بسمه تعالی

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

باج‌افزار MarraCrypt

گزارش تحلیل بدافزار

شناسه سند ..... Maher_13990402-2

نوع سند ..... گزارش فنی

شماره نگارش ۰,۱

تاریخ نگارش ۱۳۹۹/۰۴/۰۲

طبقه‌بندی سند ..... **عادی**


تهران، میدان آرژانتین، ابتدای بلوار بیهقی، نبش خیابان شانزدهم، ساختمان شماره ۱، سازمان فناوری اطلاعات ایران


(۰۲۱) ۴۲۶۵۰۰۰۰


(۰۲۱) ۴۲۶۵۰۰۰۰


cert.ir

فهرست مطالب

۱ مقدمه

براساس یافته‌های محققان حوزه بدافزار، باج‌افزار جدیدی با نام MarraCrypt از خانواده باج‌افزاری Hermes در February سال ۲۰۲۰ انتشار یافته است که با استفاده از الگوریتم RSA-4096 تمام فایل‌های موجود در سیستم را رمزگذاری کرده و پسوند [newpatek@cock.li].MARRA را به انتهای هرکدام از آن‌ها اضافه می‌کند و یک فایل راهنما بصورت MARRACRYPT_INFORMATION.HTML را در داخل هر پوشه ایجاد می‌کند. برخلاف روش نفوذ دیگر باج‌افزارها به سیستم، این باج‌افزار شبیه Worm عمل کرده و از طریق درایوهای فلش، درایوهای مجازی و غیره به سیستم کاربر انتقال می‌یابد. از آن‌جایی که این باج‌افزار بصورت روش Worm عمل می‌کند اما بدین معنی نمی‌باشد که از راه‌های دیگر نمی‌شود به این باج‌افزار آلوده نشد، از جمله این روش‌ها می‌توان به ایمیل‌های اسپم، آسیب‌پذیری موجود در سیستم یا ابزارهای نصب شده و غیره اشاره کرد.

۲ مشخصات و ریزجزئیات فایل باج‌افزار

جداول و نمودارهای زیر نشان‌دهنده مشخصات فایل اجرایی باج‌افزار می‌باشد که در تحلیل استاتیک بدست آمده است و شامل مواردی همچون اندازه فایل، مقادیر هش فایل، آنتروپی، وضعیت شناسایی فایل در ویروس-توتال و ویروس‌کاو و غیره می‌باشد.

۲-۱ مشخصات فایل

این باج‌افزار یک فایل قابل اجرا بر روی سیستم‌عامل‌های ویندوز می‌باشد که با استفاده از زبان برنامه‌نویسی C++ طراحی و پیاده‌سازی شده است. جدول زیر مشخصات کلی فایل باج‌افزار جدید MarraCrypt را نشان می‌دهد.

جدول ۱ مشخصات کلی فایل باج‌افزار

نام بدافزار	MarraCrypt, Ransomware
نوع بدافزار	Ransomware, File Locker
خانواده بدافزار	Hermes Ransomware
پسوند و نام فایل	[newpetak@cock.li].MARRA

فایل راهنما	MARRACRYPT_INFORMATION.HTML
نحوه انتشار	Spread like a worm
زمان کامپایل	Sat Feb 22 2020
هش MD5	17F97F9C91B0DAF856526130CF9BD702
هش SHA1	268685C49E0BC50F7A7E977D2D71768A1E958F03
هش SHA256	BE88512C9250A558A3524E1C3BBD0299517CB0D6C3FB749C22DF32033BF081E8
کامپایلر	Microsoft Visual C++
حجم فایل	226304 bytes
آنتروپی فایل	7.396
معماری فایل	32 Bits binary
تعداد بخش	4
نام اصلی فایل	svchosta.exe

۲-۲ بخش‌های مختلف فایل

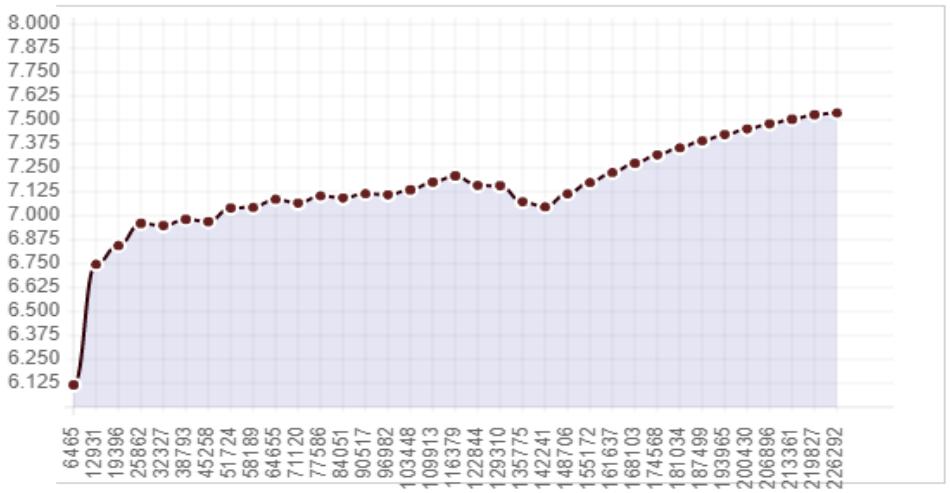
جدول شماره ۲ بخش‌های مختلف تشکیل دهنده فایل باج‌افزار را با جزئیات کامل مانند مقدار آنتروپی، اندازه خام، اندازه مجازی هر بخش و غیره نشان می‌دهد. این فایل متشکل از یازده بخش بصورت text، rdata، data و rsrc بصورت زیر می‌باشد.

جدول ۲ بخش‌های تشکیل دهنده فایل باج‌افزار

ردیف	نام بخش	آدرس مجازی	اندازه مجازی	اندازه خام	آنتروپی
1	text	0x1000	0x196d8	0x19800	6.746041
2	rdata	0x1b000	0x6df2	0x6e00	6.443129
3	data	0x22000	0x30c0	0x1600	3.262445
4	rsrc	0x26000	0x15324	0x15400	7.987300

۲-۳ آنتروپی کلی فایل

شکل زیر وضعیت آنتروپی کلی فایل را در حالت عادی بصورت نموداری نشان می‌دهد. مقدار این آنتروپی برابر با 7.396 می‌باشد که مقدار آن بالاتر از هفت می‌باشد.

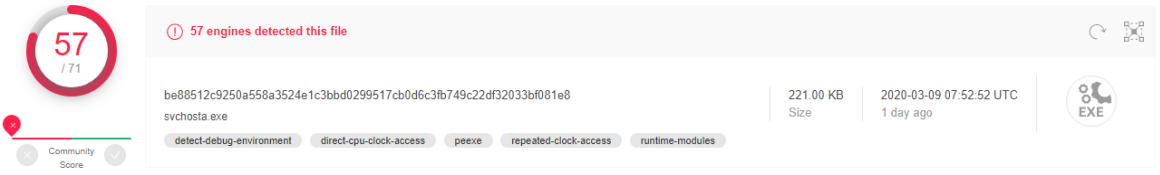


شکل ۱ آنتروپی کلی فایل باج‌افزار

این فایل دارای چهار بخش می‌باشد که با توجه به مقادیر موجود جدول شماره ۲ و شکل شماره ۱ می‌توان مشاهده کرد که مقدار آنتروپی بخش rsrc و آنتروپی کلی فایل بالاتر از هفت می‌باشد. روند صعودی و مقدار بیش از ۷ آنتروپی احتمال رفتار بدافزاری (دگردیسی و چندریختی) را در فایل اجرائی افزایش می‌دهد.

۲-۴ وضعیت شناسایی فایل در Virustotal

شکل زیر وضعیت شناسایی فایل را در ویروس‌توتال نشان می‌دهد. در این سامانه از بین ۷۱ موتور تحلیل ۵۷ موتور قادر به شناسایی فایل بعنوان یک فایل بدافزار شده‌اند و درصورت استفاده از نسخه‌های بروزشده این موتورهای آنتی‌ویروس در سیستم می‌توان از انتقال و اجرای آن جلوگیری کرد.

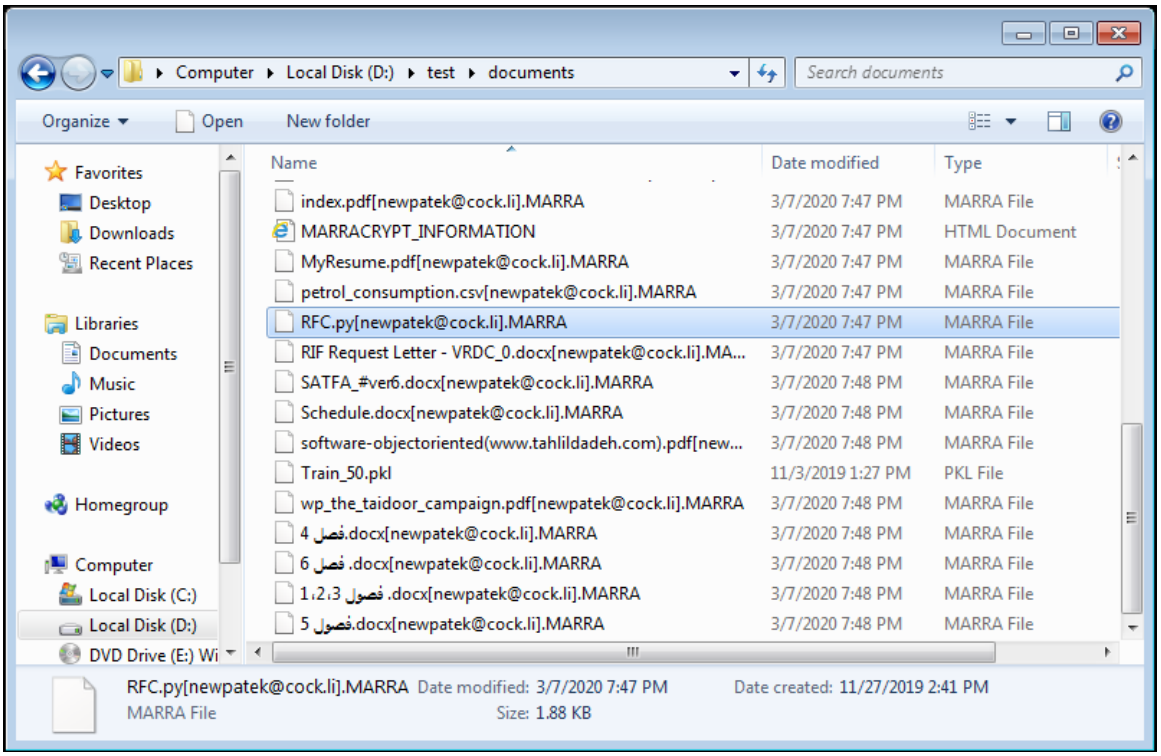


شکل ۲ وضعیت شناسایی فایل باج‌افزار در سامانه ویروس‌توتال

۳ فرایند آلوده‌سازی

براساس یافته‌های محققان حوزه بدافزار، باج‌افزار جدیدی با نام MarraCrypt از خانواده باج‌افزاری Hermes در February سال ۲۰۲۰ انتشار یافته است که با استفاده از الگوریتم RSA-4096 تمام فایل‌های موجود در سیستم (حتی فایل‌هایی که با نام فارسی نوشته شده باشند) را رمزگذاری کرده و پسوند [newpatek@cock.li].MARRA را به انتهای هرکدام از آن‌ها اضافه می‌کند و یک فایل راهنما بصورت MARRACRYPT_INFORMATION.HTML را در داخل هر پوشه ایجاد می‌کند. برخلاف روش نفوذ دیگر باج‌افزارها به سیستم، این باج‌افزار شبیه Worm عمل کرده و از طریق درایوهای فلش، درایوهای مجازی و غیره به سیستم کاربر انتقال می‌یابد. از آن‌جایی که این باج‌افزار بصورت روش Worm عمل می‌کند اما بدین معنی نمی‌باشد که از راه‌های دیگر نمی‌شود به این باج‌افزار آلوده نشد، از جمله این روش‌ها می‌توان به ایمیل‌های اسپم، آسیب‌پذیری موجود در سیستم یا ابزارهای نصب شده و غیره اشاره کرد.

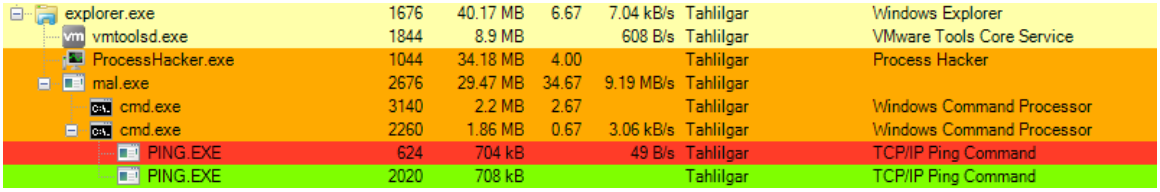
این باج‌افزار بعد از اجرا در سیستم با سطح دسترسی Admin، ابتدا با استفاده از cmd دستوراتی را در سیستم اجرا می‌کند. سپس چند فایل را در مسیرهای مختلفی از سیستم ایجاد کرده و فایل‌های سیستم را با استفاده از الگوریتم رمزنگاری RSA رمزگذاری می‌کند. در انتها نیز در داخل هر پوشه یک فایل راهنما ایجاد کرده و آن را برای کاربر قربانی شده اجرا و نمایش می‌دهد. شکل‌های زیر نمونه فایل‌های رمزشده، فایل راهنما و غیره را نشان می‌دهند.



شکل ۳ نمونه فایل‌های رمزشده توسط باج‌افزار همراه با پسوند اضافه شده

شکل ۴ محتویات فایل راهنما ایجاد شده توسط باج‌افزار

فایل راهنما که محتویات آن را می‌توان در شکل بالا مشاهده کرد شامل یک کلید و دو آدرس ایمیل بصورت‌های newpetak@cock.li و onmywrist@cock.li برای ارتباط با مهاجمان و تعیین مبلغ باج برای بازگردانی فایل-های رمزشده می‌باشد.

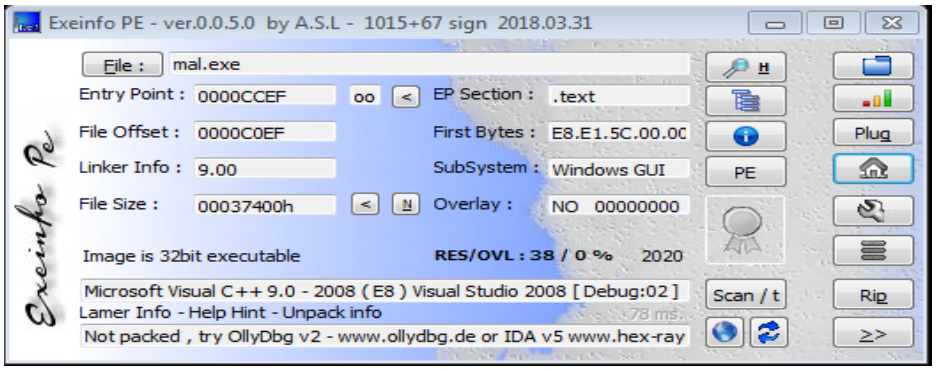


شکل ۵ بخشی از فعالیت پروسس باج‌افزار

۴ شرح تحلیل

۴-۱ شناسایی کامپایلر

با توجه به شکل زیر که با استفاده از ابزارهای تشخیص کامپایلر فایل بدست آمده است، نشان می‌دهد که زبان برنامه‌نویسی طراحی و پیاده‌سازی این باج‌افزار C++ می‌باشد که در جدول ۱ نیز به آن اشاره شد. همچنین نشان می‌دهد که توسط هیچ ابزاری Pack نشده و می‌توان با استفاده از ابزارهای تحلیلی به کدهای آن دست یافت. اما عدم استفاده از Packerها بدین مهنی نیست که هیچگونه مکانیزم دفاعی بر روی باج‌افزار صورت نگرفته است. در مراحل بعدی به این مکانیزم‌ها اشاره خواهدشد که شامل مبهم‌سازی فایل، استفاده از آنتی-دیباگرو غیره می‌باشد.



شکل ۶ شناسایی کامپایلر باج‌افزار

۲-۴ کتابخانه و توابع مورد استفاده

کتابخانه‌ها، توابع و رشته‌هایی که در طول فرایند دیس‌اسمبل فایل باج‌افزار بدست می‌آید در جداول زیر آورده شده است. این جداول شامل تمام کتابخانه‌ها (۴ مورد)، توابع موجود در مورد استفاده از هر کتابخانه و رشته‌های قابل فهم می‌باشند.

جدول ۳ کتابخانه و توابع مورد استفاده توسط باج‌افزار

Library: Kernel32.dll	Functions Count: 84
RaiseException, GetLastError, MultiByteToWideChar, lstrlenA, InterlockedDecrement, GetProcAddress, LoadLibraryA, FreeResource, SizeofResource, LockResource, LoadResource, FindResourceA, GetModuleHandleA, Module32Next, CloseHandle, Module32First, CreateToolhelp32Snapshot, GetCurrentProcessId, SetEndOfFile, GetStringTypeW, GetStringTypeA, LCMapStringW, LCMapStringA, GetLocaleInfoA, CreateFileA, HeapFree, GetProcessHeap, HeapAlloc, GetCommandLineA, HeapCreate, VirtualFree, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, VirtualAlloc, HeapReAlloc, HeapSize, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, ReadFile, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, FlushFileBuffers, SetFilePointer, SetHandleCount, GetFileType, GetStartupInfoA, RtlUnwind, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, QueryPerformanceCounter, GetTickCount, GetSystemTimeAsFileTime, InitializeCriticalSectionAndSpinCount, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, CompareStringA, CompareStringW, SetEnvironmentVariableA, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, SetStdHandle	
Library: ole32.dll	Functions Count: 1
OleInitialize	
Library: OLEAUT32.dll	Functions Count: 9
VariantInit, SafeArrayCreate, SafeArrayAccessData, SafeArrayUnaccessData, SafeArrayDestroy, SafeArrayCreateVector, VariantClear, SysFreeString, SysAllocString	
Library: mscoree.dll	Functions Count: 1
CorBindToRuntimeEx	

برخی از توابع بالا دارای درجه حساسیت بالایی می‌باشند که استفاده از آن‌ها در عملیات‌های مخربانه دارای احتمال زیادی می‌باشد. این توابع بصورت موارد زیر می‌باشد که هرکدام از کتابخانه‌های خاصی مورد استفاده قرار گرفته است.

CreateFileA, CreateToolhelp32Snapshot, FindResourceA, GetCommandLineA, GetModuleFileNameA, GetModuleHandleA, GetModuleHandleW, GetProcAddress, GetStartupInfoA, GetTickCount, IsDebuggerPresent, LoadLibraryA, LockResource, Sleep, TerminateProcess, UnhandledExceptionFilter, VirtualAlloc, WriteFile

رشته‌های موجود و قابل دسترس هنگام دیس‌اسمبل نیز در جدول زیر قابل مشاهده می‌باشد که با استفاده از عملیات مبهم‌سازی[۱] به رشته‌های ناخوانا تبدیل شده‌اند. در برخی موارد هنگام دیس‌اسمبل فایل رشته‌هایی مشاهده می‌گردد که با استفاده Base64String تبدیل شده‌اند. از بین رشته‌های موجود در جدول زیر می‌توان به آدرس‌های مسیرهایی از سیستم و غیره اشاره کرد.

جدول ۴ رشته‌های قابل استخراج از فایل باج‌افزار

[۱] Obfuscation

C:\Windows\system32\uxtheme.dll

Spec=C:\Windows\system32\cmd.exe

FP_NO_HOST_CHECK=NO

HOMEDRIVE=C:

Path=C:\Windows\system32;C:\Windows;C:\Windows

CommonProgramFiles=C:\Program Files\Common Files

encrypt and decrypt" keyC

:\ProgramData\newpatek\onmywrist.bat

strings:

!This program cannot be run in DOS mode.

.?AV_com_error@@

KERNEL32.DLL

svchosta.exe

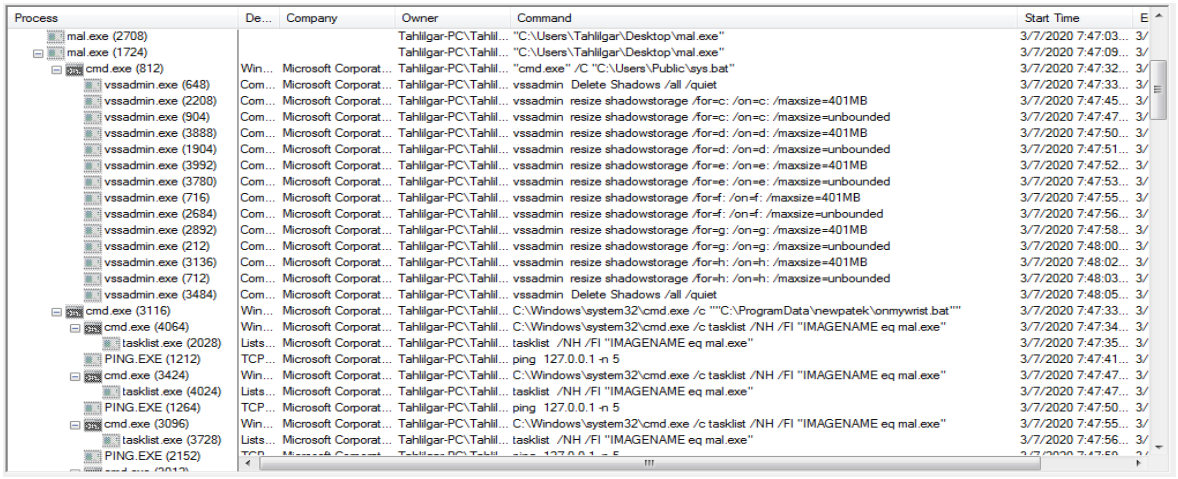
D$(W

D$4x

D$5a

۳-۴ پروسس‌های ایجاد شده توسط باج‌افزار

شکل زیر فرایندهای اجرایی توسط باج‌افزار را نشان می‌دهد که در آن در محیط cmd دستورات مختلفی را بصورت پشت سرهم اجرا می‌کند. بخش از این دستورات برای غیرفعالسازی و یا پاکسازی فایل‌های Shadow می‌باشد. بخشی نیز جهت تغییر سایز محل ذخیره‌سازی Shadow بوده و در انتها نیز مشاهده می‌گردد که با استفاده از دستور Ping روی آدرس 127.0.0.1 بررسی می‌کند.



Process	De...	Company	Owner	Command	Start Time	E
mal.exe (2708)			Tahlilgar-PC\Tahlil...	"C:\Users\Tahlilgar\Desktop\mal.exe"	3/7/2020 7:47:03...	3/
mal.exe (1724)			Tahlilgar-PC\Tahlil...	"C:\Users\Tahlilgar\Desktop\mal.exe"	3/7/2020 7:47:09...	3/
cmd.exe (812)	Win...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	"cmd.exe" /C "C:\Users\Public\sys.bat"	3/7/2020 7:47:32...	3/
vssadmin.exe (648)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin Delete Shadows /all /quiet	3/7/2020 7:47:33...	3/
vssadmin.exe (2208)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB	3/7/2020 7:47:45...	3/
vssadmin.exe (904)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded	3/7/2020 7:47:47...	3/
vssadmin.exe (3888)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB	3/7/2020 7:47:50...	3/
vssadmin.exe (1904)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded	3/7/2020 7:47:51...	3/
vssadmin.exe (3992)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=e: /on=e: /maxsize=401MB	3/7/2020 7:47:52...	3/
vssadmin.exe (3780)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=e: /on=e: /maxsize=unbounded	3/7/2020 7:47:53...	3/
vssadmin.exe (716)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=f: /on=f: /maxsize=401MB	3/7/2020 7:47:55...	3/
vssadmin.exe (2684)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=f: /on=f: /maxsize=unbounded	3/7/2020 7:47:56...	3/
vssadmin.exe (2892)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=g: /on=g: /maxsize=401MB	3/7/2020 7:47:58...	3/
vssadmin.exe (212)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=g: /on=g: /maxsize=unbounded	3/7/2020 7:48:00...	3/
vssadmin.exe (3136)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=h: /on=h: /maxsize=401MB	3/7/2020 7:48:02...	3/
vssadmin.exe (712)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin resize shadowstorage /for=h: /on=h: /maxsize=unbounded	3/7/2020 7:48:03...	3/
vssadmin.exe (3484)	Com...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	vssadmin Delete Shadows /all /quiet	3/7/2020 7:48:05...	3/
cmd.exe (3116)	Win...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	C:\Windows\system32\cmd.exe /c ""C:\ProgramData\newpatek\onmywrist.bat""	3/7/2020 7:47:33...	3/
cmd.exe (4064)	Win...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	C:\Windows\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq mal.exe"	3/7/2020 7:47:34...	3/
tasklist.exe (2028)	Lists...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	tasklist /NH /FI "IMAGENAME eq mal.exe"	3/7/2020 7:47:35...	3/
PING.EXE (1212)	TCP...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	ping 127.0.0.1 -n 5	3/7/2020 7:47:41...	3/
cmd.exe (3424)	Win...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	C:\Windows\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq mal.exe"	3/7/2020 7:47:47...	3/
tasklist.exe (4024)	Lists...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	tasklist /NH /FI "IMAGENAME eq mal.exe"	3/7/2020 7:47:47...	3/
PING.EXE (1264)	TCP...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	ping 127.0.0.1 -n 5	3/7/2020 7:47:50...	3/
cmd.exe (3096)	Win...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	C:\Windows\system32\cmd.exe /c tasklist /NH /FI "IMAGENAME eq mal.exe"	3/7/2020 7:47:55...	3/
tasklist.exe (3728)	Lists...	Microsoft Corporat...	Tahlilgar-PC\Tahlil...	tasklist /NH /FI "IMAGENAME eq mal.exe"	3/7/2020 7:47:56...	3/
PING.EXE (2152)						

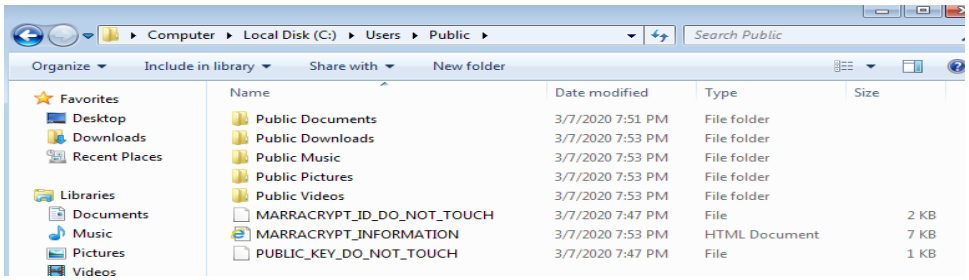
شکل ۷ زیرپروسس‌های فراخوانی شده توسط باج‌افزار (Process Tree)

۴-۴ فایل‌های ایجاد شده

همانطور که قبلا نیز ذکر گردید باج‌افزار بعد از اجرا در سیستم اقدام به ایجاد فایل‌هایی در سیستم می‌کند. این فایل‌های بصورت موارد موجود در شکل زیر می‌باشند.

1724	CreateFile	C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
1724	CreateFile	C:\Users\Public\PUBLIC_KEY_DO_NOT_TOUCH
1724	CreateFile	C:\Users\Public\MARRACRYPT_ID_DO_NOT_TOUCH
1724	CreateFile	C:\Users\Public\sys.bat
1724	CreateFile	C:\Users\Public\PUBLIC_KEY_DO_NOT_TOUCH
1724	WriteFile	C:\Users\Public\PUBLIC_KEY_DO_NOT_TOUCH

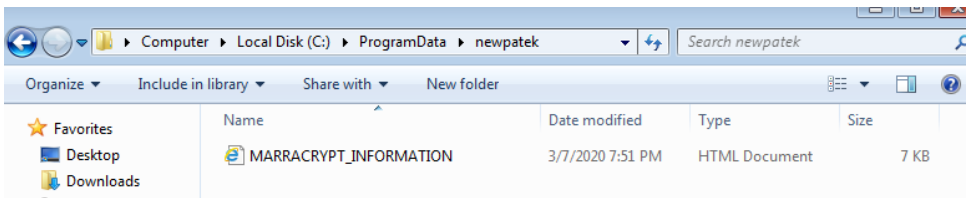
شکل ۸ فایل ایجاد شده توسط باج‌افزار در سیستم



شکل ۹ فایل‌های ایجاد شده در مسیری از سیستم

1724	CreateFile	C:\ProgramData\newpatek\onmywrist.bat
1724	CreateFile	C:\ProgramData\newpatek\onmywrist.bat
1724	WriteFile	C:\ProgramData\newpatek\onmywrist.bat
1724	CreateFile	C:\Windows\AppPatch\sysmain.sdb
1724	CreateFile	C:\ProgramData\newpatek
1724	CreateFile	C:\ProgramData\newpatek\onmywrist.bat

شکل ۱۰ لاگ مربوط به ایجاد فایل onmywrist.bat



شکل ۱۱ فایل راهنما ایجاد شده در مسیر ProgramData

۵-۴ تغییرات رجیستری

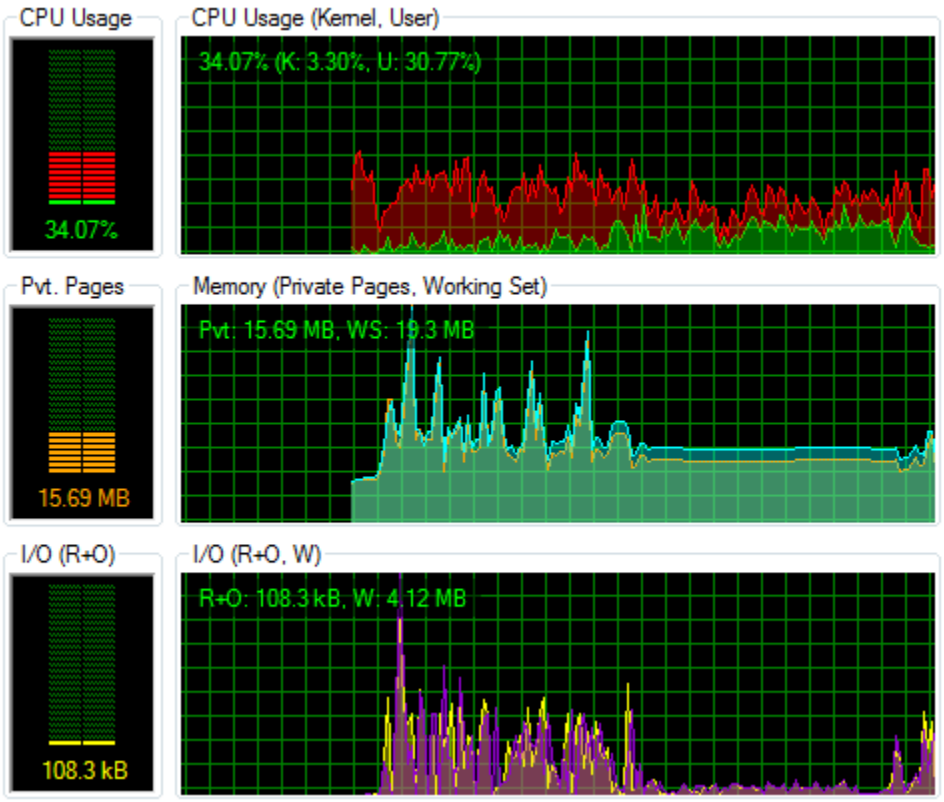
این باج‌افزار در طول فعالیت خود هیچگونه تغییراتی در بخش رجیستری ندارد.

۴-۶ ارتباطات شبکه

علاوه بر بخش رجیستری، در قسمت شبکه نیز این باج‌افزار فعالیت خاصی را نداشته و در بررسی‌ها مشاهده گردید که با هیچ آدرسی در ارتباط نمی‌باشد. فعالیت شبکه‌ای این باج‌افزار فقط دستورات Ping می‌باشد که روی آدرس 127.0.0.1 صورت می‌گیرد.

۴-۷ وضعیت منابع سیستم

شکل زیر وضعیت منابع سیستم را برای باج‌افزار نشان می‌دهد. این شکل فقط مختص فعالیت باج‌افزار در سیستم بوده و مقادیر آن از بقیه بخش‌های اجرایی تفکیک شده می‌باشد.



شکل ۱۲ وضعیت منابع سیستم در طول فعلیت باج‌افزار

با توجه به شکل بالا مشاهده می‌گردد که مقادیر هر سه منبع مصرفی در سیستم در طول فعالیت باج‌افزار بیشتر بوده و حتی در بخش‌هایی نیز به حداکثر مقدار خود رسیده است.

۴-۸ پسوندهای قابل رمزگذاری توسط باج‌افزار

این باج‌افزار قابلیت رمزگذاری روی تمامی فایل‌های سیستم بجز فایل‌هایی با پسوند exe. را دارد.

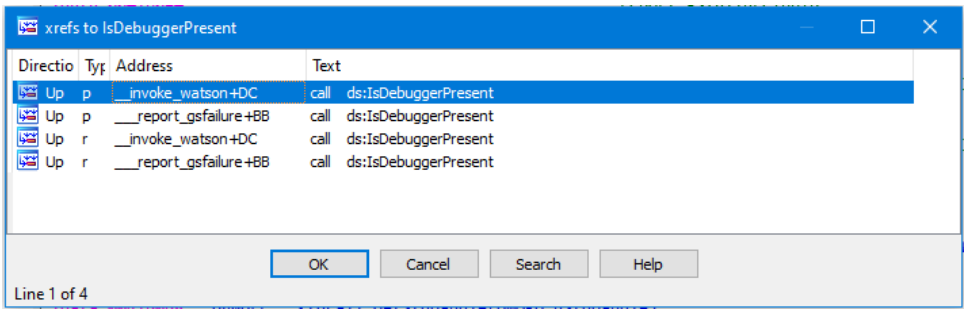
۵ تحلیل کد

۵-۱ استفاده از مکانیز آنتی دیباگ

همانطور که قبلا نیز ذکر گردید باج‌افزار برای جلوگیری از تحلیل در محیط و ابزارهای دیباگر همانند OllyDbg از روش دفاعی استفاده می‌کند. این روش دفاعی استافده از تابع IsDebuggerPresent می‌باشد که در چندین بخش از کل فایل استفاده شده است. شکل زیر نمونه‌ای از کاربرد این تابع و محل‌های مختلف مورد استفاده از این تابع را نشان می‌دهند.

```
call    ds:IsDebuggerPresent
push    0               ; lpTopLevelExceptionFilter
mov     ebx, eax
call    ds:SetUnhandledExceptionFilter
lea     eax, [ebp+ExceptionInfo]
push    eax             ; ExceptionInfo
call    ds:UnhandledExceptionFilter
test    eax, eax
jnz     short loc_40E6E5
test    ebx, ebx
jnz     short loc_40E6E5
push    2
call    sub_4138BC
pop     ecx
```

شکل ۱۳ استفاده از تابع IsDebuggerPresent برای شناسایی دیباگر



شکل ۱۴ آدرس‌های استفاده از تابع شناسایی دیباگر

۵-۲ ایجاد فایل

باج‌افزار بعد از اجرا در سیستم چندین فایل از جمله فایل راهنما را در سیستم ایجاد می‌کند. برای اینکار از تابع CreateFile استفاده می‌گردد که نحوه استفاده از آن بصورت شکل زیر می‌باشد.

```
mov     eax, [ebp+arg_0]
mov     edi, ds:CreateFileA
push    ebx             ; hTemplateFile
push    [ebp+dwFlagsAndAttributes] ; dwFlagsAndAttributes
mov     dword ptr [eax], 1
push    [ebp+dwCreationDisposition] ; dwCreationDisposition
lea     eax, [ebp+SecurityAttributes]
push    eax             ; lpSecurityAttributes
push    [ebp+dwShareMode] ; dwShareMode
push    [ebp+dwDesiredAccess] ; dwDesiredAccess
push    [ebp+lpFileName] ; lpFileName
call    edi ; CreateFileA
```

شکل ۱۵ تابع ایجاد فایل در سیستم

۵-۳ نوشتن فایل

همچنین بعد از رمزگذاری فایل‌های سیستم، فایل اصلی را پاک کرده و فایل جدید را با پسوند جدید می‌نویسد. این عملیات نیز با استفاده از تابع WriteFile صورت می‌گیرد که بصورت شکل زیر می‌باشند.

```
push    0               ; lpOverlapped
lea     eax, [ebp+NumberOfBytesWritten]
push    eax             ; lpNumberOfBytesWritten
push    esi             ; nNumberOfBytesToWrite
lea     eax, [ebp+MultiByteStr]
push    eax             ; lpBuffer
mov     eax, [ebp+var_1AD8]
mov     eax, [eax]
push    dword ptr [edi+eax] ; hFile
call    ds:WriteFile
```

شکل ۱۶ استفاده از تابع نوشتن فایل

۵-۴ خواندن فایل

باجافزار برای رمزگذاری فایل‌ها آن‌ها را یکی پس از دیگری دریافت کرده و عملیات رمزگذاری را روی آن‌ها انجام می‌دهد. برای این از تابع ReadFile استفاده می‌کند که بصورت زیر می‌باشد.

```
push    ebx             ; lpOverlapped
lea     ecx, [ebp+NumberOfBytesRead]
push    ecx             ; lpNumberOfBytesRead
push    [ebp+nNumberOfBytesToRead] ; nNumberOfBytesToRead
push    eax             ; lpBuffer
mov     eax, [edi]
push    dword ptr [esi+eax] ; hFile
call    ds:ReadFile
```

شکل ۱۷ تابع خواندن فایل از سیستم

۶ توصیه‌های امنیتی برای پیشگیری

۱) گرفتن فایل پشتیبان بصورت دوره‌ای از فایل‌های سیستم و ذخیره آن در محل دیگر

۲) استفاده از آنتی‌ویروس قوی و بروزرسانی مداوم آن
۳) خودداری از بازکردن و اجرا فایل‌های مشکوک و ناشناس
۴) خودداری از بازکردن ایمیل‌های مشکوک و ناشناس
۵) اطمینان از سالم بودن دستگاه‌های جانبی مانند فلش
۶) استفاده از رمزعبور قوی بر روی درایوهای سیستم
۷) استفاده از سیستم‌عامل جدید و بروزرسانی شده
۸) بروزرسانی مداوم سیستم عامل
۹) پیکربندی مناسب پروتکل‌های مورد استفاده در شبکه متناسب با محیط کار