باسمه تعالی

تحلیل فنی باج‌افزار

Ragnarok

تاریخ نگارش :

۱۳۹۸/۱۱/۱۰

فهرست مطالب

۱. مقدمه :

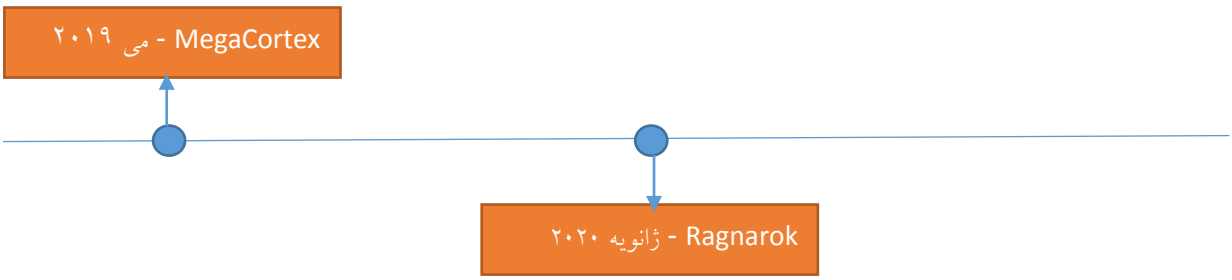
در تاریخ ۱۷ ژانویه سال ۲۰۲۰ میلادی، نسخه جدیدی از باج‌افزار MegaCortex در فضای سایبری مشاهده شد. نسخه اولیه این باج‌افزار که به عنوان Ragnarok شناخته می‌شود، پسوند .ragnarok_cry را به انتهای فایل‌های رمزشده اضافه می‌کند. براساس تحقیقات صورت گرفته و شواهد موجود، این باج‌افزار Windows Defender و Firewall ویندوز را پیش از اجرا، غیرفعال می‌کند. همچنین درصورتی که زبان نصب شده و فعال سیستم قربانی شامل زبان یکی از کشورهای روسیه، بلاروس، بخش تاتار روسیه، ترکمنستان، اوکراین، لیتوانی، قزاقستان، آذربایجان و چین باشد، فایل باج‌افزار بر روی آن سیستم اجرا نخواهد شد. تحلیل پیش رو، مربوط به نسخه به روزرسانی شده باج‌افزار Ragnarok در تاریخ ۲۳ ژانویه ۲۰۲۰ می‌باشد. این نسخه پسوند .ragnarok را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند.

۲. مشخصات فایل اجرایی :

نام فایل	since1969.exe
MD5	48452dd2506831d0b340e45b08799623
SHA-1	74993759f49d123ec334111f29cdbbf2e0276b58
SHA-256	b7319f3e21c3941fc2a960b67a150b02f1f3389825164140e75dfa023a73d34c
نوع فایل	Win32 EXE
اندازه فایل	۲۱۰کیلوبایت

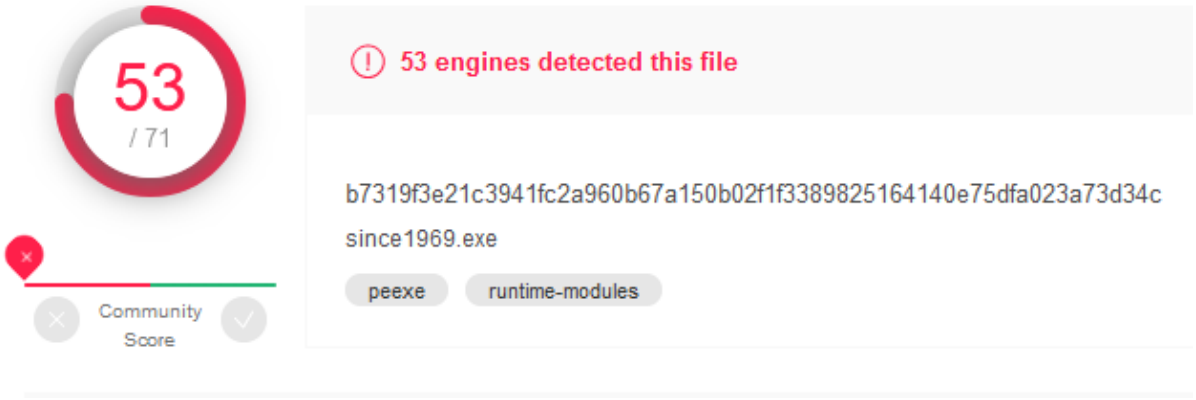
۳. شجره‌نامه

براساس گزارش‌های منتشر شده، باج‌افزار Ragnarok نسخه‌ای توسعه یافته از باج‌افزار MegaCortex می‌باشد.



٤. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ۵۳ مورد از ۷۱ از ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حـذف این باج‌افزار می‌باشند.



۵. تحلیل پویا

۵-۱ آناتومی حمله:

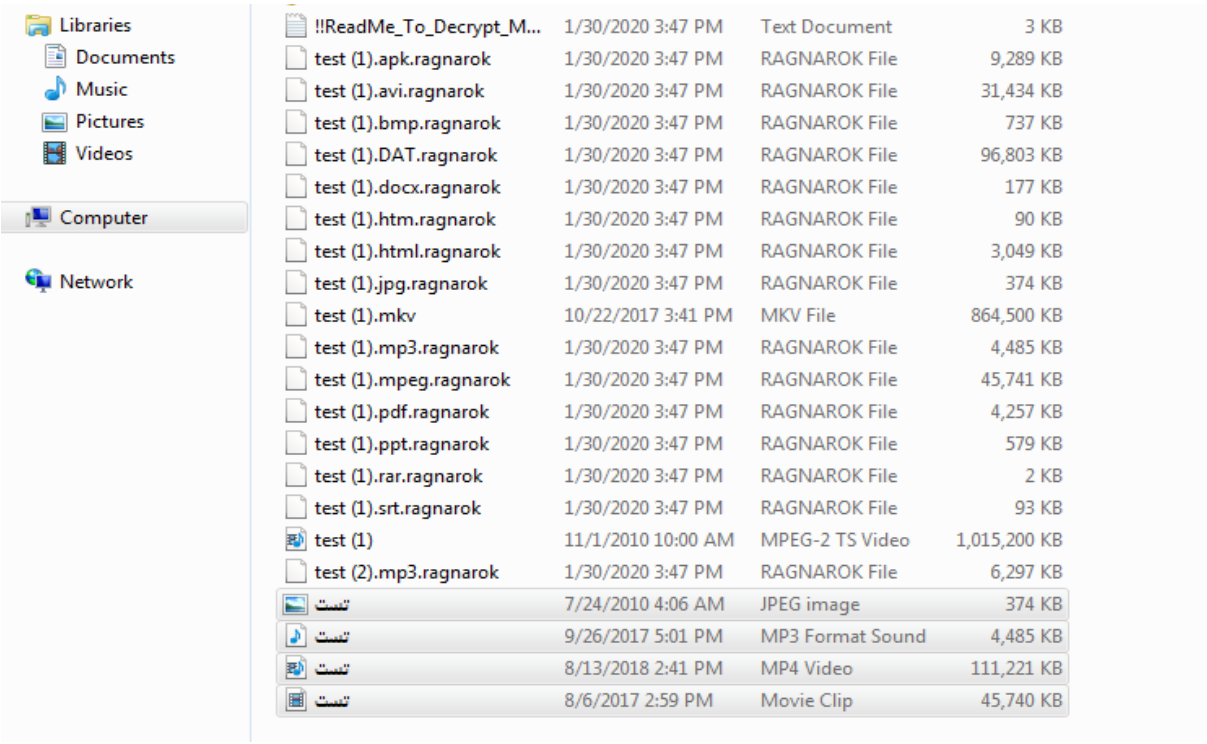
پس از اجرای باج‌افزار در محیط آزمایشگاهی، نتایج زیر مشاهده شد.

باج‌افزار Ragnarok در همان ابتدای شروع فعالیت خود در سیستم قربانی، دستورات زیر را اجرا می‌کند:

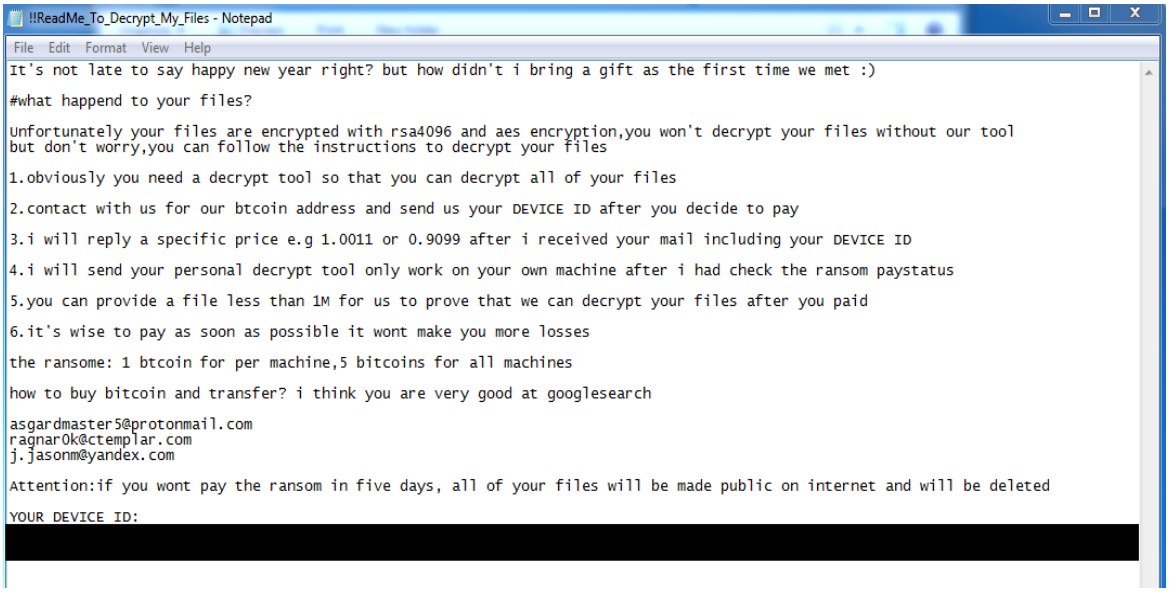
حذف فضای VSC	cmd.exe /c vssadmin delete shadows /all /quiet
عدم نمایش خطای بوت سیستم‌عامل	cmd.exe /c bcdedit /set {current} bootstatuspolicy ignoreallfailures
غیرفعال کردن قابلیت بازیابی ویندوز	cmd.exe /c bcdedit /set {current} recoveryenabled no
غیرفعال کردن Firewall ویندوز	cmd.exe /c netsh advfirewall set allprofiles state off

سپس، فرآیند رمزگذاری فایل‌ها در سیستم قربانی شروع می‌شود.

تصویر زیر، فایل‌های رمزگذاری شده توسط این باج‌افزار را نشان می‌دهد.



همانطور که در تصویر بالا قابل مشاهده است به انتهای هر فایل رمزشده پسوند ragnarok. اضافه شده است و همچنین فایل‌های با نام فارسی رمزگذاری نشده‌اند. نکته دیگری که در تصویر بالا مشاهده می‌شود این است که دو فایل با حجم بیش از ۵۰۰ مگابایت می‌باشند که رمزگذاری نشده‌اند. با بررسی‌های بیشتری که صورت گرفت، مشخص شد که باج‌افزار Ragnarok فایل‌های با حجم تقریبی حداکثر ۵۰۰ مگابایت را رمزگذاری کرده و هر فایل با حجمی بیش از این مقدار، در سیستم قربانی رمزگذاری نمی‌شود. فایل پیغام باج‌خواهی این باج‌افزار با عنوان !!ReadMe_To_Decrypt_My_Files.txt نیز، در کنار فایل‌های رمزگذاری شده قابل مشاهده است.



در ابتدای پیغام باج اشاره شده است که فایل‌های سیستم قربانی توسط الگوریتم‌های RSA4096 و AES رمزگذاری شده‌اند و قربانی هیچ شانسی جهت بازیابی آن‌ها ندارد. تنها راه رمزگشایی فایل‌های قربانی، تهیه ابزار رمزگشایی ارائه شده توسط مهاجم می‌باشد که قربانی جهت دریافت آن باید شناسه خود که در انتهای پیغام قرار داده شده است را به یکی از ایمیل‌های در نظر گرفته شده درون پیغام باج‌خواهی، ارسال کند. سپس مهاجم مبلغی را درنظر گرفته و به همراه آدرس کیف‌پول بیت‌کوین خود برای خرید این ابزار، برای قربانی ارسال می‌کند. قربانی باید مبلغ تعیین شده در پاسخ ایمیل خود را برای مهاجم ارسال کند در غیر این صورت تمام فایل‌های خود را از دست خواهد داد. درادامه پیغام، مبلغی که برای تمام سیستم‌های آلوده شده در یک شبکه تعیین شده است، ۵ بیت‌کوین ذکر شده است. در انتها نیز آدرس ایمیل‌های asgardmaster5@protonmail.com و ragnar0k@ctemplar.com و j.jasonm@yandex.com جهت ارتباط قربانی با مهاجم، قرار داده شده است.

فرآیند مربوط به باج‌افزار Ragnarok پس از انتهای فعالیت خود در سیستم قربانی، متوقف می‌شود.

۵-۲ روش انتشار:

به گزارش وب‌سایت BleepingComputer ، باج‌افزار Ragnarok از طریق اجرای اکسپلویت بر روی سرورهای ADC محصول شرکت Citrix که دارای آسیب‌پذیری با شناسه CVE-2019-19781 می‌باشند، به سیستم و شبکه مورد هدف خود نفوذ می‌کند. مکانیزم حمله باج‌افزار به این صورت است که پس از دسترسی سرورهای مذکور توسط مهاجمین، انواعی از اسکریپت‌ها بر روی آن‌ها اجرا شده که تمام سیستم‌های درون شبکه که در برابر اکسپلویت EthernalBlue آسیب‌پذیر هستند را جست‌وجو می‌کند. درصورت یافتن آن‌ها، اکسریپت‌ها سعی می‌کنند سیستم‌های آسیب‌پذیر را اکسپلویت کنند و در صورت موفقیت، یک فایل DLL درون هر سیستم آسیب‌پذیر تزریق می‌شود که فایل اصلی باج‌افزار را دانلود و نصب می‌کند.

۵-۳ روش جلوگیری:

با توجه به اینکه این باج‌افزار Ragnarok با سوء استفاده از آسیب‌پذیری CVE-2019-19781 بر روی سرورهای ADC به سیستم‌های یک شبکه نفوذ می‌کند، اکیداً توصیه می‌شود که آخرین وصله‌های امنیتی ارایه شده برای آسیب‌پذیری مذکور را از وب‌سایت Citrix دریافت و نصب نمایید.

https://support.citrix.com/article/CTX267027

https://support.citrix.com/article/CTX267679

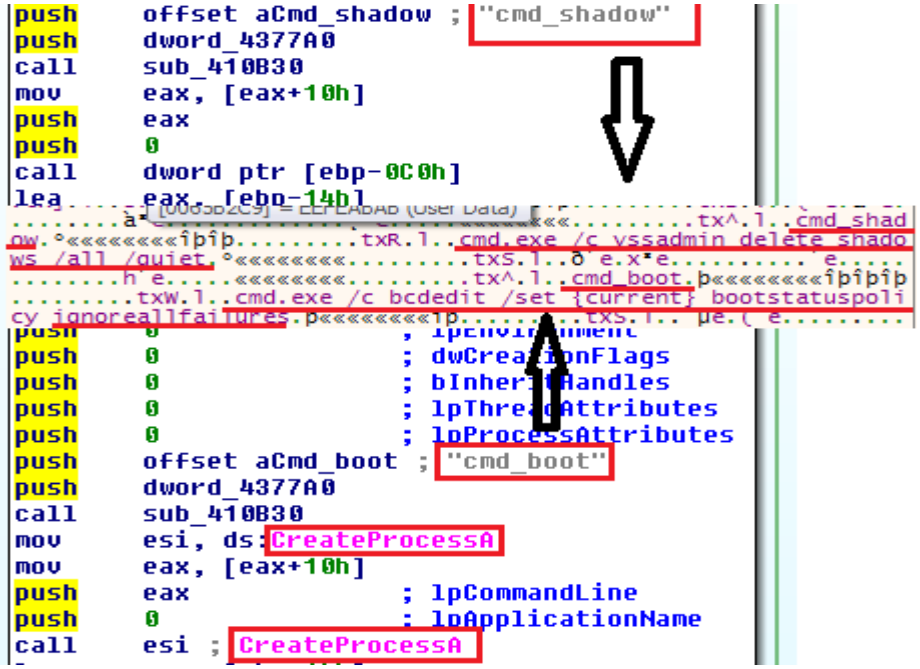
٦. تحلیل ایستا

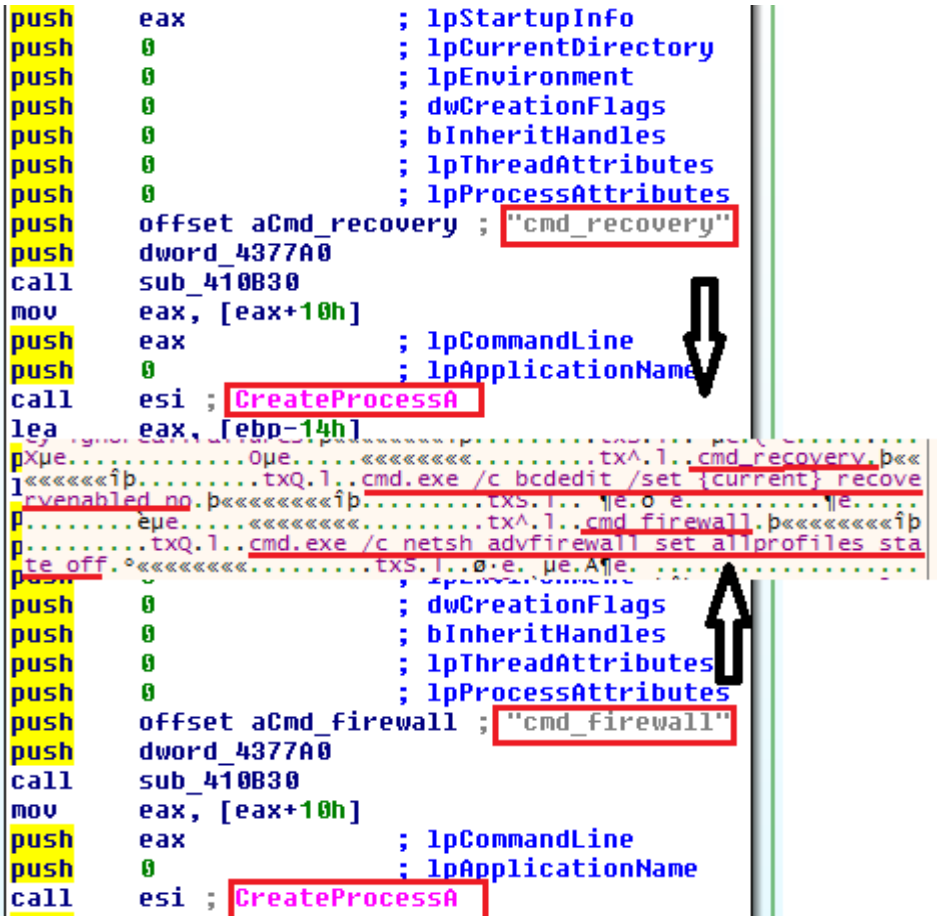
بررسی‌های اولیه بر روی فایل اجرایی این باج‌افزار نشان می‌دهد که باج‌افزار Ragnarok بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از ویندوز ویستا به بعد، اجرا خواهد شد.

File alignment	00000200	
OS version (major)	0006	Windows Vista
OS version (minor)	0000	
Image version (major)	0000	
Image version (minor)	0000	
Sub system version (major)	0006	
Sub system version (minor)	0000	
Win32 version	00000000	
Size of image	0003B000	
Size of headers	00000400	
Checksum	00000000	does NOT match file checksum 0003849F
Sub system	0002	Windows graphical user interface (GUI) subsystem
DLL characteristics	8140	Dynamic base, NX compatible

٦-١ تحلیل کد:

همانطور که در ابتدای بخش قبل اشاره شد، باج‌افزار Ragnarok قبل از انجام هر اقدامی در سیستم قربانی، دستوراتی را اجرا می‌کند.





تصاویر بالا مربوط به بخش‌هایی از کد باج‌افزار است که فرآیندهای مربوط به هر دستور را با استفاده تابع CreateProcessA ایجاد کرده و سپس دستورات را اجرا می‌کند.

پس از اجرای دستورات فوق، این باج‌افزار در ابتدا محتوای بخش پیکربندی خود را می‌خواند. تصویر زیر، قطعه کد مربوط این قسمت را نشان می‌دهد.

```
push    offset off_433000
call    sub_410B50
push    offset aReg_key ; "reg_key"
push    eax
mov     dword_4377A0, eax
call    sub_410B30
push    offset aReg_value ; "reg_value"
push    dword_4377A0
mov     dword_43779C, eax
call    sub_410B30
push    offset aExcept_languag ; "except_language"
push    dword_4377A0
mov     dword_437798, eax
call    sub_410B30
push    offset aExcept_path ; "except_path"
push    dword_4377A0
mov     dword_437794, eax
call    sub_410B30
push    offset aApi     ; "api"
push    dword_4377A0
mov     dword_437790, eax
call    sub_410B30
push    offset aReadme_content ; "readme_content"
push    dword_4377A0
mov     dword_43778C, eax
call    sub_410B30
push    offset aFile_ext ; "file_ext"
push    dword_4377A0
mov     dword_437788, eax
call    sub_410B30
push    offset aProc    ; "proc"
push    dword_4377A0
mov     dword_437784, eax
call    sub_410B30
mov     dword_437780, eax
call    sub_403810
mov     ecx, [ebp+var_4]
pop     edi
pop     esi
xor     ecx, ebp
pop     ebx
call    sub_411753
mov     esp, ebp
pop     ebp
retn
```

محتوای موارد پیکربندی فایل این باج‌افزار شامل مقدار رجیستری‌های تنظیم شده، زبان‌ها و محل‌هایی از سیستم‌عامل که در لیست سفید قرار دارند، محتوای پیغام باج‌خواهی و پسوندهایی که در لیست سفید باج‌افزار قرار دارند، در تصویر زیر قابل مشاهده است.

محتوای بخش پیکربندی فایل

سپس، فرآیند رمزگذاری فایل‌ها شروع شده و در مدت زمان کوتاهی تمام فایل‌های مورد هدف باج‌افزار در سیستم قربانی رمزگذاری می‌شوند. همانطور که درون پیغام باج‌خواهی باج‌افزار نیز اشاره شده است، باج‌افزار Ragnarok از الگوریتم‌های RSA و AES به صورت ترکیبی در کد خود بهره برده است. تصاویر زیر، بخش‌هایی از توابع مربوط به این الگوریتم‌ها را نشان می‌دهد.

```
aes_key_rand proc near

var_120= dword ptr -120h
var_11C= dword ptr -11Ch
var_118= dword ptr -118h
var_114= dword ptr -114h
var_110= dword ptr -110h
var_10C= dword ptr -10Ch
var_108= dword ptr -108h
var_104= byte ptr -104h
var_4= dword ptr -4
arg_0= dword ptr  8
arg_4= dword ptr  0Ch

push    ebp
mov     ebp, esp
sub     esp, 120h
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
mov     eax, [ebp+arg_0]
mov     ecx, [ebp+arg_4]
push    esi
push    edi
mov     [ebp+var_120], eax
```

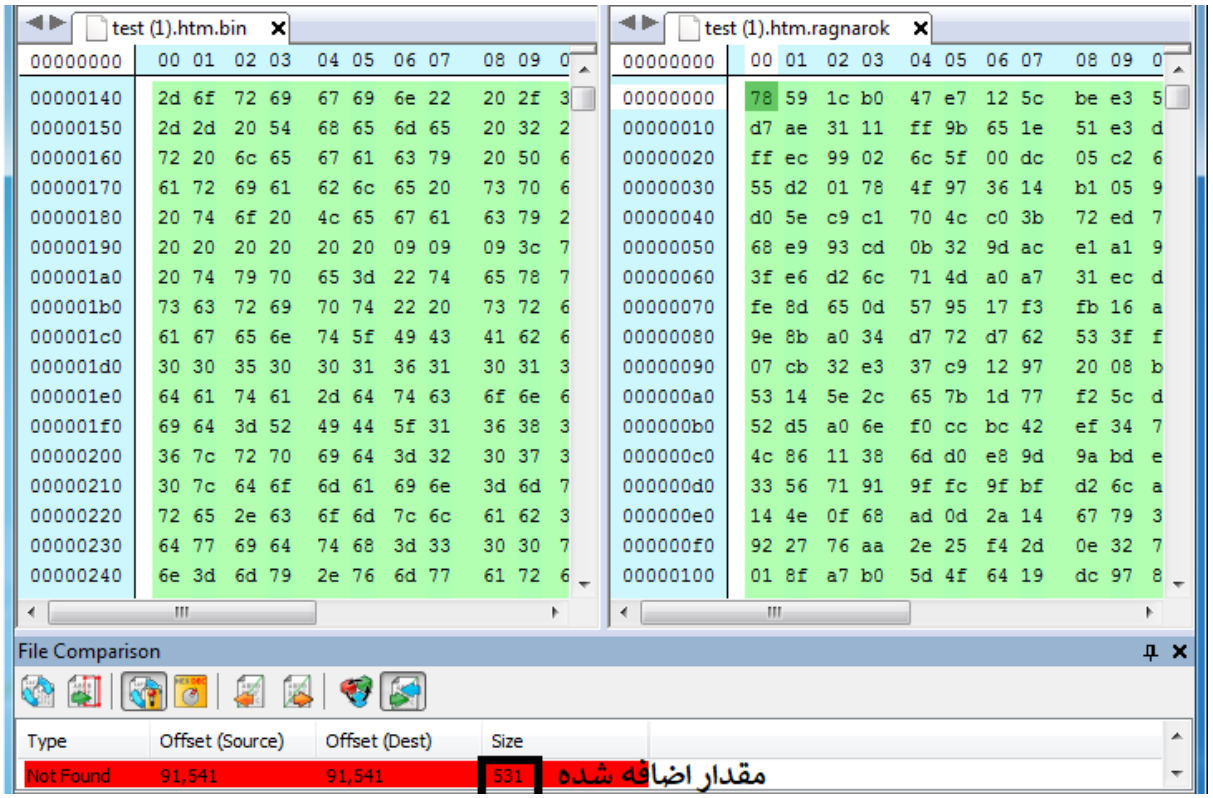
```
rsa_rand proc near

var_484= byte ptr -484h
var_3D8= byte ptr -3D8h
var_3CC= byte ptr -3CCh
var_3C0= dword ptr -3C0h
var_3BC= byte ptr -3BCh
var_144= byte ptr -144h
var_4= dword ptr -4
arg_0= dword ptr  8
arg_4= dword ptr  0Ch

push    ebp
mov     ebp, esp
sub     esp, 484h
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
mov     eax, [ebp+arg_4]
push    ebx
push    esi
push    edi
mov     edi, [ebp+arg_0]
mov     esi, 1
push    offset aRsa_rand ; "rsa_rand"
```

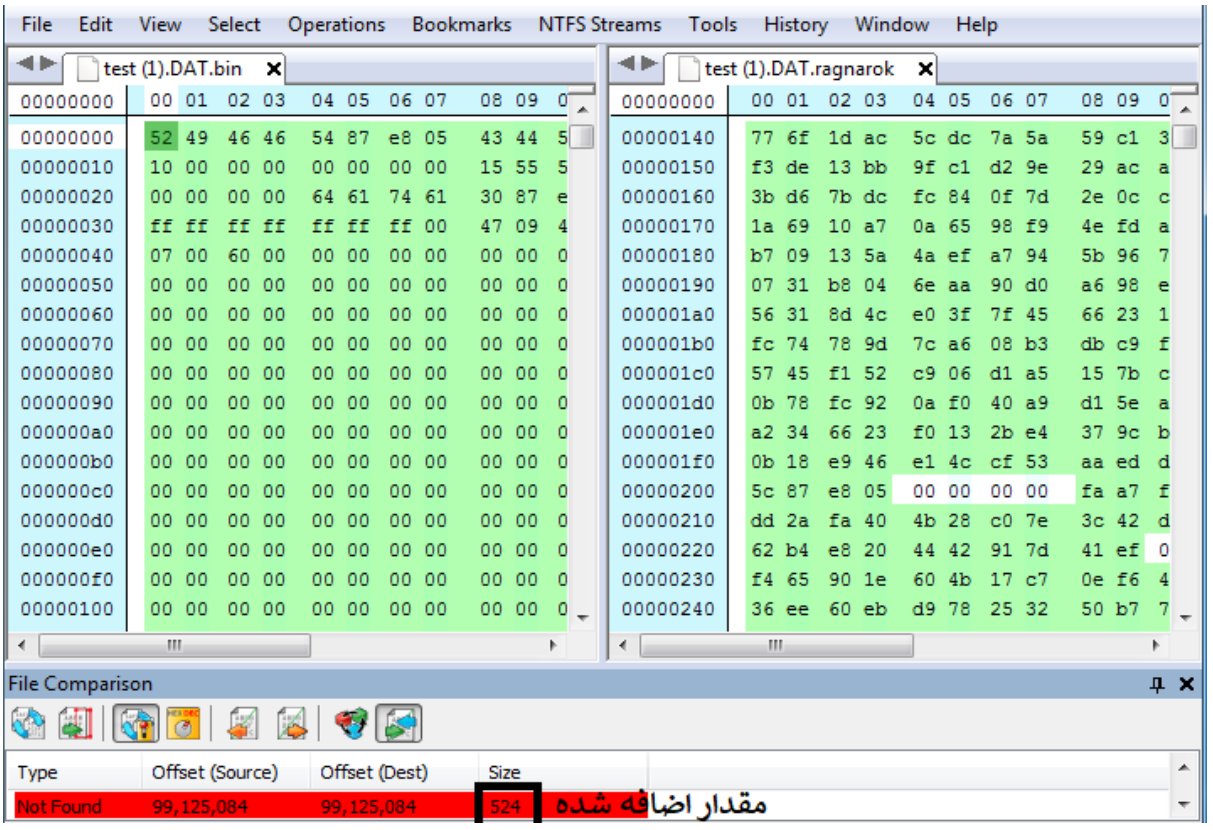
کلید عمومی استفاده شده در فرآیند رمزنگاری نیز، در تصویر زیر قابل مشاهده است.

```
sub_403810 proc near
push    esi
push    edi
push    401h
call    sub_401D80
add     esp, 4
mov     dword_434AF0, eax
push    offset aRsa_pub_n ; "rsa_pub_N"
push    dword_4377A0
call    sub_410B30
mov     edi, dword_434AF0
mov     ecx, 100h
push    offset aRsa_pub_e ; "rsa_pub_E"
mov     esi, [eax+10h]
rep movsd
push    dword_4377A0
call    sub_410B30
push    7
mov     esi, [eax+10h]
call    sub_401D80
mov     ecx, [esi]
add     esp, 4
```

```
.....(«e.....«««««««««.....tx^.l..rsa_pub_N.ï«««««««««þîþîþ
.....txß.l..9D6EACD8D5897A5E02520E6E054D0F316A588337793B8604
E36EC425F1B2ED08A516E5390EB99898292E6E3D187431BDCE14F62E04C9C280
69FD10C811E82EA6C436E52420B68C4DF452D116D023143B85A01978C474AEC4
7F10344224525616757 1E44D14EBE2E5A3BC12C2F62B1CBD4E8875D0CFA103CA
ED42A2868D8FF2D3D604B92A4FD55C7BCBFE6D9838BA6AC80FF75EBECF49F81A
9271A608817AC4908481B8BE34D914C00B9D5DB8F236A3D515108B238132D0AC
D0809E0B171FCDF96DF897598A8FC5C94512920EEF7F2152BF6CEEB2DA9BFD22
D357123BB6EC9CAA17E8A04325C1BE6AE021D67434463878332 6CE7FF7A9368C
FFF8CD680FEFD8201F284420C37D754837321ADA1B3F5306B223EEE0A8F43984
9113F103D876F46E690AB658E08BD6F09A0E710F4ACC086951A0D093 58AD8B5E
1BD3B10B2421CD22952CB1E986BE9C611D16FB0E65A775C12E9B3195761BEF17
CB9C588EBB6F71D5E51E6CE8CA12E5F699E6A5257537CE33B8AE3D9CE8D412F3
295968E65F83EC294AC877C0DCB742897D1B5EB48147E61A0EF11699E8D898A7
8893E9657CB39247717B658FD933C3405E796B3CD10BA411CC4458BEE0B22F42
DA50E65A8993AE553334B3D55A604DEB429945DB37052FEB24DC7D4E012E44FC
CA4A8656F2ECB9DCA95E749F5E6953E2DA48EC3509039C1109E63F9B89D6BCE6
AE0D5419BBDDA279.þ«««««««««îþîþîþ.....txS.l..ø¯e.è*e.....
```

پس از بررسی چند نمونه فایل سالم با نمونه رمزشده آن‌ها مشخص گردید که باج‌افزار Ragnarok تمام محتوای فایل را رمزگذاری کرده و بین ۵۲۰ تا ۵۳٤ کیلوبایت به انتهای هر فایل رمزشده اضافه می‌نماید.





۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه ضبط شده پس از اجرای باج‌افزار و همچنین بررسی نتایج سندباکس‌های آنلاین، موردی در ارتباط با باج‌افزار مشاهده نشد.

۶-۳ رمزگشایی:

در حال حاضر، هیچ‌گونه ابزاری جهت رمزگشایی فایل‌های رمزشده توسط این باج‌افزار، ارایه نشده است.