بسمه‌تعالی

گزارش تحلیلی بدافزار

Angus Ransomware

فهرست مطالب

۱ مقدمه

باج‌افزار Angus یکی از باج‌افزارهای جدید و خانواده Phobos می‌باشد که در ماه نوامبر ۲۰۱۹ میلادی انتشار یافته‌است.این باج‌افزار از طریق فایل‌های ضمیمه ایمیل‌های اسپم و آسیب‌پذیری‌های موجود وارد سیستم شده و بعد از نصب و راه‌اندازی با استفاده از الگوریتم رمزنگاری AES، اقدام به تغییر فایل‌های سیستم کرده و پسوند id[ID].[decrypt@files.mn].angus. را به انتهای هر فایل اضافه می‌کنند. همچنین به گفته محققان در برخی موارد مشاهده شده است که مهاجمان با اسکن سیستم‌هایی که RDP در آن‌ها فعال می‌باشد (با اسکن پورت 3389)، این باج‌افزار را وارد سیستم کاربر قربانی شده، می‌کنند. بعد از اتمام فرایند رمزگذاری فایل‌های سیستم یک فایل راهنما با نام info.hta ایجاد کرده و از کاربر قربانی شده درخواست ارسال ایمیل به آدرس decrypt@files.mn برای تعیین مبلغ باج دارد. از نکات قابل توجه در مورد این باج‌افزار نام انتخابی توسط مهاجمان می‌باشد. مهاجمان از 1sass.exe استفاده کرده‌اند که شبیه به پروسس اصلی سیستم‌عامل یعنی lsass.exe می‌باشد و با این کار قصد مخفی نگه داشتن پروسس باج‌افزار را دارند.

۲ مشخصات و جزئیات کامل فایل

بخش زیر اطلاعات کلی در مورد فایل بدافزار را نشان می‌دهد که شامل بخش‌های تشکیل دهنده، مقدار آنتروپی و مشخصات کلی مانند زمان کامپایل، نوع کامپایلر و غیره می‌باشد.

۲–۱ مشخصات فایل

فایل اجرایی بدافزار یک فایل قابل اجرا در سیستم عامل‌های ویندوزی می‌باشد که با استفاده از زبان برنامه نویسی C++ طراحی شده است و شامل اطلاعات زیر می‌باشد.

جدول ۱ - مشخصات کلی باج‌افزار

Angus - Ransomware	**نام و نوع بدافزار**
.id[ID].[decrypt@@files.mn].angus	**پسوند و نام فایل**
Email Spam, RDP scan, Vulnerability	**نحوه انتشار**
AES	**الگوریتم**
November 2019	**زمان کامپایل**
3dcbc7bbaaf3d79f03c47cfc0bd0d819	**هش md5**
c10c3ef64c8f5df12e2b7b2040a7ce6f951270e4	**هش SHA1**
925a5344e9f7b734eaca5bd0b1510881613522f29d05d897985fcee99daa3fcc	**هش SHA256**
Microsoft Visual C++	**کامپایلر**
(hex),4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 (text),M Z .. .. @	**بایت‌های اولیه**
51 KB	**حجم فایل**
7.183	**آنتروپی فایل**
32 bit	**معماری فایل**
5	**تعداد بخش**
-	**آدرس فایل pdb**

۲–۲ بخش‌های مختلف فایل

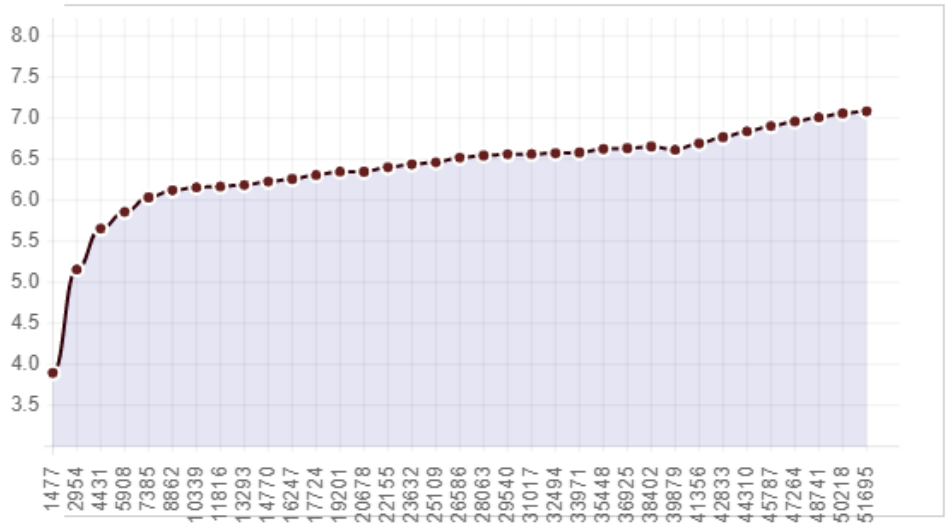
جدول شماره ۲ بخش‌های مختلف فایل بدافزار را همراه با جزئیات کامل مانند مقدار آنتروپی، اندازه مجازی و غیره نشان می‌دهد که متشکل از پنج بخش بصورت text، data، rdata، reloc و cdata می‌باشد.

جدول ۲ - بخش‌های مختلف باج‌افزار

ردیف	نام بخش	آدرس مجازی	اندازه مجازی	اندازه خام	آنتروپی
1	text	4096	31672	31744	6.62
2	rdata	36864	3146	3584	5.22
3	data	40960	10009	1536	6.4
4	reloc	53248	1368	1536	5.28
5	cdata	57344	12076	12288	7.87

۳-۲ مقدار آنتروپی

شکل زیر وضعیت آنتروپی کلی فایل را در حالت عادی بصورت نموداری نشان می‌دهد. مقدار این آنتروپی برابر با 7.183 می‌باشد که رفتار غیرعادی فایل را نشان می‌دهد.



شکل ۱ - وضعیت کلی آنتروپی فایل

با توجه به اطلاعات موجود در شکل ۱ و جدول‌های بالا، مقدار آنتروپی در بخش text بیشتر از شش و نزدیک هفت و آنتروپی کلی فایل و بخش cdata بالاتر از هفت می‌باشد. مقدار بیشتر از هفت و روند صعودی این مقدار، رفتار غیرعادی و احتمال بدافزار بودن فایل را نشان می‌دهد. همچنین اندازه مجازی و اندازه خام در بخش data دارای تفاوت زیادی می‌باشد که غیرعادی به‌نظر می‌رسد.

۳ وضعیت تشخیص فایل در آنتی‌ویروس‌ها

شکل شماره ۲ وضعیت تشخیص فایل مورد بررسی را در ویروس‌توتال نشان می‌دهد که از بین ۷۰ موتور، ۵۷ موتور این فایل را بدافزار تشخیص داده‌اند. در برخی موارد نوع تشخیص این فایل بصورت Trojan.Ransom.Phobos.F می‌باشد.

Acronis	Suspicious	Ad-Aware	Trojan.Ransom.Phobos.F
AegisLab	Trojan.Win32.Generic.4!c	AhnLab-V3	Trojan/Win32.BantaRansom.R279004
Alibaba	Ransom:Win32/Phoenix.18ea7d94	ALYac	Trojan.Ransom.Phobos
SecureAge APEX	Malicious	Arcabit	Trojan.Ransom.Phobos.F
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	Trojan.Ransom.Phobos.F
BitDefenderTheta	Gen:Trojan.Heur.FU.duW@a8DJSef	Bkav	W32.KsoyseASI.Trojan
CAT-QuickHeal	Trojan.Generic	ClamAV	Win.Dropper.Sodinokibi-7133780-0
Comodo	Malware@#1lyub8sj0yd97	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.baaf3d	Cylance	Unsafe
Cyren	W32/Phobos.C.gen!Eldorado	DrWeb	Trojan.Encoder.29362
Emsisoft	Trojan.Ransom.Phobos.F (B)	Endgame	Malicious (high Confidence)
eScan	Trojan.Ransom.Phobos.F	ESET-NOD32	A Variant Of Win32/Filecoder.Phobos.C
F-Prot	W32/Phobos.C.gen!Eldorado	F-Secure	Trojan.TR/Crypt.XPACK.Gen
Fortinet	W32/Generic.AP.2C9868!tr	GData	Trojan.Ransom.Phobos.F
Ikarus	Trojan-Ransom.Phobos	Jiangmin	Trojan.Generic.dvgao
K7AntiVirus	Trojan (0055119f1)	K7GW	Trojan (0055119f1)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.Phobos
MAX	Malware (ai Score=89)	McAfee	Ransom-Phobos!3DCBC7BBAAF3
McAfee-GW-Edition	BehavesLike.Win32.Generic.qc	Microsoft	Ransom:Win32/Phoenix.BW
NANO-Antivirus	Trojan.Win32.Filecoder.frumwc	Palo Alto Networks	Generic.ml
Panda	Trj/Genetic.gen	Qihoo-360	Win32/Trojan.BO.a47
Rising	Ransom.Phoenix!1.BC23 (CLASSIC)	SentinelOne (Static ML)	DFI - Malicious PE
Sophos AV	Troj/Phobos-B	Sophos ML	Heuristic
SUPERAntiSpyware	Ransom.Phobos/Variant	Symantec	Trojan Horse
TACHYON	Ransom/W32.Phobos.51712	TrendMicro	Ransom.Win32.CRYSIS.SMA
TrendMicro-HouseCall	Ransom.Win32.CRYSIS.SMA	VBA32	BScope.Trojan.Fuerboos
ViRobot	Trojan.Win32.Ransom.51712.A	Webroot	W32.Malware.Gen
ZoneAlarm by Check Point	HEUR:Trojan.Win32.Generic	Tencent HABO	MALWARE EVADER RANSOM

شکل ۲ – نتیجه بررسی فایل در سایت ویروس‌توتال

همچنین شکل شماره ۳ نشان‌دهنده وضعیت تشخیص فایل در سامانه ویروس‌کاو می‌باشد. در این سامانه از بین ۳۲ موتور موجود ۲۴ موتور قادر به تشخیص فایل به‌عنوان بدافزار می‌باشند.

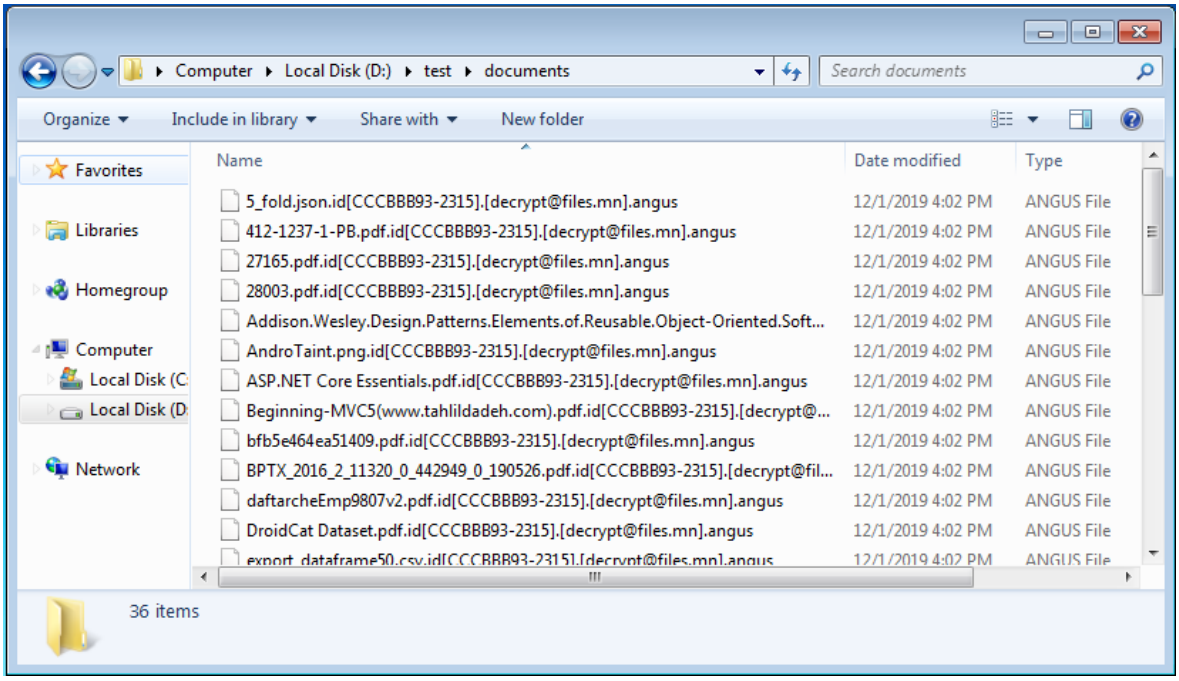
آنتی ویروس	نتیجه اسکن	
ikarus	ii	Dangerous Trojan-Ransom.Phobos
mcafee	ii	Dangerous Ransom-Phobos!3DCBC7BBAAF3 trojan
nanoav	✓	Clean
escan	ii	Dangerous Trojan.Ransom.Phobos.F
zillya	✓	Clean
gdata	ii	Dangerous Trojan.Ransom.Phobos.F
comodo	ii	Dangerous
avast	ii	Dangerous Win32:Malware-gen[PE3-6FD0B3FE00002105304171DBDCF75E58]troj;Win32:Evo-gen
clamav	ii	Dangerous Win.Dropper.Sodinokibi-7133780-0
avira	ii	Dangerous TR/Crypt.XPACK.Gen
symantec	✓	Clean
satfaa	ii	Dangerous
cyberbyte	ii	Dangerous
vba32	✓	Clean
immunet	ii	Dangerous Win.Dropper.Sodinokibi-7133780-0
clamwin	ii	Dangerous Win.Dropper.Sodinokibi-7133780-0
eset	ii	Dangerous a variant of Win32/Filecoder.Phobos.C trojan
gridinsoft	✓	Clean
windefender	ii	Dangerous RansomWin32/Phoenix.BW
bitdefender	ii	Dangerous Trojan.Ransom.Phobos.F
پادویش	ii	Dangerous
drweb	ii	Dangerous Trojan.Encoder.29362
trustport	ii	Dangerous Trojan.Ransom.Phobos.F
avg	ii	Dangerous Malware-gen
winessentials	ii	Dangerous RansomWin32/Phoenix.BW
fsecure	ii	Dangerous Gen:Trojan.Heur.FU.duW@a8DJSef
atlantis	✓	Clean
emsisoft	ii	Dangerous Trojan.Ransom.Phobos.F
kaspersky	ii	Dangerous
fprot	ii	Dangerous W32/Phobos.C.gen!Eldorado
sophos	✓	Clean

شکل ۳ - بررسی فایل در سامانه ویروس‌کاو

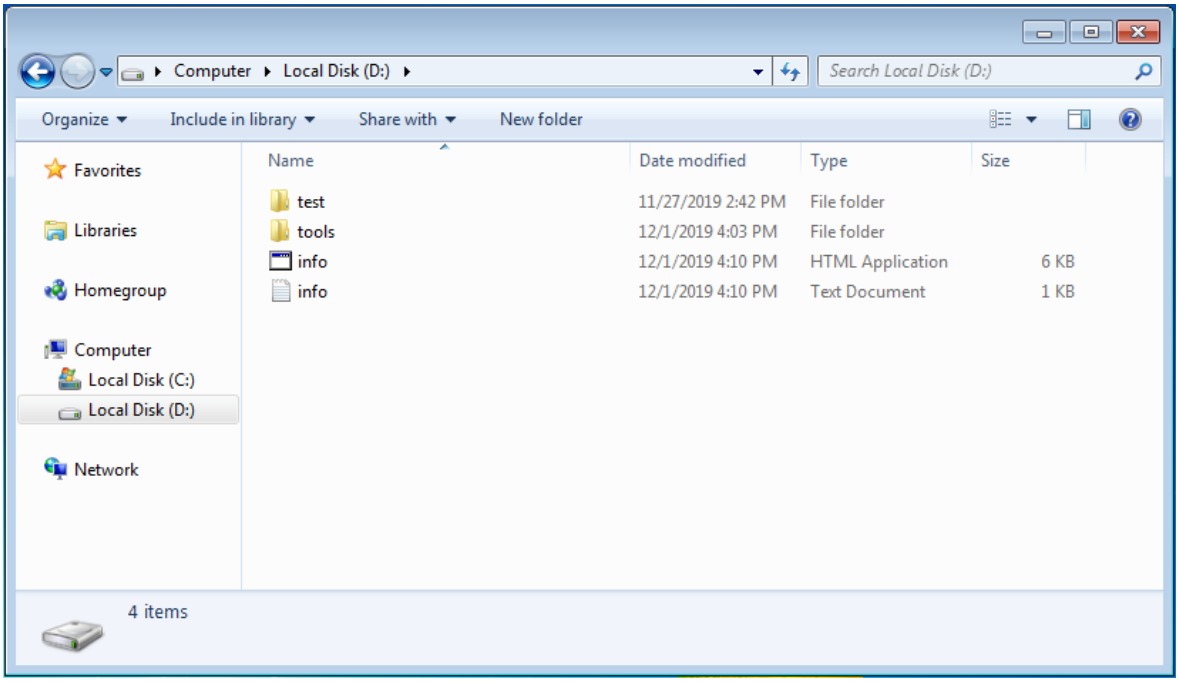
از بین این موتورها، موتوهای پادویش و ستفا قادر به شناسایی فایل به عنوان فایل مخرب شده‌اند.

۴ فرآیند آلوده‌سازی

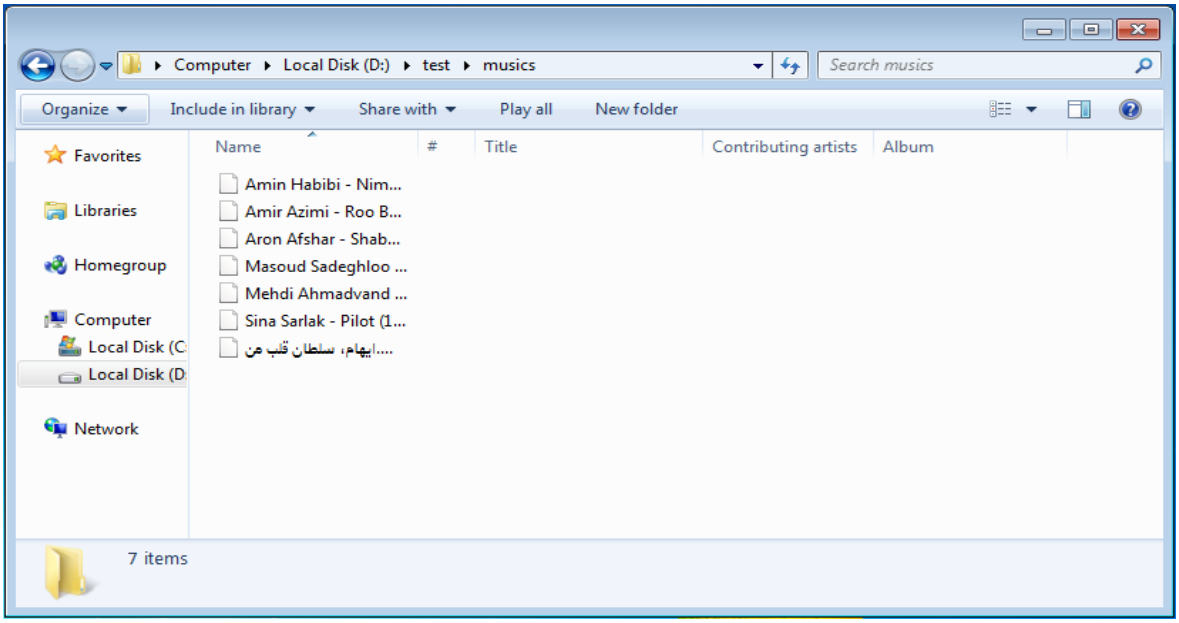
باج‌افزار Angus یکی از باج‌افزارهای انتشاریافته در ماه نوامبر ۲۰۱۹ می‌باشد که از خانواده Phobos بوده و همانند نسخه‌های دیگر این خانواده از طریق فایل‌های ضمیمه ایمیل‌های اسپم، آسیب‌پذیری-های موجود و یا حتی با اسکن پورت RDP توسط مهاجمان در سیستم کاربر قربانی شده قرار می‌گیرد. این باج‌افزار بعد از ورود و نصب در سیستم ابتدا در مسیرهایی از سیستم همانند %AppData% فایل اصلی خود را کپی کرده و برای فرایند رمزگذاری فایل‌های سیستم اجرا می‌گردد. بعد از اجرا، تمام فایل‌های سیستم را دریافت کرده و با استفاده از الگوریتم AES آن‌ها را رمز کرده و پسوند id[ID].[decrypt@files.mn].angus. را به انتهای هر فایل اضافه می‌کند و در انتها داخل هر پوشه یک فایل راهنما با نام info.hta ایجاد می‌کند. بعد از اتمام فرایند رمزگذاری فایل‌های سیستم با بررسی شبکه اتصالی سیستم، با استفاده از پورت SMB اقدام به انتشار فایل باج‌افزار می‌کند تا بتواند به سیستم‌های دیگر نیز نفوذ کرده و آن‌ها را آلوده سازد. این باج‌افزار توانایی رمزگذاری فایل‌هایی با عنوان‌های فارسی را دارد. برای بازگردانی فایل‌های رمزشده، مهاجمان درخواست ۳۵۰۰ دلار را دارند که در صورت پرداخت توسط کاربر قربانی شده باید بصورت بیت‌کوین پرداخت گردد. مهاجمان برای اطمینان دادن بایت اینکه فایل‌های رمزشده قابل برگشت می‌باشد، ۵ فایل که حجم آن‌ها کمتر از ۴ مگابایت می‌باشد را دریافت کرده و بصورت فایل‌های بازگردانی شده به کاربر برمی‌گردانند. شکل‌های زیر نمونه فایل‌های رمزشده، مسیرهای ایجاد فایل اصلی باج‌افزار و بررسی شبکه برای انتشار فایل اصلی باج‌افزار را نشان می‌دهند.



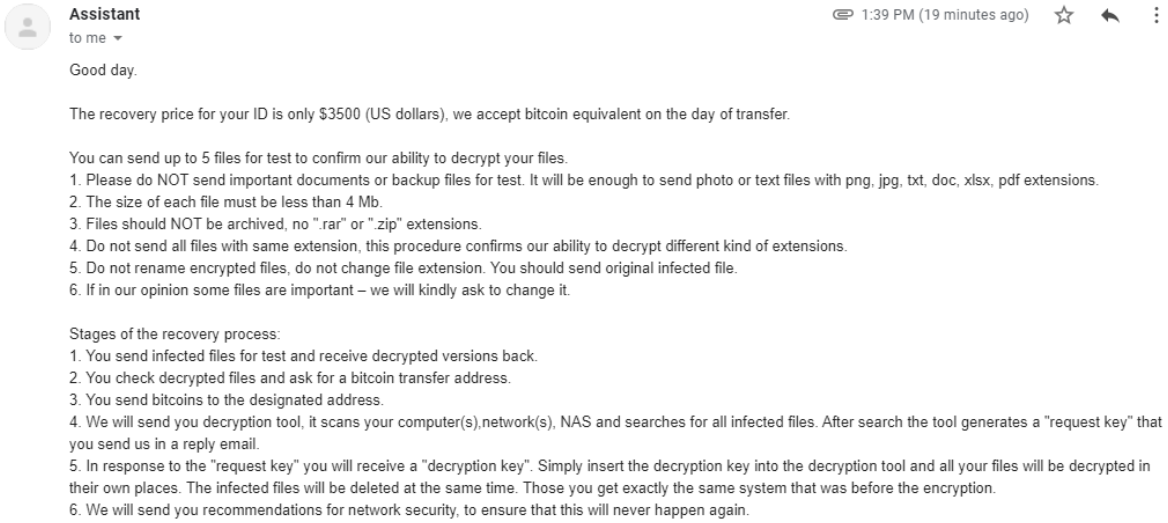
شکل ۴ نمونه فایل‌های رمز شده توسط باج‌افزار و پسوند اضافه شده



شکل ۵ ایجاد فایل‌های راهنما توسط باج‌افزار



شکل ۶ نمونه فایل‌های رمزشده توسط باج‌افزار و پسوند اضافه شده



Assistant
to me
1:39 PM (19 minutes ago)

Good day.

The recovery price for your ID is only $3500 (US dollars), we accept bitcoin equivalent on the day of transfer.

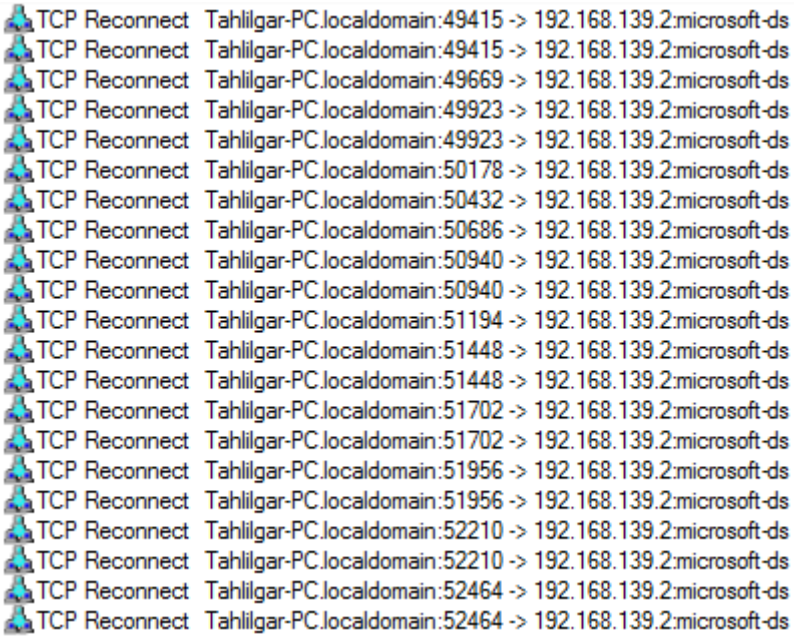
You can send up to 5 files for test to confirm our ability to decrypt your files.
1. Please do NOT send important documents or backup files for test. It will be enough to send photo or text files with png, jpg, txt, doc, xlsx, pdf extensions.
2. The size of each file must be less than 4 Mb.
3. Files should NOT be archived, no ".rar" or ".zip" extensions.
4. Do not send all files with same extension, this procedure confirms our ability to decrypt different kind of extensions.
5. Do not rename encrypted files, do not change file extension. You should send original infected file.
6. If in our opinion some files are important – we will kindly ask to change it.

Stages of the recovery process:
1. You send infected files for test and receive decrypted versions back.
2. You check decrypted files and ask for a bitcoin transfer address.
3. You send bitcoins to the designated address.
4. We will send you decryption tool, it scans your computer(s),network(s), NAS and searches for all infected files. After search the tool generates a "request key" that you send us in a reply email.
5. In response to the "request key" you will receive a "decryption key". Simply insert the decryption key into the decryption tool and all your files will be decrypted in their own places. The infected files will be deleted at the same time. Those you get exactly the same system that was before the encryption.
6. We will send you recommendations for network security, to ensure that this will never happen again.

شکل ۷ ایمیل ارسالی توسط مهاجمان و درخواست مبلغ باج

C:\Users\Tahlilgar\Desktop\1sass[phobos].exe
C:\Users\Tahlilgar\Desktop\1sass[phobos].exe
C:\Users\Tahlilgar\AppData\Local\1sass[phobos].exe
C:\Users\Tahlilgar\AppData\Local\1sass[phobos].exe
C:\Users\Tahlilgar\Desktop\1sass[phobos].exe
C:\Users\Tahlilgar\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1sass[ph.
C:\Users\Tahlilgar\Desktop\1sass[phobos].exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\1sass[phobos].exe
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\1sass[phobos].exe

شکل ۸ مسیرهایی که باج‌افزار فایل اصلی خود را در آن‌ها قرار داده است



شکل ۹ بررسی شبکه مورد نظر جهت انتشار فایل باج‌افزار به سیستم‌های دیگر

شکل ۱۰ محتویات فایل info.hta

۵ شرح تحلیل

گزارش زیر نتیجه تحلیل استاتیک و پویا در مورد فایل بدافزار در آزمایشگاه می‌باشد که از جعبه-شنی‌های آنلاین و آفلاین موجود استفاده شده است.

۵-۱ توابع و کتابخانه‌های سیستمی مورد استفاده

جدول زیر لیست کتابخانه‌های قابل دستیابی از فایل بدافزار را نشان می‌دهد که از تعداد بیشتری تشکیل یافته است.

جدول ۳ - کتابخانه‌های سیستمی مورد استفاده

MPR.dll	WS2_32.dll	IPHLPAPI.dll	KERNEL32.dll	USER32.dll
ADVAPI32.dll	SHELL32.dll	ole32.dll		

همچنین جدول ۴ توابع قابل استخراج از فایل بدافزار را نشان می‌دهد، تعداد تابع استفاده شده در این باج‌افزار بیشتر می‌باشد که از کتابخانه‌های سیستمی مختلفی مورد استفاده قرار گرفته است.

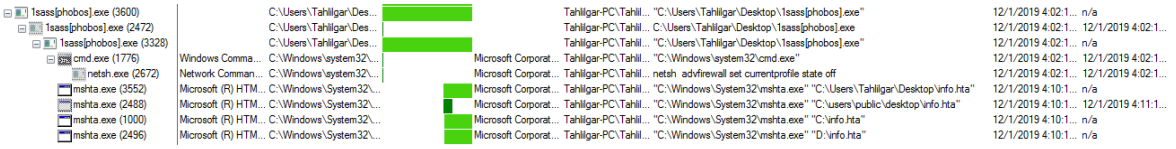
جدول ۴ - توابع استفاده شده در بدافزار

MPR.dll
WNetEnumResourceW, WNetUseConnectionW, WNetOpenEnumW, WNetCloseEnum
WS2_32.dll
ioctlsocket, connect, ntohl, select, getpeername, htons, recv, socket, closesocket, getsockopt
IPHLPAPI.dll
GetIpAddrTable
KERNEL32.dll
SetFilePointerEx, GetFileAttributesW, SetFileAttributesW, MoveFileW, ReadFile, GetProcAddress, SetEndOfFile, ExitProcess, WaitForSingleObject, GetComputerNameW, SetEvent, GetLogicalDrives, GetTickCount, Sleep, CopyFileW, CreateEventW, WaitForMultipleObjects, CloseHandle, CreateThread, InitializeCriticalSectionAndSpinCount, LeaveCriticalSection, EnterCriticalSection, ResetEvent, DeleteCriticalSection, CreateMutexW, CreateProcessW, GetCurrentProcess, SetHandleInformation, WriteFile, OpenProcess, GetLocaleInfoW, ReadProcessMemory, TerminateProcess, GetModuleFileNameW, CreateFileW, FlushFileBuffers, OpenMutexW, GetLastError, GetCurrentThreadId, Process32FirstW, GetExitCodeThread, CreatePipe, Process32NextW, GetModuleHandleA, CreateToolhelp32Snapshot, ReleaseMutex, GetVersion, DeleteFileW, GetCurrentProcessId, GetVolumeInformationW, ExpandEnvironmentStringsW, HeapAlloc, GetProcessHeap, HeapReAlloc, HeapFree, FindFirstFileW, FindClose, FindNextFileW, SystemTimeToFileTime, QueryPerformanceCounter, GetLocalTime, GetFileSizeEx

USER32.dll
GetShellWindow, GetWindowThreadProcessId
ADVAPI32.dll
DuplicateTokenEx, LookupAccountSidW, OpenProcessToken, GetTokenInformation, EqualSid, RegSetValueExW, RegCloseKey, RegOpenKeyExW, FreeSid, AllocateAndInitializeSid, RegQueryValueExW
SHELL32.dll
ShellExecuteExW
ole32.dll
CoGetObject, CoInitializeEx, CoUninitialize

۵-۲ پروسس‌های اجراشده

شکل زیر پروسس‌های ایجاد شده توسط باج‌افزار را نشان می‌دهد. در این شکل مشاهده می‌گردد که ابتدا با استفاده از cmd یک دستوری را اجرا می‌کند که این دستور بصورت زیر می‌باشد. بعد از اجرای دستور نیز با استفاده از پروسس mshta اقدام به ایجاد فایل‌های info.hta می‌کند که فایل راهنما جهت تماس با مهاجمان می‌باشد.



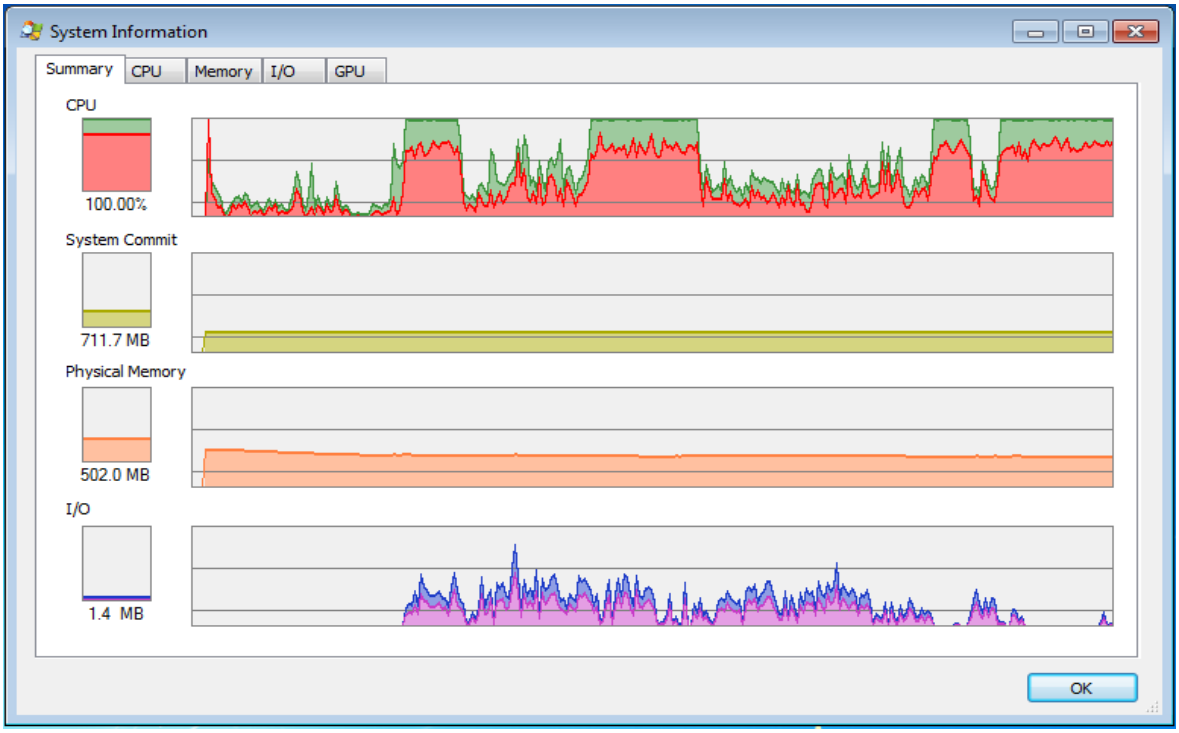
شکل ۱۱ پروسس‌های فعال شده توسط فایل اجرایی باج‌افزار

دستور اجرا شده در cmd به صورت زیر می‌باشد که با استفاده از این دستور فایروال سیستم را غیرفعال می‌کند.

- Netsh advfirewall set currentprofile state off

۵-۳ وضعیت منابع سیستم

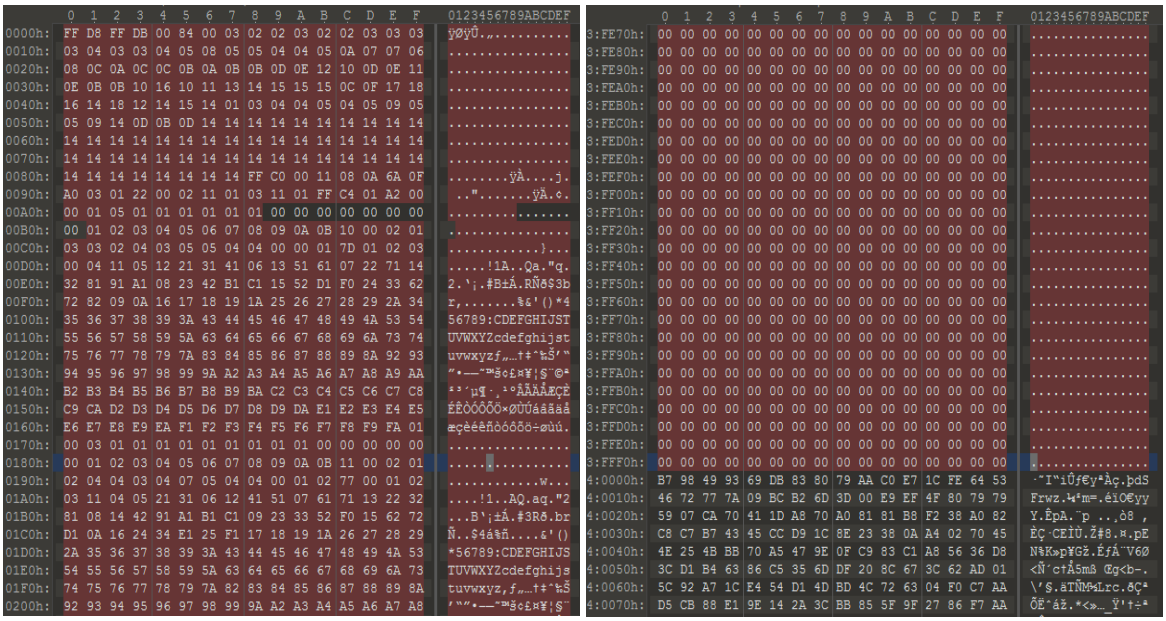
شکل زیر وضعیت منابع سیستم را در زمانی نشان می‌دهد که باج‌افزار در حال فعالیت بوده و فایل-های سیستمی را رمزگذاری می‌کند. با توجه به شکل مشاهده می‌گردد که در بیشتر مواقع میزان مصرفی CPU به حداکثر مقدار خود رسیده و منابع دیگر مانند IO نیز با بیشترین مقدار در حال فعالیت هستند.



شکل ۱۲ وضعیت منابع سیستم در طول اجرای باج‌افزار

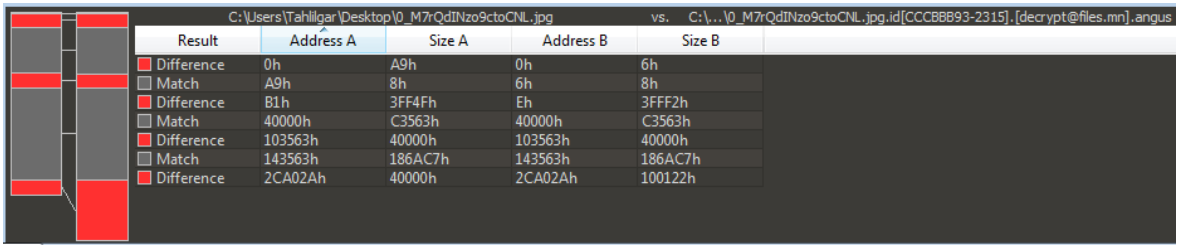
۴-۵ نمونه فایل رمزشده

نمونه فایل تست شده برای این باج‌افزار یک فایل jpg می‌باشد که ساختار باینری آن قبل و بعد از رمزگذاری بصورت شکل ۱۳ می‌باشد. بخش سمت راست مربوط به حالت رمزشده و بخش سمت چپ مربوط به حالت عادی فایل می‌باشد.



شکل ۱۳ وضعیت باینری فایل قبل و بعد از رمزگذاری

شکل زیر نیز مقایسه بین دو فایل قبل و بعد از عملیات رمزگذاری را نشان می‌دهد. مقادیر قرمز رنگ تفاوت‌های باینری و قسمت‌های خاکستری نیز مقادیر باینری شبیه را نشان می‌دهند.



شکل ۱۴ مقایسه باینری فایل قبل و بعد از فرایند رمزگذاری

۵-۴-۱ پسوندهای قابل رمزگذاری توسط باج‌افزار

این باج‌افزار توانایی رمزگذاری روی فایل‌هایی با پسوند زیر دارد. همچنین می‌تواند فایل‌هایی که با عنوان فارسی هستند را رمزگذاری کند.

.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

۶ توصیه‌های امنیتی برای پیشگیری

- گرفتن فایل پشتیبان بصورت دوره‌ای از فایل‌های سیستم و ذخیره آن در محل دیگر
- استفاده از آنتی‌ویروس قوی و بروزرسانی مداوم آن
- خودداری از بازکردن و اجرا فایل‌های مشکوک و ناشناس
- خودداری از بازکردن ایمیل‌های مشکوک و ناشناس
- اطمینان از سالم بودن دستگاه‌های جانبی مانند فلش
- استفاده از رمزعبور قوی بر روی درایوهای سیستم
- استفاده از سیستم‌عامل جدید و بروزرسانی شده

- بروزرسانی مداوم سیستم عامل
- پیکربندی مناسب پروتکل‌های مورد استفاده در شبکه متناسب با محیط کار