بسمه تعالی

تحلیل باج افزار MoneroPay

مقدمه:

رصد فضای مجازی در هفته جاری از انتشار باج‌افزار جدیدی موسوم به MoneroPay (که با نام SpriteCoin نیز شناخته می شود) در فضای سایبری خبر می دهد که با توجه به نقشه پراکندگی آلودگی، ظاهراً کاربران انگلیسی زبان را هدف قرار داده است. نکته حائز اهمیت در خصوص تحلیل این باج افزار این است که : *"ما بر این عقیده ایم این باج افزار تشریح کننده روشی جدید برای برای پرداخت باج به کلاهبرداران اینترنتی است تا اینکه به عنوان یک عنصر استخراج کننده ارز دیجیتال باشد."* در ادامه گزارش تحلیل باج افزار مورد اشاره که توسط تیم تحلیل باج‌افزار مرکز آپا دانشگاه بجنورد تهیه گردیده است تقدیم می گردد.

روش ورود:

فایل اولیه باج افزار MoneroPay یک فایل پک شده متشکل از دو فایل اجرایی به نام های spritecoind.exe و spritecoinwallet.exe و دو کتابخانه به نامهای boost.dll و cryptonight.dll می‌باشد.

Filename	Packed	Unpacked	Quota	Date/Time	CRC-32
ZIP archive					
boost.dll	3146208	3145728	100.0%	1/6/2018 1:27...	2C80C287
cryptonight.dll	1048736	1048576	100.0%	1/6/2018 1:28...	166755BC
spritecoind.exe	235396	1228800	19.2%	1/6/2018 1:28...	473D2287
spritecoinwallet.exe	19509	3145728	0.6%	1/6/2018 5:52...	036C06BA

این باج افزار برای نخستین بار در آدرس اینترنتی 'hxxp://pagebin[.]com/xxqZΛVES' که یکی از دامنه های وب سایت pagebin.com (سرویسی برای ساخت و به اشتراک گذاری صفحات ساده وب) می باشد مشاهده گردید.

SpriteCoin

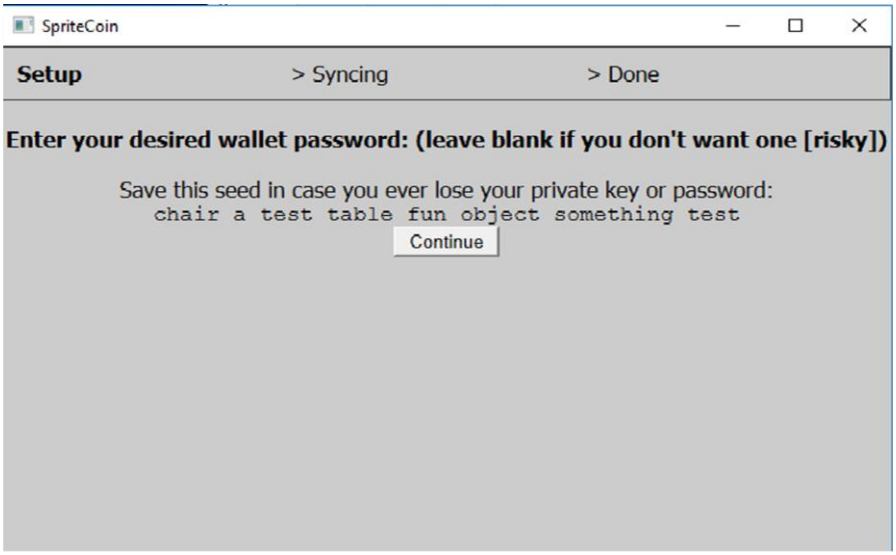
SpriteCoin is a new cryptocurrency written entirely in JavaScript (with C for the mining module). It uses the CryptoNight algorithm but is not cryptonote-based. With a max supply of 1 trillion coins and a block time of 45 seconds, this is sure to be a profitable coin for you (I hope).

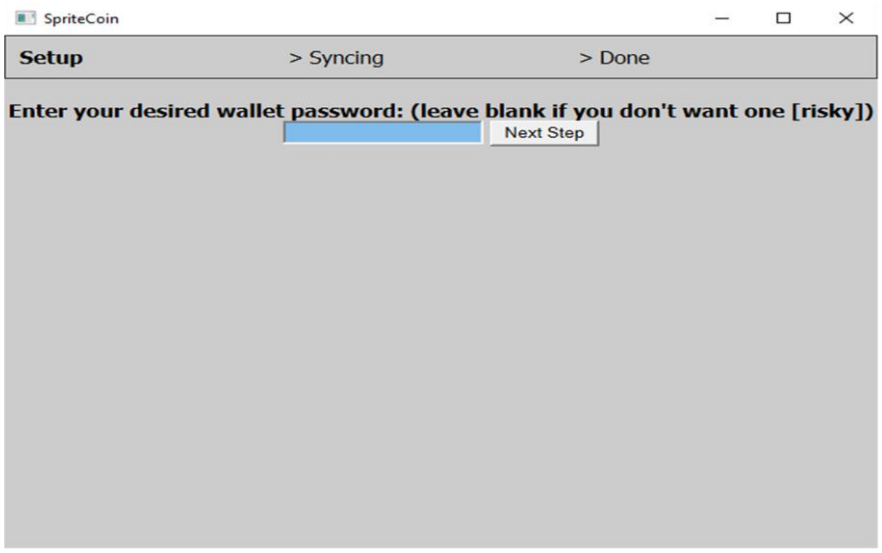
Download for Windows (scan it with VirusTotal if you don't trust it)

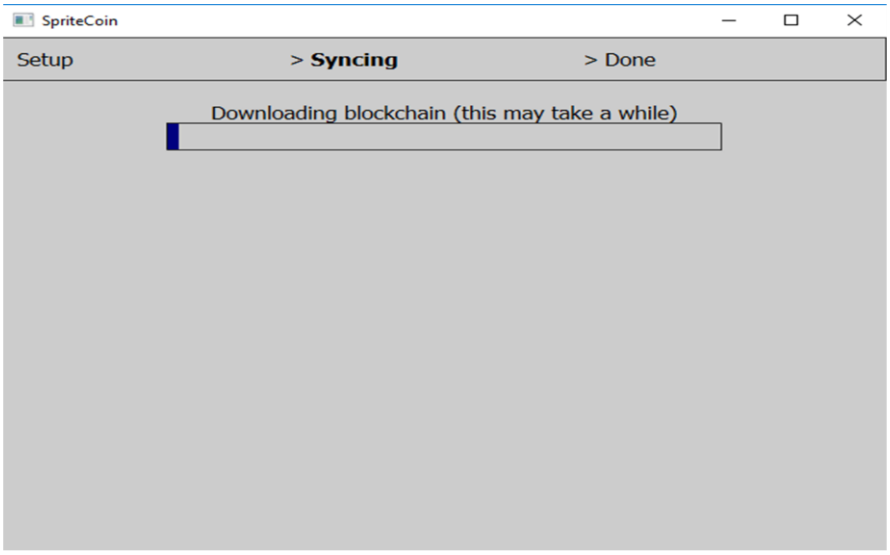
بررسی ها نشان می‌دهد این باج افزار از طریق پروتکل RDP با سوء استفاده از ضعف این پروتکل در پیکربندی نادرست وارد سیستم قربانی می شود. هرزنامه ها و پیوست ایمیل های آلوده نیز سهم به سزائی در انتشار این باج افزار دارند.

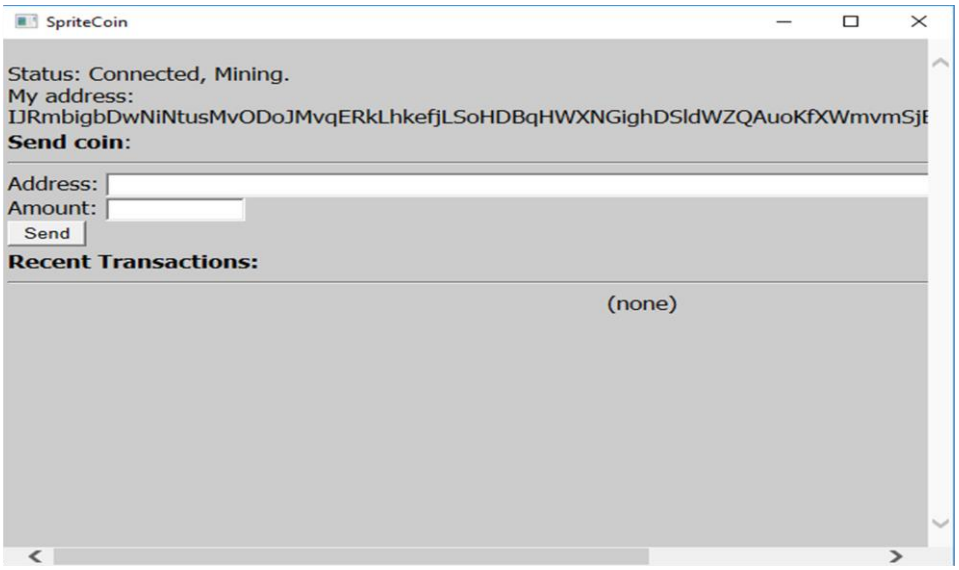
عملکرد باج افزار :

تحلیل های آزمایشگاهی نشان می دهد فایل spritecoinwallet.exe پس از اجرا با تظاهر به دانلود فناوری Blockchain توجه قربانی را به خود جلب کرده که در همین حال فرآیند spritecoind.exe در پشت صحنه فایل های سیستم قربانی را رمزگذاری می کند. این مراحل توسط کارشناسان این مرکز بررسی و آزمایش گردیده که تصاویر زیر گویای این موضوع می باشند :

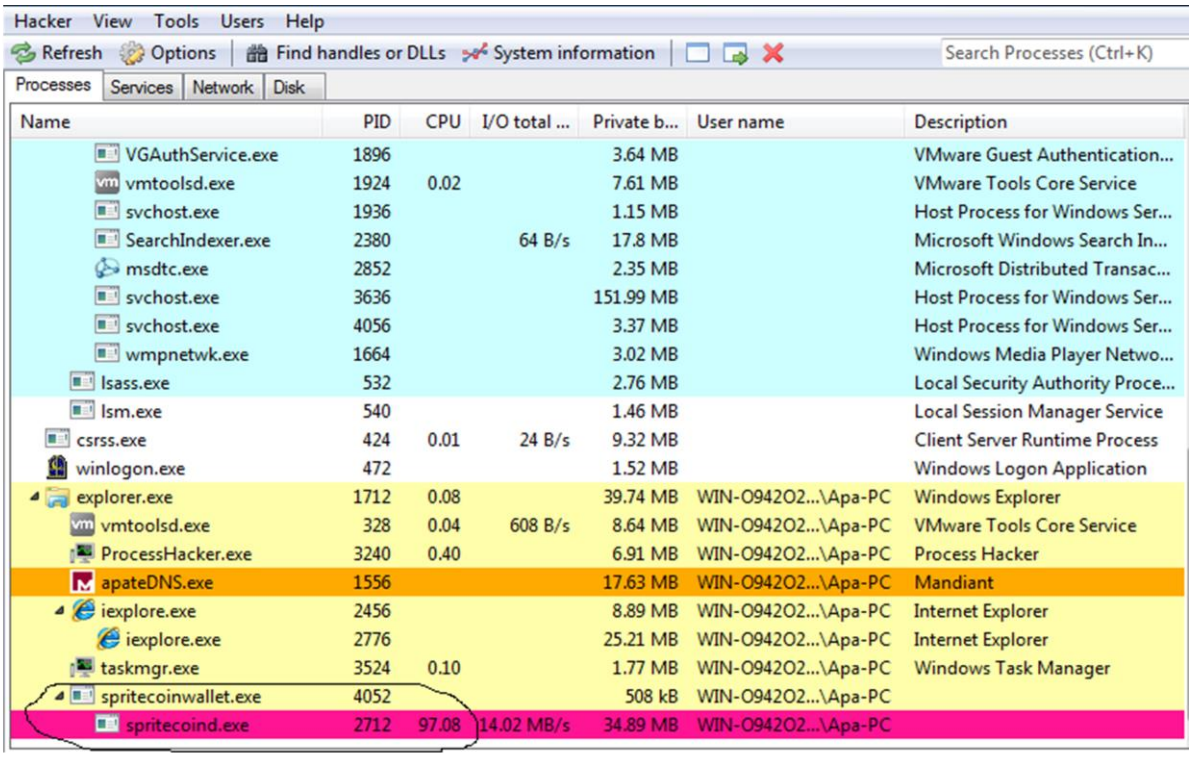








نکته بسیار حائز اهمیت در مورد این باج افزار این است که در نگاه اول گمان ها به سمت این موضوع می‌رود که باج افزار مذکور علاوه بر رمزگذاری فایل های سیستم قربانی احتمالاً از منابع سیستم برای استخراج ارز دیجیتال استفاده می‌کند. همانطور که در تصویر زیر مشاهده می‌کنید، فرآیند spritecoind.exe به میزان قابل توجهی پردازنده سیستم را به خود مشغول کرده است که خود عاملی در جهت تایید این موضوع می باشد. اما مهندسی معکوس کدهای این باج افزار توسط کارشناسان این مرکز، احتمال این موضوع را رد می کند.



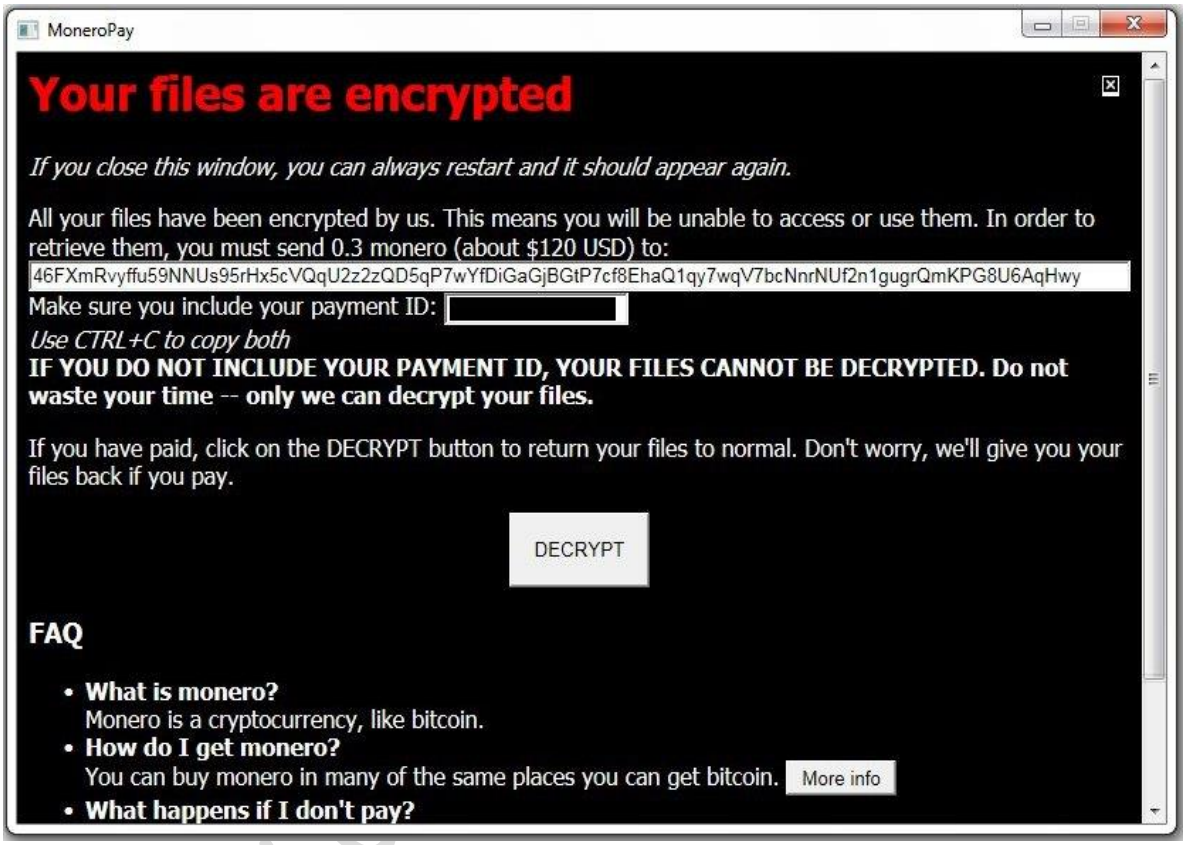
لازم به ذکر است بررسی ها کماکان ادامه دارد و در صورت اثبات استخراج ارز توسط باج افزار مذکور گزارش تکمیلی تقدیم خواهد شد. نتایج آزمایشگاهی نشان داد باج افزار MoneroPay پس از رمزگذاری فایلهای سیستم قربانی پسوند encrypted. را به انتهای فایل های رمزگذاری شده اضافه می‌کند و فایل اجرایی باج افزار در مسیر C:\Users\User\AppData\Local\Temp\Rar$EXa۰.۱۸۸\spritecoind.exe قرار می‌گیرد. در انتهای این فرآیند فایل اجرایی مربوطه متوقف می‌شود. پسوند فایل های هدف عبارتند از :

.txt, .doc, .docx, .xls, .index, .pdf, .zip, .rar, .css, .lnk, .xlsx, .ppt, .pptx, .odt, .jpg, .bmp, .png, .csv, .sql, .mdb, .sln, .php, .asp, .aspx, .html, .xml, .psd, .bk, .bat, .mp۳, .mp٤, .wav, .wma, .avi, .divx, .mkv, .mpeg, .wmv, .mov, .ogg, .java, .csv, .kdc, .dxg, .xlsm, .pps, .cpp, .odt, .php, .odc, .log, .exe, .cr۲, .mpeg, .jpeg, .xqx, .dotx, .pps, .class, .jar, .psd, .pot, .cmd, .rtf, .csv, .php, .docm, .xlsm, .js, .wsf, .vbs, .ini, .jpeg, .gif, .۷z, .dotx, .kdc, .odm, .xll, .xlt, .ps, .mpeg, .pem, .msg, .xls, .wav, .odp, .nef, .pmd, .r۳d, .dll, .reg, .hwp, .۷z, .p۱۲, .pfx, .cs, .ico, .torrent, .c

بررسی ها نشان می دهد این باج‌افزار از الگوریتم رمزنگاری متقارن (AES) برای رمزگذاری فایلهای سیستم قربانی بهره می‌گیرد.

پیغام باج‌خواهی:

براساس پیغام باج‌خواهی، این باج‌افزار برای رمزگشایی فایلهای سیستم قربانی مبلغ ۰.۳ مونرو معادل ۱۲۰ دلار درخواست می‌دهد. در شکل زیر تصویر پیغام باج‌خواهی این باج افزار را مشاهده می‌کنید:



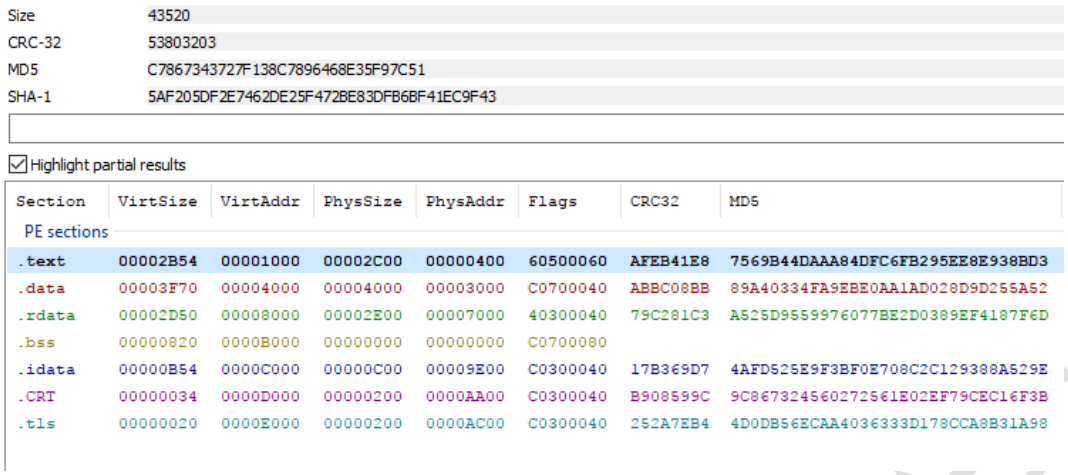
اطلاعات فایلهای اجرایی:

Size	240640
CRC-32	47BA383D
MD5	0470B627E6A84D0FB1F0010F9927835C
SHA-1	8DEA010CF5C9ADC2D9D9235781767B8672C65199

Highlight partial results

Section	VirtSize	VirtAddr	PhysSize	PhysAddr	Flags	CRC32	MD5
PE sections							
UPX0	0217B000	00001000	00000000	00000200	E0000080		
UPX1	0003B000	0217C000	0003A800	00000200	E0000040	5085B02A	703BDBCED595EE66788B411C6E9EE21E
UPX2	00001000	021B7000	00000400	0003AA00	C0000040	AB5A1826	F859F75E5BF9E8272772453EAF430484

spritecoind.exe



Size	43520
CRC-32	53803203
MD5	C7867343727F138C7896468E35F97C51
SHA-1	5AF205DF2E7462DE25F472BE83DFB6BF41EC9F43

Highlight partial results

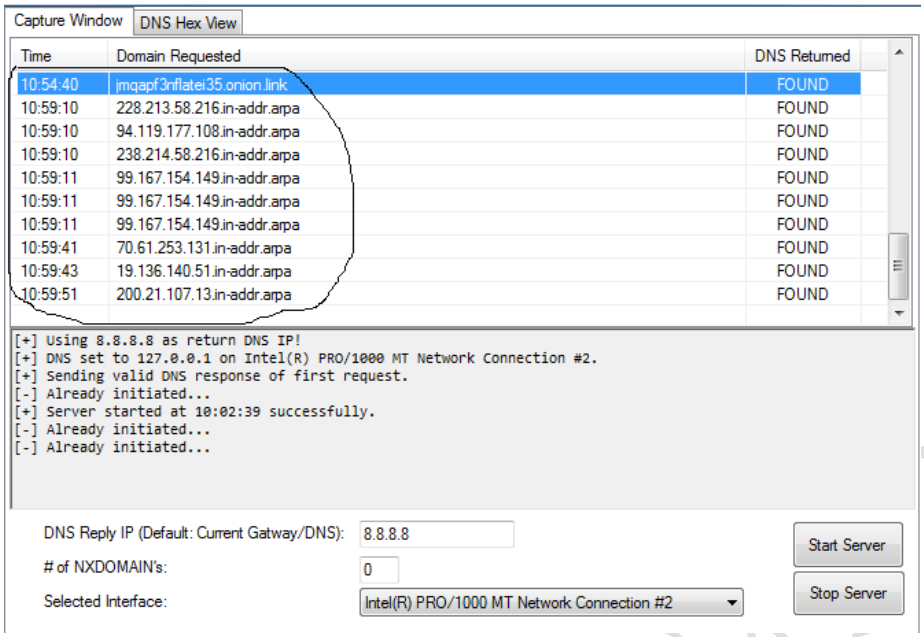
Section	VirtSize	VirtAddr	PhysSize	PhysAddr	Flags	CRC32	MD5
PE sections							
.text	00002B54	00001000	00002C00	00000400	60500060	AFEB41E8	7569B44DAAA84DFC6FB295EE8E938BD3
.data	00003F70	00004000	00004000	00003000	C0700040	ABBC08BB	89A40334FA9EBE0AA1AD028D9D255A52
.rdata	00002D50	00008000	00002E00	00007000	40300040	79C281C3	A525D9559976077BE2D0389EF4187F6D
.bss	00000820	0000B000	00000000	00000000	C0700080		
.idata	00000B54	0000C000	00000C00	00009E00	C0300040	17B369D7	4AFD525E9F3BF0E708C2C129388A529E
.CRT	00000034	0000D000	00000200	0000AA00	C0300040	B908599C	9C8673245602725 61E02EF79CEC16F3B
.tls	00000020	0000E000	00000200	0000AC00	C0300040	252A7EB4	4D0DB56ECAA4036333D178CCA8B31A98

spritecoinwallet.exe

تحلیل ترافیک شبکه:

بررسی خروجی سندباکس های آنلاین نشان می دهد این باج افزار پس از اجرا سعی در برقراری ارتباط با آدرس های اینترنتی زیر و نیز تعدادی آدرس آی پی از طریق پورت ۸۰ و پروتکل TCP را دارد. تحلیل ترافیک شبکه باج افزار مذکور توسط کارشناسان این مرکز به خوبی گویای این موضوع می باشد.

- http://jmqapf۳nflatei۳۵.onion.link/
- http://hho۵۲bhyvh٦۵fhlb.onion.link/
- http://vf٤fnnmhlz۲gporh.onion.link/
- http://h٤eb۵eq٦zfl۵qo٤d.onion.link/
- http://۵qgerbbyhdz۵bwca.onion.link/
- http://ziplamtg۲fn۳q۷۳۳.onion.link/



در ادامه لیست کامل دامنه‌های درخواست داده شده که از سایت https://www.hybrid-analysis.com استخراج شده است، به شرح زیر می‌باشد :

کشور	آدرس IP	دامنه
آمریکا	۱۰٤.۲۰.۱۷.۲٤۲	ipv٤.icanhazip.com
سنگاپور	۱۰۳.۱۹۸.۰.۲	jmqapf۳nflatei۳٥.onion.link
سنگاپور	۱۰۳.۱۹۸.۰.۲	jmqapf۳nflatei۳٥.onion.link:۸۰
آلمان	۱۸٥.۱۹٤.۱٤۱.٥۸	ip-api.com

شناسایی:

در حال حاضر یعنی در زمان نگارش این گزارش تعداد ۳٤ مورد از ٦۷ آنتی ویروس موجود در وب سایت Virustotal.com قادر به شناسایی فایل spritecoind.exe بوده وآن را حذف یا غیر فعال می‌کنند. اما این عدد در مورد فایل spritecoinwallet.exe تنها ٦ مورد می باشد که این نشان دهنده خطرناک بودن این باج‌افزار می باشد.

Antivirus	Result	Update
AegisLab	Ransom.Moneropay.Thaooah!c	20180116
ALYac	Trojan.Ransom.MoneroPay	20180116
CrowdStrike Falcon (ML)	malicious_confidence_70% (W)	20171016
Cylance	Unsafe	20180116
Endgame	malicious (high confidence)	20171130
TrendMicro-HouseCall	Ransom_MONEROPAY.THAOOAH	20180116

“spritecoinwallet.exe” Detection Rate

Antivirus	Result	Update
Ad-Aware	Trojan.GenericKD.12741655	20180113
AegisLab	Troj.Ransom.W32.BlockerIc	20180113
ALYac	Trojan.GenericKD.12741655	20180113
Antiy-AVL	Trojan[Ransom]/Win32.Blocker	20180113
Arcabit	Trojan.Generic.DC26C17	20180113
Baidu	Win32.Trojan.WisdomEyes.16070401.9500.9995	20180112
BitDefender	Trojan.GenericKD.12741655	20180113
CrowdStrike Falcon (ML)	malicious_confidence_90% (W)	20171016
Cylance	Unsafe	20180113
eGambit	Unsafe.AI_Score_98%	20180113
Emsisoft	Trojan.GenericKD.12741655 (B)	20180113
Endgame	malicious (moderate confidence)	20171130
F-Secure	Trojan.GenericKD.12741655	20180113
GData	Trojan.GenericKD.12741655	20180113
Ikarus	Win32.SuspectCrc	20180113
Sophos ML	heuristic	20170914
K7AntiVirus	Riskware (0040eff71)	20180113
K7GW	Riskware (0040eff71)	20180112
Kaspersky	Trojan-Ransom.Win32.Blocker.kpug	20180113
MAX	malware (ai score=95)	20180113
McAfee	Artemis!14EA53020B4D	20180113
McAfee-GW-Edition	BehavesLike.Win32.Downloader.tz	20180113
Microsoft	Ransom:Win32/Genasom	20180113
eScan	Trojan.GenericKD.12741655	20180113
Palo Alto Networks (Known Signatures)	generic.ml	20180113
SentinelOne (Static ML)	static engine - malicious	20171224
Sophos AV	Mal/Behav-044	20180113
Symantec	Trojan.Gen.2	20180112
Tencent	Win32.Trojan.Blocker.Dzug	20180113
TrendMicro	Ransom_Guperd.R002C0DAA18	20180113
TrendMicro-HouseCall	Ransom_Guperd.R002C0DAA18	20180113
VIPRE	Trojan.Win32.Generic!BT	20180113
ViRobot	Trojan.Win32.Z.Agent.1228800.CS	20180113
ZoneAlarm by Check Point	Trojan-Ransom.Win32.Blocker.kpug	20180113

“spritecoind.exe” Detection Rate