

باسمه تعالی

تحلیل فنی باج افزار ZOLDON Crypter V۳.۰

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج افزار ZOLDON Crypter V۳.۰ که با نام های encryptor-extortionist, doxware نیز شناخته می شود خبر می دهد. بررسی ها نشان می دهد که فعالیت این باج افزار در اوایل ماه آگوست سال ۲۰۱۸ میلادی شروع شده است و به نظر می رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می باشد. این باج افزار برای محیط های دارای سیستم عامل ویندوز ۶۴ بیتی توسعه یافته و برخلاف اکثریت باج افزارها پسوند فایل ها را پس از رمزگذاری عوض نمی کند. به نظر می رسد باج افزار ZOLDON Crypter V۳.۰ در حال توسعه بوده و در آینده شاهد نسخه های کاملتری از آن باشیم.

مشخصات فایل اجرایی :

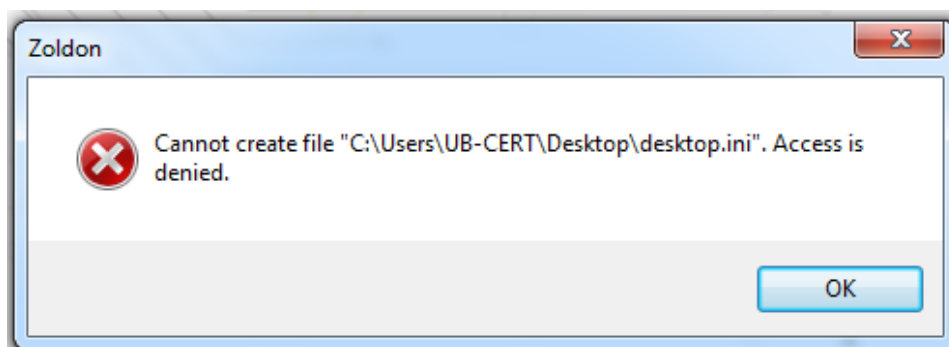
نام فایل	ZOLDON Bitcoin Miner Pro V۳.۱.exe
اندازه	۱.۳۶ MB
SHA-۱	e۴ec۰۹۴f۴۰f۳۵۰۵b۲cvf۵e۶f۹۳۰b۱۷bca۰۹f۵۴۱
SHA-۲۵۶	۵۱۵۶۹۶aafeaav۴dd۰f۴۰۳۸b۲۴۳۳۶f۶۳۶a۹۲۵eacbv۷b۷۰aa۴۶۹bda۲۲ba۹d۴d۱۳b
MD۵	ce۲۰fb۴c۶d۴۴۷۹۷۲۵۹۳۵۵b۵f۷efb۹۰۴c
کامپایلر	UPX -> www.upx.sourceforge.net

فایل اجرایی این باج افزار دارای هفت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
UPX۰	۰	۴۰۹۶	۳۲۸۴۹۹۲	۰
UPX۱	۷.۹۴	۳۲۸۹۰۸۸	۱۳۲۳۰۰۸	۱۳۲۰۹۶۰
.rsrc	۳.۸۳	۴۶۱۲۰۹۶	۱۱۰۵۹۲	۱۰۸۵۴۴

تحلیل پویا :

برای بررسی عمیق تر باج افزار ZOLDON Crypter V3.0 ، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که پس از خطای زیر باج افزار پنجره باج خواهی به شکل زیر را می گشاید.



طبق بررسی ها، این باج افزار فایل ها را رمزگذاری نمی کند.

باج افزار برای رمزگشایی فایل ها، از قربانیان طلب ۱۵۰ دلار بیت کوین به عنوان باج می کند و مدت ارسال باج را ۲۴ ساعت اعلام کرده است که در صورت عدم پرداخت مبلغ باج را به ۴۰۰ دلار افزایش داده و ۲۴

ساعت دیگر نیز فرصت می دهد. مهاجم، ایمیلی به آدرس zoldon-staff@mail.ru را نیز برای ارتباط گیری قربانی با وی، در متن باج خواهی قرار داده است که در قبال دریافت مبلغ باج، کلید رمزگشایی را در اختیار او قرار می دهد. در صورت عدم پرداخت فایل ها تا ۷۲ ساعت، باجگیر به انتشار تمام فایل های قربانی در بستر اینترنت دست خواهد زد.


ضمناً قربانیان می بایست مبلغ باج را به آدرس کیف پول بیت کوین زیر ارسال نمایند.

1AHhnEDuHS1AFkSdcq3nQRZEPHs1QECAtv

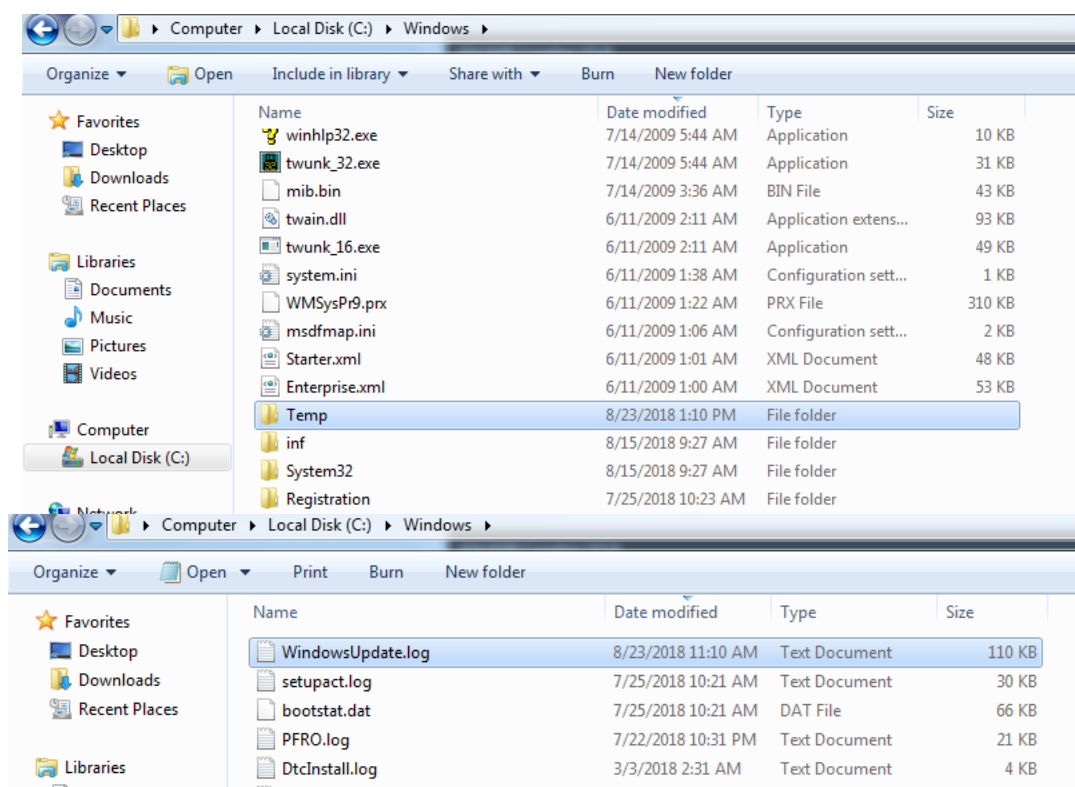
بررسی ها نشان می دهد که این کیف پول تا کنون تراکنشی نداشته است :

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

Summary		Transactions	
Address	1AHhnEDuHS1AFkSdcq3nQRZEPHs1QECAtv	No. Transactions	0
Hash 160	65e1d425a1c1151c8b10db35b47b5a03fa8c5f78	Total Received	0 BTC
		Final Balance	0 BTC



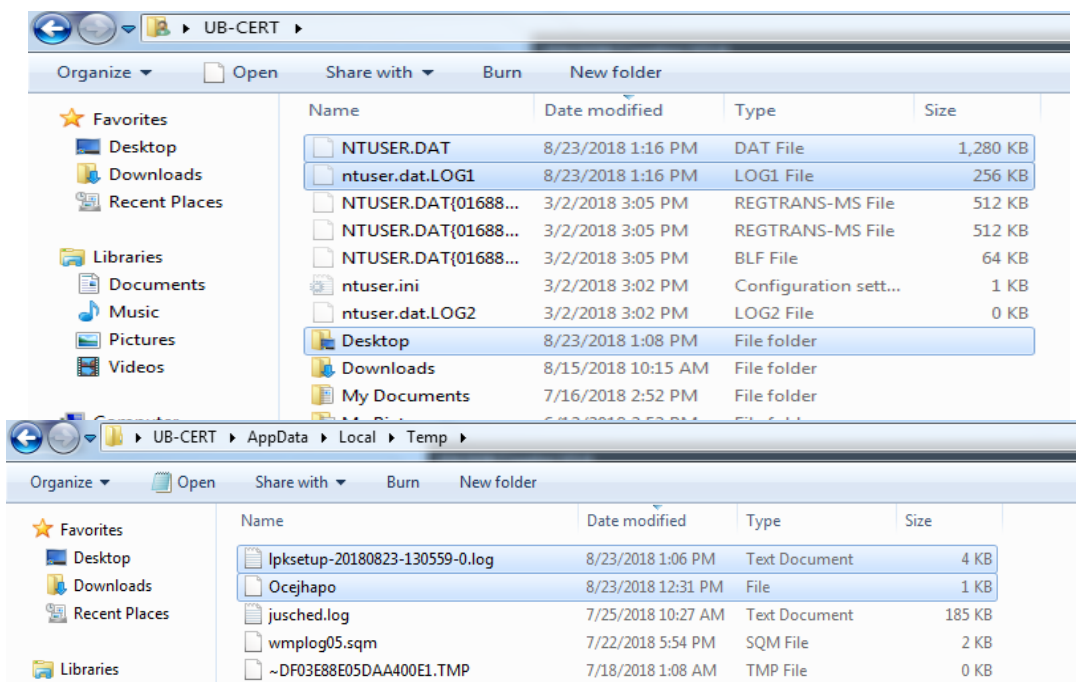
در تصاویر زیر فایل های اضافه شده و تغییر یافته در مسیر درایو سیستم عامل و پوشه Windows پس از اجرای باج افزار را مشاهده می کنید :



The top screenshot shows the Windows Explorer window for 'C:\Windows'. The 'Temp' folder is selected in the file list. The bottom screenshot shows the contents of the 'Temp' folder, with 'WindowsUpdate.log' highlighted.

Name	Date modified	Type	Size
winhlp32.exe	7/14/2009 5:44 AM	Application	10 KB
twunk_32.exe	7/14/2009 5:44 AM	Application	31 KB
mib.bin	7/14/2009 3:36 AM	BIN File	43 KB
twain.dll	6/11/2009 2:11 AM	Application extens...	93 KB
twunk_16.exe	6/11/2009 2:11 AM	Application	49 KB
system.ini	6/11/2009 1:38 AM	Configuration sett...	1 KB
WMSysPr9.prx	6/11/2009 1:22 AM	PRX File	310 KB
msdfmap.ini	6/11/2009 1:06 AM	Configuration sett...	2 KB
Starter.xml	6/11/2009 1:01 AM	XML Document	48 KB
Enterprise.xml	6/11/2009 1:00 AM	XML Document	53 KB
Temp	8/23/2018 1:10 PM	File folder	
inf	8/15/2018 9:27 AM	File folder	
System32	8/15/2018 9:27 AM	File folder	
Registration	7/25/2018 10:23 AM	File folder	

Name	Date modified	Type	Size
WindowsUpdate.log	8/23/2018 11:10 AM	Text Document	110 KB
setupact.log	7/25/2018 10:21 AM	Text Document	30 KB
bootstat.dat	7/25/2018 10:21 AM	DAT File	66 KB
PFR0.log	7/22/2018 10:31 PM	Text Document	21 KB
DtInstall.log	3/3/2018 2:31 AM	Text Document	4 KB



محتوای فایل lpksetup-۲۰۱۸۰۸۲۳-۱۳۰۵۵۹-۰.log

```

lpksetup-20180823-130559-0.log - Notepad
File Edit Format View Help
13:05:59:606 : INFO: _wsetlocale returns: English_united States.1252
13:05:59:606 : PERF: CbsClient::Initialize - ENTER
13:06:02:399 : INFO: created cbs session 0x269d78
13:06:02:414 : DEBUG: Found TI process (C:\Windows\servicing\TrustedInstaller.exe)
13:06:02:414 : PERF: CbsClient::Initialize - LEAVE
13:06:05:488 : PERF: CbsClient::Initialize - ENTER
13:06:05:503 : PERF: CbsClient::Initialize - LEAVE
13:06:05:503 : PERF: Enumerating installed languages - ENTER
13:06:05:706 : DEBUG: CreateFromIdentity("Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-US~6.1.7601.17514")
13:06:05:722 : DEBUG: CreateFromIdentity("Client")
13:06:05:737 : LanguagePack en-US created.
13:06:05:737 : type: MUI
13:06:05:768 : identity: Microsoft-Windows-Client-LanguagePack-Package~31bf3856ad364e35~amd64~en-US~6.1.7601.17514
13:06:05:800 : WARN: Unable to open Lpksetup reg key
13:06:05:815 : DEBUG: CreateFromIdentity("Microsoft-Windows-Client-Refresh-LanguagePack-Package~31bf3856ad364e35~amd64~en-US~6.1.7601.17514")
13:06:05:831 : DEBUG: CreateFromIdentity("Client")
13:06:05:846 : LanguagePack en-US created.
13:06:05:846 : type: MUI
13:06:05:846 : identity: Microsoft-Windows-Client-Refresh-LanguagePack-Package~31bf3856ad364e35~amd64~en-US~6.1.7601.17514
13:06:05:862 : WARN: Unable to open Lpksetup reg key
13:06:05:878 : PERF: Enumerating installed languages - LEAVE
13:06:07:640 : INFO: Session 0x269d78 finalized, reporting no required reboot
13:06:07:640 : INFO: destroying cbsession 0x269d78
13:06:07:640 : INFO: attempt to re-finalize session 0x269d78 not acted on
13:06:07:656 : PERF: RestorePointEnd - ENTER
13:06:07:734 : PERF: RestorePointEnd - LEAVE
13:06:07:734 : DEBUG: Cleaning working path in a new process
  
```

محتوای فایل Ocejhapo

```

Hex Workshop - [C:\Users\UB-CERT\AppData\Local\Temp\Ocejhapo]
File Edit Disk Options Tools Plug-Ins Window Help
Legacy ASCII
0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11 12 13 14 15 0123456789ABCDEF012345
00000000 5B 52 65 67 42 61 63 6B 75 70 5D 0D 0A 50 72 6F 78 79 48 74 74 70 [RegBackup]..ProxyHttp
00000016 31 2E 31 3D 34 32 39 34 39 36 37 32 39 35 0D 0A 5B 43 6F 6E 66 69 1.1=4294967295..[Conf
0000002C 67 42 61 63 6B 75 70 5D 0D 0A 43 6F 6E 6E 43 68 61 6E 67 65 64 3D gBackup]..ConnChanged=
00000042 31 0D 0A 43 6F 6E 6E 46 6C 61 67 73 3D 31 0D 0A 1..ConnFlags=1..
  
```

طبق بررسی‌های انجام شده اکثر آنتی‌ویروس‌های معتبر، این باج‌افزار را به عنوان یک تروجان شناسایی نموده‌اند. لذا احتمال نفوذ باج‌افزار به سیستم از راه‌های متداول از جمله هرزنامه‌ها وجود دارد.

تحلیل ایستا :

پس از تحلیل کد فایل اجرایی باج‌افزار ZOLDON Crypter ۷۳.۰ نتایج زیر حاصل گردید :

فایل اجرایی باج‌افزار حاوی انتروپی غیر معمولی بود که مشخص گردید برای جلوگیری از تحلیل، با استفاده از UPX پک شده است.

UPX\ with unusual entropies ۷.۹۳۶۸۴۸۰۸۵۹۸

"Sample_۰b۶da۱۷۴cb۴ca۴ad۰ca۷eb۰.exe.bin" has a section named "UPX۰"

"Sample_۰b۶da۱۷۴cb۴ca۴ad۰ca۷eb۰.exe.bin" has a section named "UPX۱"

پس از آنپک نمودن فایل اجرایی باج‌افزار، موارد زیر از آن استخراج گردید.

قطعه کد گرفتن زمان سیستم و تعیین ۲۴ ساعت مهلت پرداخت اولیه و ثانویه:

```

push    eax
push    eax
mov     eax, [esp+24h+IdleTime.dwLowDateTime]
xor     edx, edx
or      eax, [esp+24h+var_24]
or      edx, [esp+24h+var_20]
add     esp, 8
mov     [ebx], eax
mov     [ebx+4], edx
mov     eax, [esp+1Ch+UserTime.dwHighDateTime]
xor     edx, edx
mov     edx, eax
xor     eax, eax
push    edx
push    eax
mov     eax, [esp+24h+UserTime.dwLowDateTime]
xor     edx, edx
or      eax, [esp+24h+var_24]
or      edx, [esp+24h+var_20]
add     esp, 8
mov     [ebx+8], eax
mov     [ebx+0Ch], edx
mov     eax, [esp+1Ch+KernelTime.dwHighDateTime]
xor     edx, edx
mov     edx, eax
xor     eax, eax
push    edx
push    eax
mov     eax, [esp+24h+KernelTime.dwLowDateTime]
xor     edx, edx
or      eax, [esp+24h+var_24]

```

کتابخانه‌های مورد استفاده توسط باج‌افزار ZOLDON Crypter V۳.۰ :

oleaut۳۲.dll	shell۳۲.dll	user۳۲.dll	version.dll	winspool.driv
VariantCopy	SHGetMalloc	GetDC	VerQueryValueW	OpenPrinterW

ADVAPI۳۲.dll	comctl۳۲.dll	KERNEL۳۲.DLL	gdi۳۲.dll	msvcrt.dll	ole۳۲.dll
RegCloseKey	ImageList_Add	VirtualFree ExitProcess VirtualProtect LoadLibraryA VirtualAlloc GetProcAddress	Pie	memset	IsEqualGUID

بر اساس بررسی‌های صورت گرفته، باج‌افزار ZOLDON Crypter V۳.۰ پس از اجرا، فرایند زیر را ایجاد می‌کند :

- [Sample_۵b۶da۱۷۴cb۴ca۵ad۰ca۷eb۵.exe](#) (PID: ۳۴۰۴)

تغییرات رجیستری:

کلیدهای رجیستری اضافه شده:

```
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Multimedia\ActiveMovie\Filter Cache64
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\ZOldon
```

مقادیر اضافه شده:

```
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Multimedia\ActiveMovie\Filter Cache64\0
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\Fnzcyr_5o6qn174po4pn54nq0pn7ro5.rkr
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Microsoft\Windows\CurrentVersion\Run\ZOldon: "C:\Users\UB-CERT\Desktop\Sample_5b6da174cb4ca54ad0ca7eb5.exe"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\ZOldon\start: "8/20/2018"
```

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 ZOLDON Crypter ۷۳.۰ نشدیم.

ابزار رمزگشایی :

در حال حاضر وجود ندارد.

شناسایی :

در حال حاضر تعداد ۴۱ مورد از ۶۷ آنتی‌ویروس معتبر دنیا قادر به تشخیص آلودگی این باج‌افزار در سامانه VirusTotal شده‌اند.



Ad-Aware	⚠ Trojan.GenericKD.31162221	Antiy-AVL	⚠ Trojan[Ransom]/Win32.AGeneric
Arcabit	⚠ Trojan.Generic.D1DB7F6D	Avast	⚠ Win32:Malware-gen
AVG	⚠ Win32:MdeClass	Avira	⚠ TR/FileCoder.xhaoy
BitDefender	⚠ Trojan.GenericKD.31162221	CAT-QuickHeal	⚠ Trojan.IGENERIC
ClamAV	⚠ Win.Trojan.Agent-6641204-0	Comodo	⚠ UnclassifiedMalware
Cylance	⚠ Unsafe	Cyren	⚠ W32/GenBl.CE20FB4C!Olympus
DrWeb	⚠ Trojan.Encoder.25821	Emsisoft	⚠ Trojan.GenericKD.31162221 (B)
eScan	⚠ Trojan.GenericKD.31162221	ESET-NOD32	⚠ a variant of Win32/Filecoder.NMJ
F-Secure	⚠ Trojan.GenericKD.31162221	Fortinet	⚠ W32/Filecoder.NMJ!tr
GData	⚠ Trojan.GenericKD.31162221	Ikarus	⚠ Trojan-Ransom.FileCoder
Jiangmin	⚠ Trojan.Gen.xu	K7AntiVirus	⚠ Trojan (00510ab41)
K7GW	⚠ Trojan (00510ab41)	Kaspersky	⚠ Trojan-Ransom.Win32.Gen.kgx
Malwarebytes	⚠ Ransom.Zoldon	MAX	⚠ malware (ai score=100)
McAfee	⚠ Artemis!CE20FB4C6D44	McAfee-GW-Edition	⚠ BehavesLike.Win32.Dropper.tc
Microsoft	⚠ Trojan:Win32/Occamy.C	Panda	⚠ Trj/GdSda.A
Qihoo-360	⚠ Win32/Trojan.Ransom.f73	Rising	⚠ Ransom.Gen18.DE83 (CLOUD)
Sophos AV	⚠ Mal/Generic-S	Symantec	⚠ Trojan Horse
Tencent	⚠ Win32.Trojan.Raas.Auto	TrendMicro	⚠ Ransom_ZOLDON.THHAOAH
TrendMicro-HouseCall	⚠ Ransom_ZOLDON.THHAOAH	VBA32	⚠ BScope.Trojan.Bitrep
Webroot	⚠ W32.Malware.Gen	Zillya	⚠ Trojan.GenericKD.Win32.137184
ZoneAlarm	⚠ Trojan-Ransom.Win32.Gen.kgx	AegisLab	✔ Clean