

باسمه تعالی

تحلیل فنی باج افزار Ryuk

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، 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 می کند. یکی طولانی تر، خوش بیان تر و خوش تعبیرتر که خواهان مبلغ باج بالاتر یعنی ۵۰ بیت کوین است و دیگری کوتاه تر و رک 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 می گیرد! همچنین این باج افزار قربانیان خود را با دانش و هدف قبلی انتخاب می کند 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. بررسی ها نشان می دهد که فعالیت این باج افزار در اواسط ماه آگوست سال ۲۰۱۸ میلادی شروع شده است. این باج افزار از الگوریتم رمزنگاری AES + RSA استفاده می کند.

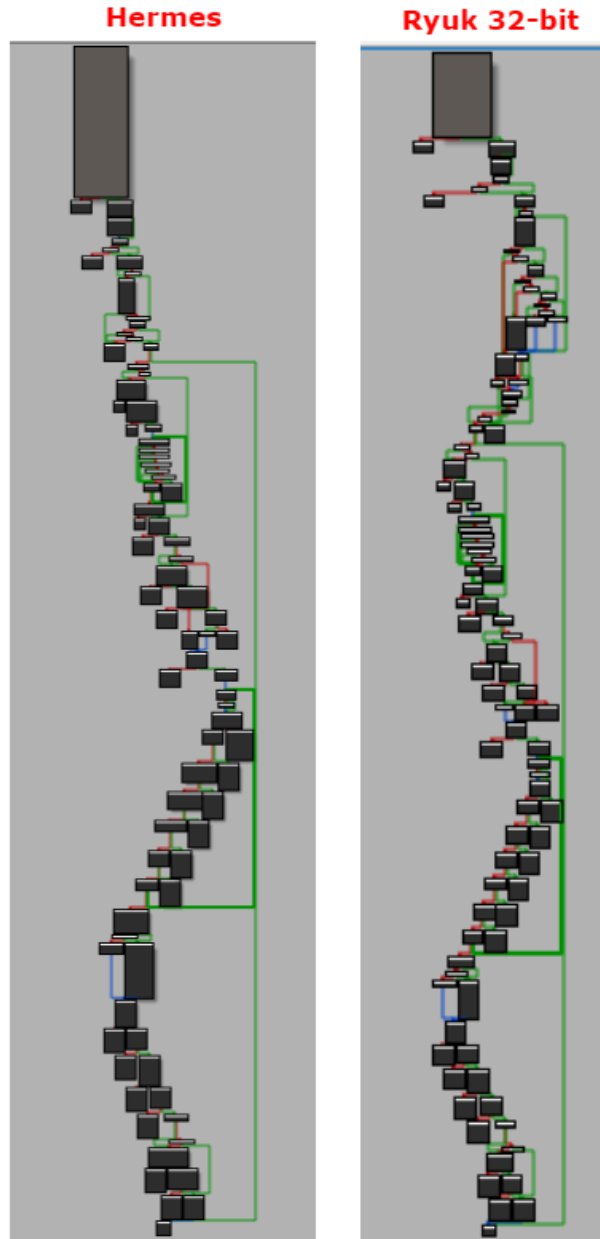
مشخصات فایل اجرایی :

نام فایل	۲۳f8aa9effb3c08a62۷۳۰fe۷fee۵۷۹۹۸۸۰a۸f۳۲۲ce1d۵۵ec۴۹a۱۳a۳f۸۵۳۱۲db۲.exe ۲۱۰.exe.bin ryuk.exe
MD۵	۵ac۰f۰۵۰f۹۳f۸۷e۶۹۰۲۶faea۱fbb۴۴۵۰
SHA-۱	۹۷۰۹۷۷۴fde۹ec۷۴۰ad۶fed۸ed۷۹۹۰۳۲۹۶ca۹d۵۷۱
SHA-۲۵۶	۲۳f8aa9effb3c08a62۷۳۰fe۷fee۵۷۹۹۸۸۰a۸f۳۲۲ce1d۵۵ec۴۹a۱۳a۳f۸۵۳۱۲db۲
اندازه فایل	۳۸۴ KB
کامپایلر / پکر	Microsoft Visual C++ ۸

فایل اجرایی این باج افزار دارای پنج بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
.text	۶.۶۱	۴۰۹۶	۴۴۲۳۱	۴۴۵۴۴
.rdata	۴.۸۹	۴۹۱۵۲	۲۲۸۵۸	۲۳۰۴۰
.data	۶.۲	۷۳۷۲۸	۳۲۲۵۲۴	۳۲۰۰۰۰
gfids	۱.۴۶	۳۹۷۳۱۲	۱۸۰	۵۱۲

۴۰۹۶	۳۶۰۴	۴۰۱۴۰۸	۶.۱۶	.reloc
------	------	--------	------	--------



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

Identified by

• ransomnote_email: WayneEvenson@tutanota.com

[Click here for more information about Ryuk](#)

🔔 Would you like to be notified if there is any development regarding this ransomware? [Click here.](#)

تحلیل پویا :

برای بررسی عمیق تر باج افزار Ryuk 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 می کنید. باج افزار Ryuk با استفاده از task kill فرآیندهای زیادی را از بین می برد از جمله پایگاه های داده، پشتیبان ها، آنتی ویروس ها و نرم افزارهای 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.
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.exe	< 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
dllhost.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
lsass.exe		4,100 K	11,040 K	496	Local Security Authority Proc...	Microsoft Corporation
lsm.exe		2,592 K	4,288 K	504	Local Session Manager Serv...	Microsoft Corporation
csrss.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
vmtoolsd.exe	0.10	11,584 K	23,772 K	1736	VMware Tools Core Service	VMware, Inc.
fg76lp.exe	2.16	27,700 K	27,052 K	1636	Fast and Secure Gateway to...	Dynamic Internet Technol...
procexp64.exe	2.15	15,104 K	30,848 K	3276	Sysinternals Process Explorer	Sysinternals - www.sysinter...
lschex.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	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	Hardware Interrupts and DPCs	
smss.exe		436 K	1,128 K	252	Windows Session Manager	Microsoft Corporation
csrss.exe		2,004 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		5,684 K	9,556 K	488	Services and Controller app	Microsoft Corporation
svchost.exe		4,328 K	9,624 K	596	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		7,976 K	13,252 K	2648	WMI Provider Host	Microsoft Corporation
vmacthlp.exe		1,428 K	4,096 K	660	VMware Activation Helper	VMware, Inc.
svchost.exe	< 0.01	4,420 K	8,792 K	704	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.13	18,048 K	18,828 K	788	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		15,692 K	15,712 K	27988	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe		5,772 K	13,580 K	832	Host Process for Windows S...	Microsoft Corporation
dwm.exe	5.13	61,864 K	78,992 K	1440	Desktop Window Manager	Microsoft Corporation
svchost.exe	0.01	26,012 K	39,940 K	856	Host Process for Windows S...	Microsoft Corporation
svchost.exe		7,544 K	14,444 K	112	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.04	15,228 K	17,524 K	612	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		9,488 K	16,164 K	1100	Spooler SubSystem App	Microsoft Corporation
svchost.exe		10,468 K	13,424 K	1148	Host Process for Windows S...	Microsoft Corporation
taskhost.exe	11.18	60,300 K	40,720 K	1316	Host Process for Windows T...	Microsoft Corporation
UploaderService.exe		3,136 K	7,832 K	1468	TechSmith Uploader Service	TechSmith Corporation
VGAAuthService.exe		4,580 K	10,472 K	1676	VMware Guest Authenticatio...	VMware, Inc.
vmttoolsd.exe	6.09	10,784 K	20,588 K	1792	VMware 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	Microsoft Windows Search I...	Microsoft Corporation
SearchProtocolHost.e...		2,740 K	7,136 K	23088	Microsoft Windows Search P...	Microsoft Corporation
SearchFilterHost.exe	0.02	3,048 K	8,084 K	39612	Microsoft Windows Search F...	Microsoft Corporation
svchost.exe		1,948 K	5,608 K	2096	Host Process for Windows S...	Microsoft Corporation
dllhost.exe		4,336 K	11,420 K	2316	COM Surrogate	Microsoft Corporation
msdtc.exe		3,520 K	8,004 K	2752	Microsoft Distributed Transa...	Microsoft Corporation
svchost.exe		3,292 K	18,588 K	2840	Host Process for Windows S...	Microsoft Corporation
svchost.exe		67,160 K	23,920 K	1772	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,628 K	4,572 K	920	Host Process for Windows S...	Microsoft Corporation
svchost.exe		968 K	2,668 K	42596	Host Process for Windows S...	Microsoft Corporation
lsass.exe	0.07	4,112 K	11,060 K	496	Local Security Authority Proc...	Microsoft Corporation
lsm.exe	0.02	2,592 K	4,292 K	504	Local Session Manager Serv...	Microsoft Corporation
csrss.exe	1.30	10,588 K	11,712 K	392	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		2,516 K	6,740 K	440	Windows Logon Application	Microsoft Corporation
explorer.exe	0.02	44,968 K	77,272 K	1452	Windows Explorer	Microsoft Corporation
vmttoolsd.exe	2.09	17,072 K	29,904 K	1736	VMware Tools Core Service	VMware, Inc.
fg761p.exe	10.78	30,708 K	28,252 K	1636	Fast and Secure Gateway to...	Dynamic Internet Technol...
procexp64.exe	5.72	20,820 K	36,824 K	3276	Sysinternals Process Explor...	Sysinternals - www.sysinter...
HWorks64.exe		7,640 K	19,176 K	2880	Hex Workshop	BreakPoint Software, Inc.
wincomp3.exe	< 0.01	7,612 K	16,480 K	2340	Compare It! - file compare an...	Grig Software, www.grigso...
chrome.exe	0.04	32,040 K	83,244 K	2200	Chromium	The Chromium Authors
usched.exe		3,648 K	10,380 K	1908	Java Update Scheduler	Oracle Corporation

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

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 Ryuk 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 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
File Edit Format View Help
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.

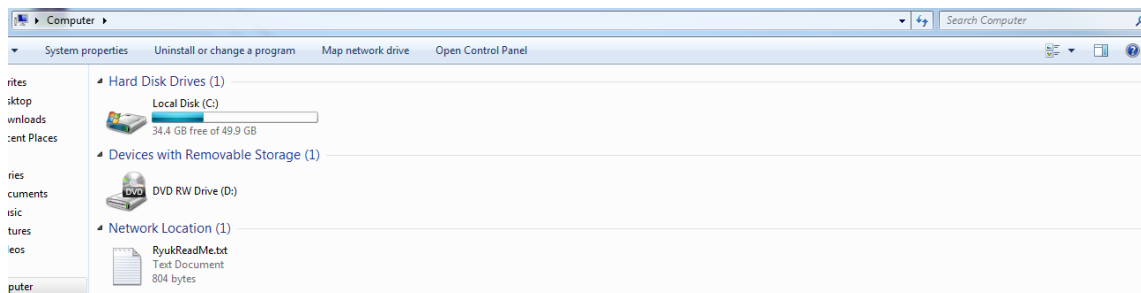
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
wayneEvenson@protonmail.com
or
wayneEvenson@tutanota.com

BTC wallet:
14hVkm7Ft2rXDBFTNkKRC3kGstMgp2A4hk

Ryuk
No system is safe
```

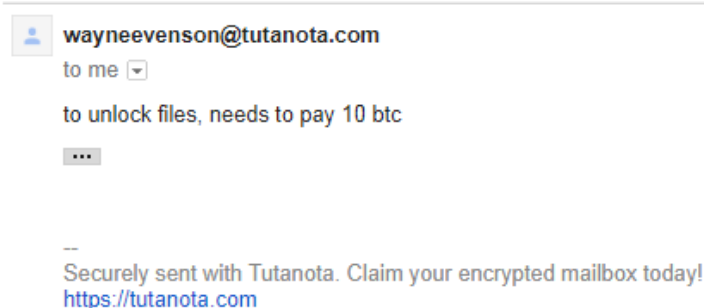
بر اساس پیغام باج خواهی، که در ابتدای آن اشاره شده که شبکه شما مورد نفوذ قرار گرفته است، تمام فایل های هر میزبان در شبکه با الگوریتمی قوی رمزگذاری شده است.



مهاجم مبلغ باج را در واحد پول بیت کوین تعیین کرده و برای برقراری ارتباط، دو ایمیل به آدرس WayneEvenson@protonmail.com و WayneEvenson@tutanota.com را تعیین نموده است.


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

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




پس از ۵ روز با ایمیل transitaly@keemail.me پیشنهاد ۱.۵ بیت کوین داده شد :

Ryuk 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

--

مهاجم آدرس کیف پول زیر را در پیغام باج خواهی به قربانی معرفی می کند:

۱۴hVKm۷Ft۲rxDBFTNkkRC۳kGstMGp۲A۴hk

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	
Address	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
Hash 160	2890a8b7bf8e92e5f024fd6cd260e7621c12b981

Transactions	
No. Transactions	0
Total Received	0 BTC
Final Balance	0 BTC

Request Payment

Donation Button



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

The screenshots show the following navigation steps and file listings:

- Local Disk (C:)**: Lists folders like Tools, Tor Browser, TCPView, snapshot_2018-01-28_12-18, Psiphon3, regshot_1.8.3_beta1_win32_x64, Program Files (x86), PEID-0.94, PerfLogs, pestudio, ProcessExplorer, Program Files, jd-gui-windows-1.4.0, MDS_and_SHA, odbg110, IDAPro6.6, Users, DiskMon, dnSpy, and apateDNS.
- Windows**: Lists files WindowsUpdate.log (110 KB), setupact.log (30 KB), and bootstat.dat (66 KB).
- Temp**: Lists folders Temp, inf, and System32.
- vmware-vmxvc.log**: A text document file (95 KB).
- UB-CERT**: Lists files NTUSER.DAT (1,280 KB), ntuser.dat.LOG1 (256 KB), and RyukReadMe.txt (1 KB), along with various system folders like Desktop, Favorites, Links, Saved Games, Searches, Downloads, My Documents, My Music, My Pictures, My Videos, Contacts, and AppData.
- UB-CERT > AppData > Roaming**: Lists a large number of folders and files, including ACJavaDecomp, Blueberry, dnSpy, Hex-Rays, Identities, LogSys, Media Center Programs, Microsoft, PE Explorer, Psiphon3, Sun, TechSmith, Telegram Desktop, WinRAR, Wireshark, www.shadowexplorer.com, jd-gui.cfg, and RyukReadMe.txt.

UB-CERT > AppData > Local > Temp

Name	Date modified	Type
DF0A588A2B8607C19E.TMP		
DF3985F283D89F5E6C.TMP		
Ocejhapo		
wmplog05.sqm		
wmplog02.sqm		
wmplog04.sqm		
wmplog01.sqm		
wmplog03.sqm		
dd_vcristMSI4668.txt		
dd_vcristUH4668.txt		
JavaDeployReg.log		
wmsetup.log		
wmplog00.sqm		
Microsoft Visual C++ 2010 x86 Redist...		
RGID5F.tmp-tmp		
RGIF384.tmp-tmp		
Snagit_12_20180304232743.log		
Microsoft .NET Framework 4.5.2 Hot...		
Microsoft .NET Framework 4.7.1 Set...		
Snagit_12_20180304232743_0_Snagitl...		
StructuredQuery.log		
UB-CERT.bmp		
vminst.log		
Microsoft Visual C++ 2010 x64 Redis...		
SDKSetup_7.0.6918.0.log		
tmp-h88.xpi		
unattend.cmd		
vmmsi.log_20180302_150456.log		
Microsoft Visual C++ 2010 x86 Redis...		
ASPNETSetup_00000.log		
ASPNETSetup_00002.log		
dd_Setup_decompression_log.bt		
Microsoft Visual C++ x64 Redis...		
RGID5F.tmp		
RGIF384.tmp		
jusched.log		
dd_NDP452-KB2974336-x86-x64-EN...		
dd_vcrist_amd64_20180302155244...		
dd_wcf_CA_smci_20180302_115252_...		
Microsoft .NET Framework 4.5.2 Hot...		
Microsoft .NET Framework 4.7.1 Set...		
dd_SetupUtility.txt		
dd_vcristMSI4627.txt		
dd_wcf_CA_smci_20180302_115250_...		
dd_wcf_CA_smci_20180610_085850_...		
dd_wcf_CA_smci_20180610_085857_...		
AB73E0368C8A8A64.tmp		
ASPNETSetup_00001.log		
ASPNETSetup_00003.log		
chromium_installer.log		
dd_vcrist_amd64_20180302155244...		
Dgijwuto		
RyukReadMe.txt		
{cffaad72-47bd-4c5e-9d60-f5ef5ce4faf1}	8/27/2018 11:14 AM	File folder
WPDNSE	8/27/2018 11:14 AM	File folder
Microsoft Visual C++ 2010 x86 Redistrib...	8/27/2018 11:10 AM	File folder
vmware-UB-CERT	8/27/2018 11:10 AM	File folder
hspcrfdata_UB-CERT	8/27/2018 11:10 AM	File folder
KLUDA57.tmp.dir	8/27/2018 11:10 AM	File folder
Low	8/27/2018 11:10 AM	File folder
Microsoft Visual C++ 2010 x64 Redistrib...	8/27/2018 11:10 AM	File folder
FlashBackBackup	8/27/2018 11:10 AM	File folder
FlashBackTemp	8/27/2018 11:10 AM	File folder
FTSUploadAgentTemp	8/27/2018 11:10 AM	File folder

Computer > Local Disk (C:) > ProgramData

Name	Date modified	Type	Size
RyukReadMe.txt	8/27/2018 11:05 AM	Text Document	1 KB
VMware	8/27/2018 11:05 AM	File folder	
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	
Package Cache	8/27/2018 11:05 AM	File folder	
Blueberry	8/27/2018 11:05 AM	File folder	
LogSys	8/27/2018 11:05 AM	File folder	
Microsoft	8/27/2018 11:05 AM	File folder	

UB-CERT > AppData > Local

Name	Date modified	Type	Size
GDIPFONTCACHEV1.DAT	8/27/2018 11:29 AM	DAT File	57 KB
IconCache.db	8/27/2018 11:10 AM	Data Base File	1,752 KB
RyukReadMe.txt	8/27/2018 11:06 AM	Text Document	1 KB
Temp	8/27/2018 11:48 AM	File folder	
CrashDumps	8/27/2018 11:28 AM	File folder	
VirtualStore	8/27/2018 11:14 AM	File folder	
MSfree Inc	8/27/2018 11:10 AM	File folder	
Programs	8/27/2018 11:10 AM	File folder	
TechSmith	8/27/2018 11:10 AM	File folder	
dnSpy	8/27/2018 11:10 AM	File folder	
Microsoft	8/27/2018 11:10 AM	File folder	
Chromium	8/27/2018 11:06 AM	File folder	
assembly	8/27/2018 11:06 AM	File folder	

Desktop

Name	Size	Item type	Date modified
RyukReadMe.txt	1 KB	Text Document	9/4/2018 1:49 AM
desktop.ini	1 KB	Configuration sett...	3/2/2018 3:03 PM
Victims		File folder	9/4/2018 10:46 AM
victim		File folder	9/4/2018 1:49 AM
RyukReadMe.txt	1 KB	Text Document	9/4/2018 1:30 AM
desktop.ini	1 KB	Configuration sett...	7/14/2009 9:24 AM
Recycle Bin			
Control Panel			
Network			
Computer			
UB-CERT			
Libraries			

محتوای DESKTOP.INI

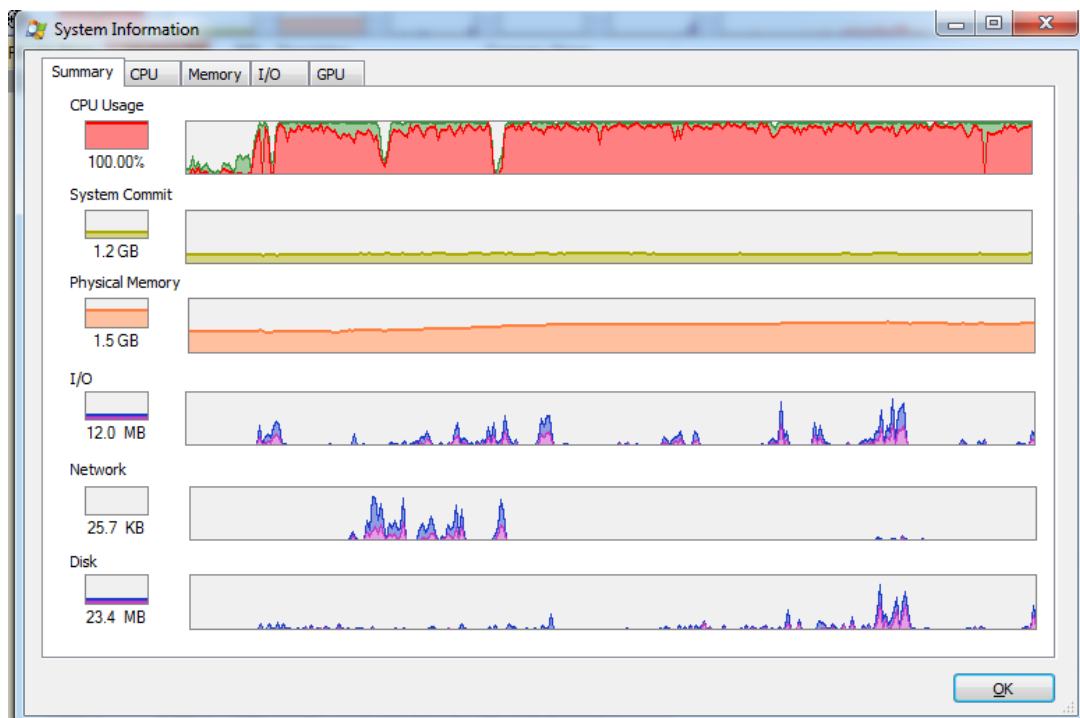
```
desktop.ini - Notepad
File Edit Format View Help

[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell132.dll,-21802
InfoTip=@%SystemRoot%\system32\shell132.dll,-12688
IconResource=%SystemRoot%\system32\imageres.dll,-3

desktop.ini - Notepad
File Edit Format View Help

[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell132.dll,-21779
InfoTip=@%SystemRoot%\system32\shell132.dll,-12688
IconResource=%SystemRoot%\system32\imageres.dll,-113
IconFile=%SystemRoot%\system32\shell132.dll
IconIndex=-236
```

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



تحلیل ایستا:

پس از تحلیل کد باج افزار Ryuk به نتایج زیر دست پیدا کردیم. مقایسه نمونه فایل سالم و رمزگذاری شده همسان، نشان می دهد که پس از رمزگذاری بیش از دو برابر محتوای اولیه حجم افزوده شده است.

مقایسه نمونه فایل، قبل و بعد از رمزگذاری:

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

Type	Source	Count	Count	Target	Count	Count
Replaced	00000000	19522	4C42	00000000	19522	4C42

در تابع log شاهد آن هستیم که کد از طریق VirtualAllocEx, WriteProcessMemory و CreateRemoteThread به فرآیندهای سیستمی تزریق می شود :

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

تزریق در صورتی 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\p5p5NrgJn0js HALPmcxz\Desktop\86c314bc2dc37ba84f7364acd5108c2b.virus.exe"
modifies memory of "c:\windows\system32\taskhost.exe"

"c:\users\p5p5NrgJn0js HALPmcxz\Desktop\86c314bc2dc37ba84f7364acd5108c2b.virus.exe"
modifies memory of "c:\windows\system32\dwm.exe"

"c:\users\p5p5NrgJn0js HALPmcxz\Desktop\86c314bc2dc37ba84f7364acd5108c2b.virus.exe"
modifies memory of "c:\windows\system32\taskeng.exe"
```

کلیدهای رجیستری اضافه شده به سیستم پس از اجرای باج افزار :

```
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
```

باج افزار Ryuk برای ماندگاری و تثبیت خود در سیستم قربانی، از کلید رجیستری زیر استفاده می کند.






```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Adds "C:\Users\5p5NrgJn0js HALPmcxz\Desktop\86c314bc2dc37ba84f7364acd5108c2b.virus.exe" to
Windows startup via registry.
```

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

KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll	KERNEL۳۲.dll
GetLastError	GetStdHandle	InitializeSListHead	TerminateProcess
InitializeCriticalSectionAndSpinCount	DeleteCriticalSection	GetProcessHeap	GetModuleHandleExW
HeapFree	GetCurrentProcess	SetStdHandle	IsValidCodePage
GetSystemTimeAsFileTime	GetWindowsDirectoryW	RaiseException	CreateFileW
EnterCriticalSection	GetConsoleMode	WideCharToMultiByte	FindClose
LCMapStringW	HeapSize	HeapSize	TlsGetValue
GetModuleFileNameW	GetCurrentProcessId	TlsFree	GetFileType
GetConsoleCP	WriteConsoleW	FindFirstFileExA	TlsSetValue
GetVersionExW	GetCommandLineW	SetUnhandledExceptionFilter	ExitProcess
FreeLibrary	GetCPInfo	WriteFile	GetCurrentThreadId
QueryPerformanceCounter	UnhandledExceptionFilter	DecodePointer	SetLastError
IsDebuggerPresent	LoadLibraryExW	CloseHandle	LeaveCriticalSection
GetTickCount	MultiByteToWideChar	IsProcessorFeaturePresent	FlushFileBuffers
TlsAlloc	GetStartupInfoW	FindNextFileA	LoadLibraryA
GetOEMCP	SetFilePointerEx	GetACP	RtlUnwind
GetEnvironmentStringsW	FreeEnvironmentStringsW	HeapReAlloc	GetModuleFileNameA
		GetStringTypeW	GetCommandLineA
			GetProcAddress
			GetModuleHandleW
			HeapAlloc

بر اساس بررسی های صورت گرفته، باج افزار Ryuk پس از اجرا، فرایندهای زیر را ایجاد می کند :

-  210.exe (PID: 2664)
 -  PbDRp.exe C:\210.exe (PID: 2860)
 -  cmd.exe /C REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ /d "%PUBLIC%\PbDRp.exe" /f (PID: 2056)
 -  reg.exe REG ADD "HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "svchos" /t REG_SZ /d "%PUBLIC%\PbDRp.exe" /f (PID: 4016)
 -  taskhost.exe (PID: 1332)
 -  dwm.exe (PID: 1444)
 -  conhost.exe (PID: 1292)
 -  conhost.exe (PID: 2708)
 -  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 باج افزار Ryuk نشدیم.

خروجی سامانه VirusTotal :

در حال حاضر تعداد ۴۹ مورد از ۶۶ آنتی ویروس و آنتی بدافزار موجود در سامانه VirusTotal قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

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.blysh
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	⚠ Unsafe	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.fn
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.l	Webroot	⚠ W32.Invader
ZoneAlarm	⚠ HEUR:Trojan.Win32.Invader	AegisLab	✔ Clean

خروجی سامانه ویروس کاو مرکز ماهر :

در حال حاضر تعداد ۱ مورد از ۱۱ آنتی ویروس و آنتی بدافزار موجود در سامانه ویروس کاو مرکز ماهر قادر به شناسایی این باج افزار بوده و آن را حذف یا غیرفعال می کنند.

نام فایل: 23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2.exe


حجم فایل: ۳۸۴ کیلوبایت


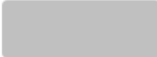
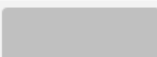






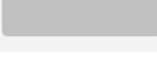

تاریخ اسکن: ۷ شهریور ۱۳۹۷ - ۱۰:۱۱

MD5: 5ac0f050f93f86e69026faea1fbb4450

SHA1: 9709774fde9ec740ad6fed8ed79903296ca9d571

SHA256: 23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2

وضعیت: 

Clean		2.3.190.2675	یادویش
		نتیجه ای یافت نشد	sophos
		نتیجه ای یافت نشد	f_secure
		نتیجه ای یافت نشد	kaspersky
		نتیجه ای یافت نشد	eset
		نتیجه ای یافت نشد	drweb
		نتیجه ای یافت نشد	clam_av
		نتیجه ای یافت نشد	comodo
		نتیجه ای یافت نشد	bitdefender
		نتیجه ای یافت نشد	avast
Dangerous: Trojan.Cridex		7.9.0.30	symantec