



ID: 829692
Sample Name: terraform.exe
Cookbook: default.jbs
Time: 21:37:32
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report terraform.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 7
URLs from Memory and Binaries 7
World Map of Contacted IPs 11
General Information 11
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASNs 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Roaming\terraform.d\checkpoint_signature 12
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Authenticode Signature 13
Entrypoint Preview 13
Data Directories 15
Sections 15
Imports 15
Network Behavior 16
Statistics 16
Behavior 16
System Behavior 16
Analysis Process: terraform.exePID: 1076, Parent PID: 3452 16
General 16
File Activities 16
File Created 16
File Written 17
File Read 17
Analysis Process: conhost.exePID: 5256, Parent PID: 1076 17
General 17
Disassembly 17

Copyright Joe Security LLC 2023

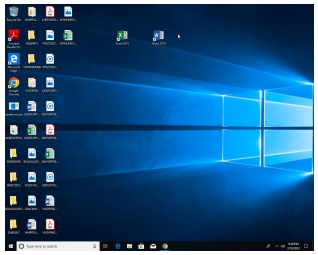
Windows Analysis Report

terraform.exe

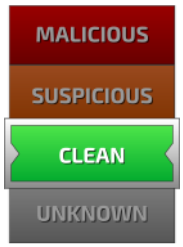
Overview

General Information

Sample Name:	terraform.exe
Analysis ID:	829692
MD5:	1c2071749f5f8…
SHA1:	e12db835a1ba…
SHA256:	8ad242bfaf1c0…
Infos:	



Detection

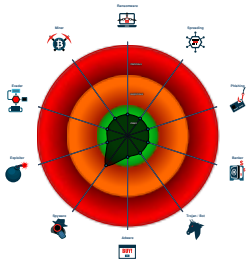


Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Queries the volume information (nam…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- terraform.exe (PID: 1076 cmdline: C:\Users\user\Desktop\terraform.exe MD5: 1C2071749F5F8BE8EB27874EEF8CD6D0)
  - conhost.exe (PID: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2023

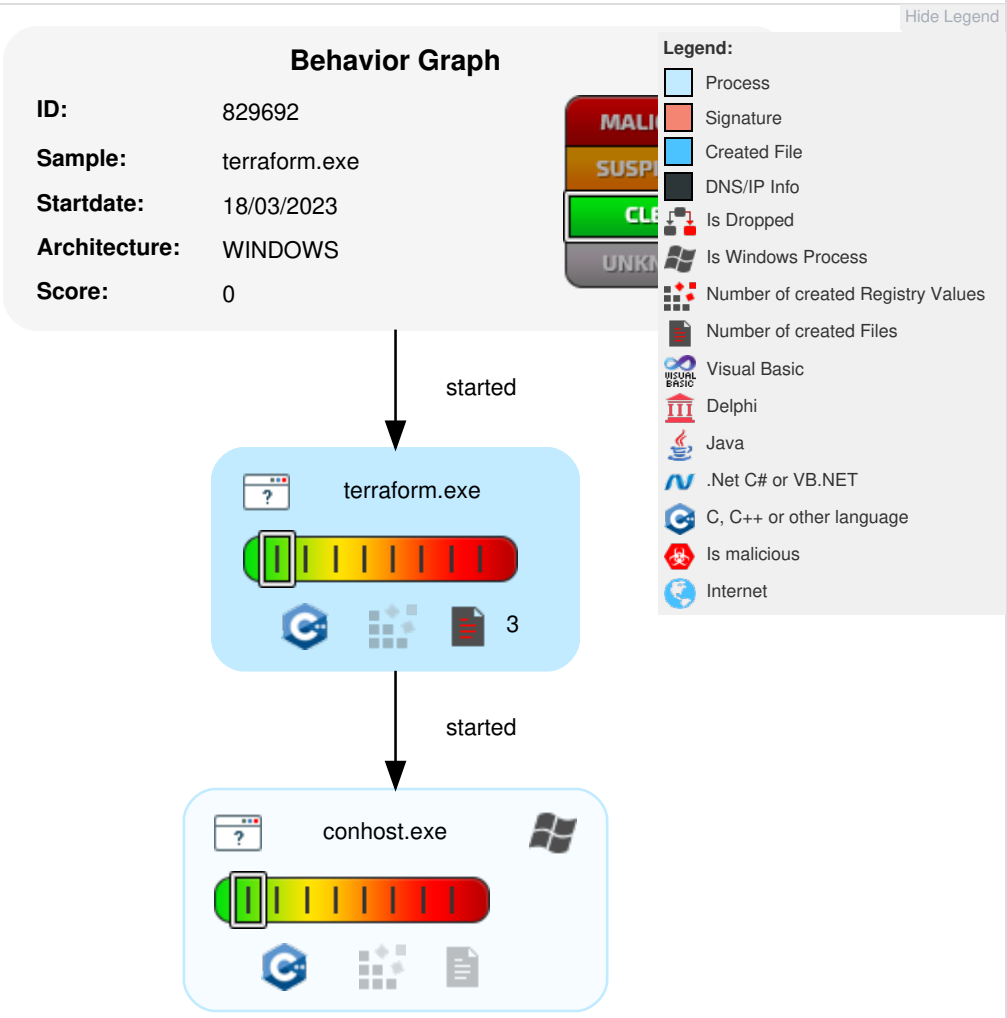
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	2 Command and Scripting Interpreter	Path Interception	1 Process Injection	1 Masquerading	OS Credential Dumping	1 1 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Process Injection	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

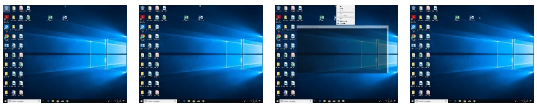
Behavior Graph



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
terraform.exe	0%	ReversingLabs		
terraform.exe	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Copyright Joe Security LLC 2023

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://git.k8s.io/enhancements/keps/sig-node/585-runtime-class	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/glusterfs/README.md#create-a-podpodIPs	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#spec-and-status.	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataDEPRECAT	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resourcesexterna	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataDEPRECAT	0%	Virustotal		Browse
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataPersiste	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/rbd/README.md#how-to-use-it	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata.RuleWit	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/enhancements/keps/sig-node/585-runtime-class	0%	Virustotal		Browse
http://https://examples.k8s.io/volumes/cephfs/README.md#how-to-use-itPhase	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resourcesexterna	0%	Virustotal		Browse
http://https://%s.amazonaws.com/%s/%shttps://%s.cos.%s.myqcloud.comhttps://batch.chinacloudapi.cnhttps://ba	0%	Avira URL Cloud	safe	
http://https://issues.k8s.io/61966The	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/glusterfs/README.md#create-a-podpodIPs	0%	Virustotal		Browse
http://169.254.170.2i/o	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/rbd/README.md#how-to-use-itEcsContainer	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#concurrency-cont	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata	0%	Avira URL Cloud	safe	
http://https://pkg.go.dev/cloud.google.com/go/storage#hdr-Credential_requirements_for_	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/iscsi/README.mdResource	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kindsDestr	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/mysql-cinder-pd/README.mdA	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataAllocata	0%	Avira URL Cloud	safe	
http://pr.k8s.io/79391	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/cephfs/README.md#how-to-use-itContainer	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/rbd/README.mdThe	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadatauid	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/mysql-cinder-pd/README.mdAt	0%	Avira URL Cloud	safe	
http://https://examples.k8s.io/volumes/glusterfs/README.mdThe	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataCurrent	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataThe	0%	Avira URL Cloud	safe	
http://https://kubernetes-csi.github.io/docs/ephemeral-local-volumes.html	0%	Avira URL Cloud	safe	
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#spec-and-statust	0%	Avira URL Cloud	safe	

Domains and IPs

Copyright Joe Security LLC 2023

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kubernetes.io/docs/concepts/storage/persistent-volumes#persistentvolumeclaims	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/storage/volumes#awselasticblockstoreThe	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/storage/volumes#hostpathUnschedulable	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataDEPRECAT	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/tasks/configure-pod-container/configure-service-account/can	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/nodes/node/#phase	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/workloads/controllers/replicationcontroller#pod-templateOnly	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#spec-and-status.	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/storage/volumes#emptydirNo	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/nodes/node/#addresses	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/#container-hooksUncountedTe	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#resourcesexterna	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://examples.k8s.io/volumes/glusterfs/README.md#create-a-podpodIPs	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://git.k8s.io/enhancements/keps/sig-node/585-runtime-class	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/storage/persistent-volumes#binding	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataPersiste	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/#label-selectorsThe	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/workloads/controllers/replicationcontroller#pod-templateThe	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://developers.google.com/protocol-buffers/docs/reference/go/faq#namespace-conflictinvalid	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/storage/volumes#awselasticblockstorename	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/storage/volumes#nfsgetting	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/workloads/controllers/jobs-run-to-completion/Route	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/containers/imagesError	terraform.exe, 00000000.00000000.255005973.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kinds	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://examples.k8s.io/volumes/rbd/README.md#how-to-use-it	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/services-networking/service/#publishing-services-service-typesWi	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://developers.google.com/accounts/docs/application-default-credentialsk8s.io.api.admissionregis	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata.RuleWit	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/storage/volumes#gcepersistentdiskData	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/workloads/pods/init-containers/	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/storage/volumes#hostpathTerraform	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://github.com/kubernetes/apiserver/blob/master/pkg/authentication/user/user.go	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/#label-selectorsGCEPersiste	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/workloads/controllers/daemonset/Optional:	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/HostAliases	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/storage/volumes#gcepersistentdiskNodeStageSecretRef	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://examples.k8s.io/volumes/cephfs/README.md#how-to-use-itPhase	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://%s.amazonaws.com/%s/%shttps://%s.cos.%s.myqcloud.comhttps://batch.chinacloudapi.cnhttps://ba	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	low
http://https://kubernetes.io/docs/concepts/scheduling-eviction/pod-overhead/	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://issues.k8s.io/61966The	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/#label-selectorspersistentV	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/overview/working-with-objects/names/#names	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://tools.ietf.org/html/rfc3339)	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/storage/persistent-volumes#persistent-volumes	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probesRegistry	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#pod-phaseThe	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false		high
http://https://examples.k8s.io/volumes/rbd/README.md#how-to-use-itEcsContainer	terraform.exe, 00000000.00000000.2550597373.000000000303C000.00000002.00000001.01000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://169.254.170.2i/o	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	low
http:// https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#concurrency-cont	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://tools.ietf.org/html/rfc4122#section-4.3)	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://kubernetes.io/docs/concepts/overview/working-with-objects/namespaces/Optional.	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadata	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://kubernetes.io/docs/concepts/storage/persistent-volumes#persistent-volumesOwnerReference	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/services-networking/service/#virtual-ips-and-service-proxiesno	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://pkg.go.dev/cloud.google.com/go/storage#hdr-Credential_requirements_for_	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle/#restart-policyAPIVersion	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://github.com/opencontainers/runtime-spec/blob/master/config.md#platform-specific-configuration	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://examples.k8s.io/volumes/iscsi/README.mdResource	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#types-kindsDestr	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://examples.k8s.io/mysql-cinder-pd/README.mdA	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://kubernetes.io/docs/concepts/overview/working-with-objects/names/#uids	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://pr.k8s.io/79391	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.terraform.io/downloads.htmlThe	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://kubernetes.io/docs/user-guide/identifiers#names	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/services-networking/service/#virtual-ips-and-service-proxies	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://kubernetes.io/docs/concepts/storage/persistent-volumes#persistentvolumeclaims00c6858e06b7040	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataAllocata	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.terraform.io/docs/cloud/workspaces/naming.html	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://www.terraform.io/language/provider-checksum-verification	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://kubernetes.io/docs/concepts/workloads/pods/pod-lifecycle#container-probesdefaultRuntimeClass	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://golang.org/pkg/unicode/#IsPrint.	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://examples.k8s.io/volumes/cephfs/README.md#how-to-use-itContainer	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kubernetes.io/docs/concepts/policy/resource-quotas/type	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://examples.k8s.io/volumes/rbd/README.mdThe	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/workloads/controllers/replicationcontroller/#what-is-a-replicati	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://examples.k8s.io/mysql-cinder-pd/README.mdAt	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://intl.cloud.tencent.com/document/product/598/10588).If	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://examples.k8s.io/volumes/glusterfs/README.mdThe	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/storage/persistent-volumes#persistentvolumeclaimsDaemonSetUpdate	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataThe	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadatauid	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://learn.hashicorp.com/collections/terraform/provision	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#metadataCurrent	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kubernetes.io/docs/concepts/architecture/nodes/#capacity	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/tasks/access-application-cluster/create-external-load-balancer/	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://www.iana.org/assignments/service-names).	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/overview/working-with-objects/labels/#label-selectorstUnknowntSt	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/containers/images#specifying-imagepullsecrets-on-a-podDEPRECATED	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/configuration/assign-pod-node/Adapts	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes-csi.github.io/docs/ephemeral-local-volumes.html	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://yaml.org/spec/1.2/spec.html)	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/tasks/administer-cluster/namespaces/observedGeneration	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://github.com/grpc/grpc/blob/master/doc/health-checking.md).	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/configuration/secrtThe	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/concepts/containers/container-lifecycle-hooks/#container-hooksresource	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://tools.ietf.org/html/rfc4648#section-4APIVersion	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http://https://kubernetes.io/docs/tasks/configure-pod-container/security-context/	terraform.exe, 00000000.00000000.2550597 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://github.com/OAI/OpenAPI-Specification/blob/master/versions/2.0.md#data-types	terraform.exe, 00000000.00000000.2550059 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false		high
http:// https://git.k8s.io/community/contributors/devel/sig-architecture/api-conventions.md#spec-and-statust	terraform.exe, 00000000.00000000.2550059 73.000000000303C000.00000002.00000001.01 000000.00000003.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829692
Start date and time:	2023-03-18 21:37:32 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	2
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
Sample file name:	terraform.exe
Detection:	CLEAN
Classification:	clean0.winEXE@2/1@0/0
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: .exe • Stop behavior analysis, all processes terminated

Warnings

- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

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\terraform.d\checkpoint_signature

Process:	C:\Users\user\Desktop\terraform.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	394
Entropy (8bit):	4.555193924304714
Encrypted:	false
SSDEEP:	6:DtdlB44ckCA7Kib/woN/MKN41kCA+IDefMqcoq/MKN44bPCAorFUFyouuc7PPMKE:RdrckHDNskrCfSNjPEUEo30elj
MD5:	62F73EAD179B70293BD82C081F9F2010
SHA1:	0BC355628EAB41886E5434868B0AD1D0EB952F0D
SHA-256:	D68F18C3ACD9B26BC28A18BC804E3703F0749B73B9A76EAA3BE83F7868E1160B
SHA-512:	30695C0FD05CED35E707835BBD04C0B6D5B27A2D7C3EA264362C88D2E1991F9B2754DCBAE2C28EA33FB301D99A79BD87E18DEBEAFBBE5292841C81A45899865
Malicious:	false
Reputation:	low
Preview:	7b81de41-aa3a-8566-f8c2-c1b0568efddb...This signature is a randomly generated UUID used to de-duplicate.alerts and version information. This signature is random, it is.not based on any personally identifiable information. To create.a new signature, you can simply delete this file at any time..See the documentation for the software using Checkpoint for more.information on how to disable it...

Static File Info

General

File type:	PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
Entropy (8bit):	6.1362431210196355
TrID:	• Win64 Executable (generic) (12005/4) 74.95% • Generic Win/DOS Executable (2004/3) 12.51% • DOS Executable Generic (2002/1) 12.50% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.04%
File name:	terraform.exe
File size:	65422512
MD5:	1c2071749f5f8be8eb27874eef8cd6d0
SHA1:	e12db835a1ba37da876609049bceae91d078949b
SHA256:	8ad242bfaf1c06b364e7f94e4dc7e468f4583232032a1627df28655df0db6e4b

Copyright Joe Security LLC 2023

SHA512:	fe1c1255f4436327922a4fa74e2329fb7e8e29596177dbee43fcd5e9a412afd41ee44a66121929ca6fcc15b2df39f157d1d95cf201b1c70ce3ec5089fc7f26ca
SSDEEP:	1572864:lKmmvHWTSqKqhXP2fcV06ngaD6HuFp/7Ke8BSQY7UtCxQeXfI2WbTCFJzGU0iFpl:TT
TLSH:	16E74947F45680E4C1EDD134CA258662BB313C899B3033D72F61FAB82B76BE4667A354
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d..... ....."".....R.....@.....K.....`... .....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4689e0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DEBUG_STRIPPED
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6
File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	9cbefe68f395e67356e2a5d8d1b285c0

Authenticode Signature

Signature Valid:	**true**
Signature Issuer:	CN=DigiCert Trusted G4 Code Signing RSA4096 SHA384 2021 CA1, O="DigiCert, Inc.", C=US
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 1/9/2023 4:00:00 PM 1/9/2026 3:59:59 PM
Subject Chain	• CN="HashiCorp, Inc.", OU=HashiCorp Security, O="HashiCorp, Inc.", L=San Francisco, S=California, C=US
Version:	3
Thumbprint MD5:	FA839AEA713AC65409D9B5CDB665E59B
Thumbprint SHA-1:	7868E4F55FD7B047CD8BF93FEA8C38509CFB5939
Thumbprint SHA-256:	0F3E822C8907D52A1A7DCCDD6EFC6626270187FDB263E50BFC37AA2515F4CEA8
Serial:	0B26FB4E1C1A6BC3264602189258449D

Entrypoint Preview

Instruction
jmp 00007FF12048D140h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
pushfd
cld
dec eax
sub esp, 000000E0h
dec eax
mov dword ptr [esp], edi
dec eax
mov dword ptr [esp+08h], esi
dec eax
mov dword ptr [esp+10h], ebp
dec eax
mov dword ptr [esp+18h], ebx
dec esp
mov dword ptr [esp+20h], esp
dec esp
mov dword ptr [esp+28h], ebp
dec esp
mov dword ptr [esp+30h], esi
dec esp
mov dword ptr [esp+38h], edi
movups dqword ptr [esp+40h], xmm6
movups dqword ptr [esp+50h], xmm7
inc esp
movups dqword ptr [esp+60h], xmm0
inc esp
movups dqword ptr [esp+70h], xmm1
inc esp
movups dqword ptr [esp+00000080h], xmm2
inc esp
movups dqword ptr [esp+00000090h], xmm3
inc esp
movups dqword ptr [esp+000000A0h], xmm4
inc esp
movups dqword ptr [esp+000000B0h], xmm5
inc esp
movups dqword ptr [esp+000000C0h], xmm6
inc esp
movups dqword ptr [esp+000000D0h], xmm7
dec eax
sub esp, 30h
dec ecx
mov edi, eax
dec eax

Copyright Joe Security LLC 2023

Instruction
mov edx, dword ptr [00000028h]
dec eax
cmp edx, 00000000h
jne 00007FF120490E8Eh
dec eax
mov eax, 00000000h
jmp 00007FF120490F05h
dec eax
mov edx, dword ptr [edx+00000000h]
dec eax
cmp edx, 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3e6a000	0x47c	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3e62200	0x22b0	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3e6b000	0x7b636	.reloc
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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x3c76be0	0x140	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d1a1ac	0x1d1a200	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x1d1c000	0x1f56658	0x1f56800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3c73000	0x1f6470	0x175200	False	0.4149706867671692	data	5.582797825302087	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.idata	0x3e6a000	0x47c	0x600	False	0.3333333333333333	data	3.7179068130601314	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.reloc	0x3e6b000	0x7b636	0x7b800	False	0.11984438259109312	data	5.462801439594526	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.symtab	0x3ee7000	0x4	0x200	False	0.02734375	data	0.020393135236084953	IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

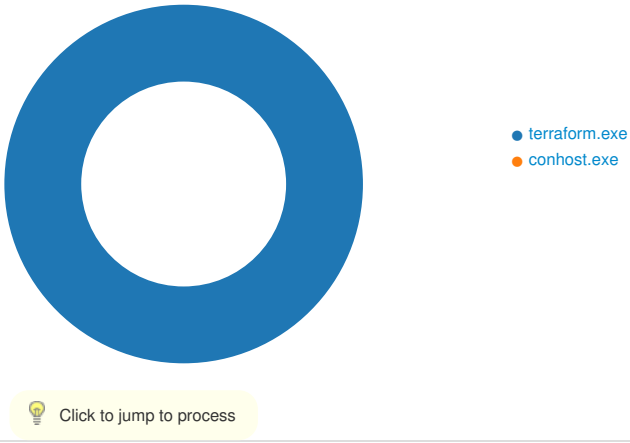
DLL	Import
kernel32.dll	WriteFile, WriteConsoleW, WaitForMultipleObjects, WaitForSingleObject, VirtualQuery, VirtualFree, VirtualAlloc, SwitchToThread, SuspendThread, SetWaitableTimer, SetUnhandledExceptionFilter, SetProcessPriorityBoost, SetEvent, SetErrorMode, SetConsoleCtrlHandler, ResumeThread, PostQueuedCompletionStatus, LoadLibraryA, LoadLibraryW, SetThreadContext, GetThreadContext, GetSystemInfo, GetSystemDirectoryA, GetStdHandle, GetQueuedCompletionStatusEx, GetProcessAffinityMask, GetProcAddress, GetEnvironmentStringsW, GetConsoleMode, FreeEnvironmentStringsW, ExitProcess, DuplicateHandle, CreateWaitableTimerExW, CreateThread, CreateIoCompletionPort, CreateFileA, CreateEventA, CloseHandle, AddVectoredExceptionHandler

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

Behavior



System Behavior

Analysis Process: terraform.exe PID: **1076**, Parent PID: **3452**

General

Target ID:	0
Start time:	21:38:26
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\terraform.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\terraform.exe
Imagebase:	0x1320000
File size:	65422512 bytes
MD5 hash:	1C2071749F5F8BE8EB27874EEF8CD6D0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\terraform.d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1388BFE	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\terraform.d\checkpoint_signature	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	1388BFE	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\terraform.d\checkpoint_signature	0	394	37 62 38 31 64 65 34 31 2d 61 61 33 61 2d 38 35 36 36 2d 66 38 63 32 2d 63 31 62 30 35 36 38 65 66 64 64 62 0a 0a 0a 54 68 69 73 20 73 69 67 6e 61 74 75 72 65 20 69 73 20 61 20 72 61 6e 64 6f 6d 6c 79 20 67 65 6e 65 72 61 74 65 64 20 55 55 49 44 20 75 73 65 64 20 74 6f 20 64 65 2d 64 75 70 6c 69 63 61 74 65 0a 61 6c 65 72 74 73 20 61 6e 64 20 76 65 72 73 69 6f 6e 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 20 54 68 69 73 20 73 69 67 6e 61 74 75 72 65 20 69 73 20 72 61 6e 64 6f 6d 2c 20 69 74 20 69 73 0a 6e 6f 74 20 62 61 73 65 64 20 6f 6e 20 61 6e 79 20 70 65 72 73 6f 6e 61 6c 6c 79 20 69 64 65 6e 74 69 66 69 61 62 6c 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2e 20 54 6f 20 63 72 65 61 74 65 0a 61 20 6e 65 77 20 73 69 67 6e 61 74 75 72 65 2c 20 79 6f 75 20 63 61	7b81de41-aa3a-8566-f8c2-c1b0568efddbThis signature is a randomly generated UUID used to de-duplicatealerts and version information. This signature is random, it isnot based on any personally identifiable information. To createa new signature, you ca	success or wait	1	1388BFE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\terraform.exe	0	64	success or wait	8	1388BFE	ReadFile

Analysis Process: conhost.exe PID: **5256**, Parent PID: **1076**

General

Target ID:	1
Start time:	21:38:32
Start date:	18/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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

No disassembly