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 Nevada

گزارش فنی

شناسه سند	MaherReports_14020118
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۴۰۲/۰۱/۱۸
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

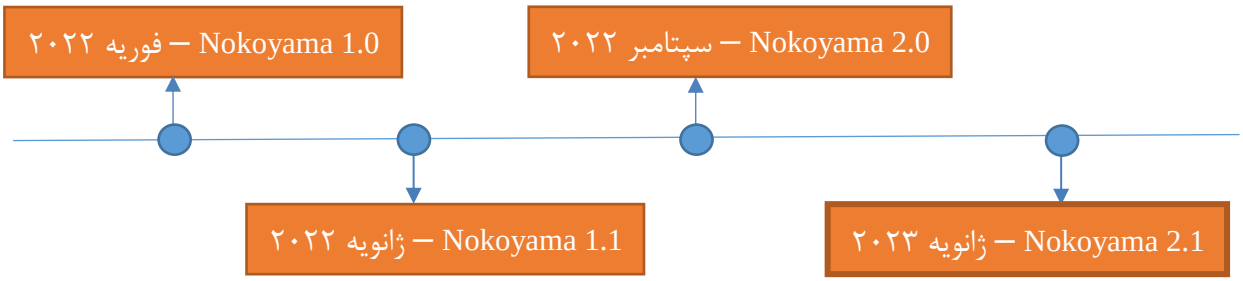
در ابتدای فوریه ۲۰۲۳ (میانه بهمن ۱۴۰۱) باج‌افزار Nevada در حملاتی در سطح اینترنت دیده شد. نمونه تحلیل شده در این گزارش، اولین انتشار از باج‌افزار Nevada پس از فعال‌سازی سیستم RaaS خود در دسامبر ۲۰۲۲ بوده است و در ژانویه ۲۰۲۳ ساخت آن به اتمام رسیده است. طبق بررسی‌های صورت گرفته، باج‌افزار Nevada گونه‌ای از خانواده باج‌افزار Nekoyawa است. این باج‌افزار برای فعالیت خود احتیاجی به اتصال به اینترنت ندارد و چه با دسترسی مدیر سیستم (Administrator) و چه بدون آن، اطلاعات سیستم را رمزگذاری می‌کند. الگوریتم رمزنگاری این باج‌افزار از نوع X25519 بعلاوه Salsa20 می‌باشد. طبق نتایج بدست آمده نشان می‌دهد که ظاهراً هدف باج‌افزار Nevada یک یا چند گروه خاص نمی‌باشد.

۲ مشخصات فایل اجرایی

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

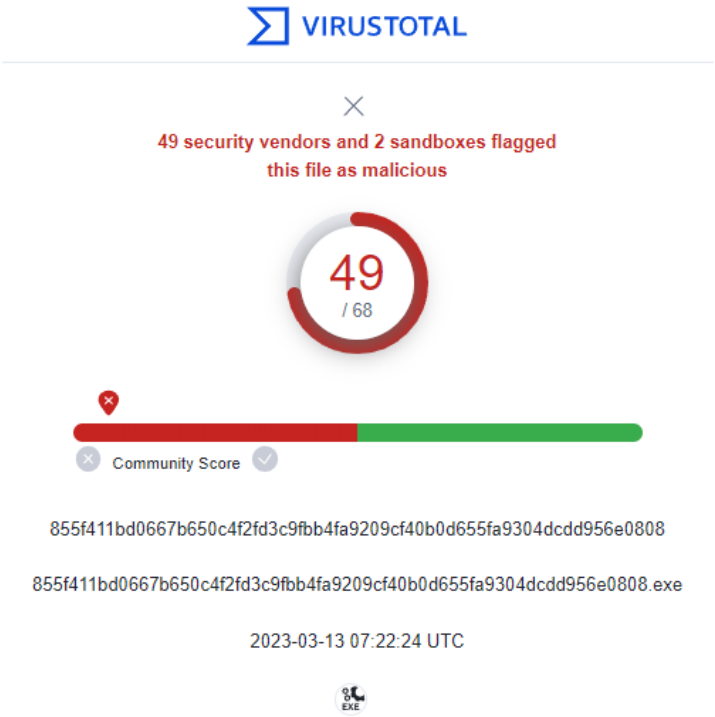
۳ شجره‌نامه

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

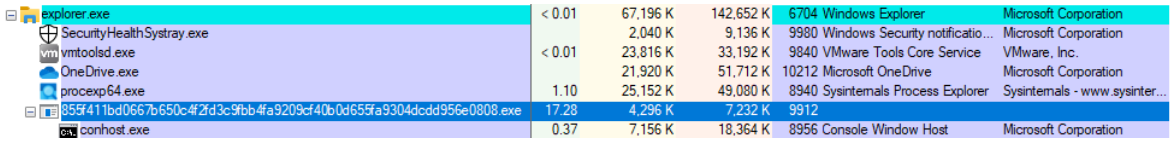
درحال حاضر ۴۹ مورد از ۶۸ ضد بدافزار سامانه VirusTotal باج‌افزار Nevada را به عنوان یک برنامه مخرب شناسایی می‌کنند:



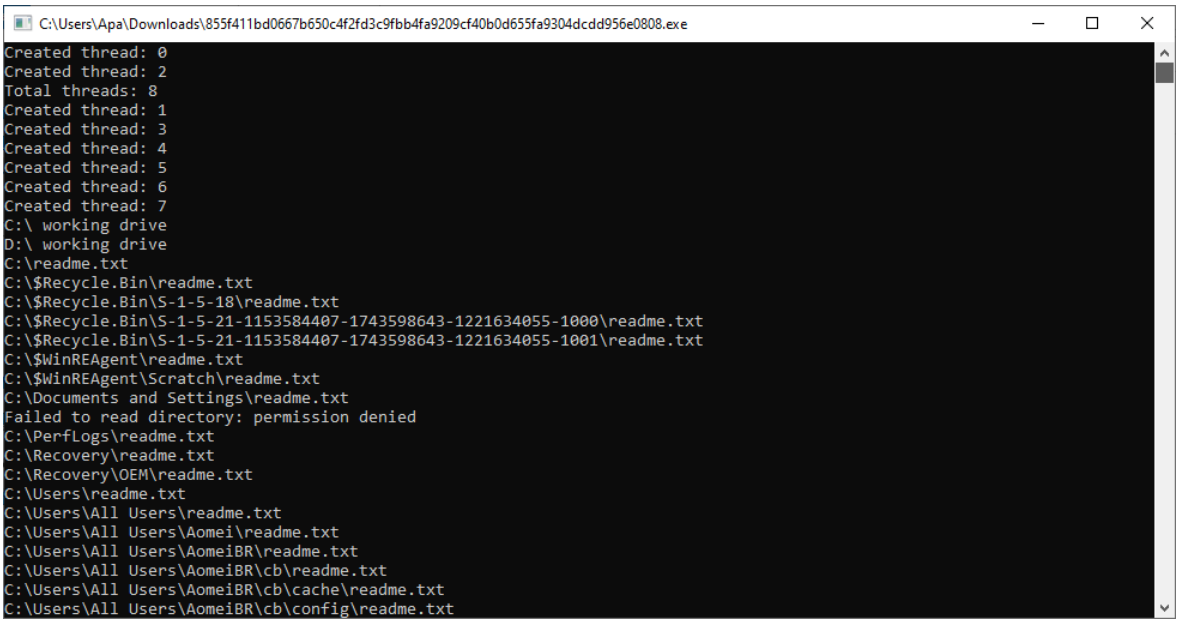
۵ تحلیل پویا

۵-۱ آناتومی حمله

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



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:

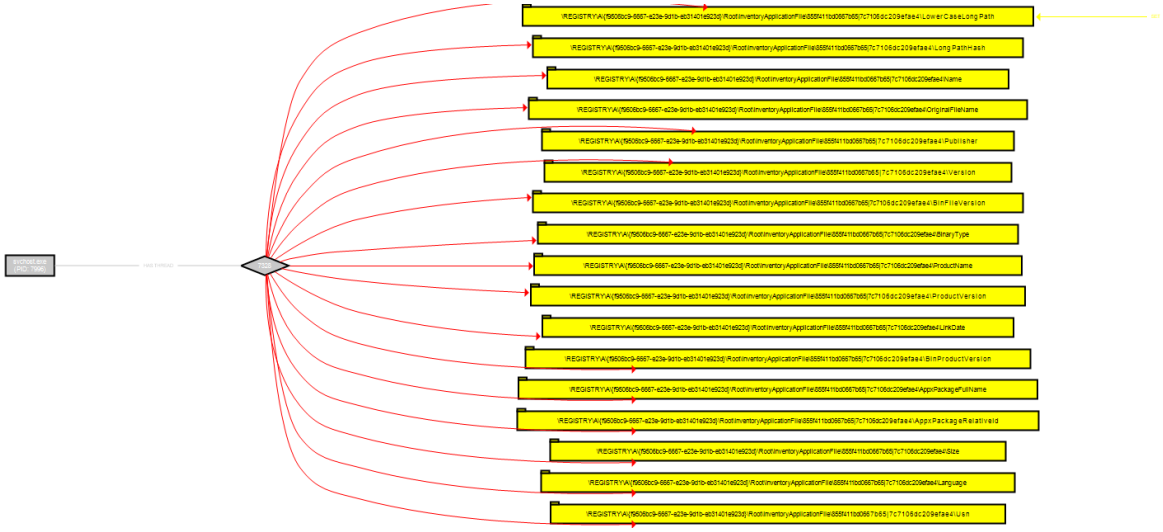


این اطلاعات شامل ساخت و تعداد رشته‌های فعال در فرآیند، درایوهایی که قرار است فایل‌های درون آن‌ها رمزنگاری شوند، قرار دادن فایل readme.txt در دایرکتوری‌ها و خطاهای موجود می‌باشد.

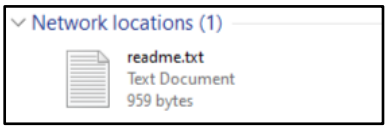
طبق نتایج بدست آمده در محیط آزمایشگاهی، این نمونه از باج‌افزار Nevada اطلاعات درون فضای VSS ویندوز را دست‌کاری نمی‌کند. با این حال باج‌افزار مذکور برای اجرای کامل می‌بایست دسترسی ادمین داشته باشد، در غیر این صورت نمی‌تواند در برخی دایرکتوری‌ها به طور کامل عملیات خود را پیاده‌سازی کند:

```
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
```

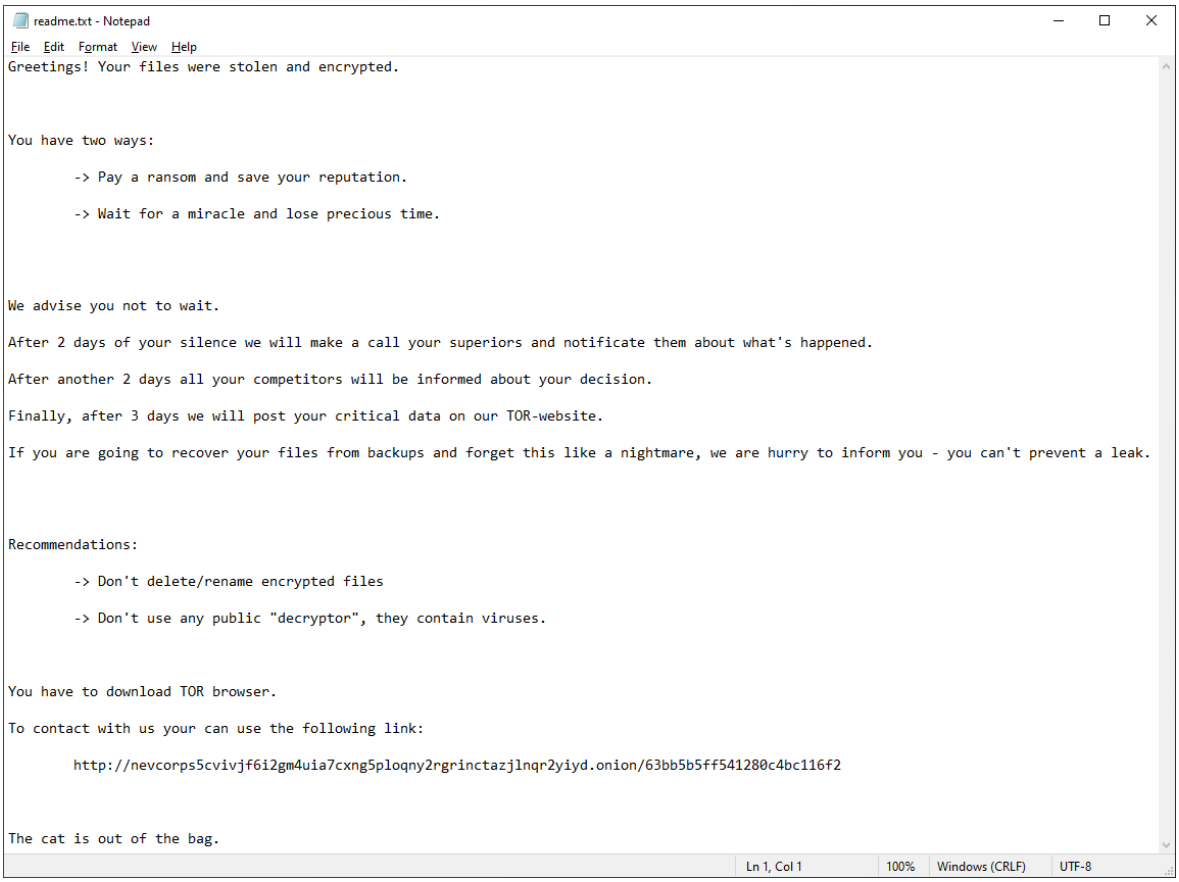
بررسی‌های انجام شده در محیط آزمایشگاهی نشان می‌دهد که باج‌افزار Nevada با فایل‌ها سر و کار دارد، بنابراین با یک‌سری کلیدهای رجیستری مرتبط با آن ارتباط برقرار می‌کند:



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 redme.txt بدین گونه است:



در متن باجِ باج‌افزار Nevada به موارد زیر اشاره شده است:

فایل‌های شما دزدیده و رمزگذاری شده‌اند و دو راه پیشنهاد می‌دهد که یکی پرداخت باج و حفظ شهرت است و دیگری صبر برای معجزه و از دست دادن تایم باارزش است.

آن‌ها توصیه می‌کنند که صبر کردن را انتخاب نکنید چون بعد از ۲روز اگر شما گزارشی ندهید خودمان با سرپرست‌تان تماس می‌گیریم و شرح حال می‌کنیم؛ بعد از ۲روز دیگر نیز همه‌ی رقبای شما از تصمیم شما باخبر خواهند شد؛ در نهایت بعد از ۳روز اطلاعات حیاطی شما را در وبسایت TOR خودمان منتشر می‌کنیم.

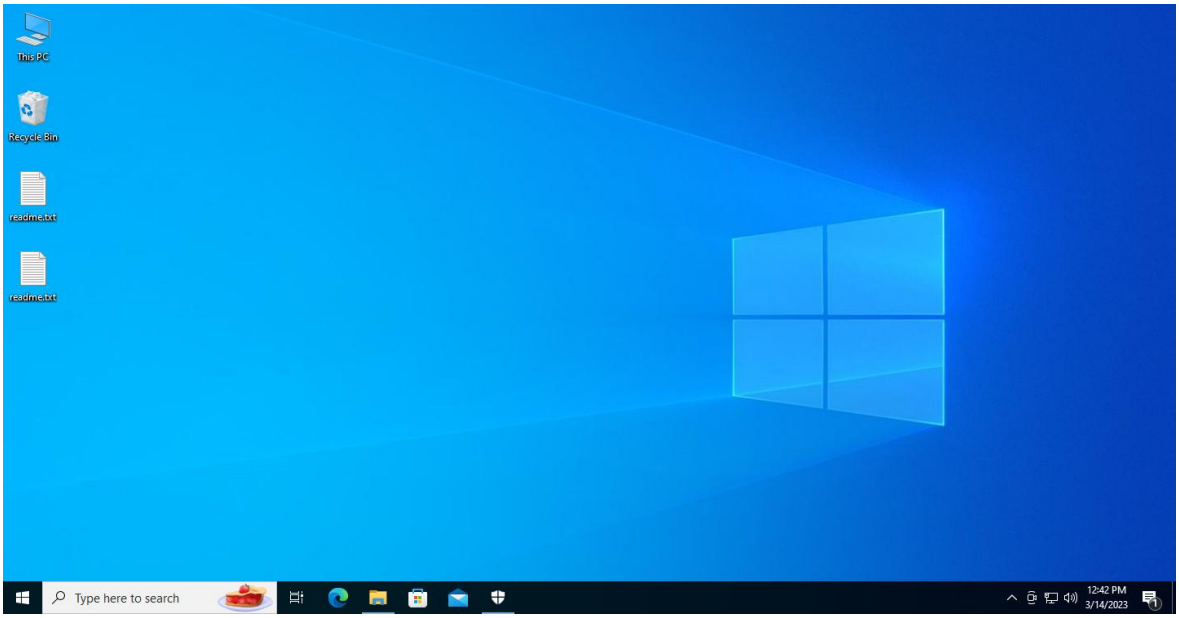
همچنین تهدید می‌کنند که اگر می‌خواهید فایل‌های خود را از طریق پشتیبان‌گیری‌ها بازیابی کنید، آن را فراموش کنید چون که با این کار از انتشار آنها جلوگیری نمی‌شود.

دو توصیه دیگر هم ارِائه می‌دهند که "فایل‌ها را پاک نکنید یا تغییر نام ندهید" و "از رمزگشاهای عمومی استفاده نکنید که حاوی ویروس می‌باشند" می‌باشد.

سازندگان باج‌افزار Nevada، راه ارتباطی قربانیان که از طریق لینکی در TOR می‌باشد را نیز در متن پیغام باج‌خواهی قرار داده‌اند.

جمله آخر نیز ضرب‌المثلی است به معنی "ماجرا لو رفته است" می‌باشد.

باج‌افزار 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 باج قرار می‌گیرد.)



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

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

فایل‌هایی که با این باج‌افزار 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:

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

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

۵-۲ 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 می شود که درصورت غیرفعال بودن آنتی‌ویروس و اجرای مستقیم یا فعال‌سازی ماکروها در اسناد اجرا می‌شود.

۵-۳ 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

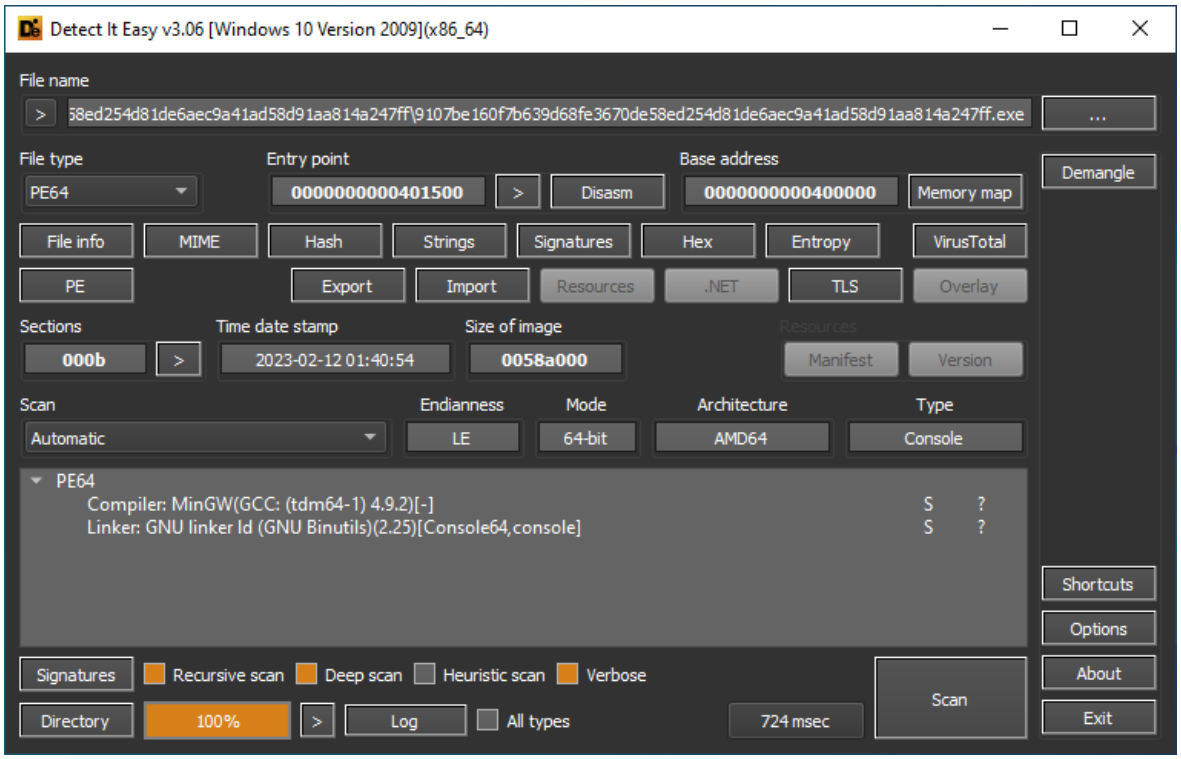
بررسی‌ها بر روی نمونه تست شده باج‌افزار Nevada نشان می‌دهد که باج‌افزار مذکور بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از ۷ یا ویندوز سرور ۲۰۰۸ به بعد به شرط ۶۴ بیتی بودن، اجرا خواهد شد.

os-version	6.0	Windows Server 2008
image-version	0.0	0.0
subsystem-version	6.0	6.0

machine	0x8664	Amd64

۶-۱ 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");
32  if ( !ProcAddress )
33    return 0i64;
34  v4 = GetProcAddress(v2, "RmRegisterResources");
35  if ( !v4 )
36    return 0i64;
37  v5 = GetProcAddress(v2, "RmGetList");
38  if ( !v5 )
39    return 0i64;
40  v6 = GetProcAddress(v2, "RmShutdown");
41  if ( !v6 )
42    return 0i64;
43  v7 = GetProcAddress(v2, "RmEndSession");
```

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
٥	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");
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");
48  v10 = sub_42C8E0(0x18ui64, 0x726550797265551i64, 0x7265746E756F43i64, v9);
49  if ( dword_976970 )
50    sub_457E60(v11);
51  else
52    qword_91E7A8 = v10;
53  strcpy(v30, "QueryPerformanceFrequency");
54  v14 = sub_42C8E0(0x1Aui64, 0x79636E65757161[illegible], 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 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.

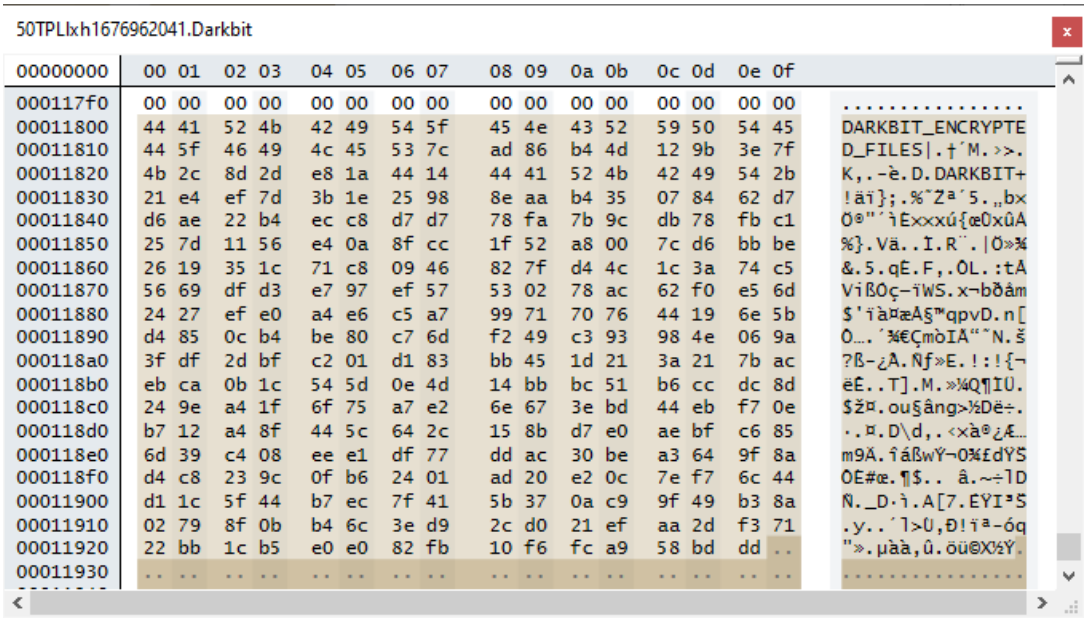
```
"names": {
    "thumbs.db": 1,
    "desktop.ini": 1,
    "darkbit.jpg": 1,
    "recovery_darkbit.txt": 1,
    "system volume information": 1
},
```

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"
]
```


به‌نظر 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 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:



۶-۲ تحلیل ترافیک شبکه

پس از بررسی ترافیک شبکه ضبط شده پس از اجرای باج‌افزار Nevada 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: *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*