بسمه‌تعالی

گزارش تحلیلی بدافزار

Kharma Ransomware

فهرست مطالب

۱ مقدمه

باج‌افزار Kharma یکی از بدافزارهای رمزگذار فایل و از خانواده Dharma/Crysis می‌باشد که در ماه نوامبر ۲۰۱۹ میلادی از طریق فایل‌های ضمیمه ایمیل‌های آلوده، وب‌سایت‌های تورنت و تبلیغات مخرب انتشار یافته است که برای اولین بار توسط Raby کشف شده است. با توجه به فایل ایجاد شده توسط باج‌افزار در سیستم مهاجمان ادعا می‌کنند که فایل‌های سیستم با استفاده از الگوریتم RSA2048 رمزشده است. تمام فایل‌هایی که به صورت رمزشده درآمده‌اند به انتهای آن‌ها پسوند .id-ID.[teammarcy10@cock.li].kharma اضافه شده و در داخل هر پوشه دو فایل راهنما با نام‌های RETURN FILES.txt و Info.hta ایجاد می‌گردد. کاربران قربانی شده برای بازگردانی فایل‌های خود و ارتباط با مهاجمان می‌توانند با آدرس ایمیل teammarcy10@cock.li در ارتباط باشند.

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 دات‌نت طراحی شده است و شامل اطلاعات زیر می‌باشد.

جدول ۱ - مشخصات کلی باج‌افزار

Kharma - Ransomware	**نام و نوع بدافزار**
.id-ID.[teammarcy10@cock.li].kharma	**پسوند و نام فایل**
Infected email attachments (macros), torrent websites, malicious ads.	**نحوه انتشار**
November 2019	**زمان کامپایل**
A7ED8D2F98253CE0A8492691190A6477	**هش md5**
075CE36BE0DF13E7C18BA6917F59211695E0BB55	**هش SHA1**
80EA514104F77B355CA6A4B8BC024F8A13370CC06D376A5EA36D9AF2F05CB04C	**هش SHA256**
Microsoft Visual Studio .NET (managed)	**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**
133632 bytes	**حجم فایل**
7.811	**آنتروپی فایل**
32 bits	**معماری فایل**
3	**تعداد بخش**
sad sa assd sa	**File Description**
C:\Users\User\Documents\Visual Studio 2015\Projects\34\34\obj\x86\Release\34.pdb	**آدرس فایل pdb**

۲–۲ بخش‌های مختلف فایل

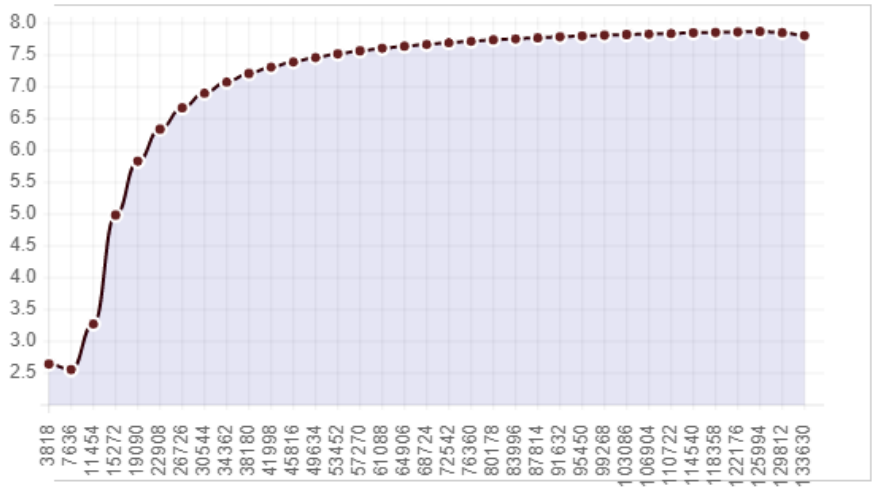
جدول شماره ۲ بخش‌های مختلف فایل بدافزار را همراه با جزئیات کامل مانند مقدار آنتروپی، اندازه مجازی و غیره نشان می‌دهد که متشکل از سه بخش بصورت text، rsrc و reloc می‌باشد.

جدول ۲ - بخش‌های مختلف باج‌افزار

ردیف	نام بخش	آدرس مجازی	اندازه مجازی	اندازه خام	آنتروپی
1	text	8192	130532	130560	7.86
2	rsrc	139264	1560	2048	3.43
3	reloc	147456	12	512	0.1

۳-۲ مقدار آنتروپی

شکل زیر وضعیت آنتروپی کلی فایل را در حالت عادی بصورت نموداری نشان می‌دهد. مقدار این آنتروپی برابر با 7.811 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 و آنتروپی کلی فایل بالاتر از هفت می‌باشد. همچنین مقدار آنتروپی برای بخش reloc تقریبا نزدیک صفر می‌باشد. مقدار بیشتر از هفت و روند صعودی این مقدار و همچنین مقدار صفر آنتروپی، رفتار غیرعادی و احتمال بدافزار بودن فایل را نشان می‌دهد.

۳ وضعیت تشخیص فایل در آنتی‌ویروس‌ها

شکل شماره ۲ وضعیت تشخیص فایل مورد بررسی را در ویروس‌توتال نشان می‌دهد که از بین ۶۹ موتور، ۵۰ موتور این فایل را بدافزار تشخیص داده‌اند. در برخی موارد نوع تشخیص این فایل بصورت Trojan.Ransom.Crysis می‌باشد.

Ad-Aware	Gen:Heur.MSIL.Androm.1	AegisLab	Trojan.Win32.Generic.4!c
AhnLab-V3	Trojan/Win32.Androm.C3577319	ALYac	Trojan.Ransom.Crysis
SecureAge APEX	Malicious	Arcabit	Trojan.MSIL.Androm.1
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1015447	BitDefender	Gen:Heur.MSIL.Androm.1
BitDefenderTheta	Gen:NN.ZemsilF.32515.im0@auMrPMh	CAT-QuickHeal	Trojan.Generic
Comodo	Malware@#8hmm9j82m9y	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.f98253	Cylance	Unsafe
Cyren	W32/Trojan.GRSN-1344	DrWeb	Trojan.Encoder.30142
Emsisoft	Gen:Heur.MSIL.Androm.1 (B)	Endgame	Malicious (high Confidence)
eScan	Gen:Heur.MSIL.Androm.1	ESET-NOD32	A Variant Of MSIL/Kryptik.TTR
F-Secure	Heuristic.HEUR/AGEN.1015447	FireEye	Generic.mg.a7ed8d2f98253ce0
Fortinet	MSIL/Generic.TTR!tr.ransom	GData	Gen:Heur.MSIL.Androm.1
Ikarus	Trojan.MSIL.Crypt	Jiangmin	Trojan.Generic.eiwee
K7AntiVirus	Trojan (0055bd6a1)	K7GW	Trojan (0055bd6a1)
Kaspersky	HEUR:Trojan.Win32.Generic	Malwarebytes	Ransom.FileCryptor
MAX	Malware (ai Score=86)	MaxSecure	Trojan.Malware.300983.susgen
McAfee	RDN/Generic.grp	Microsoft	Trojan:Win32/Occamy.C
NANO-Antivirus	Trojan.Win32.Encoder.giyqzs	Palo Alto Networks	Generic.ml
Panda	Trj/GdSda.A	Qihoo-360	Win32/Trojan.cdf
SentinelOne (Static ML)	DFI - Malicious PE	Sophos AV	Mal/Generic-S
Sophos ML	Heuristic	Symantec	Trojan Horse

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 ۱۵ موتور قادر به تشخیص فایل به‌عنوان بدافزار می‌باشند.

آنتی ویروس	نتیجه اسکن	
gdata	ii	Dangerous Gen:Heur.MSIL.Androm.1
comodo	ii	Dangerous
avast	✓	Clean
clamav	✓	Clean
avira	ii	Dangerous HEUR/AGEN.1015447
symantec	✓	Clean
winessentials	✓	Clean
windefender	✓	Clean
bitdefender	ii	Dangerous Gen:Heur.MSIL.Androm.1
پادویش	✓	Clean
drweb	ii	Dangerous Trojan.Encoder.30142
trustport	ii	Dangerous Gen:Heur.MSIL.Androm.1
avg	ii	Dangerous Malware-gen
cyberbyte	✓	Clean
vba32	✓	Clean
immunet	✓	Clean
gridinsoft	✓	Clean
clamwin	✓	Clean
satfaa	ii	Dangerous
eset	ii	Dangerous a variant of MSIL/Kryptik.TTR trojan
ikarus	ii	Dangerous Trojan.MSIL.Crypt
fsecure	ii	Dangerous Gen:Heur.MSIL.Androm.1
atlantis	✓	Clean
escan	ii	Dangerous Gen:Heur.MSIL.Androm.1
emsisoft	ii	Dangerous Gen:Heur.MSIL.Androm.1
kaspersky	ii	Dangerous

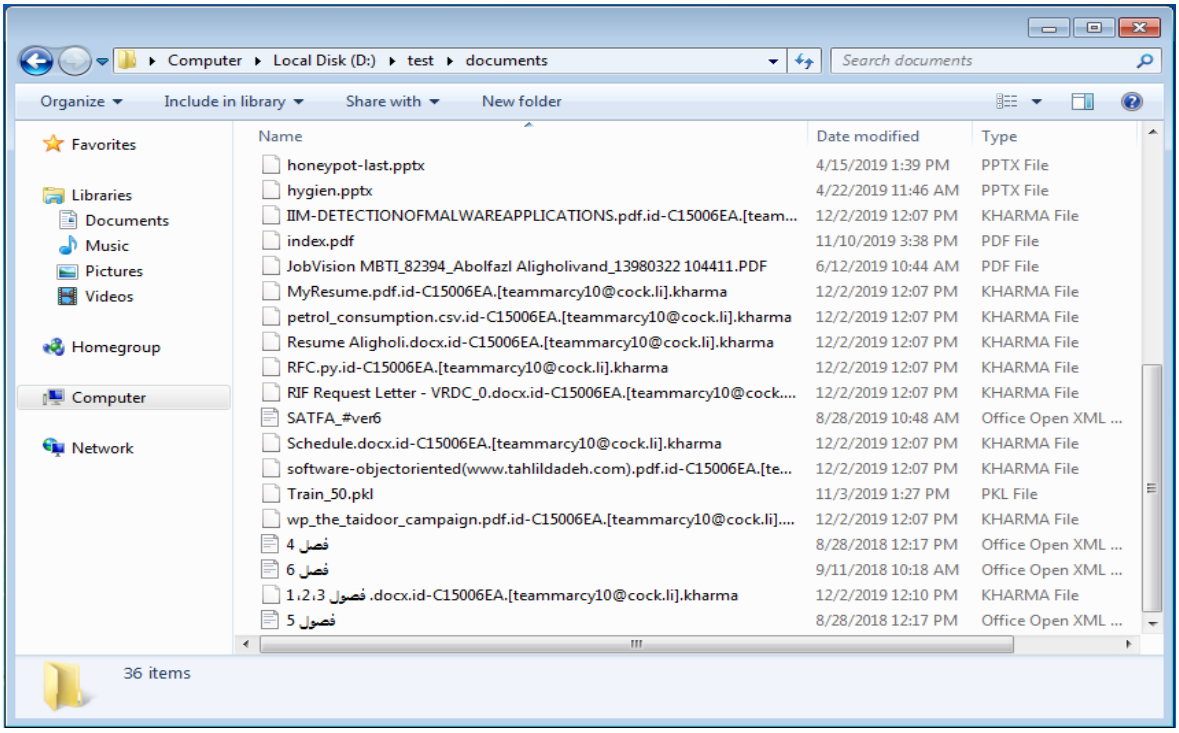
شکل ۳ بررسی فایل در سامانه ویروس‌کاو

از بین این موتورها، موتورهای بومی و موجود در این سامانه، پادویش قادر به شناسایی نبوده ولی ستفا قادر به شناسایی فایل به عنوان فایل مخرب شده است.

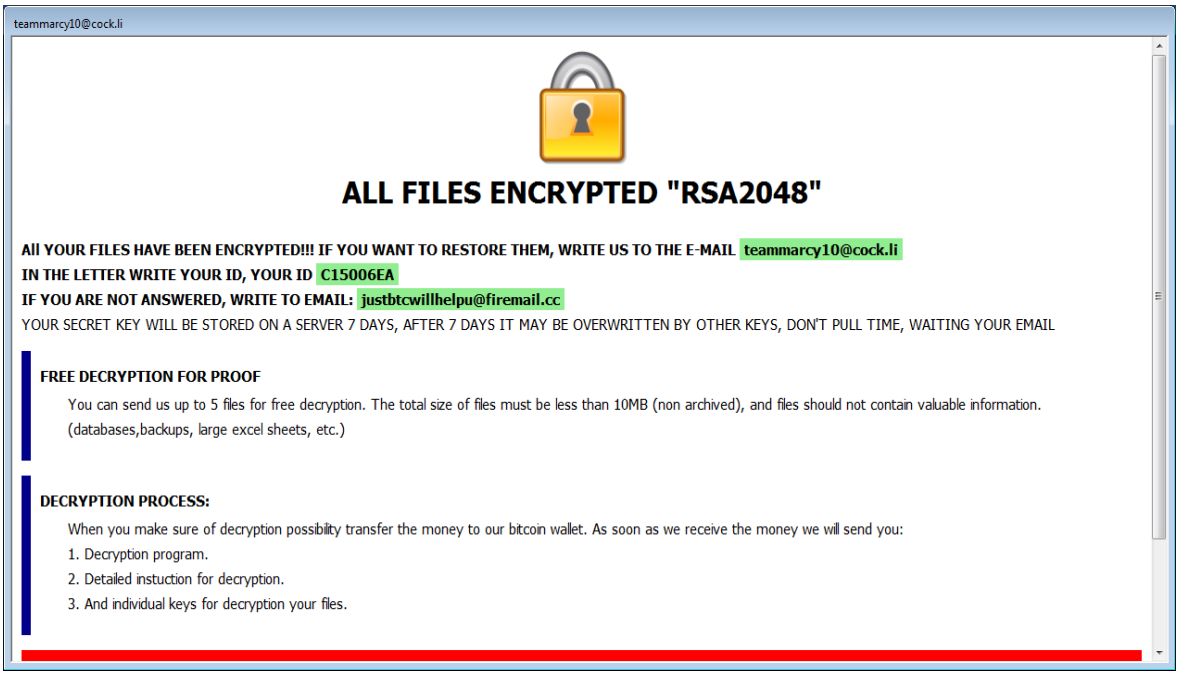
۴ فرآیند آلوده‌سازی

باج‌افزار Kharma یکی از باج‌افزارهای تازه انتشار یافته در ماه نوامبر ۲۰۱۹ از خانواده باج‌افزارهای Dharma/Crysis می‌باشد که با استفاده از فایل‌های ضمیمه ایمیل‌های جعلی، تبلیغات آلوده و وب-سایت‌های تورنت به سیستم کاربران قربانی شده انتقال می‌یابند. بر اساس ادعای طراحان این باج‌افزار و با توجه به متنی که در فایل راهنمایی که توسط آن ایجاد می‌شود، الگوریتم مورد استفاده شده برای عملیات رمزگذاری RSA 2048 می‌باشد. این باج‌افزار بعد از رمزگذاری فایل پسوند .id-ID.[teammarcy@cock.li].Kharma را به انتهای آن اضافه کرده و فایل را ناخوانا می‌کند. بعد از اتمام فعالیت نیز دو فایل راهنما با نام‌های RETURN FILES.txt و Info.hta برای راهنمایی کاربران در جهت ارتباط با مهاجمان ایجاد می‌شود. روند کلی فعالیت این باج‌افزار بعد از انتقال و نصب در سیستم به صورت زیر می‌باشد.

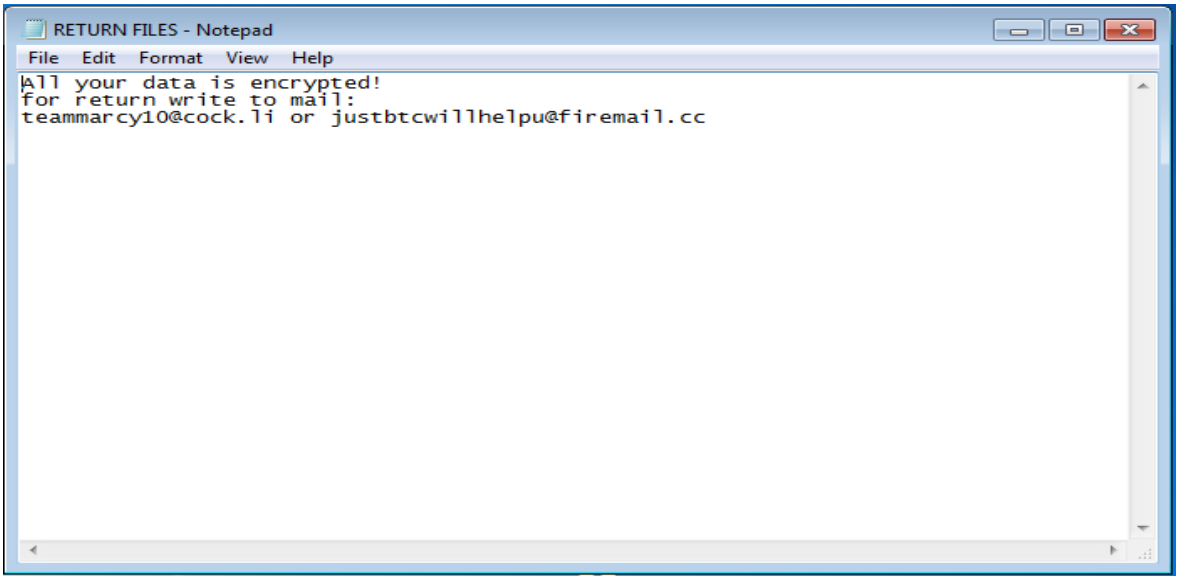
باج‌افزار بعد از اجرا ابتدا بعد از بررسی رجیستری‌های خاص در سیستم، پروسس‌های vssadmin.exe را با استفاده از دستور shell اجرا کرده و دستوری را با استفاده از این پروسس اجرا می‌کند. سپس تمامی فایل‌های موجود را بررسی کرده و آن‌ها را بصورت یک فایل رمزشده ذخیره کرده و فایل سالم را حذف می‌کند. بعد از اتمام فعالیت رمزگذاری نیز با استفاده از دستور shell پروسس tasklist.exe را جهت اجرای دستوراتی اجرا می‌کند. در انتها نیز دو فایل راهنما که قبلا نیز ذکر شده است در محیط دسکتاپ سیستم ایجاد شده و آن‌ها را برای اجرا در هر بار اجرای سیستم‌عامل در قسمت Run جیستری ثبت می‌کند. شکل‌های زیر نمونه فایل‌های رمزشده، فایل راهنما و موارد دیگر را نشان می-دهند.



شکل ۴ نمونه فایل‌های رمزشده توسط باج‌افزار



شکل ۵ فایل راهنمای ایجاد شده توسط باج‌افزار



شکل ۶ فایل راهنمای ایجاد شده توسط باج‌افزار

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 کنترل شبکه

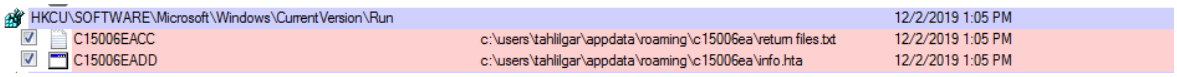
با توجه به بررسی‌هایی که صورت گرفت هیپگونه فعالیتی مبنی بر فعالیت و ارتباط شبکه‌ای مشاهده نگردید.

۵-۲ رجیستری

جدول و شکل زیر آدرس رجیستری‌های ثبت شده در سیستم را توسط باج‌افزار نشان می‌دهد. همانطور که قبلا نیز ذکر گردید بعد از اتمام رمزگذاری فایل‌های سیستم، باج‌افزار فایل‌های راهنما را در آدرس Run رجیستری ثبت می‌کند تا این فایل‌های راهنما در هر بار اجرای سیستم‌عامل برای کاربر نشان داده شود.

جدول ۳ آدرس رجیستری ثبت شده توسط باج‌افزار

عملیات	آدرس رجیستری
SetValueKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\C15006EACC
SetValueKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\C15006EADD



شکل ۷ آدرس رجیستری ثبت شده توسط باج‌افزار

۵-۳ پروسس‌های اجراشده

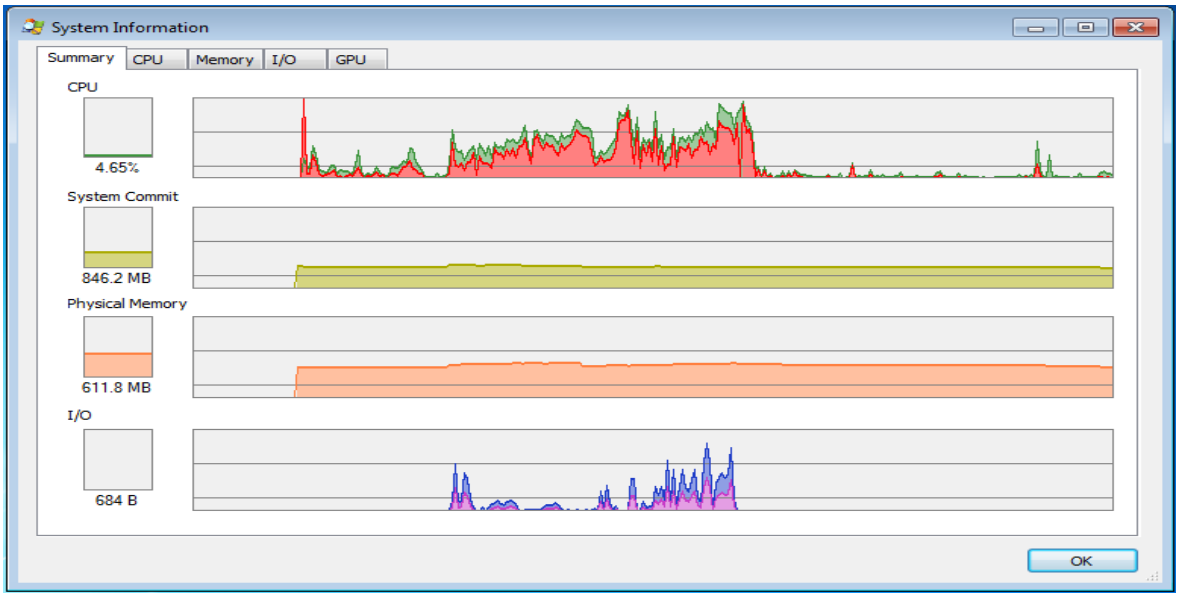
شکل زیر پروسس‌های ایجاد شده توسط باج‌افزار را نشان می‌دهد. در این شکل مشاهده می‌گردد که با استفاده از tasklist دستوراتی را در سیستم اجرا می‌کند. سپس با استفاده از mshta فایل راهنما را ایجاد می‌کند.

Description	Image Path	Life Time	Company	Owner	Command
sad sa assd sa	C:\Users\Tahlilgar\Desktop\34.exe		dg dfsda ghdsf	Tahlilgar-PC\Tahlil...	"C:\Users\Tahlilgar\Desktop\34.exe"
Lists the current running tasks	C:\Windows\system32\tasklist.exe		Microsoft Corporat...	Tahlilgar-PC\Tahlil...	"tasklist" /v /fo csv
Lists the current running tasks	C:\Windows\system32\tasklist.exe		Microsoft Corporat...	Tahlilgar-PC\Tahlil...	"tasklist" /v /fo csv
Lists the current running tasks	C:\Windows\system32\tasklist.exe		Microsoft Corporat...	Tahlilgar-PC\Tahlil...	"tasklist" /v /fo csv
Lists the current running tasks	C:\Windows\system32\tasklist.exe		Microsoft Corporat...	Tahlilgar-PC\Tahlil...	"tasklist" /v /fo csv
Terminates Processes	C:\Windows\system32\taskkill.exe		Microsoft Corporat...	Tahlilgar-PC\Tahlil...	"taskkill" /f /pid 2032
Microsoft (R) HTML Applicatio...	C:\Windows\System32\mshta.exe		Microsoft Corporat...	Tahlilgar-PC\Tahlil...	"C:\Windows\System32\mshta.exe" "C:\Users\Tahlilgar\Desktop\Info.hta"

شکل ۸ پروسس‌های فعال و اجرا شده توسط فایل باج‌افزار

۵-۴ وضعیت منابع سیستم

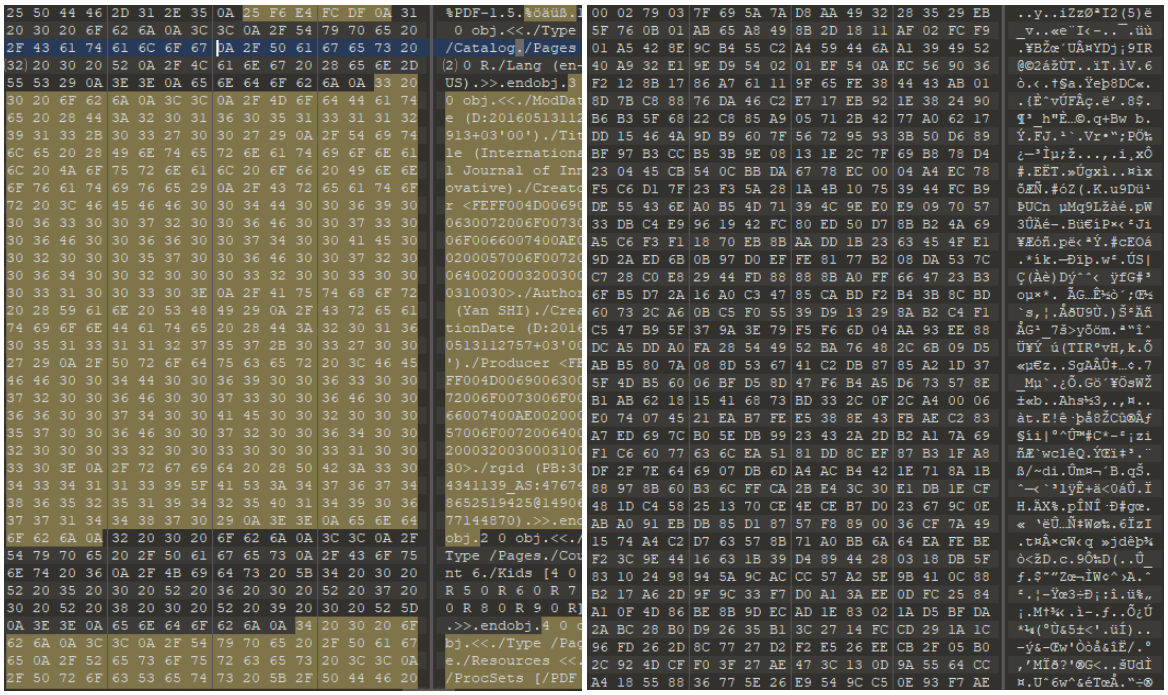
شکل زیر وضعیت منابع سیستم را در زمانی نشان می‌دهد که باج‌افزار در حال فعالیت بوده و فایل-های سیستمی را رمزگذاری می‌کند. با توجه به شکل مشاهده می‌گردد که در بیشتر مواقع میزان مصرفی CPU به حداکثر مقدار خود رسیده و منابع دیگر مانند IO نیز با بیشترین مقدار در حال فعالیت هستند.



شکل ۹ وضعیت منابع سیستم در طول فعالیت باج‌افزار در سیستم

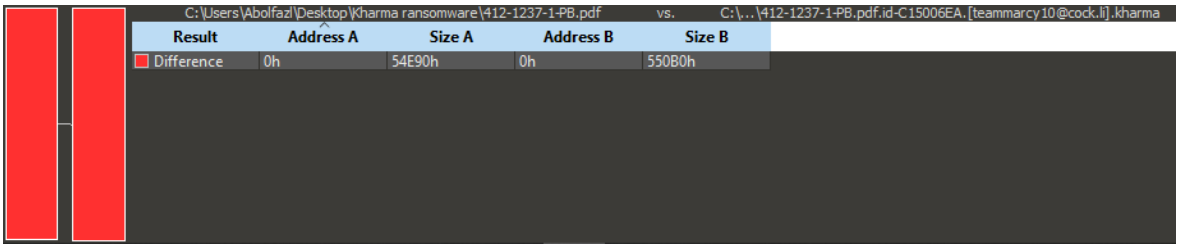
۵-۵ نمونه فایل رمزشده

نمونه فایل تست شده برای این باج‌افزار یک فایل pdf می‌باشد که ساختار باینری آن قبل و بعد از رمزگذاری بصورت شکل ۱۱ می‌باشد. بخش سمت راست مربوط به حالت رمزشده و بخش سمت چپ مربوط به حالت عادی فایل می‌باشد.



شکل ۱۰ ساختار باینری فایل pdf در حالت عادی و رمزشده

شکل زیر نیز تفاوت باینری دو فایل را در حالت‌های قبل و بعد از عملیات رمزگذاری نشان می‌دهد. با توجه به شکل مشاهده می‌گردد تمام ساختار فایل رمز شده و هیچ نقطه مشترکی وجود ندارد.



شکل ۱۱ تفاوت میان ساختار باینری فایل pdf در حالت‌های رمز شده و عادی

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