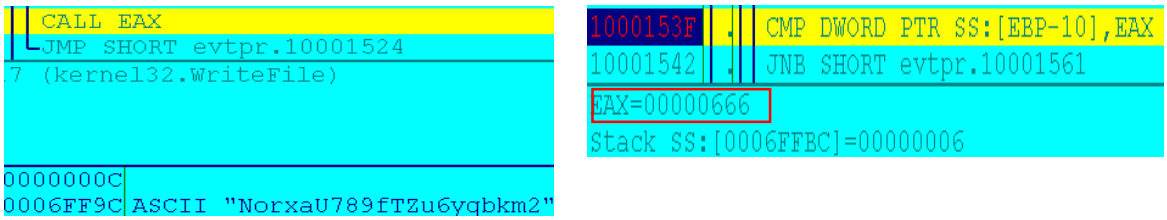
توضیحات فنی

دلیل نامگذاری بدافزار به نام Norxa، استفاده بدافزار از عبارت خاص NorxaU789fTZu6yqbkm2 برای رونویسی فایل‌های خود و از بین بردن آثار فعالیت خود است. طبق تحقیقات صورت پذیرفته ماژول های این بدافزار برای سیستم های ۳۲ بیتی و ۶۴ بیتی به صورت اختصاصی توسعه داده شده اند.

گفتنی است که این عملیات بر روی یک فایل مشخص، ۶۶۶ بار تکرار می‌شود تا فایل مورد نظر قابل بازیابی نباشد.



این بدافزار از چندین ریسمان[1]موازی برای اجرای هم‌زمان عملیات خود استفاده می کند و از مکانیزم انتقال پیام که شامل ارسال و دریافت پیام می‌شود، بهره می‌گیرد.

بر این اساس می‌توان گفت، این بدافزار از چند ماژول عملیاتی و یک ماژول هماهنگ کننده تشکیل شده است که با یکدیگر در تعامل هستند.

ذکر این نکته ضروری است که مهاجمین، برای نسخه ۶۴ بیتی ویندوز دو ماژول مختلف با نام‌های d5.dll و sqm.dll طراحی کرده‌اند که در فرایند spoolsv.exe اجرا می‌شوند. این دو فایل از نظر حجم و عملکرد به ترتیب مشابه ماژول‌های evtpr.dll و evtprext.dll در سیستم‌های ۳۲بیتی هستند.

[1] Thread

ماژول‌های sqm.dll و evtprext.dll وظیفه برقراری ارتباط اینترنتی با آدرس‌های IP و عملیات رمزنگاری را بر عهده دارند، و ماژول‌های d5.dll و evtpr.dll وظیفه ایجاد و راه‌اندازی اولیه مؤلفه‌های بدافزار را عهده دار هستند.

همچنین هر دوی این ماژول‌ها دارای یک منبع رمز شده هستند، که در حین اجرا رمزگشایی می‌شوند. در بررسی فرآیند spoolsv.exe مشخص شد، که توابعی هوک شده از ntdll.dll در بخشی از حافظه فرایند spoolsv.exe اجرا می شوند. اسامی توابع هوک شده عبارتند از:

```
ntdll.dll!NtOpenKey
ntdll.dll!NtCreateKey
ntdll.dll!NtSetInformationFile
ntdll.dll!NtMapViewOfSection
ntdll.dll!NtTerminateProcess
ntdll.dll!NtOpenFile
ntdll.dll!NtTerminateThread
ntdll.dll!NtCreateFile
ntdll.dll!NtSetValueKey
ntdll.dll!NtCreateUserProcess
ntdll.dll!NtDeleteFile
ntdll.dll!NtDeleteValueKey
ntdll.dll!NtOpenKeyEx     ntdll.dll!NtRenameKey
                          ntdll.dll!NtDeleteKey
```

به عبارت دیگر یک ماژول بدخواه با بهره‌برداری از فضای آدرسی فرایند spoolsv، تلاش می‌کند تا تعدادی از فراخوانی‌های سیستمی را هوک کرده و بتواند نتایج توابع دلخواه را مشاهده کرده و تغییر دهد.

در سیستم های ۳۲ بیتی نیز فرآیند Svchost.exe این وظیفه را برعهده دارد، بر این اساس این فرایند تلاش می‌کند تا با آدرس ۱۸۵,۱۱۸,۱۱۳,۱۱۷ از طریق پروتکل https ارتباط برقرار کرده و نسبت به ارسال اطلاعات و دریافت دستورات اقدام نماید. با بررسی این فرایند مشخص شد، دو ماژول evtpr.dll و evtprext.dll به این فرآیند تزریق شده‌اند.

```
Offset(P)  Local Address              Remote Address             Pid
---------- ------------------------- -------------------------- ---
0x09652e30 127.0.0.1:1029            127.0.0.1:14147            2948
0x09761860 0.0.0.0:1109              185.118.113.117:443        808
```

هر دو ماژول بدافزار، از روشی مشخص برای پاکسازی فرآورده‌های خود استفاده می‌کنند و برای انجام این عملیات، یک ریسمان خاص را در فضای فرایند ایجاد می‌کنند.

عملیات پاکسازی زمانی انجام می‌شود که رخدادی فعال شود یا زمان خاصی timeout گردد. این امر نشانه برنامه‌ریزی دقیق بدافزار برای خاتمه دادن به فعالیت خود بر روی سیستم قربانی است.

نکته جالب توجه آن است که چند ثانیه قبل از ایجاد dll های مشکوک در سیستم، فایل kernel32.dll سیستم عامل ویندوز با صفر، رونویسی شده و یک فایل kernel32.dll جدید در سیستم ایجاد می‌شود. توابع شناسایی شده در جدول زیر نشان داده شده است.

نام فایل	مقدار هش	نتیجه بررسی
sqm.dll	DA07bdf45d47d2587fd1042e0cf198b7	این فایل دارای فراخوانی‌هایی از winhttp.dll است که برای انجام ارتباطات شبکه‌ای بکار می‌رود.
D5.dll	12127a02bff84fed17f018a4e37ed87a	نام اصلی این فایل "." است. این فایل دارای یک منبع از نوع RCDATA و به شماره ۶۸۷۳ است که دارای محتوای رمزشده است.
evtpr.dll	B0E6C3F639E5D3FBB2757FC15B77EE9۳	فایل دارای یک منبع رمزنگاری شده و تعدادی export بدون نام است. نام export اصلی فایل servicemain.dll است.
evtprext.dll	DB07296090F0B72251479051D06FE۲۱۹	توابع export آن نامشخص است.

فایل evtpr.dll دارای یک منبع با نوع ۶۸۲۱ و نام ۶۱ است که به صورت رمزشده درون فایل نگهداری می-شود. با بررسی بدنه فایل در محیط disassembler، رشته‌های مختلفی از قبیل کلید ریجستری، نام APIها و سایر رشته‌ها نظیر رشته زیر مشاهده می‌شود که به صورت آرایه‌ای از کاراکترها تعریف شده است:

```
mov     [ebp+var_30], 'N'
mov     [ebp+var_30+1], 'o'
mov     [ebp+var_30+2], 'r'
mov     [ebp+var_30+3], 'x'
mov     [ebp+var_30+4], 'a'
mov     [ebp+var_30+5], 'U'
mov     [ebp+var_30+6], '7'
mov     [ebp+var_30+7], '8'
mov     [ebp+var_30+8], '9'
mov     [ebp+var_30+9], 'f'
mov     [ebp+var_30+0Ah], 'T'
mov     [ebp+var_30+0Bh], '2'
mov     [ebp+var_30+0Ch], 'u'
mov     [ebp+var_30+0Dh], '6'
mov     [ebp+var_30+0Eh], 'y'
mov     [ebp+var_30+0Fh], 'q'
mov     [ebp+var_30+10h], 'b'
mov     [ebp+var_30+11h], 'k'
mov     [ebp+var_30+12h], 'm'
mov     [ebp+var_30+13h], '2'
mov     [ebp+var_1C], 0
```

این رشته همان مقداری است که در فرایند فورنزیکی و در فضای SLACK فایل evtpr.dll در هارد دیسک مشاهده شده است. در مجموع ماژول های شناسایی شده عملیات زیر را انجام می دهند:

- ثبت سرویس بدافزار در سیستم و مدیریت آن
- ایجاد و مدیریت سایر مولفه‌ها همکار
- پاکسازی فرآورده‌ها و ردپاهای بدافزار از روی سیستم
- برقراری ارتباط با آدرس‌های IP مهاجم
- مدیریت عملیات رمزنگاری
- مدیریت پیام‌های مختلف ردوبدل شده میان ماژول‌های مختلف بدافزار
- مدیریت زمانبندی ریسمان‌ها و عملیات احتمالی بدافزار در آینده
- هوک برخی از توابع سیستمی

لیستی از IOCهای مربوط به این بدافزار در ادامه ارائه شده است که به منظور شناسایی سیستم‌های آلوده، می-توان از آن‌ها استفاده نمود..

لیست IOCها

➢ اسامی فایل‌ها

- d5.dll
- sqm.dll
- evtpr.dll
- evtpr32.dll
- evtpr.dat
- evtprext.dll
- lnk{%08X-%04X-%04X-%02X%02X-%02X%02X%02X-%02X%02X%02X}.tmp

➢ مقادیر هش

- 3B0E6C3F639E5D3FBB2757FC15B77EE9
- 219DB07296090F0B72251479051D06FE
- DA07bdf45d47d2587fd1042e0cf198b7
- 12127a02bff84fed17f018a4e37ed87a

➢ کلیدهای ریجستری

- وجود مقدار C:\Windows\System32\evtpr.dll در کلید ریجستری زیر: system\ControlSet001\Services\COM+ Event Processor\Parameters
- وجود مقدار C:\ProgramData\Microsoft\sqm\upload\d5.dll در کلید ریجستری زیر: SYSTEM\CurrentControlSet\Control\Print\Monitors

- **ارتباطات شبکه‌ای**
  - آدرس‌های IP:
    - **۱۱۹,۲۳۵,۲۵۲,۲۱۰:۴۴۳**
    - **۱۸۵,۱۱۸,۱۱۳,۱۱۷:۴۴۳**
  - فرمت برخی از URLهای ارتباط HTTPS بدافزار با IPهای مشکوک:

```
s://185.118.113.117/db/update/customerId=23552&licenseKey=jcdejtt
s://185.118.113.117/db/update/customerId=23552&licenseKey=axffnfiow
s://185.118.113.117/db/update/customerId=23552&licenseKey=evqjrguup
s://185.118.113.117/db/update/customerId=23552&licenseKey=jyfaonpfp
s://185.118.113.117/db/update/customerId=23552&licenseKey=ekfgslr
s://185.118.113.117/db/update/customerId=23552&licenseKey=dmqxiqh
```