باسمه تعالى

تحليل فنى باجافزار Ryuk





مقدمه :

مشاهده و رصد فضای سایبری در زمینه باجافزار، از شروع فعالیت نمونه جدیدی به نام Ryuk خبر می دهد. این باج افزار از ترکیب کد های Hermes و پیغام متنی اولین نسخه Bitpaymer ایجاد شده است. جامعه هدف آن شرکت های بزرگ ایالت متحده ی آمریکا بوده که باجگیر مبلغ باج بالایی را نیز خواهان است. این باج افزار دو پیغام باج خواهی داشته که کاربر یکی از آن ها را دریافت میکند. یکی طولانی تر ،خوش بیان تر وخوش تعبیرتر که خواهان مبلغ باج بالاتر یعنی ۵۰ بیت کوین است و دیگری کوتاه تر و رُک تر که مبلغی بین ۱۵ تا ۳۵ بیت کوین را پیشنهاد می دهد که هنوز جای سوال باقیست که چگونه برای فرستادن بین دو پیغام باج خواهی به قربانی تصمیم میگیرد! همچنین این باج افزار قربانیان خود را با دانش و هدف قبلی انتخاب میکند و طی دو هفته مبلغ بسیاری باج را بدست آورده و جزو باج افزارهای خطرناک انتخاب شده است. این باج افزار پس از رمزگذاری فایل ها پسوندی را به انتهای فایل های رمزگذاری شده اضافه نمی کند. بررسیها نشان می دهد که فعالیت این باج افزار دراواسط ماه آگوست سال ۲۰۱۸ میلادی شروع شده است. این باج افزار از الگوریتم رمزنگاری AES + RSA استفاده می کند.

مشخصات فایل اجرایی :

۲۳f٨aa٩٤ffb٣c٠٨a٦٢٧٣٥fe٧fee٥٧٩٩٨٨٠a٨f٣٢٢ce١d٥٥ec٤٩a١٣a٣f٨٥٣١٢db٢.exe ۲۱۰.exe.bin ryuk.exe	نام فايل
°ac·f·°·f٩٣f٨٦e٦٩·٢٦faea١fbb٤٤٥٠	MD٥
۹۷،۹۷۷٤fde٩ec٧٤.ad٦fed٨ed٧٩٩.٣٢٩٦ca٩d٥٧١	SHA-1
<pre>**fhaa%*ffb**c+haitv**ofe*feeov%%%%%+aAf***ceidooec*%ai*a*fAo***db*</pre>	SHA-۲٥٦
κνε KB	اندازه فايل
Microsoft Visual C++ A	کامپایلر / پکر

اندازه خام	اندازه مجازی	آدرس مجازی	آنتروپي	نام بخش
٤٤٥٤٤	22271	٤٠٩٦	٦.٦١	.text
22.5.	77707	29107	٤.٨٩	.rdata
۳۲۰۰۰	37077	VTVYA	٦.٢	.data
017	۱۸۰	341417	١.٤٦	.gfids

فایل اجرایی این باجافزار دارای پنج بخش است :





مركزماهر

تصویر ۱ تشابه کد Ryuk با باج افزار Hermes





1 Result Ryuk

This ransomware has no known way of decrypting data at this time.
 It is recommanded to back up your operated files, and have for a

It is recommended to backup your encrypted files, and hope for a solution in the future.

ransomnote_email: WayneEvenson@tutanota.com

Click here for more information about Ryuk

A Would you like to be notified if there is any development regarding this ransomware? Click here.

تحليل پويا :

برای بررسی عمیقتر باجافزار Ryuk فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باجافزار را از نزدیک مورد بررسی قرار دهیم.

در دو تصویر زیر وضعیت فرآیندها قبل و بعد از آلودگی را مشاهده میکنید.باج افـزار Ryuk بـا اسـتفاده از task kill فرآیندهای زیادی را از بین می برد از جملـه پایگـاه هـای داده، پشـتیبان هـا، آنتـی ویـروس هـا و نرمافزارهای ویرایش اسناد.





Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	89.55	0 K	24 K	0		
🖃 📰 System	4.09	128 K	780 K	4		
Interrupts	1.14	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		436 K	1,128 K	252	Windows Session Manager	Microsoft Corporation
CSrss.exe		1,996 K	4,476 K	332	Client Server Runtime Process	Microsoft Corporation
🖃 🔳 wininit.exe		1,432 K	4,328 K	384	Windows Start-Up Application	Microsoft Corporation
services.exe		5,476 K	9,480 K	488	Services and Controller app	Microsoft Corporation
svchost.exe		4,348 K	9,632 K	596	Host Process for Windows S	Microsoft Corporation
WmiPrvSE.exe		8,744 K	14,396 K	2648	WMI Provider Host	Microsoft Corporation
WmiPrvSE.exe		2,628 K	6,456 K	3272	WMI Provider Host	Microsoft Corporation
vmacthlp.exe		1,428 K	4,096 K	660	VMware Activation Helper	VMware, Inc.
svchost.exe		4,496 K	8,800 K	704	Host Process for Windows S	Microsoft Corporation
svchost.exe		18,736 K	19,568 K	788	Host Process for Windows S	Microsoft Corporation
audiodg.exe		15,816 K	15,820 K	2276	Windows Audio Device Grap	Microsoft Corporation
svchost.exe		5,900 K	13,668 K	832	Host Process for Windows S	Microsoft Corporation
dwm.exe	0.39	59,660 K	74,700 K	1440	Desktop Window Manager	Microsoft Corporation
svchost.exe	0.02	34,288 K	44,256 K	856	Host Process for Windows S	Microsoft Corporation
WMIADAP.exe	0.16	2,140 K	5,440 K	3480	WMI Reverse Performance	Microsoft Corporation
svchost.exe		7,312 K	14,100 K	112	Host Process for Windows S	Microsoft Corporation
svchost.exe	0.01	15,736 K	17,764 K	612	Host Process for Windows S	Microsoft Corporation
spoolsv.exe		9,436 K	16,152 K	1100	Spooler SubSystem App	Microsoft Corporation
svchost.exe		10,456 K	13,232 K	1148	Host Process for Windows S	Microsoft Corporation
taskhost.exe		8,532 K	9,880 K	1316	Host Process for Windows T	Microsoft Corporation
UploaderService.exe		3,136 K	7,832 K	1468	TechSmith Uploader Service	TechSmith Corporation
VGAuthService.exe		4,580 K	10,472 K	1676	VMware Guest Authenticatio	VMware, Inc.
vm vmtoolsd.exe	1.56	10,716 K	20,432 K	1792	VMware Tools Core Service	VMware, Inc.
ManagementAgentHost.e	0.15	5,912 K	11,312 K	1844		
SearchIndexer.exe	0.02	24,136 K	21,660 K	540	Microsoft Windows Search I	Microsoft Corporation
SearchProtocolHost.e	< 0.01	2,424 K	8,256 K	1700	Microsoft Windows Search P	. Microsoft Corporation
SearchFilterHost.exe		2,484 K	6,444 K	1608	Microsoft Windows Search F	Microsoft Corporation
svchost.exe		2,052 K	5,640 K	2096	Host Process for Windows S	Microsoft Corporation
dlhost.exe	< 0.01	4,336 K	11,416 K	2316	COM Surrogate	Microsoft Corporation
🛵 msdtc.exe	< 0.01	3,520 K	8,004 K	2752	Microsoft Distributed Transa	Microsoft Corporation
svchost.exe	0.07	3,396 K	18,640 K	2840	Host Process for Windows S	Microsoft Corporation
svchost.exe		67,216 K	27,944 K	1772	Host Process for Windows S	Microsoft Corporation
sppsvc.exe		2,704 K	8,816 K	3168	Microsoft Software Protectio	Microsoft Corporation
svchost.exe		1,680 K	4,588 K	920	Host Process for Windows S	Microsoft Corporation
sass.exe		4,100 K	11,040 K	496	Local Security Authority Proc	Microsoft Corporation
sm.exe		2,592 K	4,288 K	504	Local Session Manager Serv	Microsoft Corporation
CSISS.exe	0.04	10,552 K	8,916 K	392	Client Server Runtime Process	Microsoft Corporation
🏰 winlogon.exe		2,516 K	6,740 K	440	Windows Logon Application	Microsoft Corporation
explorer.exe	1.09	48,724 K	76,608 K	1452	Windows Explorer	Microsoft Corporation
vm vmtoolsd.exe	0.10	11,584 K	23,772 K	1736	VMware Tools Core Service	VMware, Inc.
👩 fg761p.exe	2.16	27,700 K	27,052 K	1636	Fast and Secure Gateway to	Dynamic Internet Technol
👰 procexp 64.exe	2.15	15,104 K	30,848 K	3276	Sysintemals Process Explorer	Sysinternals - www.sysinter
🛃 jusched.exe		3,804 K	10,464 K	1908	Java Update Scheduler	Oracle Corporation

تصویر ۱: فرایندهای در حال اجرای سیستم عامل قبل از اجرای باجافزار





Process	CPU	Private Bytes	Working Set	PID D	Description	Company Name
System Idle Process		0 K	24 K	0		
🖃 🔜 System	52.02	132 K	1,068 K	4		
Interrupts	7.12	0 K	0 K	n/a Ha	ardware Interrupts and DPCs	
smss.exe		436 K	1,128 K	252 W	lindows Session Manager	Microsoft Corporation
CSrss.exe		2,004 K	4,476 K	332 Cli	ient Server Runtime Process	Microsoft Corporation
🖃 📰 wininit.exe		1,432 K	4,328 K	384 W	/indows Start-Up Application	Microsoft Corporation
services.exe		5,684 K	9,556 K	488 Se	ervices and Controller app	Microsoft Corporation
svchost.exe		4,328 K	9,624 K	596 Ho	ost Process for Windows S	Microsoft Corporation
WmiPrvSE.exe		7,976 K	13,252 K	2648 W	/MI Provider Host	Microsoft Corporation
vmacthlp.exe		1,428 K	4,096 K	660 VI	Mware Activation Helper	VMware, Inc.
svchost.exe	< 0.01	4,420 K	8,792 K	704 Ho	ost Process for Windows S	Microsoft Corporation
svchost.exe	0.13	18,048 K	18,828 K	788 Ho	ost Process for Windows S	Microsoft Corporation
audiodg.exe		15,692 K	15,712 K	27988 W	/indows Audio Device Grap	Microsoft Corporation
svchost.exe		5,772 K	13,580 K	832 Ho	ost Process for Windows S	Microsoft Corporation
dwm.exe	5.13	61,864 K	78,992 K	1440 De	esktop Window Manager	Microsoft Corporation
svchost.exe	0.01	26,012 K	39,940 K	856 Ho	ost Process for Windows S	Microsoft Corporation
svchost.exe		7,544 K	14,444 K	112 Ho	ost Process for Windows S	Microsoft Corporation
svchost.exe	0.04	15,228 K	17,524 K	612 Ho	ost Process for Windows S	Microsoft Corporation
spoolsv.exe		9,488 K	16,164 K	1100 Sp	pooler SubSystem App	Microsoft Corporation
svchost.exe		10,468 K	13,424 K	1148 Ho	ost Process for Windows S	Microsoft Corporation
taskhost.exe	11.18	60,300 K	40,720 K	1316 Ho	ost Process for Windows T	Microsoft Corporation
UploaderService.exe		3,136 K	7,832 K	1468 Te	echSmith Uploader Service	TechSmith Corporation
VGAuthService.exe		4,580 K	10,472 K	1676 VI	Mware Guest Authenticatio	VMware, Inc.
vm vmtoolsd.exe	6.09	10,784 K	20,588 K	1792 VI	Mware Tools Core Service	VMware, Inc.
ManagementAgentHost.e		68,080 K	71,836 K	1844		
SearchIndexer.exe	2.46	34,436 K	31,224 K	540 Mi	icrosoft Windows Search I	Microsoft Corporation
SearchProtocolHost.e		2,740 K	7,136 K	23088 Mi	icrosoft Windows Search P	Microsoft Corporation
SearchFilterHost.exe	0.02	3,048 K	8,084 K	39612 Mi	icrosoft Windows Search F	Microsoft Corporation
svchost.exe		1,948 K	5,608 K	2096 Ho	ost Process for Windows S	Microsoft Corporation
dlhost.exe		4,336 K	11,420 K	2316 CC	OM Surrogate	Microsoft Corporation
s msdtc.exe		3,520 K	8,004 K	2/52 Mi	icrosoft Distributed Transa	Microsoft Corporation
svchost.exe		3,292 K	18,588 K	2840 Ho	ost Process for Windows S	Microsoft Corporation
svchost.exe		67,160 K	23,920 K	1//2 Ho	ost Process for Windows S	Microsoft Corporation
svchost.exe		1,628 K	4,5/2 K	920 Ho	ost Process for Windows S	Microsoft Corporation
svcriosi.exe	0.07	J00 K	2,000 K	42000 1	ost Frocess for Windows 5	Microsoft Corporation
sdss.cxc	0.07	4,112 K	1 200 K	400 L0	noal Session Manager Service	Microsoft Corporation
	1 20	2,332 K	4,232 K	202 CI	lient Cenver Duntime Process	Microsoft Corporation
	1.50	2 516 K	6 740 K	332 CI	lient Server Nuntime Hocess	Microsoft Corporation
	0.02	2,510 K	77 272 K	1/52 W	lindows Euglin Application	Microsoft Corporation
	2.09	17 072 K	29 904 4	1736 V	Mware Tools Core Service	VMware Inc
fo761p exe	10.78	30 708 K	28,304 K	1636 F=	ast and Secure Gateway to	Dynamic Internet Technol
more vn 64 eve	5.72	20,820 K	36 824 K	3276 5	vsintemals Process Evolorer	Sysintemals - www.sysinter
MWorks64 eve	5.72	7 640 K	19 176 K	2880 H	ev Workshop	Break Point Software Joo
wincmp3 eve	< 0.01	7,612 K	16 480 K	2340 C	omnare Itl - file comnare an	Grig Software, www.grigeo
	0.04	32 040 K	83 244 K	2200 CH	homium	The Chromium Authors
Riusched exe	0.04	3 648 K	10.380 K	1908 Ja	ava Update Scheduler	Oracle Compration
		0,01011	10,000 10	1000 00	and opadio conodalor	ordere corporation

CPU Usage: 100.00% Commit Charge: 24.65% Processes: 50 Physical Usage: 62.06%

طبق بررسیهای صورت گرفته، باجافزار Ryuk پس از اجرا از شروع فعالیت برخی فرآیندها و نرمافزارها جلوگیری می کند. پس از اجرای باجافزار پیغام باجخواهی گشوده میشود که این پیغام در تمامی فولدرهای رمزگذاری شده نیز وجود دارد.

تصویر زیر پیغام باج خواهی باج افزار Ryuk را با نام RyukReadMe.txt نشان می دهد که بر روی پس زمینه سیستم قربانی و تمام فولدرهای رمزگذاری شده مستقر شده است :





RyukReadMe.txt - Notepad

<u>File Edit Format View Help</u> Your network has been penetrated. All files on each host in the network have been encrypted with a strong algorithm. Backups were either encrypted or deleted or backup disks were formatted. Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover. We exclusively have decryption software for your situation No decryption software is available in the public. DO NOT RESET OR SHUTDOWN - files may be damaged. DO NOT RENAME OR MOVE the encrypted and readme files. DO NOT DELETE readme files. This may lead to the impossibility of recovery of the certain files. To get info (decrypt your files) contact us at WayneEvenson@protonmail.com Or WayneEvenson@tutanota.com BTC wallet: 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk Ryuk No system is safe

بر اساس پیغام باجخواهی، که در ابتدای آن اشاره شده که شبکه شما مورد نفوذ قرار گرفته است، تمام فایلهای هر میزبان در شبکه با الگوریتمی قوی رمزگذاری شده است.

🖳 🕨 Comput	er >	• • Search Computer		٩
▼ System p	roperties Uninstall or change a program Map network drive Open Control Panel			0
rites sktop wnloads :ent Places	Hard Disk Drives (1) Local Disk (C:) 34.4 GB free of 49.9 GB Devices with Removable Storage (1)			
ries cuments Isic	DVD RW Drive (D:)			
tures ieos puter	Network Location (1) RyukReadMe.txt Text Document 804 bytes			

مهاجم مبلغ باج را در واحد پول بیـت کـوین تعیـین کـرده و بـرای برقـراری ارتبـاط، دو ایمیـل بـه آدرس WayneEvenson@protonmail.com و WayneEvenson@tutanota.com را تعیین نموده است.

در ادامه برای حصول اطمینان قربانی پیشنهاد رمزگشایی سه فایل را میدهد.

در تصویر زیر پاسخ مهاجم به ایمیل را مشاهده می کنید که در آن تقاضای پرداخت ۱۰ بیت کوین را دارد.

4	wayneevenson@tutanota.com
	to me 💌
	to unlock files, needs to pay 10 btc

Securely sent with Tutanota. Claim your encrypted mailbox today! https://tutanota.com





پس از ٥ روز با ایمیل transitaly@keemail.me پیشنهاد ۱.٥ بیت کوین داده شد :

Ryuł	JK Inbox x	
+	transitaly@keemail.me to me 👻	
	Good morning, can decrypt files from ryuk, have software, interested?	
+	transitaly@keemail.me to me	
	Its cost some btc, more lower what u must pay for this. 1.5 btc for decrypt	
	-	
	ں کیف پول زیر را در پیغام باج خواہی به قربانی معرفی می <i>کند</i> :	مهاجم آدرس



طبق بررسی های صورت گرفته این کیف پول تاکنون حال هیچ تراکنشی نداشته است.

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

Summary		Transa	octions	
Address	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk	No. Tra	ansactions	0
Hash 160	2890a8b7bf8e92e5f024fd6cd260e7621c12b981	Total R	eceived	0 BTC
		Final B	alance	0 BTC
			Request Payment	Donation Button

در تصاویر زیر فایل های اضافه شده و تغییر یافته در مسیر درایو سیستم عامل و پوشـه Windows پـس از اجرای باجافزار را مشاهده میکنید :





مرکزمـاهر





	n Share with T Burn New fold	er				20 - FT	- 4		
		n V							
tes	-DF0A5B8A2BB607C19E.TMP	DF3985F283D89F5E6C	.TMP	Ocejhapo	wmplog01.sqm	wmplog03.sqm			
top	wmplog05.sqm	wmplog02.sqm		wmplog04.sqm	wmsetup.log	wmplog00.sqm			
nloads	dd_vcredistMSI4668.txt	dd_vcredistUI4668.txt		JavaDeployReg.log	Microsoft .NET Framework 4.5.2 Hot	Microsoft .NET Framework 4.7.1 Set			
ent Places	Microsoft Visual C++ 2010 x86 Redis.	RGI3D5F.tmp-tmp		RGIF384.tmp-tmp	Snagit_12_20180304232743.log	Snagit_12_20180304232743_0_SnagitI.			
	StructuredQuery.log	SUB-CERT.bmp		vminst.log	Microsoft Visual C++ 2010 x64 Redis	. SDKSetup_7.0.6918.0.log			
es	tmp-ht8.xpi	🚳 unattend.cmd		vmmsi.log_20180302_150456.log	ASPNETSetup_00000.log	ASPNETSetup_00002.log			
uments	dd_Setup_decompression_log.txt	Microsoft Visual C++ 2	010 x64 Redis	Microsoft Visual C++ 2010 x86 Red	lis RGBD5F.tmp	RGIF384.tmp			
ic	📄 jusched.log	dd_NDP452-KB2974336-x86-x64-EN dd_vcredist_amd64		dd_vcredist_amd64_2018030215524	4 dd_wcf_CA_smci_20180302_115252	Microsoft .NET Framework 4.5.2 Hot.			
ures	O Microsoft .NET Framework 4.7.1 Set		dd_SetupUtility.txt	dd_vcredistMSI4627.txt	dd_vcredistUI4627.txt				
os	dd_wcf_CA_smci_20180302_115250	dd_wcf_CA_smci_20180	610_085850	dd_wcf_CA_smci_20180610_085857	AB73E0368C8A8A64.tmp	ASPNETSetup_00001.log			
	ASPNETSetup_00003.log	chromium_installer.log		dd_vcredist_amd64_2018030215524	4 Dgiwueto	RyukReadMe.txt			
	{cffaad72-47bd-4c5e-9d60-f5ef5ce4f.	af1) 8/27/2018 11:14 AM	File folder						
	WPDNSE	8/27/2018 11:14 AM	File folder						
	Microsoft Visual C++ 2010 v86 Redis	trib 8/27/2018 11:10 AM	File folder						
	wmware-UB-CERT	8/27/2018 11:10 AM	File folder						
	henorfdata UR-CEPT	9/27/2010 11:10 AM	File folder						
	KUDA57 tmp dir	8/27/2010 11:10 AIVI	File folder						
	KLODAS7.tmp.dir	0/27/2010 11:10 AIVI	File folder						
	Manage Minut Courses Con Con	0/2//2018 11:10 AM	File felder						
	Microsoft Visual C++ 2010 xb4 Kedis	anb 8/2//2018 11:10 AM	Filefolder						
	J FlashBackBackup	8/2//2018 11:10 AM	Filefolder						
	JE FlashBackTemp	8/27/2018 11:10 AM	Filefolder						
	ISUploadAgentTemp	8/2//2018 11:10 AM	Filefolder						
Comput	ter 🕨 Local Disk (C:) 🕨 ProgramData 🕨				•	Search ProgramData			
🦳 🦳 Oper	n Burn New folder					8= -	1 (
es	Name	Date modified	Туре	Size					
top	RvukReadMe.txt	8/27/2018 11:05 AM	Text Document	1 KB					
nloads	VMware	8/27/2018 11:05 AM	File folder						
nt Places	regid.1995-08.com.techsmith	8/27/2018 11:05 AM	File folder						
	TechSmith	8/27/2018 11:05 AM	File folder						
	Oracle	8/27/2018 11:05 AM	File folder						
uments	Package Cache	8/27/2018 11:05 AM	File folder						
ic	Bluebern:	9/27/2010 11:05 AM	File folder						
· · · ·	JeeSus	9/27/2010 11:05 AM	File folder						
rer	Logays	0/2//2010 11:00 AIVI	FileToldel						
ires	Alexanda	8/27/2018 11-05 AM	City And Alex						
os	Microsoft	8/27/2018 11:05 AM	File folder			4. Carach (and			
vs	Microsoft T > AppData > Local >	8/27/2018 11:05 AM	File folder		•	5 Search Local			
res os UB-CERT	Microsoft T > AppData > Local > n Share with → Burn New fold	8/27/2018 11:05 AM	File folder		•	4. Search Local 8Ξ ▼ □] (
os UB-CERT Open es	AppData > Local > n Share with - Burn New fold Name	8/27/2018 11:05 AM r Date modified	File folder Type	Size	•	€9] Search Local ﷺ ▼ []]] (
rres os UB-CERT Open tes top	Microsoft AppData > Local > Share with → Burn New fold Name DDPFONTCACHEV1.DAT	8/27/2018 11:05 AM r Date modified 8/27/2018 11:29 AM	File folder Type DAT File	Size 57 KB		49 Search Local ﷺ ▼ □] (
rres os UB-CERT Open res top nloads	Microsoft AppData > Local > Share with Burn New folds Name GDIPFONTCACHEVI.DAT ConCache.db	8/27/2018 11:05 AM er Date modified 8/27/2018 11:29 AM 8/27/2018 11:10 AM	File folder Type DAT File Data Base File	Size 57 KB 1,752 KB	-	49 Search Local ﷺ ▼ □] (
res ps UB-CERT Oper es top nloads nt Places	Microsoft AppData > Local > Share with Burn New folde Name DispiPFONTCACHEV1.DAT Concache.db RyukReadMe.bt	8/27/2018 11:05 AM Pr Date modified 8/27/2018 11:29 AM 8/27/2018 11:10 AM 8/27/2018 11:06 AM	File folder Type DAT File Data Base File Text Document	Size 57 KB 1,752 KB 1 KB		49 Search Local ∄≅ ▼ □] (
res ps UB-CERT Oper es top nloads nt Places	Microsoft AppData > Local > Share with Burn New fold Name GDIPFONTCACHEVI.DAT Concache.db RyukReadMe.bt Temp	8/27/2018 11:05 AM Pr Date modified 8/27/2018 11:04 AM 8/27/2018 11:06 AM 8/27/2018 11:06 AM	File folder Type DAT File Data Base File Text Document File folder	Size 57 KB 1,752 KB 1 KB		49 Search Local ﷺ ▼ □] (
res os UB-CERT Open es top nloads nt Places es	Microsoft AppData > Local > Share with > Burn New fold Name GDIPFONTCACHEVLDAT KucnCache.db KyukReadMe.bt Temp CrashDumps	8/27/2018 11:05 AM Pr Date modified 8/27/2018 11:29 AM 8/27/2018 11:20 AM 8/27/2018 11:04 AM 8/27/2018 11:28 AM	File folder Type DAT File Data Base File Text Document File folder File folder	Size 57 KB 1,752 KB 1 KB	-	49 Search Local ﷺ ♥ □] (
res os UB-CERT Open es top nloads nt Places es iments	Microsoft AppData > Local > Share with ~ Burn New fold Name DigDPFONTCACHEVI.DAT ConCache.db RyukReadMe.bt Temp ConshDumps ViruuStore	8/27/2018 11:05 AM Pate modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:06 AM 8/27/2018 11:48 AM 8/27/2018 11:48 AM	File folder Type DAT File Data Base File Text Document File folder File folder File folder	Size 57 KB 1,752 KB 1 KB		4 y Search Local ∄≣ ▼ □			
res os UB-CERI Open es top nloads nt Places es top c	Microsoft AppData > Local > Share with Burn New fold Name GDIPFONTCACHEV1.DAT Concache.db RyukReadMe.bt Temp CrashDumps VirtualStore MStree Inc	8/27/2018 11:05 AM Provide the modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:49 AM 8/27/2018 11:49 AM 8/27/2018 11:49 AM 8/27/2018 11:40 AM	File folder Type DAT File Data Base File Text Document File folder File folder File folder File folder	Size 57 KB 1,752 KB 1 KB		49 Search Local ﷺ ▼ □			
ires os UB-CERT Open es top nloads nt Places es ires ic ires	Microsoft AppData > Local > Share with > Burn New fold Name GDIPFONTCACHEVI.DAT ConCachedb RyukReadMe.bt Temp CrashDumps WittualStore Misfree Inc Programs	8/27/2018 11:05 AM Pate modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:28 AM 8/27/2018 11:28 AM 8/27/2018 11:28 AM 8/27/2018 11:29 AM	File folder Type DAT File Data Base File Text Document File folder File folder File folder File folder	Size 57 KB 1,752 KB 1 KB	-	4y Search Local ﷺ ♥ □] (
irres os • UB-CERT • Open es top niloads nt Places es es mments ic tres os	Microsoft AppData > Local > Share with Burn New fold Name GDIPFONTCACHEVI.DAT CLOCCachedb PyukkeadMe.bt Temp CrashDumps VirtualStore MSfree Inc Programs TechSmith	8/27/2018 11:05 AM Date modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:10 AM 8/27/2018 11:48 AM 8/27/2018 11:48 AM 8/27/2018 11:41 AM 8/27/2018 11:40 AM 8/27/2018 11:40 AM	File folder Type DAT File Data Base File Text Document File folder File folder File folder File folder File folder	Size 57 KB 1,752 KB 1 KB		ify Search Local ∰≣ ▼ □] (
rres os • UB-CERT • Open res top nloads nt Places es es ic cres os	Microsoft AppData > Local > Share with Burn New fold Name GDIPFONTCACHEVI.DAT SionCache.db RyukReadMe.bt Temp CrashDumps VirtualStore MSfree Inc Programs TechSmith dnSvv	8/27/2018 11:05 AM P Date modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:20 AM 8/27/2018 11:40 AM 8/27/2018 11:40 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM	File folder Type DAT File Data Base File Text Document File folder File folder File folder File folder File folder File folder	Size 57 KB 1,752 KB 1 KB		49 Search Local ﷺ ▼ □] (
vres os	Microsoft AppData > Local > Share with Burn New fold Name SoliPFONTCACHEVI.DAT ConcAche.db NyukReadMe.bt Temp ConshDumps VirtualStore MSfree Inc Programs TechSmith dnSpy Microsoft	8/27/2018 11:05 AM Pate modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:06 AM 8/27/2018 11:06 AM 8/27/2018 11:04 AM 8/27/2018 11:04 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM	File folder Type DAT File DAT Base File Text Document File folder	Size 57 KB 1,752 KB 1 KB		4y Search Local ﷺ ♥ □			
vres os UB+CERT es top nloads nt Places es uments ic res ss uter IDisk (C)	Microsoft AppData > Local > Share with Burn New fold Name GDIPFONTCACHEVLDAT ConCache.db NgukeasMe.bt Temp CrashDumps VitualStore MSfree Inc Programs TechSmith dnSpy Microsoft Charming	8/27/2018 11:05 AM Pate modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:06 AM 8/27/2018 11:46 AM 8/27/2018 11:40 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM	File folder Type DAT File Data Base File Text Document File folder File folder File folder File folder File folder File folder File folder File folder File folder	Size 57 KB 1,752 KB 1 KB		(49) Search Local ﷺ ▼ □			
vres os	Microsoft AppData > Local > Share with Burn New fold Name GDIPFONTCACHEVI.DAT ConCache.db RyukReadMe.bt Temp CrashDumps VirtualStore MSfree Inc Programs TechSmth dnSpy Microsoft Chromium ascenbly	8/27/2018 11:05 AM Part modified 8/27/2018 11:29 AM 8/27/2018 11:29 AM 8/27/2018 11:20 AM 8/27/2018 11:40 AM 8/27/2018 11:40 AM 8/27/2018 11:40 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM 8/27/2018 11:10 AM	File folder Type DAT File Data Base File Test Document File folder File folder File folder File folder File folder File folder File folder File folder File folder File folder	Size 57 KB 1,752 KB 1 KB	-	49 Search Local ﷺ ▼ □			

Desktop				
:e 🔻 🦳 Open	Share with 🔻 🛛 Burn	New folde	r	
rorites	Name	Size	Item type	Date modified
lesktop	RyukReadMe.txt	1 KB	Text Document	9/4/2018 1:49 AM
lownloads	🗿 desktop.ini	1 KB	Configuration sett	3/2/2018 3:03 PM
ecent Places	퉬 Victims		File folder	9/4/2018 10:46 AM
	퉬 victim		File folder	9/4/2018 1:49 AM
raries	RyukReadMe.txt	1 KB	Text Document	9/4/2018 1:30 AM
locuments	desktop.ini	1 KB	Configuration sett	7/14/2009 9:24 AM
Ausic	🥑 Recycle Bin			
ictures	🐖 Control Panel			
ïdeos	年 Network			
	👰 Computer			
mputer	UB-CERT			
ocal Disk (C:)	ز Libraries			





محتوای DESKTOP.INI

desktop.ini - Notepad
File Edit Format View Help
[.ShellClassInfo] LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21802 InfoTip=@%SystemRoot%\system32\shell32.dll,-12688 IconResource=%SystemRoot%\system32\imageres.dll,-3
🗍 desktop.ini - Notepad
File Edit Format View Help
 [.ShellClassInfo] LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21779 InfoTip=@%SystemRoot%\system32\shell32.dll,-12688 IconResource=%SystemRoot%\system32\imageres.dll,-113 IconFile=%SystemRoot%\system32\shell32.dll IconIndex=-236

طبق آزمایشات صورت گرفته، سرعت رمزگذاری فایل ها توسط باجافزار Ryuk ارتباط مستقیمی با منابع سیستم قربانی دارد. این باجافزار پس از اجرا، بیش از همه پردازنده سیستم قربانی را اشغال میکند. لذا در صورت برخورداری از پردازنده ای با سرعت بالاتر در محیط واقعی، انتظار میرود سرعت رمزگذاری نیز افزایش یابد.

System Information
Summary CPU Memory I/O GPU
CPU Usage
System Commit
1.2 GB
Physical Memory
1.5 GB
I/O
12.0 MB
Network
25.7 КВ
Disk
23.4 MB





تحليل ايستا:

پس از تحلیل کد باجافزار Ryuk به نتایج زیر دست پیدا کردیم. مقایسه نمونه فایل سالم و رمزگذاری شده همسان، نشان میدهد که پس از رمزگذاری بیش از دو برابر محتوای اولیه حجم افزوده شده است. مقایسه نمونه فایل، قبل و بعد از رمزگذاری :

C:\Users\UB-C	ERT\D	esktop	\victir	n\web	mana	ii.docx					3	C:\Users\UB-C	ERT\D	esktop	\web	manai	docx						x
	0	1	2	3	4	5	6	7	8	012345678			0	1	2	3	4	5	6	7	8	012345678	
00000000	ЗE	CE	35	50	9B	56	9E	E 4	2 F	>.5p.V/	*	00000000	90	76	92	в4	BF	AC	15	C7	48	_vH	*
00000009	06	64	7A	BB	в6	FC	94	D6	С3	.dz		00000009	36	E5	34	A2	59	14	1A	66	A9	6.4.Yf.	
00000012	6A	6D	Α7	F3	0 E	52	09	6D	ЗD	jmR.m=		00000012	9C	CF	D2	76	DF	9F	23	AF	7B	· · · ▼ · · # · {	
0000001B	46	46	E2	26	ЗF	5C	7D	64	6E	FF.&?\}dn		0000001B	15	D7	6D	21	80	35	7A	87	43	m!.5z.C	
00000024	D9	8 E	43	55	38	76	78	E 6	44	CU8vx.D		00000024	EЗ	64	54	E 6	ΕE	62	В8	4 D	D1	.dTb.M.	
0000002D	94	E 5	8 D	52	92	DE	AC	F2	CA	R		0000002D	в7	32	6A	31	7 F	4 E	BC	3C	E2	.2j1.N.<.	
00000036	56	C0	8 E	в2	20	25	2 F	18	13	V %/		00000036	84	95	9 D	56	F4	4 F	84	47	62	V.O.Gb	
0000003F	24	в9	2B	54	FD	7A	DF	50	в1	\$.+T.z.P.		0000003F	FO	ED	DA	99	ΕE	Ε7	A2	4 F	71	Qq	
00000048	74	17	27	FF	87	1A	11	4 E	30	t.'NO		00000048	64	FB	60	76	AA	8A	60	8 A	97	d.`v`	
00000051	DA	78	93	ΕE	79	E1	64	F8	DC	.xy.d		00000051	72	5D	AE	44	C5	0 F	AF	5E	16	r].D^.	
0000005A	69	A6	AA	С1	15	E8	D7	9B	EC	i		0000005A	EA	31	ΕF	ВD	C9	34	в3	C8	DF	.14	
00000063	FB	0D	E 9	C4	A9	4C	В9	00	C8	L		00000063	18	94	22	Ε7	6C	E7	05	68	AD	".lh.	
0000006C	BE	07	89	AE	19	ΕE	89	12	1B			0000006C	C7	22	72	CF	A9	61	AE	64	1D	."ra.d.	
00000075	E0	FA	35	23	D5	D3	E 6	5A	55	5#ZU		00000075	D5	73	96	01	78	D4	A1	83	15	.sx	
0000007E	C0	C9	8A	46	84	57	D5	в0	Α7	F.W		0000007E	В4	34	C2	F2	6B	90	31	0C	3C	.4k.1.<	
00000087	BA	5B	C1	CE	86	9A	AC	7A	79	.[zy		00000087	D5	CD	21	32	0A	7 D	BA	1A	C7	!2.}	
00000090	62	33	в2	13	EC	6B	A3	5A	95	b3k.Z.		00000090	D6	F1	87	6F	5E	04	9E	C7	8A		
00000099	BA	BE	CA	37	36	1F	41	5F	27	76.A_'		00000099	FB	80	A1	7 E	62	39	17	53	A9	~b9.S.	
000000A2	BF	6F	EЗ	08	03	FA	D2	8 E	41	.oA		000000A2	45	08	DC	CF	В9	6A	33	0E	2 F	Ej3./	
000000AB	FD	95	22	34	44	9D	14	62	65	"4Dbe		000000AB	A1	26	B8	2 B	59	90	1A	1A	8C	.&.+Y	
000000B4	A4	EF	9B	8 F	CE	AF	В9	A1	в5	• • • • • • • • • •		00000084	5D	2C	0 D	A1	FF	13	85	5F	AA	1	
000000BD	6F	7A	78	8B	93	75	EF	0B	4 E	ozxuN		000000BD	32	04	55	25	86	86	52	D9	D3	2.U%R	
000000000	57	EA	4 A	BF	77	4A	6E	2 D	D1	W.J.wJn		000000000	52	1F	5A	86	C9	В9	0 F	8B	60	R.Z`	
DODOOOCF	A2	BC	9B	8 F	8 B	77	2D	3E	AC	w->.	Ψ.	DODOOCF	7 F	F3	53	0B	CA	89	E7	29	F2	s).	Ψ.

تعداد بایت های جایگزین شده ی نمونه فایل بعد از رمزگذاری:

•	web manai.do	ocx vs web man	nai.docx			A	11	•	6 2 X
	Туре	Source 16	Count 19	Count 😼	Target 16	Count 10	Count	16	
	Replaced	00000000	19522	4C42	00000000	19522	4C42		
Results	Compare	Checksum	🛛 🛗 Find	Bookmarks 🖺	Output				
6C 0			00 00 00 00 1		00004200	7 28 88 05 FF 1	A 01 00 12 00	AR 7F 21 23	λ2 52 + lb
00 0	0 00 00 00 00 00 10	44 00 00 64 6F	63 50 72 6F	DdocFro	00004AE0 9	F 59 EA B8 F9 (58 EB D4 00 F0	DD A2 D7 76	E7 E1 .Yh
70 7	3 2F 63 6F 72 65	2E 78 6D 6C 50	4B 01 02 14 ps	/core.xmlFK	00004AF0 9	A 49 B5 FE A9 8	BC 3C 03 AE 45	D1 ED DC AB	E3 50 .I<.
00 1	4 00 08 08 08 00	00 00 21 00 EA	D1 38 0A DC		00004B00 B	7 7C 52 24 BB B	32 05 4E 71 7D	24 90 12 7D	61 78 . R\$N
01 0	0 00 E3 03 00 00	10 00 00 00 00	00 00 00 00		00004B10 D	9 0C 59 62 85 6	54 D8 C1 B4 0B	60 AE AC EO	D4 FCYb.d
00 0	0 00 00 00 BB 45	00 00 64 6F 63	50 72 6F 70	EdocFrop	00004B20	0 4D 59 E6 E1 2	27 FB D7 97 FA	28 07 17 57	D1 48 .MY'
00 01		00 00 05 47 00		app.xmirk	00004840	0 00 F1 56 FF 1	12 AF A3 03 8F	10 88 00 00 0F 45 5F F1	C7 1E V 7
00 0.	D 00 0D 00 11 00				00004B50 4	9 2F 10 A9 6E 1	LA 92 C8 6B 48	F4 39 4A 1D	B1 A4 I/n
					00004B60 E	6 E3 OF 3B F1 H	76 FC 47 5B D7	09 FE C2 63	75 83;G
					00004B70 E	1 OC 6F 91 87 H	3B CC 9A 45 E3	46 47 09 51	A9 FC
					00004B80 6	5 72 3E 88 5D 5	50 69 E0 D8 44	EC AE 5B AD	62 6F er>.]Pi.
					00004B90 D	3 68 93 2C 50 1	LC D4 B1 49 72	FA 1D 6B 78	8A 18 .h., P
					00004BA0 4	/ 4/ 1A 02 A4 2	2E 95 37 96 74	70 51 F7 25	32 06 GG7
					00004880 4	C 00 A4 E6 3B I	2 33 94 AU E3	AF FF F8 45	7D 35;.U.
					00004BD0 C	B 5B 88 7A 67 B	C 37 10 EB F0	57 DF E9 E7	96 9C .[.zg.7.
					00004BE0 C	B F0 A2 AB D0 2	2E 38 A2 82 8F	A1 5F B9 C5	04 618.
					00004BF0 2	B 95 B2 5D D5 1	74 32 5E DD 87	88 9A AF EF	20 BF +].t2^
					00004c00 5	E 3A E1 74 72 (CE 88 C5 52 B0	A5 FA OB 45	D5 E4 ^:.tr]
					00004c00 5 00004c10 4	E 3A E1 74 72 0 B D0 3E E0 A1 H	CE 88 C5 52 B0 29 34 6D DE 77	A5 FA 0B 45 A2 C8 3B 39	D5 E4 ^:.tr1 03 5D K.>4m
					00004c00 5 00004c10 4 00004c20 D	E 3A E1 74 72 0 B DO 3E EO A1 E E 6D F5 07 DF 6	CE 88 C5 52 B0 29 34 6D DE 77 5F A5 AF 2A B9	A5 FA 0B 45 A2 C8 3B 39 84 52 D5 1F	D5 E4 ^:.tr1 03 5D K.>4m FB A2 .mo





در تابع log شاهد آن هستیم که کد از طریق VirtualAllocEx, WriteProcessMemory و CreateRemoteThread

[0074.400] VirtualAllocEx (hProcess=0x238, [0074.445] WriteProcessMemory (in: hProcess [0074.454] CreateRemoteThread (in: hProcess

تزریق درصورتی انجام می شود که نام فرآیند مربوطه در لیست سفید نباشد و توسط NT AUTHORITY اجرا

نشده باشد. در این تحلیل "taskhost.exe", "dwm.exe" , "taskeng.exe" تغییر داده شدند.

"c:\users\°p°nrgjn•js halpmcxz\desktop\^\c^r) ^{\$}bc^rdc^rVba⁵f^{Vrl}^{\$}acd^o) • ^Ac^rb.virus.exe" modifies memory of "c:\windows\system^{rr}\taskhost.exe"

"c:\users\°p°nrgjn•js halpmcxz\desktop\^٦c٣) ٤bc^rdc^{rv}ba^٤f^v٣٦٤acd°)•^c^rb.virus.exe" modifies memory of "c:\windows\system^{rr}\dwm.exe"

"c:\users\°p°nrgjn•js halpmcxz\desktop\^٦c^r) [£]bc^rdc^rVba^[£]f^{Yr}[‡]acd[°]) • ^c^rb.virus.exe" modifies memory of "c:\windows\system^r{\taskeng.exe"

کلیدهای رجیستری اضافه شده به سیستم پس از اجرای باجافزار :

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchos
HKEY_CURRENT_USER\Software\Microsoft\Command Processor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor\PathCompletionChar

باجافزار Ryuk برای ماندگاری و تثبیت خود در سیستم قربانی، از کلید رجیستری زیر استفاده میکند.

 ${\it HKEY_CURRENT_USER\SOFTWARe\Microsoft\Windows\CurrentVersion\Run}$

Adds "C:\Users\5p5NrGJn0jS HALPmcxz\Desktop\86c314bc2dc37ba84f7364acd5108c2b.virus.exe" to Windows startup via registry.





این باجافزار از کتابخانههای ویندوزی به همراه توابعی از هرکدام از کتابخانهها استفاده میکند که در جدول زیر قابل مشاهده است :

		ADVAPITT.dll		SHELLTT.dll		
		SystemFunction • ٣	Sh	ellExecuteW		
		ç				
KERNEL T.dll		KERNEL T.dll		KERNELTT.dll		KERNEL T.dll
GetLastError InitializeCriticalSectionAnd SpinCount HeapFree GetSystemTimeAsFileTime EnterCriticalSection LCMapStringW GetModuleFileNameW GetConsoleCP GetVersionExW	Ge Ge Ge He Ge Ge Ge	etStdHandle eleteCriticalSection etCurrentProcess etWindowsDirectoryW etConsoleMode eapSize etCurrentProcessId riteConsoleW etCommandLineW etCPInfo		InitializeSListHead GetProcessHeap SetStdHandle RaiseException WideCharToMultil te TlsFree FindFirstFileExA SetUnhandledExce tionFilter	By ≥p	TerminateProcess GetModuleHandleExW IsValidCodePage CreateFileW FindClose TIsGetValue GetFileType TIsSetValue ExitProcess GetCurrentThreadId
FreeLibrary QueryPerformanceCounter IsDebuggerPresent GetTickCount TIsAlloc GetOEMCP GetEnvironmentStringsW	Ur Lo M Ge Se Fro	nhandledExceptionFilte adLibraryExW ultiByteToWideChar etStartupInfoW tFilePointerEx eeEnvironmentStringsV	er N	WriteFile DecodePointer CloseHandle IsProcessorFeatur resent FindNextFileA GetACP HeapReAlloc GetStringTypeW	eP	SetLastError LeaveCriticalSection FlushFileBuffers LoadLibraryA RtlUnwind GetModuleFileNameA GetCommandLineA GetProcAddress GetModuleHandleW HeapAlloc

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

■ <u>210.exe</u> (PID: 2664)

- PbDRp.exe C:\210.exe (PID: 2860)
 - cmd.exe /C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Curre ntVersion\Run" /v "svchos" /t REG_SZ /d "%PUBLIC%\PbDRp.exe" /f (PID: 2056)
 - Image: Reg ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current tVersion\Run" /v "svchos" /t REG_SZ /d "%PUBLIC%\PbDRp.exe" /f (PID: 4016)
 - o taskhost.exe (PID: 1332)
 - o dwm.exe (PID: 1444)
 - o conhost.exe (PID: 1292)
 - ∘ Il conhost.exe (PID: 2708)
 - o conhost.exe (PID: 3164)





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 Ryukنشدیم.

خروجي سامانه VirusTotal :

در حال حاضر تعداد ٤٩ مورد از ٦٦ آنتی ویروس و آنتی بـدافزار موجـود در سـامانه VirusTotal قـادر بـه شناسایی این باجافزار بوده وآن را حذف یا غیرفعال میکنند.

Ad-Aware	Trojan.Ransom.Ryuk.A	AhnLab-V3	Dropper/Win32.Ryukran.R234915
ALYac	Trojan.Ransom.Ryuk	Antiy-AVL	Trojan/Win32.Invader
Arcabit	Trojan.Ransom.Ryuk.A	Avast	Win64:Malware-gen
AVG	Win64:Malware-gen	Avira	TR/FileCoder.biysh
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401
BitDefender	Trojan.Ransom.Ryuk.A	CAT-QuickHeal	Program.Unwaders
CrowdStrike Falcon	malicious_confidence_100% (W)	Cybereason	malicious.fde9ec
Cylance	Lunsafe	DrWeb	Trojan.Encoder.25857
Emsisoft	Trojan.Ransom.Ryuk.A (B)	Endgame	malicious (high confidence)
eScan	Trojan.Ransom.Ryuk.A	ESET-NOD32	a variant of Win64/Filecoder.T
F-Secure	Trojan.Ransom.Ryuk.A	Fortinet	W64/Filecoder.T!tr
GData	Trojan.Ransom.Ryuk.A	Ikarus	Trojan-Ransom.FileCoder
Jiangmin	Trojan.Invader.bsk	K7AntiVirus	Trojan (0053a8931)
K7GW	Trojan (0053a8931)	Kaspersky	HEUR:Trojan.Win32.Invader
Malwarebytes	Ransom.FileCryptor	MAX	malware (ai score=100)
McAfee	Ransom-Ryuk	McAfee-GW-Edition	BehavesLike.Win32.Dropper.fh
Microsoft	Ransom:Win32/Jabaxsta.B!dr	NANO-Antivirus	Trojan.Win32.Invader.fgronb
Palo Alto Networks	generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Win32/Trojan.836	Rising	Trojan.Filecoder!8.68 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Troj/Ransom-FAB
Sophos ML	heuristic	Symantec	Trojan.Cridex
Tencent	Win32.Trojan.Raas.Auto	TrendMicro-HouseCall	Ransom_RYUK.THHBAAH
VBA32	Trojan.Invader	VIPRE	Trojan.Win32.Generic!BT
ViRobot	Dropper.S.Agent.393216.I	Webroot	W32.Invader
ZoneAlarm	HEUR:Trojan.Win32.Invader	AegisLab	Clean





خروجی سامانه ویروسکاو مرکز ماهر :

در حال حاضر تعداد ۱ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروسکاو مرکـز مـاهر قادر به شناسایی این باجافزار بوده وآن را حذف یا غیرفعال میکنند.

			لوبايت	حجم فایل: ۳۸۴ کی					
سکن: ۷ شهریور ۱۳۹۷ - ۱۱:۱۱									
5ac0f050f93f86e69026faea1fbb4450 :N									
9709774fde9ec740ad6fed8ed79903296ca9d571 :SHA									
	23f8aa94ffb3c08a6273	5fe7fee5799880a8f322	2ce1d55ec49a13a3f8531	2db2 :SHA256					
				وضعیت:					
Clean		~	2.3.190.2675	پادویش					
			.نتیجهای یافت نشد	sophos					
			انتیجهای یافت نشد.	f_secure					
			انتیجهای یافت نشد.	kaspersky					
			نتیجهای یافت نشد.	eset					
			نتیجهای یافت نشد.	drweb					
			نتیجهای یافت نشد.	clam_av					
			نتیجهای یافت نشد.	comodo					
			نتیجهای یافت نشد.	bitdefender					
			نتیجهای یافت نشد.	avast					
Dangerous: Trojan.Cride	×	ii	7.9.0.30	symantec					

نام فايل: 23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2.exe