باسمه تعالی

تحلیل فنی باج‌افزار Dharma (.cmb)

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از ادامه فعالیت باج‌افزار Dharma حکایت دارد. این باج‌افزار که یکی از شایع‌ترین باج‌افزارهای سطح کشور است، تاکنون به چندین پسوند مختلف منتشر شده است و قربانیان زیادی را مجبور به پرداخت باج کرده است که دلیل آن غیرقابل رمزگشایی بودن فایل‌ها پس از رمزگذاری توسط این باج‌افزار است. در این گزارش به نمونه جدیدی از این باج‌افزار و با پسوند جدید می‌پردازیم.

در این نسخه باج‌افزار، پسوند کامل اضافه شده به فایل‌های رمزگذاری شده از الگوی زیر پیروی می‌کند :

id-<id>.[<email>].cmb

مثال:

id-٧٢٤٤٠BCB.[paymentbtc@firemail.cc].cmb

مشخصات فایل اجرایی :

نام فایل	Sample_٥b٦d٣c٤٧b٨ebb٥٠a٦١٣٠٧٩٤d.exe
MD٥	d٥٠f٦٩f٠d٣a٧٣c٠a٥٨d٢ad٠٨aedac١c٨
SHA-١	c٢٥ff١bb٢ea٣e٠٨٠٤ab٣f٣٧٠ad٢٨٧٧b٠b٧c٥٦٩٠٣
SHA-٢٥٦	c٢ab٢٨٩cbd٢٥٧٣٥٧٢c٣٩cac٣f٢٣٤d٧٧fdf٧٦٩e٤٨a١٧١٥a١٤feddaea٨ae٩d٩٧٠٢
اندازه فایل	٩٢.٥ KB
کامپایلر	نامشخص (احتمالا Microsoft Visual Studio)

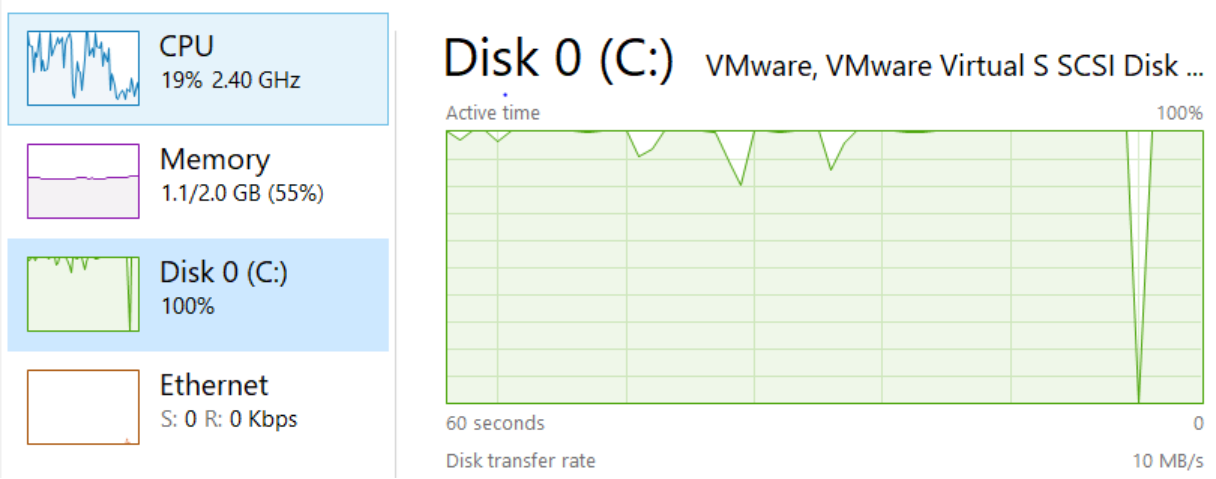
فایل اجرایی این باج‌افزار دارای سه بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	٥.٩٧	٤٠٩٦	٣٩٩٧٣	٤٠٤٤٨
.rdata	٧.٧٩	٤٥٠٥٦	٩٧٨٢	٩٧٨٢
.data	٧.٩٨	٥٧٣٤٤	٤٣٧٣٣	٤٣٠٠٨

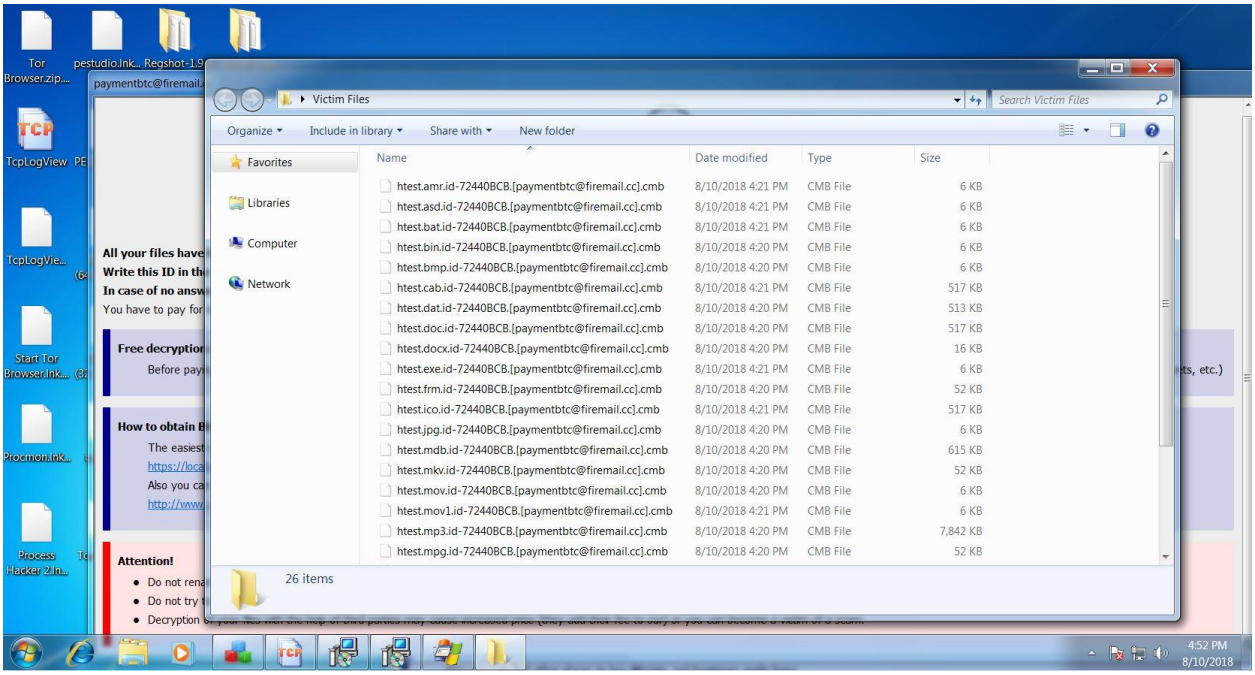
تحلیل پویا :

برای بررسی عمیق‌تر این باج‌افزار، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. فرآیند اجرای این باج‌افزار بسیار ساده می‌باشد. پس از ورود به سیستم (غالباً از طریق سرویس ریموت دسکتاپ) و بررسی محیط آن اقدام به رمزگذاری فایل ها با استفاده از الگوریتم رمزنگاری خود می کند. با توجه به گستردگی تنوع فایل‌های رمز شده، احتمالا باج‌افزار به دنبال پسوند خاصی نبوده و صرفاً چند مورد استثنا را در فرآیند رمزگذاری خود رعایت می‌کند. این استثناها می‌توانند پسوندهای خاصی باشند و یا دایرکتوری و نام فایل خاص!

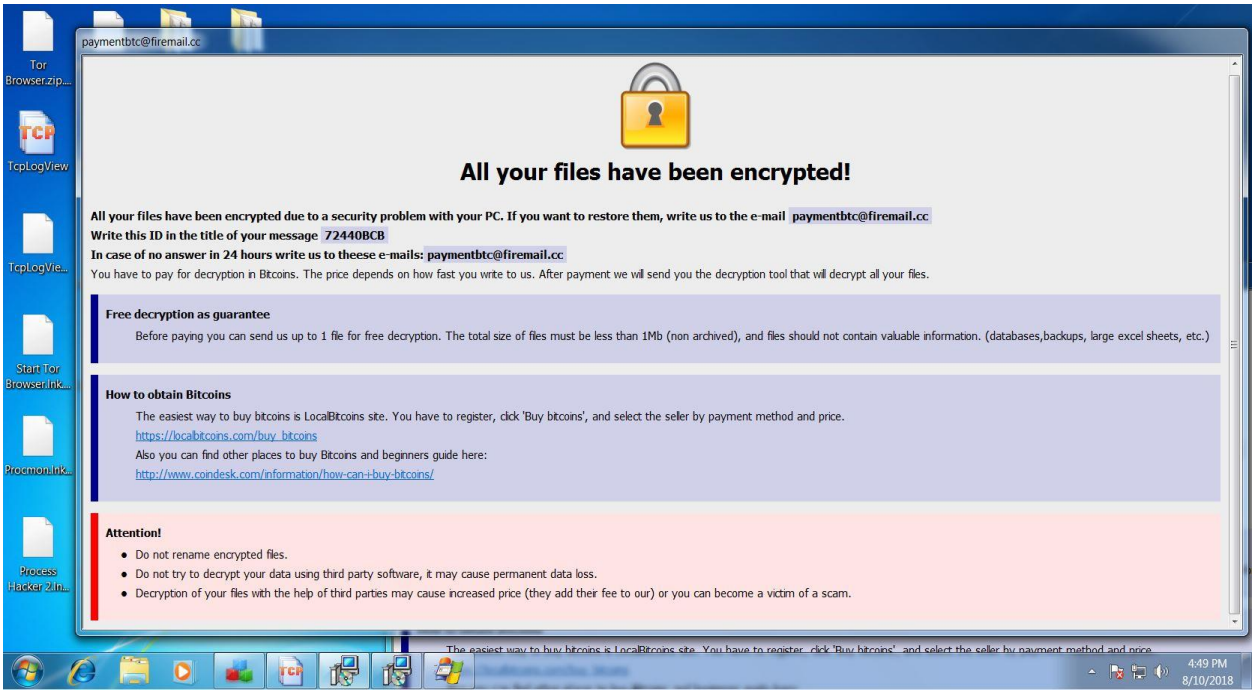
طبق بررسی‌های صورت گرفته، سرعت رمزگذاری فایل‌ها ارتباط مستقیمی با منابع سیستم قربانی دارد. در آزمایش‌های صورت گرفته، همانطور که در تصویر زیر نیز قابل مشاهده است، باج‌افزار Dharma (.cmb) بیش از همه، دیسک را درگیر می‌کند. لذا هرچه سرعت خواندن/نوشتن دیسک بالاتر باشد، فرآیند رمزگذاری نیز سریعتر اتفاق می افتد. اما بطور میانگین این مدت زمان برای دیسکی با ظرفیت ۱۰۰ گیگابایت بین ۲ تا ٤ دقیقه است.



پس از اتمام رمزگذاری ، فایل های سیستم قربانی به شکل زیر تغییر پیدا می کنند :



حال پیغام باج خواهی باج‌افزاربه صورت پنجره ای با عنوان paymentbtc@firemail.cc برای قربانی نمایش داده می شود:



در این پیغام که مشابه سایر نمونه‌های باج‌افزار Dharma می‌باشد، به این مطلب اشاره شده است که قربانی برای ارتباط با مهاجم باید شناسه خود را به آدرس ایمیل paymentbtc@firemail.cc ارسال کند و اگر طی ۲۴ ساعت پاسخی دریافت نشد، دوباره ایمیل ارسال شود. همچنین در ادامه پیام باج صراحتاً ذکر شده که مبلغ باج به واحد ارز دیجیتالی بیت‌کوین می‌باشد و میزان باج درخواستی نیز به سرعت قربانی در ارسال

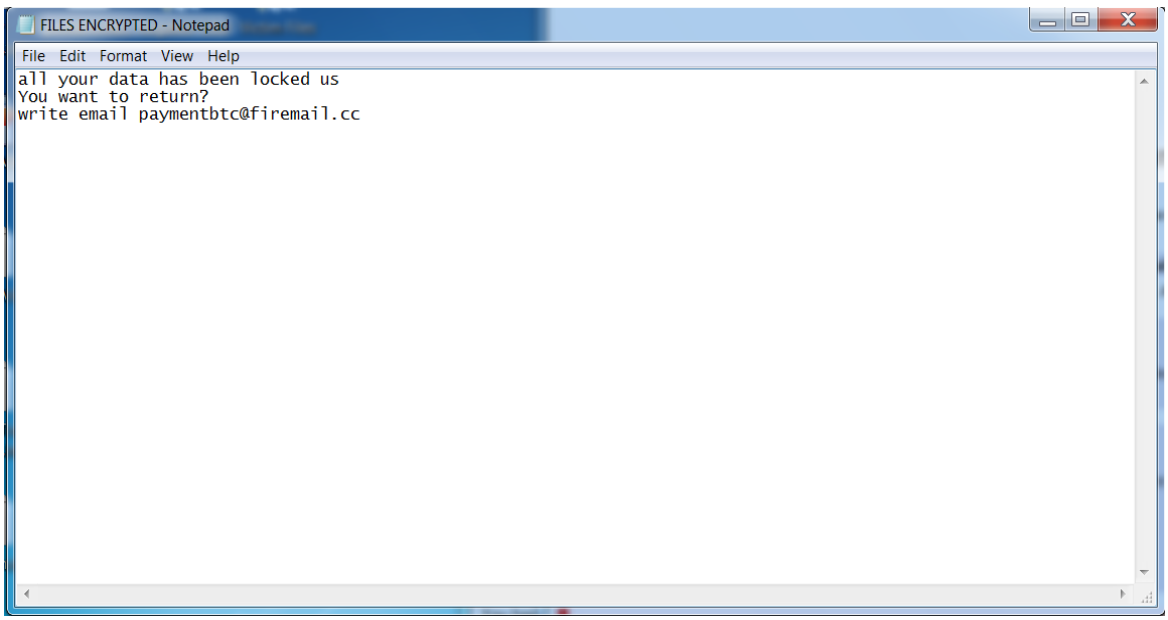
ایمیل بستگی خواهد داشت. با توجه به اینکه میزان باج درخواستی در پیام باج باج‌افزار Dharma موجود نیست به همین خاطر قربانی برای فهمیدن این موضوع الزاما باید با مهاجم از طریق ایمیل گفتگو کند. این موضوع بدین معنی است که هر چه دیرتر ایمیل به مهاجم ارسال شود، میزان باج درخواستی نیز افزایش خواهد یافت. در ادامه نیز پیشنهاد رمزگشایی یک فایل به عنوان تضمین به قربانی داده شده که فایل مذکور باید غیر فشرده و حجم آن کمتر از ۱ مگابایت بوده و دارای اطلاعات ارزشمند مانند پایگاه داده و پشتیبان و فایل‌های اکسل و مشابه این فایل‌های پر ارزش نباشد. در ادامه نیز سه هشدار به قربانی داده شده است که:

۱-نام فایل‌های رمز شده را تغییر ندهد.

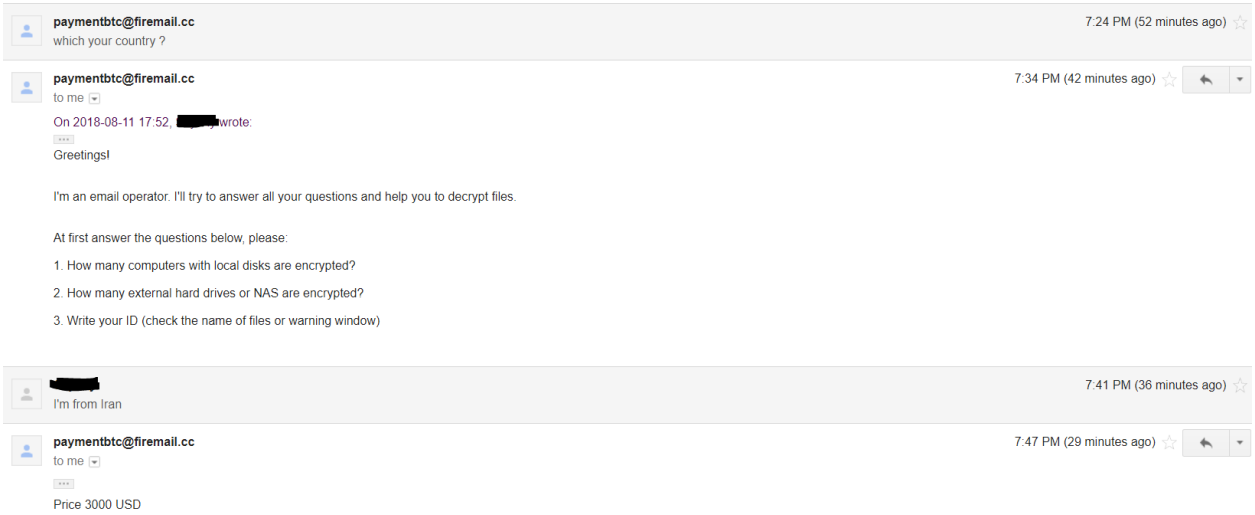
۲-به دنبال رمزگشایی فایل‌ها از طریق رمزگشاهای دیگر نباشد؛ چون امکان از دست رفتن فایل‌ها به صورت دائمی وجود دارد.

۳- با این توجیه که استفاده از رمزگشاهای دیگر صرفا هزینه بیشتری را بر قربانی تحمیل می‌کند، قربانی را از استفاده از رمزگشاهای دیگر بر حذر داشته است.

البته این پیغام، تنها پیغام باج خواهی باج‌افزار نیست ، پیغامی مشابه با عنوان FILES ENCRYPTED.txt در دسکتاپ قربانی و همچنین در چند دایرکتوری دیگر بخصوص درایو C ظاهر می شود. در تصویر زیر می توانید این پیغام را مشاهده کنید :



از آنجایی که مبلغ باج درخواستی در پیغام باج‌خواهی مشخص نشده است، پس از ارتباط گیری با مهاجم به صورت ناشناس، پیام زیر را دریافت نمودیم :



paymentbtc@firemail.cc 7:24 PM (52 minutes ago)
which your country ?

paymentbtc@firemail.cc 7:34 PM (42 minutes ago)
to me
On 2018-08-11 17:52, [redacted] wrote:
Greetings!

I'm an email operator. I'll try to answer all your questions and help you to decrypt files.

At first answer the questions below, please:
1. How many computers with local disks are encrypted?
2. How many external hard drives or NAS are encrypted?
3. Write your ID (check the name of files or warning window)

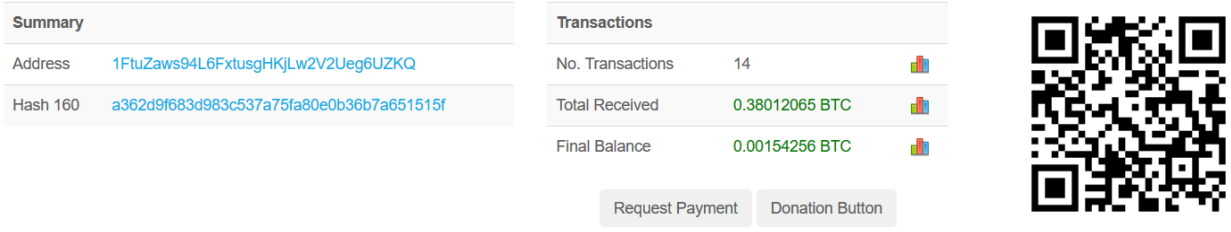
[redacted] 7:41 PM (36 minutes ago)
I'm from Iran

paymentbtc@firemail.cc 7:47 PM (29 minutes ago)
to me
Price 3000 USD

همانطور که قابل ملاحظه است، فرستنده خود را به عنوان اپراتور ایمیل معرفی نموده و مبلغ باج را ۳۰۰۰ دلار آمریکا (به واحد بیت کوین) تعیین نموده است که می بایست این مبلغ به کیف پول بیت‌کوین به آدرس ۱FtuZaws۹٤L٦FxtusgHKjLw۲V۲Ueg٦UZKQ منتقل گردد. در ادامه نیز سه پرسش مطرح کرده است:

۱. چه تعداد رایانه با دیسک های محلی رمز شده‌اند؟
۲. چه تعداد هارد اکسترنال یا NAS رمز شده‌اند؟
۳. شناسه قربانی چیست؟

طبق بررسی های صورت گرفته، این کیف پول تاکنون تعداد ١٤ تراکنش معادل ۰.۳۸۰۱۲۰٦٥ BTC داشته است.

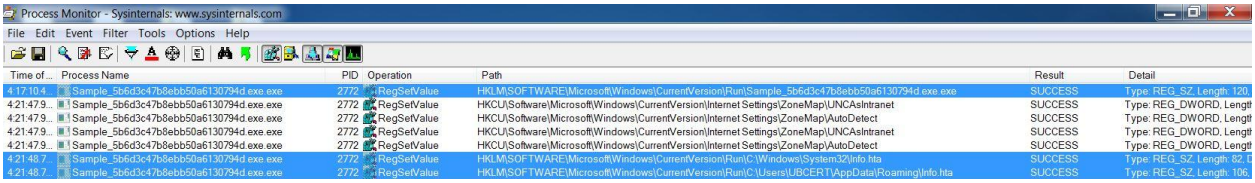


Summary	
Address	1FtuZaws94L6FxtusgHKjLw2V2Ueg6UZKQ
Hash 160	a362d9f683d983c537a75fa80e0b36b7a651515f

Transactions	
No. Transactions	14
Total Received	0.38012065 BTC
Final Balance	0.00154256 BTC

Request Payment | Donation Button

با توجه به بررسی‌های صورت گرفته از طریق ابزار Process Monitor، این باج‌افزار کلیدهای رجیستری زیر را تغییر می‌دهد که سه مورد آن مربوط به اجرای باج‌افزار پس از هر راه‌اندازی مجدد سیستم است:



همچنین باج‌افزار، فایل اجرایی خود به همراه یک فایل دیگر به نام info.hta را در مسیرهای زیر کپی می‌کند:

نام فایل	مسیر
Sample_٥b٦d٣c٤٧b٨ebb٥٠a٦١٣٠٧٩٤d.exe	C:\Windows\System٣٢ C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
Info.hta	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

فایل info.hta که مسئول نمایش پیغام باج‌خواهی بوده و در نسخه های قبلی Dharma نیز وجود داشت هم‌اکنون توسط نسخه به روز آنتی‌ویروس ESET با نام Win٣٢/Filecoder.Crysis قابل شناسایی است. در تصویر زیر محتوای این فایل نمایش داده شده است :

```
    <div>All your files have been encrypted!</div>
  </div>
    <div class='bold'>All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail <s
   <div class='bold'>In case of no answer in 24 hours write us to theese e-mails:<span class='mark'>paymentbtc@firemail.cc</span></div>

    <div>
    You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that
  </div>

  <div class='note info'>
      <div class='title'>Free decryption as guarantee</div>
    <ul>Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should
    </div>

    <div class='note info'>
      <div class='title'>How to obtain Bitcoins</div>
      <ul>
        The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and
          <br><a href='https://localbitcoins.com/buy_bitcoins'>https://localbitcoins.com/buy_bitcoins</a>
      <br> Also you can find other places to buy Bitcoins and beginners guide here:
          <br><a href='http://www.coindesk.com/information/how-can-i-buy-bitcoins/'>http://www.coindesk.com/information/how-can-i-buy-bitcoins/</a>
      </ul>
    </div>

    <div class='note alert'>
      <div class='title'>Attention!</div>
      <ul>
        <li>Do not rename encrypted files.</li>
```

تجربه نشان داده است که باج‌افزارهای خانواده Dharma معمولاً از طریق سرویس ریموت دسکتاپ (RDP) وارد سیستم قربانی شده و علاوه بر فایل‌های موجود در درایوهای محلی، محتویات پوشه های نگاشت شده در شبکه را نیز رمزگذاری می‌کنند. این نسخه باج‌افزار نیز از این قائده مستثنی نیست. لذا به تمام مدیران و راهبران شبکه، توصیه می‌گردد نسبت به امن‌سازی شبکه سازمان خصوصاً پروتکل RDP بر اساس استانداردهای موجود توجه و اهتمام ویژه داشته باشند.

تحلیل ایستا:

با توجه به مقادیر (٤D ٥A) یا MZ موجود در دو بایت ابتدایی این نمونه باج‌افزار، این فایل از نوع اجرایی و یا PE می‌باشد. از آنجا که فایل‌های PE به دلیل لزوم تبدیل کد سطح بالا به زبان ماشین از طریق کامپایلرها کامپایل می‌شوند، زمان کامپایل به صورت هگزادسیمال در Header این فایل‌ها موجود است. با توجه به اینکه این باج‌افزار در روز ۳ مارس ۲۰۱۷ کامپایل شده است، احتمالا طبق برنامه ریزی قبلی این نمونه باج‌افزار منتشر شده است.

مقادیر Import Table نیز به دلیل تعداد کم و همچنین وجود LoadLibrary و GetProcAddress و نیز وجود رشته‌های ASCII ناخوانای بسیار زیاد در فایل باینری این باج‌افزار، بدین معنی است که این باج‌افزار دارای خاصیت ضد مهندسی معکوس بوده و خواندن کد این باج‌افزار به راحتی مقدور نمی‌باشد.

طبق بررسی‌هایی که بر روی فایل‌های مختلف قبل و بعد از رمزگذاری انجام دادیم شاهد این بودیم که باج‌افزار Dharma (.cmb) بسته به نوع و حجم فایل‌ها، رفتار متفاوتی را از خود نشان می‌دهد و تمام فایل‌ها را به یک شکل رمزگذاری نمی‌کند. باج‌افزار برای سرعت بخشیدن به کار خود، در صورت مواجهه با فایل‌های با حجم زیاد، تنها قسمت‌هایی از فایل را به صورت متناوب رمزگذاری می‌کند. الگوی کلی رمزگذاری فایل‌ها توسط این باج‌افزار به شکل زیر است :

Type	Source	Count	Count	Target	Count	Count
Insert...	00000000	57	39	00000000	0	00
Match...	00000039	512	0200	00000000	512	0200
Insert...	00000239	473	01D9	00000200	0	00
Match...	00000412	512	0200	00000200	512	0200
Insert...	00000612	305	0131	00000400	0	00
Match...	00000743	256	0100	00000400	256	0100
Repla...	00000843	695293	000A9BF...	00000500	693246	000A93FE
Match...	000AA440	2054	0806	000A98FE	2054	0806
Insert...	000AAC...	78	4E	000AA104	0	00
Match...	000AAC...	2054	0806	000AA104	2054	0806
Repla...	000AB49...	164665	00028339	000AA9...	162618	00027B3A
Match...	000D37...	2054	0806	000D2444	2054	0806
Insert...	000D3F...	78	4E	000D2C...	0	00
Match...	000D4027	2054	0806	000D2C...	2054	0806
Repla...	000D482...	123341	0001E1CD	000D3450	122488	0001DE78
Match...	000F29FA	41	29	000F12C8	41	29
Repla...	000F2A23	1791	06FF	000F12F1	3453	0D7D
Match...	000F3122	35	23	000F206E	35	23
Repla...	000F3145	1736	06C8	000F2091	1626	065A
Match...	000F380D	40	28	000F26EB	40	28
Repla...	000F3835	5415	1527	000F2713	4003	0FA3
Match...	000F4D5C	55	37	000F36B6	55	37
Repla...	000F4D93	25286	62C6	000F36ED	23362	5B42
Match...	000FB059	37	25	000F922F	37	25
Repla...	000FB07E	9115	239B	000F9254	7110	1BC6
Match...	000FD419	41	29	000FAE1A	41	29
Repla...	000FD442	17368	43D8	000FAE43	17759	455F
Match...	0010181A	33	21	000FF3A2	33	21
Repla...	0010183B	4444	115C	000FF3C3	4832	12E0
Match...	00102997	40	28	001006A3	40	28
Repla...	001029BF	8878	22AE	001006CB	8961	2301
Match...	00104C6D	40	28	001029CC	40	28

بررسی‌های صورت گرفته نشان می‌دهد که باج‌افزار Dharma (.cmb) پس از اجرا، فرایندهای زیر را ایجاد می‌کند :

- Sample_5b6d3c47b8ebb50a6130794d.exe
  - cmd.exe "C:\Windows\system32\cmd.exe"
    - mode.com
    - vssadmin.exe vssadmin delete shadows /all /quiet

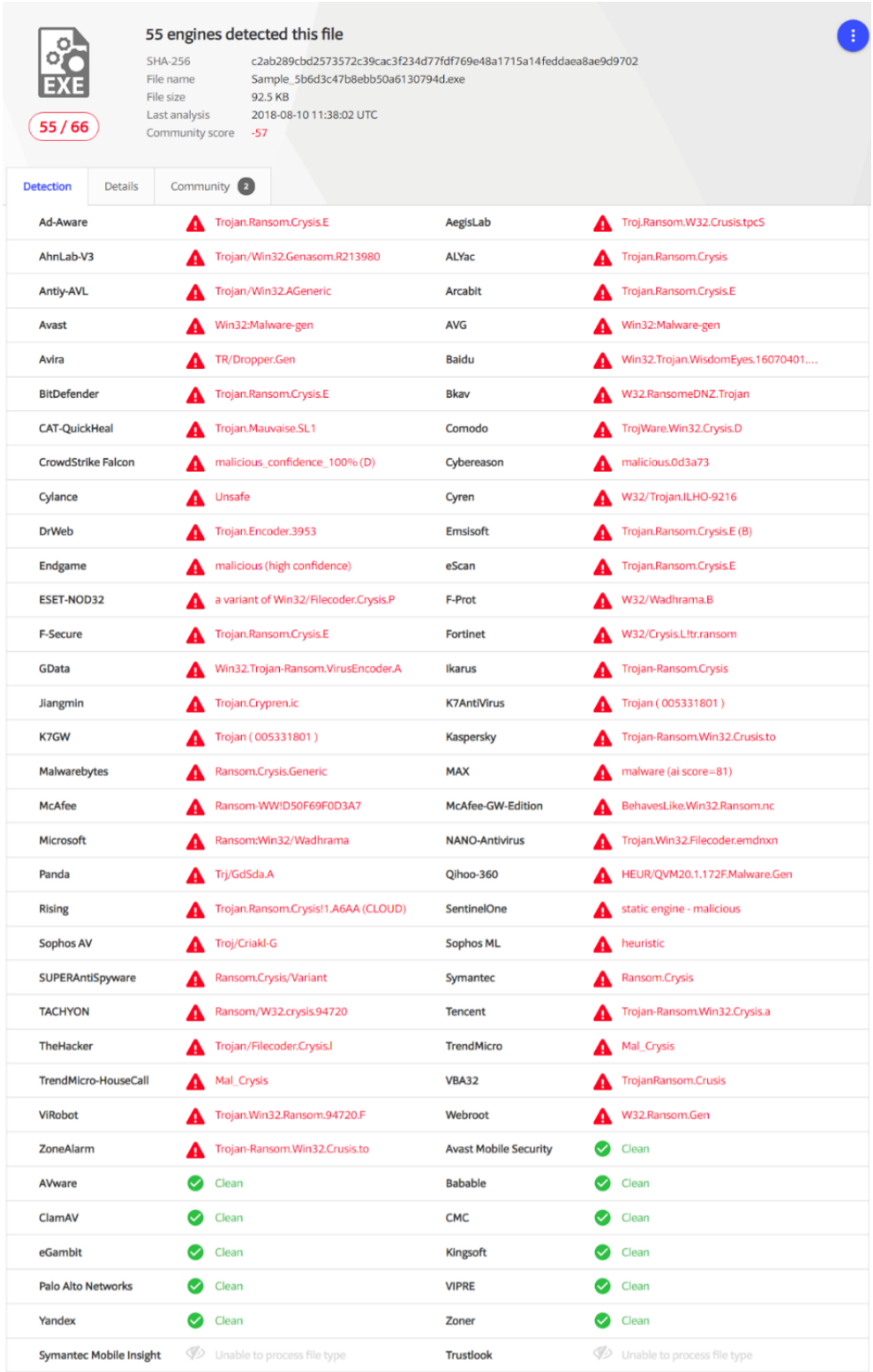
شایان ذکر است که باج‌افزار Dharma (.cmb) محتوای موجود در VSS ویندوز را نیز حذف می‌کند تا فرآیند بازگردانی فایل‌ها با مشکل مواجه گردد. باج‌افزار این کار را از طریق فرآیند vssadmin.exe و با اجرای دستور vssadmin delete shadows /all /quiet انجام می‌دهد.

تحلیل ترافیک شبکه :

طبق بررسی‌ها از طریق ابزارهای تحلیل ترافیک، این باج‌افزار فاقد هر گونه ترافیک شبکه می‌باشد.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۵ مورد از ٦٦ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده وآن را حذف یا غیرفعال می‌کنند.



55 engines detected this file

SHA-256	c2ab289cbd2573572c39cac3f234d77fdf769e48a1715a14feddaea8ae9d9702
File name	Sample_5b6d3c47b8ebb50a6130794d.exe
File size	92.5 KB
Last analysis	2018-08-10 11:38:02 UTC
Community score	-57

55 / 66

Detection | Details | Community 2

Ad-Aware	Trojan.Ransom.Crysis.E	AegisLab	Troj.Ransom.W32.Crusis.tpcS
AhnLab-V3	Trojan/Win32.Genasom.R213980	ALYac	Trojan.Ransom.Crysis
Antiy-AVL	Trojan/Win32.AGeneric	Arcabit	Trojan.Ransom.Crysis.E
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Dropper.Gen	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Trojan.Ransom.Crysis.E	Bkav	W32.RansomeDNZ.Trojan
CAT-QuickHeal	Trojan.Mauvaise.SL1	Comodo	TrojWare.Win32.Crysis.D
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.0d3a73
Cylance	Unsafe	Cyren	W32/Trojan.ILHO-9216
DrWeb	Trojan.Encoder.3953	Emsisoft	Trojan.Ransom.Crysis.E (B)
Endgame	malicious (high confidence)	eScan	Trojan.Ransom.Crysis.E
ESET-NOD32	a variant of Win32/Filecoder.Crysis.P	F-Prot	W32/Wadhrama.B
F-Secure	Trojan.Ransom.Crysis.E	Fortinet	W32/Crysis.L!tr.ransom
GData	Win32.Trojan-Ransom.VirusEncoder.A	Ikarus	Trojan-Ransom.Crysis
Jiangmin	Trojan.Crypren.ic	K7AntiVirus	Trojan (005331801)
K7GW	Trojan (005331801)	Kaspersky	Trojan-Ransom.Win32.Crusis.to
Malwarebytes	Ransom.Crysis.Generic	MAX	malware (ai score=81)
McAfee	Ransom-WW!D50F69F0D3A7	McAfee-GW-Edition	BehavesLike.Win32.Ransom.nc
Microsoft	Ransom:Win32/Wadhrama	NANO-Antivirus	Trojan.Win32.Filecoder.emdnxn
Panda	Trj/GdSda.A	Qihoo-360	HEUR/QVM20.1.172F.Malware.Gen
Rising	Trojan.Ransom.Crysis!1.A6AA (CLOUD)	SentinelOne	static engine - malicious
Sophos AV	Troj/Criakl-G	Sophos ML	heuristic
SUPERAntiSpyware	Ransom.Crysis/Variant	Symantec	Ransom.Crysis
TACHYON	Ransom/W32.crysis.94720	Tencent	Trojan-Ransom.Win32.Crysis.a
TheHacker	Trojan/Filecoder.Crysis.l	TrendMicro	Mal_Crysis
TrendMicro-HouseCall	Mal_Crysis	VBA32	TrojanRansom.Crusis
ViRobot	Trojan.Win32.Ransom.94720.F	Webroot	W32.Ransom.Gen
ZoneAlarm	Trojan-Ransom.Win32.Crusis.to	Avast Mobile Security	Clean
AVware	Clean	Babable	Clean
ClamAV	Clean	CMC	Clean
eGambit	Clean	Kingsoft	Clean
Palo Alto Networks	Clean	VIPRE	Clean
Yandex	Clean	Zoner	Clean
Symantec Mobile Insight	Unable to process file type	Trustlook	Unable to process file type

خروجی سامانه ویروس‌کاو مرکز ماهر :

در حال حاضر تعداد ۱۰ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه بومی ویروس کاو قادر به شناسایی این باج افزار بوده وآن را حذف یا غیرفعال می‌کنند.