باسمه تعالی

تحلیل فنی باج‌افزار ZOLDON Crypter V۳.۰

مقدمه :

مشاهده و رصد فضای سایبری در زمینه باج‌افزار، از شروع فعالیت نمونه جدیدی از خانواده‌ی باج‌افزار ZOLDON Crypter V۳.۰ که با نام های encryptor-extortionist, doxware نیز شناخته می‌شود خبر می‌دهد. بررسی‌ها نشان می‌دهد که فعالیت این باج‌افزار در اوایل ماه آگوست سال ۲۰۱۸ میلادی شروع شده است و به نظر می‌رسد تمرکز آن بیشتر بر روی کاربران انگلیسی زبان می‌باشد. این باج‌افزار برای محیط‌های دارای سیستم عامل ویندوز ٦٤ بیتی توسعه یافته و برخلاف اکثریت باج افزارها پسوند فایل ها را پس از رمزگذاری عوض نمی کند. به نظر می‌رسد باج افزار ZOLDON Crypter V۳.۰ در حال توسعه بوده و در آینده شاهد نسخه های کاملتری از آن باشیم.

مشخصات فایل اجرایی :

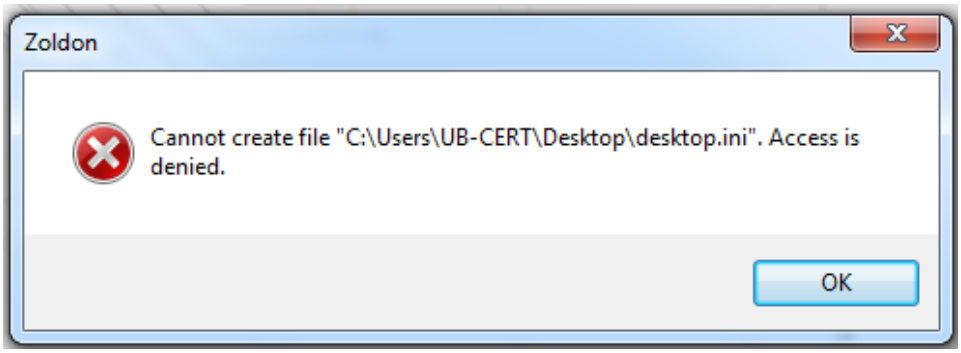
نام فایل	***ZOLDON Bitcoin Miner Pro V۳.۱.exe***
اندازه	۱.۳٦ MB
SHA-۱	e٤ec۰۹٤f٤۰f۳٥۰٥b۲cvf٥e٦f۹۹۳۰b۱vbca۰۹f٥٤۱
SHA-۲٥٦	٥۱٥٦۹٦aafeaav٧٤dd۰f٤۰۳۸b۲٤۳۳٦f٦۳٦a۹۲٥eacbvbv۷۰aa٤٦۹bda۲۲ba۹d٤d۱۳b
MD٥	ce۲۰fb٤c٦d٤٤v۹v۲٥۹۳٥٥b٥fvefb۹۰٤c
کامپایلر	UPX -> www.upx.sourceforge.net

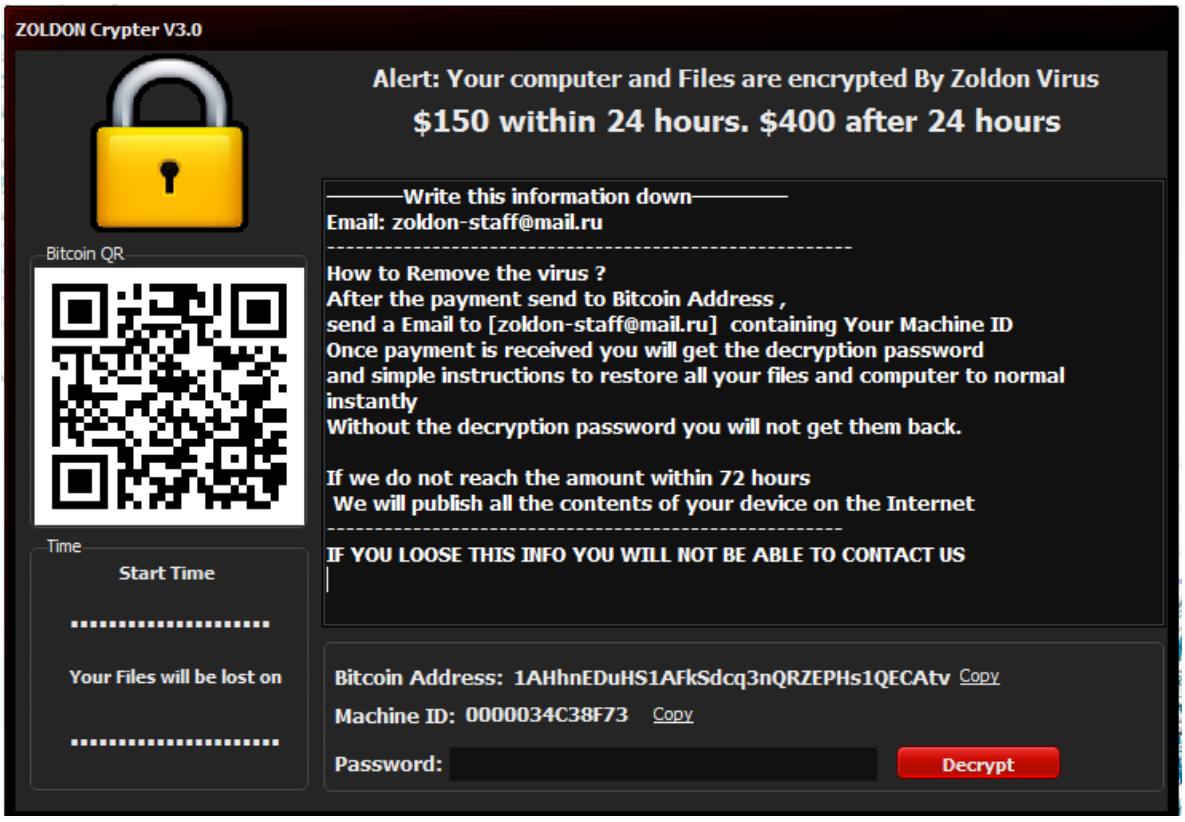
فایل اجرایی این باج‌افزار دارای هفت بخش است :

نام بخش	آنتروپی	آدرس مجازی	اندازه مجازی	اندازه خام
UPX۰	۰	٤۰۹٦	۳۲۸٤۹۹۲	۰
UPX۱	۷.۹٤	۳۲۸۹۰۸۸	۱۳۲۳۰۰۸	۱۳۲۰۹٦۰
.rsrc	۳.۸۳	٤٦۱۲۰۹٦	۱۱۰٥۹۲	۱۰۸٥٤٤

تحلیل پویا :

برای بررسی عمیق‌تر باج‌افزار ZOLDON Crypter V۳.۰ ، فایل اجرایی آن را در محیط آزمایشگاهی اجرا کردیم تا عملکرد باج‌افزار را از نزدیک مورد بررسی قرار دهیم. نتایج حاصل از این بررسی نشان داد که پس از خطای زیر باج‌افزار پنجره باج خواهی به شکل زیر را می گشاید.





طبق بررسی ها، این باج افزار فایل ها را رمزگذاری نمی‌کند.

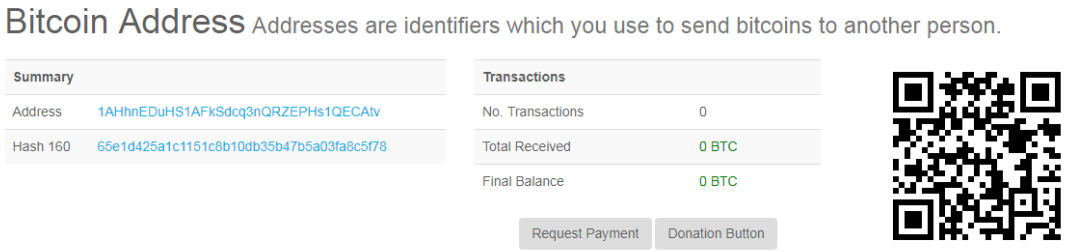
باج‌افزار برای رمزگشایی فایل‌ها، از قربانیان طلب ۱۵۰ دلار بیت کوین به عنوان باج می‌کند و مدت ارسال باج را ۲٤ ساعت اعلام کرده است که در صورت عدم پرداخت مبلغ باج را به ٤۰۰ دلار افزایش داده و ۲٤

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

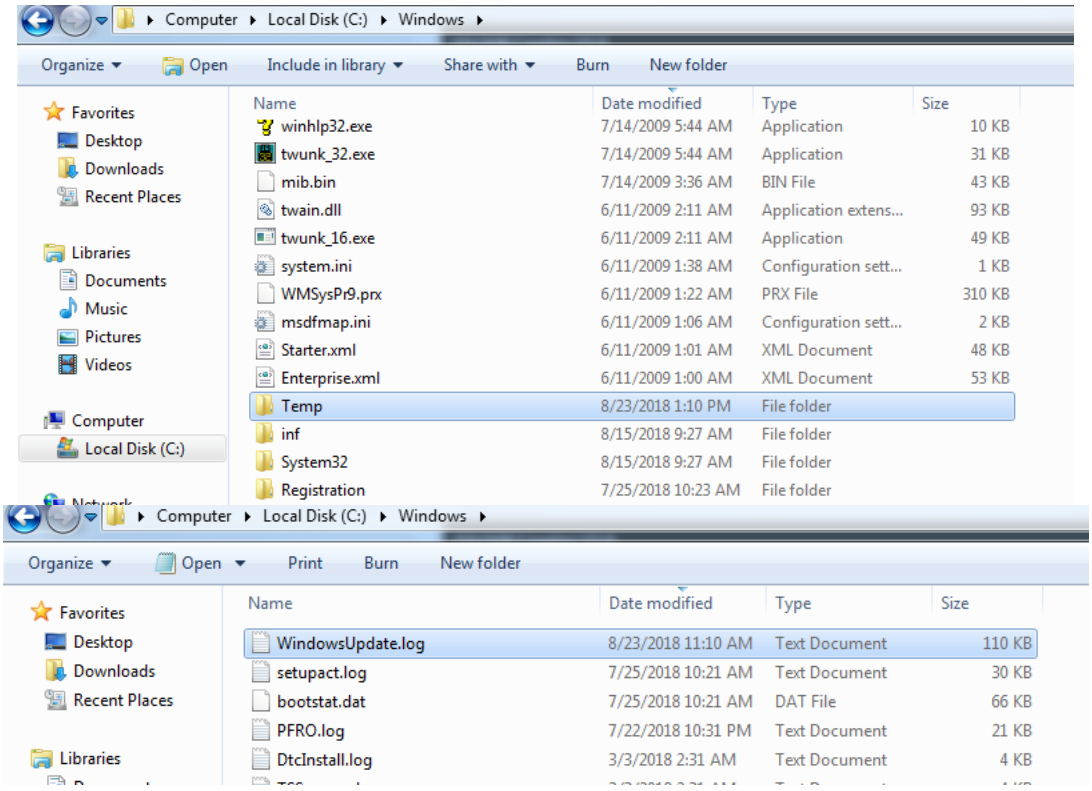
ضمناً قربانیان می‌بایست مبلغ باج را به آدرس کیف پول بیت کوین زیر ارسال نمایند.

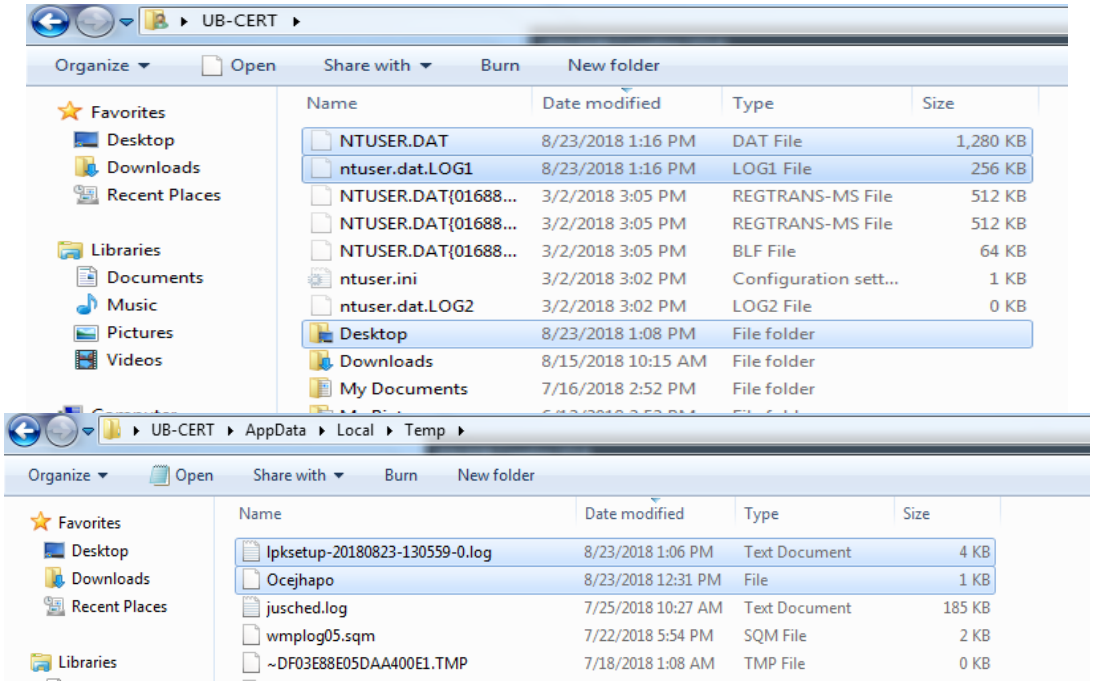
1AHhnEDuHS1AFkSdcq3nQRZEPHs1QECAtv

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

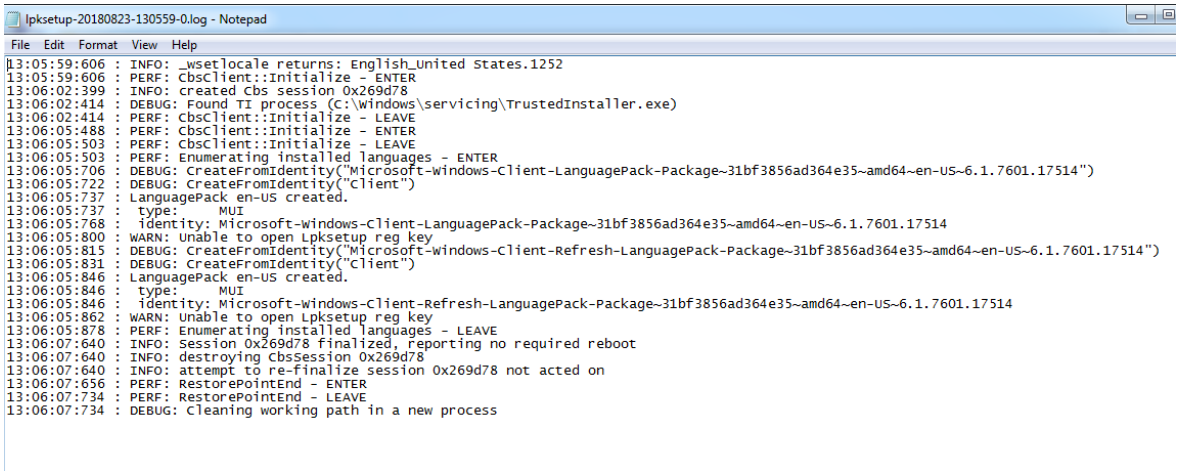


در تصاویر زیر فایل های اضافه شده و تغییر یافته در مسیر درایو سیستم عامل و پوشه Windows پس از اجرای باج‌افزار را مشاهده می‌کنید :

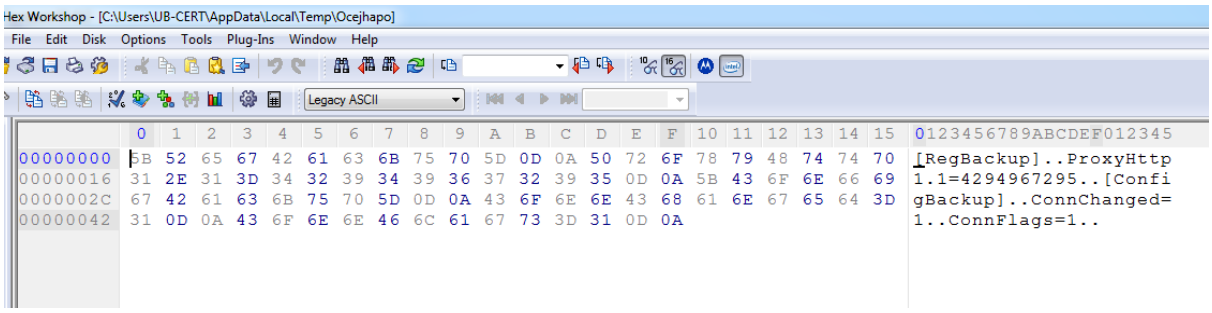




محتوای فایل lpksetup-۲۰۱۸۰۸۲۳-۱۳۰۵۵۹-۰.log



محتوای فایل Ocejhapo



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

تحلیل ایستا :

پس از تحلیل کد فایل اجرایی باج‌افزار ZOLDON Crypter V۳.۰ 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.

UPX۱ with unusual entropies ۷.۹۳٦۸٤۸۰۸٥۹۸

"Sample_٥b٦da۱۷٤cb٤ca٥٤ad۰ca۷eb٥.exe.bin" has a section named "UPX۰"
"Sample_٥b٦da۱۷٤cb٤ca٥٤ad۰ca۷eb٥.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 ٢٤ 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.drv**
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_٥b٦da١٧٤cb٤ca٥٤ad٠ca٧eb٥.exe (PID: ٣٤٠٤)

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\Z0ldon

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\Z0ldon: "C:\Users\UB-CERT\Desktop\Sample_5b6da174cb4ca54ad0ca7eb5.exe"
HKU\S-1-5-21-2853862532-1823478465-2883723831-1000\Software\Z0ldon\start: "8/20/2018"

تحلیل ترافیک شبکه :

پس از بررسی ترافیک شبکه، متوجه هیچ گونه درخواست DNS و تلاش برای برقراری ارتباط با میزبـان در نقطه‌ی جغرافیایی خاص توسط باج‌افزار ZOLDON Crypter V۳.۰ نشدیم.

ابزار رمزگشایی :

در حال حاضر وجود ندارد.

شناسایی :

در حال حاضر تعداد ٤١ مورد از ٦٧ 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.Gen!8.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