باسمه تعالی

تحلیل فنی باج‌افزار

Buran

فهرست مطالب

۱. مقدمه : ۳
۲. مشخصات فایل اجرایی : ۳
۳. شجره‌نامه ۳
٤. میزان تهدید فایل باج‌افزار: ۳
٥. تحلیل پویا ٤
٥-۱ آناتومی حمله: ٤
٥-۲ روش انتشار: ٥
٥-۳ روش جلوگیری: ٦
٦- تحلیل ایستا ٦
٦-۱ تحلیل کد: ٦
٦-۲ تحلیل ترافیک شبکه: ۱۰
٦-۳ رمزگشایی: ۰۱

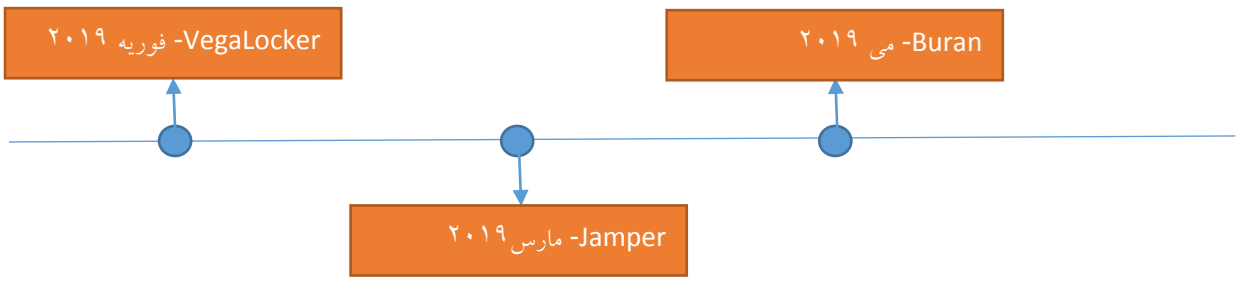
۱. مقدمه :

در اواسط ماه می سال ۲۰۱۹ میلادی، اخباری مبنی بر انتشار باج‌افزاری با عنوان Buran منتشر شد. این باج‌افزار نسخه توسعه یافته باج‌افزار Jamper می‌باشد. براساس گزارش وب‌سایت id-ransomware نسخه اولیه این باج‌افزاراز طریق انجمن‌هایی با آدرس‌های ifud.ws، verified.sc، exploitinqx4sjro.onion، forum.zloy.bz، darkmarket.la به صورت سرویس(RaaS) به فروش می‌رسد. پس از نسخه اول، نسخه دوم و نسخه ای با عنوان Ghost از این باج‌افزار در ماه ژوئن منتشر شد و از اواسط ماه نوامبر، اخباری مربوط به نسخه جدید این باج‌افزار در فضای سایبری منتشر شد که تحلیل پیش رو، مربوط به آخرین نسخه از این باج‌افزار یعنی Buran 3.0 می‌باشد.

۲. مشخصات فایل اجرایی :

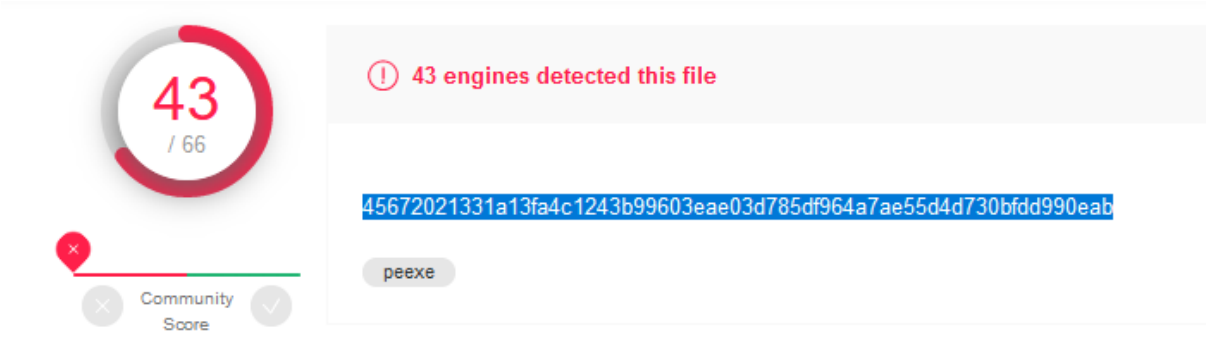
نام فایل	Random
MD5	875bd68b20c710bc26a922db61641ee8
SHA-1	6c79e04caf8f68c6b55a1ed7bbdc660b23debbc9
SHA-256	45672021331a13fa4c1243b99603eae03d785df964a7ae55d4d730bfdd990eab
نوع فایل	Win32 EXE
اندازه فایل	۱۷۶ کیلوبایت

۳. شجره‌نامه



٤. میزان تهدید فایل باج‌افزار

درحال حاضر تعداد ٤٣ مورد از ٦٦ ضدبدافزار سامانه VirusTotal، قادر به شناسایی، توقف و یا حذف این باج‌افزار می‌باشند.



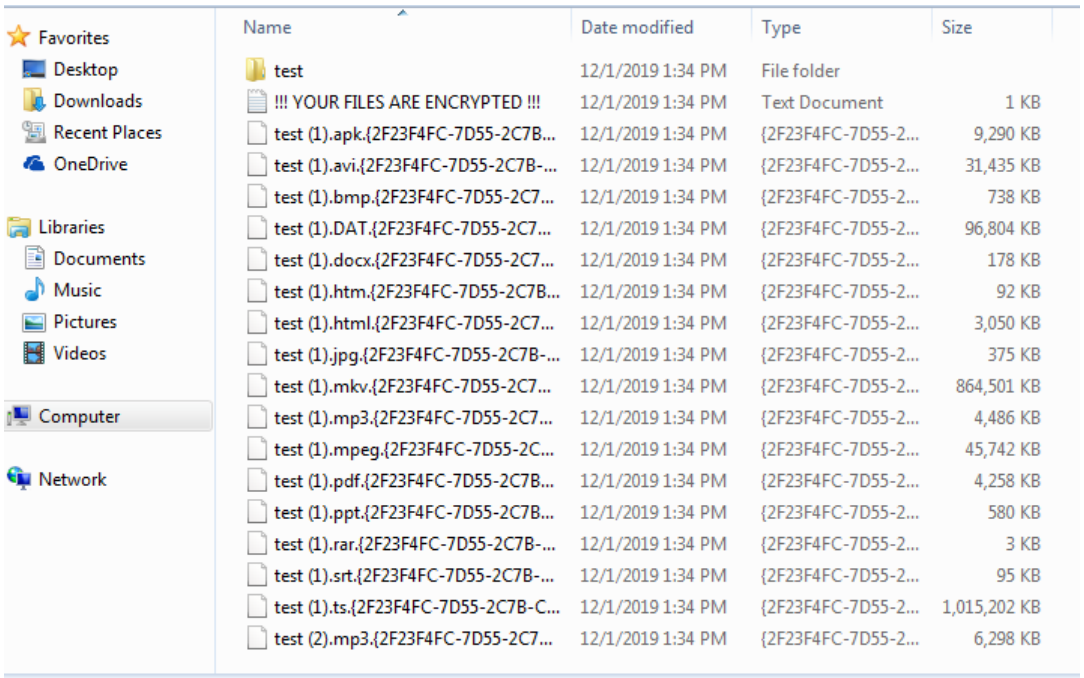
٥. تحلیل پویا

٥-١ آناتومی حمله:

باج‌افزار Buran در همان ابتدای فعالیت خود در سیستم قربانی، دستورات زیر را اجرا می‌کند.

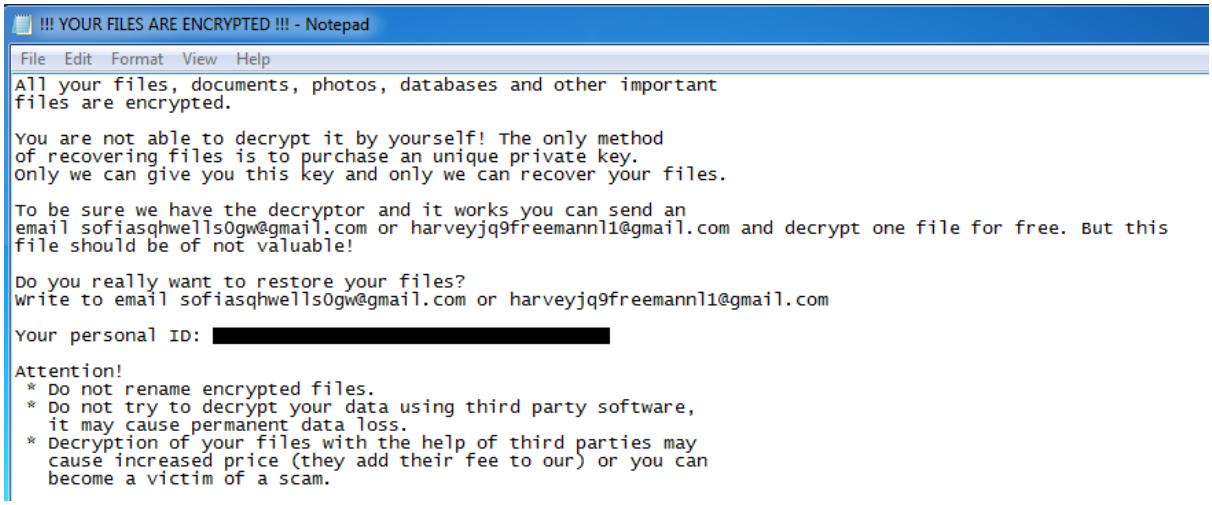
C:\Windows\system32\cmd.exe /C chcp 1250 && net view	نمایش لیست کامپیوترهایی که با سیستم قربانی در یک شبکه قرار دارند.
"C:\Windows\system32\taskmgr.exe" /4	باز کردن و دسترسی به برنامه TaskManager سیستم‌عامل

سپس، فرآیند رمزگذاری فایل‌ها آغاز می‌شود.



همانطور که قابل مشاهده است، تمامی فایل‌های قربانی رمزگذاری شده‌اند و شناسه‌ای که برای قربانی درنظر گرفته شده است، به عنوان پسوند به انتهای هر فایل رمزگذاری شده اضافه شده است. این باج‌افزار قدرتمند تمامی انواع فایل‌ها را در سیستم قربانی رمزگذاری می‌کند و فقط فایل‌های اجرایی با پسوند exe از رمزگذاری در امان می‌مانند که این امر سبب می‌شود بخشی از نرم‌افزارهای درون سیستم‌عامل پس از پایان فرآیند رمزگذاری، بدون هیچ‌گونه مشکلی اجرا شوند.

فایل پیغام باج‌خواهی باج‌افزار با عنوان !!! YOUR FILES ARE ENCRYPTED نیز، درون هر پوشه و در کنار فایل‌های رمز شده قرار می‌گیرد. این فایل پس از اتمام فعالیت باج‌افزار در سیستم قربانی و همزمان با توقف فایل اجرایی باج‌افزار، بر روی صفحه نمایش سیستم قربانی نمایان می‌شود.



براساس ادعای مهاجم یا مهاجمین، تنها راه رمزگشایی فایل‌های سیستم قربانی، تهیه کلید خصوصی یکتا می‌باشد که قربانی جهت دریافت آن، باید از طریق آدرس ایمیل‌های sofiasqhwells0gw@gmail.com و harveyjq9freemannl1@gmail.com با مهاجم ارتباط برقرار کند. برای جلب اعتماد قربانی، یک فایل کم ارزش، به صورت رایگان رمزگشایی خواهد شد. مبلغ باج‌خواهی نیز، پس از برقراری ارتباط با مهاجمین مشخص خواهد شد.

۵-۲ روش انتشار:

با توجه به اینکه این باج‌افزار به صورت یک سرویس ارایه شده است و فرد خریدار باج‌افزار از هر روشی جهت انتشار آن می‌تواند استفاده کند، احتمال انتشار باج‌افزار از طریق هر یک از روش‌های مرسوم همچون مهندسی اجتماعی، بارگذاری در وب‌سایت‌های نامعتبر، پیوست‌های مخرب درون ایمیل‌ها، انتشار از طریق شبکه‌های اجتماعی و ... وجود دارد.

۵-۳ روش جلوگیری:

با توجه به مشخص نبودن روش انتشار باج‌افزار، توصیه می‌شود اقدامات عمومی همچون عدم بازکردن پیوست‌های درون ایمیل‌هایی که به صورت هرزنامه دریافت می‌شوند، به روز رسانی سیستم‌عامل، آنتی‌ویروس و مرورگرهای فعال در سیستم‌عامل در دستور کار قرار گیرد. ضمناً در صورت دریافت هرگونه فایل مشکوک، حتماً قبل از اجرا، آن را در سامانه ویروس کاو مرکز ماهر به نشانی https://viruskav.cert.ir اسکن نمایید.

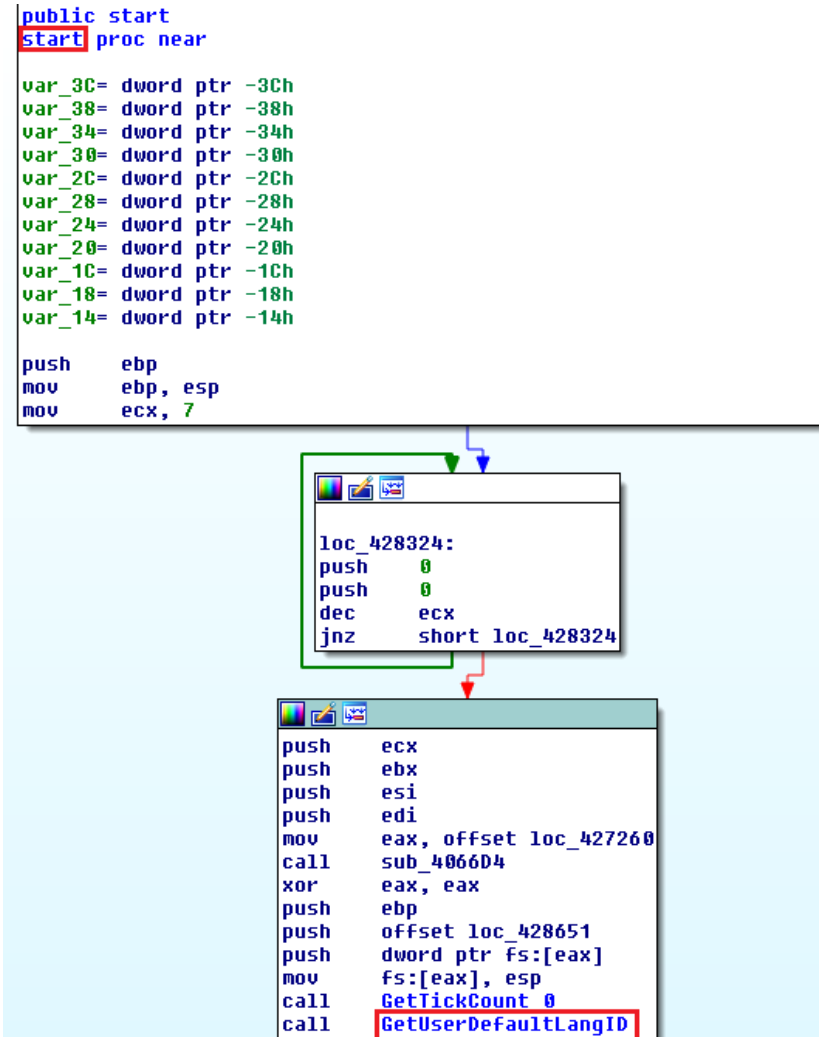
٦. تحلیل ایستا

بررسی اولیه فایل اجرایی این نسخه از باج‌افزار Buran نشان می‌دهد که همانند دیگر نسخه‌های این باج‌افزار، بر روی تمامی نسخه‌های سیستم‌عامل ویندوز قابل اجرا است.

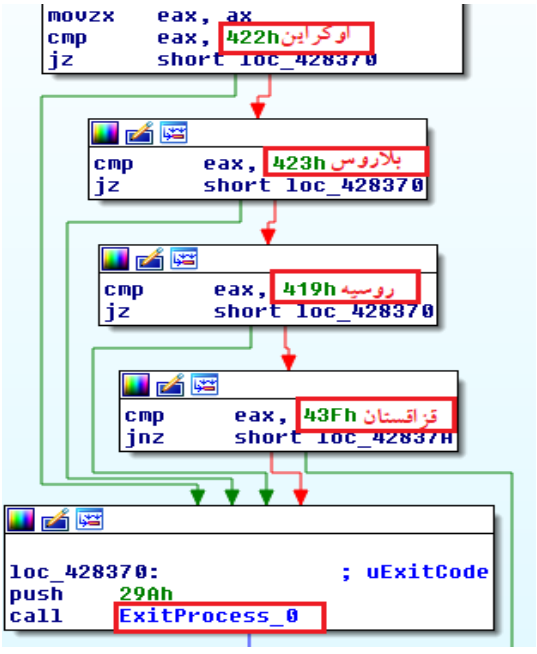
Base of code	00001000	
Base of data	00075000	
Image base	00400000	
Section alignment	00001000	
File alignment	00000200	
OS version (major)	0004	Windows 95/NT 4.0
OS version (minor)	0000	
Image version (major)	0000	
Image version (minor)	0000	
Sub system version (major)	0004	

٦-١ تحلیل کد:

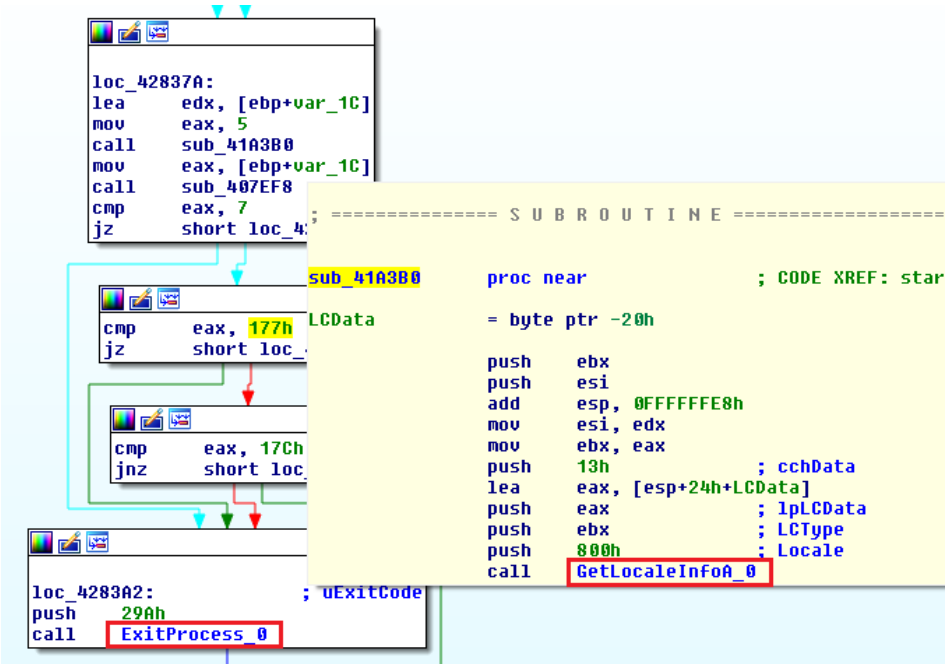
کد باج‌افزار از تابع Strat شروع می‌شود و در ابتدا، از طریق تابع GetUserDefaultLangID شناسه زبان یا زبان‌های فعال در سیستم قربانی، دریافت می‌شود.



سپس، این شناسه در صورتی که با هر کدام از شناسه‌های زیر برابر باشد، فایل باج‌افزار متوقف شده و بر روی سیستم قربانی اجرا نمی‌شود.



این بررسی از طریق موقعیت جغرافیایی سیستم قربانی و نام زبان یا زبان‌های فعال بـر روی سیسـتم قربـانی نیز صورت می‌گیرد و در صورتی که در محدوده کشورهای فوق باشد، فایل باج‌افزار بر روی سیستم قربانی اجرا نخواهد شد.



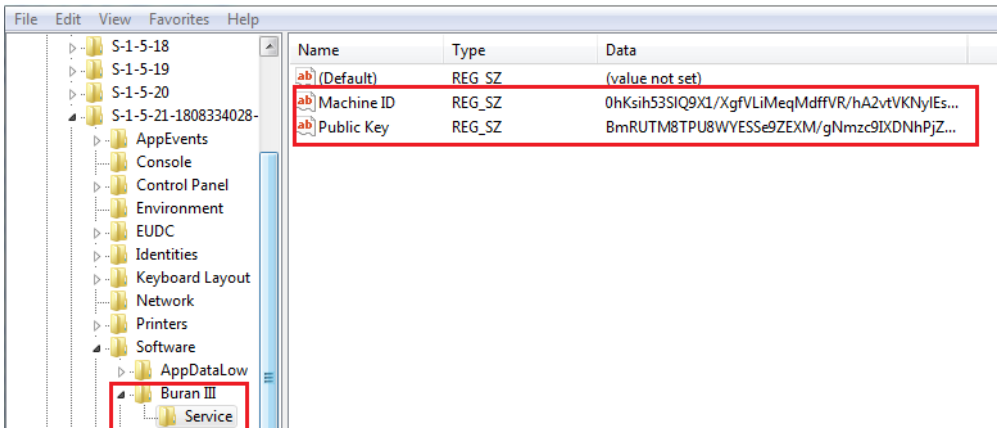
در ادامه، مقادیر رجیستری مربوط به باج‌افزار که شامل کلید عمومی استفاده شـده در فرآینـد رمزگـذاری و مقدار شناسه قربانی می‌باشد، درون سیستم قربانی ایجاد خواهد شد.

```
hKey= dword ptr  4
lpSubKey= dword ptr  8
Reserved= dword ptr  0Ch
lpClass= dword ptr  10h
dwOptions= dword ptr  14h
samDesired= dword ptr  18h
lpSecurityAttributes= dword ptr  1Ch
phkResult= dword ptr  20h
lpdwDisposition= dword ptr  24h

jmp     ds:__imp_RegCreateKeyExA
RegCreateKeyExA endp
```

```
hKey= dword ptr  4
lpValueName= dword ptr  8
Reserved= dword ptr  0Ch
dwType= dword ptr  10h
lpData= dword ptr  14h
cbData= dword ptr  18h

jmp     ds:__imp_RegSetValueExA
RegSetValueExA endp
```



این باج‌افزار، در ادامه فعالیت خود در سیستم قربانی، نسخه سیستم‌عامل و نوع هر درایوی از سیستم‌عامل که در سیستم قربانی جست و جو می‌کند را، دریافت می‌کند.

```
lpRootPathName= dword ptr  4

jmp     ds:__imp_GetDriveTypeA
GetDriveTypeA endp
```

```
lpVersionInformation= dword ptr  4

jmp     ds:__imp_GetVersionExA
GetVersionExA endp
```

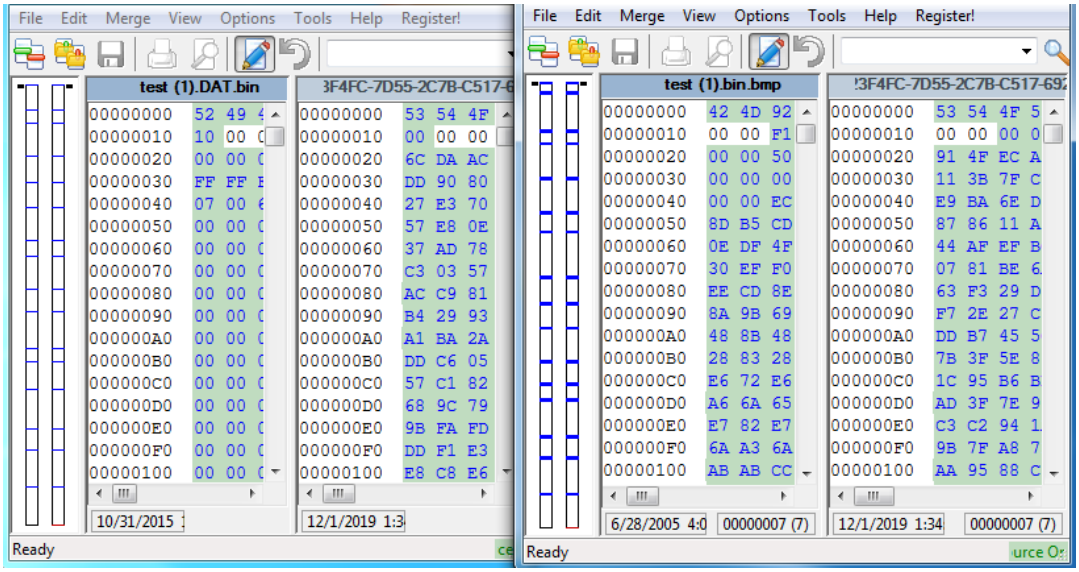
در نهایت فرآیند رمزگذاری شروع می‌شود و تمامی فایل‌های درون سیستم قربانی در مدت زمان کمی رمزگذاری خواهند شد.

```
INS DWORD PTR ES:[EDI],DX                    I/O command
INC EBP
JS SHORT ntdll_1a.77E5CF1B
PUSH EDI
IMUL EBP,DWORD PTR DS:[ESI+0x53],0x6F436D71
INS DWORD PTR ES:[EDI],DX                    I/O command
INS DWORD PTR ES:[EDI],DX                    I/O command
OUTS DX,DWORD PTR ES:[EDI]                   I/O command
OUTS DX,BYTE PTR ES:[EDI]                    I/O command
INC ESP
POPAD
JE SHORT ntdll_1a.77E5CF8C
JO SHORT ntdll_1a.77E5CF9C
IMUL EBP,DWORD PTR DS:[ESI+0x74],0x53746553
JE SHORT ntdll_1a.77E5CFA8
IMUL EBP,DWORD PTR DS:[ESI+0x67],0x6E695700
PUSH EBX
JNO SHORT ntdll_1a.77E5CFAD
INC EBP
OUTS DX,BYTE PTR ES:[EDI]                    I/O command
```

با توجه به اینکه این باج‌افزار مقداری با عنوان کلید عمومی در سیستم قربانی ایجاد می‌کند و درپیغام باج‌خواهی نیز به کلید خصوصی یکتا جهت رمزگشایی فایل‌ها اشاره شده است، از الگوریتم RSA نیز در

فرآیند رمزگذاری فایل‌ها استفاده شده است. کلید عمومی جهت رمزگشایی کلید رمزگذاری فایل‌ها و کلید خصوصی جهت رمزگشایی این کلید و در نهایت رمزگشایی فایل‌ها استفاده شده است.

بررسی نمونه فایل‌های رمزشده با نمونه سالم آن‌ها نشان می‌دهد که این باج‌افزار از الگوی یکسانی جهت رمزگشایی فایل‌ها استفاده می‌کند.



۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه حین اجرای باج‌افزار، ترافیک مشکوکی مربوط به این باج‌افزار مشاهده نشد.

۶-۳ رمزگشایی:

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