

باسمه تعالی

تحلیل فنی باج افزار Horsuke

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی به نام Horskuke خبر می دهد. این باج افزار که از خانواده باج افزار Scarab می باشد به نام Scarab-Horsia نیز شناخته می شود و پس از رمزگذاری فایل ها پسوند .horskuke@nuke.africa را به انتهای فایل های رمزگذاری شده اضافه می کند. بررسی ها نشان می دهد که فعالیت این باج افزار در ماه می سال ۲۰۱۸ میلادی شروع شده و به نظر می رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد. این باج افزار از الگوریتم رمزنگاری AES استفاده می کند و از طریق هرزنامه و سرویس دسترسی از راه دور (RDP) وارد سیستم قربانی می شود.

مشخصات فایل اجرایی :

نام فایل	inside.exe Horskuke.exe
MD۵	de8d979884eec2cef0ded628eef4290c
SHA-۱	07eedbb498962aa17a03a712e09e19ffefd7cd8d
SHA-۲۵۶	e7c00830cee1e390bde9b4a21c874c74f16414f391a1221c3f038f6ce7b3d7ee
اندازه فایل	۴۰۲.۵ KB
کامپایلر / پکر	BobSoft Mini Delphi -> BoB / BobSoft

فایل اجرایی این باج افزار دارای هشت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.txt	۷.۱۸	۴۰۹۶	۲۳۶۸۰۴	۲۳۷۰۵۶
.itext	۴.۷۱	۲۴۱۶۶۴	۶۹۲	۱۰۲۴
.data	۴.۷۶	۲۴۵۷۶۰	۱۱۴۶۴	۱۱۷۷۶
.bss	۰	۲۵۸۰۴۸	۲۵۳۰۴	۰
.idata	۴.۶۴	۲۸۶۷۲۰	۴۳۳۲	۴۶۰۸
.tls	۰	۲۹۴۹۱۲	۸	۰
.rdata	۰.۲۱	۲۹۹۰۰۸	۲۴	۵۱۲
.rsrc	۸	۳۰۳۱۰۴	۱۵۵۷۰۸	۱۵۶۱۶۰

تحلیل پویا :

برای بررسی عمیق تر باج افزار Horsuke فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم.

در دو تصویر زیر وضعیت فرآیندها قبل و بعد از آلودگی را مشاهده میکنید:

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	94.44	0 K	24 K	0		
System	0.41	132 K	952 K	4		
Interrupts	0.65	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	1,140 K	252	Windows Session Manager	Microsoft Corporation
csrss.exe	0.01	2,180 K	4,640 K	332	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,452 K	4,372 K	384	Windows Start-Up Application	Microsoft Corporation
services.exe		5,164 K	9,164 K	488	Services and Controller app	Microsoft Corporation
svchost.exe		4,336 K	9,760 K	600	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		8,444 K	14,328 K	2644	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		2,688 K	6,488 K	2216	WMI Provider Host	Microsoft Corporation
vmacthlp.exe		1,436 K	4,108 K	664	VMware Activation Helper	VMware, Inc.
svchost.exe		4,264 K	8,728 K	708	Host Process for Windows S...	Microsoft Corporation
svchost.exe		18,268 K	18,932 K	788	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		15,736 K	15,732 K	3484	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe		5,516 K	13,296 K	832	Host Process for Windows S...	Microsoft Corporation
dwm.exe	0.16	43,776 K	51,288 K	1352	Desktop Window Manager	Microsoft Corporation
svchost.exe	0.10	25,692 K	42,360 K	860	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,792 K	14,652 K	1020	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	19,968 K	25,356 K	776	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		9,520 K	16,228 K	1112	Spooler SubSystem App	Microsoft Corporation
svchost.exe		10,544 K	13,192 K	1160	Host Process for Windows S...	Microsoft Corporation
taskhost.exe		8,080 K	10,000 K	1260	Host Process for Windows T...	Microsoft Corporation
UploaderService.exe		3,104 K	7,808 K	1500	TechSmith Uploader Service	TechSmith Corporation
VGAuthService.exe		4,592 K	10,504 K	1704	VMware Guest Authenticatio...	VMware, Inc.
vmtoolsd.exe	0.04	10,012 K	20,076 K	1848	VMware Tools Core Service	VMware, Inc.
ManagementAgentHost.e...	0.16	5,852 K	11,248 K	1916		
SearchIndexer.exe	0.01	28,704 K	23,892 K	1760	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		1,920 K	5,580 K	1908	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		3,528 K	8,036 K	2684	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		3,568 K	17,292 K	2788	Host Process for Windows S...	Microsoft Corporation
svchost.exe		66,812 K	24,052 K	2324	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,172 K	6,484 K	2884	Host Process for Windows S...	Microsoft Corporation
lsass.exe		4,792 K	11,252 K	496	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		2,572 K	4,264 K	504	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.08	10,712 K	9,440 K	392	Client Server Runtime Process	Microsoft Corporation
conhost.exe		1,432 K	4,920 K	3144	Console Window Host	Microsoft Corporation
winlogon.exe		2,712 K	6,916 K	440	Windows Logon Application	Microsoft Corporation
explorer.exe	0.12	56,728 K	88,604 K	1380	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.12	14,382 K	27,072 K	1748	VMware Tools Core Service	VMware, Inc.

تصویر ۱: فرایندهای در حال اجرای سیستم عامل قبل از اجرای باج افزار

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	89.17	0 K	24 K	0		
System	1.29	132 K	1,016 K	4		
Interrupts	4.20	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		440 K	1,140 K	252	Windows Session Manager	Microsoft Corporation
csrss.exe		2,180 K	4,636 K	332	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,452 K	4,372 K	384	Windows Start-Up Application	Microsoft Corporation
services.exe	0.01	5,160 K	9,156 K	488	Services and Controller app	Microsoft Corporation
svchost.exe		4,328 K	9,840 K	600	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		8,808 K	14,640 K	2644	WMI Provider Host	Microsoft Corporation
vmacthlp.exe		1,436 K	4,108 K	664	VMware Activation Helper	VMware, Inc.
svchost.exe	< 0.01	4,368 K	8,808 K	708	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	18,276 K	18,960 K	788	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		15,592 K	15,592 K	2820	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe		5,516 K	13,356 K	832	Host Process for Windows S...	Microsoft Corporation
dwm.exe	1.13	64,652 K	73,684 K	1352	Desktop Window Manager	Microsoft Corporation
svchost.exe	0.01	22,724 K	38,432 K	860	Host Process for Windows S...	Microsoft Corporation
taskeng.exe		2,244 K	6,452 K	3016	Task Scheduler Engine	Microsoft Corporation
svchost.exe		7,804 K	14,684 K	1020	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	20,024 K	25,252 K	776	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		9,520 K	16,228 K	1112	Spooler SubSystem App	Microsoft Corporation
svchost.exe	< 0.01	10,596 K	13,208 K	1160	Host Process for Windows S...	Microsoft Corporation
taskhost.exe		8,264 K	10,220 K	1260	Host Process for Windows T...	Microsoft Corporation
UploaderService.exe		3,104 K	7,808 K	1500	TechSmith Uploader Service	TechSmith Corporation
VGAUTHService.exe		4,592 K	10,504 K	1704	VMware Guest Authenticatio...	VMware, Inc.
vmtoolsd.exe	0.06	10,168 K	20,208 K	1848	VMware Tools Core Service	VMware, Inc.
ManagementAgentHost.e...	0.15	5,852 K	11,248 K	1916		
SearchIndexer.exe		31,516 K	24,076 K	1760	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		1,920 K	5,580 K	1908	Host Process for Windows S...	Microsoft Corporation
msdtc.exe		3,528 K	8,036 K	2684	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		3,568 K	17,288 K	2788	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	66,812 K	22,144 K	2324	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,172 K	6,484 K	2884	Host Process for Windows S...	Microsoft Corporation
lsass.exe		4,816 K	11,276 K	496	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		2,572 K	4,272 K	504	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	0.09	10,460 K	6,520 K	392	Client Server Runtime Process	Microsoft Corporation
conhost.exe		1,432 K	4,920 K	3144	Console Window Host	Microsoft Corporation
winlogon.exe		2,712 K	6,916 K	440	Windows Logon Application	Microsoft Corporation
explorer.exe	0.06	65,812 K	95,304 K	1380	Windows Explorer	Microsoft Corporation
vmtoolsd.exe	0.12	14,464 K	27,236 K	1748	VMware Tools Core Service	VMware, Inc.

تصویر ۲: باج افزار در حال اجرا می باشد و از شروع فعالیت فرایندها و نرم افزارها جلوگیری می کند.

طبق بررسی های صورت گرفته، باج افزار HORSUKE پس از اجرا از شروع فعالیت برخی فرایندها و نرم افزارها جلوگیری می کند. پس از اجرای باج افزار پیغام باج خواهی گشوده می شود که این پیغام در تمامی فولدرهای رمز گذاری شده نیز وجود دارد.

تصویر زیر پیغام باج خواهی باج افزار HORSUKE را با نام HOW TO RECOVER ENCRYPTED FILES.TXT نشان می دهد که بر روی پس زمینه سیستم قربانی مستقر شده است :

```
HOW TO RECOVER ENCRYPTED FILES.TXT - Notepad
File Edit Format View Help
=====
          H O R S U K E
=====

Your files are now encrypted!

Your personal identifier:
6A02000000000011DDEAD91D915C43008035B329710FD37B693F5875F4C00892166DA56C6748D7AEAEDEE9B715568BA
5377F174F6F4B5BA2E334AA5C8BD4BD23D930E5E753511F39E5F576D745CE5BE8CC7FA09000DE0B1A92B7DDBD6973DD46D6
59DEBDC75D382AA95DEE18ADF28C21B9DAA341868C2BBCAEBD988E78B94DFA1B558DD8A66B89C37BDD475A3E851857DEEDD
0BEF757662D13E84DED69BB5E69FF088A3A74ED5BC7EBA015E3E748A1CEB8C77BEC642E1F6DB17B877DD43EC3E2C3D2839F
22DB13B0438F9A8743EA166C13193749BC991EC982BDC1B754F3A3FA36A116498EEB730EB6DBFE73CFAD58D81BB44E48C044
93883EF35490421C57B9C8A90E68890EE87D8A074ACAD2B44898721E0D89B0338DFBDD87B7ED88A581BFC98650161207A91C
8E46F69C6A118CE012F0F708D4BA9A066B6CB967E

All your files have been encrypted due to a security problem with your PC.

Now you should send us email with your personal identifier.
This email will be as confirmation you are ready to pay for decryption key.
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 will decrypt all your files.

Contact us using this email address: horsuke@nuke.africa
If you don't get a reply or if the email dies, then contact us to saviours@airmail.cc

Free decryption as guarantee!
Before paying you can send us up to 3 files for free decryption.
The total size of files must be less than 10Mb (non archived), and files should not contain
valuable information (databases, backups, large excel sheets, etc.).

How to obtain Bitcoins? |
* The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
'Buy bitcoins', and select the seller by payment method and price:
https://localbitcoins.com/buy_bitcoins
* Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins

Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price
(they add their fee to our) or you can become a victim of a scam.
```

بر اساس پیغام باج‌خواهی، که در ابتدای آن شناسه ای با طول ۶۴۴ کاراکتر مختص هر قربانی قرار داده شده، مهاجم اعلام می‌کند که فایل های قربانی را رمزگذاری کرده و سپس قربانی را ملزم به فرستادن ایمیل با شناسه یاد شده برای دریافت کلید رمزگشا می‌کند. مهاجم مبلغ باج را به صورت بیت کوین تعیین کرده و اعلام می‌کند که مبلغ باج به سرعت فرستادن ایمیل بستگی دارد. ضمناً برای برقراری ارتباط، ایمیلی به آدرس horsuke@nuke.africa در نظر گرفته شده که در صورت عدم دریافت پاسخ از ایمیل مذکور، ایمیل جایگزین به آدرس saviours@airmail.cc نیز تعبیه شده است.

در ادامه برای حصول اطمینان قربانی، تعدادی از فایل های وی را تحت شرایط زیر به صورت رایگان رمزگشایی می‌کند:

- ۱- حداکثر سه فایل که آرشیو نشده باشند.
 - ۲- مجموع حجم فایل ها حداکثر ۱۰ مگابایت باشد
 - ۳- فایل ها شامل اطلاعات ارزشمند نباشند. (پایگاه های داده، فایل های پشتیبان، صفحات اکسل و...).
- سپس در ادامه نحوه تهیه بیت کوین را آموزش داده و هشدارهایی را نیز برای تهدید قربانی می‌دهد.

ضمناً در پیغام باج‌خواهی مهلتی برای پرداخت باج نیز تعیین نشده است.

پس از برقراری ارتباط به صورت ناشناس با مهاجم، پاسخ اولیه مبنی بر گذشت زمان و عدم توانایی رمزگشایی بود:

```
Hello. It was not easy to get your decryption key cuz it's so much time passed... Here is your files uploaded down bellow:
```

<https://privatlab.com/s/v/XyZ7DG9R5dsoaOLm5XkZ>

در پاسخ بعدی ایمیلی دریافت نمودیم که در آن مهاجم مبلغ ۰.۷ بیت کوین را جهت ارسال به آدرس کیف پول ۱GgRTWRrZ۳Xu۸۴XWTpTa۶۶nxoKcGkZHwpF تعیین نمود.

```
To restore all files that belong to your id transfer 0.7 btc to wallet address 1GgRTWRrZ3Xu84XWTpTa46nxoKcGkZHwpF After conifiration of your transaction we will send you a decryptor software and instruction how to use it. Please, contact us just in case of you're agree to pay. Respect your and our time.
```

طبق بررسی‌های انجام شده، در حال حاضر کیف پول مربوط به این باج‌افزار تراکنشی نداشته است.

Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1GgRTWRrZ3Xu84XWTpTa46nxoKcGkZHwpF	No. Transactions	0
Hash 160	abfe8663e734710affaf6580281d3f84ea75e4be	Total Received	0 BTC
		Final Balance	0 BTC

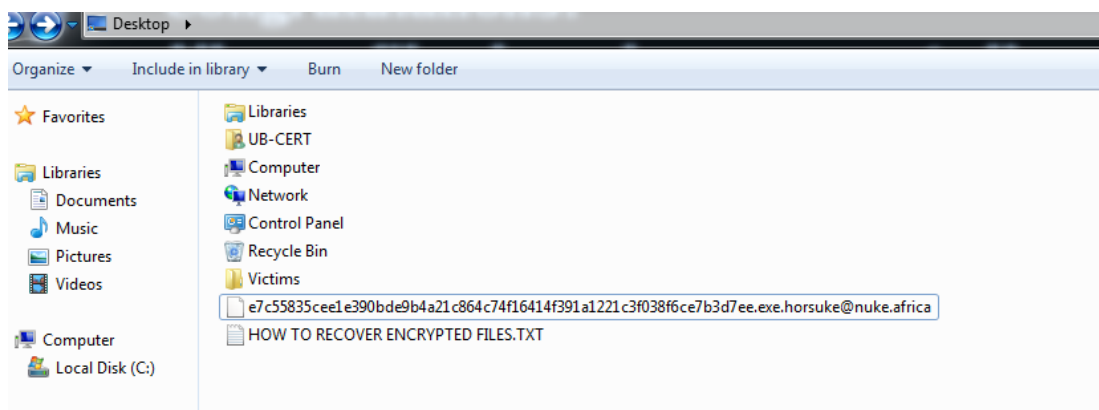
[Request Payment](#) [Donation Button](#)



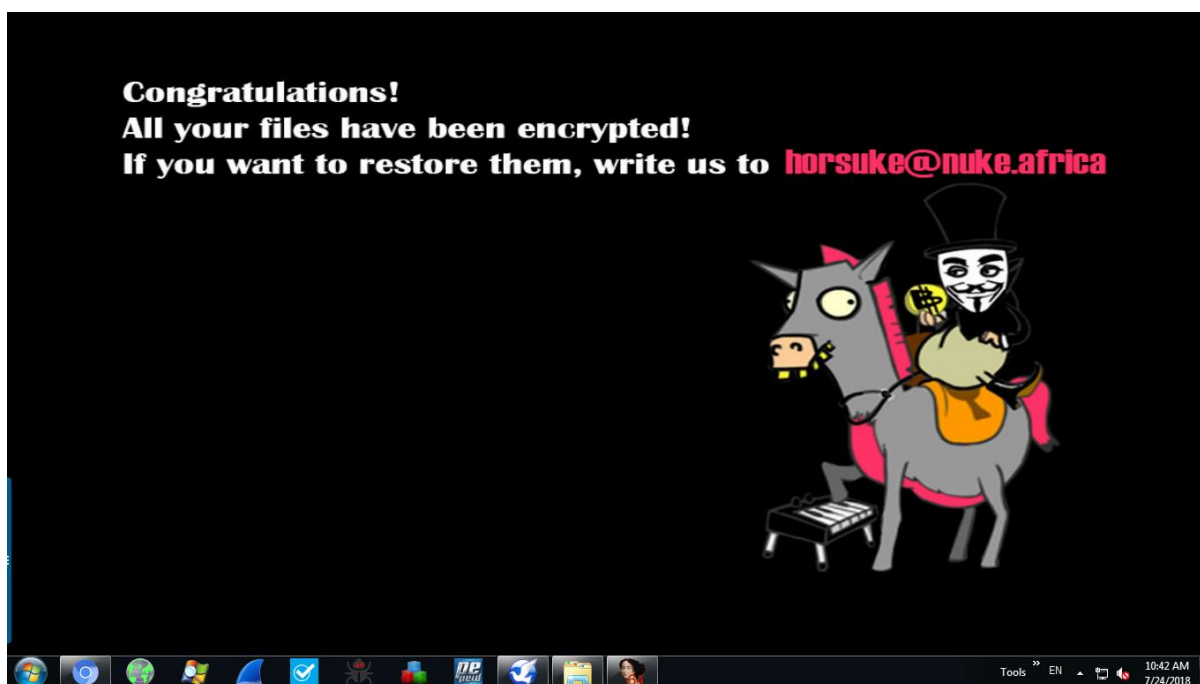
همانطور که اشاره شد، باج‌افزار Horsuke پس از رمزگذاری پسوند horsuke@nuke.africa را به انتهای فایل‌های رمزگذاری شده اضافه می‌کند. تصویر زیر نشان‌دهنده فایل‌های رمزگذاری شده توسط این باج‌افزار می‌باشد:

Name	Date modified	Type	Size
Print Form_files	7/25/2018 1:53 PM	File folder	
lpd.info.horsuke@nuke.africa	12/26/2006 8:12 PM	AFRICA File	3 KB
1 (1).bmp.horsuke@nuke.africa	2/21/2011 6:32 AM	AFRICA File	1,244 KB
1 (4).png.horsuke@nuke.africa	1/31/2015 11:44 AM	AFRICA File	199 KB
1 (46).jpg.horsuke@nuke.africa	2/10/2014 11:46 AM	AFRICA File	327 KB
1.pot.horsuke@nuke.africa	11/15/2016 1:25 PM	AFRICA File	242 KB
2 O'clock Spotlight.ple	5/29/2015 1:05 AM	PLE File	22 KB
03_01_layout.mov.horsuke@nuke.africa	11/7/2015 9:23 PM	AFRICA File	10,073 KB
4_5854862790426099907.mp4.horsuke@n...	9/17/2017 8:07 AM	AFRICA File	1,420 KB
73 - www.farsbooks.mihanblog.com.rar...	1/1/2017 8:28 PM	AFRICA File	984 KB
adlink_7582.html.horsuke@nuke.africa	11/30/2015 12:31 ...	AFRICA File	1 KB
adsutil.vbs.horsuke@nuke.africa	8/22/2013 7:25 PM	AFRICA File	15 KB
analytics.js.horsuke@nuke.africa	11/30/2015 12:31 ...	AFRICA File	26 KB
AppLocker.psd1	6/18/2013 4:59 PM	PSD1 File	2 KB
AppxBlockMap.xml.horsuke@nuke.africa	5/13/2018 9:58 PM	AFRICA File	1 KB
bb.jpeg.horsuke@nuke.africa	9/24/2015 11:40 AM	AFRICA File	1,540 KB
BEH AARAMI.PPt.horsuke@nuke.africa	1/8/2011 6:15 PM	AFRICA File	535 KB
berme.doc.horsuke@nuke.africa	1/8/2011 6:15 PM	AFRICA File	129 KB
Block.bat	7/20/2016 2:55 AM	Windows Batch File	2 KB
Block.class.horsuke@nuke.africa	4/8/2012 1:49 PM	AFRICA File	3 KB
block.xsd.horsuke@nuke.africa	6/18/2013 4:55 PM	AFRICA File	2 KB
BLOCK_SF.TTF	5/26/2002 4:21 AM	TrueType font file	166 KB
block-flashsubdoc-digest256.pset	12/5/2017 11:02 AM	PSET File	1 KB
BlockingHttpServer.java.horsuke@nuke.a...	2/11/2018 8:35 AM	AFRICA File	14 KB
blocklist-gfx.json.horsuke@nuke.africa	12/4/2016 11:37 PM	AFRICA File	28 KB
clock.ico.horsuke@nuke.africa	7/29/2004 3:42 PM	AFRICA File	159 KB
CloudConnecti...	12/27/2012 3:01 PM	VUE File	1 KB

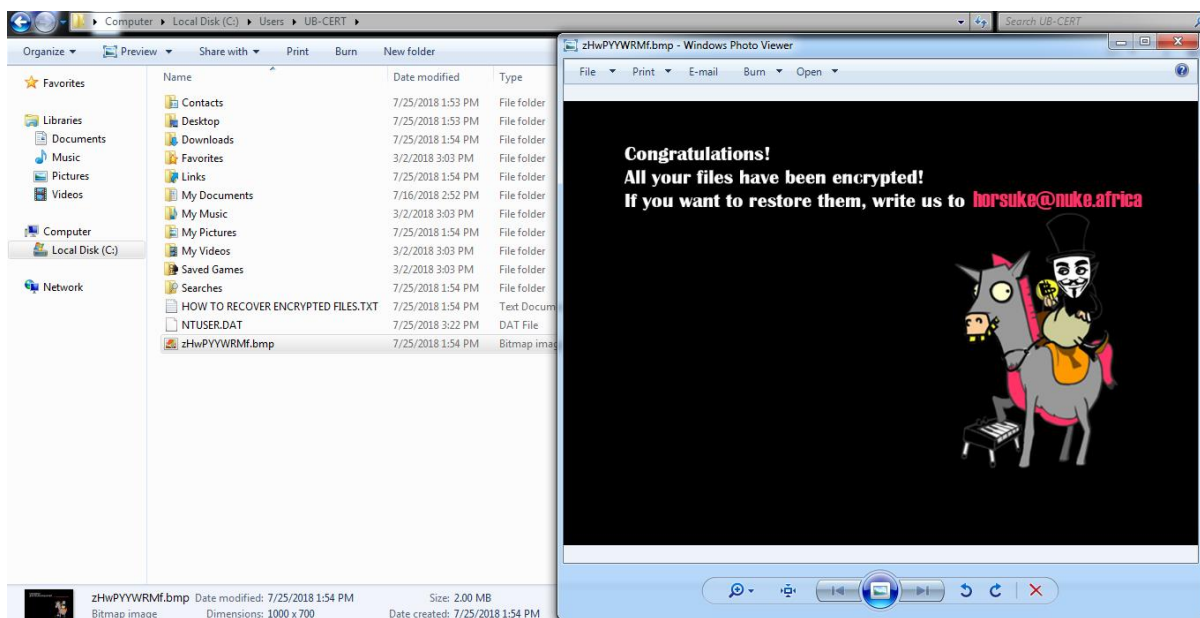
طبق مشاهدات صورت گرفته، باج افزار فایل اجرایی خود را نیز رمزگذاری می کند :



در ادامه، تصویر پس زمینه توسط باج افزار تغییر پیدا می کند.



باج افزار در این تصویر ضمن تبریک و اعلام رمزگذاری فایل های قربانی، ایمیلی به آدرس horsuke@nuke.africa را به قربانی معرفی می کند. فایل این تصویر به نام zHwPYYWRMf.bmp در فولدر users در درایو اصلی سیستم قربانی قرار گرفته است.



در تصاویر زیر فایل های اضافه شده و تغییر یافته در مسیر درایو سیستم عامل و پوشه Windows را مشاهده می کنید :

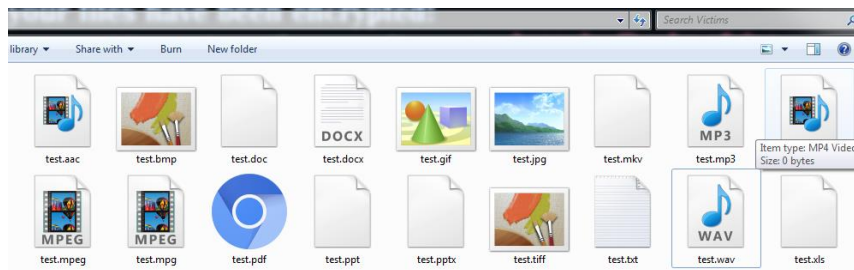
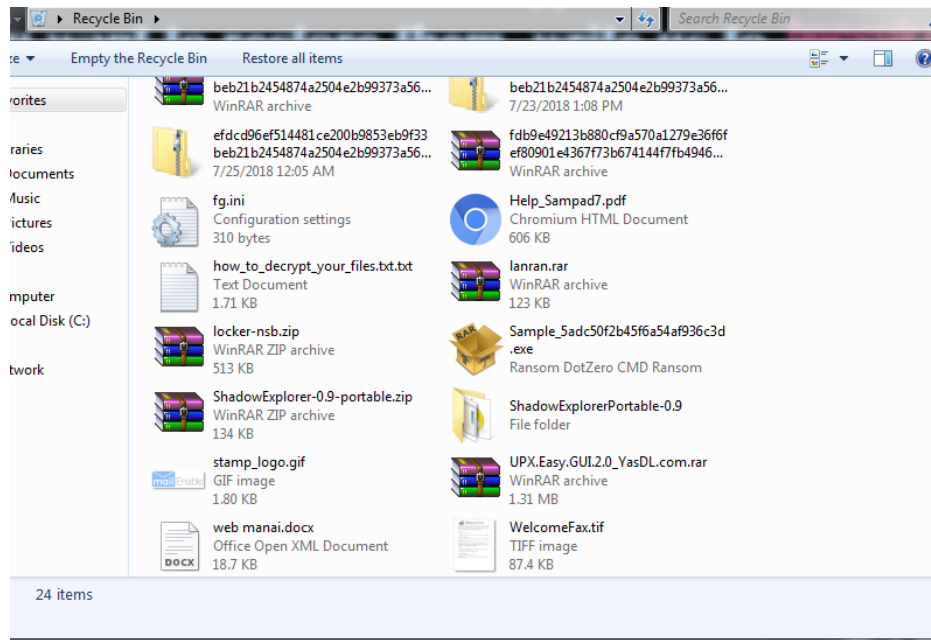
Name	Date modified	Type	Size
~res-x64.txt	7/24/2018 10:52 PM	Text Document	1,596 KB
Ocejhapo	7/24/2018 10:43 PM	File	1 KB
jusched.log	7/24/2018 11:10 AM	Text Document	185 KB
wmplog05.sqm	7/22/2018 5:54 PM	SQM File	2 KB
~DF03E88E05DAA400E1.TMP	7/18/2018 1:08 AM	TMP File	0 KB
~DF185DF0FF34507614.TMP	7/18/2018 1:08 AM	TMP File	0 KB
wmplog04.sqm	7/18/2018 12:18 AM	SQM File	2 KB
wmplog03.sqm	7/18/2018 12:13 AM	SQM File	2 KB
wmplog02.sqm	7/18/2018 12:12 AM	SQM File	2 KB
wmplog01.sqm	7/18/2018 12:10 AM	SQM File	2 KB
wmplog00.sqm	7/18/2018 12:10 AM	SQM File	1 KB
wmsetup.log	7/18/2018 12:10 AM	Text Document	5 KB
dd_Setup_decompression_log.txt	6/10/2018 1:34 PM	Text Document	2 KB
Microsoft .NET Framework 4.7.1 Setup_2...	6/10/2018 1:34 PM	Chromium HTML ...	957 KB
dd_SetupUtility.txt	6/10/2018 1:34 PM	Text Document	5 KB
Microsoft .NET Framework 4.7.1 Setup_2...	6/10/2018 1:33 PM	Text Document	16,843 KB
ASPNETSetup_00003.log	6/10/2018 1:29 PM	Text Document	3 KB
ASPNETSetup_00002.log	6/10/2018 1:29 PM	Text Document	5 KB
RGIF384.tmp	6/10/2018 1:29 PM	TMP File	11 KB
RGIF384.tmp-tmp	6/10/2018 1:29 PM	TMP-TMP File	9 KB
dd_wcf_CA_smci_20180610_085857_442.txt	6/10/2018 1:28 PM	Text Document	3 KB
dd_wcf_CA_smci_20180610_085850_133.txt	6/10/2018 1:28 PM	Text Document	5 KB
Microsoft .NET Framework 4.7.1 Setup_2...	6/10/2018 1:21 PM	Chromium HTML ...	1,050 KB
tmp-ht8.xpi	6/10/2018 1:07 PM	XPI File	1,608 KB
Dgiwueto	6/9/2018 10:38 PM	File	6 KB
Snagit_12_20180304232743.log	3/4/2018 11:29 PM	Text Document	20 KB

3 items selected Date modified: 7/24/2018 10:52 PM Date created: 3/2/2018 4:09 PM - 7/24/2018 10:52 PM
Size: 1.73 MB

Name	Date modified	Type	Size
StructuredQuery.log	3/2/2018 3:23 PM	Text Document	1 KB
dd_wcf_CA_smci_20180302_115250_882.txt	3/2/2018 3:22 PM	Text Document	7 KB
dd_wcf_CA_smci_20180302_115252_582.txt	3/2/2018 3:22 PM	Text Document	3 KB
bch59BD.tmp	3/2/2018 3:22 PM	TMP File	0 KB
vminst.log	3/2/2018 3:04 PM	Text Document	147 KB
vmmsi.log_20180302_150456.log	3/2/2018 3:04 PM	Text Document	3,315 KB
FXSAPIDebugLogFile.txt	3/2/2018 3:03 PM	Text Document	0 KB
dd_vcredistMSI4668.txt	3/2/2018 3:03 PM	Text Document	412 KB
dd_vcredistUI4668.txt	3/2/2018 3:03 PM	Text Document	12 KB
dd_vcredistMSI4627.txt	3/2/2018 3:03 PM	Text Document	424 KB
dd_vcredistUI4627.txt	3/2/2018 3:03 PM	Text Document	12 KB
UB-CERT.bmp	3/2/2018 3:03 PM	Bitmap image	49 KB
unattend.cmd	3/2/2018 2:48 PM	Windows Comma...	1 KB
storePwd.exe	3/2/2018 2:48 PM	Application	63 KB
storePwd.ini	3/2/2018 2:48 PM	Configuration sett...	1 KB
upgrader.exe	3/2/2018 2:48 PM	Application	595 KB
hspferdata_UB-CERT	7/25/2018 10:28 AM	File folder	
WPDNSE	7/25/2018 10:22 AM	File folder	
FlashBackBackup	7/16/2018 2:54 PM	File folder	
FlashBackTemp	7/16/2018 2:54 PM	File folder	
FTSuploadAgentTemp	7/16/2018 2:52 PM	File folder	
{cffaad72-47bd-4c5e-9d60-f5ef5ce4faf1}	3/2/2018 3:54 PM	File folder	
Microsoft Visual C++ 2010 x86 Redistrib...	3/2/2018 3:27 PM	File folder	
Microsoft Visual C++ 2010 x64 Redistrib...	3/2/2018 3:27 PM	File folder	
vmware-UB-CERT	3/2/2018 3:09 PM	File folder	
KLUDA57.tmp.dir	3/2/2018 3:04 PM	File folder	
Low	3/2/2018 3:02 PM	File folder	

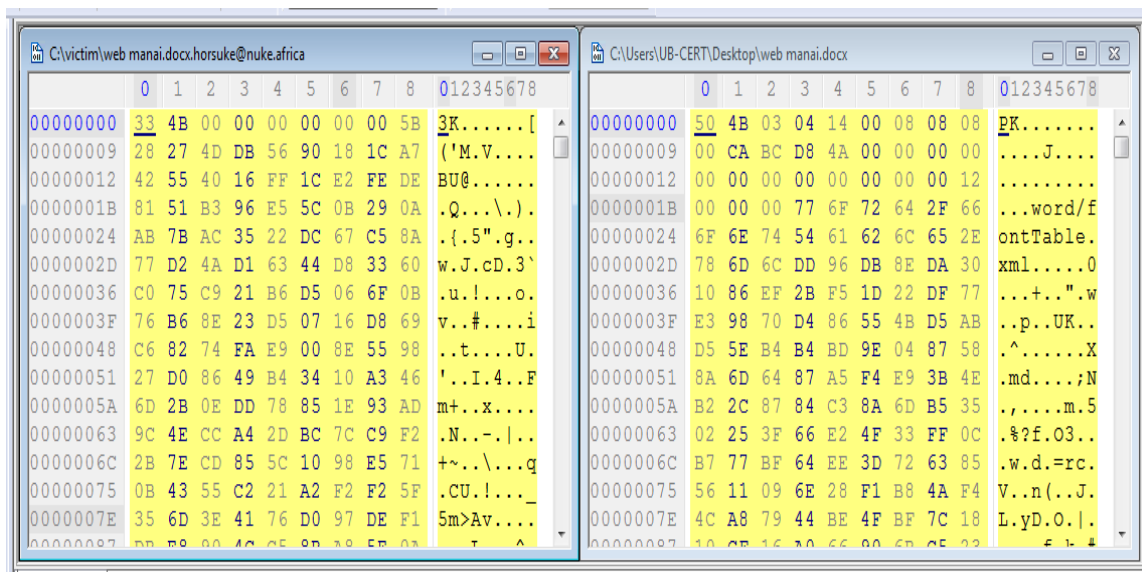
2 items selected Date modified: 7/25/2018 10:22 AM

طبق بررسی های صورت گرفته، محتویات Recycle bin و فایل های فاق محتوا (با حجم ۰ بایت) توسط باج افزار رمزگذاری نمی شوند.



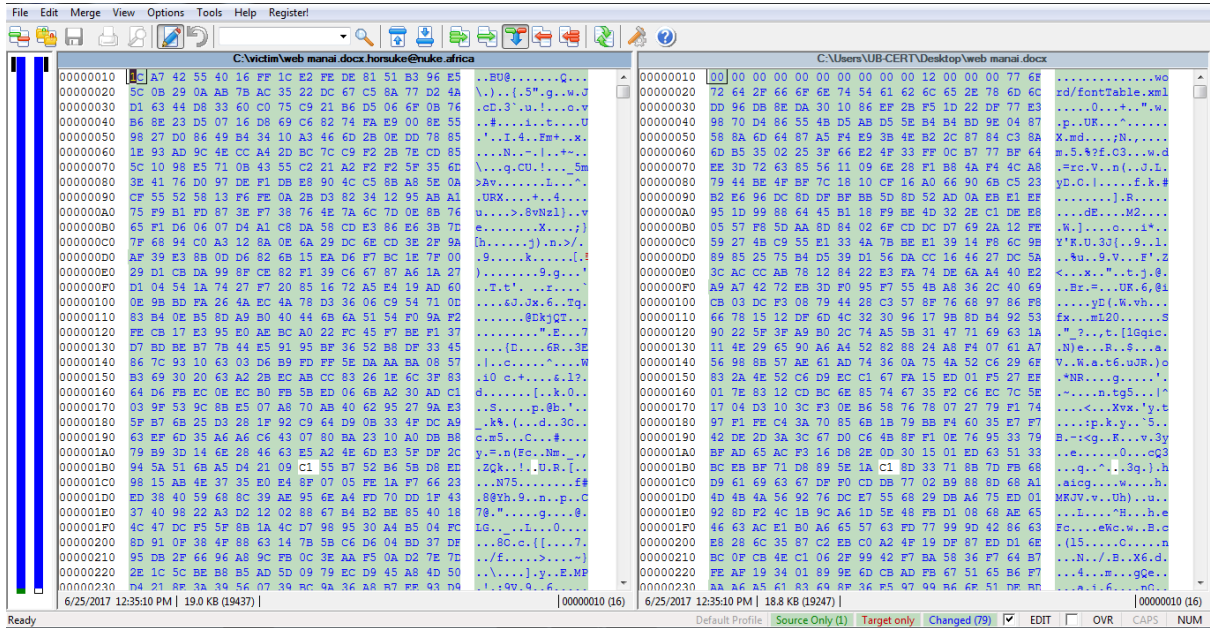
تحلیل ایستا:

پس از تحلیل کد باج افزار Horsuke به نتایج زیر دست پیدا کردیم.



نمونه فایل قبل و بعد از رمزگذاری

بیش از دوبرابر محتوای اولیه حجم افزوده شده است.



تعداد بایت های جایگزین شده نمونه فایل بعد از رمز گذاری:

Type	Source	Count	Count	Target	Count	Count
Replaced	00000000	19437	4BED	00000000	19247	4B2F

قطعه کد دریافت زمان محلی سیستم قربانی :

```

:004061E4 ; ===== SUBROUTINE =====
:004061E4 ; Attributes: thunk
:004061E4 ; void __stdcall GetLocalTime(LPSYSTEMTIME lpSystemTime)
:004061E4 GetLocalTime proc near ; CODE XREF: sub_40CEAC+8+p
:004061E4 ; sub_40CED8+4+p
:004061E4 lpSystemTime = dword ptr 4
:004061E4 jmp ds: __imp_GetLocalTime
:004061E4 GetLocalTime endp
:004061E4 ;
:004061EA align 4
:004061EC ; [00000006 BYTES: COLLAPSED FUNCTION GetLocaleInfoA_0. PRESS CTRL-NUMPAD+ TO EXPAND]
:004061F2 align 4
:004061F4 ; [00000006 BYTES: COLLAPSED FUNCTION GetModuleFileNameA_0. PRESS CTRL-NUMPAD+ TO EXPAND]
:004061FA align 4
:004061FC ; [00000006 BYTES: COLLAPSED FUNCTION GetModuleFileNameW. PRESS CTRL-NUMPAD+ TO EXPAND]
000055E4 00000000004061E4: GetLocalTime (Synchronized with Hex View-1)

```

کلید رجیستری اضافه شده:

HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\zHwPYYWRMf

مقادیر اضافه شده:

HKU\DEFAULT\Software\Classes\Local
Settings\MuiCache\22\52C64B7E\@C:\Windows\system32\MCTRes.dll,-200005: "Websites for United
States"
HKU\DEFAULT\Software\Classes\Local
Settings\MuiCache\22\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites Bar"
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Program Files\Common
Files\system\wab32res.dll,-10100: "Contacts"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\iPointSize:
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfCharSet:
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfWeight:
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfItalic:
HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Notepad\lfUnderline:
HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Notepad\lfOrientation:
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Notepad\lfStrikeOut:
HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Notepad\lfFaceName: "Fixedsys"
HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA}\Count\{P:\Hfref\HO-
PREG\Qrfxgbc\r7p55835pr1r390oqr9o4n21p864p74s16414s391n1221p3s038s6pr7o3q7rr.rkr:
HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Windows\CurrentVersion\Run\zHwPYYWRMf: "notepad.exe "C:\Users\UB-
CERT\HOW TO RECOVER ENCRYPTED FILES.TXT"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\zHwPYYWRMf\idle: "1"
HKU\S-1-5-18\Software\Classes\Local
Settings\MuiCache\22\52C64B7E\@C:\Windows\system32\MCTRes.dll,-200005: "Websites for United
States"
HKU\S-1-5-18\Software\Classes\Local
Settings\MuiCache\22\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites Bar"
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\22\52C64B7E\@C:\Program Files\Common
Files\system\wab32res.dll,-10100: "Contacts"

کلیدهای رجیستری تغییر یافته:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{D4546416-77DE-4750-
923A-1ED584EB8218}\DateLastConnected
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter
HKLM\SOFTWARE\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{47047898-
1E6D-11E8-878B-806E6F6E6963}: "70564856"
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Perflib\009\Counter

```
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Perflib\CurrentLanguage\Counter
HKLM\SYSTEM\ControlSet001\services\SharedAccess\Epoch\Epoch:
HKLM\SYSTEM\ControlSet001\services\SharedAccess\Epoch2\Epoch:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\LeaseObtainedTime:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\T1:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\T2:
HKLM\SYSTEM\ControlSet001\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\LeaseTerminatesTime:
HKLM\SYSTEM\ControlSet001\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-
806e6f6e6963}DeleteProcess (Leave):
HKLM\SYSTEM\RNG\Seed
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Epoch\Epoch:
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Epoch2\Epoch:
HKLM\SYSTEM\CurrentControlSet\services\SharedAccess\Epoch2\Epoch:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\LeaseObtainedTime: 0x5B5DBD3A
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\LeaseObtainedTime: 0x5B5DC803
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\T1:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\T2:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\T2:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\LeaseTerminatesTime:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\LeaseTerminatesTime:
HKLM\SYSTEM\CurrentControlSet\services\Tcpip\Parameters\Interfaces\{8167A8F1-246C-4A44-8F56-
D71BA9D2C1D3}\DhcpInterfaceOptions:
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-
806e6f6e6963}DeleteProcess (Enter)
HKLM\SYSTEM\CurrentControlSet\services\VSS\Diag\VolSnap\Volume{47047898-1e6d-11e8-878b-
806e6f6e6963}DeleteProcess (Leave )
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\WallpaperStyle:
"10"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\WallpaperStyle:
"2"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\Wallpaper:
"C:\Users\UB-CERT\AppData\Roaming\Microsoft\Windows\Themes\TranscodedWallpaper.jpg"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Control Panel\Desktop\Wallpaper:
"C:\Users\UB-CERT\zHwPYYWRMf.bmp"
```

```

HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA}\Count\HRZR_PGYFRFFVBA
HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA}\Count\{S380S404-1Q43-42s2-9305-67QR0028SP23}\rkybere.rkr:
HKU\S-1-5-21-2853862532-1823478465-2883723831-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA}\Count\P:\ertfubg_1.8.3_orgn1_jva32_k64\ertfubg_k64.rkr
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).x:
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).y
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local
Settings\Software\Microsoft\Windows\Shell\BagMRU\MRUListEx
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local
Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).x: 0xFFFF8300
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000_Classes\Local
Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1162x591x96(1).y: 0xFFFFFFFF:

```

این باج افزار از کتابخانه های ویندوزی به همراه توابعی از هر کدام از کتابخانه ها استفاده می کند که در جدول زیر قابل مشاهده است :

advapi۳۲.dll	kernel۳۲.dll	kernel۳۲.dll	kernel۳۲.dll	oleaut۳۲.dll
RegDeleteKeyA	GetLastError	GetTickCount	FindNextFileW	VariantChangeType
RegCloseKey	GetEnvironmentVariable	GetThreadLocale	GetLocaleInfoA	SafeArrayGetLBound
RegQueryValueExA	A	GetVersionExA	LocalAlloc	SafeArrayPtrOfIndex
RegSetValueExA	GetStdHandle	GlobalUnlock	OpenProcess	SysAllocStringLen
RegEnumValueA	FileTimeToDosDateTime	GetModuleFileNameA	LockResource	VariantClear
RegCreateKeyExA	IstrlenA	GlobalHandle	SetFileTime	SafeArrayCreate
RegOpenKeyExA	GetModuleFileNameW	RtlUnwind	GetCommandLineW	SysReAllocStringLen
RegDeleteValueA	GlobalFree	LoadLibraryA	CreateThread	SafeArrayGetUBound
RegEnumKeyExA	WaitForSingleObject	WinExec	UnhandledExceptionFilter	VariantCopy
	FreeLibrary	CreateProcessW		SysFreeString
	QueryPerformanceCounter	DeleteCriticalSection	MultiByteToWideChar	VariantInit
	EnterCriticalSection	GetStartupInfoA	GetLocalTime	
		GetDateFormatA	GetCPInfo	
		LoadLibraryExA	GetCommandLineA	
		SizeofResource	GetProcAddress	

shell۳۲.dll	user۳۲.dll	wininet.dll	kernel۳۲.dll	kernel۳۲.dll
SHGetMalloc	CharLowerBuffW	InternetReadFile	EnumCalendarInfoA	FormatMessageA
ShellExecuteW	GetSystemMetrics	InternetOpenUrlA	ReadFile	OpenMutexA

SHGetPathFromIDListW SHGetSpecialFolderLocation	GetLastInputInfo LoadStringA DispatchMessageA CharLowerBuffA SystemParametersInfoW CharToOemA CharNextA CharUpperBuffA MessageBoxA PeekMessageA TranslateMessage CharNextW GetKeyboardType DestroyWindow	InternetCloseHandle InternetOpenA	IstrcpynA FindFirstFileW GetACP GetDiskFreeSpaceA GlobalLock FreeResource GlobalAlloc TerminateProcess CreateProcessA FileTimeToLocalFileTime InitializeCriticalSection LoadResource CreateFileW VirtualQuery VirtualFree FindClose TlsGetValue Sleep MoveFileW SetFileAttributesW TlsSetValue CloseHandle ExitProcess GetCurrentThreadId FindResourceA VirtualAlloc DeleteFileW LeaveCriticalSection	CreateMutexA SetFilePointer RaiseException CompareStringA WideCharToMultiByte GetFileAttributesA GetModuleHandleA CreatePipe FindFirstFileA SetEndOfFile GlobalReAlloc WriteFile
--	---	--------------------------------------	--	---

```

004452D8 _bss          ends
004452D8
a:004463B4 ;
a:004463B4 ; Imports from oleaut32.dll
a:004463B4 ;
a:004463B4 ; Section 5. (virtual address 00046000)
a:004463B4 ; Virtual size           : 000010EC ( 4332.)
a:004463B4 ; Section size in file      : 00001200 ( 4608.)
a:004463B4 ; Offset to raw data for section: 0003D400
a:004463B4 ; Flags C000040: Data Readable Writable
a:004463B4 ; Alignment      : default
a:004463B4 ; =====
a:004463B4
a:004463B4 ; Segment type: Externs
a:004463B4 ; _idata
a:004463B4 ; void __stdcall SysFreeString(BSTR bstrString)
a:004463B4 ;             extrn __imp_SysFreeString:dword
a:004463B4 ;             ; DATA XREF: SysFreeString↑r
a:004463B8 ; INT __stdcall SysReAllocStringLen(BSTR *pbstr, const OLECHAR *psz, unsigned int len)
a:004463B8 ;             extrn __imp_SysReAllocStringLen:dword
a:004463B8 ;             ; DATA XREF: SysReAllocStringLen↑r
a:004463BC ; BSTR __stdcall SysAllocStringLen(const OLECHAR *strIn, UINT ui)
a:004463BC ;             extrn imp_SysAllocStringLen:dword
0003D400 00000000004463B4: .idata:__imp_SysFreeString (Synchronized with Hex View-1)

```

بر اساس بررسی‌های صورت گرفته، باج‌افزار Horsuke پس از اجرا، فرایندهای زیر را ایجاد می‌کند:

- [HonestSample_0afd4a909931360644caeb88.exe](#) (PID: 3688)
 - [cmd.exe](#) /c copy /y "C:\HonestSample_0afd4a909931360644caeb88.exe" "%APPDATA%\winlogon.exe" (PID: 3968)
 - [HonestSample_0afd4a909931360644caeb88.exe](#) runas (PID: 3292)

- [cmd.exe](#) /c copy /y
"C:\HonestSample_٥afd٤a٩٥٩٩٣١٣٦٥٦٤٤caeb٨٨.exe"
"%APPDATA%\winlogon.exe" (PID: ٢٣٢٤)
- [winlogon.exe](#) (PID: ١٢٧٢)
 - [mshta.exe](#) "javascript:o=new
ActiveXObject('WScript.Shell');x=new
ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{i=x.GetFile('winlogon.exe').Path;o.RegWrite('HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\RunOnce\\zh
wPYWRF',i);}catch(e){},١٠);" (PID: ٣٦٩٦)
 - [mshta.exe](#) "javascript:eval(new
ActiveXObject('WScript.Shell').RegRead('HKCU\\Software\\MC
DVV\\TOFLK'));close();" (PID: ١٩٢٨)
 - [cmd.exe](#) /c wadmin DELETE SYSTEMSTATEBACKUP -
keepVersions:٠ (PID: ٢٧٧٢)
 - [wbadmin.exe](#) wbadmin DELETE
SYSTEMSTATEBACKUP -keepVersions:٠ (PID:
٣٣٧٦)
 - [cmd.exe](#) /c wmic SHADOWCOPY DELETE (PID: ٤٦٤)
 - [WMIC.exe](#) wmic SHADOWCOPY DELETE (PID:
٣٧٢٤)
 - [cmd.exe](#) /c vssadmin Delete Shadows /All /Quiet (PID:
٢٤٩٢)
 - [vssadmin.exe](#) vssadmin Delete Shadows /All
/Quiet (PID: ٢٩٣٦)
 - [cmd.exe](#) /c bcdedit /set {default} recoveryenabled No
(PID: ٤٣٢)
 - [bcdedit.exe](#) bcdedit /set {default}
recoveryenabled No (PID: ٣٦٤٤)
 - [cmd.exe](#) /c bcdedit /set {default} bootstatuspolicy
ignoreallfailures (PID: ٣٠٢٤)
 - [bcdedit.exe](#) bcdedit /set {default}
bootstatuspolicy ignoreallfailures (PID: ٢٢٤٠)
 - [~wtmپ٠٠١.exe](#) (PID: ٢٣٩٢)
 - [walm.exe](#) (PID: ١٠٤٨)
 - [cmd.exe](#) /c start /max notepad.exe "%USERPROFILE%\HOW
TO RECOVER ENCRYPTED FILES.TXT" (PID: ٣٢٢٠)
 - [notepad.exe](#) "%USERPROFILE%\HOW TO RECOVER
ENCRYPTED FILES.TXT" (PID: ٢٥٥٦)
 - [mshta.exe](#) "javascript:o=new
ActiveXObject('Scripting.FileSystemObject');setInterval(function(){try{o.DeleteFile('winlogon.exe');close()}catch(e){},١٠);"
(PID: ٣٢١٢)

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار Horsuke نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۵۳ مورد از ۶۷ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج‌افزار بوده و آن را حذف یا غیرفعال می‌کنند.



Kaspersky	⚠️ HEUR:Trojan-Ransom.Win32.Generic	Malwarebytes	⚠️ Ransom.Horsuke
MAX	⚠️ malware (ai score=99)	McAfee	⚠️ GenericRXDM-JB!DE8D979884EE
McAfee-GW-Edition	⚠️ BehavesLike.Win32.Generic.gc	Microsoft	⚠️ Ransom:Win32/Higuniel.A
NANO-Antivirus	⚠️ Trojan.Win32.Filecoder.fbyqbw	Palo Alto Networks	⚠️ generic.ml
Panda	⚠️ Trj/GdSda.A	Qihoo-360	⚠️ Win32/Trojan.Ransom.793
SentinelOne	⚠️ static engine - malicious	Sophos AV	⚠️ Mal/Generic-S
Sophos ML	⚠️ heuristic	Symantec	⚠️ Trojan.Gen.2
Tencent	⚠️ Win32.Trojan.Generic.Wurd	TrendMicro	⚠️ Ransom_HORSUKE.THEAGAH
TrendMicro-HouseCall	⚠️ Ransom_HORSUKE.THEAGAH	VBA32	⚠️ BScope.Trojan.Encoder
VIPRE	⚠️ Trojan.Win32.Generic!BT	ViRobot	⚠️ Trojan.Win32.Z.Ransom.412160
Yandex	⚠️ Trojan.Filecoder!4ozwfU+5bfY	Zillya	⚠️ Trojan.Filecoder.Win32.7754
ZoneAlarm	⚠️ HEUR:Trojan-Ransom.Win32.Generic	Antiy-AVL	✅ Clean
Ad-Aware	⚠️ DeepScan:Generic.Ransom.Amnesia.4...	AegisLab	⚠️ Troj.Ransom.W32lc
AhnLab-V3	⚠️ Trojan/Win32.Ransom.C2527025	ALYac	⚠️ Trojan.Ransom.Scarab
Arcabit	⚠️ DeepScan:Generic.Ransom.Amnesia.4...	Avast	⚠️ FileRepMalware
AVG	⚠️ FileRepMalware	Avira	⚠️ TR/Dropper.Gen
AVware	⚠️ Trojan.Win32.Generic!BT	Baidu	⚠️ Win32.Trojan.WisdomEyes.16070401....
BitDefender	⚠️ DeepScan:Generic.Ransom.Amnesia.4...	CAT-QuickHeal	⚠️ Trojan.Higuniel
ClamAV	⚠️ Win.Ransomware.Scarab-6336012-1	Comodo	⚠️ TrojWare.Win32.TrojanDownloader.De...
CrowdStrike Falcon	⚠️ malicious_confidence_100% (W)	Cybereason	⚠️ malicious.884eec
Cylance	⚠️ Unsafe	Cyren	⚠️ W32/Trojan.MNYA-8045
DrWeb	⚠️ Trojan.Encoder.11464	Emsisoft	⚠️ DeepScan:Generic.Ransom.Amnesia.4... (B)
Endgame	⚠️ malicious (high confidence)	eScan	⚠️ DeepScan:Generic.Ransom.Amnesia.4...
ESET-NOD32	⚠️ a variant of Win32/Filecoder.FS	F-Secure	⚠️ DeepScan:Generic.Ransom.Amnesia.4...
Fortinet	⚠️ W32/Msht.GJ!tr	GData	⚠️ DeepScan:Generic.Ransom.Amnesia.4...
Ikarus	⚠️ Trojan-Ransom.FileCoder	Jiangmin	⚠️ Trojan.Generic.ccfmz
K7AntiVirus	⚠️ Trojan (004f6e981)	K7GW	⚠️ Trojan (004f6e981)

خروجی سامانه ویروس کاو مرکز ماهر :

نام فایل: e7c55835cee1e390bde9b4a21c864c74f16414f391a1221c3f038f6ce7b3d7ee.exe پرینت

حجم فایل: ۴۰۳ کیلوبایت

تاریخ اسکن: ۶ مرداد ۱۳۹۷ - ۱۲:۰۴

MD5: de8d979884eec2cef5ded628eef4290c

SHA1: 06eedbb498962aa17a53a712e59e19fffd7cd8d

SHA256: e7c55835cee1e390bde9b4a21c864c74f16414f391a1221c3f038f6ce7b3d7ee

وضعیت: 

نتیجه اسکن	نسخه آنتی ویروس	آنتی ویروس
Malware: Malware.Subld.127805343	ii	2.3.190.2675 پادویش
Clean	✓	9.14.2 sophos
Dangerous: Trojan.Ransom.BYN	ii	11.00 f_secure
Suspicious: HEUR:Trojan-Ransom.Win32.Generic	i	5.5 kaspersky
Dangerous: Win32/Filecoder.FS	ii	4.5.3.38123 eset
Dangerous: Trojan.Encoder.11464	ii	11.0.1.1607061217 drweb
Dangerous: Win.Ransomware.Scarab-6336012-1	ii	0.99.2 clam_av
Dangerous: TrojWare.Win32.TrojanDownloader.Delf.Gen	ii	1.1.268025.1 comodo
Dangerous: Trojan.Ransom.BYN	ii	11.0.1.18 bitdefender
Clean	✓	2.1.2 avast
Dangerous: Trojan.Gen.2	ii	7.9.0.30 symantec