شکار تهدید باج‌افزار NetWalker

شکار تهدیدات

آکادمی راوین

طه توکلی

نسخه ۰.۱

۲ اسفند ۱۴۰۰

فهرست مطالب

فهرست شکل‌ها

۱.۰ پیش‌گفتار

امروزه زمان بسیار بیشتری را نسبت به گذشته در اینترنت می گذرانیم. که به دلیل لزوم محدودیت‌های ناشی از ویروس کرونا ایجاد شده‌است. چنین وضعیتی برای هکرها بسیار مفید است، زیرا به آنها فرصتی می‌دهد به دلیل ایجاد فرآیندهای دورکاری سازمان‌ها، رایانه‌های بیشتری را نسبت به قبل آلوده کنند. به همین دلیل هکرها تقریبا هر روز ویروس‌های جدیدی را برای اهدافشان ایجاد می‌کنند. آن‌ها به داده‌های ارزشمند مختلف مانند اسناد و فایل‌های با اهمیت حمله می‌کنند. یکی از جدیدترین ویروس‌هایی که دنیا را بر این اساس هدف قرار می‌دهد، باج‌افزار NetWalker است که به رمزنگاری فایل‌های شما می‌پردازد و در ادامه از شما باج‌خواهی می‌کند.

این ویروس به هیچ یک از خانواده‌های باج‌افزارهای رمزگذاری فایل که از قبل شناخته شده تعلق ندارد و یک گونه‌ی کاملا جدید است و به راحتی می‌تواند به یکی از گسترده‌ترین ویروس‌ها تبدیل شود. هکرها برای مرحله‌ی ایجاد دسترسی اولیه از وب‌سایت‌های آلوده و یا آلوده‌سازی اسناد مایکروسافت آفیس و یا از طریق فایل پیوست ایمیل و ارسال فایل مخرب به واسطه‌ی آن اقدام کرده‌اند. هنگامی که قربانی احتمالی این پیوست را باز می‌کند، سیستم‌عامل کد باج‌افزار -Net Walker را اجرا می‌کند. هنگامی که این ویروس با موفقیت وارد سیستم‌عامل می‌شود، کلیدهای رجیستری و مقادیر آنها را تغییر می‌دهد. سپس فرآیندهای سیستم را آلوده می‌کند و به وسیله آن داده‌ها را رمزگذاری می‌کند. در نتیجه، فایل‌ها پسوندهای جدیدی دریافت می‌کنند که شبیه یک شناسه هستند، برای مثال فایل a.zip به a.zip.mailto[knoocknoo@cock.li].8c00d تبدیل می‌شود و در عمل فایل شما رمز شده‌است و شما دیگر به آن دسترسی نخواهید داشت.

از نمونه‌های پر اهمیت آلوده‌سازی توسط این باج‌افزار می‌شود به دو حمله گسترده گزارش شده در گروه Toll که یک شرکت حمل و نقل و تدارکات استرالیایی است و وب سایت Illinois Champaign-Urbana Public-Health District (CUPHD) اشاره‌کرد.
این حمله، اف‌بی‌آی و وزارت امنیت داخلی ایالات متحده را مجبور کرد وارد عمل شوند و نشان دهنده شدت این بحران و اهمیت آشنایی با این نوع برای جلوگیری از حملات بیشتر است.

حتی تصور اینکه شما صبح وارد رایانه خود شوید و با چنین صحنه مواجه شوید ترسناک است چه برسد به آلوده‌سازی فایل‌های سازمانی و اطلاعات مهم ارگان‌های یک کشور.

نکته ۱.۰ آن‌ها قربانیان خود را پس از پرداخت پول نادیده می‌گیرند یا حتی ویروس دیگری را بجای رمزگشا ارسال می‌کنند. به همین دلیل اکیداً به شما توصیه می‌کنیم از هرگونه تماس با آن‌ها خودداری کنید.

8C00D-Readme.txt - Notepad
File Edit Format View Help

```
Hi!
Your files are encrypted.
All encrypted files for this computer has extension: .8c00d

--

If for some reason you read this text before the encryption ended,
this can be understood by the fact that the computer slows down,
and your heart rate has increased due to the ability to turn it off,
then we recommend that you move away from the computer and accept that you have been compromised,
rebooting/shutdown will cause you to lose files without the possibility of recovery and even god will not be able to help you,
it could be files on the network belonging to other users, sure you want to take that responsibility?

--

Our encryption algorithms are very strong and your files are very well protected, you can't hope to recover them without our help.
The only way to get your files back is to cooperate with us and get the decrypter program.
Do not try to recover your files without a decrypt program, you may damage them and then they will be impossible to recover.

We advise you to contact us as soon as possible, otherwise there is a possibility that your files will never be returned.
For us this is just business and to prove to you our seriousness, we will decrypt you some files for free,
but we will not wait for your letter for a long time, mail can be abused, we are moving on, hurry up with the decision.

Contact us:
1.knoocknoo@cock.li
2.eeeooppaaaxxx@tuta.io

Don't forget to include your code in the email:
{code_1b1ea859_8c00d:
Cnki0xc53Zy8qJjq36VnPOwwzzI9zQNmNBios9upwrg84JSJci
ktCYY3zeZBl9XXdXefRexJQIBHTcJSo5v/rrB7LapkGPBYWage
G0a93CS4MO9/dYcOiRAj3FCQ755Rf69hAqO7rZjlkXEOFr0GXR
qcyc1Y4AaF7kGEm3htNpew8dcSdlIbfjJW61jBZ/LH3tvCHjbx
VG/tV05Q3KHWZHihW5XjZVg6eGHi7LMtmhNV+pGMQXiewsIMFu
Nz14fXoEzz2F1mioOFu0KLbyQgMTpEWnM=}
```

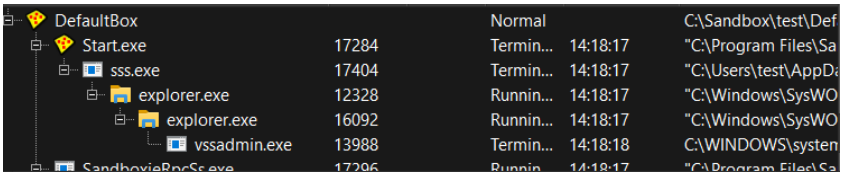
شکل ۱ پیغام باج‌افزار

۲.۰ تحلیل

این بخش به تحلیل NetWalker می‌پردازد.

۱.۲.۰ روند اجرایی

پس از اجرای فایل، روند اجرایی زیر رخ می دهد:



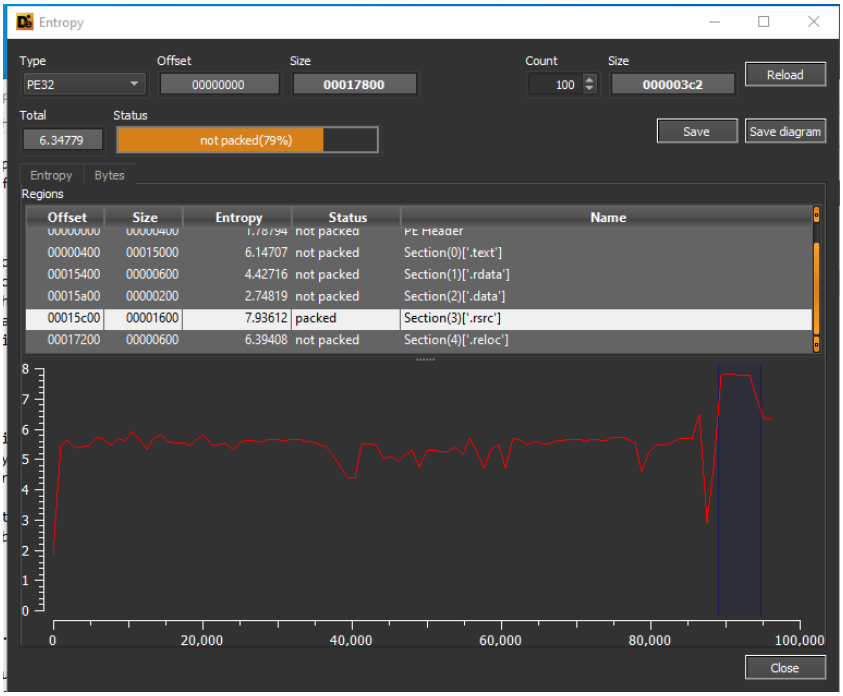
شکل ۲ روند اجرایی

که در این فرآیند ایتدا به واسطه‌ی Explorer.exe فرآیند Process Hollowing [۱] رخ می‌دهد و فرآیند اجرایی باج‌افزار را شکل می‌دهد و سپس از vssadmin برای پاک کردن shad-owcopy ها استفاده کرده است برای اینکه روند بازگردانی فایل‌های backup را با مشکل مواجه کند. در ادامه فرآیند اصلی حذف می‌شود و ادامه کار به وسیله‌ی explorer.exe آلوده‌شده انجام می‌شود.

۱ عبارتست از تکنیکی که به واسطه‌ی آن یک فرآیند در حالت تعلیق ایجاد می‌شود، سپس از Map حافظه خارج می‌شود و با کد مخرب جایگزین می‌شود.

۲.۲.۰ آنتروپی

همان‌طور که در شکل نشان داده شده‌است آنتروپی بالایی در section های مختلف به ویژه در بخش rsrc. وجود دارد که نشانه درهم‌سازی کد برای فرار از شناخت مبتنی بر امضا آنتی‌ویروس می‌باشد.



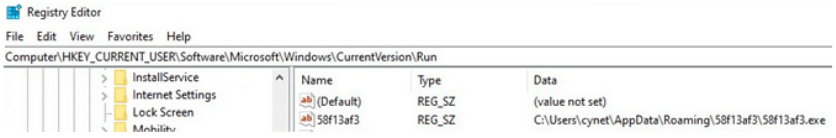
شکل ۳ آنتروپی

؟؟

۳.۲.۰ تکنیک پایداری

به منظور حفظ پایداری [۲] فایل مخرب در ماشین کاربر، payload فایل اجرایی اصلی را از محل خود حذف می‌کند و آن را در پوشه "AppData\Roaming" رها می‌کند و یک کلید رجیستری ایجاد می‌کند که هر بار فایل را اجرا می کند. دلیل اینکه مهاجمان دوست دارند فایل‌های مخرب

[2] Persistance



شکل ۴ تکنیک پایداری

را به "AppData" منتقل کنند این است که این یک مسیر مخفی است که کاربر معمولی متوجه وجود یک فایل مخرب در آن نمی‌شود و لازم نیست یک کاربر admin برای آن داشته باشید.

۴.۲.۰ نمونه‌ی VBS

از نمونه‌های بدست‌آمده از این باج‌افزار نمونه‌ی VBS هست که که کامل درهم‌سازی و مبهم شده است و در ادامه بخشی از آن آمده‌است.

شکل ۵ نمونه VBS

۳.۰ نمونه آشکارسازها

۱.۳.۰ چکیده ها

94994

تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-08-31	5ae06a8d117e8764768322450397158 25fbfbefc0d2463ab6c30295dd1d4afa6	sha256
	4f7dd00a005caf046dd7e494fea25be2264974264d567edfc89122242b7c41bc	sha256
	ae431797c551c20fe2f3fe1adc08a566edfabf45abbd924f0c8da06381ab6e48	sha256
	e56d45628f0c2bda30ab235657704aac50a8433bdb4215c77a2e0f52f0f31a49	sha256
	f743c0849d69b5ea2f7eaf28831c86c1536cc27ae470f20e49223cbdba9c677c	sha256
	8e030188e0d03654d5e7a7738a9d6a9a	md5
	81c965ff526e7afd73c91543fee381a3	md5
	531c0c5e943863b00c7157c05603113a	md5
	0d890fc8e761b764ba3a04af07197e20	md5
	96e1849976d90425e74f075ed6bf8c30	md5
	5af5e3426926e551ed3acc5bea45eac6	md5
	e24a174fff19d873df0fa5eddd9ec534617ed9d7	sha1

جدول ۱ آشکارساز رویداد 94994

جدول ۲ آشکارساز رویداد 94960

94960		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-05-27	b1f0093b89561c6123070165bd2261e2	md5
	aac57162dc1311f07a869f7163bd30e0d62dcc0e	sha1
	f4656a9af30e98ed2103194f798fa00fd1686618e3e62fba6b15c9959135b7be	sha256

جدول ۳ آشکارساز رویداد 94739

94739		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-06-09	853fa18adc3f9263a0f98a9a257dd70d7e1aee0545ab47a114f44506482bd188	sha256
	8587037c15463d10a17094ef8fa9f608cc20c99fa0206ce496b412f8c7f4a1b8	sha256
	58e923ff158fb5aecd293b7a0e0d305296110b83c6e270786edcc4fea1c8404c	sha256
	73de5babf166f28dc81d6c2faa369379	md5
	e393a9ecf0d0a8babaa5efcc34f10577aff1cad1	sha1
	3d6203df53fcaa16d71add5f47bdd060	md5
	7a1288c7be386c99fad964dbd068964f	md5
	8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160	sha256
	9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967	sha256
	de04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d	sha256
	258ed03a6e4d9012f8102c635a5e3dcd	md5
	a3bc2a30318f9bd2b51cb57e2022996e7f15c69e	sha1

جدول ۴ آشکارساز رویداد 94509

94509		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-03-23	58e923ff158fb5aecd293b7a0e0d305296110b83c6e270786edcc4fea1c8404c	sha256
	416556c9f085ae56e13f32d7c8c99f03efc6974b2897070f46ef5f9736443e8e	sha256
	73de5babf166f28dc81d6c2faa369379	md5
	e393a9ecf0d0a8babaa5efcc34f10577aff1cad1	sha1
	3d6203df53fcaa16d71add5f47bdd060	md5
	d7d7f3c95d03367c61bcfdfe4e7ab47a	md5
	775f5027abc97c0ec8e9202a4ed4cc14	md5
	b0008e752f488d7e97a8d2452411527e	md5
	207d2a5aa3a00b8c908b6cffcf6dded8	md5
	7a1288c7be386c99fad964dbd068964f	md5
	8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160	sha256
	9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967	sha256

جدول ۵ آشکارساز رویداد 80752

80752		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-10-28	0681c37cfbb640a08028c3ba49e92dc82268f8ad2aa865b86efafc834ade3682	sha256
	de04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d	sha256
	750a8e4f994a9ef9fc0b37a4d171b46457e1455195a1f8c1e926d354125f6470	sha256
	dbbefe25c1c2ad178d1c91a69d91a7f06c9c1e40cce74d124c1a6f147eb6ab96	sha256
	4863840ed49a1779ad7acc7fbfa1ee80c531813f05c73be76c5ae2807a9036b3	sha256
	4158ad6eca8c3087ed221953f7a69d3d40a772c5af415f32e110a46da8a9f8ac	sha256
	0061e41a2ce989b4561b514db2f03d6206fb582a716a7b09b01950b3016415b1	sha256
	7aac112635cbde748a97b38f6a52aaebbc3f0050f81cf36ccdc6c294c214fd73	sha256
	9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967	sha256
	e935f3917b5c33eda4fec9dccfce78564bf7979fe36685825ccd5a03de8c18df	sha256
	1f234d834d4e61492821d5e34dc7180ad5009b53e253e9d3bd2c79df7899563d	sha256
	1a387a66d0ae9f0aabeb33f46856fcd8d7621d210d87494f696b831f94537f1b	sha256

جدول ۶ آشکارساز رویداد 80328

80328		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-10-14	de04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d	sha256
	fd29001b8b635e6c51270788bab7af0bb5adba6917c278b93161cfc2bc7bd6ae	sha256
	8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160	sha256
	3ba905e1cda7307163d4c8fe3fd03c2fbce7eda030522084e33d0604c204630e	sha256
	9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967	sha256
	ad8d379a4431cabd079a1c34add903451e11f06652fe28d3f3edb6c469c43893	sha256
	8f834966a06f34682b78e1644c47ab488b394b80109ddea39fc9a29ed0d56a0c	sha256
	58e923ff158fb5aecd293b7a0e0d305296110b83c6e270786edcc4fea1c8404c	sha256
	993b73d6490bc5a7e23e02210b317247	md5
	59881abed688ceba3d67c2ff22076ad8	md5
	7a1288c7be386c99fad964dbd068964f	md5
	258ed03a6e4d9012f8102c635a5e3dcd	md5

جدول ۷ آشکارساز رویداد 73574

73574		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-08-19	5af5e3426926e551ed3acc5bea45eac6	md5
	e24a174fff19d873df0fa5eddd9ec534617ed9d7	sha1
	f743c0849d69b5ea2f7eaf28831c86c1536cc27ae470f20e49223cbdba9c677c	sha256
	3b447099ca280dabd22d36f84ebfd3bb	md5
	49fd831a738b21ee0a1b3b62cd15801abe8c32d5	sha1
	6a511d4178d6d2f98f8af34311d0e15dc8dc1c4b643e6943f056da6ce242e70d	sha256
	531c0c5e943863b00c7157c05603113a	md5
	caa18377e764a3a27c715b3d69ba2258ee4eb0b2	sha1
	4f7dd00a005caf046dd7e494fea25be2264974264d567edfc89122242b7c41bc	sha256
	0d890fc8e761b764ba3a04af07197e20	md5
	21c0ed7abaafbfd14c777aa370f397e4351654a6	sha1
	5ae06a8d117e876476832245039715825fbfbefc0d2463ab6c30295dd1d4afa6	sha256

جدول ۸ آشکارساز رویداد 70073

70073		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-08-05	129a0f0f4dd667e3ecbcc252b890f306eb041ad0295cb1511343c307c12a658d	sha256
	29aef7903990290 29e0443455d72a8b928854a0706f2e211ae7a03bba0e3d4f4	sha256
	0d0ed90929351c08c47dbd7541073d037240718c4a2fd63c09d2377090d4cd7a	sha256
	fd29001b8b635e6c51270788bab7af0bb5adba6917c278b93161cfc2bc7bd6ae	sha256
	26dfa8512e892dc8397c4ccbbe10efbcf85029bc2ad7b6b6fe17d26f946a01bb	sha256
	e1a8a38dda16a7815bd20a96f46bd978ac41f2acf927993ad965abb258123d8c	sha256
	5daf828fd452f5325c28bc145a86d3d943cd86bb13ffe35c440ebf3cd2a45522	sha256
	f298725e197f974b7a8407c5d79114a4ac322c573813d543141ccf1d9119dd8b	sha256
	b2d68a79a621c3f9e46f9df52ed19b8fec22c3cf5f4e3d8630a2bc68fd43d2ee	sha256
	f2b96f7d6f1bfd464507790120d07bba46cb4c98563993357 48f93ebd52b5696	sha256
	4df67a9e8abab33856a586cea38b0d365fbbe0d91ee848f270c65f0125d2d677	sha256
	eb1470786fda58fc8291e099c7fcd5d36a04de85d1f6fe8683c1950b7119314e	sha256

جدول ۹ آشکارساز رویداد 70030

70030		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-07-31	58e923ff158fb5aecd293b7a0e0d305296110b83c6e270786edcc4fea1c8404c	sha256
	5b80cbbdcb697c0b8ec26e6cf0ff305c	md5
	6a64553da499c1d9a64d97f4de3882f5	md5
	27304b246c7d5b4e149124d5f93c5b01	md5
	7a1288c7be386c99fad964dbd068964f	md5
	258ed03a6e4d9012f8102c635a5e3dcd	md5
	3d6203df53fcaa16d71add5f47bdd060	md5
	8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160	sha256
	59881abed688ceba3d67c2ff22076ad8	md5
	e393a9ecf0d0a8babaa5efcc34f10577aff1cad1	sha1
	655352e00c7e478c3fed38bc6f407982dec3768d	sha1
	6fd314af34409e945504e166eb8cd88127c1070e	sha1

جدول ۱۰ آشکارساز رویداد 69847

69847		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-07-29	258ed03a6e4d9012f8102c635a5e3dcd	md5
	73de5babf166f28dc81d6c2faa369379	md5
	3d6203df53fcaa16d71add5f47bdd060	md5
	7a1288c7be386c99fad964dbd068964f	md5
	5b80cbbdcb697c0b8ec26e6cf0ff305c	md5
	993b73d6490bc5a7e23e02210b317247	md5
	27304b246c7d5b4e149124d5f93c5b01	md5
	8fbc17d634009cb1ce261b5b3b2f2ecb	md5
	59881abed688ceba3d67c2ff22076ad8	md5
	6a64553da499c1d9a64d97f4de3882f5	md5
	655352e00c7e478c3fed38bc6f407982dec3768d	sha1
	a3bc2a30318f9bd2b51cb57e2022996e7f15c69e	sha1

جدول ۱۱ آشکارساز رویداد 68183

68183		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-06-08	44b5d24e5e8fd8e8ee7141f970f76a13c89dd26c44b336dc9d6b61fda3abf335	sha256
	853fa18adc3f9263a0f98a9a257dd70d7e1aee0545ab47a114f44506482bd188	sha256
	346fdff8d24cbb7ebd56f60933beca37a4437b5e1eb6e64f7ab21d48c862b5b7	sha256
	bd3fdf1b50911d537a97cb93db13f2b4026f109ed23a393f262621faed81dae1	sha256
	868cb8251a245c416cd92fcbd3e30aa7b7ca7c271760fa120d2435fd3bf2fde9	sha256
	ce399a2d07c0851164bd8cc9e940b84b88c43ef564846ca654df4abf36c278e6	sha256
	ac0882d87027ac22fc79cfe2d55d9a9d097d0f8eb425cf182de1b872080930ec	sha256
	8587037c15463d10a17094ef8fa9f608cc20c99fa0206ce496b412f8c7f4a1b8	sha256
	ae03734805e3b7ec0fa52c5a4f07a725	md5
	b58476f659782f7708547268476017fda	md5
	12a470956f7437a00d7bcf47f1995ea7	md5
	80675f08a4dad40a316865619f6adaaa	md5

جدول ۱۲ آشکارساز رویداد 68182

68182		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-06-08	3d845a707f2825746637922d7dd10fab18558209	sha1
	853fa18adc3f9263a0f98a9a257dd70d7e1aee0545ab47a114f44506482bd188	sha256
	bf38aca2c659f9eb2b2fa2fad82ccf55b496b0cb	sha1
	868cb8251a245c416cd92fcbd3e30aa7b7ca7c271760fa120d2435fd3bf2fde9	sha256
	bd3fdf1b50911d537a97cb93db13f2b4026f109ed23a393f262621faed81dae1	sha256
	03023d7e3a54d915cca82429dfeedb1bebd5c182	sha1
	e20a4cc7f13f517491e772ce9e5c236aad2785f0	sha1
	7301382916d9f5274a4fb847579f75bc69c9c24b	sha1
	8e7a5500007c1552e1231bd1157433f7ef638672	sha1
	ce399a2d07c0851164bd8cc9e940b84b88c43ef564846ca654df4abf36c278e6	sha256
	44b5d24e5e8fd8e8ee7141f970f76a13c89dd26c44b336dc9d6b61fda3abf335	sha256
	346fdff8d24cbb7ebd56f60933beca37a4437b5e1eb6e64f7ab21d48c862b5b7	sha256

جدول ۱۳ آشکارساز رویداد 66432

66432		
تاریخ	آشکارساز باج‌افزار	تابع چیکده‌ساز
2020-03-31	acec0bb9d9bd199d3e6a77b763cebee8f67275996d3c55af8c617fef76f2e87f	sha256
	2b35aa9c70ef66197abfb9bc409952897f9f70818633ab43da85b3825b256307	sha256
	08710023c219f26237a9c8de5454a1de17117a2da651b4391afce8e331f31dfa	sha256
	4c9e35f3d5f555dda5f4373cf23fbb289c6067c70841be7022ba6da62e49cccb	sha256
	b49c9eba58537f8d856daded80bc9493a83c508d73423b98686d4e8b232d61c3	sha256
	7cbcad4d6e9ad8438e5febd3830bff9aef4729b98d23935ad7f9e6d290272732	sha256
	906eff4ac2f5244a59cc5e318469f2894f8ced406f1e0e48e964f90d1ff9fd88	sha256
	d2b231eb83de043acfcdf1c938c6b49e465d585fe4ce79f42add43a17aba1300	sha256
	9aea43b22f214228caf4fc714f426c0a140b7dd70b010bf3778cd1c0ec440851	sha256
	3bbd2beaa7953543e3cfb09d064db83b11034ff81255429b82e2de40d661ee29	sha256

۲.۳.۰ دامنه ها

- sophosproductupdate.com
- filedownloaderserverx.com
- sophoswarehouse.com
- sophosenterprisecenter.com
- filedownloaderserver.com
- updatefileservercross.com
- sophostraining.org
- filedownloaderservers.com
- sophosfirewallupdate.com
- ragnarokfromasgard.com
- drhuzaifa.com
- dewakartu.info
- dewarejeki.info
- erasmus-plius.tomasjs.com
- easytogets.com
- rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion
- pb36hu4spl6cyjdfhing7h3pw6dhpk32ifemawkujj4gp33ejzdq3did.onion

۳.۳.۰ آدرس های پست الکترونیکی

- hariliuios@tutanota.com
- 2hamlampampom@cock.li
- galgalgalgalk@tutanota.com
- johprohnpo@cock.li
- cancandecan@tutanota.com
- galgalgalgawk@tutanota.com
- kavariusing@tutanota.com
- eeaammzzyy@cock.li
- hamlampampom@cock.li
- kazkavkovkiz@cock.li
- eeaammzzyy@tuta.io
- hariliuios@tutanota.com
- kkeessnnkkaa@cock.li
- eeeooppaaaxxx@tuta.io
- hhaaxxhhaaxx@tuta.io
- kkkwwwsvvv@cock.li
- knoocknoo@cock.li
- pabpabtab@tuta.io
- sevenoneone@cock.li
- kokbiglock@cock.li
- repairdb@seznam.cz
- sevenonone@cock.li
- kokoklock@cock.li
- rrrkkktttaaa@cock.li
- hubert.h@hhs.gov

۴.۳.۰ آدرس های IP

- 85.96.49.152
- 109.236.109.159
- 13.72.105.98
- 186.10.98.177
- 198.23.200.241

فهرست نمادها