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 Makop

گزارش تحلیلی

شناسه سند	MaherReportsTemplate_14010906
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۴۰۱/۰۹/۰۶
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

1. مقدمه: ۳

۲. مشخصات فایل‌های اجرایی: ۳

۳. شجره‌نامه ۴

۴. میزان تهدید فایل باج‌افزار ۴

5. تحلیل پویا ۴

۵-۱ آناتومی حمله ۴

۵-۲ روش انتشار: ۹

۵-۳ روش مقابله: ۱۰

۶. تحلیل ایستا ۱۰

۶-۱ تحلیل کد: ۱۰

۶-۲ تحلیل ترافیک شبکه: ۱۵

۶-۳ رمزنگاری و رمزگشایی: ۱۵

7. شناسه‌های تهدید (IOCs) ۱۶

8. شناسایی (Detection) ۱۶

۱. مقدمه:

در اوایل سال ۲۰۲۲ حساب کاربری @siri_urz در توییتر از یک باج‌افزار جدید به نام Makop رونمایی کرد. نسخه اولیه این باج‌افزار پسوند makop. را به انتهای فایل‌های رمزشده اضافه می‌کرد. بر اساس تحقیقات صورت گرفته و شواهد موجود، این خانواده باج‌افزاری برای فعالیت خود احتیاجی به اتصال به اینترنت ندارند و بدون دسترسی مدیر سیستم (Administrator) نیز فعالیت خود را به انجام می‌رسانند. باج‌افزار Makop از دو رفتار متفاوت در رمزگذاری فایل‌های سیستم قربانی استفاده می‌کند و بر همین اساس، با دو نوع فایل اجرایی متفاوت نیز مواجه هستیم. یکی از آنها دقیقاً شبیه باج‌افزار Phobos است که ۳ بخش از فایل‌ها را رمز می‌کند و گونه دیگر تنها ابتدای فایل‌ها را رمز می‌کند. مشاهدات حاکی از آن است که باج‌افزارهای خانواده Makop برای توزیع در بین مهاجمین از مدل RaaS استفاده می‌کنند. الگوی پسوندگذاری باج‌افزار در گونه‌های مختلف، به خوبی نمایانگر این موضوع است.

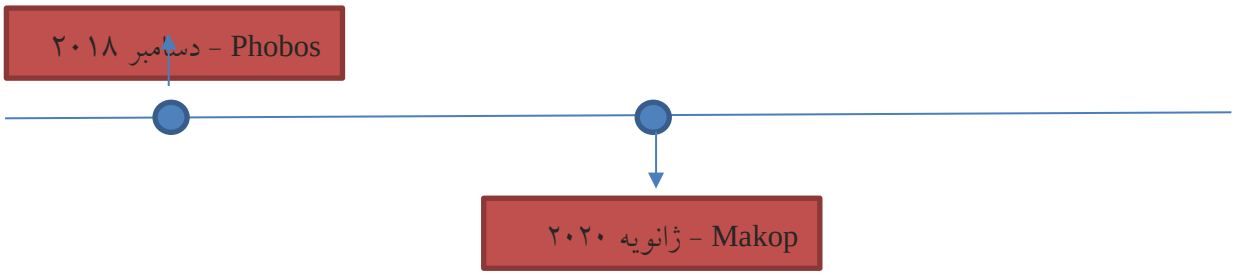
۲. مشخصات فایل‌های اجرایی:

نام فایل	d0dd0f7658b938f9a3036ce308f5018ae0cf3bc516aaf3c18b947afee136c043.exe
MD5	8D809510A9AE7B8EF6FC6A25E5FEAA22
SHA-1	EB0888326ADBBBDF1537A965C4D26C71549D43F6
SHA-256	D0DD0F7658B938F9A3036CE308F5018AE0CF3BC516AAF3C18B947AFEE136C043
نوع فایل	Win32 EXE
اندازه فایل	42.00 KB (43008 bytes)

نام فایل	ad534790700a9daa5fda6452692590e5e8c86d6a86aec0110822d0b54a6c21d9.exe
MD5	586d6732d8c8d4045b05276f2a0cbf53
SHA-1	e58187c1708079e9487310f8c4b34722e4271f35
SHA-256	ad534790700a9daa5fda6452692590e5e8c86d6a86aec0110822d0b54a6c21d9
نوع فایل	Win32 EXE
اندازه فایل	847.65 KB (867994 bytes)

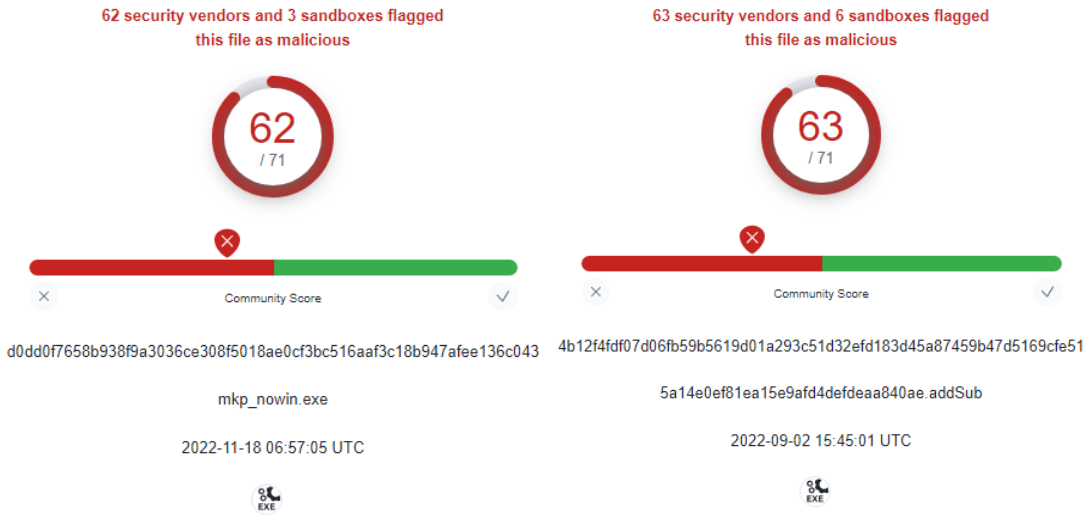
۳. شجره‌نامه

براساس گزارش‌های منتشر شده، ظاهراً باج‌افزار Makop نسخه‌ای توسعه یافته از باج‌افزار Phobos می‌باشد.



۴. میزان تهدید فایل باج‌افزار

دو نمونه از خانواده Makop در این تحلیل استفاده شده، که درحال حاضر ضدبدافزارهای سامانه VirusTotal بدین گونه آن‌ها را تحلیل می‌کنند:



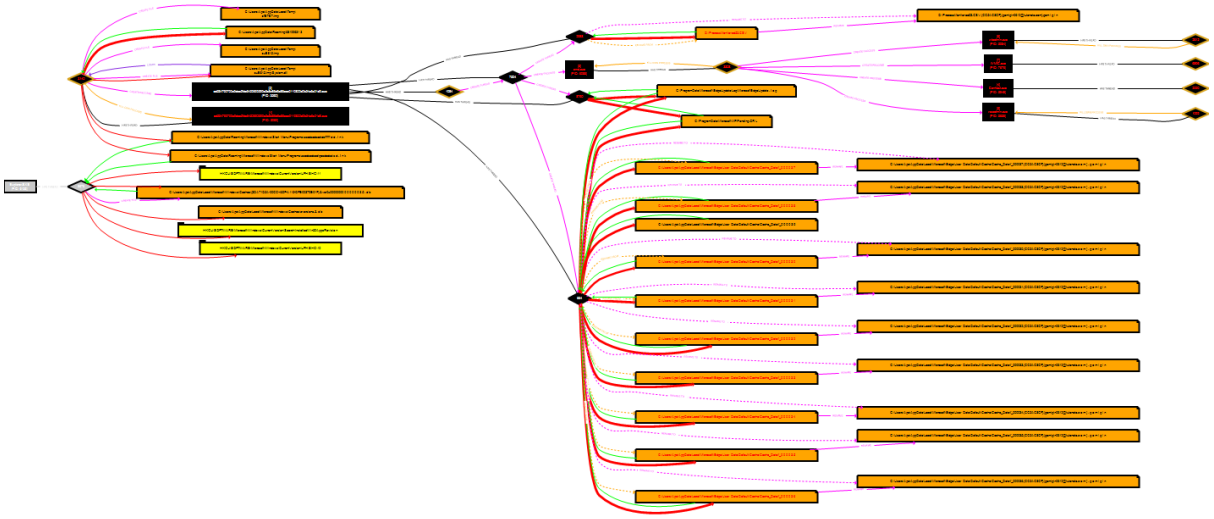
۵. تحلیل پویا

۵-۱ آناتومی حمله

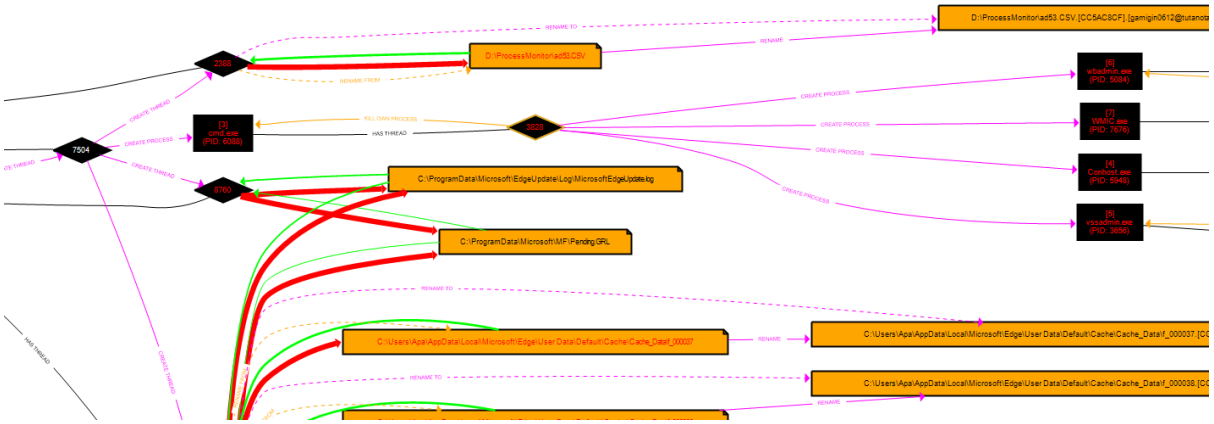
باج‌افزار Makop از آیکن نرم‌افزار اکسل برای فایل اجرایی خود استفاده کرده تا کاربران ناآگاه را فریب دهد.

پس از اجرای باج‌افزار در محیط آزمایشگاهی، رفتار زیر مشاهده شد:

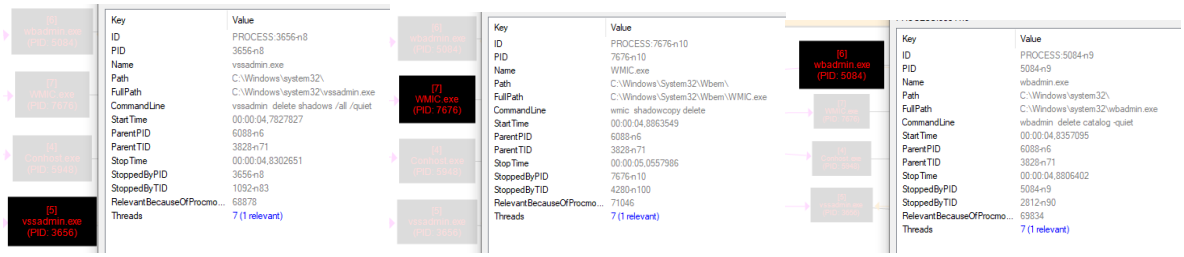
(گراف‌ها مربوط به نمونه ad534790700a9daa5fda6452692590e5e8c86d6a86aec0110822d0b54a6c21d9 می‌باشند.)



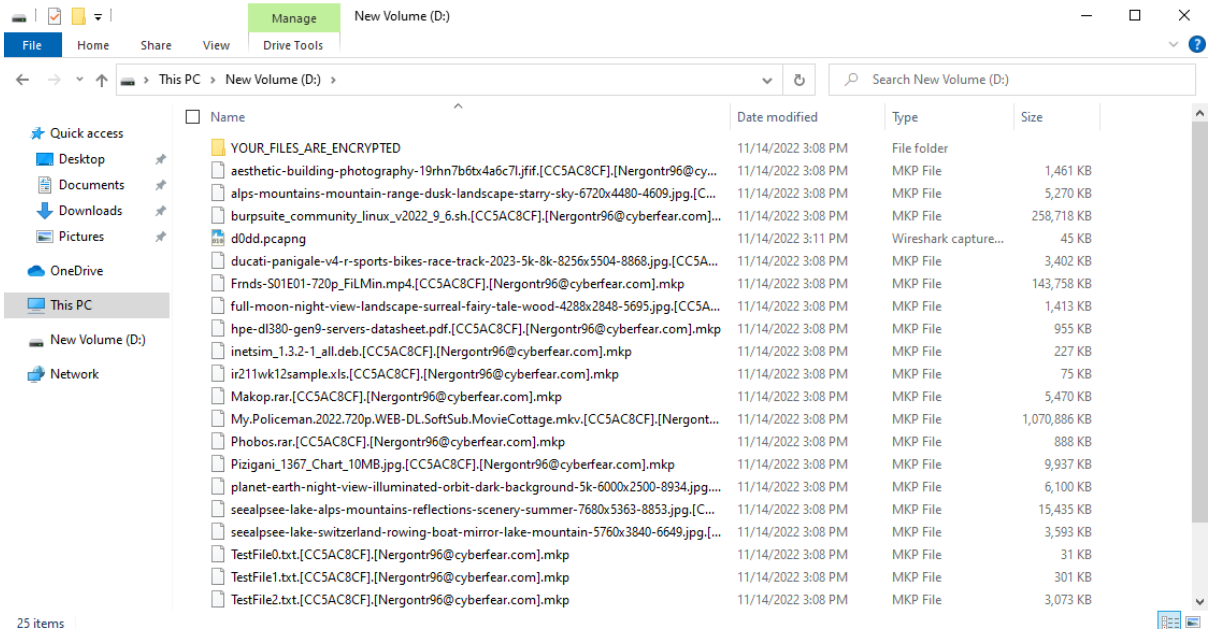
باج‌افزار در همان ابتدای فعالیت خود با فراخوانی cmd.exe در سیستم قربانی، دستورات زیر را اجرا می‌کند:



حذف فضای VSC	*cmd.exe vssadmin delete shadows /all /quiet*
حذف اطلاعات بکآپ‌ها	*cmd.exe wbadmin delete catalog -quiet*
حذف فایل‌های VSC	*cmd.exe wmic shadowcopy delete*



سپس، فرآیند رمزگذاری فایل‌ها در سیستم قربانی شروع می‌شود؛ ابتدا تغییرات روی فایل‌ها صورت می‌گیرد و بعد از آن نام آنها تغییر می‌کند. تصویر زیر، فایل‌های رمزگذاری شده توسط نمونه اول را نشان می‌دهد.



همانطور که در تصویر بالا قابل مشاهده است به انتهای هر فایل رمزشده پسوند زیر اضافه شده است:

.[CC5AC8CF].[Nergontr96@cyberfear.com].mkp

الگوی نامگذاری پسوندها به این صورت می‌باشد:

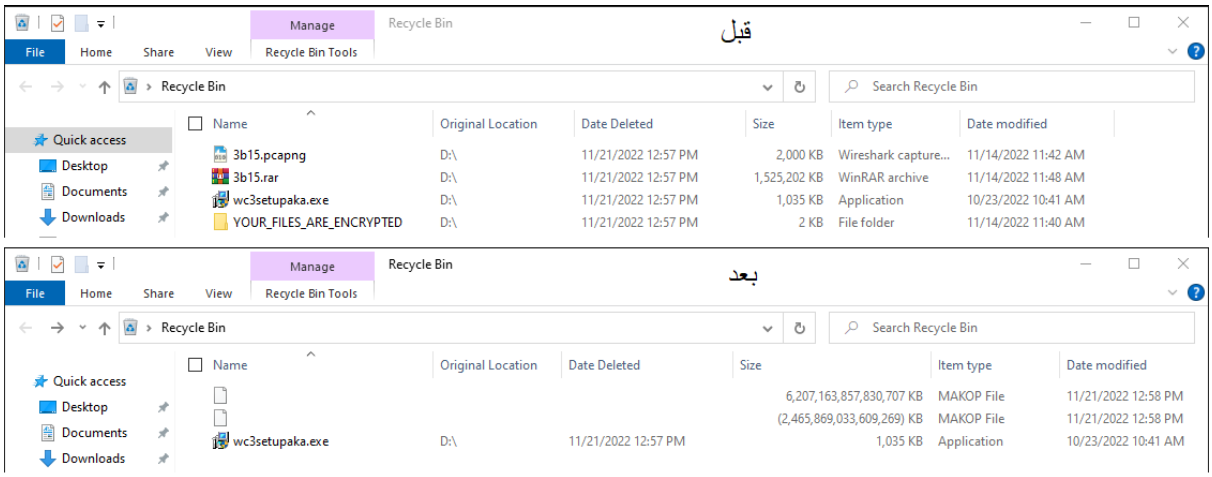
"original-filename.[unique-ID].[email-address].makop-extension"

می‌باشد. از جمله پسوندهای دیگری که این خانواده باج‌افزاری استفاده می‌کند عبارتند از:

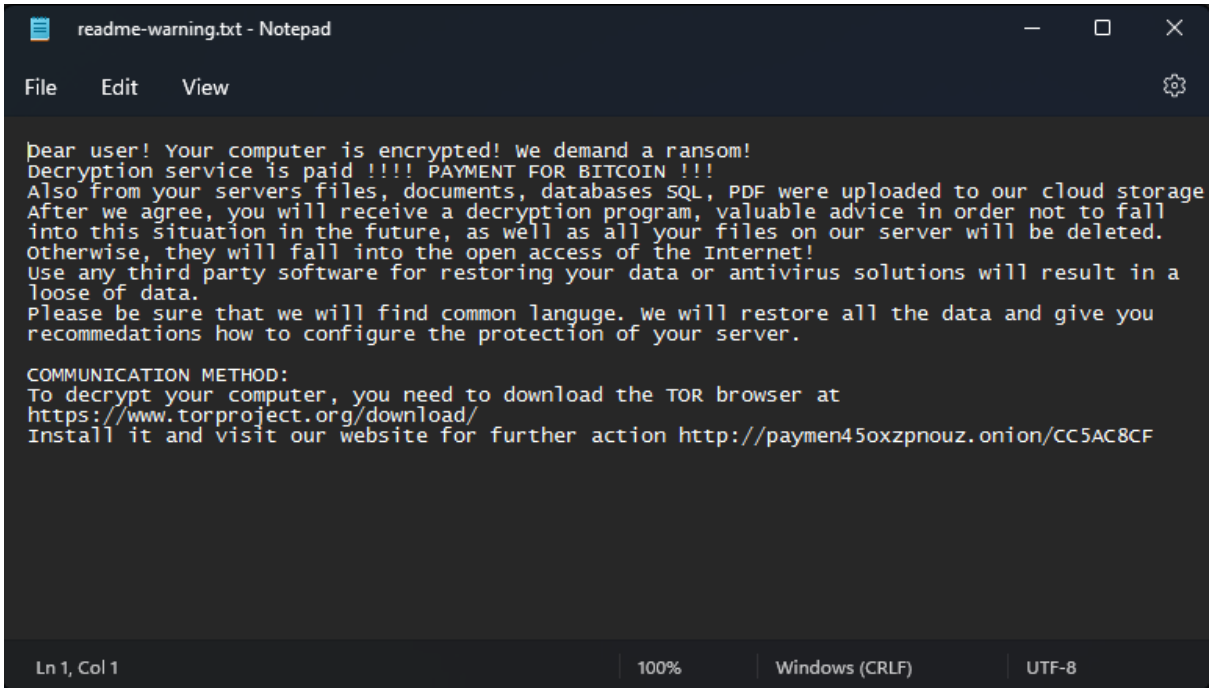
.makop ، .gamigin ، .razer و .KJHslgjkjdfg

با بررسی دقیق‌تر این باج‌افزار متوجه می‌شویم که فایل‌هایی با پسوندهای exe. و dll. جزو لیست سفید باج‌افزار هستند و در این فرآیند، رمزگذاری نمی‌شوند. ضمناً دایرکتوری‌های Windows یا Winnt در درایو سیستم‌عامل (در اینجا :C) دست نخورده باقی می‌مانند.

باج‌افزار Makop فایل‌های درون Recycle Bin را نیز رمز می‌کند و پوشه‌های درونش را پاک می‌کند. همچنین میانبرهای برنامه‌ها روی دسکتاپ یا منوی استارت، پس از اجرای باج‌افزار حذف می‌شوند.

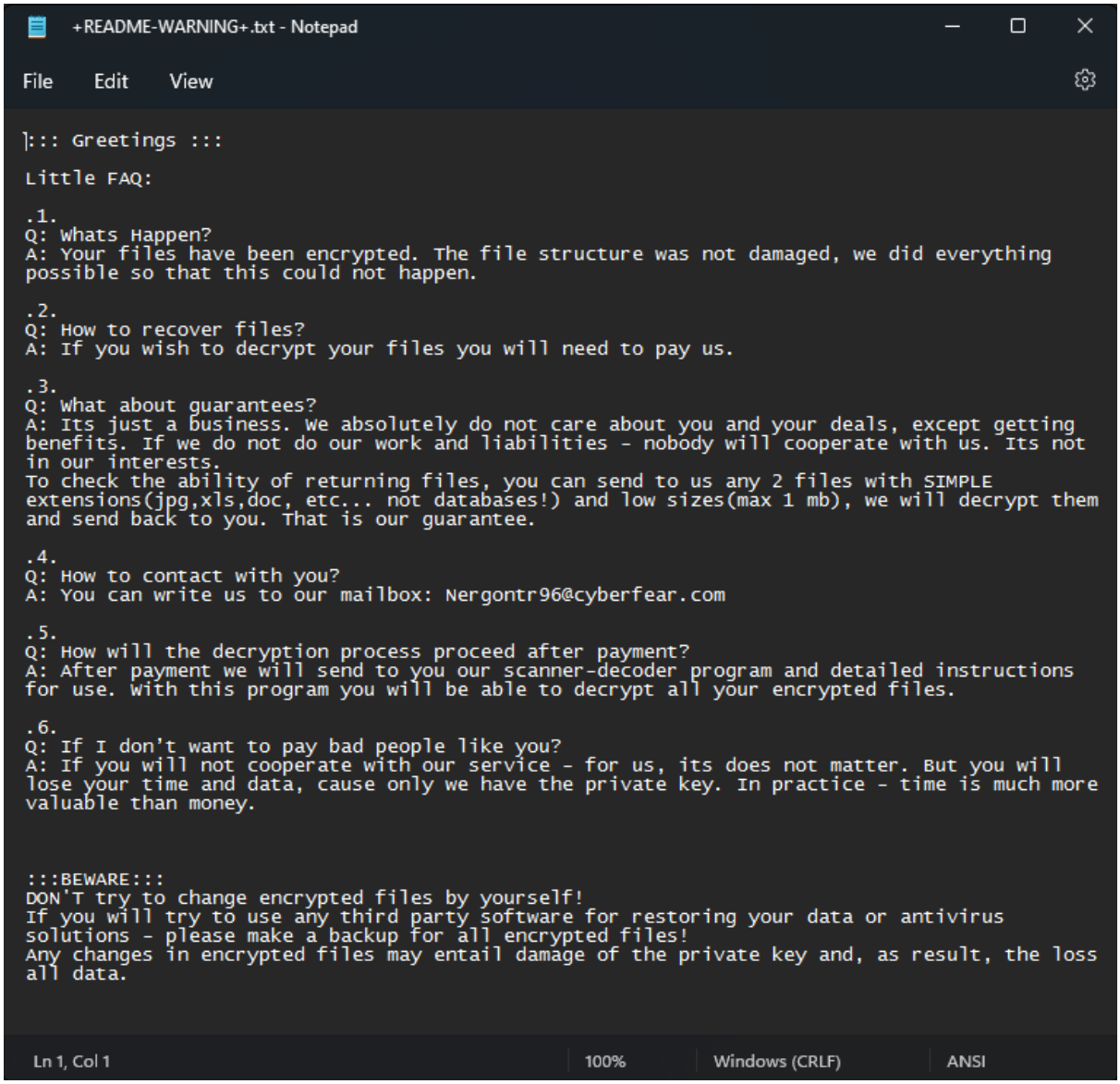


در ادامه، فایل پیغام باج‌خواهی این باج‌افزار با عنوان +README-WARNING+.txt یا readme-warning.txt بر روی Desktop و همینطور در پوشه‌ای به نام YOUR_FILES_ARE_ENCRYPTED در دایرکتوری‌هایی که عملیات رمزگذاری صورت گرفته و همچنین در برخی نمونه‌های باج‌افزار، بصورت فایلی به اشتراک‌گذاشته شده در شبکه شده قابل مشاهده است.



(پیغام بالا مربوط به نمونه 4b12f4fdf07d06fb59b5619d01a293c51d32efd183d45a87459b47d5169cfe51 می‌باشد)

در پیغام باج‌خواهی فوق، پرداخت باج بصورت بیتکوین و بدون ذکر مبلغ درخواست شده و جملاتی برای ترساندن مخاطب مانند "بارگذاری اطلاعات مهم برروی سرور آن‌ها" و یا "درصورت همکاری نکردن اطلاعات در اینترنت منتشر می‌شود" استفاده شده است؛ همچنین راه ارتباطی برای تبادل بیان شده است.

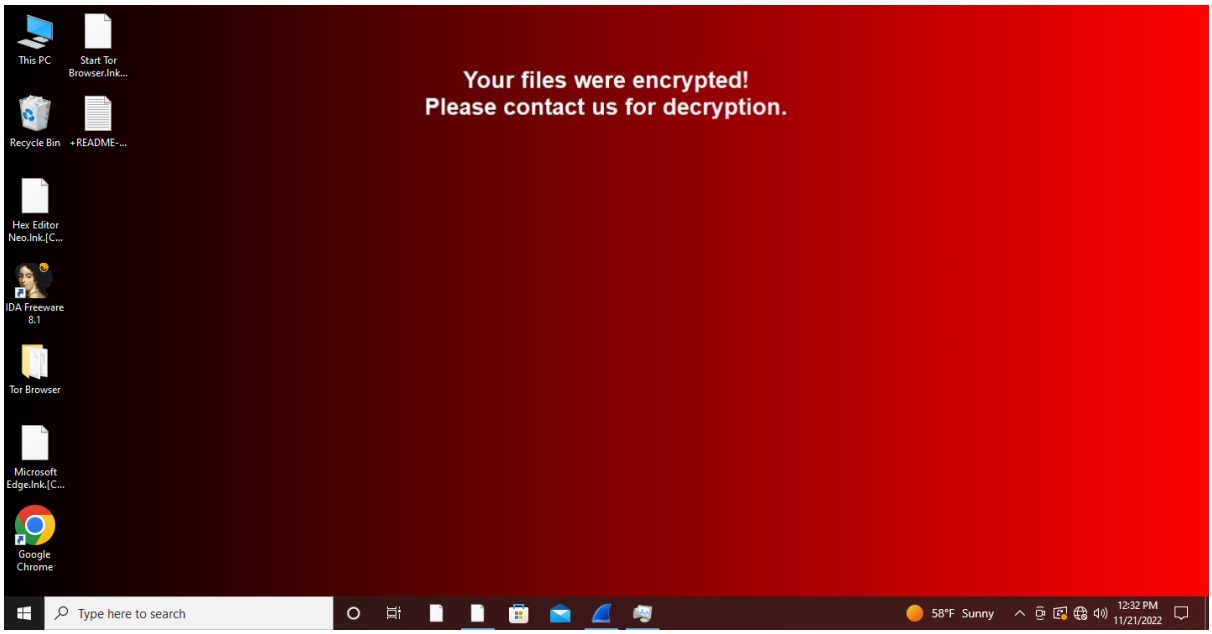


(پیغام بالا مربوط به نمونه d0dd0f7658b938f9a3036ce308f5018ae0cf3bc516aaf3c18b947afee136c043 می‌باشد)

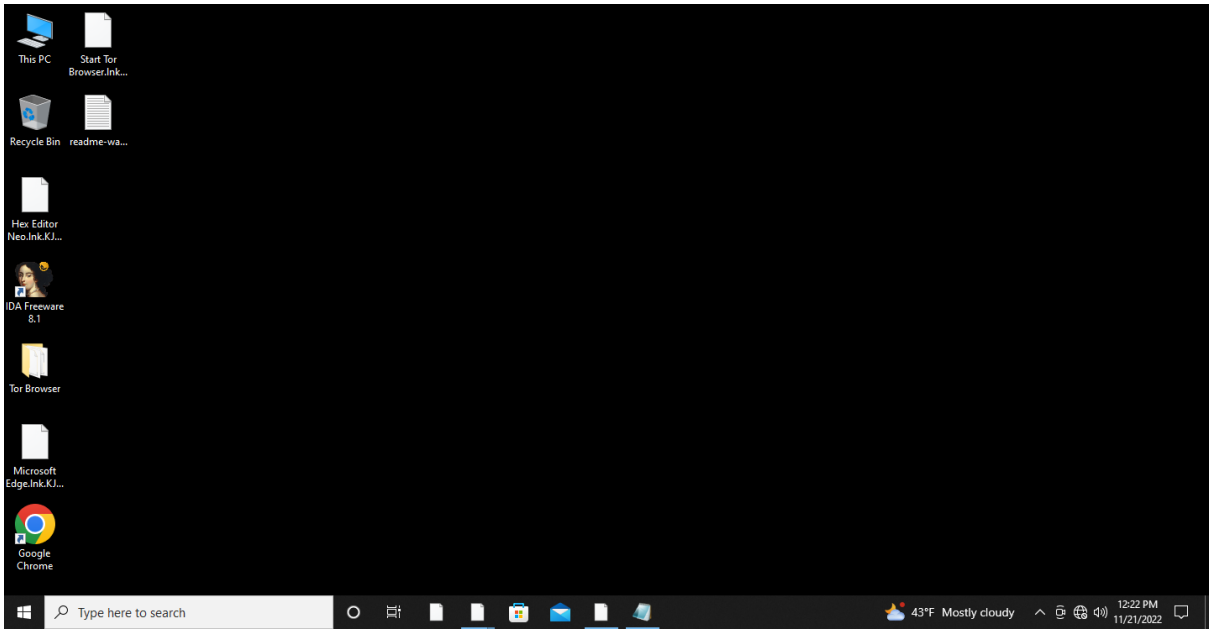
اما بر اساس پیغام باج‌خواهی فوق که برای خانواده Makop معمول‌تر است گفته شده که فایل‌ها رمز شده‌اند ولی به ساختار آن‌ها آسیبی نرسیده است و برای بازیابی خواستار پرداخت باج شده است. برای اطمینان هم گفته شده می‌توان دو فایل ساده و کم‌حجم برای مهاجمین فرستاد تا رایگان رمزگشایی کنند. همچنین یک آدرس ایمیل برای برقراری ارتباط با مهاجمین آورده شده است. در ادامه به عباراتی از قبیل اینکه "فایل‌ها برای آن‌ها اهمیتی ندارد"، "اگر سعی در رمزگشایی شود ممکن است خراب شوند" و ... اشاره شده است.

همانطور که در ابتدا اشاره شد، با دو گونه باج‌افزار Makop با رفتارهای متفاوت مواجه هستیم. هر دو گونه را در محیط آزمایشگاهی اجرا کردیم و نتایج زیر حاصل شد:

گونه اول:



گونه دوم:



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

۵-۲ روش انتشار:

طبق شواهد موجود و گزارشات بدست آمده، باج‌افزار Makop معمولاً از طریق ایمیل‌های فیشینگ به قربانی می‌رسد و یا بصورت ماکرو در سندهای آفیس قرار داده می‌شود. گزارشاتی نیز مبنی بر انتشار باج‌افزار از طریق پروتکل دسترسی از راه دور (RDP) به دست رسیده است. هدف این باج‌افزار بطور کلی سیستم‌های خانگی و اداری با اطلاعات نسبتا مهم می‌باشد.

۵-۳ روش مقابله:

هم‌اکنون خانواده باج‌افزار Makop توسط اکثر آنتی‌ویروس‌های معتبر قابل شناسایی است. توصیه می‌گردد ضمن بروزرسانی سیستم‌عامل و نرم‌افزارها، از نصب و بروزرسانی آنتی‌ویروس معتبر اطمینان حاصل کنید. در سازمان‌ها پیشنهاد می‌گردد علاوه بر موارد فوق، در لایه‌های مختلف شبکه از ماژول آنتی‌اسپم استفاده گردد و از طریق آموزش کاربران در مواجهه با اسپم‌ها و ایمیل‌های فیشینگ، ریسک آلودگی به باج‌افزار را کاهش دهید. همچنین به عنوان یک اصل، همواره محدودیت‌های لازم را برای استفاده از سرویس‌های دسترسی از راه دور رایج از قبیل RDP، Anydesk و ... بکار بگیرید.

۶. تحلیل ایستا

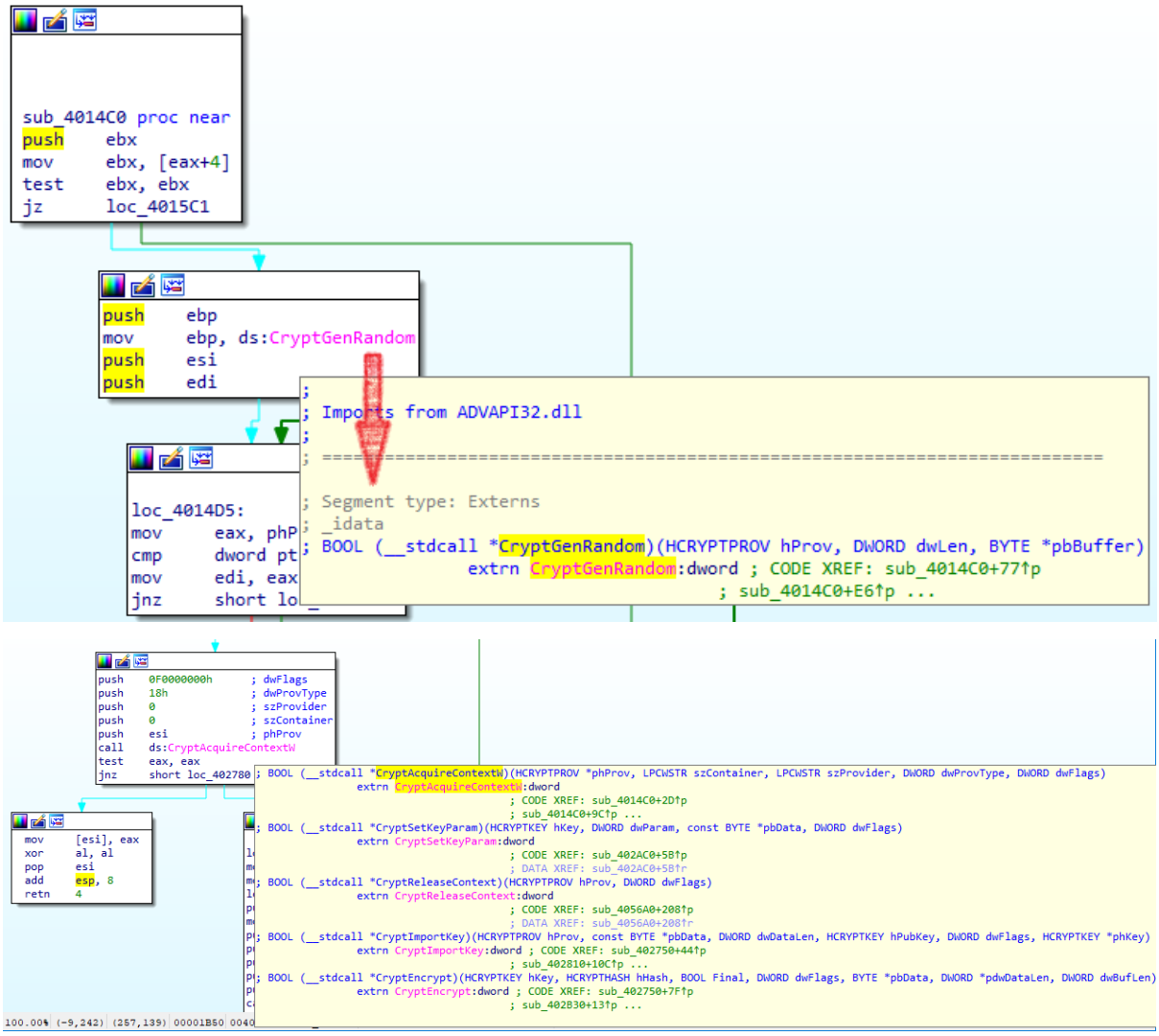
بررسی‌های اولیه بر روی فایل‌های اجرایی این خانواده باج‌افزار نشان می‌دهد که باج‌افزار Makop بر روی تمامی نسخه‌های سیستم‌عامل ویندوز از NT به بعد، اجرا خواهد شد.

linker-version	80.0	80.0
os-version	4.0	Windows NT 4.0
image-version	0.0	0.0
subsystem-version	4.0	4.0

۶-۱ تحلیل کد:

کد باج‌افزارهای خانواده Makop بصورت obfuscate شده می‌باشد ولی بطور کلی یک رفتار کلی ثابت دارد که به همین دلیل در اینجا تنها بر روی یکی از نمونه بررسی کد را انجام می‌دهیم.

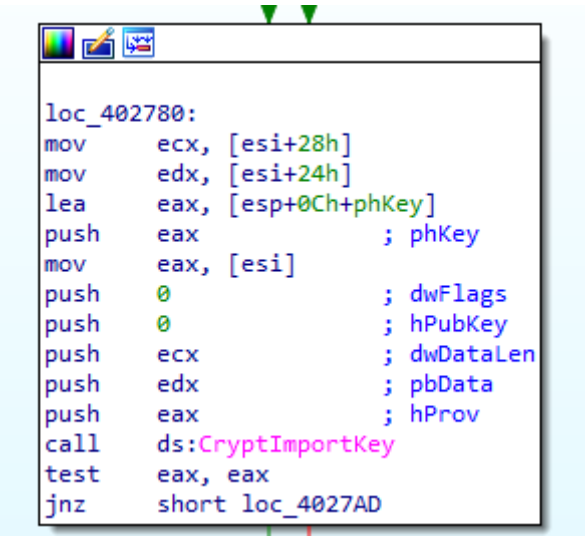
(نمونه d0dd0f7658b938f9a3036ce308f5018ae0cf3bc516aaf3c18b947afee136c043)



تصاویر بالا فرآیندهای مربوط به بازخوانی کلید عمومی با الگوریتم رمزنگاری RSA و همچنین ساخت کلیدهای بعدی برمبنای الگوریتم رمزنگاری متقارن AES256 را در کد باج‌افزار نشان می‌دهد.

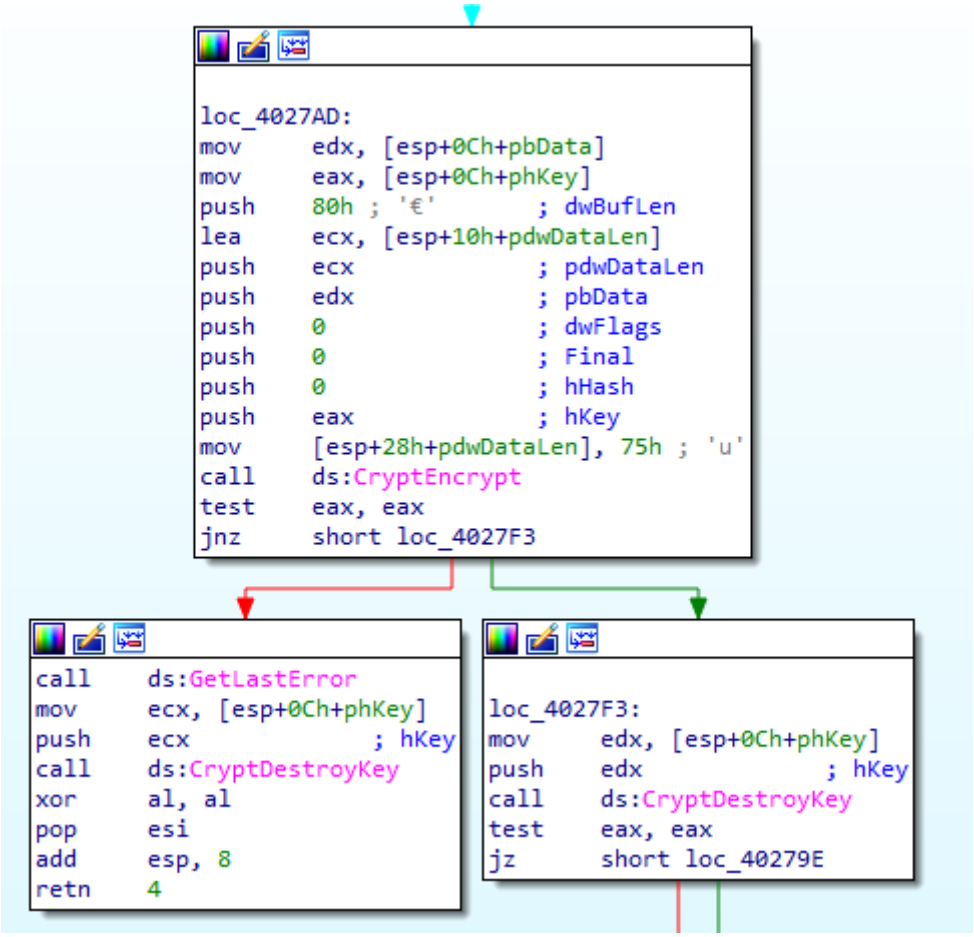
```
mov     esi, ds:wsprintfW
push    ebp
lea     edx, [esp+48h+var_24]
push    offset aC       ; "\\\\.\\%c:"
push    edx             ; LPWSTR
call    esi ; wsprintfW
push    ebp
lea     eax, [esp+54h+RootPathName]
push    offset aC_0     ; "%c:\\"
push    eax             ; LPWSTR
call    esi ; wsprintfW
add     esp, 18h
lea     ecx, [esp+44h+RootPathName]
push    ecx             ; lpRootPathName
call    ds:GetDriveTypeW
push    ebx             ; nFileSystemNameSize
push    ebx             ; lpFileSystemNameBuffer
push    ebx             ; lpFileSystemFlags
push    ebx             ; lpMaximumComponentLength
lea     edx, [esp+54h+VolumeSerialNumber]
push    edx             ; lpVolumeSerialNumber
push    ebx             ; nVolumeNameSize
mov     esi, eax
push    ebx             ; lpVolumeNameBuffer
lea     eax, [esp+60h+RootPathName]
push    eax             ; lpRootPathName
call    ds:GetVolumeInformationW
test    eax, eax
jnz     short loc_401362
```

در این بخش از کد باج‌افزار شروط پسوند فایل و دایرکتوری را برای بررسی لیست سفید و لیست سیاه بررسی می‌کند.



```
loc_402780:
mov     ecx, [esi+28h]
mov     edx, [esi+24h]
lea     eax, [esp+0Ch+phKey]
push    eax             ; phKey
mov     eax, [esi]
push    0               ; dwFlags
push    0               ; hPubKey
push    ecx             ; dwDataLen
push    edx             ; pbData
push    eax             ; hProv
call    ds:CryptImportKey
test    eax, eax
jnz     short loc_4027AD
```

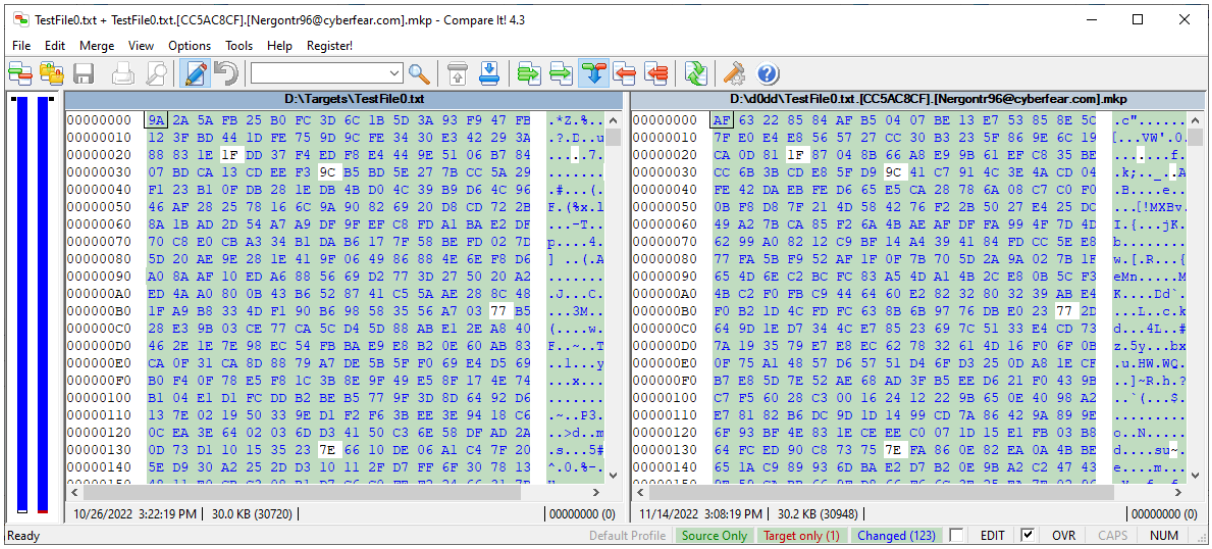
در اینجا عملیات رمزنگاری فایل‌ها با import شدن کلید عمومی شروع می‌شود.



و بدین گونه بخشی از رمزگذاری انجام و کلیدها از حافظه پاک می‌شوند.

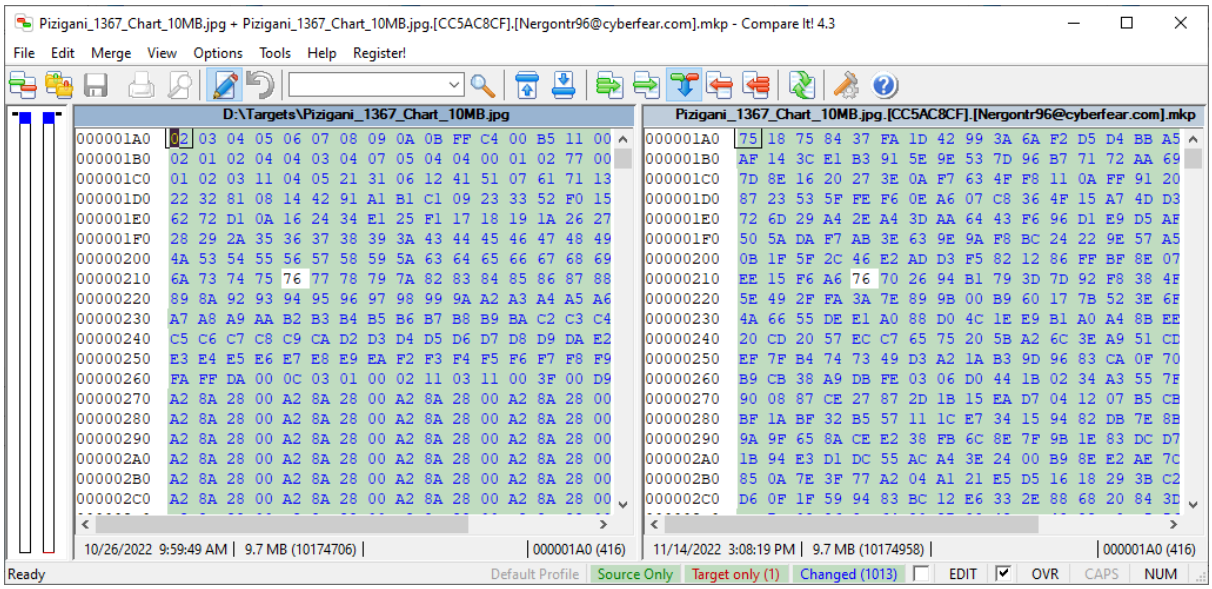
```
LABEL_9:
  wsprintfW(PathName, L"%s\\%s", a2, a5);
  DirectoryW = CreateDirectoryW(PathName, 0);
  if ( DirectoryW )
  {
    a2 = PathName;
LABEL_11:
    LOBYTE(DirectoryW) = sub_4075F0(a3, (int)a2, a1, a4);
  }
  return DirectoryW;
```

پس از بررسی چند نمونه فایل سالم با نمونه رمزشده آن‌ها در خانواده باج‌افزار Makop مشخص گردید که باج‌افزار همیشه دو کلید جدید تولید می‌کند که بردار مقدار اولیه آن در انتهای فایل اضافه می‌شود؛ همچنین فایل‌های با حجم زیر 1.5MB را بطور کامل رمزگذاری می‌کند.

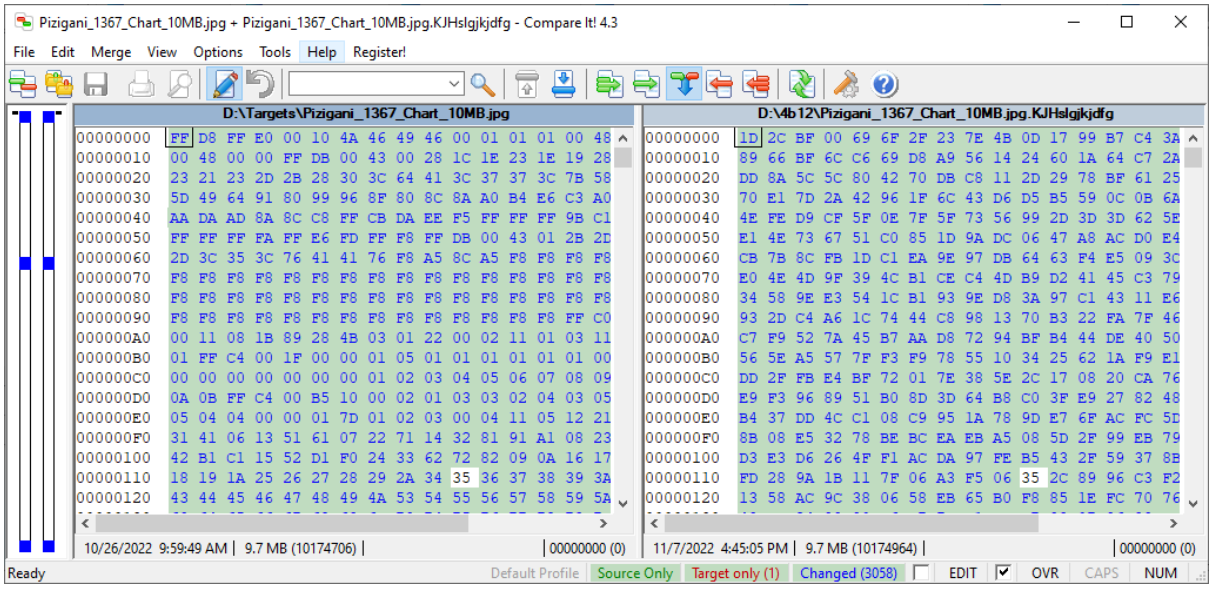


این باج‌افزار برای فایل‌های با حجم بیشتر از 1.5MB دو رفتار متفاوت نشان می‌دهد.

در برخی گونه‌ها تنها ابتدای هر فایل را به اندازه 256KB رمز می‌کند و در انتهای فایل نیز بین ۲۵۲ تا ۳۳۲ بایت به انتهای هر فایل رمزشده اضافه می‌نماید:



و در برخی دیگر سه بخش از فایل به مکان‌های ابتدا، یک‌سوم بعد از ابتدای فایل و انتهای فایل را رمزگذاری می‌کند و در انتهای فایل نیز بین ۲٤٤ تا ۳٤۰ بایت به انتهای هر فایل رمزشده اضافه می‌نماید:



۶-۲ تحلیل ترافیک شبکه:

پس از بررسی ترافیک شبکه ضبط شده حین اجرای باج‌افزار و همچنین بررسی نتایج سندباکس‌های آنلاین، هیچ‌گونه ارتباط شبکه‌ای مرتبط با باج‌افزار مشاهده نشد و نتایج نشان داد که باج‌افزار Makop کاملاً آفلاین فعالیت می‌کند.

۶-۳ رمزنگاری و رمزگشایی:

خانواده باج‌افزار Makop با الگوریتم رمزنگاری متقارن AES256 فایل‌ها را رمزگذاری می‌کند. بدین گونه که باج‌افزار از یک کلید با طول ۲۵۶ بایت برای رمزگشایی کلید عمومی RSA استفاده می‌کند، در ادامه دو کلید جدید با استفاده از الگوریتم AES256 می‌سازد که با استفاده از آن‌ها اطلاعات فایل‌ها رمز می‌شوند، که برای هر کلید یک بردار مقدار اولیه جدید (IV) ۱۶بایتی نیز ساخته و در انتهای فایل ذخیره می‌شود. در انتها نیز هر دو کلید AES که برای رمزگذاری استفاده می‌شوند توسط کلید عمومی RSA رمزگذاری می‌شوند.

در نهایت باتوجه به رمزگذاری صورت گرفته توسط این خانواده در حال حاضر هیچ‌گونه ابزاری جهت رمزگشایی فایل‌های رمزشده توسط این باج‌افزار، ارایه نشده است.

۷. شناسه‌های تهدید (IOCs)

نمونه‌ها (Samples):

```
4b12f4fdf07d06fb59b5619d01a293c51d32efd183d45a87459b47d5169cfe51
3b15b66bf6a7d7ebab6437906686037f23a797d15e0fbff3d6741d3f58db8f1e
fe52d906fa596e7ae16633074ff7178b3ac40e26a93f0009f1b33d5cbf219e91
a6566bc4c76a36a0e880d2151e0a86a59c3af57082b7c83a669dba3f28afb959
7b367f4c26ea8c16697cd8b2d41e568a1fa3a6a7909475b7e0850dc38f374dce
50b0c7858bc2bb2d1fa3d441bd2c4e3930b88b77c6cef11a51af5705727d6639
```

۸. شناسایی (Detection)

با توجه به اینکه باج‌افزار Makop بلافاصله پس از اجرا، فضای VSS را حذف می‌کند، با استفاده از رول زیر در اسپلانک می‌توان گسترش باج‌افزار در شبکه را شناسایی کرد:

```
((EventCode="4688" OR EventCode="1") (CommandLine="*vssadmin* *delete* *shadows*" OR CommandLine="*wmic* *shadowcopy* *delete*" OR CommandLine="*vssadmin* *resize* *shadowstorage*")) OR (EventCode="5857" ProviderName="MSVSS__PROVIDER") OR (EventCode="5858" Operation="*Win32_ShadowCopy*")
```