بسمه تعالی

گزارش تحلیلی باج افزار pysa

Pysa Ransomware

فهرست مطالب

۲) معرفی باج افزار Pysa

باج افزار pysa به عنوان جدیدترین باج افزار شناسایی شده است. محققان امنیت سایبری متوجه شدند این تهدید متعلق به خانواده Mespinoza Ransomware می باشد. اکثر باج افزارها به شیوه ای یکسان عمل میکنند آنها به یک سیستم هدفمند نفوذ می کنند، داده ها را رمزنگاری می کنند و سپس از قربانی می خواهند برای دریافت کلید رمزنگشایی باج پرداخت کنند . که قرار هست پرونده های اسیب دیده را باز کنند. بیشتر اوقات، نویسندگان باج افزار مبلغ سنگین و به ندرت چندین صد دلار درخواست می کنند.

ابن باج افزار فایل های رمزنگاری شده را غیر قابل دسترس می کند و حتی restore points و shadow copies را نیز حذف می کند تا کاربر نتواند فایل ها را بازیابی کند. کاربران انکلیسی زبان را هدف قرار داده است و با این حال، تقریبا در کل کره زمین منتشر شده است. این ویروس از اول دسامبر ۲۰۱۹ فعال شد و تنها در مدت چند روز موفق به نفوذ بسیار از رایانه های کشورهای مختلف شد.

۳) پیامدهای منفی بدافزار Pysa

- قفل شدن کلیه ی پرونده های کاربران
- از دسترس خارج شدن کلیه ی پرونده های مهم و حساس
- درخواست پرداخت بین کویین در ازای ارسال کد رمزگشایی
- خسارت های مالی فراوان برای بازگشت اطلاعات و حذف باج افزار
- عدم تضمین بازگشت اطلاعات بعد از پرداخت باج درخواستی

۴) بررسی فنی باج افزار

این بخش اطلاعات کلی و فنی باج افزار را نشان می دهد که شامل بخش های تشکیل دهنده، section ها را ااایه کرده است.

- مشخصات فایل آلوده

جدول ۱:اطلاعات کلی باج افزار Pysa

نام باج افزار	Pysa Ransomware
حجم فایل	516608 (bytes)
نوع باج افزار	Crypto Ransomware
هشMD5	E9454A2FF16897E177D8A11083850EC7
هشSHA1	6B6855931E69D27F5F2E2D828FBEB4DB91688996
هشSHA256	E9662B468135F758A9487A1BE50159EF57F3050B753DE2915763B4ED78839EAD
خانواده	Mespinoza
زمان کامپایل	Sun Jan 19 03:28:47 2020
نوع فایل	Executable, 32 bit

- **مشخصات section ها**

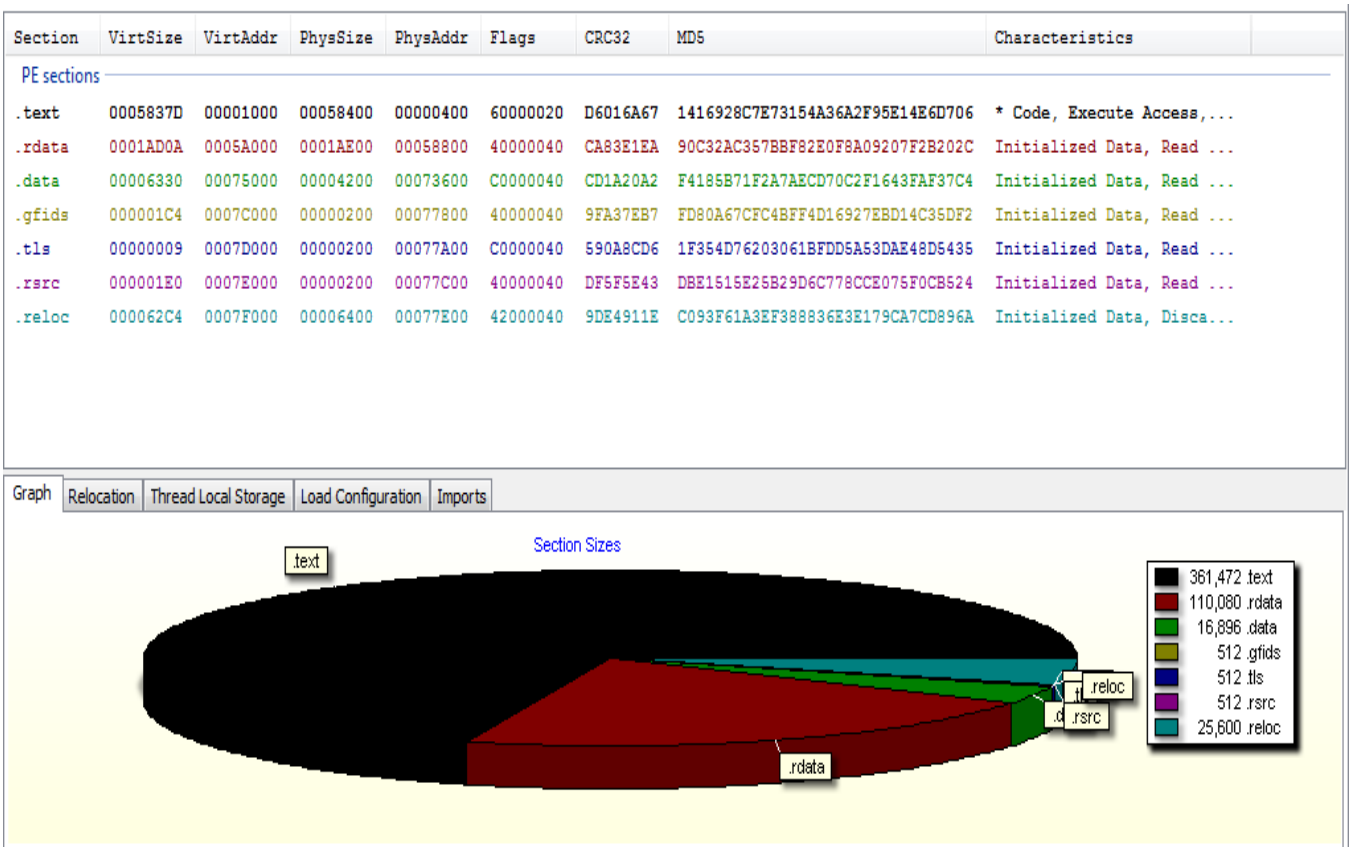
اطلاعات section ها نیز در شکل ۱ نشان داده شده است که از ۷ بخش.text, .data, .rdata, .gfids, .tls, .rsrc و .reloc تشکیل شده است.

۵) عملکرد باج افزار

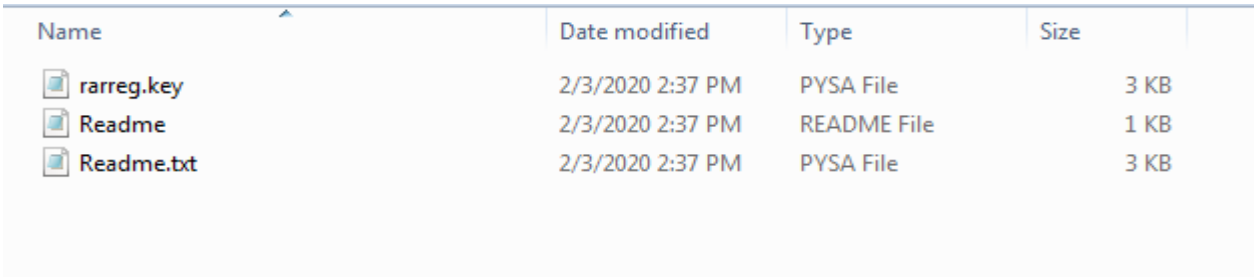
این باج افزار در ابتدا فایل اجرایی اولیه خود را پاک می کند و به یک فایل Readme تبدیل می کند و پس از آن کلیه ی فایل های قربانی بر روی سیستم را رمزنگاری می کند و پسوند .pysa را به آنها اضافه نموده تا غیر قابل دسترس باشند. همچنین فایل تکست با نام Readme را درون کلیه ی فولدرهای سیستم قربانی می سازد

که درون این فایل نحوه ی ارتباط با مهاجم و سوالات رایج قربانی را نوشته است تا قربانی متوجه شود پس از آلوده شدن، چگونه باید برخورد کند. نمونه ی این فایل تکست در شکل ۲ نشان داده شده است.

قابل ذکر است که کلیه ی اطلاعات و ارتباط با کاربران تنها به زبان انگلیسی ارائه شده است و هیچ گونه زبان دیگری قابل پشتیبانی نیست.



شکل ۱: PE Section



شکل ۲: فایل read me

این باج افزار زمینه ی سیستم را عوض نخواهد کرد ولی پس از re-start شدن سیستم و قبل از بالا آمدن سیستم قربانی صفحه ی ای مانند شکل ۳ را نشان خواهد داد. که علاوه بر بیان اسم خود، نحوه ی ارتباط با مهاجم را نشان داده است.

شکل ۳: پیام نمایشی باج افزار

- **فولدرهای اضافه شده در سیستم**

C:\Users\n.soltani\AppData\Local\Microsoft\Windows\History\History.IE5\MSHist012020021620200217

- **فایلهای تغییر داده شده**

جدول2 : modified files

C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.chk
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSS.log
C:\ProgramData\Microsoft\Search\Data\Applications\Windows\MSStmp.log
C:\ProgramData\VMware\VMware VGAuth\logfile.txt.0
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS.chk
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSS.log
C:\Users\All Users\Microsoft\Search\Data\Applications\Windows\MSStmp.log
C:\Users\All Users\VMware\VMware VGAuth\logfile.txt.0
C:\Users\n.soltani\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\n.soltani\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\n.soltani\AppData\Local\Microsoft\Windows\UsrClass.dat
C:\Users\n.soltani\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1
C:\Users\n.soltani\AppData\Local\Temp\nsk6087.tmp
C:\Users\n.soltani\AppData\Local\Temp\nsq6B03.tmp
C:\Users\n.soltani\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\n.soltani\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\1b4dd67f29cb1962.automaticDestinations-ms
C:\Users\n.soltani\NTUSER.DAT
C:\Users\n.soltani\ntuser.dat.LOG1
C:\Windows\System32\config\SOFTWARE

C:\Windows\System32\config\SOFTWARE.LOG1
C:\Windows\System32\config\SYSTEM
C:\Windows\System32\config\SYSTEM.LOG1

- **فایلهای رمزنگاری شده**

این باج افزار فایلهایی با پسوند های مختلف که در جدول ۳ لیست شده را رمزنگاری می نماید.

جدول ۳: پسوند فایلهای رمزنگاری شونده

.doc	.xlsx	.docx	.xls
.pdf	.frm	.mdf	.myd
.bak	.trc	.sql	.sdf
.pst	.qic	.vhdx	.bkf
.dwg	.rar	.zip	.mdb
.text	.sys	.dll	.exe
.ndf	.mwb	.db3	.tls
.backupdb	.bac	.acr	.wrk
.fbk	.bup	.bkup	.bck
.avhdx	.vfd	.spf	.mig
.sqb	.pbf	.vmrs	.vmcx
.vrb	.vbm	.vbk	.tis
.pla	.dsd	.cad	.win
			.pln

- **توابع و کتابخانه های باج افزار**

این باج افزار شامل کتابخانه ها و توابع نشان داده شده در شکل ٤ و ٥ است که تعداد کتابخانه ها و توابع برای یک فایل اجرایی سالم غیر قابل قبول می باشد.

library (4)	blacklist (0)	type (1)	imports (102)	description
kernel32.dll	-	implicit	93	Windows NT BASE API Client DLL
user32.dll	-	implicit	2	Multi-User Windows USER API Client DLL
advapi32.dll	-	implicit	6	Advanced Windows 32 Base API
shell32.dll	-	implicit	1	Windows Shell Common Dll

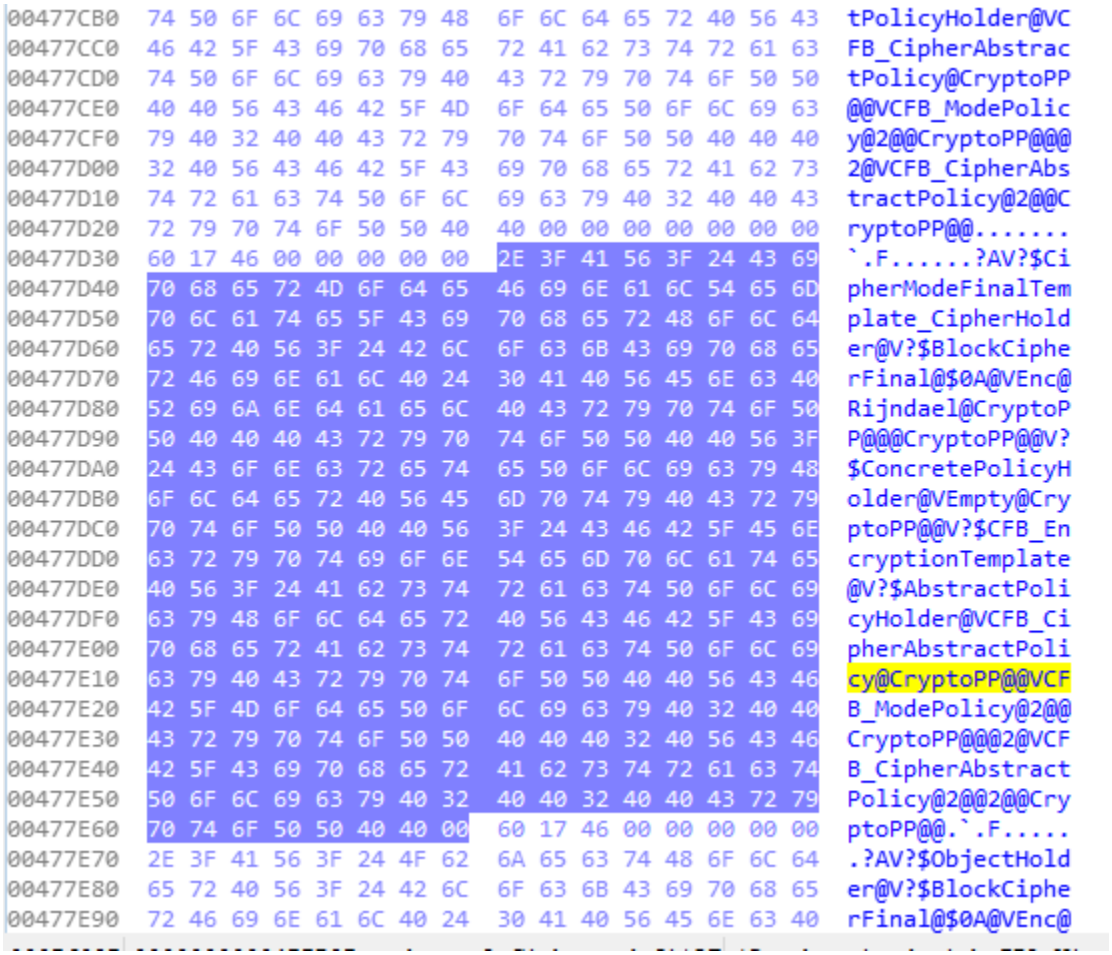
شکل ۴: کتابخانه های باج افزار Pysa

name (102)	group (12)	anonymous (0)	type (1)	blacklist (30)	anti-debug (0)	u
GetLogicalDriveStringsW	23	-	implicit	x	-	
GetModuleFileNameA	21	-	implicit	x	-	
GetModuleHandleExW	21	-	implicit	x	-	
FreeConsole	20	-	implicit	x	-	
ReadConsoleW	20	-	implicit	x	-	
WriteConsoleW	20	-	implicit	x	-	
QueryPerformanceCounter	19	-	implicit	x	-	
RaiseException	18	-	implicit	x	-	
QueryPerformanceFrequency	7	-	implicit	x	-	
InterlockedPushEntrySList	7	-	implicit	x	-	
FindFirstFileW	6	-	implicit	x	-	
FindNextFileW	6	-	implicit	x	-	
FindClose	6	-	implicit	x	-	
MoveFileExW	6	-	implicit	x	-	
FindFirstFileExA	6	-	implicit	x	-	
FindNextFileA	6	-	implicit	x	-	
CryptReleaseContext	4	-	implicit	x	-	
CryptAcquireContextA	4	-	implicit	x	-	
CryptGenRandom	4	-	implicit	x	-	
CreateThread	2	-	implicit	x	-	
GetCurrentProcess	2	-	implicit	x	-	
TerminateProcess	2	-	implicit	x	-	
GetCurrentProcessId	2	-	implicit	x	-	
GetCurrentThreadId	2	-	implicit	x	-	
GetEnvironmentStringsW	2	-	implicit	x	-	
FreeEnvironmentStringsW	2	-	implicit	x	-	

شکل ۵: توابع باج افزار Pysa

- **وجود رشته های مشکوک**

در بررسی کد این باج افزار، رشته های نامشکوک دیده شده است که نشان می دهد محتوای این فایل آلوده می باشد و حاوی باج افزار است که این رشته های در شکل ٦ نشان داده شده است.



شکل ۶: رشته های مشکوک

- **تحلیل ترافیک شبکه**

پس از بررسی ترافیک شبکه ضبط شده پس از اجرای باج افزار و همچنین بررسی نتایج سندباکس های آنلاین، موردی در ارتباط با این باج افزار مشاهده نشد.

۶) نتایج بررسی آنتی ویروس های مختلف

این باج افزار نیز توسط آنتی ویروس های مختلف نشان داده شده در شکل ۷ با اسم های محتلف به عنوان باج افزار نیز شناسایی می شود. https://www.virustotal.com/

engine (68)	detection (47)	date (dd.mm.yyyy)	age (days)
MicroWorld-eScan	Trojan.GenericKD.32976398	03.02.2020	1
FireEye	Trojan.GenericKD.32976398	03.02.2020	1
CAT-QuickHeal	Trojanransom.Encoder	03.02.2020	1
McAfee	RDN/Ransom	03.02.2020	1
K7AntiVirus	Trojan (0055d79d1)	03.02.2020	1
Alibaba	Ransom:Win32/generic.ali2000010	27.05.2019	253
K7GW	Trojan (0055d79d1)	03.02.2020	1
CrowdStrike	win/malicious_confidence_60% (W)	02.07.2019	217
TrendMicro	Ransom.Win32.FILECODER.THABCBO	03.02.2020	1
BitDefenderTheta	Gen:NN.ZexaF.34084.FCW@aymTYqhi	20.01.2020	15
Cyren	W32/Ransom.YOGI-7486	03.02.2020	1
Symantec	Downloader	02.02.2020	2
APEX	Malicious	01.02.2020	3
Paloalto	generic.ml	03.02.2020	1
Kaspersky	HEUR:Trojan-Ransom.Win32.Encoder.gen	03.02.2020	1
BitDefender	Trojan.GenericKD.32976398	03.02.2020	1
NANO-Antivirus	Trojan.Win32.Encoder.gwskjy	03.02.2020	1
AegisLab	Trojan.Win32.Encoder.j!c	03.02.2020	1
Tencent	Win32.Trojan.Filecoder.Akev	03.02.2020	1
Ad-Aware	Trojan.GenericKD.32976398	03.02.2020	1
Sophos	Mal/Generic-S	03.02.2020	1
Comodo	Malware@#2vl69pgpxj24q	03.02.2020	1
F-Secure	Trojan.TR/FileCoder.vqktg	03.02.2020	1
DrWeb	Trojan.Encoder.30815	03.02.2020	1
Zillya	Trojan.Filecoder.Win32.12097	01.02.2020	3
McAfee-GW-Edition	RDN/Ransom	03.02.2020	1
Trapmine	malicious.high.ml.score	23.01.2020	12
Emsisoft	Trojan.Ransom (A)	03.02.2020	1

شکل ۷: نتایج بررسی آنتی ویروس های مختلف

۷) توصیه های امنیتی برای پیشگیری

- برنامه های آگاهی و اموزشی را اجرا کنید. از آنجا که کاربران نهایی اهداف هستند، کارمندان و افراد باید از تهدیدهای باج افزارها و نحوه تحویل آن مطلع باشند.
- فیلترهای Spam قوی را فعال کنید تا ایمیل های فیشینگ از رسیدن به کاربران نهایی جلوگیری کنند و ایمیل های ورودی را احراز هویت کنند. از فن آوری هایی مانند گزارش خط مشی فرستنده(SPF)[1] ، گزارش های تایید هویت دامنه (DMARC)[2]و DomainKeys Identified Mail (DKIM) برای جلوگیری از جعل ایمیل استفاده کنید.

[1] Sender Policy Framework
[2] Domain Message Authentication Reporting and Conformance

- تمامی ایمیل های دریافتی و خروجی را برای شناسایی تهدیدها و فیلتر کردن فایل های اجرایی از رسیدن به کاربران نهایی اسکن کنید.
- پیکربندی فایروال ها برای جلوگیری از دسترسی به آدرس های مخرب IP شناخته شده است.
- سیستم عامل ها، نرم افزارها و فایروال های روی سیستم را پچ[3] کنید. توجه داشته باشید که با یک نرم افزار مدیریت پچ متمرکز این کار را انجام دهید.
- برنامه های ضد ویروس و ضد تروجان را برای انجام اسکن منظم به طور خودکار تنظیم کنید.
- مدیریت استفاده از حساب های ممتاز بر اساس اصل حداقل امتیاز: هیچ کاربر نباید دسترسی اداری را مجاز دانسته، مگر اینکه مطلقا مورد نیاز باشد و کسانی که نیاز به حساب کاربری مدیر دارند باید از آنها در صورت لزوم استفاده کنند.
- اسکریپت های ماکرو را از فایل های اداری ارسال شده از طریق ایمیل غیرفعال کنید .با استفاده از نرم افزار Office Viewerبرای باز کردن فایل های مایکروسافت آفیس از طریق ایمیل به جای برنامه های کاربردی full office suite استفاده کنید.
- پیاده سازی سیاست های محدودیت نرم افزار (SRP)[4] یا سایر کنترل ها برای جلوگیری از اجرای برنامه ها از مکان های معمول باج افزار ، مانند پوشه های موقتی که از مرورگرهای محبوب و یا برنامه های فشرده سازی / آزاد شده از فشردگی، از جمله پوشه AppData / LocalAppData پشتیبانی می کند.
- در صورت عدم استفاده از پروتکل از راه دور دسکتاپ (RDP)[5] ،آن راغیرفعال کنید.
- استفاده از برنامه لیست سفید ، که تنها به سیستم اجازه می دهد برنامه های شناخته شده و مجاز توسط سیاست امنیتی را اجرا کند.
- محیط های سیستم عامل و یا برنامه های خاص را در یک محیط مجازی اجرا کنید.

http://malwarewarrior.com/how-to-remove-pysa-ransomware-and-decrypt-pysa-files/

[3] Patch
[4] Software Restriction Policies
[5] Remote Desktop protocol