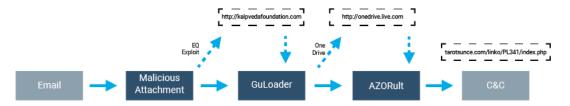
Malware Analysis Spotlight: AZORult Delivered by GuLoader

X vmray.com/cyber-security-blog/azorult-delivered-by-guloader-malware-analysis-spotlight/





Earlier this year, in one of our blog posts we covered <u>GuLoader</u>, a downloader outfitted with advanced anti-analysis techniques that has delivered FormBook, NanoCore, LokiBot, and Remcos among others. Recently, we've observed GuLoader delivering AZORult.

Active for many years, AZORult is an information stealer that has seen many iterations and is typically spread via spam emails or malicious software.

GuLoader's evasive techniques coupled with AZORult's information-stealing capabilities make this an interesting combination for an attacker to hit their target.

In this Malware Analysis Spotlight, we will analyze a delivery chain that uses malicious e-mail attachments and GuLoader to spread AZORult.

Analysis of the AZORult Delivery Chain

Our investigation started from a single sample that matched our AZORult v3 network communication <u>YARA rule</u>. We decided to get more background information and look for the delivery method. The delivery payload turned out to be an RTF document delivered as an email attachment (Figure 1) and exploiting a vulnerability in one of Microsoft's Office products.

Starting from the email, the attack actually contained three steps and downloaded two payloads during its execution. At least one of the payloads was AZORult. We also investigated the other parts of the executions chain and it turned out that the infamous GuLoader was used as one of the links in the execution chain.

🌍 PO NO. 135 Resin 6711 - Mozilla Thunderbird	_		×
<u>Eile E</u> dit <u>V</u> iew <u>G</u> o <u>M</u> essage <u>T</u> ools <u>H</u> elp			
🖵 Get Messages 👻 🖋 Write 🗖 Chat 🗿 Address Book 🛛 🖏 Tag 🌱			≡
From 🔂 🦘 Reply All 🗸	→ Fo	rward	More ~
Subject PO NO. 135 Resin 6711	11/	9/2020,	8:28 PM
To 🏠			
Dear Sir,			
Pls find enclosed herewith Purchase Order no. 135 Dated- 10.11.2020 of M/s. Reliance	e Indu	stries I	Ltd.
1. Resin (6711) ; 21 MT ; @ 99.	.031		
Thanks & Regards			
The second se			
a to period other second			
A D COLORADO			
✔ ① 1 attachment: PO .doc 831 KB) Save 🗸
PO.doc 831 KB			
(*)			

Figure 1: Spam email that delivers the malicious RTF document.

Line Balandar

The document is abusing the equation editor (<u>CVE-2017-11882</u>) vulnerability to achieve execution on the victim's machine. This leads to the download and execution of the next payload which is GuLoader (Figure 2).

In our investigation, we found multiple unique domains responsible for hosting the GuLoader payload (see list of IOCs) associated with similar spam emails leveraging this type of execution chain.

lost B	ehavior					
*	File (1)					
	Operation	Filename	Additional Information	Success	Count	Logfile
	Create	C:\Users\aETAdzjz\AppData\Roaming\fghvhghvgfdgfhchfg.exe	desired_access = GENERIC_WRITE, file_attributes = FILE_ATTRIBUTE_NORMAL	\checkmark	1	FN
*	Process (1)					
	Operation	Process	Additional Information	Success	Count	Logfile
	Create	C:\Users\aETAdzjz\AppData\Roaming\fghvhghvgfdgfhchfg.exe	cmd_line = C:\Users\aETAdzjz\AppData\Roaming \fghvhghvgfdgfhchfg.exe, show_window = SW_SHOWNORMAL	\checkmark	1	FN

Figure 2: VMRay Analyzer – Download of the next GuLoader payload by exploiting a vulnerability in the equation editor.

As we have described in one of our previous <u>Threat Bulletin</u>, GuLoader is equipped with advanced anti-analysis, sandbox detection, and evasion techniques to increase its chances of delivering malware to its intended target.

In the <u>VMRay Analyzer Report</u>, we observed the typical behavior of GuLoader, using shellcode in two instances (processes). The shellcode uses its advanced techniques to thwart dynamic analysis followed by the final payload downloaded from a publicly available cloud provider.

Compared to the previously analyzed GuLoader samples, this one shows additional behavior in the enumeration of products currently advertised/installed (<u>MsiEnumProductsA</u>) and services (<u>EnumServicesStatusA</u>) (Figure 3). This might be an indicator of further detection or evasion techniques present in this GuLoader sample.

	EnumWindows (lpEnumFunc=0x2504cf, lParam=0x18f254) returned 1	F0195.4991	EnumWindows (lpEnumFunc=0x1c01bs, 1Param=0x19f758) returned 1
[0111.913]	LoadLibraryA (lpLibFileName="ntdll") returned 0x77bb0000		LoadLibrary& (lpLibFileName="nudl]") returned 0x77970000
[0111.914]	LoadLibraryA (lpLibFileName="ntdll") returned 0x77bb0000		LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
[0111.914]	LoadLibraryA (lpLibFileName="ntdll") returned 0x77bb0000		LoadLibrary% (lpLibFileName="ntdll") returned 0x77970000
	NtFrotectVirtualMemory (in: FrocessHandle=0xffffffff, BaseAddress=0x18f23c*=0x77bc0000, NumberOfBytes		NtProtectVirtualMemory (in: ProcessHandle=0xffffffff, BaseAddress=0x19f740*=0x'
	NtFrotectVirtualMemory (in: FrocessHandle=0xffffffff, BaseAddress=0x18f23c+=0x77bc0000, NumberOfBytes		
	LoadLibraryA (lpLibFileName="ntd11") returned 0x77bb0000		NtProtectVirtualMemory (in: ProcessMandle=0xffffffff, BaseAddress=0x19f740*=0x'
	NtSetInformationThread (ThreadMandle=Oxffffffe, ThreadInformationClass=Ox11, ThreadInformation=Ox0,		LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
	LoadLibraryA (lpLibFileName="kernel32") returned 0x75b90000		<pre>NtSetInformationThread (ThreadHandle=Oxffffffffe, ThreadInformationClass=Oxll, '</pre>
	CreateFileA (LpFileName="C:\\Program Files\\Qemu-ca\\qemu-ca.exe" (normalized: "c:\\program files\\ge		LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
	CreateFileA (lpfileName="C:\Program FileS\\qga\\qga <exe" "c:\program="" (mormalized:="" files\\qga\qga.e<="" td=""><td></td><td>CreateFileA (lpFileName="C:\\Program Files\\Qemu-ga\\qemu-ga.exe" (normalized:</td></exe">		CreateFileA (lpFileName="C:\\Program Files\\Qemu-ga\\qemu-ga.exe" (normalized:
	Createriles (aprilename-C://rogram files/\dga.dga.exe (hormalized: "C://program files/\dga.dga.e LoadLibtary% (hplibFileName-modl") returned 0x77bb0000		CreateFileA (lpFileName="C:\\Program Files\\qga\\qga.exe" (normalized: "c:\\pro
		[0202.762]	LoadLibrary& (lpLibFileName="ntdll") returned 0x77970000
	NtAllocateVirtualMemory (in: ProcessMandle=Oxffffffff, BaseAddress=Ox18f2c0+=0x0, ZeroBits=Ox0, Regio	[0202.772]	NtAllocateVirtualMemory (in: ProcessHandle=0xffffffff, BaseAddress=0x19f7c4*=0:
	LoadLibraryA (lpLibFileName="Msi.dll") returned 0x745e0000	[0202.854]	LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
	LoadLibraryA (lpLibFileName="Hsi.dll") returned 0x745e0000	[0202.855]	LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
	MsiEnumProductsA (in: iProductIndex=0x0, lpProductBuf=0x3a70000 out: lpProductBuf="(90160000-008C-	[0202.855]	LoadLibrary& (lpLibFileName="ntdll") returned 0x77970000
[0112.067]	MsiGetProductInfo& (in: szProduct="(90160000-008C-0000-1000-0000000FFICE)", szAttribute="Publisher",	10202.8551	LoadLibrary& (lpLibFileName="ntdll") returned 0x77970000
			LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
			LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
			LoadLibrary& (lpLibFileName="ntdll") returned 0x77970000
[0112.072]	MsiEnumProductsA (in: iProductIndex=0x4, lpProductBuf=0x3a70000 out: lpProductBuf="(ad8a2fal-06e7-		LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
0112.0731	MsiGetFroductInfoA (in: szFroduct="(ad8a2fal-06e7-4b0d-927d-6e54b3d31028)", szAttribute="Publisher",		
00000000000	LoadLibraryA (lplibFileName="ntdll") returned 0x77bb0000		LoadLibraryA (lpLibFileName="ntdll") returned 0x77970000
	LoadLibraryA (lpLibFileName="ntdll") returned 0x77bb0000		LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
	LoadLibrarvA (lpLibFileName="ntdll") returned 0x77bb0000		LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
	LoadLibraryA (pLibFileName"noll') returned 0x77bb0000		LoadLibrary& (lpLibFileName="kernel32") returned 0x772d0000
	LoadLibraryA (pLibFileName"nodl") returned 0x77bb0000		LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
			LoadLibrary& (lpLibFileName="kernel32") returned 0x772d0000
	LoadLibraryA (lpLibFileName="ntdll") returned 0x77bb0000	[0202.857]	LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
	LoadLibraryA (lpLibFileName="ntdll") returned 0x77bb0000	[0202.050]	LoadLibraryA (lpLibFileName="kernel32") returned 0x772d00000
	LoadLibraryA (lpLibFileName="ntdll") returned 0x77bb0000	[0202.858]	LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
	LoadLibrary& (lpLibFileName="ntdll") returned 0x77bb0000	[0202.858]	LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
[0112.101]	LoadLibraryA (lpLibFileName-"kernel32") returned 0x75b90000	[0202.858]	LoadLibraryA (lpLibFileName="kernel32") returned 0x772d0000
	LoadLibrarv& (lpLibFileName="advapi32") returned 0x75cf0000	10210.222	Loadlibraryd (151ibFilaNamasTadyani337) raturnad 0275460000
[0112.114]	NtGetContextThread (in: ThreadHandle=0xfffffffe, Context=0x3a65004 out: Context=0x3a65004*(ContextFlags=0x10010)		LoadLibraryA (IpLibFileName="advap132") returned 0x7560000
[0112.114] [0112.115]	NtGetContextThread (in: ThreadHandle=0xfffffffe, Context=0x3a65004 out: Context=0x3a65004*(ContextFlags=0x10010, OpenSCHanagerA (lpHachineName=0x0, lpDatabaseName=0x0, dwDesiredAccess=0x4) returned 0x2a7ee0	0210.229	NtGetContextThread (in: ThreadHandle=0xfffffffe, Context=0x3055004 out: Context=
[0112.114] [0112.115] [0112.120]	MtGetContextThread(in: ThreadHandle='xffffffe, Context='xla65004 out: Context='xla65004 (ContextFlags=0x10010, OpenSCMsagerA (lpHschineNam='xx), lpDstabaseNam='xx), dxGetred&cces='xxi) returned (xla7ee) LoadLibrary, (lpLbFleNam='xxxy:1x)-returned (xla7ef0000	0210.229	<pre>NtGetContextThread (in: ThreadHandle=0xffffffe, Context=0x3055004 out: Context= CreateProcessInternalW (in: hUserToken=0x0, lpApplicationName="C:\\Users\\FDIHVy\\</pre>
[0112.114] [0112.115] [0112.120] [0112.126]	NG+CONSTANTING (in: Turesdiand=-Virtual/STFFFF, Constan-VilatSO() Gut Constan-VilatSO()+(ConstanTing=-01000) Constant-Virtual(), Distant-Virtual(Stant-Virtual), Gut Constant-Vilate() LoskLineryA (DilbTileName-Virtual)) NG+CONSTANTING (in: Turesdiand=-Virtual)), Gut Constant-VilatSO()+(ConstantFing=-01000),	0210.229 0210.232 0210.246	<pre>HtGetContextThread (in: ThreadHandl==0xffffffe, Context=0x3055004 out: Context= CreateProcessInternalW (in: hUserTokenexx0, lpApplicationName="C:\Users\\FDINVy\\ LoadLibray& (lpLibFileName="ncdl") returned 0x7970000</pre>
[0112.114] [0112.115] [0112.120] [0112.126]	MtGetContextThread(in: ThreadHandle='xffffffe, Context='xla65004 out: Context='xla65004 (ContextFlags=0x10010, OpenSCMsagerA (lpHschineNam='xx), lpDstabaseNam='xx), dxGetred&cces='xxi) returned (xla7ee) LoadLibrary, (lpLbFleNam='xxxy:1x)-returned (xla7ef0000	0210.229 0210.232 0210.246 0210.254	NideContextThread (in: ThreadBandle="wifffffe, Context="%1055004 out: Context= CreateForcesinternalW (in: NberToken="%0;]kpglicationName="%10bertolWFDIMV\ LoadLibraryA (lpLibFleName="midli") returned %77970000 NideContextThread (in: ThreadBandle="wifffffe, Context="%1055004 out: Context="%1055004")
[0112.114] [0112.115] [0112.120] [0112.126] [0112.127]	NG+CONSTANTING (in: Turesdiand=-Virtual/STFFFF, Constan-VilatSO() Gut Constan-VilatSO()+(ConstanTing=-01000) Constant-Virtual(), Distant-Virtual(Stant-Virtual), Gut Constant-Vilate() LoskLineryA (DilbTileName-Virtual)) NG+CONSTANTING (in: Turesdiand=-Virtual)), Gut Constant-VilatSO()+(ConstantFing=-01000),	0210.229 0210.232 0210.246 0210.254 0210.254]NUGECONCENTIAread (in: ThreadMandle=Neffffff, Context=NeNOSOOF out: Context= CreateFrocesInternalN (in: NUserToken=NM), [phplicationName="Ci\Users\VDiPy\ LoadLhargy (clubPileName="Cill") returned ox"39"0000 NUGECONTExtThread (in: ThreadMandle=Neffffff, Context=NUSOOOF out: Context= NUDmapViewOffsetion (FrocesMandle=Niff, BasAddres=NuSOOOO) returned 0x0
[0112.114] [0112.115] [0112.120] [0112.126] [0112.127] [0112.132]	NGetConcestTaread (in: TarcedMandle-Scifffo, Context-GlabitOC out: Context-SlabOol+(ContextFlage-GlaOol) OpenSCMangerA (lpLibTlaMame=Nong), lpDatabaseBame=Non, dxGetredAocess=Ost) returned 0x2aTeco DadLibraryA (lpLibTlaMame=Nong)32" returned 0x75cT0000 NuGetContextThread (in: ThreadMandle-Scifffffe, Context-SlabSOOl+(ContextFlage-Cx1001), EmmderviceStatak (in: Nichamage=Cw12aTec, dxderviceTyme=Nich, dxderviceState=Nich, lpServices=Cx13T000c, cbbdf	[0210.229] [0210.232] [0210.246] [0210.254] [0210.261] [0210.269]	NVORCONCENTRY-SS (in: ThreadMandt=bgfffff, Context=bg055004 out: Context= CreateFroceshierenaW (in: NberTokem-bb, jabplicationMame="C:\Ubers/VDUHY/ LoadLbaryA (jpLiFleName="null") returned (w7970000 NberContextFired (in: ThreadMandt=bgfffff, Context=bg155004 out: Context= NtDmsgViewOfSetion (ProcessIanl=bg18, BaseAddress=bg15000) returned 000 NberContextFired (in: ThreadMandt=bg1ffff, Context=bg155004) out: Context= NtDmsgViewOfSetion (ProcessIanl=bg18ff, Context=bg155004) out: Context=
[0112.114] [0112.115] [0112.120] [0112.126] [0112.127] [0112.132] [0112.132]	NGetConstatTured (in: Turesdiand=-offffff, Contar-Glass) out Context-class(0)+(ContextFlag=-0:1012) CpenDChanger(LiphchineHame-N), lptthatestman=VM, objectiredAccess=VR) returned 0x1a*ee0 LoskLinraryA (lpLibrileHame=*drugh13*) returned 0x75ef000 NGetContextFlag=dianle=-offfffe, Context-VasA65004 out Context-class(0)+(ContextFlag=-0x1001), ImuderviceStatusA (in: hSCHanger=VasA62), ddetviceTyp=vXN0, ddetviceState=VR), lpfervices=vk187000, cbBuff LoskLinraryA (lpLibrileHame=*drugh13*) returned 0x75ef0000	[0210.229 [0210.232 [0210.246 [0210.254 [0210.261 [0210.269 [0210.277	NüderContextThread (in: ThreadMandle=wigfffff, Context=wig055004) out: Context= CreateFrocestInternalW (in: NbertOken=Wig, lphpliationRame="citUbers/NDERWy/ LoadLhearyA (phiLFileMame="citUt") returned %x7970000 RiberContextThread (in: ThreadMandle=wigfffff, Context=wig050504) out: Context= RiberContextThread (in: ThreadMandle=wigffff), Context=wig050504) out: Context= RiberContextThread (in: ThreadMandle=wigfff), Context=wig050504) out: Context= RiberContextThread (in: ThreadMandle=wigfff), Context=wig050504) out: Context=
[0112.114] [0112.120] [0112.120] [0112.126] [0112.127] [0112.132] [0112.133]	NGetConstatTured (in: Turesdiand:=%ffffff, Contat-inision (out Contat-inision*(ContatTiag=~0.101.) GenCManaget (plothindiane=work), lpothedrame=w0, wdoestreducess=w0.) retured 0x1a*ee LeadLitraryA (lpLibiledame=*drugn13*) retured 0x75cf000 NGetContatThread (in: ThreadManle=%fffffe, Contat-Vanka6500) (out Contat-CalaGood*(ContatTiag=~0x1001), ImmderviceStatusA (in: hSCHanaget=%classe), dderviceTyp=~0x10, dderviceState=%s), lpServices=%x187000c, cbBuff LoadLitraryA (lpLibiledame=*drugn13*) retured 0x7150000	[0210.229 [0210.232 [0210.246 [0210.254 [0210.261 [0210.269 [0210.277 [0210.330]	NVOCTOORENTIAread (in: ThreadMandle=bgfffff, Context=bg1055004 out: Context= CreateFrocestInternalW (in: NberTokem-bv0, jabplicationMames"Ci\Users/NVDHWY\ LoadLbaryA (jpLiFileName="soli1") returned (w7970000 NbetContextEntread (in: ThreadMandle=bgfffff, Context=bg105004 out: Context= NtDmagView0f5etion (ProcessIanle=bg10, BaseAddress=bg1000) returned 0x0 NbetContextEntread (in: ThreadMandl=bg10fff, Context=bg1000) returned 0x0 NbetContextEntread (in: ThreadMandl=bg10fff, Context=bg1000) returned 0x0 NbetContextEntread(in: ThreadMandl=bg10fff, Context=bg1000) returned 0x0 NbetContextEntread(in: ThreadMandl=bg10fff, Context=bg1000) returned 0x0 NbetContextEntread(in: ThreadMandl=bg10fff, Context=bg1000) returned 0x0 context= NbetContextEntread(in: ThreadMandl=bg10fff, Context=bg10000) returned 0x0 context=
[0112.114] [0112.120] [0112.120] [0112.126] [0112.137] [0112.132] [0112.132] [0112.135] [0112.141]	NdetConsexThread (in: ThreadManle=Chiffff, Context=CaleSOO() out Context=CaleSOO(ContextFlage=CalOD), DescRingarya (lpithielame=ContextCaleSon), DetabaseRing=Context=CaleSon() returned CaleTeo LoadLinearya (lpithielame=ContextCaleTeo, Context=CaleSOO() out Context=CaleSoO((ContextFlage=CalOD), NomeContextFlage=CalOD), TextDesCaleTeo, descript=CalO, descript=CalOD, ISSUE InsetTeorements (ln: hSCBanageroScalete, descript=CalOD), descript=CalOD, descript=CalOD), Context=CalOD, CaloEC, CaloEC, descript=CalOD, descript=CalOD, descript=CalOD, descript=CalOD), Context=CalOD, CaloEC,	[0210.229] [0210.232] [0210.246] [0210.254] [0210.261] [0210.269] [0210.330] [0210.339]	NöörContextThread (in: ThreadMandle=virfffff, Context=virl050504 out: Context= CreateFrocestInternalW (in: NberToke=nob, jabpliatoitanMase="ci\Uberty=i\Ub
[0112.114] [0112.125] [0112.120] [0112.127] [0112.132] [0112.132] [0112.132] [0112.132] [0112.141] [0112.147]	NGetConstatTured [in: Turesdiand=wfffffff, Contart-Ministor] out Context-ministor+(ContextFlags-0x100.2) CpenDSdmaper[in:[internation=wco,]pittaberBamew00, wdoestredAccessw0rd] returned 0x2a*eo LoskiltraryA [pitkFleBame="download" NGetContextFlags=download" LoskiltraryA [pitkFleBame="download" LoskiltraryA [pitkFleBame="download" LoskiltraryA [pitkFleBame="download" LoskiltraryA [pitkFleBame="download" LoskiltraryA [pitkFleBame="download" LoskiltraryA [pitkFleBame="download" LoskiltraryA [pitkFleBame="download" LoskiltraryA [pitkFleBame="download" NGetContextFlags=0x10010, NGetC	[0210.229] [0210.232] [0210.242] [0210.264] [0210.269] [0210.269] [0210.370] [0210.339] [0210.347]	NVOCTOORENTIPHEAG (in: ThreadMandle=bgfffff, Context=bg055004 out: Context= CreateFrocestInternalW (in: NberTokem-bv0, jabplicationMame="Ci\Users/VDUHVy\ LoadLbaryA (jpLiFileMame="sol1") returned (w7970000 NbectContextFiresd (in: ThreadMandle=bgfffff, Context=bg05004) out: Context= NtDmayViewOffection (ProcessMandle=bgffff, Context=bg05004) out: Context= NtDectContextFiresd (in: ThreadMandl=bgffff, Context=bg05004) out: Context= NtCertoIntextFiresd (in: ThreadMandl=bgffff, Context=bg05004) out: Context= NtCertoIntextFiresd (in: ThreadMandl=bgffff, Context=bg05004) out: Context=
[0112.114] [0112.115] [0112.120] [0112.126] [0112.127] [0112.132] [0112.132] [0112.133] [0112.147] [0112.147]	NdetConstarThread (in: ThreadManle="xffffff, Context-%lat600" out Context-slat600" (ContextFlage-%l010), OpenChanger(LiptachineMane="xdvglill") returned 0x75cf000 LoddLineray(LiptachineMane="xdvglill") returned 0x75cf000 HostContextFlage-%l010], EnamEervicedstatum& (in: hdChangerwick1)*ec, doterviceType=%20, doterviceState=%l, lpServices%la7000c, dbWf LoddLineray(LiptaChineMane="xdvglill") returned 0x75cf000 LoddLineray(LiptaChineMane="xdvglill") returned 0x75b000 HostContextFlage=%x101"), returned 0x75b000 HostContextFlage=%x101"), returned 0x75b000 HostContextFlage=%x101"), returned 0x75b000 HostContextFlage=%x101", returned 0x75b000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x10000 HostContextFlage=%x100000 HostContextFlage=%x100000 HostContextFl	[0210.229] [0210.246] [0210.254] [0210.269] [0210.267] [0210.330] [0210.339] [0210.355]	NööstöntestThread (in: ThreadMandle-sigfffff, Context-slö55004 out: Context- CreateFrocest/NorINY/L LadiLbraryA (bjLbFleMame-"scill") returned %x7970000 NössTortest() (bjLbFleMame-"scill") returned %x7970000 NössTortest() (bjLbFleMame-"scill") returned %x80 NössTortest() (bjLbFleMame-"scill") returned %x80 NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLFleMame-"scill") (bjLFleMa
[0112.114] [0112.115] [0112.126] [0112.126] [0112.127] [0112.132] [0112.132] [0112.135] [0112.141] [0112.141] [0112.143] [0112.153]	NetectonsearEnced (in: ThreadManle="offffff, Constar-Glassics") out Constar-Glassics' Constar-Glassics	[0210.229 [0210.234] [0210.254] [0210.254] [0210.261] [0210.267] [0210.330] [0210.339] [0210.339] [0210.347] [0210.347]	NüderContextThread (in: ThreadMandle=wifffff, Context=wid05000) out: Context- CreateFrocestInternalW (in: NberToken=Wig, japplicationMames="citUbers/ LoadLhearyA [cpLiFileImas="statl"] returned my"190000 HittageYimeOntion (frocesMandle=wifffff, Scheddress=(Statl)) out: Context= HittageYimeOntion (frocesMandle=wifffff, Context=wi005000) out: Context= HittageYimeOntion(frocesMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOntextThread (in: ThreadMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOntextThread(in: ThreadMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOntextThread(in: ThreadMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOffection (in: SectionMandle=wiffffff, Context=wiff), BaeAddress=wiff) HittageYimeOffection (in: SectionMandle=wiffffff, Context=wiff) HittageYimeOffection (in: SectionMandle=wiffffff, Context=wiff)), BaeAddress=wiff)
[0112.114] [0112.115] [0112.120] [0112.126] [0112.127] [0112.132] [0112.132] [0112.132] [0112.141] [0112.141] [0112.147] [0112.140]	NdetConstarThread (in: ThreadManle=Nffffff, Constar=Nla6500 out Constar=Nla6500*(ConstarThag=OutOUT) CompConstant, [lphchinelmac.wol, lphchaetMame/00, hotSciredocessor() returned OutDate() LoadLitraryA (lphLhileHame=No, lphchaetMame/00, hotSciredocessor() returned OutDate() EnamEerviceSciredocessor() returned OutDate() out Constar=Nla6500*(ConstarFlag=OutOUT) EnamEerviceSciredocessor() returned OutDate() defension out Constar=Nla6500*(ConstarFlag=OutOUT) EnamEerviceSciredocessor() returned OutDate() EnamEerviceSciredocessor() returned OutDate() CloseSciredocessor() returned OutDate() EnamEerviceSciredocessor() returnedOutDate() EnamEerviceSciredocessor() returnedOutDate() EnamEerviceSciredocessor() returnedOutDate() EnamEerviceSciredocessor() returnedOutDate() EnamEerviceSciredocessor() returnedOutDate() EnamEerviceSciredocessor() returnedOutDate() EnamEerviceSciredocessor() ret	[0210.229 [0210.234] [0210.254] [0210.254] [0210.261] [0210.267] [0210.330] [0210.339] [0210.339] [0210.347] [0210.347]	NööstöntestThread (in: ThreadMandle-sigfffff, Context-slö55004 out: Context- CreateFrocest/NorINY/L LadiLbraryA (bjLbFleMame-"scill") returned %x7970000 NössTortest() (bjLbFleMame-"scill") returned %x7970000 NössTortest() (bjLbFleMame-"scill") returned %x80 NössTortest() (bjLbFleMame-"scill") returned %x80 NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLbFleMame-"scill") (bjLbFleMame-"scill") NössTortest() (bjLbFleMame-"scill") (bjLFleMame-"scill") (bjLFleMa
[0112.114] [0112.120] [0112.120] [0112.122] [0112.122] [0112.132] [0112.135] [0112.141] [0112.141] [0112.141] [0112.140] [0112.140] [0112.140]	NdetConstarThread (in: ThreadManle=Conffrence, Constar-Caladious) out Constar-Caladious (ConstarFlags-Calod), ConstarFlags-Calod),	[0210.229] [0210.2346] [0210.246] [0210.264] [0210.269] [0210.277] [0210.377] [0210.339] [0210.347] [0210.347] [0210.347] [0210.442]	NüderContextThread (in: ThreadMandle=wifffff, Context=wid05000) out: Context- CreateFrocestInternalW (in: NberToken=Wig, japplicationMames="citUbers/ LoadLhearyA [cpLiFileImas="statl"] returned my"190000 HittageYimeOntion (frocesMandle=wifffff, Scheddress=(Statl)) out: Context= HittageYimeOntion (frocesMandle=wifffff, Context=wi005000) out: Context= HittageYimeOntion(frocesMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOntextThread (in: ThreadMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOntextThread(in: ThreadMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOntextThread(in: ThreadMandle=wiffffff, Context=wi005000) out: Context= HittageYimeOffection (in: SectionMandle=wiffffff, Context=wiff), BaeAddress=wiff) HittageYimeOffection (in: SectionMandle=wiffffff, Context=wiff) HittageYimeOffection (in: SectionMandle=wiffffff, Context=wiff)), BaeAddress=wiff)
(0112.114) (0112.115) (0112.120) (0112.126) (0112.126) (0112.132) (0112.133) (0112.133) (0112.133) (0112.133) (0112.133) (0112.141) (0112.141) (0112.160) (0112.174) (0112.174)	NdetConstarThread (in: ThreadManle=Affffff, Constar-willeGood) out Constar-willGood (ConstarTiage-OriOod) CompConstant, []phalnielawa-willy, bytabaseMamev00, hytabaseStaredAccessOr() returned OriZafee0 LoadLitrary([]philielawa-winy[]]) returned OriZefo00 EnumeroviceStatusA (in: hOCAnageroAdlete, deferviceType=XEO, deferviceState=Ox), 1pServices-oxisT0000, cbbuff LoadLitrary([]philielawa-winy[]]) returned OriZefo00 CloseSterviceMandle (hDOObject=OxIa) or oxist LoadLitrary([]philielawa-winy[]]) returned OriZefo00 CloseSterviceMandle (hDOObject=OxIa) or oxist LoadLitrary([]philielawa-winy[]]) returned OriZefo00 CloseSterviceMandle (hDOObject=OxIa) or oxist NetworkertThread (in: ThreadManle=Affffff, Constar-winkSt000 out Constar-Vala50004 (ContextFlage=Ox10000, NetworkertThread (in: ThreadManle=Affffff, Constar-Vala5000 out Context-Vala5004 (ContextFlage=Ox10000, CreateFloceStSternal (in: Networker-Ox), lappLationMame-Criver()/Effd(), VapOstar/Networker(), CreateFloceStSternal (in: ThreadManle=Afffffff, Context-Vala5000 out Context-Vala5004 (ContextFlage=Ox1000, NetworkertThread (in: ThreadManle=Afffffff, Context-Vala5000 out Context-Vala5004 (ContextFlage=Ox1000, CreateFloceStSternal (in: ThreadManle=Afffffff, Context-Vala5000 out Context-Vala5004 (ContextFlage=Ox1000, NetworkertThread (in: ThreadManle=Afffffff, Context-Vala5000 out Context-Vala5004 (ContextFlage=Ox1000, NetworkertThread (in: ThreadManle=Affffff, Context-Vala5000 out Context-Vala5004 (ContextFlage=Ox1000, NetworkertContextThread (in: ThreadManle=Affffff, Context-Vala50000) out Context-Vala5004 (ContextFlage=Ox1000, NetworkertContextThread (in: ThreadManle=Affffff, Context-Vala50000) out Context-Vala5004 (ContextFlage=Ox1000, NetworkertContextThread (in: ThreadManle=Affffff, Context-Vala50000) out Context-Vala5004 (ContextFlage=Ox1000, NetworkertContextThread(in: ThreadManle=Afffffff, Context-Vala50000) out Context-Vala5004 (ContextFlage=Ox1000, NetworkertContextThreadManle=Afffffff, Context-Vala50000) out Context-Vala	[0210.229] [0210.346] [0210.346] [0210.364] [0210.364] [0210.360] [0210.330] [0210.330] [0210.335] [0210.347] [0210.345] [0210.403]	NööstöntextThread (in: ThreadMandle=wifffff, Context=wi005500;) out: Context= CreateFrocest/NorINV/L LoadLbraryA (bpLiFileMame="rdd1") returned %r790000 NööstÖntextThread (in: ThreadMandle=wifffff, Context=wi005500;) out: Context= NtÖmegView078ettion (ProcestAndle=wi204, BaseAddress=wi600000) returned 0x0 NtööstÖntextThread (in: ThreadMandle=wifffff, Context=wi005500;) out: Context= NtöpevTile (in: fileManl==wi10f00; Beireddocess=wi00;) objectAttlbress=wi0010100 NtöricontextThread (in: ThreadMandle=wiffff, Context=wi005500;) out: Context= NtöpevTile (in: fileManl=wi10f00; Beireddocess=wi0010; ObjectAttlbress=wi0010; NtöpevTitu. NtöricontextThread (in: ThreadMandle=wiffff), Context=wi00500;) out: Context= Ntöpertofettion (in: SectionManl==wi005), ProcestAndle=wi0014, DavdTress=wi0010; NtöpevTitualMenory (in: ProcestAndle=wi005), BaseAddress=wi0016; Ntőe=wi005 Nt&liooxetvTitualMenory (in: ProcestAndl==wi054, BaseAddress=wi0016; Ntőe=wi054, Bered Ntére=wi0500; Ntőe=wi054, BaseAddress=wi05016; Ntőe=Wi0500; NtållooxetvTitualMenory (in: ProcestAndl==wi054, BaseAddress=wi05016; Ntőe=wi0500; NtállooxetvTitualMenory (in: ProcestAndl==wi054, BaseAddress=wi05016; Ntőe=wi0500; NtállooxetvTitualMenory (in: ProcestAndl==wi054, BaseAddress=wi05016; Ntőe=wi0500; NtállooxetvTitualMenory (in: ProcestAndl==wi054, BaseAddress=wi05016; Ntőe=wi0500; NtállooxetvTitualMenory (in: ProcestAndl==wi054, BaseAddress=wi05016; Ntőe=wi050; NtállooxetvTitualMenory (in: ProcestAndl==wi054, BaseAddress=wi05016; Ntőe=wi050; NtállooxetvTitualMenory (in: ProcestAndl==wi054), BaseAddress=wi05016; Ntőe=wi050; NtállooxetvTitualMenory (in: ProcestAndl==wi054), BaseAddress=wi05016; NtállooxetvTitualMenory (in: ProcestAndl==wi054), BaseAddress=wi05016; NtállooxetvTit
(012.114) (012.115) (012.120) (012.120) (012.127) (012.133) (012.133) (012.133) (012.147) (012.147) (012.160) (012.161) (012.161) (012.174) (012.174)	NdetConstarThread (in ThreadManle=Chiffff, Constar-ChickSOO(out Constar-ChickSOO(ConstarThage-ChiOl), DetConstarThread (in ThreadManle=Chiffff, Constar-ChickSOO(out Constar-ChickSOO((ConstarThage-ChiOl), DetConstarThread (in ThreadManle=Chiffff, Constar-ChickSOO(out Constar-ChickSOO((ConstarThage-ChiOl), DetConstarThread (in ThreadManle=Chiffff, Constar-ChickSOO(out Constar-ChickSOO((ConstarThage-ChiOl), DetConstarThread (in ThreadManle=Chifff, Constar-ChickSOO(out Constar-ChickSOO((ConstarThage-ChiOl), DetConstarThread (in ThreadManle=Chifff, Constar-ChickSOO(out Constar-ChiksSOO((ConstarThage-ChiOl), BioGeonestributed (in ThreadManle=Chifff, Constar-ChickSOO(out Constar-ChiksSOO((ConstarThage-ChiOl), BioGeonestributed (in ThreadManle=Chifff, Constar-ChiksSOO(out Constar-ChiksSOO((ConstarThage-ChiOl), DetConstarThread (in ThreadManle=Chiffff, Constar-ChiksSOO() out Constar-ChiksSOO((ConstarThage-ChiOl), DetConstarThread (in ThreadManle=Chiffff, Constar-ChiksSOO() out Constar-ChiksSOO((ConstarThage-ChiOl), CreatFrocessInternal (In TherToencon, IndepIncationMane=Chi/UserSouthIng) (Lapotan(Thread), UserSouthIng), DetConstarThread (in ThreadManle=Chiffff, Constar-ChiksSOO() Constar-ChiksSOO((ConstarThage-ChiOl), BioGeonestributed (in ThreadManle=Chiffff, Constar-ChiksSOO) (ConstarThage-ChiCol), BioGeonestributed (in ThreadManle=Chiffff, Constar-ChiksSOO) (ConstarThage-Chicol), BioMangYterOffection (ProcessInalle=Chifff, ConstarChiksSOO) (ConstarThage-Chicol), BioMangYterOffection (ProcessInalle=Chifff, ConstarChiksSOO) (ConstarThage-Chicol), BioMangYterOffection ([0210.229] [0210.326] [0210.346] [0210.266] [0210.369] [0210.369] [0210.377] [0210.339] [0210.339] [0210.347] [0210.347] [0210.460] [0210.400] [0210.400] [0210.600]	NüderContextThread (in: ThreadMandle=virfffff, Context=virf05500) out: Context= CreateFrocest/NotHV/L LoadLhearyA (pLikFieldmas="stdll") returned %x790000 HoleContextThread (in: ThreadMandle=virfffff, Context=virf05100) out: Context= NüderContextThread (in: ThreadMandle=virffff, Context=virf05100) out: Context= NüderContextThread (in: ThreadMandle=virfffff, Context=virf05000) out: Context= NüderContextThread (in: ThreadMandle=virffff, Context=virf05000) out: Context= NüderContextThread (in: ThreadMandle=virffff, Context=virf05000) out: Context=virf060000, buffer=virf0100000000000000000000000000000000000
(012.116) (012.120) (012.120) (012.120) (012.123) (012.133) (012.133) (012.133) (012.147) (012.147) (012.160) (012.160) (012.179) (012.179) (012.181)	NetectonsexThread (in: ThreadManl=-offffff, Context-Caladion out Context-Caladion+ContextTage-Calodion Context-Caladion Detailed Section Context-Caladion out Context-Caladion+ContextTage-Calodion LoadLiteraryA (pluFiled Section, Detailed Section Context-Caladion+ContextTage-Calodion LoadLiteraryA (pluFiled Section, Detailed Section) Context-Caladion+ContextTage-Calodion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage-Calodion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage-Calodion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage-Caladion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage-Caladion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage-Caladion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage-Caladion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage=Caladion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage=Caladion LoadLiteraryA (pluFiled Section) Context-Caladion Context-Caladion+ContextTage=Caladion Context-Caladion+ContextTage=Caladion LoadLiteraryA (pluFiled Section) Context-Caladion+ContextTage=Caladion Context-Caladion+ContextTage=Caladion LoadLiteraryA (pluFiled Section) Context-Caladion+ContextTage=Caladion Context-Caladion+ContextTage=Caladion LoadLiteraryA (pluFiled Section) Context-Caladion+ContextTage=Caladion ContextTage=Caladion ContextTage=Caladion Context-Caladion+ContextTage=Caladion Context-Caladion+ContextTage=Caladion ContextTage=Caladion ContextTage=Caladi	[9210.229] [0210.332] [0210.346] [0210.346] [0210.346] [0210.346] [0210.347] [0210.347] [0210.330] [0210.347] [0210.347] [0210.453] [0210.453] [0210.453] [0210.500] [0210.550]	NööttöntextThread (in: ThreadMandle=bifffff, Context=bi055004 out: Context= CreateFrocest/NoTHV/L LaafLbraryA (pLiFIIeName="roil1") returned 0xT970000 NööttöntextThread (in: ThreadMandle=bifffff, Context=bi055004 out: Context= NtOmmayTextOffection (ProcessMandle=kiffff, Context=bi055004 out: Context= NtOGtoffile (in: FlieMandle=biffff, Context=bi055004 out: Context= NtOetconsetThread (in: ThreadMandle=biffff, Context=bi055004 out: Context= NtOetconsetThread (in: ThreadMandle=bifff, Context=bi055004 out: Context= NtOetconsetThread (in: ThreadMandle=bifff), RocestAndle=bi054, BaseAdtres=bi05005, Biffer=bi1650 NtOetcontextThread (in: ThreadMandle=bifffff), Context=bi05400 out: Context= NtOetconsetThread (in: ThreadMandle=bifffff), Context=bi05400 out: Context=bi05000 out: Context=bi05400 out: Contex
(0122.116) (0122.120) (0122.120) (0122.120) (0122.123) (0122.132) (0122.133) (0122.133) (0122.133) (0122.133) (0122.141) (0122.141) (0122.160) (0122.160) (0122.174) (0122.161) (0122.183) (0122.183)	NdetConstarThread (in: ThreadManle-Mifffff, Constar-MandSOO out Constar-MandSOO+(ConstarThage-ManDO), DemChanger, (jptichieldman, (), pictuberBamev(), Advisorieldman, () returned Out Constar-MandSOO+(ConstarThage-ManDO), DemChanger, (jptichieldman, (), pictuberBamev(), Advisorieldman, (), pictured (), pictured([0210.229] [0210.332] [0210.346] [0210.361] [0210.361] [0210.361] [0210.370] [0210.330] [0210.339] [0210.340] [0210.355] [0210.400] [0210.555] [0210.556] [0210.516]	NösciontextThread (in: ThreadMandle=wifffff, Context=wis05500) out: Context- CreateFrocestInternalW (in: NbertOken=Wig, japplicationReme="citUberst/jumlications. LoadLiveryA [cpLiFileIname="citUberst]; returned methylowofsectors(NotIFV). LoadLiveryA [cpLiFileIname="citUberst]; ResAddress=wis05000 out: Context= NtbmspriseContextThread (in: ThreadMandle=wiffffff, Context=wis050000) out: Context= NtberContextThread (in: ThreadMandle=wiffffff, Context=wis050000) out: Context= NtberContextThread (in: ThreadMandle=wiffffff, Context=wis05000) out: Context= NtberContextThread (in: NterContext=wis05000) out: Context= NtberContextThread (in: NterContext=wis05000) out: Context= NtberContextThread (in: NterContext=wis05000), projectAtribute-wis05000 NtBerContextThread (in: NterContext=wis05000), projectAtribute-wis05000 NtBerContextThread (in: NterContext=wis05000), projectAtribute-wis05000 NtBerContextThread (in: NterContext=wis05000), projectAtribute-wis05000 NtBerContextThread (in: NterContext=wis05000), projectAtribute-wis05000) NtBerContextThread (in: NterContext=wis05000), Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wifffff, Context=wis05000), point Context= NtBerContextThread (in: ThreadMandle=wifffff), Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wiffff), Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wiffff), Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wiffff), Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wifff), Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wifff), Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wifff), Context=wis050000) (contextThreadMande=wiff)); Context=wis050000, point Context= NtBerContextThread (in: ThreadMandle=wiff); Context=wis050000) (contextThreadMande=wiff); ContextThreadMande=wiff); ContextThreadMande=wiff); ContextThreadMande=wiff); ContextThreadMande=wiff); ContextThreadMande=wiff); Contex
(012.114) (012.120) (012.120) (012.122) (012.123) (012.132) (012.133) (012.133) (012.133) (012.141) (012.141) (012.147) (012.147) (012.147) (012.149) (012.178) (012.178) (012.181) (012.191) (012.191) (012.202)	NdetConstarThread (in: ThreadManl=~dfffff, Constar-wished004 out Constar-wished004 (ConstarTage-wished), loadLineryd (lpibLinieldame-00, lpibLinieldame-00, holdenieldame/00, holdenieldame	[0210.229] [0210.332] [0210.346] [0210.346] [0210.346] [0210.340] [0210.340] [0210.340] [0210.347] [0210.355] [0210.347] [0210.355] [0210.510] [0210.510] [0210.510] [0210.511]	NööstöntestThread (in: ThreadMandle=virfffff, Context=virld50004 out: Context= CreateFrocestrivering (in: ThreadMandle=virfffff, Context=virld50004 out: Context= NööstöntestThread (in: ThreadMandle=virfffff, Context=virld50000 tout: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld50000 tout: Context= NöbsenTiel (in: ThreadMandle=virfffff, Context=virld50000 out: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld50000 out: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld50000 out: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld5000000000000000000000000000000000000
(0122.116) (0122.120) (0122.120) (0122.120) (0122.121) (0122.132) (0122.132) (0122.133) (0122.133) (0122.133) (0122.133) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143)	NdetConstatTuresd (in: Turesdimalie-Nifffff, Constat-NikoS00) out: Context-NikoS00+(ContextFlage-NikoS0, possible state (jstatine), jstatesdimae(statesdime(statesdime), period (jet), period (jet), period (jet), Losdimaryk (jstatine), possible statesdimae(statesdime(statesdime), period (jet), period (jet), Losdimaryk (jstatine), possible statesdime(state	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.361] [0210.361] [0210.339] [0210.339] [0210.347] [0210.460] [0210.461] [0210.510] [0210.510] [0210.516] [0210.526]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(0122.114) (0122.115) (0122.125) (0122.125) (0122.132) (0122.132) (0122.132) (0122.142) (0122.142) (0122.142) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143)	NdetConstarThread (in: ThreadManle=Conffrence, Constar-Caladiool out Context-Caladiool (ContextFlag=Calod), DetContextFlag=Calod), DetContextFlag=Calod) out Context-Caladiool ContextFlag=Calod), DetContextFlag=Calod), DetContextFlag=Calod), EndetContextFlag=Calod), DetContextFlag=Calod), EndetContextFlag=Calod), DetContextFlag=Calod), DetContextFlag=Calod), DetContextFlag=Calod), NdetContextFlag=Calod), NdetCalod, NdetCalod), DetCalod), NdetCalod), NdetC	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.361] [0210.361] [0210.339] [0210.339] [0210.347] [0210.460] [0210.461] [0210.510] [0210.510] [0210.516] [0210.526]	NööstöntestThread (in: ThreadMandle=virfffff, Context=virld50004 out: Context= CreateFrocestrivering (in: ThreadMandle=virfffff, Context=virld50004 out: Context= NööstöntestThread (in: ThreadMandle=virfffff, Context=virld50000 tout: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld50000 tout: Context= NöbsenTiel (in: ThreadMandle=virfffff, Context=virld50000 out: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld50000 out: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld50000 out: Context= NöbsenTiel (in: ThreadMandle=virffff, Context=virld5000000000000000000000000000000000000
(0122.110) (0122.120) (0122.120) (0122.120) (0122.120) (0122.132) (0122.132) (0122.132) (0122.132) (0122.147) (0122.147) (0122.147) (0122.149) (0122.149) (0122.200) (0122.223)	NetConstantIness (in: ThreadManl=-offffff, Contact-also() [out Contact-also() (ContactTage-Cast). OpenSChanger() [pitchieldame-Sci.]pitchieldame() [out Contact-also() [return ContactTage-Cast). LoadLinearyA (pitchieldame-Sci.]pitchieldame() [return Contact-also()] return Contact LoadLinearyA (pitchieldame-Sci.]pitchieldame() [return Contact-also()] return Contact LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci. LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci. Constructions, [return Contact also () [return Contact-also()] return Contact-also()] return Contact-also() LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci. LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci. LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci. LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci. LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci. LoadLinearyA (pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci.]pitchieldame-Sci. NetContactTager () [Retribution () [Retributio	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.361] [0210.361] [0210.339] [0210.339] [0210.347] [0210.460] [0210.461] [0210.510] [0210.510] [0210.516] [0210.526]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(0122.114) (0122.115) (0122.125) (0122.125) (0122.132) (0122.132) (0122.132) (0122.132) (0122.142) (0122.142) (0122.142) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.243)	NdetConstarThread (in: ThreadManle=Chiffff, Constar=Chief6004 [out: Constar=Chief6004 [ConstarThag=Chi000], DotheredBane=Con AdvertedDataSci () returned Chief6004 [Out: Constar=Chief6004 [ConstarThag=Chi000], DotheredBane=Con AdvertedDataSci () returned Chief6004 [Out: Constar=Chief6004 [ConstarThag=Chi000], DotheredBane=ConstarTheory () returned Chief6004 [Out: Constar=Chief6004 [Ou	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.361] [0210.361] [0210.339] [0210.339] [0210.347] [0210.460] [0210.461] [0210.510] [0210.510] [0210.516] [0210.526]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(0122.1.10) (0122.12) (0122.12) (0122.12) (0122.12) (0122.132) (0122.132) (0122.132) (0122.132) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.24) (0122.24) (0122.24)	<pre>NdetContextTrans() Intra-dimant=-Nifffff, Context-NistSON out Context-NistSON*(ContextTiag=-NiSOL) Continence(), Uptable NdetContextTrans() (Iptable NdetContextTrans() (Iptable NdetContextTrans()), NdetContextTiag=-NiSOL() Context-Dimantic (Int Trans()), NdetNdetContextTiag=-NiSOL(), Lamilineary() (IptiFileImme-Songli)); returned 0x75sC0000 (ConserviceImmed (Int Trans()); returned 0x75sC0000); returned 0x NdetContextTrans(); Int NoteTrans(); NdetNdetNdetNdetNdetNdetNdetNdetNdetNdet</pre>	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.361] [0210.361] [0210.339] [0210.339] [0210.347] [0210.460] [0210.461] [0210.510] [0210.510] [0210.516] [0210.526]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(0122.1.10) (0122.12) (0122.12) (0122.12) (0122.12) (0122.132) (0122.132) (0122.132) (0122.132) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.14) (0122.24) (0122.24) (0122.24)	NdetConstarThread (in: ThreadManle=Chiffff, Constar=Chief6004 [out: Constar=Chief6004 [ConstarThag=Chi000], DotheredBane=Con AdvertedDataSci () returned Chief6004 [Out: Constar=Chief6004 [ConstarThag=Chi000], DotheredBane=Con AdvertedDataSci () returned Chief6004 [Out: Constar=Chief6004 [ConstarThag=Chi000], DotheredBane=ConstarTheory () returned Chief6004 [Out: Constar=Chief6004 [Ou	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.261] [0210.339] [0210.339] [0210.339] [0210.437] [0210.436] [0210.400] [0210.400] [0210.500] [0210.510] [0210.510] [0210.516]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(0122.114) (0122.125) (0122.125) (0122.125) (0122.133) (0122.133) (0122.133) (0122.133) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.243) (0122.243) (0122.243) (0122.243) (0122.243)	<pre>NdetContextTrans() Intra-dimant=-Nifffff, Context-NistSON out Context-NistSON*(ContextTiag=-NiSOL) Continence(), Uptable NdetContextTrans() (Iptable NdetContextTrans() (Iptable NdetContextTrans()), NdetContextTiag=-NiSOL() Context-Dimantic (Int Trans()), NdetNdetContextTiag=-NiSOL(), Lamilineary() (IptiFileImme-Songli)); returned 0x75sC0000 (ConserviceImmed (Int Trans()); returned 0x75sC0000); returned 0x NdetContextTrans(); Int NoteTrans(); NdetNdetNdetNdetNdetNdetNdetNdetNdetNdet</pre>	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.261] [0210.339] [0210.339] [0210.339] [0210.437] [0210.436] [0210.400] [0210.400] [0210.500] [0210.510] [0210.510] [0210.516]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(0122.112) (0122.123) (0122.123) (0122.123) (0122.123) (0122.133) (0122.133) (0122.133) (0122.133) (0122.133) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.143) (0122.243) (0122.243) (0122.243) (0122.243) (0122.243) (0122.243) (0122.243)	NdetConstarThread (in: ThreadManle-Stiffer, Constar-SlatSOO(] out Context-SlatSOO(* (ContextTage-SlatSOO), DescReament, Classical State (International S	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.261] [0210.339] [0210.339] [0210.339] [0210.437] [0210.436] [0210.400] [0210.400] [0210.500] [0210.510] [0210.510] [0210.516]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(012.115) (012.115) (012.120) (012.120) (012.120) (012.120) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.121) (012.201) (012.2	<pre>NdetConstarThread (in ThreadManl=~dfffff, Constar-wished00) out Constar-wished00+(ConstarTage-wished) LosdLinery(ipLibTieldame="advgli3") returned 0x75cf000 LosdLinery(ipLibTieldame="advgli3") returned 0x75cf000 LosdLinery(ipLibTieldame="advgli3") returned 0x75cf000 LosdLinery(ipLibTieldame="advgli3") returned 0x75cf000 LosdLinery(ipLibTieldame="advgli3") returned 0x75cf000 LosdLinery(ipLibTieldame="advgli3") returned 0x75cf000 Roberty(interval) provide the start of the star</pre>	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.261] [0210.339] [0210.339] [0210.339] [0210.437] [0210.436] [0210.400] [0210.400] [0210.500] [0210.510] [0210.510] [0210.516]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMame="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x00000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(ff), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff), Context=%x00000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff), Context=%x00000000000000000000000000000000000
(012.115) (012.115) (012.120) (012.20) (012	NetectoresetTresd (in Treesdimale=Stiffer, Context=Station) out Context=Station+(ContextTage=Station), Context=Station+(ContextTage=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), Station=Station=Station=Station=Station=Station=Station=Station=Station, Station=Statio	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.261] [0210.339] [0210.339] [0210.339] [0210.437] [0210.436] [0210.400] [0210.400] [0210.500] [0210.510] [0210.510] [0210.516]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMmas="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMmas="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(fft, Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x0
(012.11) (012.11) (012.12) (012.22) (01	<pre>NdetConstarThread (in ThreadManl=~Nfffff, Constar~lateS00 out Constar~lateS00*(ConstarTage~lateS13ge~lateS13ge) Constarts (in Section 2014) (in Secti</pre>	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.261] [0210.339] [0210.339] [0210.339] [0210.437] [0210.436] [0210.400] [0210.400] [0210.500] [0210.510] [0210.510] [0210.516]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMmas="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMmas="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(fft, Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x0
(012.11) (012.11) (012.12) (012.22) (01	NetectoresetTresd (in Treesdimale=Stiffer, Context=Station) out Context=Station+(ContextTage=Station), Context=Station+(ContextTage=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), LostLineryA (jpLifieldame=Station=Station), Station=Station=Station=Station=Station=Station=Station=Station=Station, Station=Statio	[0210.229] [0210.246] [0210.246] [0210.246] [0210.246] [0210.261] [0210.261] [0210.261] [0210.339] [0210.339] [0210.339] [0210.437] [0210.436] [0210.400] [0210.400] [0210.500] [0210.510] [0210.510] [0210.516]	NüderContextThread (in: ThreadMandle=wiff(ff, Context=wis05500) out: Context= CreateFrocest(NUDHW)/ LoadLhearyA (pLLHFleMmas="stdll") returned %x790000 Microsofter Microsofter (NUDHW)/ LoadLhearyA (pLLHFleMmas="stdll") returned %x790000 NUDerContextThread (in: ThreadMandle=wiff(fft, Context=%x000000) out: Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteChattlaut NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, DudteContextThread (in: ThreadMandle=wiff(fft), Context=%x000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x0000000, Dudt Context= NUDerContextThread (in: ThreadMandle=wiff(fft), Context=%x0

Figure 3: VMRay Analyzer's function log - Comparison of GuLoader's new behavior (left) with previously analyzed samples (right)

Last, it downloads the final AZORult stealer payload, maps it into its own process, and transfers control flow (Figure 4).

HTTP Session #3

Information	Value	•			
Server Name	oned	rive.live.com			
Server Port	80				
Total Data Sent	232 b	pytes			
Total Data Received	977 b	pytes			
Operation	Information		Success	Count	Logfile
Open Session	user_agent = Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0 = INTERNET_OPEN_TYPE_PRECONFIG	0) like Gecko, access_type	~	1	FN
Open Connection	protocol = http, server_name = onedrive.live.com, server_port = 80		~	1	FN
Open HTTP Request	http_verb = GET, http_version = HTTP 1.1, target_resource = /downloa INTERNET_FLAG_PRAGMA_NOCACHE, INTERNET_FLAG_NO_CACHE_W INTERNET_FLAG_RELOAD		√	1	FN
Send HTTP Request	headers = WINHTTP_NO_ADDITIONAL_HEADERS, url = http://onedrive /download?cid=4C3F5C65A99DA195&resid=4C3F5C65A99DA195%21 authkey=AGyBKeKMs6qKShY		~	1	FN
Read Response	size = 65536, size_out = 65536		\checkmark	1	FN D
Read Response	size = 65536, size_out = 49216		√	1	FN D
Read Response	size = 65536, size_out = 0		\checkmark	1	FN
Close Session			1	1	FN

AZORult's Behavior

From this point on, the behavior of AZORult is visible. AZORult is an information stealer that targets login credentials, cookies, cryptocurrency wallets, and more (Figure 5).



Figure 5: VMRay Analyzer – AZORult's data collection

AZORult v3 always appends the XOR key used to encrypt the following message sent to its C&C at the beginning of the message. Thus, the initial communication always starts with three NUL bytes followed by an XOR encrypted ID hash (Figure 6). In our investigation, we found multiple servers used as its C&C (see IOCs) that all contain the same path.

3 Hosts		HTTP Requests	s (2) DNS Requests (1)						
Requests 🔻 Severity	*	Method	URL		Response	Dest. IP	Dest. Port	-	Severity
kalpvedafoundation.com	<u> </u>	POST	tarot-sunce.com/linko/PL341/	index.php	200	178.218.167.4	80	-	UNKNOWN
enedrive.live.com		POST	tarot-sunce.com/linko/PL341/	index.php	200	178.218.167.4	80	-	UNKNOWN
80	Ψ								
tarot-sunce.com	٠								
		Request Res	sponse Function Logs (2)	Stream (3210) Direct	ion		Size		
		133.205949		→			279 B		
		133.325070		+ +			1396 B		
		133.325109		< +			1396 B		
		133.325125		< +			1396 B		
		133.325144		< +			1396 B		
		133.325152		←			1396 B		
		6F 74 2D 73 7 6E 74 65 6E 7 35 0D 0A 43 6 3A 20 6E 6F 2	29 0D 0A 48 6F 73 74 3A 2 75 6E 63 65 2E 63 6F 6D 0 74 2D 4C 65 6E 67 74 68 3 61 63 68 65 2D 43 6F 6E 6 2D 63 61 63 68 65 2D 43 6F 6E 7 2D 63 61 63 68 65 0D 0A 6 3A 11 8B 30 6C EA 26 65 65	DD 0A 43 6F 3A 20 31 30 74 72 6F 6C DD 0A 00 00	.com Conte	sunc ent - Le Cache - - cache 0 lê &			

Figure 6: VMRay Analyzer – AZORult's initial message sent to its C&C server.

Conclusion

By using GuLoader in the delivery chain, the attackers can profit from the many features provided by GuLoader that are not offered by AZORult on its own. This obstructs dynamic analysis, complicates manual analysis and provides a flexible, easy distribution of tasks to the attacker without the requirement of advanced specialized knowledge. Despite all that, the <u>VMRay Analyzer</u> monitored the complete delivery chain from the initial RTF document to the final payload.

As mentioned before, these documents are sent via spam emails which are typical attack vectors that attackers use as an entry into the network. Including the <u>VMRay Email Threat Defender</u> (ETD) in the network helps to detect and prevent such attacks.

IOCs

Designed	
Documents	5ff8a87fd7626d4beab7a5be7f285f1d1d64478509f27aca6fd9de
9a5f4116b1be763a38e25cb14869b57daf9ae4fe1c2e72adc433eccc95d5f539	
08df240668051225b392d88174dadd0db2703ee1ba93c62e3b020cb2be188c17	-
6a39c54717f2c9f76f5cf9bde58ca256ab1ed77985b3f590d3797fd6655c19ac	-
f0fb1c2a2150e9a33488974952af6c8f0cd52d463ab656e36d17b7d224d04f8e	-

	_
cc88795da896ebd8df6fdd996179ae53285c021b0d7437fa9bffca4e5fbc0473	
d0f83c5b91494e26b3c0cc108aa43f6865a17eee870a28f1f7d89669e177d279	-
3bd6858a664535a00192021b4b89ab96d47fcf08c32fee5ea97ded3099e39ba8	-
GuLoader using MsiEnumProducts	e000b0cae7df0753ea12d97175e393bacf905613eef1a59d7e17
1e6a09e38553c090a119156022d61670adf96f8a635a3dac11f11dd395c107ba	
4487e0798fb74f9891c48625b3a189dbd1e05e2c400cd710f4ea0bdf03b9adbd	_
c256466dc256d55f7cba0f1c2201f208b82deabd903dd3a71a4e7989e6a61ff7	_
c87290bb28696eddacaadc0f01805f841bda964d55efa9c39d0a06f1d31ede3b	-
1623c45e067729ec3b334294da18855e0e5312fd4d9d28f95d4e38b074255892	_
b5389059c8b005b1968197bb1bb38edc024501c02bf8941d287b1c01358b121a	_
e97e14f57e6f9ad987e4b5079b7ba8a387115b89784958d40d1f65d79d027315	_
Domains hosting GuLoader	kalpvedafoundation[.]com
cieloabiertocasahogar[.]com	
www[.]cecadperu[.]com	_
AZORult C&Cs	skilldrivinget[.]com/ojman/PL341//index[.]php
laninesolution[.]com/roky/PL341/index[.]php	
tarot-sunce[.]com/linko/PL341/index[.]php	-
eksodus[.]id/ghytoja/PL341/index[.]php	_
laninesolution[.]com/roky/PL341/index[.]php	-