC1.staff.technion.ac.il",
  "STAFF-DC2.staff.technion.ac.il",
  "staff-dc3.staff.technion.ac.il",
  "TD-CC-ROOT.cc.technion.ac.il",
  "TD-CC-ROOTC.cc.technion.ac.il",
  "td-cc-rootd.cc.technion.ac.il",
  "dadp.csf.technion.ac.il",
  "DAPHP.csf.technion.ac.il",
  "PAD6.csf.technion.ac.il",
  "RAD.csf.technion.ac.il",
  "TD-TR-DC1.tr.technion.ac.il",
  "TD-TR-DC3.tr.technion.ac.il",
  "TD-MA-DC",
  "TD-MA-DC3",
  "IEM-DC1",
  "IEM-DC2",
  "TD-CE-DANY1",
  "TD-CE-DANY2",
  "CIS-Shayol",
  "CIS-ritar",
  "cis-rafish",
  "VM-VEEAM-MGT",
  "cis-stav",
  "Dean-NaamaD",
  "Dorm-Einav",
  "HR-ORLICG.staff",
  "Dean-NaamaD"
]

```

به نظر می‌رسد محتویات hostnames برای حمله از طریق Active Directory به دیگر سیستم‌های موجود در شبکه بوده است و می‌توان دوباره پی برد که این سمپل به‌طور ویژه برای دانشگاه Technion نوشته شده است. پس از بررسی چند نمونه فایل سالم با نمونه رمزنگاری شده مشخص شد که پس از عملیات رمزنگاری مقدار 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:

50TPLxh1676962041.Darkbit																
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
00011810	44	5f	46	49	4c	45	53	7c	ad	86	b4	4d	12	9b	3e	7f
00011820	4b	2c	8d	2d	e8	1a	44	14	44	41	52	4b	42	49	54	2b
00011830	21	e4	ef	7d	3b	1e	25	98	8e	aa	b4	35	07	84	62	d7
00011840	d6	ae	22	b4	ec	c8	d7	d7	78	fa	7b	9c	db	78	fb	c1
00011850	25	7d	11	56	e4	0a	8f	cc	1f	52	a8	00	7c	d6	bb	be
00011860	26	19	35	1c	71	c8	09	46	82	7f	d4	4c	1c	3a	74	c5
00011870	56	69	df	d3	e7	97	ef	57	53	02	78	ac	62	f0	e5	6d
00011880	24	27	ef	e0	a4	e6	c5	a7	99	71	70	76	44	19	6e	5b
00011890	d4	85	0c	b4	be	80	c7	6d	f2	49	c3	93	98	4e	06	9a
000118a0	3f	df	2d	bf	c2	01	d1	83	bb	45	1d	21	3a	21	7b	ac
000118b0	eb	ca	0b	1c	54	5d	0e	4d	14	bb	bc	51	b6	cc	dc	8d
000118c0	24	9e	a4	1f	6f	75	a7	e2	6e	67	3e	bd	44	eb	f7	0e
000118d0	b7	12	a4	8f	44	5c	64	2c	15	8b	d7	e0	ae	bf	c6	85
000118e0	6d	39	c4	08	ee	e1	df	77	dd	ac	30	be	a3	64	9f	8a
000118f0	d4	c8	23	9c	0f	b6	24	01	ad	20	e2	0c	7e	f7	6c	44
00011900	d1	1c	5f	44	b7	ec	7f	41	5b	37	0a	c9	9f	49	b3	8a
00011910	02	79	8f	0b	b4	6c	3e	d9	2c	d0	21	ef	aa	2d	f3	71
00011920	22	bb	1c	b5	e0	e0	82	fb	10	f6	fc	a9	58	bd	dd	..
00011930	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..	..

## ۲-۶ تحلیل ترافیک شبکه

پس از بررسی ترافیک شبکه ضبط شده پس از اجرای باج افزار Nevada و همچنین بررسی نتایج سندباکس های آنلاین، هیچ گونه ارتباط شبکه ای در مورد باج افزار مشاهده نشد و این سمپل کاملاً آفلاین فعالیت می کند.

## ۷ شناسه های تهدید (IOCs)

Samples:

**SHA256:** 855f411bd0667b650c4f2fd3c9fbb4fa9209cf40b0d655fa9304dcdd956e0808

Ransom Note:

*readme.txt*

Detection names:

**Kaspersky:** Trojan-Ransom.Win32.Encoder.tmm

**BitDefender:** Trojan.GenericKD.65749092

**ESET:** Win64/Filecoder.HH

**Windows Defender:** Ransom:Win64/Nevada