June 2021 Version 2.0.0



DomainTools App for IBM QRadar User Guide



Overview	3
What's New in 2.0.0	4
2.0.0 Release Notes	4
Deployment Guide	5
App Components	5
Table: Right Click Actions	5
Table: Settings	11
Prerequisites	12
DomainTools App Bundle	12
DomainTools API Key	12
Firewall Rule	12
QRadar Credentials to Install App	12
Extract Domains From Offenses for Enrichment	12
App Installation	14
Uninstalling Prior Versions	14
Installation Steps	14
App Configuration Steps	15
Managing API Connectivity	16
Key App Functionalities	17
Right Click Context	17
Associated Domain Count Explanation	17
Average Risk Score Explanation	17
Offense Summary Custom Fragment	17
Associated Domain Count Explanation	18
Quickly Open Up Investigations in DomainTools Iris	18
Troubleshooting & Known Issues	20
Issue Tracker	20
Issue Details	21
showRtClickDomainTools is not defined	21
Right-click "Show in DomainTools Iris" triggers a popup blocker in Firefox	22

≡ 16	BM QRadar																		(III)	Ċ	2
Dashboard	Offenses	Log Activity	Network Activity	Assets	Reports	Risks	Vuinerabilit	es A	imin Pulse	Use Case	Manager								anananana k	System Time:	: 3:26 PM
Search ¥	Quick Searches	Add Filter	Save Critoria 🗊 Sav	ve Resu*-	1. a			••••••							2	3					0
► Current	Current Statistics				omainTools Domain Data																
Records M	latched Over T	ime																			14
Reset Zoo	म्म			5	Summary								4/15/21, 3:20	PM - 4/15/21,	3:25 PM 🗸						
250					Field Nam	е			Value												
500				-	Original Vi	alue			G5Z7TH4Q43.	TTAROIL.wo	kangmedia.cor	m				-					
250		1			Domain Name wokangmedia.com										-						
3:20:00	PM 3:20:15 PM	4 3:20:30 PM	1 3:20:45 PM 3:21:00	PM	Overall Bi	ek Senta			80							3:24:0	0 PM 3:24:15	PM 3:24:30	PM 3:24:45	PM 3:25:00	c l
					overan ru	ak ocore															
					Reason				age,domain na	me,infrastruc	ure,registration	n									÷.
					Create Da	ite			2020-10-13												
logsource_	logsource_i	URL	UrlHo	st	Last Upda	ted Date			2021-04-1472	:04:21						ntityip	destinationi	destination	category	username	
Squid We	WebProxy	G5Z7TH4	G5Z7TH4Q43.qTTARC	Olt.woh	C1-1-1											0.0.0	199.30	0	4034	N/A	10
Squid We	WebProxy	3P6L7T4	3P6L7T4GF4.µKKEsA	N.dou	Status				Active							.0.0.0	199.30	0	4034	N/A	
Squid We	WebProxy	YQ2Y8SV	YQ2Y8SVZ36.XOfxlzV	/q.kike												0.0.0	199.30	0	4034	N/A	
Squid We	WebProxy	777FSJX	777FSJXKS2.rkZeTLe	U.code												.0.0.0	199.30	0	4034	N/A	
Squid We	WebProxy	KZ3QVJV	KZ3QVJVSXR.lecIRFt	uQ.ilov							ſ	10-27-00	-	and an entry	Constanting of	.0.0.0	199.30	0	4034	N/A	
Squid We	WebProxy	7TIIYNN4	7TIIYNN4WK.LLFJZos	sf.sdzh								Oper	n in Don	nainTools I	ris Close	0.0.0	199.30	0	4034	N/A	
Squid We	WebProxy	0AWUP38	0AWUP38GQS.sBkwy	hwx.pi							34					0.0.0	199.30	0	4034	N/A	
Squid We	WebProxy	8KRUAZE	8KRUAZEJZB.mqzxLf	yt.linksysnir	n.com N	I/A	16185000	255	10.10	2 113	135000	75 0		1	4	0.0.0.0	199.30	0	4034	N/A	
Squid We	WebProxy	51UL0H3	51UL0H3V9N.uOvtxoE	EY.govstcad	I-reb N	I/A	16185000	255	10.10	6 113	135000	75 0		1	4	0.0.0.0	199.30	0	4034	N/A	

Fig 1: DomainTools Domain Data Modal

Overview

The DomainTools App provides direct access to DomainTools industry-leading threat intelligence data, predictive risk scoring, and critical attributes to gain situational awareness on malicious domains inside of QRadar.

Customers who deploy the app in QRadar benefit from:

- Rich context on domains and IP addresses, delivered directly within IBM QRadar.
- Domain risk assessment based on proximity and threat profile scores, giving you an answer to the question "Could this be bad?" for every domain, even if it has never before been reported to an industry block list or threat feed.
- IP risk assessment based on the average risk scores of any domains hosted on that IP.
- Full domain and IP profile information directly in the Offense Summary view.

What's New in 2.0.0

DomainTools App for IBM QRadar 2.0.0 is the General Availability (GA) release of our app for IBM QRadar SIEM. Please review the release notes to understand the key features and changes in this release.

2.0.0 Release Notes

Changes and Fixes

- Completely re-designed integration to operate more seamlessly within newer versions of QRadar (v7.4.1 Patch 2+)
- On demand enrichment summaries for domains, SSL hashes, and IPs throughout QRadar.
- Quick maneuvering to open DomainTools Iris investigations from domains, SSL hashes, and IPs.
- Custom fragment for offenses showing enrichment data for domains associated with that offense.
- Removed the threat hunting dashboard, offense creation, and domain profile persistence due to architectural limitations in QRadar

Deployment Guide

App Components

The QRadar app is provisioned with the following main components.

Table: Right Click Actions

These actions allow a user to right click on the designated fields to on demand enrich the specified entity.

Item	Properties (Case Sensitive)	Description
Domains	UrlHost	Shows a summary of key data points for the selected domain including:
	urlhost	Original Value Domain Name Overall Rick Score
	url_host	 Reason Create Date
	Url_Host	 Last Updated Date Status
	urlHost	Guided Pivots that are under the 500 count threshold
	URLHOST	UriHost X509 Certificate Fingerprint Hash starttime protocolid sourceip logsourceic XGIP3C82A.mqOFWomy.nehotel.ga N/A 16191102 255 10.10.1 113 135 DI UD00011/GE Domenonium V/A 16191102 255 10.10.1 113 135
URL_ Url url URL	URL_HOST	ALEHDOSofty Similarias Transmission and
	Url	UQ7M8219M.MsRsUdzd.ivoryfrpt View in DSM Editor F9PFD8RF8.WOMNRWq.coltran Plugin options F0WB0RN1V_IoVIII Mst International Internation
	url	
	URL	
	Domain	
	domain	
	DOMAIN	
	Destination Host Name	
	Hostname	
	Source Host Name	
	URL Path	
	URL Query String	

	Referrer URL	DomainTools Do	main Data	a				×		
	Originating Host	Summary								
	Recipient Host	Field Name		Value						
	· · ·	Original Value		RILHD098M.ySmBnkas.uvcleancarservice.com						
	Remote Host	Domain Name		uvcleancarservice.com						
		Overall Bisk Score		77						
	DNS Domain Name	Heason		age,oomain name,inirastructure,registration						
		Create Date		2020-10-08						
	DNS Response	Last Updated Date		2021-04-21T22	03:18					
		Status		Active						
		Guided Piv	ots							
		Field Name		v	alue	Associated Do	main Count			
		REGISTRANT CONTACT ORG WMD Cleaning		MD Cleaning	39					
				39						
						Open in Do	omainTools Iris	Close		
	action.	 IP) Avera Count ISP ASN 	ge Dom try Code	ain Risk S	icore for do	mains asso	ociated wit	n the IP		
		sourceip logs	sourceid	qid	sourceport	eventcount	magnitude	identityip		
		10.10.3 162	2	13500075	0	1	4	0.0.0.0		
		163.44 162		13500075	136 225	9	2	0.0.0.0		
		10.10 Filte	er on sourc	ceip is not 16	3.44.136.225		4	0.0.0.0		
			se Positive)			2	0.0.0.0		
		163.4 View	w in DSM B	Editor			2	0.0.0.0		
		163.4 Mor	re Options.			Naviga	- ate			
		···· 163.44 162	2	13500075	0	1 Inform	ation			
		10.10.3 162	,		0	1 Pup E	oronsics Pocov	•		
				13500075	1.2.1	Null F	DI El ISICS RECUS	ery		
		163.44 162	2	13500075 13500075	0	1 Run F	orensics Searc	ery		
		163.44162163.44162	2	13500075 13500075 13500075	0	1 Run F	orensics Searc	ery		
1		 163.44 162 163.44 162 163.44 162 	2	13500075 13500075 13500075 13500075	0 0 0	Run F Run F Plugin	orensics Searc options IP Data	ery		
		163.44 162 163.44 162 163.44 162 163.44 162 163.44 162	2	13500075 13500075 13500075 13500075 13500075	0 0 0 0	Run F Plugin Show	orensics Searc options IP Data Mailserver IP D	ery h		
		 163.44 162 163.44 162 163.44 162 163.44 113 10.10.3 113 	2	13500075 13500075 13500075 13500075 13500075 13500075	0 0 0 0 0	Run F Plugin Show	options options I <u>P Data</u> Mailserver IP D	ery		
		 163.44 162 163.44 162 163.44 162 163.44 113 10.10.3 113 163.44 113 		13500075 13500075 13500075 13500075 13500075 13500075 13500075	0 0 0 0 0 0	Run F Plugin Show Show	orensics Recov options I <u>P Data</u> Mailserver IP D Nameserver IP In DomainTools	ery n Data Lata		

		DomainTools IP Data							
		Field Name	Value						
		Original Value	163.44.136.225						
		IP Shared Domain Count	450						
		IP Average Domain Risk Score	75						
		Country Code	sg						
		ISP	GMO Internet Pte Ltd						
		ASN	59349						
		Open in	DomainTools Iris Close						
Mailserver IPs	Due to how QRadar handles IPs, all data with the IP data type has this action.	 Shows a summary of key data points for including: Original Value Shared Domain Count (number Mailserver IP) Average Domain Risk Score for Mailserver IP Example: 	the selected Mailserver IP of domains associated with the domains associated with the						

		logeourceid	aid	sourcepo	t av	entcount	magnitude	identitvin	destination
		162	13500075	0	1	enteount	4	0.0.0.0	216.23
		162	13500075	0			0	0.0.0.0	107.15
		162	13500075	0		Filter on	destinationip i	s 107.152.46.	105
		162	13500075	0		Filter on	destinationip i	s not 107.152	.46.105
		162	13500075	0	+	False Po	ositive		
		162	13500075	0		View in	DSM Editor		
		162 Na	vigate			More Op	otions		
		162 Info	ormation		▶ 1		2	0.0.0.0	107.15.
		162 Ru	n Forensics F	Recoverv	1		4	0.0.0.0	216.23.
		162 Ru	n Forensics S	Search	1		2	0.0.0.0	107.15.
		162 Plu	iain options		▶ 1		2	0.0.0.0	107.15.
		162 Sh	ow IP Data		6		2	0.0.0.0	107.15.
		113 Sh	ow Mailserve	IP Data	1		2	0.0.0.0	107.15.
		113 Sh	ow Namesen	er IP Data	1		4	0.0.0.0	216.23.
		113 Sh	ow In Domain		1		2	0.0.0.0	107.15.
		113	13500075	0	1		4	0000	216.23
		Field Na	me				Value		
		Original V Shared D	Value Domain Coun	t			107.152.4	6.105	
		Average	Domain Rick	Score			59		
		Average			000	n in Do	mainTools		loso
				L	Ope	in in Do	main tools		lose
Nameserver IPs	Due to how QRadar handles IPs, all data with the IP data type has this action.	Shows a su including: Or Sh Na Av Na	ummary o riginal Val nared Don ameserve verage Do ameserve	f key data nain Coun r IP) main Risk r IP	poir t (nu Sco	its for th Imber o re for do	ne selected f domains a omains ass	Nameser associated ociated wi	ver IP I with the ith the

				1			1.1	d	
		ourceic	qia	sourceport	eventcount	magnitude	identityip	destination	
			13500075	0	0	+ 2	0.0.0.0	107 15	
			13500075	0	Filter on	destinationip i	s 107.152.46.	105	
			13500075	0	Filter on	destinationip i	s not 107.152	.46.105	
			13500075	0	🔸 False Po	ositive		Ë	
			13500075	0	View in I	DSM Editor	M Editor		
		Na	vigate		More Op	otions	ns ►		
		Inf	ormation		1	2	0.0.0.0	107.15.	
		Ru	n Forensics F	ecoverv	1	4	0.0.0.0	216.23	
		Ru	n Forensics S	earch	1	2	0.0.0.0	107.15	
		Plu	ugin options		1	2	0.0.0.0	107.15	
		Sh Sh	ow IP Data		6	2	0.0.0.0	107.15	
		Sh Sh	ow Mailserve	IP Data	1	2	0.0.0.0	107.15	
		Sh Sh	ow Nameson	or IP Data	1	4	0.0.0.0	216.23	
		in ch	ow In Domain	Toole Irie	1	2	0.0.0.0	107.15	
		10 51	ow in Domai						
						Value			
		Ori	ginal Value			107.15	2.46.105		
		Sha	ared Domain	Count		12			
		Ave	erage Domain	Risk Score		55			
					Open in	DomainToo	ols Iris	Close	
SSL Hashes	X509 Certificate Fingerprint Hash	Shows includi	a summar ng: Original Shared D SSL Hash Average SSL Hash	y of key dat Value Domain Cou Domain Ris	a points for Int (number sk Score for	the selecte of domains domains as	d SSL Hasl	n d with the <i>r</i> ith the	

		X509 Certificate Fingerprint Hash starttim 2 16182411 1951552631022a56871997bc1d0b074 Filter on X50 2 Filter on X50 195152031022a56871997bc1d0b074 Filter On X50	protocolid sourceip logsourceic qid 255 10 10.3 102 13500075 0 certificate Financial 195152001022a588719e70e7 0 certificate Financial 195152001022a588719e70e7 1 Editor 5 255 183.44 162 13500075	sourceport eve 0 1 0b0070137723934f bc1a0b07c13772393 bc1a0b07c1377239 0	Alter and the second se	de Identitylp 0.0.0.0 0.0.0	dest 912 912 911 911 911 911 911		
		DomainTools SS	L Hash Data			×			
		Field Name	Value						
		Original Value	195152d01022a568719	195152d01022a568719e7bc1d0b07c13f723934f					
		Shared Domain Count	1						
		Average Domain Risk Sc	ore 56						
			Open in Domain	Tools Iri	s C	lose			
Iris Investigation	UrlHost	Opens up a new tab in t	he DomainTools Iris for	further	investig	gation.			
Opener	urlhost	I his action will be avail	able to all entitles previo	busiy ais	cussea.				
	url_host	7B8Q2DBSC3N.weddingrings.com.ph 7B8Q2DBSC3N.alexandria-blig.com	2 195152d01022a568719e7bc1d0b07c13f72	starttime 16182417 16182417	255 255	10.10.3	. 16		
	Url_Host	7B8Q2DBSC3N.weddingrings.com.ph 7B8Q2DBSC3N.五方天雅汽车服务园 7B8Q2DBSC3N.abnmrobok.com	2 195152d01022a568719e7bc1d0b07c13f72 195152d01022a568719e7bc1d0b07c13f72	16182479 16182479 16182479	255 255 255	10.10.3	. 16		
	urlHost	7B8Q2DBSC3N.caiicloud.com 7B8Q2DBSC3N.xn-w39at4kv2g6u	Filter on UrlHost is 78802DBSC3N.caiicloud.cc	16192470 om id.com	255 255	163.44	. 16 . 16		
	URLHOST	7B8Q2DBSC3N.itunes-plus-music. 7B8Q2DBSC3N.weddingrings.com. 7B8Q2DBSC3N.abnmrobnk.com	False Positive /iew in DSM Editor	255 255		163.44 10.10.3	. 16 . 16 . 16		
	URL_HOST	7B8Q2DBSC3N.calicloud.com 7B8Q2DBSC3Nalexandria-blig.com	Plugin options 195152d01022a568719e7bc1d0b07c13f72	1618241	Show Doma Show In Dor	in Data mainTools Iris			
	Url								
	url								
	URL								
	Domain								
1									
	domain								

Destination Host	Name	🕼 tris	Q Inspect: calicloud.com				⊕ 1
Hostname		? HelpØ Settings	Donain Profile Screenshet History	What History Hesting Histo	y SSLProfile		Screensbats
Source Host Name	e	 Search Tags Investigations 	Find ar matrix a tag to add.		kane Phis	+ sa	No screenshot available.
URL Path		A transformation (24/11/2) A transformation (24/11/2) A transformation (24/11/2) A transformation (21/11/2) A transformation (21/11/2)	Deerst	Seale Domain Name, Ir Supportin	Threat frastructure, Age L'hidence.	Profile .	
URL Query String		A Reserve Control (CCC) A Reserve (general RAD)	95 • Pointing	94 R Malware Doma	15 If Span Ortally	14 * Presimity	
Referrer URL		A Second galaxies (10.5372) A Second galaxies (10.5272) A Second galaxies (10.7273) Second galaxies (10.7774) Second galaxies (10.7774) With Class Constraints Second galaxies (10.7774)	Recently Resolved As yiniae.calicload.com open.calicload.com devens.calicload.com gateway.calicload.com			101.89,173.188 104.37,30.39 106.39,30.21 106.39,30.21	
Originating Host		 Rossen Climit A(1); Univer Discontinuous Disco	ervice-googlamyses caliblest.com			106.39.30.18	
Recipient Host		 Mittine Tree 2018 advant Mittine (atvertised) Chariff Tree 26 Adve parts 	Do net show no this again				Civale as housiligation How
Remote Host							
DNS Query							
DNS Domain Nam	ne						
DNS Response							
X509 Certificate Fingerprint Hash							
Due to how QRad handles IPs, all da the IP data type ha action.	ar ta with ave this						

Table: Settings

Field Name	Description
API User	DomainTools API Username
API Key	DomainTools API Key
Enable Proxy	Checkbox for enabling using the Proxy Server and Proxy Port settings
Proxy Server	Server URL for proxy
Proxy Port	Port for proxy
Enable Custom Certificate	Checkbox for enabling using the Custom Certificate setting
Custom Certificate	Path for custom certificate. See App Configuration Steps->Managing API Connectivity->Adding Custom SSL Certificate for more information.
Domain Field	This is for extracting domains from events that are part of Offenses. See Prerequisites->Extract Domains From Offenses for Enrichment for more information.

Prerequisites

DomainTools App Bundle

The latest app is available on <u>IBM App Exchange</u>. The minimum compatible version is QRadar v7.4.1 Patch 2.

DomainTools API Key

You will need a DomainTools Iris Investigate API username and API key to complete the app set up. DomainTools provides access to obtain API credentials by creating an account for the primary point of contact in your organization. If you wish to evaluate the app and need to obtain new API keys, contact us via email at <u>sales@domaintools.com</u>. Account rate limits apply.

Firewall Rule

Ensure you can reach <u>https://api.domaintools.com/</u> from the QRadar server. If required, update firewall rules to allow access to this endpoint for the app to be functional.

If you are on a managed infrastructure and cannot connect to the DomainTools endpoint, please reach out to us so we can help verify any additional IP allow listing activities that may be needed.

Upgrading From Previous Versions

Kindly review the <u>Uninstalling Prior Versions</u> section in this User Guide and the release notes of respective versions to be aware of any breaking changes in your environment. Please contact DomainTools Support at <u>enterprisesupport@domaintools.com</u> for assistance with the app installation.

QRadar Credentials to Install App

A QRadar account with admin access is required to successfully install and configure the app. After installation, user functions should be available with any account.

Extract Domains From Offenses for Enrichment

To ensure that Offenses provide context for triaging, we have created a custom fragment that enriches domain data of events associated with the Offense.

Use the following steps to set up extraction:

- 1. Navigate to Admin \rightarrow DomainTools \rightarrow Configuration.
- 2. In Domain Field, put the name of the property that the event's domain or URL will be.
- 3. If the event needs to add that property, navigate to Admin \rightarrow Data Sources \rightarrow Events \rightarrow DSM Editor.
- 4. Select the Log Source Type that contains the events that need the added property.
- 5. Click the + button to add a new property with the same name as Domain Field in step 2.
- 6. Fill out the necessary Property Configuration

Properties	Event Mappings	Configuration	
lter			
Source IP IP Address			
Source MAC			
Source Port			
Text Custom			İ \
roperty Config xpressions (1) Expression Expression Type	guration Regex		
roperty Config xpressions (1) Expression Expression Type Expression	guration	?(?:www\.)?([^\\$\;V	▼
roperty Config xpressions (1) Expression Expression Type Expression Capture Group	guration	?(?:www\.)?([^\s\;\/	· · · · · · · · · · · · · · · · · · ·
Text Custom roperty Config xpressions (1) Expression Expression Type Expression Capture Group Selectivity	guration	?(?:www\.)?([^\\$\;\/	▼

Once set up, the Offense Summary will automatically display the domain enrichment data. There is no programmatic way to provision these fields during app deployment. For more information on adding custom properties, please refer to this <u>QRadar documentation</u>.

App Installation

Uninstalling Prior Versions

If you are currently running an older version of the DomainTools app, uninstall the older version first and perform a fresh installation. The 1.x version of DomainTools App for IBM QRadar is no longer supported.

For best results, use the QRadar web UI to uninstall any previous versions of the DomainTools App.

Installation Steps

- 1. Obtain the latest version of the DomainTools App from IBM App Exchange.
- 2. Go to Admin \rightarrow System Configuration \rightarrow Extensions Management
- 3. Click Add and select the zip file for the DomainTools App. Select Install immediately and click Add.
- Once installation is complete, restart the QRadar web server by going Admin → Advanced → Restart Web Server



- 5. Log in to one of the search head members and verify the setup and configuration.
 - a. Navigate to $Admin \rightarrow DomainTools \rightarrow Configuration$.



b. Verify that you can access the Settings page.

App Configuration Steps

DomainTools Settings

API User	
demo_user	
API Key	
•••••	
Enable Proxy	
Proxy Server	
Proxy Port	
Enable Proxy Authentication	
Proxy Password	
Enable Custom Certificate Custom Certificate	
Domain Field	
UrlHost	
The name of the property containing URLs or domains to be enriched (e.g. UrlHost). See the DomainTools for QRadar user guide for more information.	
Save Test Connection	
Connection Successful!	

Fig 2: The API Key dashboard including a successful test for the API connectivity between the API key and DomainTools.

Managing API Connectivity

Adding and Testing API Connectivity:

- 1. Navigate to Admin \rightarrow DomainTools \rightarrow Configuration.
- 2. Add the API Credentials the API Username and API Key.
- 3. Click the **Test Connection** button to validate the connection.
- 4. Once validated, click **Save** to save the settings.

Adding an Optional Proxy Configuration:

- 1. Configure proxy configuration in the same API Key section.
- 2. Select Enable Proxy.
- 3. Add the Proxy Server and Proxy Port.
- 4. To enable proxy authentication, Select *Enable Proxy Authentication* and enter the proxy username and password in the provided fields.

Note: Due to a limitation within Python's urllib3 library, "https" URLs are not currently supported when using proxy authentication and will use http instead.

Adding an Optional Custom SSL Certificate:

1. Select Enable Custom SSL Certificate

- 2. Add the path in the *Custom SSL Certificate Path* field. You will need to ssh and add the certificate to the app which can be done by following the below directions.
 - a. Add a copy of your custom certificate to the certs directory in the DomainTools app volume. Example:/store/docker/volumes/qapp-<app-id>/certs/<your-cert.pem>
 - i. One way to find the app-id is to go to DomainTools Settings page and look at the URL. This is unlikely to be the same as the image shown

/console/plugins/1109/app_proxy/settings

DomainTools Settings

- b. It should be added under the same group used by QRadar with read permissions
- c. Update The DomainTools App configuration page with the Docker volume path that maps to the certificate installed in step a: /opt/app-root/store/certs/<your-cert.pem>
- d. Note the different paths used in step a for storing your certificate, and step c for defining the same certificate within the DomainTools app settings. The path in step c will map from our application container to the path in step a of the underlying filesystem.

Key App Functionalities

Right Click Context

Throughout the QRadar App, anywhere one of the designated properties described in the Right Click Actions Table is presented, the user can right click to gain a brief overview of DomainTools data about that entity. This contextual information on Domain, IP, Mailserver IP, Nameserver IP, and SSL Hashes can help a user determine data points of interest to be investigated further within the DomainTools Iris platform. Note that data does not persist between right-click actions, so users should be mindful of their DomainTools API usage.

Associated Domain Count Explanation

When looking at a domain summary, Associated Domain Count is the number of domains associated with the value listed. The associated domain count for a field is only shown when there are less than 500, indicating that there is potentially interesting information available in a "<u>Guided Pivot</u>" within the DomainTools Iris platform.

Average Risk Score Explanation

When looking at IP, Mailserver IP, Nameserver IP, and SSL Hash summaries, the Average Risk Score is the average risk score of domains associated with the entity value being searched. This value only shows if there are 500 or less domains associated.

= 16	3M QRadar														(III)	Ċ	2
Dashboard	Offenses	Log Activity	Network Activity Assets Repo	orta Pisks	Vulnerablities Admin	Pulse Us	e Case Manage	r							Sy	stem Time: 5	044 PM
Search ¥	Quick Searches	Add Fille	r 🕌 Save Criteria 👔 Save Results 🔗 Con	cel 🔸 False Positi-						_							0
	1				DomainTools IP	Data			×								
5										-		4					
					Field Name		Valu	ie .				A					
0 - (5:00 PM	Apr 10	6:00 AM 12:00 PM 6:	00 PM A	Original Value		163	.44.136.225		1	2:00 PM	6:00 PM	Apr 13	6:00 AM	12:00	PM	
					IP Shared Domain Count	t	451										1
logsource_	logsource_	URL	UriHost	X509 Cer	IP Average Domain Risk	Score	π			qid	sourceport	eventcount	magnitude	identityip	destinationi	destinatio	onj
Squid We	WebProxy	7B8Q2DB	7B8Q2DBSC3N.weddingrings.com.ph	2						500075	0	1	4	0.0.0.0	216.23	0	
Squid We	WebProxy	7B8Q2DB	7B8Q2DBSC3N.alexandria-blig.com	195152d01022	Country Code		sg			500075	0	9	2	0.0.0.0	107.15	0	8 I I
Squid We	WebProxy	7B8Q2DB	7B8Q2DBSC3N.itunes-plus-music.com	195152d01022						500075	0	1	2	0.0.0.0	107.15	0	- H
Squid We	WebProxy	788Q2DB	7B8Q2DBSC3N.weddingrings.com.ph	2	ISP		GM	O Internet Pte L	d	500075	0	1	4	0.0.0.0	216.23	0	
Squid We	WebProxy	788Q2DB	7B8Q2DBSC3N.abnmrobnk.com	195152d01022						500075	0	1	2	0.0.0.0	107.15	0	
Squid We	WebProxy	788Q2DB	7B8Q2DBSC3N.calicloud.com	2	ASN		593	49		500075	0	1	2	0.0.0.0	107.15	0	
Squid We	WebProxy	788Q2DB	7B8Q2DBSC3N. alexandria-blig.com	195152d01022						500075	0	6	2	0.0.0.0	107.15	0	
Squid We	WebProxy	788Q2DB	7B8Q2DBSC3N.weddingrings.com.ph	2						500075	0	1	4	0.0.0.0	216.23	0	
Squid We	WebProxy	7B8Q2DB	7B8Q2DBSC3N.五方天稚汽车服务园	195152d01022						500075	0	1	2	0.0.0.0	107.15	0	
Squid We	WebProxy	788Q2DB	7B8Q2DBSC3N.abnmrobnk.com	195152d01022		Ope	n in Doma	inTools Iris	Close	500075	0	1	2	0.0.0.0	107.15	0	
Squid We	WebProxy	7B8Q2DB	7B8Q2DBSC3N.caiicloud.com	2			100 V2 (24,00) 1	and the second statistics		500075	0	1	2	0.0.0.0	107.15	0	
Squid We	WebProxy	788Q2DB	7B8Q2DBSC3N.xnw39at4kv2g6ua6	195152d01022a	568719e7bc1d0b07c13f72	16182479	255	163.44	162	13500075	0	6	2	0.0.0.0	107.15	0	
Squid We	WebProxy	7B8Q2DB	7B8Q2DBSC3N.itunes-plus-music.com	195152d01022a	568719e7bc1d0b07c13f72	16179980	255	···· 163.44	113	13500075	0	1	2	0.0.0.0	107.15	0	

Fig 3: DomainTools summary panel for an IP

Offense Summary Custom Fragment

The Offense Summary Custom Fragment lists all domains extracted from events related to the Offense. When clicking on a domain, a table with all that domain's data including risk scores, infrastructure, and contacts is displayed. This is limited to the first 100 domains extracted.

Associated Domain Count Explanation

Associated Domain Count is the number of domains associated with the value listed. Where the associated domain count is less than 500, the number will display in blue to indicate that there is a potentially valuable "guided pivot" available in Iris. Clicking on this count will open an investigation in the DomainTools Iris platform.

Registrant Conta	ct	
Name	REDACTED FOR PRIVACY	74280304
Organization		0
Street	REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY	17389987
City	REDACTED FOR PRIVACY	72582142
State	Saare	335
Postal	REDACTED FOR PRIVACY	73680047
Country	ee	303653
Phone		0
Technical Ocean		

Fig 4: Example domain with a "guided pivot" available.

Quickly Open Up Investigations in DomainTools Iris

Throughout QRadar with the DomainTools App installed a user will be able to quickly open an investigation in the DomainTools Iris platform and continue digging for information. See the <u>Iris User Guide</u> for more information.

n Log Activity Network Activity Asse	ts Reports Risks Winerabilities A	dmin Pulse Use Case Manager	
All Offenses > Offense 73 (Summa	ry)		
DomainTools Domain Summary			
Domain O		Risk Score	Greate Date
4929552 buzz 🔀		88	2020-06-17
eucidao xvz 🗹		98	2020-11-09
fatihourme.click		99	2021-03-18
iashuianterbaik.com P		67	2020-12-09
omicowyz pw 🕑		77	2018-11-28
secondaryspecificationtowitnesstoda	vinto 🛃	100	2020-08-06
ukdenb.com 🗹		100	2021-01-18
wizwauco.work 🕑		100	2020-11-13
yongthwude.xyz 🕑		100	2020-11-10
in the second se			
DomainTools Domain Risk Informa	tion for ojmlocwwz.pw		
Field	Value		Associated Domain Count
Overall Hisk Score	11		
Proximity	17		
Evidence			
Maiware	0		
Phisning	6		
spam	0		a
Create Date	2018-11-28		344075
DomainTools Domain Information	for ojmlccwwz.pw		
Field	Value		Associated Domain Count
Create Date	2018-11-28		344075
Expiration Date	2021-11-28		865249
Status	True		NUMETO .
Admin Contact	1106		
Name			0
Oreanization			0
Chiganization			0
City			0
State			0
Dested			0
Country			0
Rhead			0
Phone Billing Contact			0
Name			0
Oroanization			0
Streat			0
City			0
State			0
Portal			0
Country			0
Disea			0
Registrant Contact			·
Name			0
Organization			0
Street			0
City			0
State			0
Postal			0
Country			0
Phone			0
Technical Contact			U
Nama	-		10
Ornanization			0
Streat			0
Cau			0
Gtate			0
Doetal			0
Country			0
Country			0
[FIIONO			U
DomainTools Domain Hosting Info	rmation for ojmiccwwz.pw		Lauranaw
IP Information	Value		Associated Domain Count
17 Information			
10.446999	1717.17.17		40000
ID ACM	714		40,69
IP ASN	714		6/400
IP Country	US Apple log		359056847
117 101	Apple Inc.		64476
E 204 42 18			
5.204.42.18	E 001 10 10		
5.204.42.18 IP Address	5.204.42.18		33
5.204,42.18 IP Address IP ASN	5.204.42.18 213155		33 72

Fig 5: Example of DomainTools Domain Data in an Offense Summary

Troubleshooting & Known Issues

DomainTools will continue to monitor the feasibility of fixing these known issues and make adjustments as needed to accommodate various QRadar deployment scenarios/environments.

To see DomainTools app logs, please follow instructions from <u>the official QRadar documentation</u>. Of specific note are app.log, dtapi.log, and startup.log.

For issues we are able to reproduce, we have included the Bug ID for your convenience. We will address these Bugs in subsequent product releases.

Issue Tracker

The list below contains all known issues and each contains a workaround or resolution step as appropriate

ID	Issue Overview						
<u>1</u>	showRtClickDomainTools is not defined						
<u>2</u>	Right-click "Show in DomainTools Iris" triggers a popup blocker in Firefox						

Issue Details

showRtClickDomainTools is not defined

When trying to on demand enrich an entity through a right click action:



Close

Fig 6: Screenshot of error messages thrown for the base search configuration fail issue.

Environments & Scenarios Observed

In environments where the DomainTools App is newly installed.

Reasoning

QRadar caches lots of the resources it loads so sometimes a newly installed app's resources don't get loaded.

Workaround

Restart Web Server from the Admin panel and <u>hard refresh</u> the browser to bypass the cached page content.

Right-click "Show in DomainTools Iris" triggers a popup blocker in Firefox

Users who right-click and select "Show in DomainTools Iris" might trigger the popup blocker in Firefox:

≡ 18	BM QRadar								Allow pop Edit Pop- Don't sho	ups for up Block w this m	er Preference essage when	es pop-l	ups ar	e blocke	۶d
Dashboard	Offenses Quick Searches	Log Activity	Network Activity Assets Save Criteria 🔋 Save Results 🔓	Reports Admin	Pulse Use Case Manager Pre-V Rules V Actions V 🔆 Event pass IDs	alidatio	n		Show 'ht	ps://rese ps://rese	arch.domaint arch.domaint	tools.c	om/iri om/iri	s/search s/search	v/?q=T0 v/?q=T0
3:15:00	PM 3:15:15	PM 3:15:30 PM 3	:15:45 PM 3:16:00 PM 3:16	:15 PM 3:16:30 PM	3:16:45 PM 3:17:00 PM 3:17:15 PM Upd (He	3:17: ste De se Char	80 PM 3:17:45 PM 3:18 tails ts)	00 PM 3	:18:15 PM 3:18:30 PM	A 3:18:4	5 PM 3:19:00) PM	3:19:1	PM 3:	19:30 P
	090000	1181	100000000000000000000000000000000000000		WERE Contillants Figure and the sh										
logsou log	goodici	OTTE	UriHost		ASU9 Certificate Fingerprint Hash		starttime	protoc	sourceip	logsou	qid	SOL	even	magn	
logsou log Squid Wi	ebPro TDE	UWMGUI4.AVJn	UriHost TDEUWMCUI4.AVJnMa	Filter on Utilideal in TO	SUMMCUIA AV InMeXC fairease work	_	starttime 1619104506283	protoc 255	sourcelp 10/10/85/219	logsol 112	qid 13500075	SOL	even	magn 3	0.0./
logsou log Squid We Squid We	ebPro TDE	UWMGUI4.AVJn	UriHost TDEUWMGUI4.AWInMa CZG5AR8K67.tVHYctYY	Filter on UrlHost is TD	EUWMCUI4.AVJnMaYG.fnijgana.work	-	starttime 1619104506283 1619104506283	protoc 255 255	sourcelp 10.10.85.219 10.10.127.255	logsol 112 112	qid 13500075 13500075	sol 0	even E	magn 4	0.0.0
ogsou log Squid We Squid We Squid We	ebPro TDE ebPro CZG ebPro 25Y	UWMGUI4.AVJn 5AR8K67.tVHYcl TVMIX3J.HUJzCy	UriHost TDEUWMGUI4.AVJnMa CZG5AR8K67.tVHYdtYY 25YTVMIX3J.HUJzCyrG	Filter on UrlHost is TD Filter on UrlHost is no	EUWMCUI4.AVJnMaYG.fnijgana.work	1	starttime 1619104506283 1619104506283 1619104506283	protoc 255 255 255	sourcelp 10.10.85.219 10.10.127.255 10.10.200.220	logsol 112 112 112	qid 13500075 13500075 13500075	SOL 0 0	even 1 1	magn 4 4	0.0.
ogsou log Squid Wi Squid Wi Squid Wi Squid Wi	ebPro TDE ebPro CZG ebPro 25Y ebPro YRD	UWMGUI4 AVJn 5AR8K67 (VHYcl TVMIX3J.HUJzCy (27VUSF.yOLaITr	UriHost TDEUWMGUI4.AVJnMa CZG5AR8K67.IVHYcIYY 25YTVMIX3J.HUJzCyrG YRIX27VUSF.yOLaITri.cl	Filter on UrlHost is TD Filter on UrlHost is no False Positive	EUWMCUI4.AVJnMaYG.fnijgana.work		starttime 1619104506283 1619104506283 1619104506283 1619104506283	protoc 255 255 255 255	sourceip 10.10.85.219 10.10.127.255 10.10.200.220 10.10.76.34	logsol 112 112 112 112 112	qid 18500075 13500075 13500075 13500075	SOL 0 0 0	even 1 1 1	magn 4 4 4	0.0.0
Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi	ebPro TDE ebPro CZG ebPro 25Y ebPro YRD ebPro 7JT0	UWMGUH AVJn ISAR8K67.tVHYcl TVMIX3J.HUJzCy K27VUSF.yOLaITr 3IINUVG.OEhFLc	UriHost TDEUWMQUK/AVIMMA CZG5AR8K67.IVHYctYY 25YTVMIX3J.HUJzCyrG YRIX27VUSF.yOLaITI.cl 7JTGIINUVG.OEhFLcoj	Filter on UrlHost is TD Filter on UrlHost is no False Positive	X509 Certificate Fingerprint Hash EUWMCUI4.AVJnMaYG.fnijgana.work TDEUWMCUI4.AVJnMaYG.fnijgana.work		starttime 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283	protoc 255 255 255 255 255	sourcelp 10.10.65.219 10.10.127.255 10.10.200.220 10.10.76.34 10.10.228.194	logson 112 112 112 112 112 112	qid 18500075 13500075 13500075 13500075 13500075	SOL 0 0 0 0	even 1 1 1 1	magn 4 4 4 4	0.0) 0.0) 0.0) 0.0)
Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi	ebPro TDE ebPro CZG ebPro 25Y ebPro YRD ebPro 7JTC ebPro UHC	UWMCUHAAVJn 55AR8K67.IVHYdl TVMIX3J.HUJzCy K27VUSF.yOLaITr 3IINUVG.OEhFLe DHF69GYS.gHMo	UriHost TDEUWMCUKAVUMMA CZG5AR8K67.tVHYKYY 25YTVMIX3J.HUJzCyrG YRIX27VUSF;yOLaITI.cl 7JTGIINUVG.OEhFLooj. UHOHF89GYS.gHMoGF	Filter on UrlHost is TD Filter on UrlHost is no False Positive View in DSM Editor	XSVV Certificate Fingerprint Hash EUWMCUI4.AVJnMaYG.fnijgana.work TDEUWMCUI4.AVJnMaYG.fnijgana.work		starttime 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283	protoc 255 255 255 255 255 255 255	sourcelp 10.10.35.219 10.10.127.255 10.10.200.220 10.10.76.34 10.10.228.194 10.10.34.35	logsol 112 112 112 112 112 112 112 112	qid 13500075 13500075 13500075 13500075 13500075 13500075	SOL 0 0 0 0 0	even 1 1 1 1 1 1 1	magn 4 4 4 4 4 4 4 4	0.0) 0.0) 0.0) 0.0) 0.0)
ogsou log Squid We Squid We Squid We Squid We Squid We Squid We	ebPro TDE ebPro CZG ebPro 25Y ebPro YRD ebPro YRD ebPro UHC ebPro PTK	UWMCUHAVJn 55AR8K67.IVHYcl 1VMIX3J.HUJZCY K27VUSF.yOLaITr 3IINUVG.OEhFLe DHF69GYS.gHMo 4Y2MYDQ.xwiPo	UriHost TDEUW/MCU/LA/VIMMS CZGSAR8K67.IVHYqtY 25YTVMIX3J.HUJzCyrG YRIX27VUSF.yOLaITI.o YTIGIINUVG.OEhFLcoj. UHOHF69GYS.gHMoGR PTK4Y2MYDD.xwiPoctH	Filter on UrlHost is TD Filter on UrlHost is not False Positive View in DSM Editor Plugin options	Sour Certificate Fingerprint Hash	•	starttime 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 1619004506283	protoc 255 255 255 255 255 255 255	sourceip 10.10.85.219 10.10.127.285 10.10.200.220 10.10.76.34 10.10.228.194 10.10.34.35 10.10.56.172	logson 112 112 112 112 112 112 112 112 112	qid 13500075 13500075 13500075 13500075 13500075 13500075 13500075	SOL 0 0 0 0 0 0 0 0	even 1 1 1 1 1 1 1	magr 4 4 4 4 4 4 4 4 4	0.01
logsou log Squid We Squid We Squid We Squid We Squid We Squid We Squid We Squid We	ebPro TDE ebPro CZG ebPro 25Y ebPro YRD ebPro YRD ebPro UHC ebPro PTK ebPro VW0	UWMCUI4 AVJn ISARBKG7 (VHYcl TVMIX3J.HUJzCY K27VUSF.yOLalTr SIINUVG.OEhFLe DHF69GYS.gHMo 4Y2MYDO.xwlPo D02ULR4R.qJAKB	UriHost TDEUWMCUIAAVInMC CZGSARK67.tVHYdtY 25YTVMIX3J.HUJzCyrG YRIX27VUSF.yOLaITILd YTGINUVG.OEhELcoj: UHOHF69GYS.gHMoGR PTK4Y2MYDQ.xwiPoetH WWO2ULR4R.qJAK86r.tames	Filter on UrlHost is TD Filter on UrlHost is not False Positive View in DSM Editor Plugin options quesus.comme Two	Sour Gertineate Fingerprint Hash EUWMCUI4.AVJnMaYG.fnijgana.work I TDEUWMCUI4.AVJnMaYG.fnijgana.work	•	starttime 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 Show Domain Data	protoc 255 255 255 255 255 255 255	sourcelp 10.10.35:219 10.10.127.255 10.10.200.220 10.10.76.34 10.10.228.194 10.10.34.35 10.10.56.172 10.10.26.172	logson 112 112 112 112 112 112 112 112 112 11	qid 13500075 13500075 13500075 13500075 13500075 13500075 13500075	SOL 0 0 0 0 0 0 0 0 0 0	even 1 1 1 1 1 1 1 1 1 1	magr 4 4 4 4 4 4 4 4 4 4 4	0.0) 0.0) 0.0) 0.0) 0.0) 0.0) 0.0)
Iogsou Iog Squid Wr Squid Wr Squid Wr Squid Wr Squid Wr Squid Wr Squid Wr	ebPro VWC ebPro VRD ebPro VRD ebPro VHC ebPro VWC ebPro VWC ebPro QMY	UWMGUI4 AVJn ISAR8K67 (VHYcl TVMIX3J.HUJzCy (27VUSF.yOLaITr 3IINUVG.OEhFLe OHF69GYS.gHMo 4Y2MYDQ.xwIPo D02ULR4R.qjAKB YOIDQGSE.WUF	UPHIOSE UPHIOSE AVAIMAN CZGSAR8K67.IVHYdYY 25YTVMIX3J.HUJzCyrG YTIIX27VUSFyOLaTTLd 7.JTGIINUVG.OEhELooj UHCHF896295.ghMoGR PTK4Y2MYDQ.xwiPocH WWOQ2ULR4H.qJAKBorJamer GMYQIDQ5E.WUFudEKm.p	Filter on UrlHost is TD Filter on UrlHost is no False Positive View in DSM Editor Plugin options quesusa.comme vex aptrayec.sxyz N/A	Sou Certificate Fingerprint Hash	•	starttime 1619104506283 1619104506283 1619104506283 16	255 255 255 255 255 255 255 255	sourcelp 10.10.85.219 10.10.127.255 10.10.200.220 10.10.76.34 10.10.228.194 10.10.24.35 10.10.56.172 10.10.217.134 10.10.216.85	logson 112 112 112 112 112 112 112 112 112 11	qid 13500075 13500075 13500075 13500075 13500075 13500075 13500075 13500075	SOL 0 0 0 0 0 0 0 0 0 0 0 0	even 1 1 1 1 1 1 1 1 1 1 1 1	magr 4 4 4 4 4 4 4 4 4 4 4 4 4	0.01
logsou log Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi Squid Wi	obPro TDE obPro CZG obPro 25Y obPro YRD obPro YRD obPro UHC obPro PTK obPro QMY obPro ZIK6	UMACUA-AVJn ISAR8K67.1VHYcl IZAR8K67.1VHYcl IVMIX3J.HUJzCY (27VUSF.yOLaITr INF89GYS.gHMo HF89GYS.gHMo HF89GYS.gHMo O20LLR4R.qJAKB D20LLR4R.qJAKB ID1KZUY.InnAKO	UHHost TDEUWIKCIUKAVIMM CZGAARBKG7.WHYTYY 2SYTWIKX3.HUJ2CyrG YTR27VUS7V0.LITH.cl YTCGINUVG.0EhFLogi, UHOHFR9QYS.gHMGGF PTK4Y2NVD2.wilPocH WW00ZULR4R.qJXB0c7.zmm QMY0IDQGSE.WUPudEKm.g ZIKBD1KZUYINAKQT7.dber ZIKBD1KZUYINAKQT7.dber	Filter on UrlHost is TD Filter on UrlHost is not False Positive View in DSM Editor Plugin options quesuscomme reve poptrzeycs.xyz N/A saps.com N/A	Sour Certificate Fingerprint Hash EUWMCUI4.AVJnMaYG.fnijgana.work TDEUWMCUI4.AVJnMaYG.fnijgana.work	•	starttime 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 1619104506283 Show Domain Data Show In DomainTock 1619104506283	255 255 255 255 255 255 255 255 255	sourcelp 10:10.85:219 10:10.127.255 10:10.200.220 10:10.76.34 10:10.228.194 10:10.34.35 10:10.56.172 10:10.217.134 10:10.216.85 10:10.156.156	logson 112 112 112 112 112 112 112 112 112 11	qid 1350075 1350075 1350075 1350075 1350075 1350075 1350075 1350075 1350075	SOL 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	even 1 1 1 1 1 1 1 1 1 1 1 1 1	magn 4 4 4 4 4 4 4 4 4 4 4 4 4 4	0.0) 0.0) 0.0) 0.0) 0.0) 0.0) 0.0) 0.0)

Fig 7: Screenshot of the popup block and workaround for Firefox users

Environments & Scenarios Observed

Observed in Firefox v87. The issue is likely to be present in other versions of Firefox.

Reasoning

Firefox default behavior is to detect and block popups.

Workaround

Allow the popup in Firefox. Further information on Firefox popup settings can be found on Mozilla's support page.