ID: 356310
Sample Name: f4b1bde3-706a-40d2-8ace-693803810b6f.exe
Cookbook: default.jbs
Time: 22:06:04
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

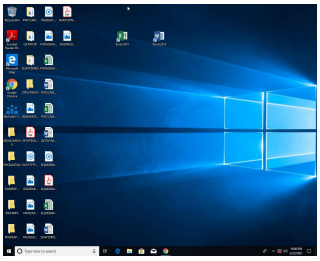
Analysis Report f4b1bde3-706a-40d2-8ace-693803810b6…

Overview

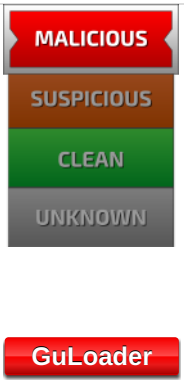
General Information

Sample Name:	f4b1bde3-706a-40d2-8ace-693803810b6f.exe
Analysis ID:	356310
MD5:	1364f8c4c00b87e..
SHA1:	4dafecb2752fe65..
SHA256:	9a7b0abc37831a..

Most interesting Screenshot:



Detection

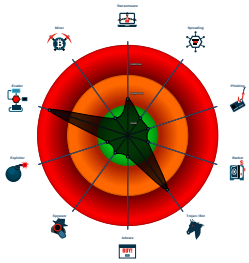


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Found evasive API chain (may stop…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions
- Abnormal high CPU Usage

Classification



Startup

- **System is w10x64**
- f4b1bde3-706a-40d2-8ace-693803810b6f.exe (PID: 4112 cmdline: 'C:\Users\user\Desktop\f4b1bde3-706a-40d2-8ace-693803810b6f.exe' MD5: 1364F8C4C00B87E5D938E9F95AF828F4)
  - RegAsm.exe (PID: 5672 cmdline: 'C:\Users\user\Desktop\f4b1bde3-706a-40d2-8ace-693803810b6f.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 5544 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- filename1.exe (PID: 6732 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 1364F8C4C00B87E5D938E9F95AF828F4)
  - RegAsm.exe (PID: 6920 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 6936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- filename1.exe (PID: 6844 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 1364F8C4C00B87E5D938E9F95AF828F4)
  - RegAsm.exe (PID: 7000 cmdline: 'C:\Users\user\subfolder1\filename1.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 7012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

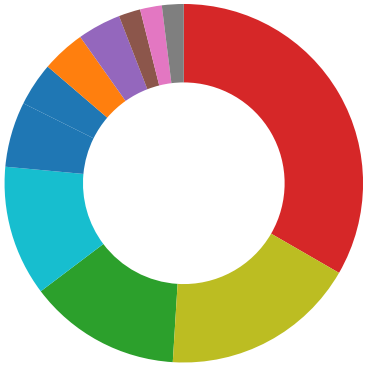
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: RegAsm.exe PID: 7000	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6920	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 5672	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

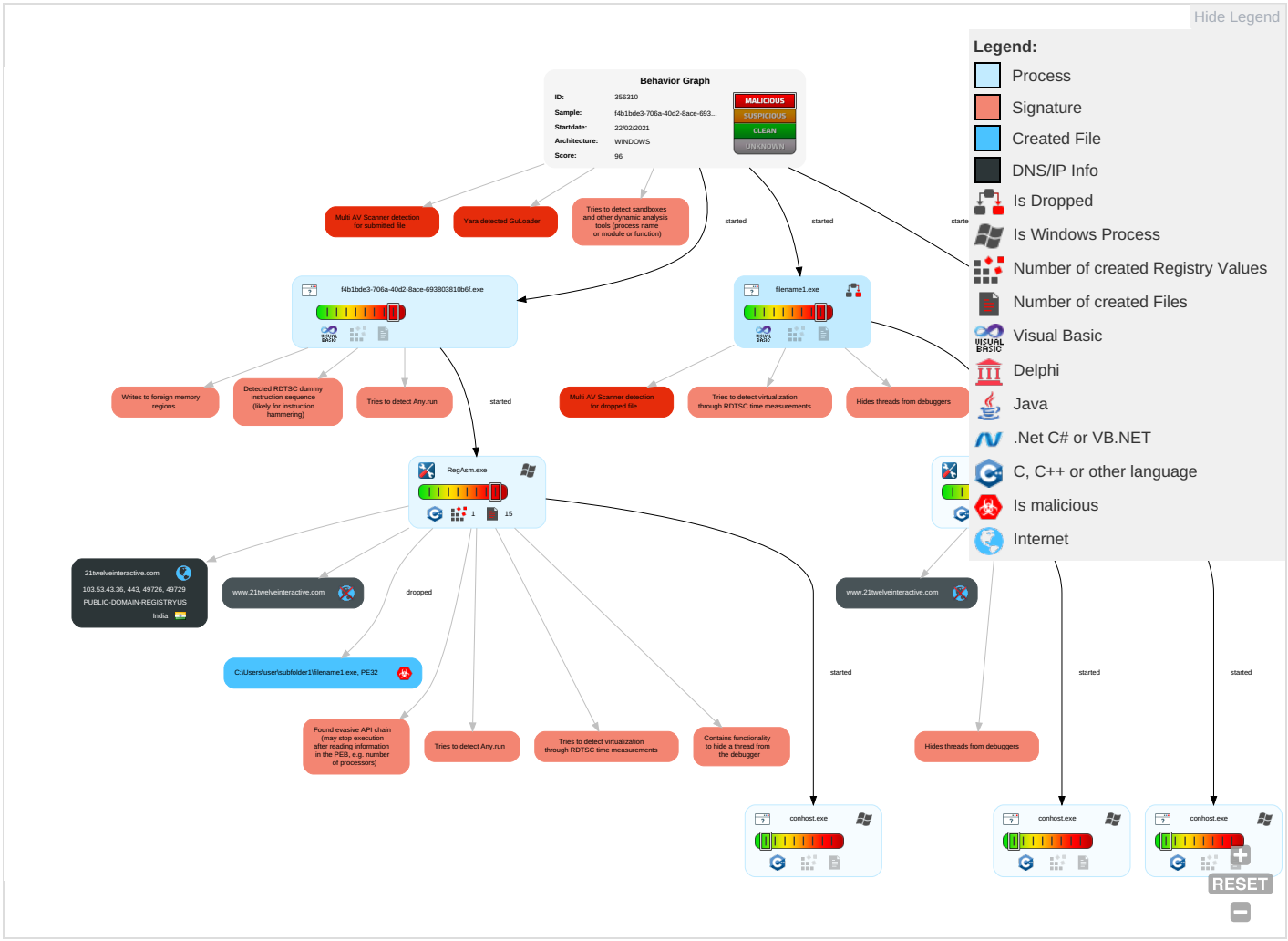
HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Native API 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 2 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Process Injection 1 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	C D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

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
f4b1bde3-706a-40d2-8ace-693803810b6f.exe	56%	Virustotal		Browse
f4b1bde3-706a-40d2-8ace-693803810b6f.exe	24%	Metadefender		Browse
f4b1bde3-706a-40d2-8ace-693803810b6f.exe	68%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\subfolder1\filename1.exe	24%	Metadefender		Browse
C:\Users\user\subfolder1\filename1.exe	68%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
21twelveinteractive.com	5%	Virustotal		Browse
www.21twelveinteractive.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/slick/js/slick.min.js	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/fg/janomo_ZhyUp244.bin0100	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/opencart-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/laravel-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/quality-assurance/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/owl-carousel/assets/ow	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-json/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/psd-to-html/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/terms-and-condition/	0%	Avira URL Cloud	safe	
http://r3.o.le	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/about-us/	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/hire-unity-3d-game-developer/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/hire-android-app-developer/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/psd-to-wordpress/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/ruby-on-rails-development/	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/fg/janomo_ZhyUp244.bin	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/react-native-app-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wordpress-development/	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/nDl	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/hire-magento-developer/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/xmlrpc.php	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/psd-to-html5/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/js/main.min.js	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/ipad-application-development/	0%	Avira URL Cloud	safe	
http://https://r6k8z9y5.rocketcdn.me/wp-content/uploads/2020/02/21twelve-logo-bg.png	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/php-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/feed/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/uploads/2019/10/new-logo1.svg	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wordpress-development-agency/	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/fg/janomo_ZhyUp244.bind	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/woocommerce-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/uploads/2020/02/conatact-left2.png	0%	Avira URL Cloud	safe	
http://css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/hybrid-app-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/jquery.jPlayer/jquery.	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.21twelveinteractive.com/#organization	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/images/flag/india.png	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/plugins/mailchimp-for-wp/assets/js/forms.min.js	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/cakephp-development/	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://www.21twelveinteractive.com/wp-content/plugins/structured-content/dist/blocks.style.build.cs	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.21twelveinteractive.com/wp-content/plugins/wp-rocket/assets/js/lazyload/16.1/lazyload.mi	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/plugins/gravityforms/css/formreset.min.css	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/plugins/mailchimp-for-wp/assets/css/form-basic.min.cs	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/psd-to-drupal/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/markup/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/js/snow.js	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/plugins/js_composer/assets/css/vc-ie8.min.css	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/fg/janomo_ZhyUp244.bincefb9XX	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/173855x	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/android-game-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/codeigniter-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/plugins/gravityforms/css/formsmain.min.css	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/joomla-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/js-framework-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/website-design/	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/U5W	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/fg/janomo_ZhyUp244.binnt	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/plugins/gravityforms/images/spinner.gif	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/drupal-development/	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com//dstro	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/corporate-website-designs/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/uploads/2020/03/WhatsApp.svg	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/hire-ipad-app-developer/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/blog/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/cross-platform-mobile-app-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/unity-3d-2d-game-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/css/animate.css	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/psd-to-email-template/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/social-media-marketing/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/sketch-to-psd-design/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/services/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/mobile-app-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/megatron-icon/css/styl	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/prettyPhoto/css/pretty	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/android-app-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/css/pages/84.css	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/shopify-development/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/comments/feed/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/hire-cross-platform-app-developer/	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/images/flag/aus.png	0%	Avira URL Cloud	safe	
http://https://21twelveinteractive.com/L	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/fg/janomo_ZhyUp244.binmobi	0%	Avira URL Cloud	safe	
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/style.css	0%	Avira URL Cloud	safe	
http://https://r6k8z9y5.rocketcdn.me/wp-content/uploads/2019/10/new-logo1.svg	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
21twelveinteractive.com	103.53.43.36	true	false	• 5%, Virustotal, Browse	unknown
www.21twelveinteractive.com	unknown	unknown	false	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/slick/js/slick.min.js	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/fg/janomo_ZhyUp244.bin0100	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/opencart-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/laravel-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/quality-assurance/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/owl-carousel/assets/ow	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-json/	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp, RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/psd-to-html/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/terms-and-condition/	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.le	RegAsm.exe, 00000014.00000002.486413359.0000000000FE1000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/about-us/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com/	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp, RegAsm.exe, 00000014.00000002.486363644.0000000000FA7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/hire-unity-3d-game-developer/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/hire-android-app-developer/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/psd-to-wordpress/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://oss.maxcdn.com/respond/1.4.2/respond.min.js	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.21twelveinteractive.com/ruby-on-rails-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com/fg/janomo_ZhyUp244.bin	RegAsm.exe, 00000005.00000002.474366584.0000000001300000.00000040.00000001.sdmp, RegAsm.exe, 00000014.00000002.486227915.0000000000D00000.00000040.00001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.21twelveinteractive.com/xmlrpc.php?rsd	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/react-native-app-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wordpress-development/	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com/nDl	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/hire-magento-developer/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/xmlrpc.php	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/psd-to-html5/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/js/main.min.js	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/ipad-application-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://twitter.com/21twelvel/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://r6k8z9y5.rocketcdn.me/wp-content/uploads/2020/02/21twelve-logo-bg.png	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/php-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/feed/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/uploads/2019/10/new-logo1.svg	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wordpress-development-agency/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com/fg/janomo_ZhyUp244.bind	RegAsm.exe, 00000014.00000002.486393836.0000000000FC1000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/woocommerce-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/uploads/2020/02/conatact-left2.png	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://css3-mediaqueries-js.googlecode.com/svn/trunk/css3-mediaqueries.js	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/hybrid-app-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

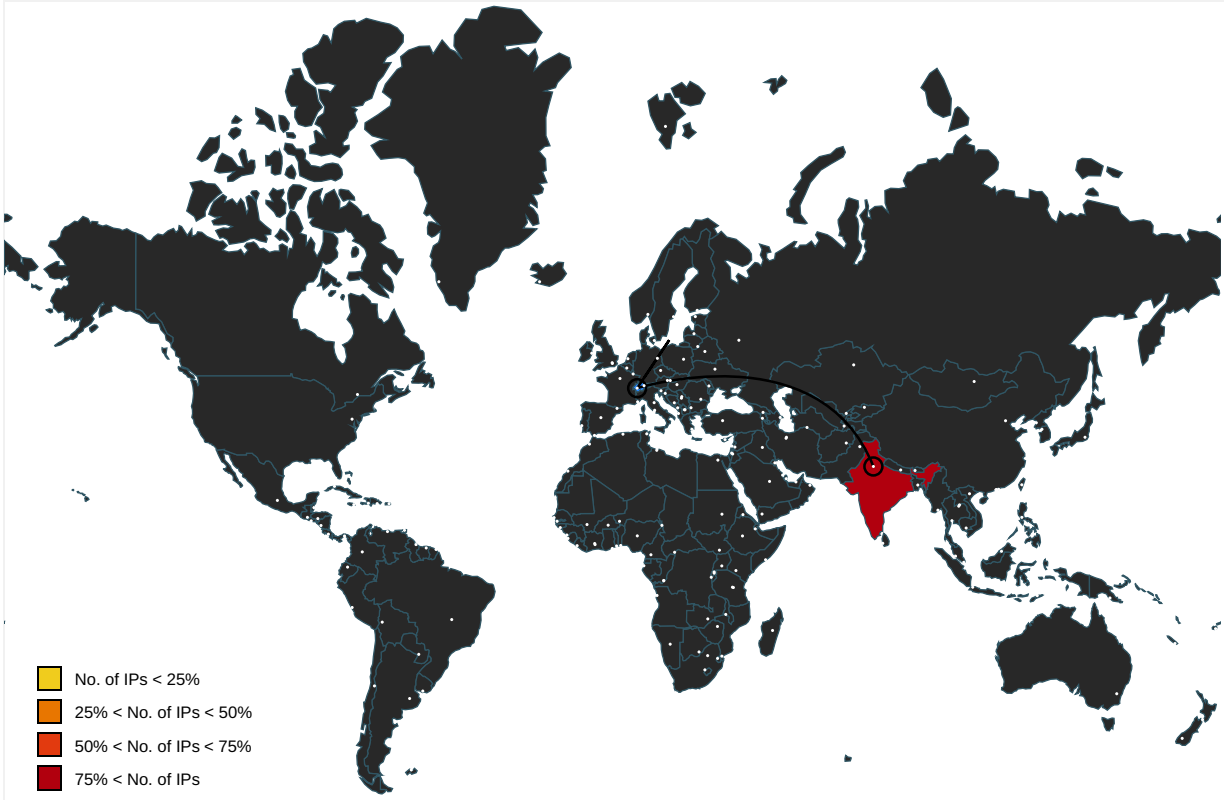
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/jquery.jPlayer/jquery.	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp, RegAsm.exe, 00000014.00000002.486363644.0000000000FA7000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.21twelveinteractive.com/#organization	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/images/flag/india.png	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/plugins/mailchimp-for-wp/assets/js/forms.min.js	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.instagram.com/21twelveinteractive/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.21twelveinteractive.com/cakephp-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/plugins/structured-content/dist/blocks.style.build.cs	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp, RegAsm.exe, 00000014.00000002.486413359.0000000000FE1000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/plugins/wp-rocket/assets/js/lazyload/16.1/lazyload.mi	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/plugins/gravityforms/css/formreset.min.css	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/plugins/mailchimp-for-wp/assets/css/form-basic.min.cs	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/psd-to-drupal/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/markup/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/js/snow.js	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://schema.org	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.21twelveinteractive.com/wp-content/plugins/js_composer/assets/css/vc-ie8.min.css	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://embed.tawk.to/5dabf4d6df22d91339a00b9d/default	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.21twelveinteractive.com/fg/janomo_ZhyUp244.bincefb9XX	RegAsm.exe, 00000014.00000002.486363644.0000000000FA7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com/173855x	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/android-game-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/codeigniter-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/plugins/gravityforms/css/formsmain.min.css	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://schema.org/	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.21twelveinteractive.com/joomla-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/js-framework-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/website-design/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com/U5W	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com/fg/janomo_ZhyUp244.binnt	RegAsm.exe, 00000014.00000002.486393836.0000000000FC1000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/plugins/gravityforms/images/spinner.gif	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/drupal-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://21twelveinteractive.com//dstro	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/corporate-website-designs/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/uploads/2020/03/WhatsApp.svg	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/hire-ipad-app-developer/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/blog/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/cross-platform-mobile-app-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.21twelveinteractive.com/unity-3d-2d-game-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/css/animate.css	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/psd-to-email-template/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/social-media-marketing/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/sketch-to-psd-design/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/services/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/mobile-app-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/megatron-icon/css/styl	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/plugins/prettyPhoto/css/pretty	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/android-app-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/css/pages/84.css	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/shopify-development/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.pinterest.com/21twelveinteractive/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.21twelveinteractive.com/comments/feed/	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/hire-cross-platform-app-developer/	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/assets/images/flag/aus.png	RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://web.whatsapp.com/send?phone=13474740020	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://21twelveinteractive.com/L	RegAsm.exe, 00000014.00000002.486363644.0000000000FA7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.21twelveinteractive.com/fg/janomo_ZhyUp244.binmobi	RegAsm.exe, 00000005.00000002.517980335.00000000016E7000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://yoast.com/wordpress/plugins/seo/	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false		high
http://https://www.21twelveinteractive.com/wp-content/themes/21twelve/style.css	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://r6k8z9y5.rocketcdn.me/wp-content/uploads/2019/10/new-logo1.svg	RegAsm.exe, 00000005.00000002.529692576.0000000002F00000.00000004.00000001.sdmp, RegAsm.exe, 00000014.00000002.494810701.0000000002A00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.53.43.36	unknown	India		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356310
Start date:	22.02.2021
Start time:	22:06:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 21s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	f4b1bde3-706a-40d2-8ace-693803810b6f.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal96.troj.evad.winEXE@12/1@4/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 3.3% (good quality ratio 2.7%) • Quality average: 43.4% • Quality standard deviation: 22.7%
HCA Information:	• Successful, ratio: 74% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.42.151.234, 104.43.193.48, 13.64.90.137, 184.30.20.56, 8.253.204.120, 67.26.83.254, 8.253.95.249, 8.248.143.254, 8.248.131.254, 40.126.31.137, 40.126.31.141, 20.190.159.134, 40.126.31.6, 20.190.159.138, 40.126.31.135, 20.190.159.132, 40.126.31.8, 51.104.139.180, 13.107.42.23, 13.107.5.88, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, www.tm.lg.prod.aadmsa.akadns.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, arc.msn.com, www.tm.a.prd.aadg.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, login.live.com, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, config.edge.skype.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, dub2.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Execution Graph export aborted for target RegAsm.exe, PID 7000 because there are no executed function • Execution Graph export aborted for target filename1.exe, PID 6732 because there are no executed function • Execution Graph export aborted for target filename1.exe, PID 6844 because there are no executed function • 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
22:07:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe
22:07:54	API Interceptor	16x Sleep call for process: RegAsm.exe modified
22:07:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\subfolder1\filename1.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 208.91.199.223
	document-550193913.xls	Get hash	malicious	Browse	• 208.91.199.118
	document-550193913.xls	Get hash	malicious	Browse	• 208.91.199.118
	SecuriteInfo.com.Trojan.Packed2.42850.3598.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	• 208.91.199.224
	ffkjg5CVrO.exe	Get hash	malicious	Browse	• 208.91.199.223
	7Lf8J7h7os.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	• 208.91.199.225
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 208.91.198.143
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	PAYMENT INVOICE-9876543456789.exe	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Exploit.Siggen3.10204.3307.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-573042818.xls	Get hash	malicious	Browse	• 103.50.162.157
	document-750895311.xls	Get hash	malicious	Browse	• 103.50.162.157
	19_02_2021.exe	Get hash	malicious	Browse	• 111.118.215.254

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	LIQUIDACION INTERBANCARIA 02_22_2021.xls	Get hash	malicious	Browse	• 103.53.43.36
	document-550193913.xls	Get hash	malicious	Browse	• 103.53.43.36
	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 103.53.43.36
	receipt145.htm	Get hash	malicious	Browse	• 103.53.43.36
	xerox for hycite.htm	Get hash	malicious	Browse	• 103.53.43.36
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 103.53.43.36
	Muligheds.exe	Get hash	malicious	Browse	• 103.53.43.36
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 103.53.43.36
	PDF.exe	Get hash	malicious	Browse	• 103.53.43.36
	pagamento.exe	Get hash	malicious	Browse	• 103.53.43.36
	message_zdm (2).html	Get hash	malicious	Browse	• 103.53.43.36
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 103.53.43.36
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 103.53.43.36
	frank_2021-02-22_02-03.exe	Get hash	malicious	Browse	• 103.53.43.36
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 103.53.43.36
	MR52.vbs	Get hash	malicious	Browse	• 103.53.43.36
	Scan_medcal equipment sample_pdf.exe	Get hash	malicious	Browse	• 103.53.43.36
	rfq02212021.exe	Get hash	malicious	Browse	• 103.53.43.36
	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	• 103.53.43.36
	RFQ-#09503.exe	Get hash	malicious	Browse	• 103.53.43.36

Dropped Files

No context

Created / dropped Files

C:\Users\user\subfolder1\filename1.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	5.390824175915418
Encrypted:	false
SSDEEP:	1536:kyPJsmDD03vxnl1eE2Kg58CXEleTxHyb5aVU:kCsE03vxnlIt5b9E0VU
MD5:	1364F8C4C00B87E5D938E9F95AF828F4
SHA1:	4DAFECB2752FE653EDBEE9CE9794DEDA34325D5F
SHA-256:	9A7B0ABC37831A4C9DC1676CC3FC7C0278E413A845ACE42FF4C82E21FC744653
SHA-512:	6713D07FADF92133E3B2FFB734AD0F89E205B0764E3C012CB3503531BB7AC50F4E9541262D2BB974F7494EA0733C0872D4A76DD296B217C0137E594B920D3EC5
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 24%, Browse • Antivirus: ReversingLabs, Detection: 68%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D..H..=.....Rich.....PE..L...+~.`.....P...@. .....`....@.....Y..(....@.. U.....(... .....text...N.....P..... ..`.data...<....`.....`.....@....rsrc... U...@...`...p.....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.390824175915418
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	f4b1bde3-706a-40d2-8ace-693803810b6f.exe
File size:	118784
MD5:	1364f8c4c00b87e5d938e9f95af828f4
SHA1:	4dafecb2752fe653edbee9ce9794deda34325d5f
SHA256:	9a7b0abc37831a4c9dc1676cc3fc7c0278e413a845ace42ff4c82e21fc744653
SHA512:	6713d07fadf92133e3b2ffb734ad0f89e205b0764e3c012cb3503531bb7ac50f4e9541262d2bb974f7494ea0733c0872d4a76dd296b217c0137e594b920d3ec5
SSDEEP:	1536:kyPJsmDD03vxnl1eE2Kg58CXEleTxHyb5aVU:kCsE03vxnlIt5b9E0VU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D...H...=.....Rich.....PE..L...+~.`.....P...@.....`....@.....

File Icon

Icon Hash:	8030b296b2b29616

Static PE Info

General

Entrypoint:	0x4014a8

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x602E7E2B [Thu Feb 18 14:48:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4730b340d48d7ad3023c8e9665279a07

Entrypoint Preview

Instruction
push 004022D0h
call 00007FAB6482EE85h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
setnb byte ptr [ebp+74EFA7F5h]
inc eax
call far 6F90h : C0DAA766h
sbb eax, dword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [edx+00h], al
push es
push eax
add dword ptr [ecx], 62h
outsd
insb
imul esi, dword ptr [esi+00h], 00000314h
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
sbb edi, edi
or edx, esi
lds eax, edx
fst dword ptr [ecx]
dec ebp
or byte ptr [ebx+5Ah], FFFFFFD1h
jnp 00007FAB6482EED8h
inc ecx
sbb al, AEh
call 00007FABC8499357h
fimul dword ptr [edi-63h]
push ds
sub al, 1Eh
cmp ah, byte ptr [ecx+4F3A5193h]
lodsd

Instruction
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
sub eax, dword ptr [eax+eax]
add byte ptr [edi], bh
add byte ptr [eax], al
add byte ptr [eax], al
add eax, 434E5500h
push edx
inc ebp
add byte ptr [41000601h], cl
jne 00007FAB6482EF0Ah
outsd
je 00007FAB6482EF01h
add byte ptr [ecx], bl
add dword ptr [eax], eax
inc edx
add byte ptr [edx], ah
add eax, 41000624h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x159f4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x24000	0x5520	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x114	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x14ec0	0x15000	False	0.376511346726	data	5.91962877849	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0xd43c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x5520	0x6000	False	0.263875325521	data	3.75302149721	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x241a8	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x242d0	0xff8	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x252c8	0x25a8	data		
RT_ICON	0x27870	0x10a8	data		
RT_ICON	0x28918	0x988	data		
RT_GROUP_ICON	0x292a0	0x4c	data		
RT_VERSION	0x292ec	0x234	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaAryMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaExitProc, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarDup, __vbaStrComp, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
InternalName	parag
FileVersion	1.00
CompanyName	Whine Caps
Comments	Whine Caps
ProductName	boliv
ProductVersion	1.00
OriginalFilename	parag.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution

Total Packets: 65

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:07:48.777015924 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:48.933082104 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:48.933263063 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:48.972296000 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:49.128247023 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:49.130306959 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:49.130333900 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:49.130351067 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:49.130553007 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:49.182723045 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:49.339215040 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:49.339370966 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:49.358275890 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:49.554413080 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.038583040 CET	443	49726	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.038682938 CET	49726	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.465137005 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.619775057 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.619947910 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.620728970 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.774965048 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.777450085 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.777473927 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.777489901 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.777554035 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.777602911 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.783005953 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.937287092 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:51.937422037 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:51.938126087 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:52.132713079 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719063044 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719094038 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719108105 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719120979 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719134092 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719146967 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719158888 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719175100 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719187975 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719201088 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.719383955 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.719414949 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.873522997 CET	443	49729	103.53.43.36	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:07:53.873553991 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873567104 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873579979 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873593092 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873610973 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873639107 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873655081 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873672009 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873684883 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873697042 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873708963 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.873713017 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873730898 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873747110 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873750925 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.873771906 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.873810053 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.873852015 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873895884 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.873912096 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.873961926 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.874033928 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.874051094 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.874068022 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.874100924 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.874109030 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:53.874140978 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:53.874182940 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.027833939 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027863979 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027887106 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027905941 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027921915 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027926922 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.027937889 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027955055 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027967930 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027968884 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.027982950 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.027996063 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028007984 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028018951 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028023005 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.028033972 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028047085 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028101921 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028119087 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028183937 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.028316975 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028330088 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.028337955 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028377056 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.028381109 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028400898 CET	443	49729	103.53.43.36	192.168.2.3
Feb 22, 2021 22:07:54.028414011 CET	49729	443	192.168.2.3	103.53.43.36
Feb 22, 2021 22:07:54.028448105 CET	49729	443	192.168.2.3	103.53.43.36

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:06:44.481205940 CET	50620	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:06:44.531315088 CET	53	50620	8.8.8.8	192.168.2.3
Feb 22, 2021 22:06:45.380598068 CET	64938	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:06:45.432338953 CET	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 22:06:46.563235998 CET	60152	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:06:46.614936113 CET	53	60152	8.8.8.8	192.168.2.3
Feb 22, 2021 22:06:47.374510050 CET	57544	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:06:47.423060894 CET	53	57544	8.8.8.8	192.168.2.3
Feb 22, 2021 22:06:48.416963100 CET	55984	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:06:48.468799114 CET	53	55984	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:09.694788933 CET	64185	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:09.743638039 CET	53	64185	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:10.753132105 CET	65110	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:10.806780100 CET	53	65110	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:12.244568110 CET	58361	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:12.296725988 CET	53	58361	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:13.255645037 CET	63492	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:13.304260015 CET	53	63492	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:14.286277056 CET	60831	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:14.334932089 CET	53	60831	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:15.848207951 CET	60100	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:15.897042036 CET	53	60100	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:16.988033056 CET	53195	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:17.045253038 CET	53	53195	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:18.216005087 CET	50141	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:18.264832973 CET	53	50141	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:19.466372013 CET	53023	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:19.514960051 CET	53	53023	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:20.941638947 CET	49563	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:20.993490934 CET	53	49563	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:21.650358915 CET	51352	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:21.727567911 CET	53	51352	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:22.238274097 CET	59349	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:22.287533998 CET	53	59349	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:23.456315041 CET	57084	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:23.505074024 CET	53	57084	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:27.604310036 CET	58823	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:27.652932882 CET	53	58823	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:39.135535002 CET	57568	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:39.184226990 CET	53	57568	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:48.335050106 CET	50540	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:48.760562897 CET	53	50540	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:50.681535959 CET	54366	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:50.732038975 CET	53	54366	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:51.051738024 CET	53034	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:51.417208910 CET	57762	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:07:51.462747097 CET	53	53034	8.8.8.8	192.168.2.3
Feb 22, 2021 22:07:51.469007015 CET	53	57762	8.8.8.8	192.168.2.3
Feb 22, 2021 22:08:33.344796896 CET	58722	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:08:33.349323034 CET	56596	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:08:33.351274014 CET	64101	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:08:33.393704891 CET	53	58722	8.8.8.8	192.168.2.3
Feb 22, 2021 22:08:33.397980928 CET	53	56596	8.8.8.8	192.168.2.3
Feb 22, 2021 22:08:33.408348083 CET	53	64101	8.8.8.8	192.168.2.3
Feb 22, 2021 22:08:47.900338888 CET	55435	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:08:48.323601007 CET	53	55435	8.8.8.8	192.168.2.3
Feb 22, 2021 22:08:50.696456909 CET	50713	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:08:50.747922897 CET	53	50713	8.8.8.8	192.168.2.3
Feb 22, 2021 22:08:56.175055027 CET	56132	53	192.168.2.3	8.8.8.8
Feb 22, 2021 22:08:56.257810116 CET	53	56132	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 22:07:48.335050106 CET	192.168.2.3	8.8.8.8	0x9dce	Standard query (0)	21twelvein teractive.com	A (IP address)	IN (0x0001)
Feb 22, 2021 22:07:51.051738024 CET	192.168.2.3	8.8.8.8	0x2dfa	Standard query (0)	www.21twel veinteractive.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 22:08:47.900338888 CET	192.168.2.3	8.8.8.8	0x5ce4	Standard query (0)	21twelvein teractive.com	A (IP address)	IN (0x0001)
Feb 22, 2021 22:08:50.696456909 CET	192.168.2.3	8.8.8.8	0xe5b0	Standard query (0)	www.21twel veinteractive.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 22:07:48.760562897 CET	8.8.8.8	192.168.2.3	0x9dce	No error (0)	21twelvein teractive.com		103.53.43.36	A (IP address)	IN (0x0001)
Feb 22, 2021 22:07:50.732038975 CET	8.8.8.8	192.168.2.3	0xd241	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 22:07:51.462747097 CET	8.8.8.8	192.168.2.3	0x2dfa	No error (0)	www.21twel veinteract ive.com	21twelveinteractive.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 22:07:51.462747097 CET	8.8.8.8	192.168.2.3	0x2dfa	No error (0)	21twelvein teractive.com		103.53.43.36	A (IP address)	IN (0x0001)
Feb 22, 2021 22:08:48.323601007 CET	8.8.8.8	192.168.2.3	0x5ce4	No error (0)	21twelvein teractive.com		103.53.43.36	A (IP address)	IN (0x0001)
Feb 22, 2021 22:08:50.747922897 CET	8.8.8.8	192.168.2.3	0xe5b0	No error (0)	www.21twel veinteract ive.com	21twelveinteractive.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 22:08:50.747922897 CET	8.8.8.8	192.168.2.3	0xe5b0	No error (0)	21twelvein teractive.com		103.53.43.36	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 22:07:49.130351067 CET	103.53.43.36	443	192.168.2.3	49726	CN=mail.21twelveinteractive.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 18:38:55 CET 2021	Wed May 19 19:38:55 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 22, 2021 22:07:51.777489901 CET	103.53.43.36	443	192.168.2.3	49729	CN=mail.21twelveinteractive.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 18:38:55 CET 2021	Wed May 19 19:38:55 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 22, 2021 22:08:48.693511009 CET	103.53.43.36	443	192.168.2.3	49735	CN=mail.21twelveinteractive.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 18:38:55 CET 2021	Wed May 19 19:38:55 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 22:08:51.115323067 CET	103.53.43.36	443	192.168.2.3	49737	CN=mail.21twelveinteractive.com CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Thu Feb 18 18:38:55 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Wed May 19 19:38:55 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

- f4b1bde3-706a-40d2-8ace-6938038..
- RegAsm.exe
- conhost.exe
- filename1.exe
- filename1.exe
- RegAsm.exe
- conhost.exe
- RegAsm.exe
- conhost.exe

System Behavior

Analysis Process: f4b1bde3-706a-40d2-8ace-693803810b6f.exe PID: 4112 Parent PID: 5628

General

Start time:	22:06:51
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\f4b1bde3-706a-40d2-8ace-693803810b6f.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\f4b1bde3-706a-40d2-8ace-693803810b6f.exe'
Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	1364F8C4C00B87E5D938E9F95AF828F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic

Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 5672 Parent PID: 4112

General

Start time:	22:07:21
Start date:	22/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\f4b1bde3-706a-40d2-8ace-693803810b6f.exe'
Imagebase:	0xee0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1\filename1.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1306BF5	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1303712	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1303712	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1303712	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1303712	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1303712	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	1303712	InternetOpenUrlA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\subfolder1\filename1.exe	unknown	118784	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4f ad a0 db 0b cc ce 88 0b cc ce 88 0b cc ce 88 88 d0 c0 88 0a cc ce 88 44 ee c7 88 48 cc ce 88 3d ea c3 88 0a cc ce 88 52 69 63 68 0b cc ce 88 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 2b 7e 2e 60 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 50 01 00 00 40 01 00 00 00 00 00 a8 14 00 00 00 10 00 00 00 60 01 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 01 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......O.................... ..D...H...=.......Rich........ ....PE..L...+~.`............. ...P...@..............`....@.	success or wait	1	130162F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\f4b1bde3-706a-40d2-8ace-693803810b6f.exe	unknown	118784	success or wait	1	1306BF5	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\subfolder1\filename1.exe	success or wait	1	1301315	RegSetValueExA

Analysis Process: conhost.exe PID: 5544 Parent PID: 5672

General

Start time:	22:07:21
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: filename1.exe PID: 6732 Parent PID: 3388

General

Start time:	22:07:56
Start date:	22/02/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	1364F8C4C00B87E5D938E9F95AF828F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 24%, Metadefender, Browse • Detection: 68%, ReversingLabs
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: filename1.exe PID: 6844 Parent PID: 3388

General

Start time:	22:08:04
Start date:	22/02/2021
Path:	C:\Users\user\subfolder1\filename1.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	1364F8C4C00B87E5D938E9F95AF828F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: RegAsm.exe PID: 6920 Parent PID: 6732

General

Start time:	22:08:23
Start date:	22/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0x870000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D03712	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D03712	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D03712	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D03712	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D03712	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D03712	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6936 Parent PID: 6920

General

Start time:	22:08:23
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegAsm.exe PID: 7000 Parent PID: 6844

General

Start time:	22:08:32
Start date:	22/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\subfolder1\filename1.exe'
Imagebase:	0xb50000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 7012 Parent PID: 7000

General

Start time:	22:08:33
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis