باسمه تعالی

تحلیل فنی باج افزار Sepsis

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی به نام Sepsis خبر می‌دهد. بررسی‌ها نشان می‌دهد فعالیت این باج‌افزار در نیمه‌ی اول ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار از الگوریتم رمزنگاری AES استفاده می‌کند و به جز دایرکتوری‌هایی خاص در درایو اصلی ویندوز که در ادامه به آن اشاره خواهیم نمود، تمام فایل‌های موجود در سیستم قربانی شامل تصاویر، فایل‌های ویدئویی، اسناد، پایگاه داده‌ها و ... را رمزگذاری می‌کند و پسوند فایل‌ها را پس از رمزگذاری به [Sepsis@protonmail.com].SEPSIS. تغییر می‌دهد. این باج‌افزار همانند اکثر باج‌افزارها، پس از رمزگذاری فایل‌ها از قربانیان تقاضای بیت‌کوین می‌کند.

مشخصات فایل اجرایی :

نام فایل	scvhost.exe
MD۵	۱۲۲۱ac۹d۶۰۷af۷۳c۶۵fd۶c۶۲bec۳d۲۴۹
SHA-۱	۵۱۸d۵a۰a۸۰۲۵۱۴۷b۹e۲۹۸۲۱bccdaf۳b۴۲c۰d۰۱db
SHA-۲۵۶	۳c۷d۹ecd۳۵b۲۱a۲a۸fac۷cce۴fdb۳e۱۱c۱۹۵۰d۵a۰۲a۰c۰b۳۶۹f۴۰۸۲acf۰۰bf۹a
اندازه فایل	۱۶.۵ KB

فایل اجرایی این باج افزار دارای چهار بخش است :

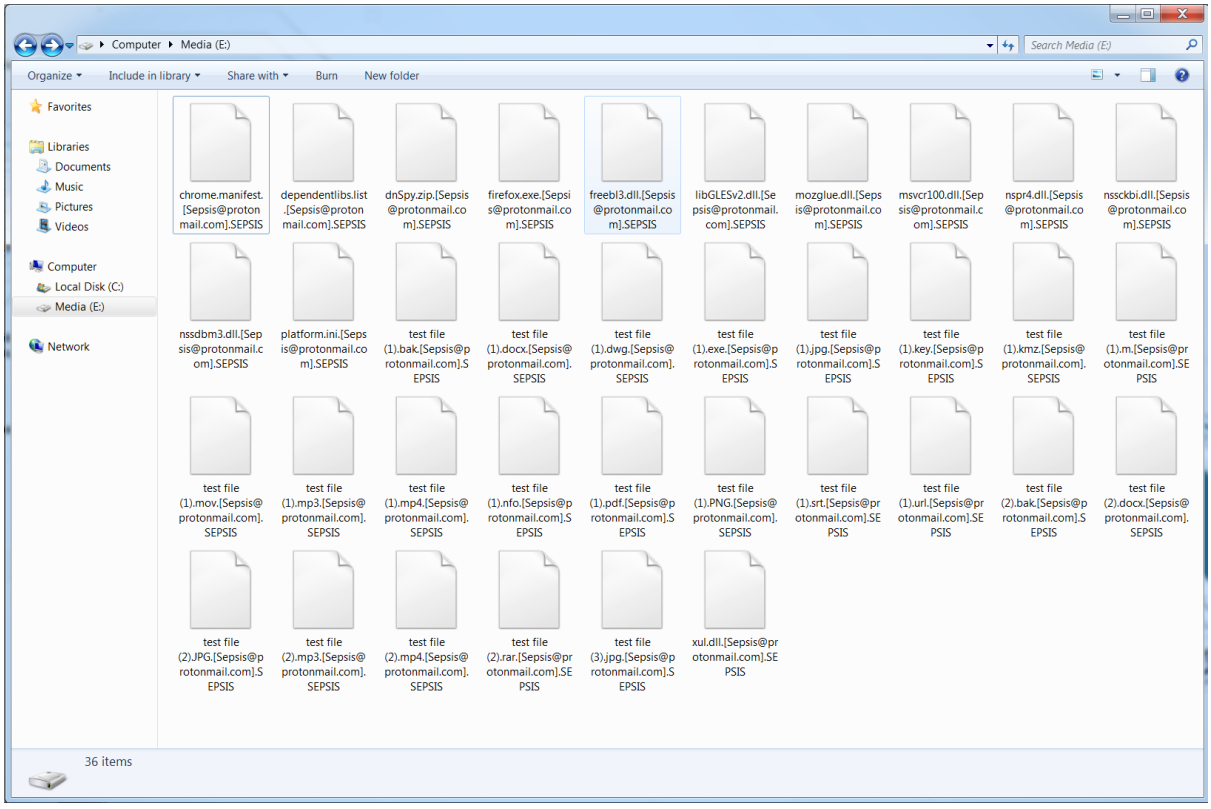
نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۱	۴۰۹۶	۵۸۲۲	۶۱۴۴
. rdata	۵.۲۲	۱۲۲۸۸	۴۱۸۸	۴۶۰۸
.data	۴.۹۳	۲۰۴۸۰	۸۱۵۲	۴۰۹۶
.reloc	۴.۷۹	۲۸۶۷۲	۶۲۴	۱۰۲۴

تحلیل پویا :

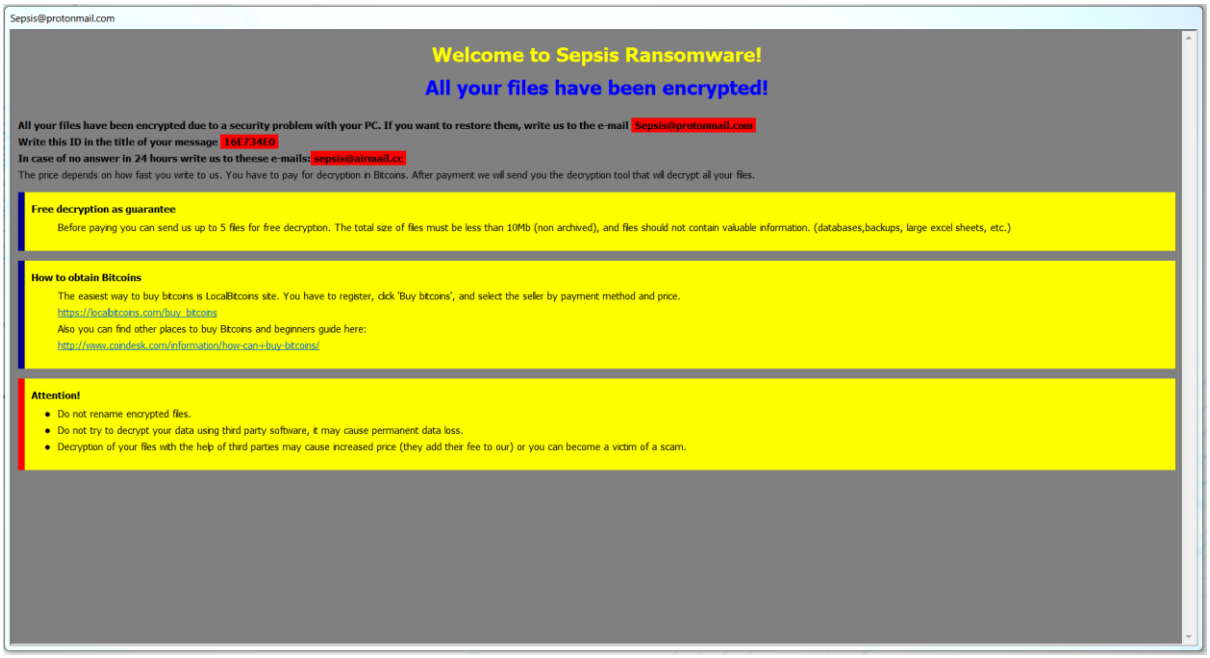
برای بررسی عمیق‌تر باج‌افزار Sepsis، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که باج‌افزار مورد اشاره پس از اجرا، فرایند مربوط به فایل اجرایی باج‌افزار را خاتمه می‌دهد و یک فرایند دیگر به نام svchost.exe در مسیر C:\Windows ایجاد می‌کند و فعالیت خود را جهت رمزگذاری فایل‌ها از این طریق ادامه می‌دهد. این باج‌افزار از الگوریتم رمزنگاری AES استفاده می‌کند و به جز دایرکتوری‌های زیر که در درایو اصلی ویندوز وجود دارند، تمام فایل‌ها را رمزگذاری می‌کند.

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، 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 آن‌ها دیگر قابل استفاده نخواهند بود. تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد.



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 باج افزار Sepsis را نشان می دهد.



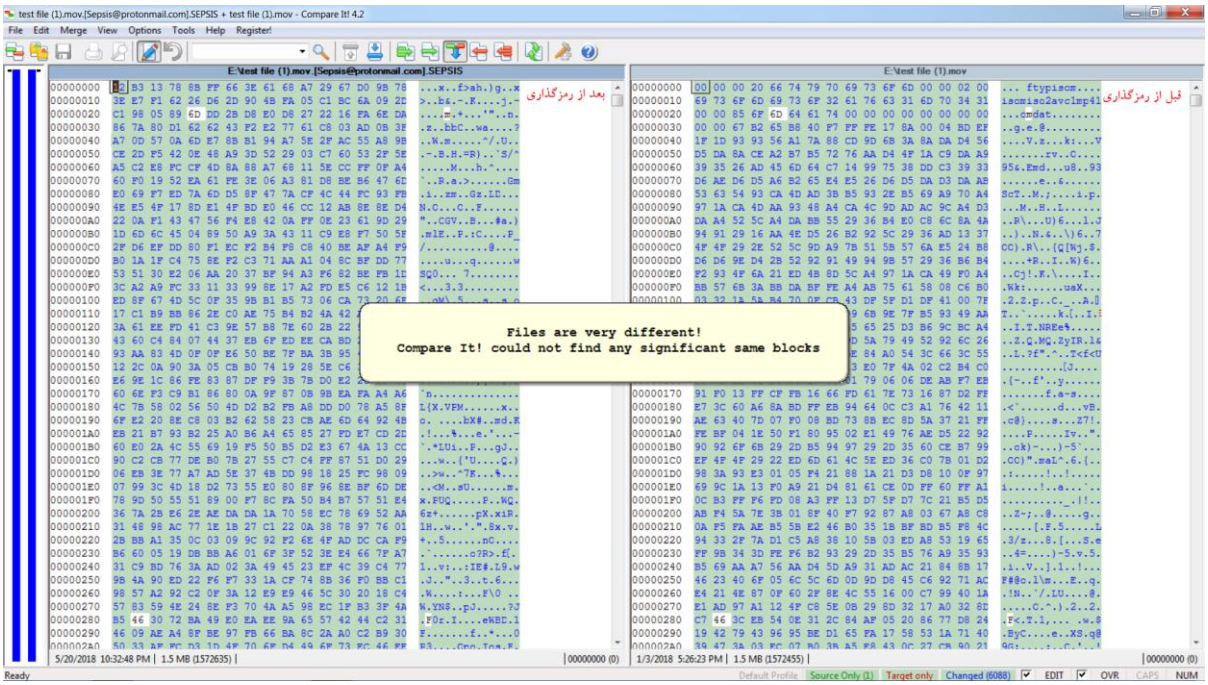
بر اساس پیغام باج‌خواهی، یک کد شناسایی منحصربفرد برای هر قربانی وجود دارد که قربانیان برای رمزگشایی فایل‌ها، باید از طریق آدرس ایمیل Sepsis@protonmail.com با مهاجمین ارتباط برقرار نمایند. در صورت عدم دریافت پاسخ از سوی مهاجمین طی ۲۴ ساعت، مهاجمین ایمیل دیگری به آدرس sepsis@airmail.cc قرار داده‌اند که 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 راه های متداول از جمله هرزنامه‌ها وجود دارد.

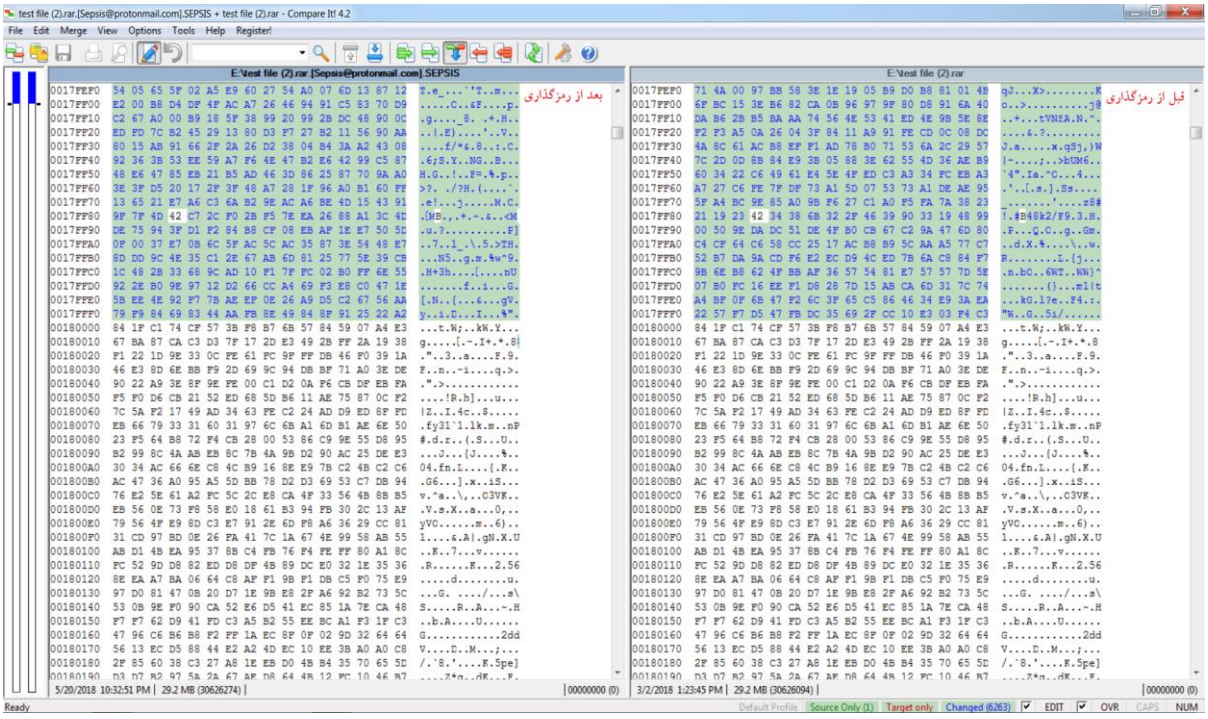
تحلیل ایستا:

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

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری توسط باج‌افزار انجام دادیم شاهد این بودیم که باج‌افزار Sepsis ساختار تمام فایل‌ها را به یک شکل رمزگذاری نمی‌کند و در مواجهه با فایل‌های مختلف رفتار متفاوتی از خود نشان می دهد. بدین صورت که ساختار بعضی از فایل‌ها را پس از رمزگذاری کاملا تغییر می‌دهد اما در مورد برخی از فایل‌ها فقط قسمتی از ساختار آن‌ها را تغییر می‌دهد، نتایج این بررسی‌ها در تصاویر زیر قابل مشاهده است :

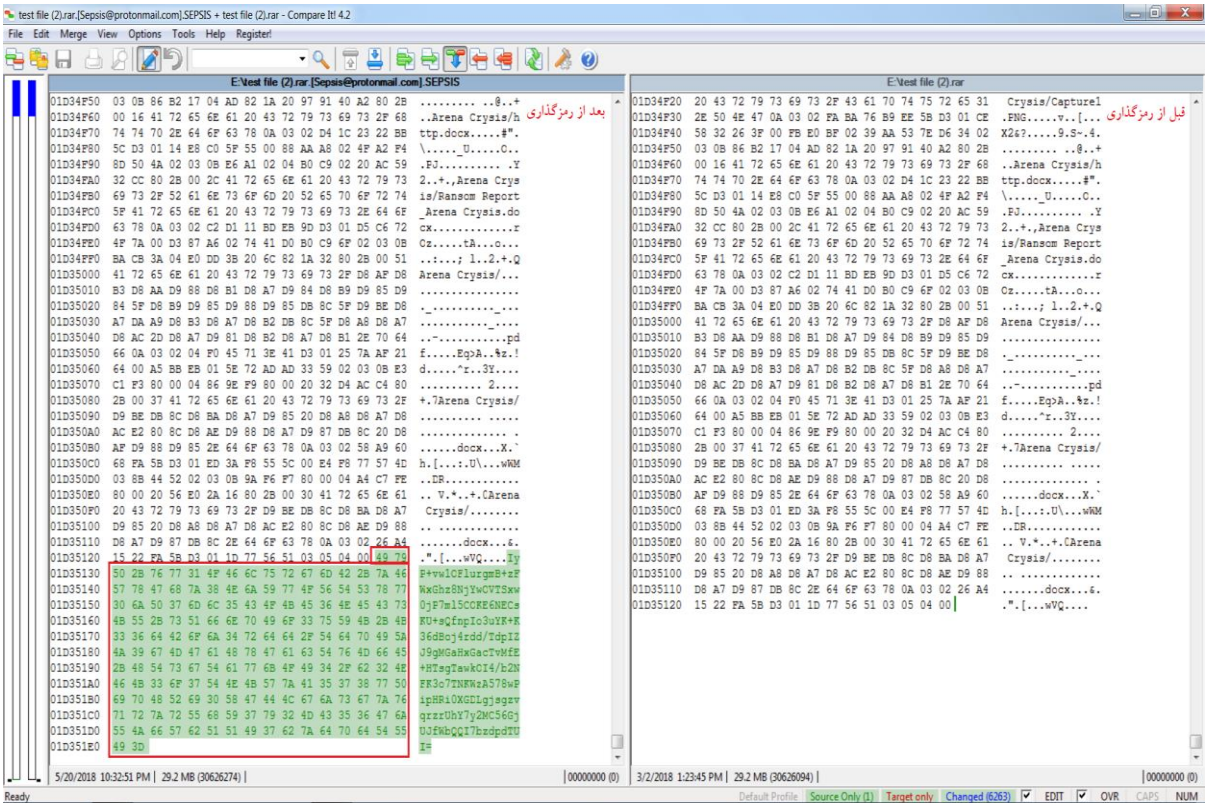


تصویر ۱ تمام ساختار فایل تغییر کرده است.

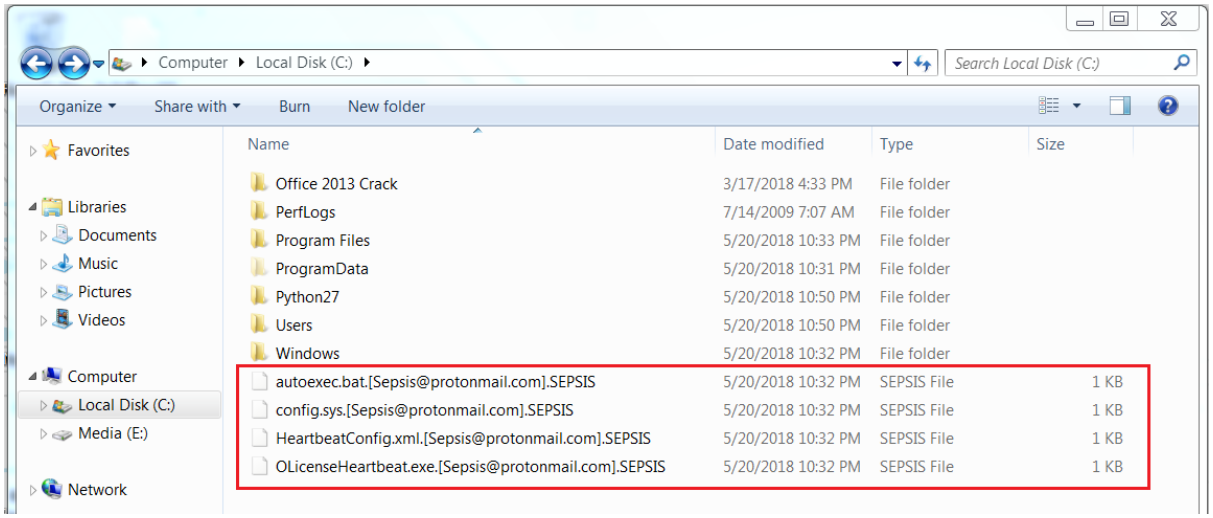


تصویر ۲ فقط بخشی از ساختار فایل تغییر کرده است.

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.



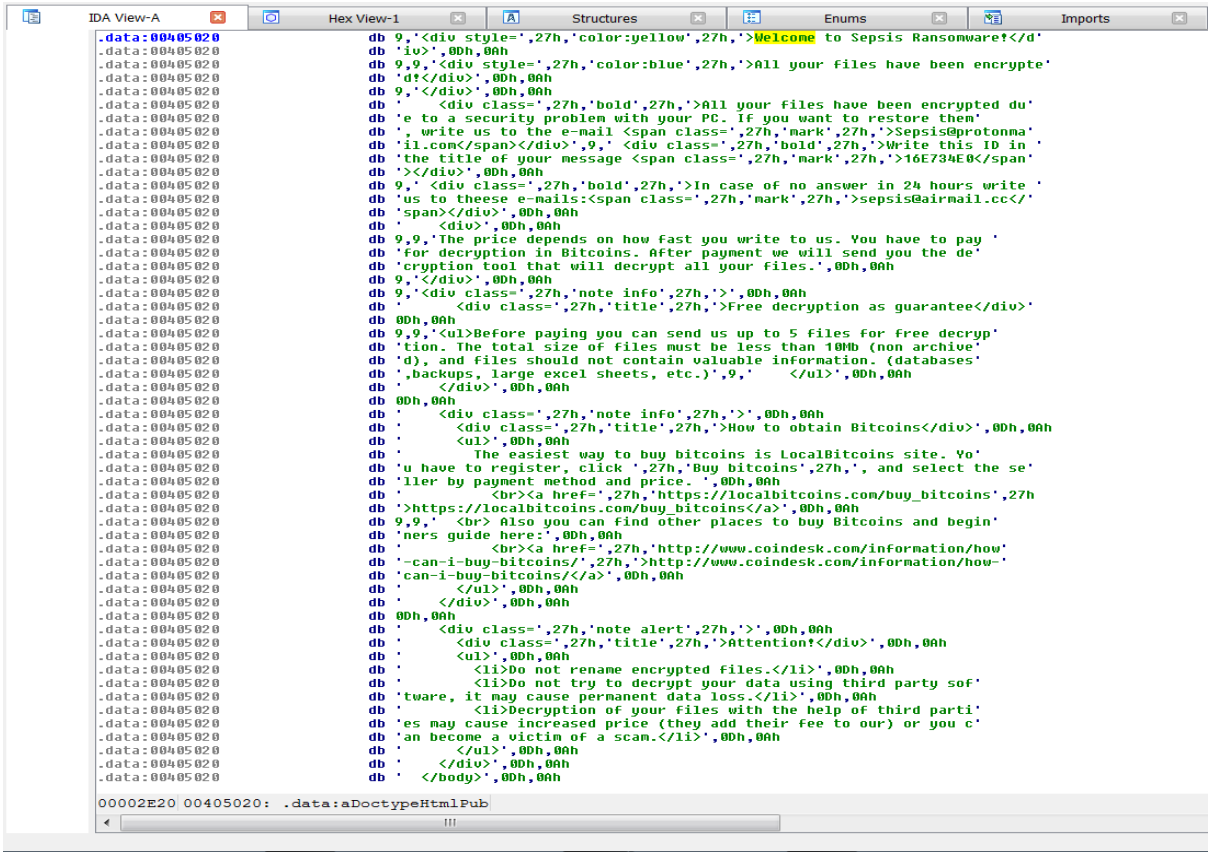
برخی از فایل‌های ایجاد شده توسط باج‌افزار، در تصویر زیر قابل مشاهده می‌باشد :



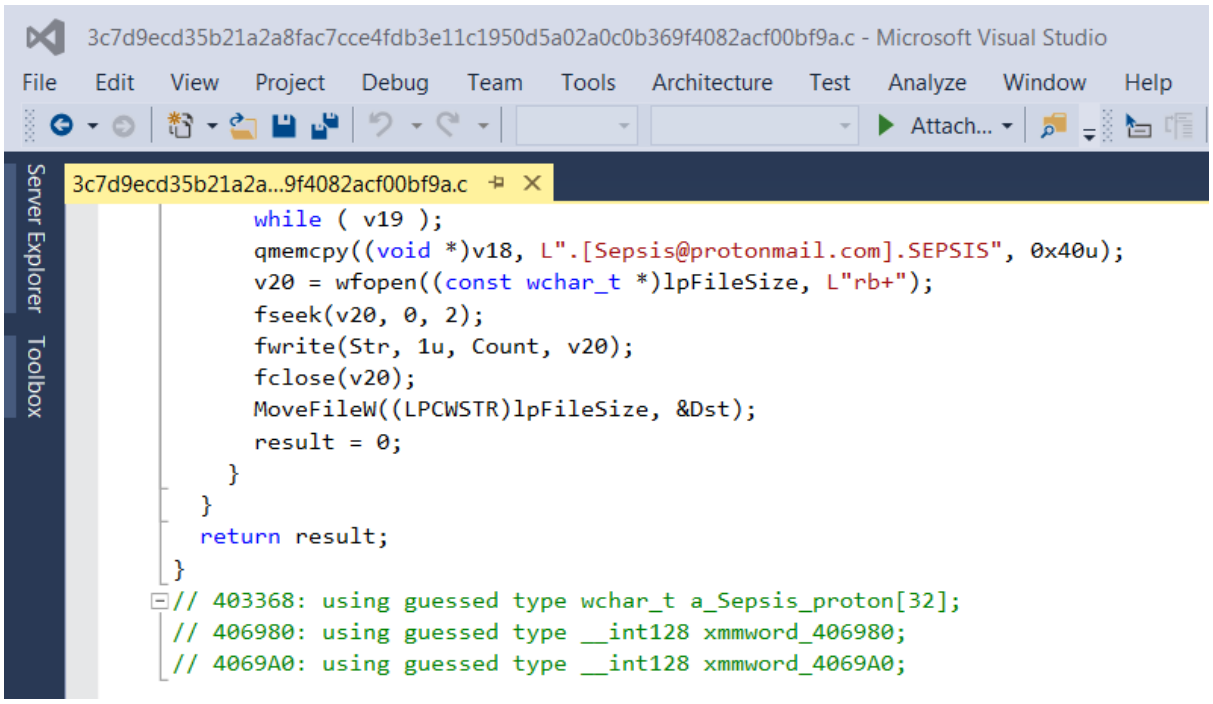
مقدار کلید عمومی باج‌افزار جهت رمزگذاری فایل‌ها در زیر قابل مشاهده می‌باشد.

```
MIGfMA•GCSqGSIb٣DQEBAQUAA٤GNADCBiQKBgQDgrfmmBw٩٩c٦k٤٧/OBto•QuJnIFNLJyqo
cECDo١SCCTpZ١RbCx٥iTwuZN٢DqaI٢z٦٩bsRWKprUBSLjSQYEPs/٣qEpQV٨qKZl٩JdlSbA٥qxTgH
mQkMMKLdy•w•O٤BDi١D٦XhOFJOXLl٣uA٤٨١oEMD+rM•p٨qxBBPY٣٢KtaQoQuahQIDAQAB
```

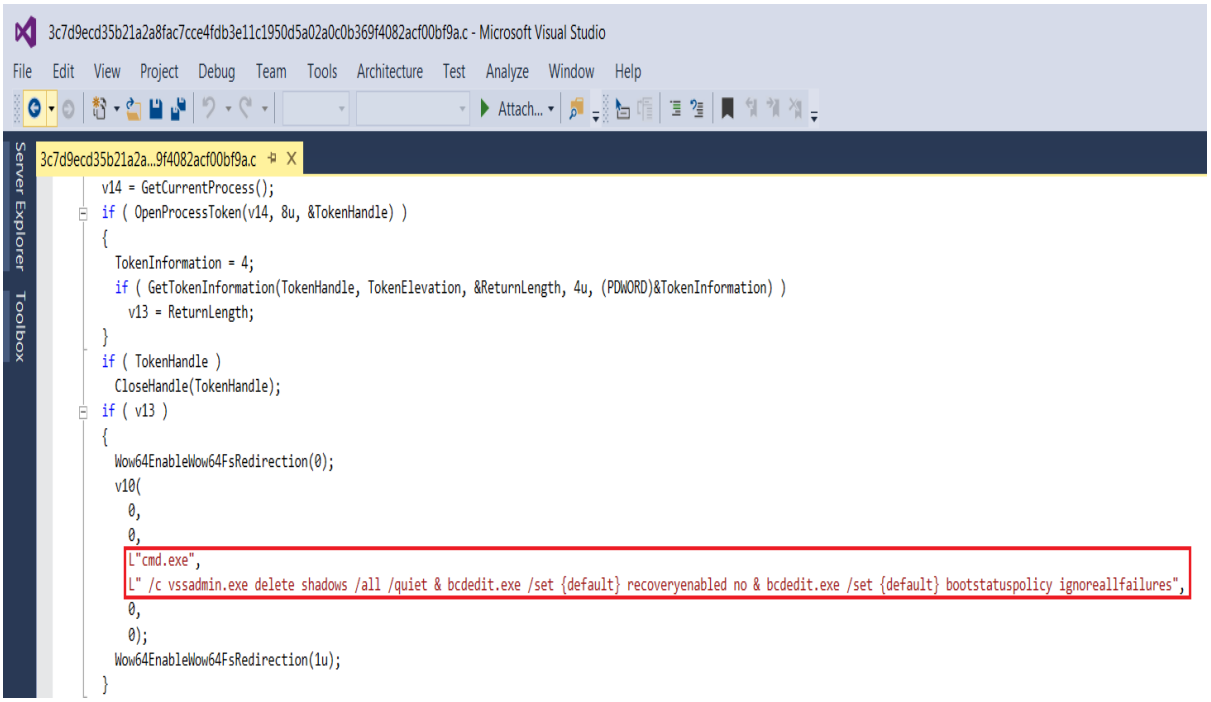
تصویر زیر مربوط به پیغام باج‌خواهی باج‌افزار می‌باشد.



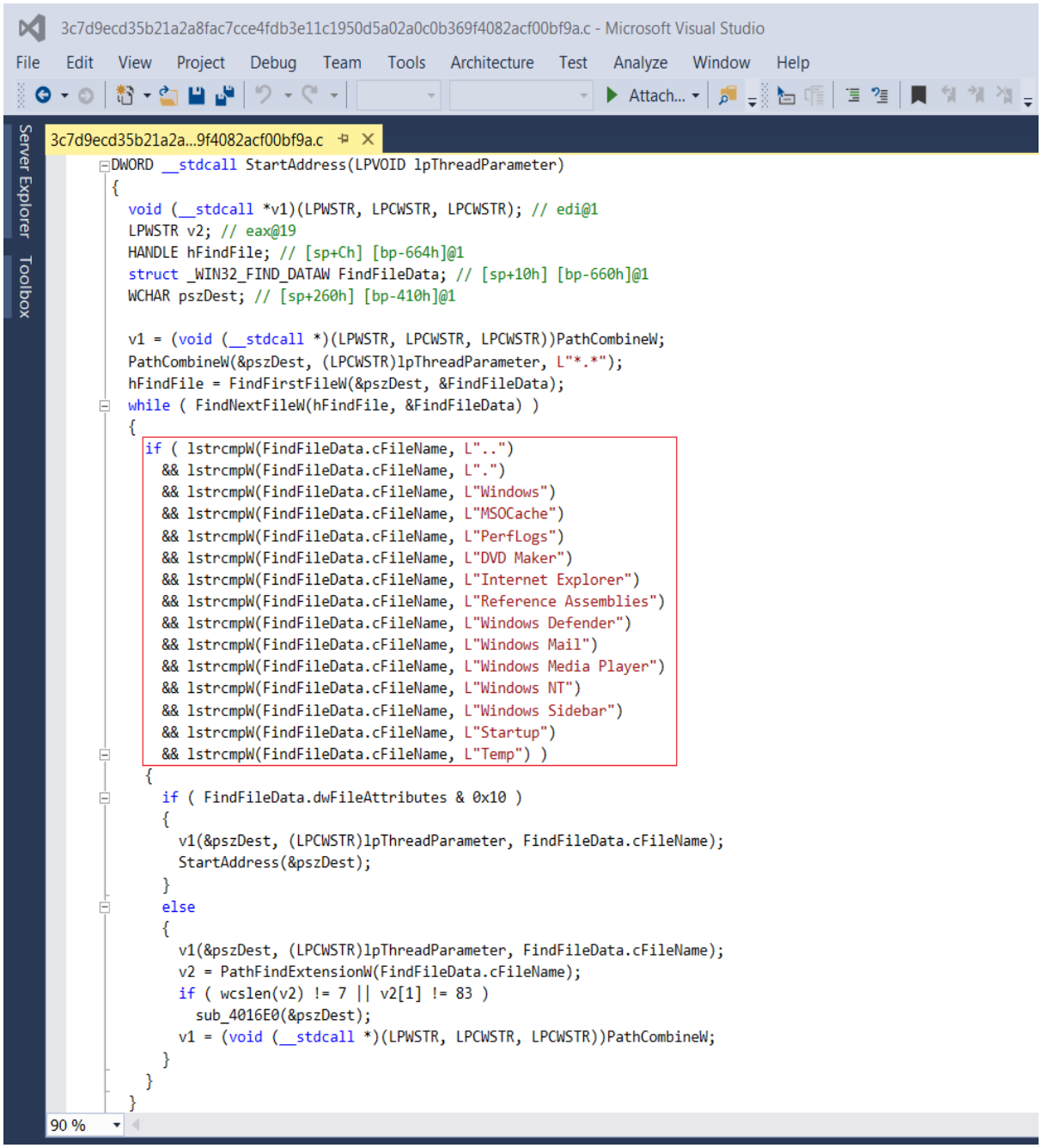
همانطور که اشاره شد باج‌افزار Sepsis پس از رمزگذاری فایل‌ها به انتهای آن‌ها پسوند [Sepsis@protonmail.com].SEPSIS را اضافه می‌کند. این موضوع پس از تحلیل کدمنبع باج افزار مورد اشاره نیز اثبات گردید.



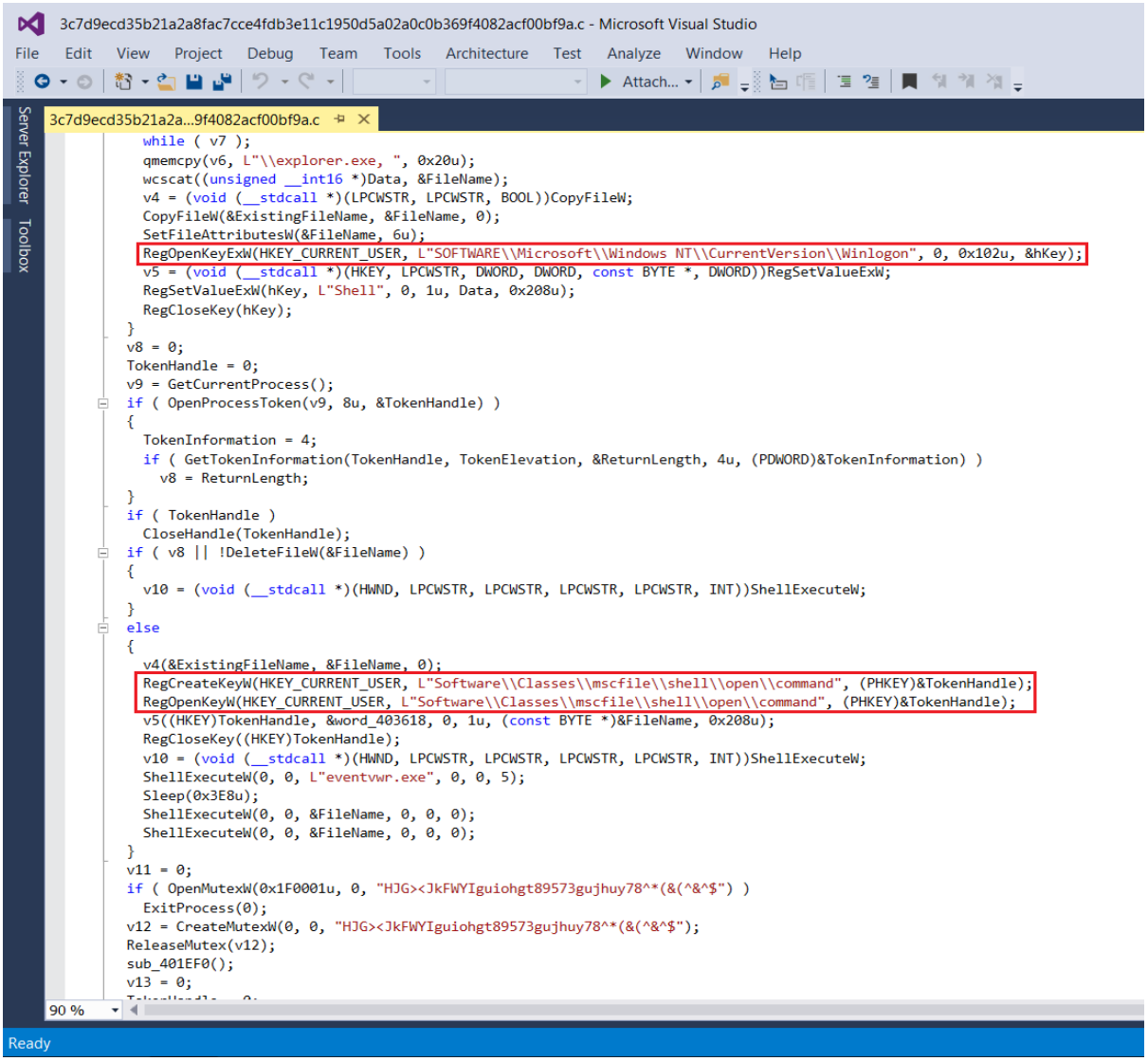
قطعه کد زیر مربوط به حذف shadow copy می‌باشد که امکان بازیابی فایل‌ها را غیرممکن می‌کند.



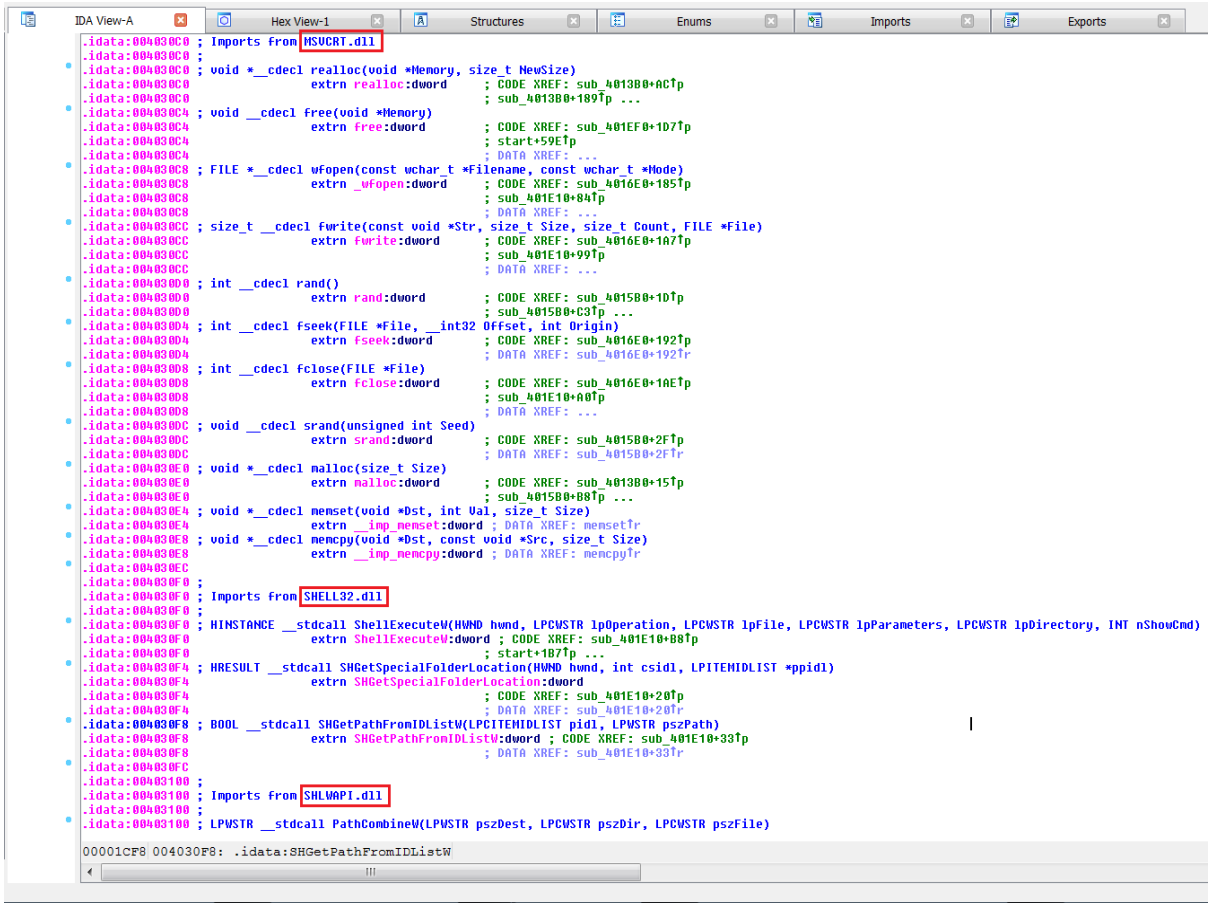
همانطور که اشاره شد باج‌افزار Sepsis فایل‌های مربوط به درایو ویندوز که در دایرکتوری‌های مشخص موجودند را رمزگذاری نمی‌کند، این موضوع پس از تحلیل کدمنبع باج افزار مورد اشاره نیز اثبات گردید.



باج‌افزار پس از حمله به سیستم قربانی، کلید رجیستری مشخص شده در تصویر را ایجاد می‌کند.



این باج‌افزار از کتابخانه‌های ویندوزی به همراه توابعی از هرکدام از کتابخانه‌ها استفاده می‌کند، در تصویر 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.



CRYPT۳۲.DLL	SHELL۳۲.dll	SHLWAPI.dll
CryptDecodeObjectEx	ShellExecuteW	PathCombineW
CryptImportPublicKeyInfo	SHGetPathFromIDListW	PathFindExtensionW
CryptStringToBinaryA	SHGetSpecialFolderLocation	

ADVAPI۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.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	Wow٦٤EnableWow٦٤FsRe	memset
RegOpenKeyExW	FindClose	Sleep	direction	rand
RegOpenKeyW	FindFirstFileW	UnmapViewOfFile		realloc
RegSetValueExW	FindNextFileW	WaitForMultipleObjects		srand
	GetCurrentProcess			

بر اساس بررسی‌های صورت گرفته، باج‌افزار Sepsis پس از اجرا، فرایندهای زیر را ایجاد می‌کند :

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

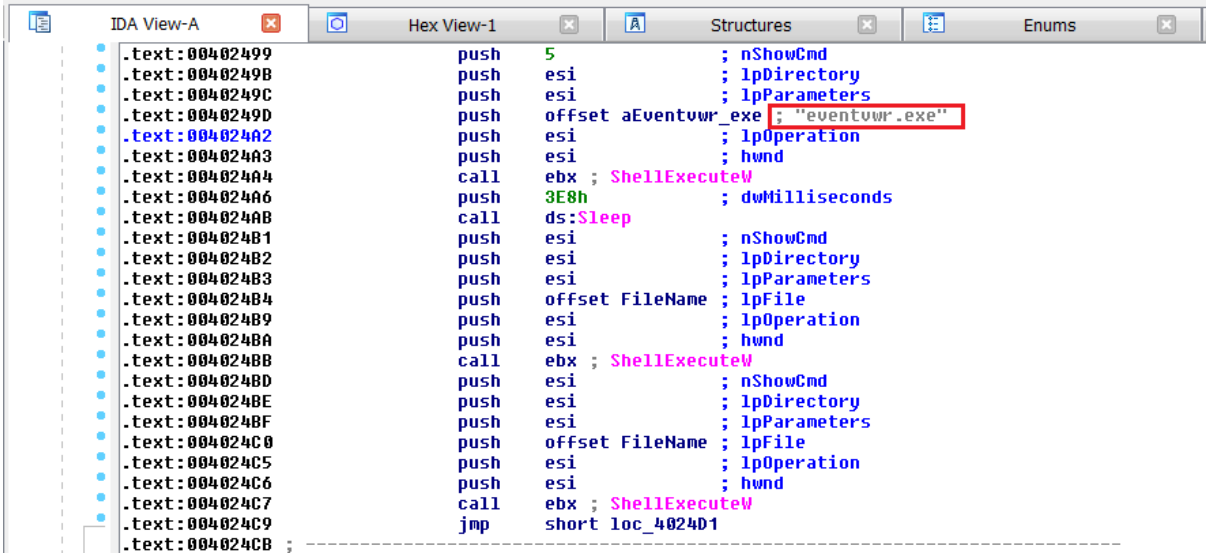
svchost.exe "C:\Users\admin\AppData\Local\Temp\svchost.exe"

vssvc.exe C:\Windows\system۳۲\vssvc.exe

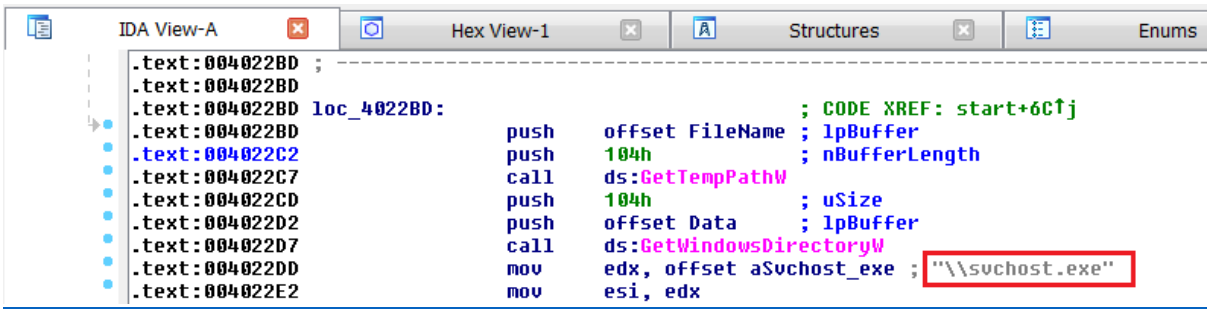
پس از اجرای باج‌افزار، فرایند اصلی باج‌افزار خاتمه پیدا می‌کند و همانطور که اشاره شد ادامه‌ی فرایند رمزگذاری فایل‌ها توسط svchost.exe ادامه پیدا می‌کند.

باج‌افزار Sepsis فرایند vssadmin.exe را به منظور حذف shadow copy و فرایند bcdedit.exe را نیز جهت جلوگیری از بازگردانی فایل‌ها توسط قربانی اجرا می‌کند.

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



تصویر ۱: فرایند eventvwr.exe



تصویر ۲: فرایند svchost.exe

تحلیل ترافیک شبکه :

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

شناسایی :

در حال حاضر تعداد ٤٥ 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	Dropped:Generic.Malware.G!g.917FBD...	AegisLab	Dropped.Generic.Malware!c
AhnLab-V3	Malware/Win32.Generic.C2503141	ALYac	Trojan.Ransom.Sepsis
Antiy-AVL	Trojan/Win32.TSGeneric	Arcabit	Generic.Malware.G!g.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.G!g.917FBD...
CAT-QuickHeal	Trojan.IGENERIC	Cylance	Unsafe
Cyren	W32/Trojan.LYJE-6925	Emsisoft	Dropped:Generic.Malware.G!g.917FBD... (B)
Endgame	malicious (moderate confidence)	eScan	Dropped:Generic.Malware.G!g.917FBD...
ESET-NOD32	Win32/Filecoder.NQP	F-Secure	Dropped:Generic.Malware.G!g.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.fbovth	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