

بسمه تعالی

# گزارش تحلیلی بدافزار

## Kharma Ransomware

## فهرست مطالب

۱	مقدمه	1
۲	مشخصات و جزئیات کامل فایل	۲
۲-1	مشخصات فایل	۲
۲-۲	بخش‌های مختلف فایل	۲
۳-۲	مقدار آنتروپی	۳
۳	وضعیت تشخیص فایل در آنتی‌ویروس‌ها	۳
۴	فرآیند آلوده‌سازی	۴
۵	شرح تحلیل	۵
۱-۵	کنترل شبکه	۵
۲-۵	رجیستری	۵
۳-۵	پروسس‌های اجرا شده	۵
۴-۵	وضعیت منابع سیستم	۵
۵-۵	نمونه فایل رمز شده	۵
۱۰	توصیه‌های امنیتی برای پیشگیری	۶

## ۱ مقدمه

باج افزار Kharma یکی از بدافزارهای رمزگذار فایل و از خانواده Dharma/Crysis می باشد که در ماه نوامبر ۲۰۱۹ میلادی از طریق فایل های ضمیمه ایمیل های آلوده، وبسایت های تورنت و تبلیغات مخرب انتشار یافته است که برای اولین بار توسط Raby کشف شده است. با توجه به فایل ایجاد شده توسط باج افزار در سیستم مهاجمان ادعا می کنند که فایل های سیستم با استفاده از الگوریتم RSA2048 رمز شده است. تمام فایل هایی که به صورت رمز شده درآمده اند به انتهای آنها پسوند `id-ID.[teammarcy10@cock.li].kharma` اضافه شده و در داخل هر پوشه دو فایل راهنما با نام های `RETURN FILES.txt` و `Info.hta` ایجاد می گردد. کاربران قربانی شده برای بازگردانی فایل های خود و ارتباط با مهاجمان می توانند 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.

### ۱-۲ مشخصات فایل

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

جدول ۱ - مشخصات کلی باج افزار

Kharma - Ransomware	نام و نوع بدافزار
.id-ID.[teammarcy10@cock.li].kharma	پسوندها 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 asssd 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

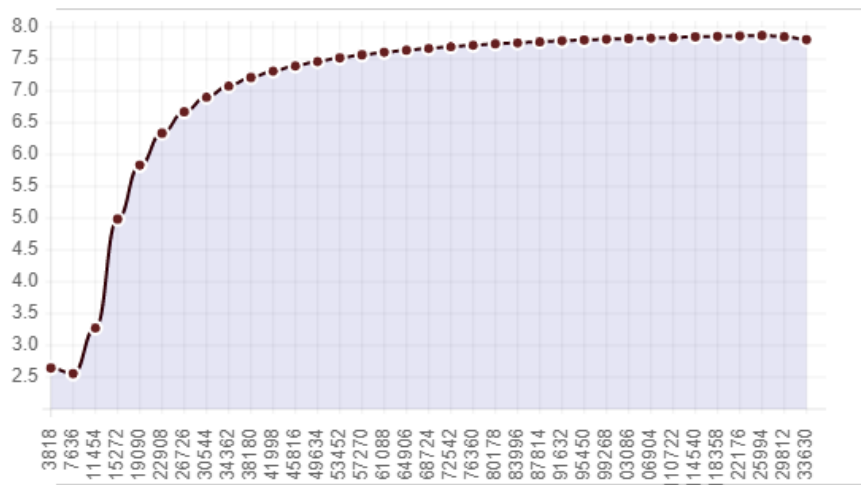
جدول شماره ۲ بخش‌های مختلف فایل بدافزار را همراه با جزئیات کامل مانند مقدار آنتروپی، اندازه مجازی و غیره نشان می‌دهد که متشکل از سه بخش بصورت text, rsrc و reloc می‌باشد.

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 تقریباً 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	① Gen:Heur.MSIL.Androm.1	AegisLab	① Trojan.Win32.Generic.4lc
AhnLab-V3	① Trojan/Win32.Androm.C3577319	ALYac	① Trojan.Ransom.Crysis
SecureAge APEX	① Malicious	Arcabit	① Trojan.MSIL.Androm.1
Avast	① Win32.Malware-gen	AVG	① Win32.Malware-gen
Avira (no cloud)	① HEUR/AGEN.1015447	BitDefender	① Gen:Heur.MSIL.Androm.1
BitDefenderTheta	① Gen:NN.Zemslif.32515.im0@auMrPMh	CAT-QuickHeal	① Trojan.Generic
Comodo	① Malware@#8hmm9j82m9y	CrowdStrike Falcon	① Win/malicious_confidence_100% (W)
Cybereason	① Malicious.198253	Cylance	① Unsafe
Cyren	① W32/Trojan.GRSN-1344	DrWeb	① Trojan.Encoder.30142
Emsisoft	① Gen:Heur.MSIL.Androm.1 (B)	Endgame	① Malicious (high Confidence)
eScan	① Gen:Heur.MSIL.Androm.1	ESET-NOD32	① A Variant Of MSIL/Kryptik.TTR
F-Secure	① Heuristic.HEUR/AGEN.1015447	FireEye	① Generic.mg.a7ed8d2f98253ce0
Fortinet	① MSIL/Generic.TTRltr.ransom	GData	① Gen:Heur.MSIL.Androm.1
Ikarus	① Trojan.MSIL.Crypt	Jiangmin	① Trojan.Generic.eiwee
K7AntiVirus	① Trojan ( 0055bd6a1 )	K7GW	① Trojan ( 0055bd6a1 )
Kaspersky	① HEUR:Trojan.Win32.Generic	Malwarebytes	① Ransom.FileCryptor
MAX	① Malware (ai Score=86)	MaxSecure	① Trojan.Malware.300983.susgen
McAfee	① RDN/Generic.grp	Microsoft	① Trojan.Win32/Occamy.C
NANO-Antivirus	① Trojan.Win32.Encoder.giyqzs	Palo Alto Networks	① Generic.ml
Panda	① Trj/GdSda.A	Qihoo-360	① Win32/Trojan.cdf
SentinelOne (Static ML)	① DFI - Malicious PE	Sophos AV	① Mal/Generic-S
Sophos ML	① Heuristic	Symantec	① Trojan.Horse

## شکل ۲ نتیجه بررسی فایل در سایت ویروس توتال

همچنین شکل شماره ۳ نشان دهنده وضعیت تشخیص فایل در سامانه [ویروس کاو](#) می باشد. در این سامانه از بین ۳۲ موتور موجود ۱۵ موتور قادر به تشخیص فایل به عنوان بدافزار می باشند.

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

شکل ۳ بررسی فایل در سامانه ویروس کاو

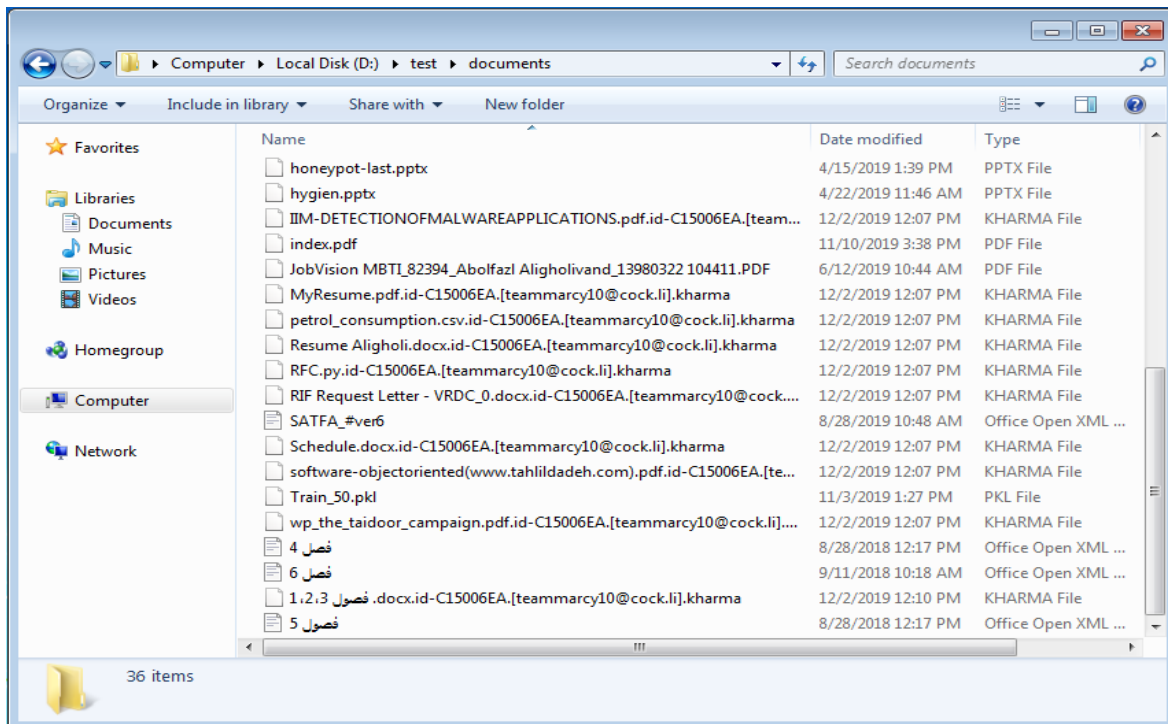
از بین این موتورها، موتورهای بومی و موجود در این سامانه، پادویش قادر به شناسایی نبوده ولی ستفا قادر به شناسایی فایل به عنوان فایل مخرب شده است.

## ۴ فرآیند آلوده سازی

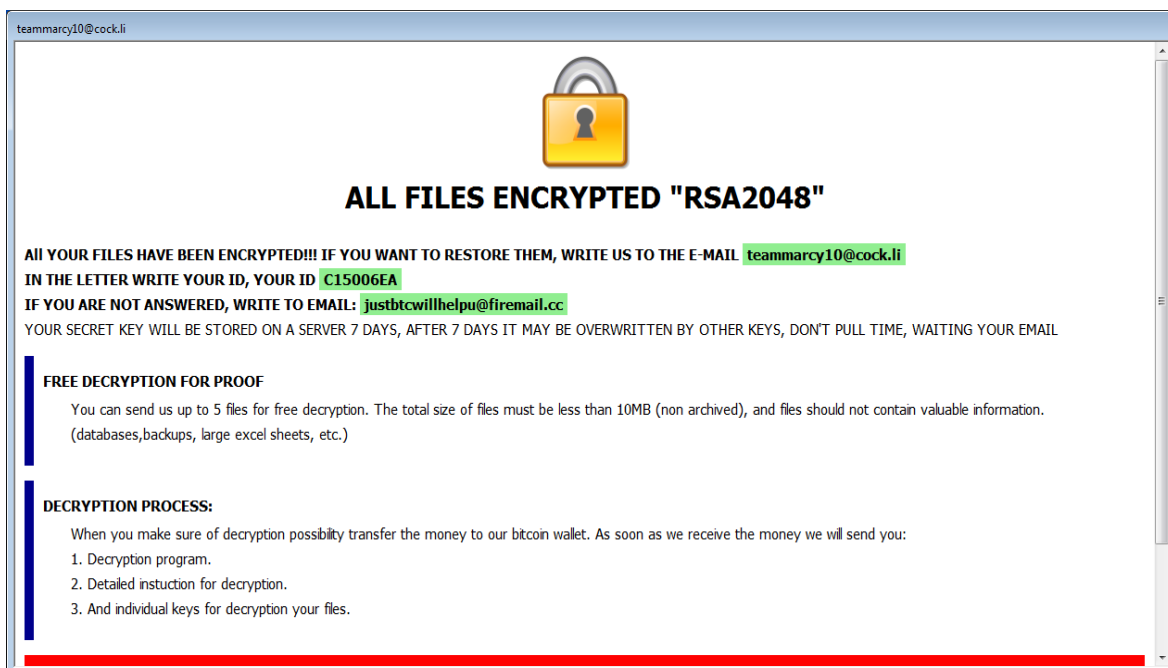
باج افزار Kharma یکی از باج افزارهای تازه انتشار یافته در ماه نوامبر ۲۰۱۹ از خانواده باج افزارهای Dharma/Crysis می باشد که با استفاده از فایل های ضمیمه ایمیل های جعلی، تبلیغات آلوده و وب-سایت های تورنت به سیستم کاربران قربانی شده انتقال می یابند. بر اساس ادعای طراحان این باج افزار و با توجه به متنی که در فایل راهنمایی که توسط آن ایجاد می شود، الگوریتم مورد استفاده شده برای عملیات رمزگذاری RSA 2048 می باشد. این باج افزار بعد از رمزگذاری فایل پسوند id-.Kharma.teammarcy@cock.li را به انتهای آن اضافه کرده و فایل را ناخوانا می کند. بعد از اتمام فعالیت نیز دو فایل راهنما با نام های RETURN FILES.txt و Info.hta برای راهنمایی کاربران در جهت ارتباط با مهاجمان ایجاد می شود. روند کلی فعالیت این باج افزار بعد از انتقال و نصب در سیستم به صورت زیر می باشد.

باج افزار بعد از اجرا ابتدا بعد از بررسی رجیستری های خاص در سیستم، پروسس های vssadmin.exe را با استفاده از دستور shell اجرا کرده و دستوری را با استفاده از این پروسس اجرا می کند. سپس تمامی فایل های موجود را بررسی کرده و آنها را بصورت یک فایل رمز شده ذخیره کرده و فایل سالم را حذف می کند. بعد از اتمام فعالیت رمزگذاری نیز با استفاده از دستور shell پروسس tasklist.exe را جهت اجرای دستوراتی اجرا می کند. 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 سیستم عامل در قسمت Run جیستری ثبت می کند. شکل های زیر نمونه فایل های رمز شده، فایل راهنما و موارد دیگر را نشان می دهند.

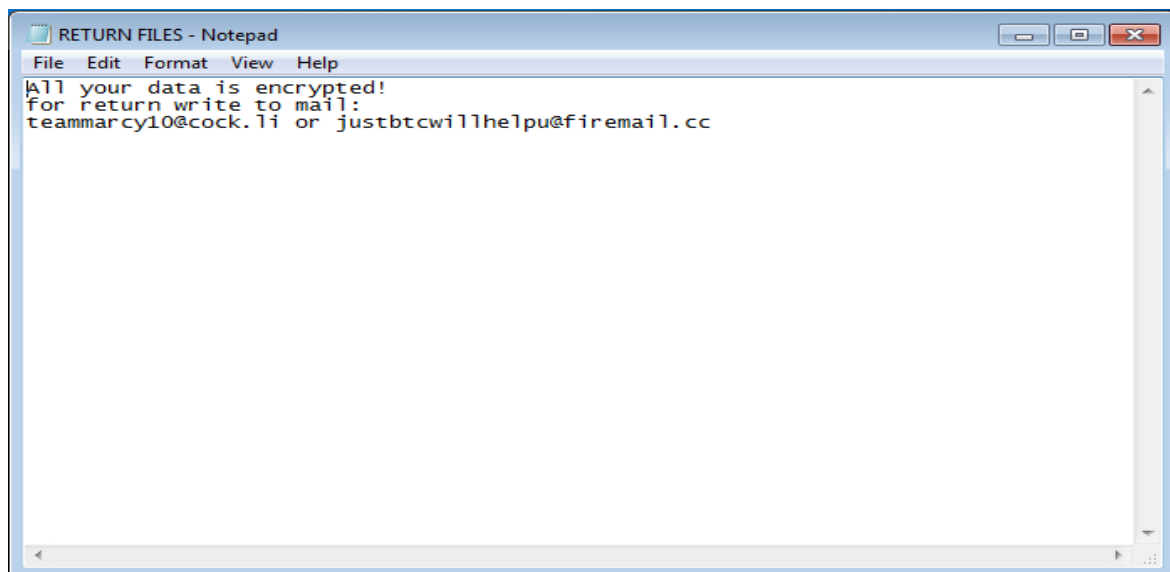




شکل ۴ نمونه فایل‌های رمز شده توسط باج افزار



شکل ۵ فایل راهنمای ایجاد شده توسط باج افزار



شکل ۶ فایل راهنمای ایجاد شده توسط باج افزار

## ۵ شرح تحلیل

گزارش زیر نتیجه تحلیل استاتیک و پویا در مورد فایل بدافزار در آزمایشگاه می باشد که از جعبه- سنی های آنلاین و آفلاین موجود استفاده شده است.

### ۱-۵ کنترل شبکه

با توجه به بررسی هایی که صورت گرفت هیچگونه فعالیتی مبنی بر فعالیت و ارتباط شبکه ای مشاهده نگردید.

### ۲-۵ رجیستری

جدول و شکل زیر آدرس رجیستری های ثبت شده در سیستم را توسط باج افزار نشان می دهد. همانطور که قبلا نیز ذکر گردید بعد از اتمام رمزگذاری فایل های سیستم، باج افزار فایل های راهنما را در آدرس Run رجیستری ثبت می کند تا این فایل های راهنما در هر بار اجرای سیستم عامل برای کاربر نشان داده شود.

جدول ۳ آدرس رجیستری ثبت شده توسط باج افزار

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

Image Path	Command	Time
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		12/2/2019 1:05 PM
C:\Users\Tahilgar\AppData\Roaming\C15006EACC	c:\users\tahilgar\appdata\roaming\c15006ea\retum files.bt	12/2/2019 1:05 PM
C:\Users\Tahilgar\AppData\Roaming\C15006EADD	c:\users\tahilgar\appdata\roaming\c15006ea\info.hta	12/2/2019 1:05 PM

شکل ۷ آدرس رجیستری ثبت شده توسط باج افزار

### ۳-۵ پروسسهای اجرا شده

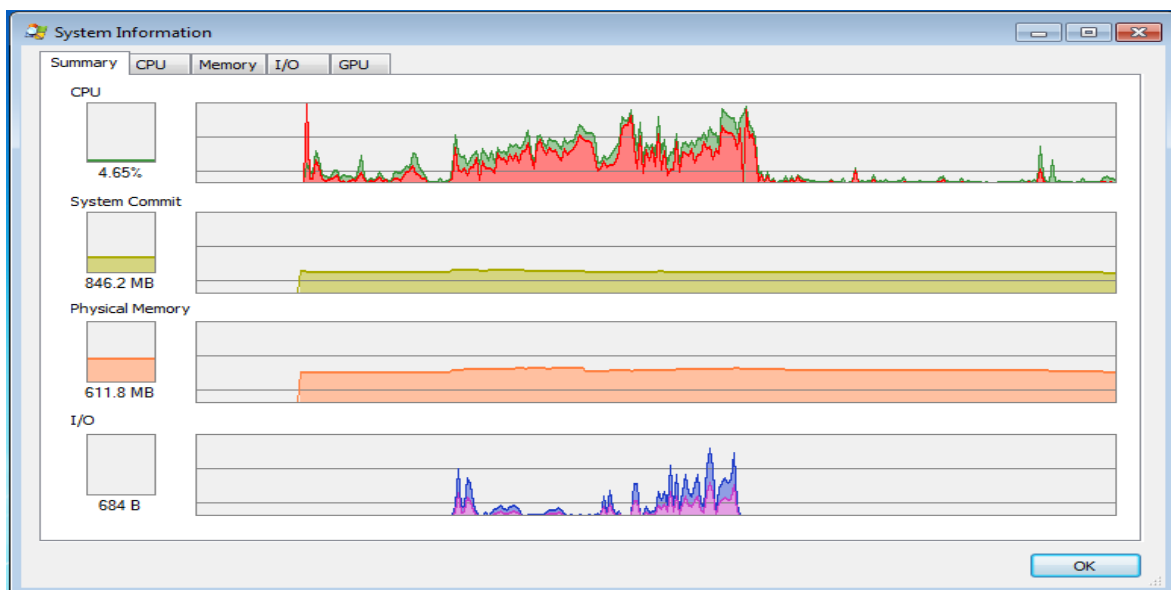
شکل زیر پروسسهای ایجاد شده توسط باج افزار را نشان می دهد. در این شکل مشاهده می گردد که با استفاده از tasklist دستوراتی را در سیستم اجرا می کند. سپس با استفاده از mshta فایل راهنما را ایجاد می کند.

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

شکل ۸ پروسسهای فعال و اجرا شده توسط فایل باج افزار

### ۴-۵ وضعیت منابع سیستم

شکل زیر وضعیت منابع سیستم را در زمانی نشان می دهد که باج افزار در حال فعالیت بوده و فایل های سیستمی را رمزگذاری می کند. با توجه به شکل مشاهده می گردد 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 باج افزار در سیستم

## ۵-۵ نمونه فایل رمز شده

نمونه فایل تست شده برای این باج افزار یک فایل pdf می باشد که ساختار باینری آن قبل و بعد از رمزگذاری بصورت شکل ۱۱ می باشد. بخش سمت راست مربوط به حالت رمز شده و بخش سمت چپ مربوط به حالت عادی فایل می باشد.

25 50 44 46 2D 31 2E 35 0A 25 F6 E4 FC DF 0A 31	%PDF-1.5.%endobj	00 02 79 03 7F 69 5A 7A D8 AA 49 32 28 35 29 EB	..y..1z20*I2(5)e
20 30 20 6F 62 6A 0A 3C 3C 0A 2F 54 79 70 65 20	0 obj.<<./Type	5F 76 0B 01 AB 65 A8 49 8B 2D 18 11 AF 02 FC F9	y..ue'I<.-.ü
2F 43 61 74 61 6C 6F 67 BA 2F 50 61 67 65 73 20	/Catalog/ Pages	01 A5 42 8E 9C B4 55 C2 A4 59 44 6A AF 39 49 52	.FBZe UA&Ydj;9IR
32)20 30 20 52 0A 2F 4C 61 6E 67 20 28 65 6E 2D	(2)0 R./Lang (en-	40 A9 32 E1 9E D9 54 02 01 EF 54 0A EC 56 90 36	@2aZt.IT.IV.6
55 53 29 0A 3E 3E 0A 65 6E 64 6F 62 6A 0A 33 20	US).>>.endobj.s	F2 12 8B 17 86 A7 61 11 9F 65 FE 38 44 43 AB 01	o.<.tga.Yep8DC&
30 20 6F 62 6A 0A 3C 3C 0A 2F 4D 6F 64 44 61 74	0 obj.<<./ModDat	8D 7B C8 88 76 DA 46 C2 E7 17 EB 92 1E 38 24 90	.(E*vUFaC.e'.89.
65 20 28 44 3A 32 30 31 36 30 35 31 33 31 31 32	e (D:20160513112	B6 B3 5F 68 22 C8 85 A9 05 71 2B 42 77 A0 62 17	q'.h"e...q+Bw b.
39 31 33 2B 30 33 27 30 30 27 29 0A 2F 54 69 74	913+03'00')./Titl	DD 15 46 4A 9D B9 60 7F 56 72 95 93 3B 50 D6 89	Y.FF.''.Vx'";Poh
6C 65 20 28 49 6E 74 65 72 6E 61 74 69 6F 6E 61	le (Internationa	BF 97 B3 CC B5 3B 9E 08 13 1E 2C 7F 69 B9 78 D4	;->Ïp;Z...;i,xÖ
6C 20 4A 6F 75 72 6E 61 6C 20 6F 66 20 49 6E 6E	l Journal of Int	23 04 45 CB 54 0C BB DA 67 78 EC 00 04 A4 EC 78	#.EET.»Ügxi..Hix
6F 76 61 74 69 76 65 29 0A 2F 43 72 65 61 74 6F	ovative)/Creat	F5 C6 D1 7F 23 F3 5A 28 1A 4B 10 75 39 44 FC B9	Ç&N.#öZ(.K.u9Dü'
72 20 3C 46 45 46 46 30 30 34 44 30 30 36 39 30	r <FEFF004D0069	DE 5B 43 6E A0 B5 4D 71 39 4C 9E E0 E9 09 70 57	BUCn pMq9I.Z&e.pW
30 36 33 30 30 37 32 30 30 36 46 30 30 37 33 30	0630072006F0073	33 DB C4 E9 96 19 42 FC 80 ED 50 D7 8B B2 4A 69	3Ü&e-.Bü&IP<<+Ji
30 36 46 30 30 36 36 30 30 37 34 30 30 41 45 30	06F0066007400AE	A5 C6 F3 F1 18 70 EB 8B AA DD 1B 23 63 45 4F E1	Y&ö&h.p&c.*Y.c&O&á
30 32 30 30 30 35 37 30 30 36 46 30 30 37 32 30	0200057006F0072	9D 2A ED 6B 0B 97 D0 EF FE 81 77 E2 08 DA 53 7C	*ik.->D&p.w'.DA 53 7C
30 36 34 30 30 32 30 30 30 33 32 30 30 33 30 30	064002000320030	C7 28 C0 E8 29 44 FD 88 88 8B A0 FF 66 47 23 B3	Ç(Ä&)Dy'<ç yf&#?
30 33 31 30 30 33 30 3E 0A 2F 41 75 74 68 6F 72	0310030>./Author	6F B5 D7 2A 16 A0 C3 47 85 CA BD F2 B4 3B 8C BD	o&u**..ÄG.&+ö';&#;
20 28 59 61 6E 20 53 48 49 29 0A 2F 43 72 65 61	(Yan SHI)./Cree	60 73 2C A6 0B C5 F0 55 39 D9 13 29 8A B2 C4 F1	's,;Ä&9Ü'.S*Äñ
74 69 6F 6E 44 61 74 65 20 28 44 3A 32 30 31 36	tionDate (D:2016	CS 47 B9 5F 37 9A 3E 79 F5 F6 6D 04 AA 93 EE 88	ÄG' 7&>y&ö&..*+i
30 35 31 33 31 31 32 37 35 37 2B 30 33 27 30 30	0513112757+03'00	DC AS DD A0 FA 28 54 49 52 BA 76 48 2C 6B 09 D5	ÜTY'ü(TIR'vH,K.Ö
27 29 0A 2F 50 72 6F 64 75 63 65 72 20 3C 46 45	')../Producer <FE	AB B5 80 7A 08 8D 53 67 41 C2 DB 87 85 A2 1D 37	&#pEz...Sg&Ü&..c.7
46 46 30 30 34 44 30 30 36 39 30 30 36 33 30 30	FF004D006900630	5F 4D B5 60 06 BF D5 8D 47 F6 B4 A5 D6 73 57 8E	'Mu'.&ö.G&'Y&ö&W&Z
37 32 30 30 36 46 30 30 37 33 30 30 36 46 30 30	72006F0073006F0	B1 AB 62 18 15 41 68 73 BD 33 2C 0F 2C 24 A0 06	I&e..A&#&3,,H..
36 36 30 30 37 34 30 30 41 45 30 30 32 30 30 30	66007400AE00200	E0 74 07 45 21 EA B7 FE E5 38 8E 43 FB AB C2 83	at.EI&e-p&ö&ö&ö&f
35 37 30 30 36 46 30 30 37 32 30 30 36 34 30 30	57006F007200640	A7 ED 69 7C B0 5E DB 99 23 43 2A 2D B2 A1 7A 69	sil '°~ü#&C'~';zi
32 30 30 30 33 32 30 30 33 30 30 33 31 30 30	200032003000310	F1 C6 60 77 63 6C EA 51 81 DD 8C EF 87 B3 1F A8	ñ&e'w&ö&Q.Y&ö+&..'
33 30 3E 0A 2F 72 67 69 64 20 28 50 42 3A 33 30	30>./rgid (PB:30	DF 2F 7E 64 69 07 DB 6D A4 AC B4 42 1E 71 8A 1B	B/-di.Üm&~'B.g&#.
34 33 34 31 31 33 39 5F 41 53 3A 34 37 36 37 34	4341139 AS:47674	88 97 8B 60 B3 6C FF CA 2B E4 3C 30 E1 DB 1E CF	~<~'ly&+&C&ö&Ü.İ
38 36 35 32 35 31 39 34 32 35 40 31 34 39 30 36	8652519425@14906	48 1D C4 58 25 13 70 CE 4E CE B7 D0 23 67 9C 0E	H.A&X&e.p&N&I'&#&#&
37 37 31 34 34 38 37 30 29 0A 3E 3E 0A 65 6E 64	77144870).>>.end	AB A0 91 EB DB 85 D1 87 57 F8 89 00 36 CF 7A 49	< 'eÜ..N&W&ö&.6IzI
6F 62 6A 0A 32 20 30 6F 62 6A 0A 3C 3C 0A 2F	obj.<2 0 obj.<<./	15 74 A4 C2 D7 63 57 8B 71 A0 BB 6A 64 EA FE BE	..t&#&C&W&ç »jd&#p&#
54 79 70 65 20 2F 50 61 67 65 73 0A 2F 43 6F 75	Type /Pages./Cov	F2 3C 9E 44 16 63 1B 39 D4 89 44 28 03 18 DB 5F	ö&C&Z&.c.9&ö&D(.(.Ü
6E 74 20 36 0A 2F 4B 69 64 73 20 5B 34 20 30 20	nt 6./Kids [4 0	83 10 24 98 94 5A 9C AC CC 57 A2 5E 9B 41 0C 88	f.&#''Z&~&I&ö&'&A..
52 20 35 20 30 20 52 20 36 20 30 20 52 20 37 20	R 5 0 R 6 0 R 7	B2 17 A6 2D 9F 9C 33 F7 D0 A1 3A EE 0D FC 25 84	'..-Y&ö&=Dj;:ä.u&#,,
30 20 52 20 38 20 30 20 52 20 39 20 30 20 52 5D	0 R 8 0 R 9 0 R	A1 0F 4D 86 BE 8B 9D EC AD 1E 83 02 1A D5 BF DA	;.M*#&.l.-f.ö&Ü
0A 3E 3E 0A 65 6E 64 6F 62 6A 0A 34 20 30 20 6F	.>>.endobj.4 0	2A BC 28 B0 D9 26 35 B1 3C 27 14 FC CD 29 1A 1C	*#(°U&ö&±< .üI'..
62 6A 0A 3C 3C 0A 2F 54 79 70 65 20 2F 50 61 67	bj.<<./Type /Pag	96 FD 26 2D 8C 77 27 D2 F2 E5 26 EE CB 2F 05 B0	-y&~&W'Ö&ö&eI&E/.'°
65 0A 2F 52 65 73 6F 75 72 63 65 73 20 3C 3C 0A	e./Resources <<	2C 92 4D CF F0 3F 27 AE 47 3C 13 0D 9A 55 64 CC	'M&I&?°@G<..SüDI
2F 50 72 6F 63 53 65 74 73 20 5B 2F 50 44 46 20	/ProcSets [/PDF	A4 18 55 88 36 77 5E 26 E9 54 9C C5 0E 93 F7 AE	H.U'°w'&eI&ö&A..°&#

شکل ۱۰ ساختار باینری فایل pdf در حالت عادی و رمز شده

شکل زیر نیز تفاوت باینری دو فایل را در حالت های قبل و بعد از عملیات رمزگذاری نشان می دهد. با توجه به شکل مشاهده می گردد تمام ساختار فایل رمز شده و هیچ نقطه مشترکی وجود ندارد.

Result	Address A	Size A	Address B	Size B
Difference	0h	54E90h	0h	55080h

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

## ۶ توصیه های امنیتی برای پیشگیری

- گرفتن فایل پشتیبان بصورت دوره ای از فایل های سیستم و ذخیره آن در محل دیگر
- استفاده از آنتی ویروس 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 رمز عبور قوی بر روی درایوهای سیستم
- استفاده از سیستم‌عامل جدید و بروزرسانی شده
- بروزرسانی مداوم سیستم‌عامل
- پیکربندی مناسب پروتکل‌های مورد استفاده در شبکه متناسب با محیط کار