Cloud Visibility Report

This cloud visibility report (CVR) provides discovery of your cloud assets and visibility of traffic flows to show the intent and actual traffic from potentially compromised workloads to malicious sites. Using DNS queries and VPC flow logs, and combining it with cloud asset information and threat intelligence it provides you with a perspective on data exfiltration attempts on egress (outbound to Internet) traffic flows. Deploying Valtix Gateways will give you visibility and actual protections for all traffic flows: inbound from Internet, outbound to Internet, east-west between VPCs and to PaaS services like AWS S3, RDS and others.

Report dated: 31/03/2021
Traffic data period: 24/03/2021 to 31/03/2021

Prepared by Valtix, Inc.

Prepared for
jigar+sedemo@valtix.com

To learn how we can help you better secure your public clouds, contact Valtix at: info@valtix.com, call 650.420.6014 or visit www.valtix.com

Executive Summary

Visibility is usually the first step to finding insights. This report provides some of the insights available in Valtix to detect malicious activity from your public cloud workloads. This report is generated by Valtix using DNS queries and VPC flow logs. Valtix uses a simple approach: Discover, Deploy and Defend using a cloud-native security-as-a-service (SaaS) from the SaaS portal or using Terraform to bake security into the DevOps process. This report provides you a summary of the Discovery capabilities of Valtix. Based on these insights you can Deploy Valtix Gateways and Defend using cloud-aware security policies.

Key Findings

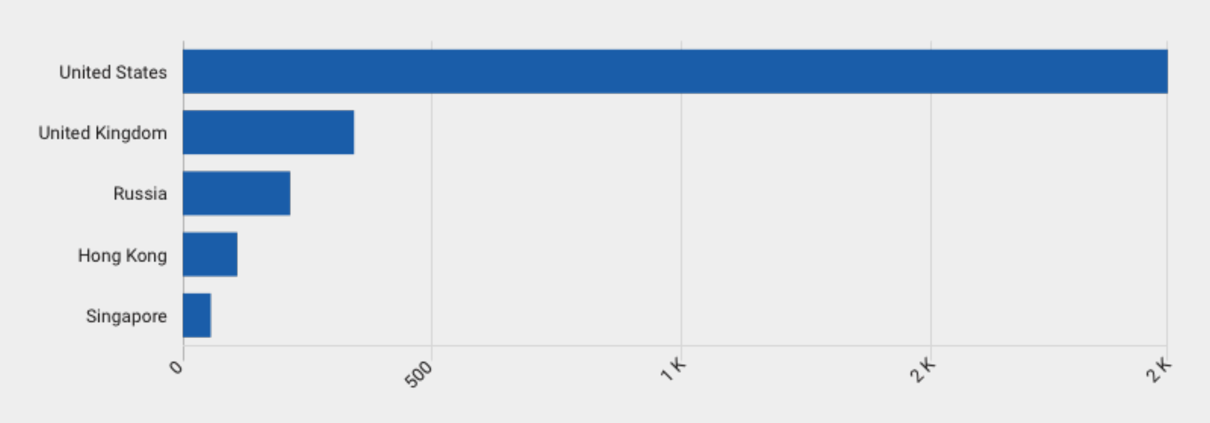
- The following instances were found to be connecting to top 3 malicious site categories:
  - 4 instances connecting to Malware Sites
  - 3 instances connecting to Phishing and Other Frauds
- 41 malicious destinations visited across top malicious categories:
  - Phishing and Other Frauds
  - Malware Sites
- Top countries by egress queries to malicious destinations

41
Malicious Sites Visited

2
Malicious Categories Visited

4
Instances Connecting Outbound to Malware Sites

8
Countries Linked to Malicious Sites



Most common DNS queries for malicious sites by destination countries

Discovered Assets

Valtix builds a continuous, near real-time, inventory of your cloud assets that are correlated with traffic flows to detect potential breaches. This also enables you to configure security policies, when Valtix Gateways are deployed, that use the meta-data such as tags of the cloud assets, instead of using IP addresses used in legacy firewall products. For example, tags assigned by application and DevOps teams such as “production”, “pci”, “staging”, “web”, “db” etc can be used to create globally consistent multi-cloud security policies.

Cloud Accounts	Regions	VPCs/VNets	Subnets	Security Groups	Load Balancers	Instances
3	19	32	117	116	17	62

Network Interfaces	Tags	Route Tables	Applications	Certificates
144	110	59	29	-

Network Security Insights

Valtix uses the discovery of your cloud assets to provide security insights. Details are available in your Valtix Controller > Discovery > Insights > Rules. These findings should be used to remediate your public cloud environment:

- Reduce the number of open security groups with large open port ranges, both for inbound from Internet, east-west and outbound to Internet.
- Deploy inline network security for inspection using Valtix Gateways.

Findings

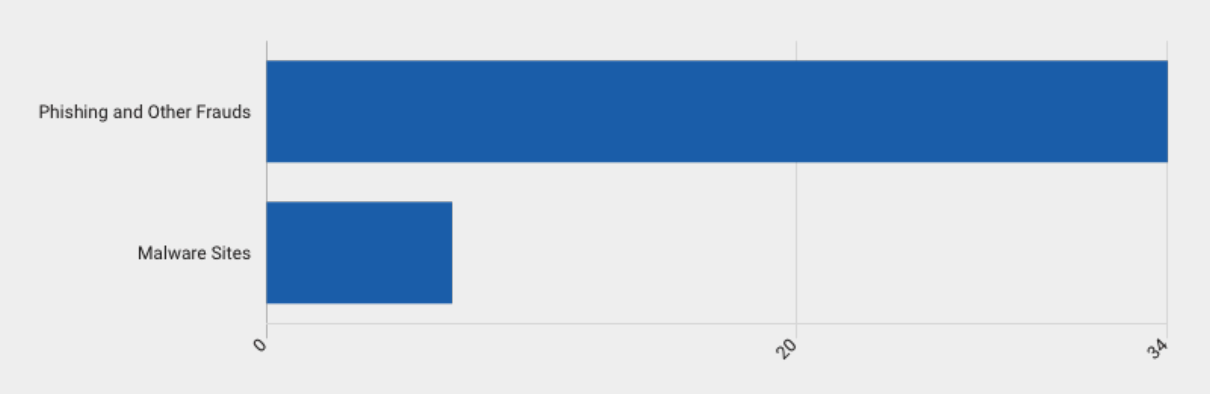
- 26 Public Subnets (subnet with auto assigned public IP addresses)
- 72 Network interfaces with public IPs
- 17 Application Load Balancers with no cloud WAF
- 17 Public Security Groups with more than 10 open ingress (Internet-facing) ports
- 97 Security Groups with more than 20 open egress (outbound to Internet) ports

DNS Traffic Insights

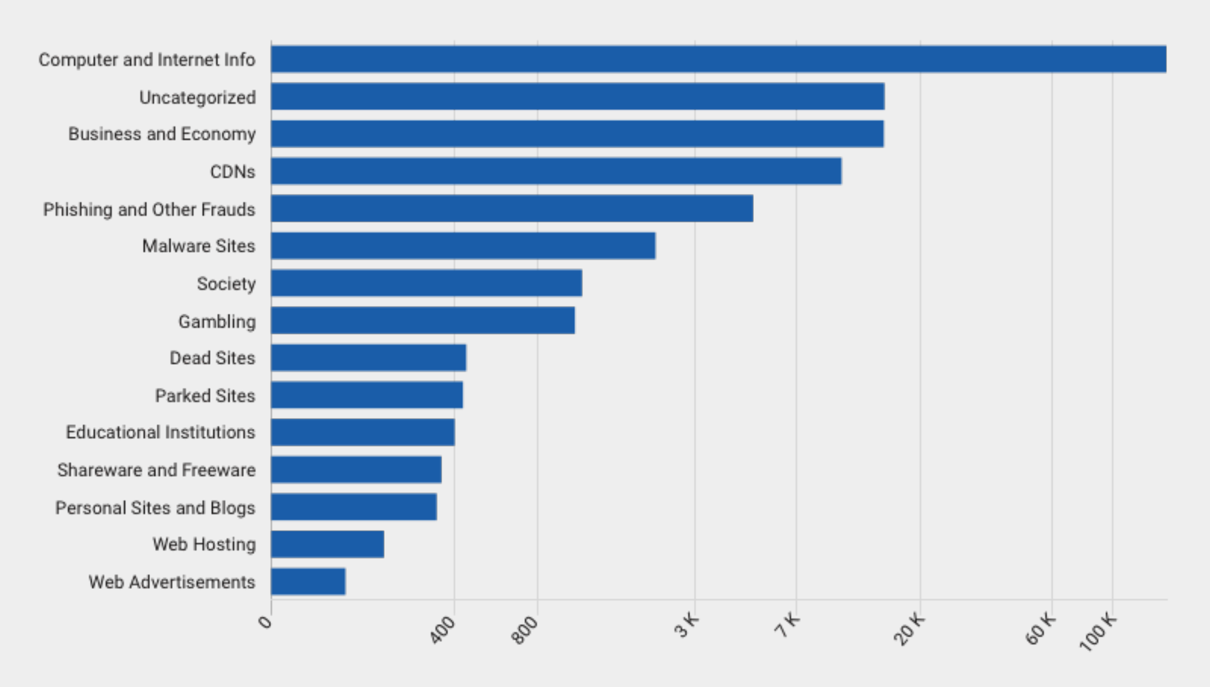
DNS traffic from cloud service providers (AWS Route53) provides unique insights into how your applications are behaving. They show the normal usage pattern of instances and potentially dangerous behavior, whether its malicious insiders or compromised attackers that connect to known bad destinations. This visibility is a key insight that can help you deploy inline protections of Valtix Gateways to stop the attack and break the kill chain to stop exfiltration.

Key Findings

- 5360 total unique destinations visited across 34 domain categories
- 41 malicious destinations visited across malicious categories



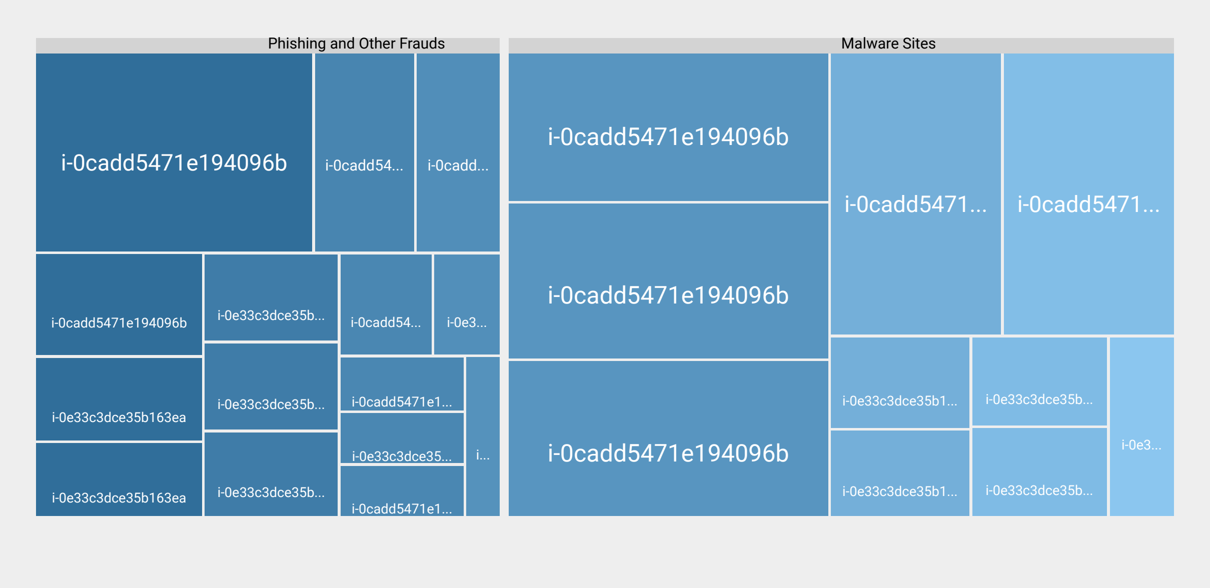
Egress Traffic to FQDN/Domains Belonging to Malicious Categories



Egress Traffic to FQDN/Domains of Top Categories

Egress Traffic by Instances

To truly understand and investigate potential compromise and exfiltration you have to look at instances that are connecting to malicious sites with DNS queries. In the Valtix Controller you can correlate this to see which other instances are connecting to those sites, and see the VPC flow logs to review actual traffic flows.



Instances with the highest DNS queries to malicious destinations

DNS queries to malicious destinations by instance-id (Top 25)

No.	Destination	Category	Instance Name / Instance ID	Record Count
1	davidneujahr.com.	Phishing and Other Frauds	i-0cadd5471e194096b	378
2	magic4you.nu.	Malware Sites	i-0cadd5471e194096b	313
3	divineenterprises.net.	Malware Sites	i-0cadd5471e194096b	308
4	mactep.org.	Malware Sites	i-0cadd5471e194096b	308
5	purplehoodie.com.	Malware Sites	i-0cadd5471e194096b	308
6	17ebook.com.	Malware Sites	i-0cadd5471e194096b	307
7	grub-bokep.mobilelegend-event7.gq.	Phishing and Other Frauds	i-0cadd5471e194096b	146
8	www.https.mobilelegend-event7.gq.	Phishing and Other Frauds	i-0cadd5471e194096b	134
9	www.grub-bokep.mobilelegend-event7.gq.	Phishing and Other Frauds	i-0cadd5471e194096b	132
10	ryml-postalsupport.com.	Phishing and Other Frauds	i-0e33c3dce35b163ea	122
11	magic4you.nu.	Malware Sites	i-0e33c3dce35b163ea	118
12	www.vidios-viral.duckdns.org.	Phishing and Other Frauds	i-0e33c3dce35b163ea	117
13	17ebook.com.	Malware Sites	i-0e33c3dce35b163ea	116
14	divineenterprises.net.	Malware Sites	i-0e33c3dce35b163ea	116
15	purplehoodie.com.	Malware Sites	i-0e33c3dce35b163ea	116
16	mactep.org.	Malware Sites	i-0e33c3dce35b163ea	115
17	www.grub-bokep.mobilelegend-event7.gq.	Phishing and Other Frauds	i-0e33c3dce35b163ea	115
18	www.ryml-postalsupport.com.	Phishing and Other Frauds	i-0e33c3dce35b163ea	115
19	grub-bokep.mobilelegend-event7.gq.	Phishing and Other Frauds	i-0e33c3dce35b163ea	114
20	www.vidios-viral.duckdns.org.	Phishing and Other Frauds	i-0cadd5471e194096b	108
21	lloydsunauthorised-device-connect.com.	Phishing and Other Frauds	i-0e33c3dce35b163ea	101
22	vidios-viral.duckdns.org.	Phishing and Other Frauds	i-0cadd5471e194096b	101
23	grupnotnot23.duckdns.org.	Phishing and Other Frauds	i-0e33c3dce35b163ea	100
24	join-whatsapp-frontalgaming.duckdns.org.	Phishing and Other Frauds	i-0cadd5471e194096b	100
25	jobsaraby.online.	Phishing and Other Frauds	i-0e33c3dce35b163ea	98

What are Malicious Site Categories?

Malicious sites are domains and fully-qualified domain names (FQDN) for sites that have exhibited behavior that compromises security, for example drive-by downloads to install malware or spyware, or open command-and-control (C2) connections to attackers. These are categorized into seven specific categories listed in the table below. Valtix uses industry-leading web classification from WebRoot BrightCloud® to provide threat intelligence to categorize these sites.

Malicious Category
Keyloggers
Malware Sites
Phishing
Anonymizing proxies
Spyware & Adware
Bot nets
SPAM URLs

What data is part of this Cloud Visibility Report from Valtix?

Valtix is using the following data collected by the Valtix Controller from your public cloud environment and provides insights into threat vectors for outbound (egress) traffic to the Internet:

- **Cloud asset information** - near real-time inventory of your cloud deployments
- **DNS query logs** - public cloud DNS queries from AWS Route 53
- **VPC flow logs** - this is currently not included in the CVR, but available in your Valtix Controller account to correlate DNS queries from instances to actual traffic behavior
- **DNS/FQDN web classification** - this categorizes the site's reputation across 72 categories, including 7 malicious categories
- **Geo-IP classification** - mapping the resolved IP address for DNS to countries

How do I use this report?

Valtix is synthesizing above information in real-time and across a large scale to give you insights into your network security posture. This becomes the basis of determining your traffic patterns, and which instances might be compromised. This will help you decide where to deploy Valtix Gateways for actual inline protection, and how to configure security policies for:

- TLS decryption
- URL and FQDN filtering (with option to disable TLS decryption for specific FQDNs/domains or categories)
- Data loss prevention (DLP)
- IDS/IPS and antivirus (AV) to stop malware

For example, using the CVR information, you can deploy Valtix Gateways and create a policy that leverages cloud asset information (aka attribute-based access control) says:

- Allow my PCI workloads to connect to Financial Services sites
- Allow my Dev instances to connect to github.com/myOrgRepo, dev-s3-bucket and dev-aws-rds-test-db, but not to any "prod" systems
- Block outbound traffic from all my public cloud to any malicious sites

Note: Classification of domains/FQDNs into categories and geo-IP, especially malicious ones, is a continuously evolving landscape. Valtix provides this mapping using the industry-leader BrightCloud. This threat intelligence, especially malicious ones, is the starting point of an investigation that should be handled by the incident response (IR) team.