June 2021 Version 2.0.0

DomainTools App for IBM QRadar User Guide

DOMAINTOOLS®

Overview 3

What's New in 2.0.0 4

- 2.0.0 Release Notes 4

Deployment Guide 5

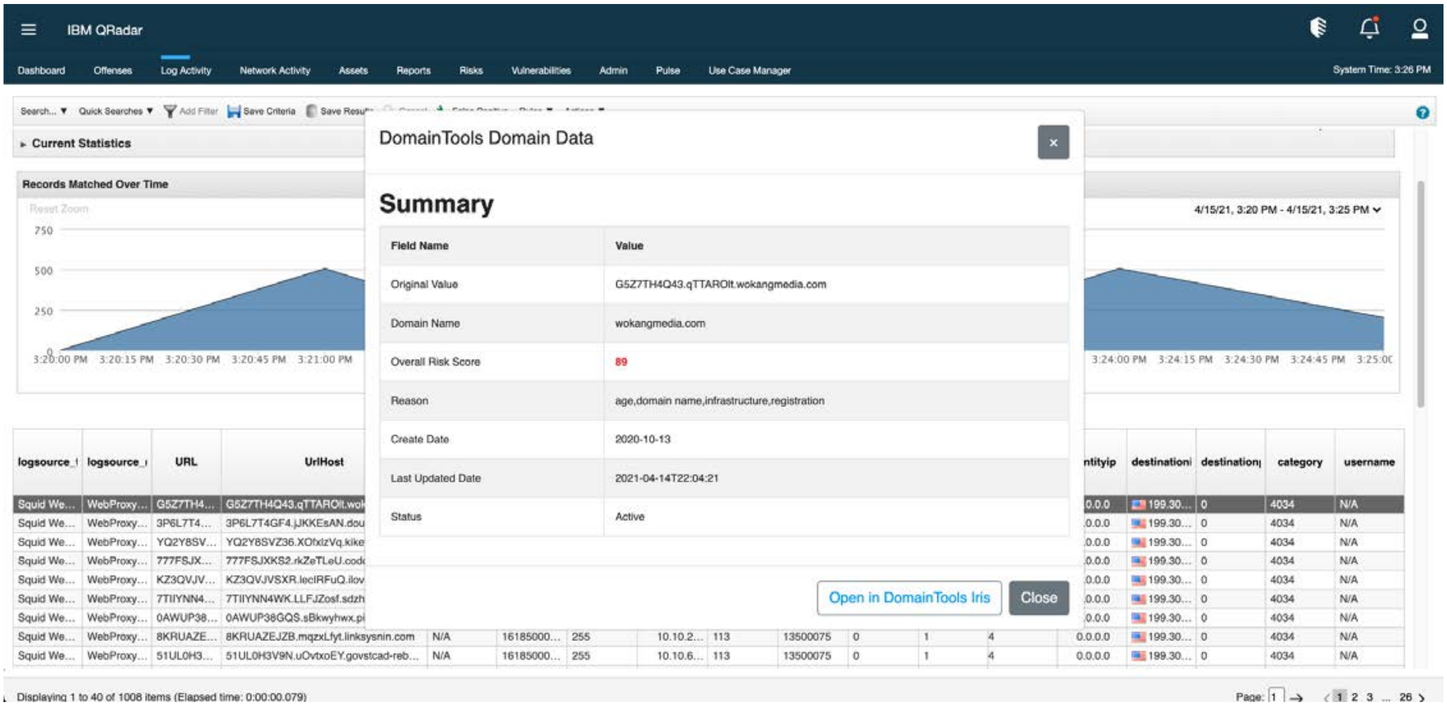
- App Components 5
  - Table: Right Click Actions 5
  - Table: Settings 11
- Prerequisites 12
  - DomainTools App Bundle 12
  - DomainTools API Key 12
    - Firewall Rule 12
  - QRadar Credentials to Install App 12
  - Extract Domains From Offenses for Enrichment 12
- App Installation 14
  - Uninstalling 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



DomainTools Domain Data

Summary

Field Name	Value
Original Value	G5Z7TH4Q43.qTTAROlt.wokangmedia.com
Domain Name	wokangmedia.com
Overall Risk Score	89
Reason	age,domain name,infrastructure,registration
Create Date	2020-10-13
Last Updated Date	2021-04-14T22:04:21
Status	Active

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

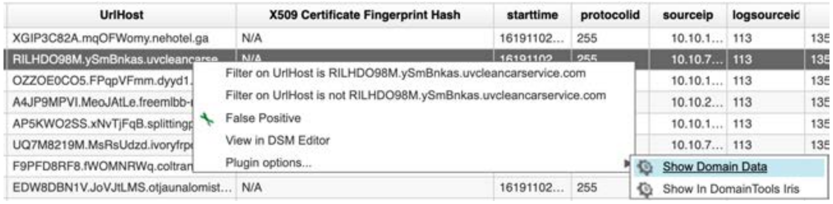
Deployment Guide

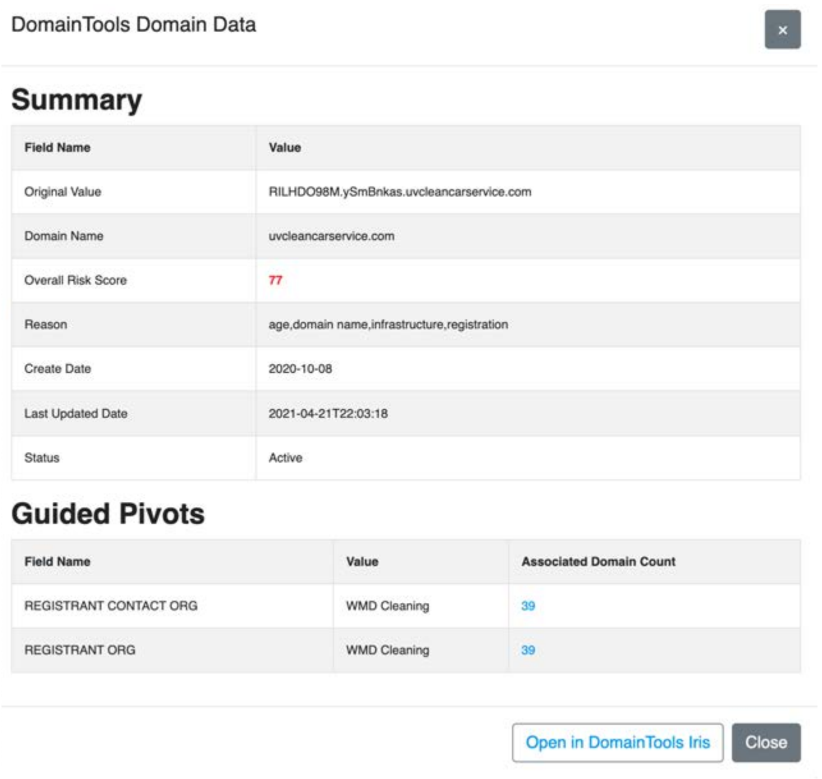
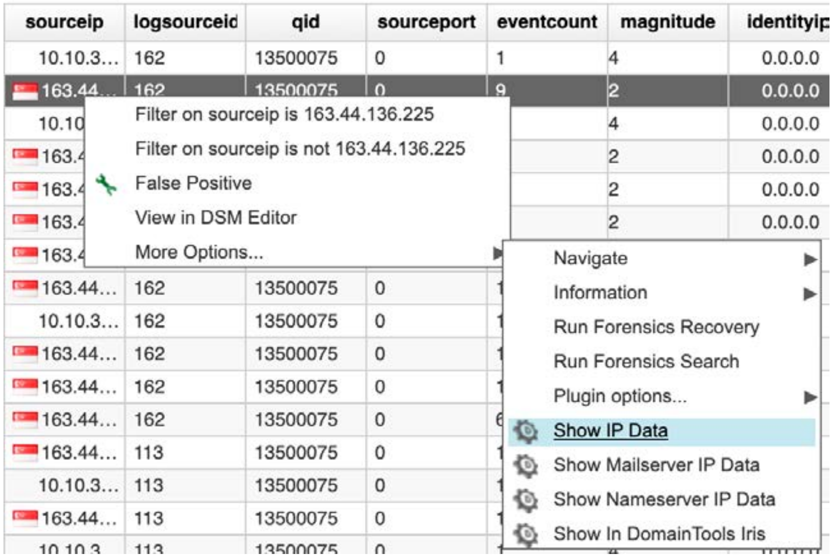
App Components

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: ● Original Value ● Domain Name ● Overall Risk Score ● Reason ● Create Date ● Last Updated Date ● Status ● Guided Pivots that are under the 500 count threshold  UrlHost / X509 Certificate Fingerprint Hash / starttime / protocolid / sourceip / logsourceic XGIP3C82A.mqOFWomy.nehotel.ga / N/A / 16191102... / 255 / 10.10.1... / 113 / 135 RILHDO98M.ySmBnkas.uvcleancarse / N/A / 16191102 / 255 / 10.10.7... / 113 / 135 OZZOE0CO5.FPqpVFmm.dyyd1. / 10.10.1... / 113 / 135 A4JP9MPVI.MeoJAtLe.freemlbb-(/ 10.10.2... / 113 / 135 AP5KWO2SS.xNvTjFqB.splittingp / 10.10.1... / 113 / 135 UQ7M8219M.MsRsUdzd.ivoryfrp / 10.10.7... / 113 / 135 F9PFD8RF8.fWOMNRWq.coltran EDW8DBN1V.JoVJtLMS.otjaunalomist... / N/A / 16191102... / 255 Filter on UrlHost is RILHDO98M.ySmBnkas.uvcleancarservice.com Filter on UrlHost is not RILHDO98M.ySmBnkas.uvcleancarservice.com False Positive View in DSM Editor Plugin options... Show Domain Data Show In DomainTools Iris
	urlhost	
	url_host	
	Url_Host	
	urlHost	
	URLHOST	
	URL_HOST	
	Url	
	url	
	URL	
	Domain	
	domain	
	DOMAIN	
	Destination Host Name	
	Hostname	
	Source Host Name	
	URL Path	
	URL Query String	

	Referrer URL Originating Host Recipient Host Remote Host DNS Query DNS Domain Name DNS Response	
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 the selected IP including: ● Original Value ● Shared Domain Count (Number of domains associated with the IP) ● Average Domain Risk Score for domains associated with the IP ● Country Code ● ISP ● ASN 

DomainTools Domain Data

×

Summary

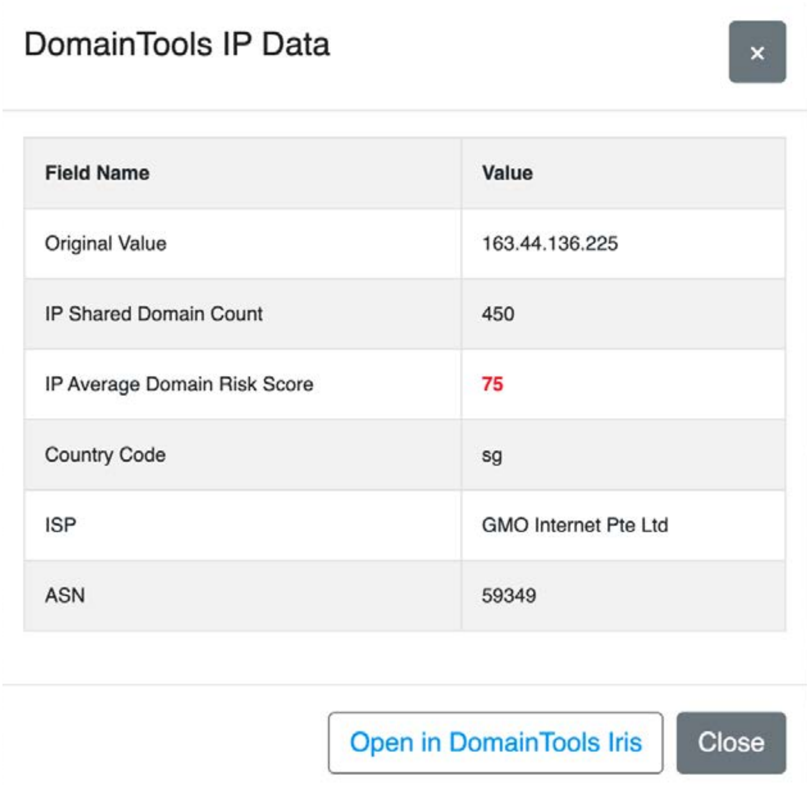
Field Name	Value
Original Value	RILHDO98M.ySmBnkas.uvcleancarservice.com
Domain Name	uvcleancarservice.com
Overall Risk Score	77
Reason	age,domain name,infrastructure,registration
Create Date	2020-10-08
Last Updated Date	2021-04-21T22:03:18
Status	Active

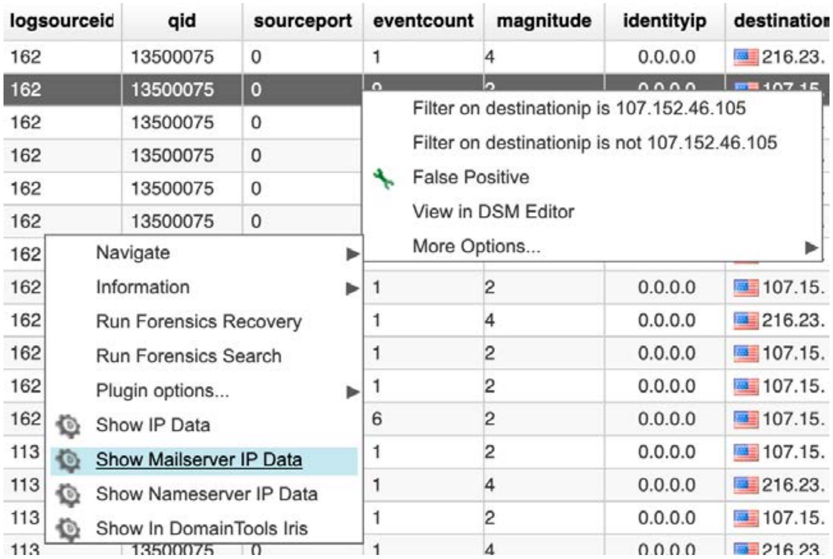
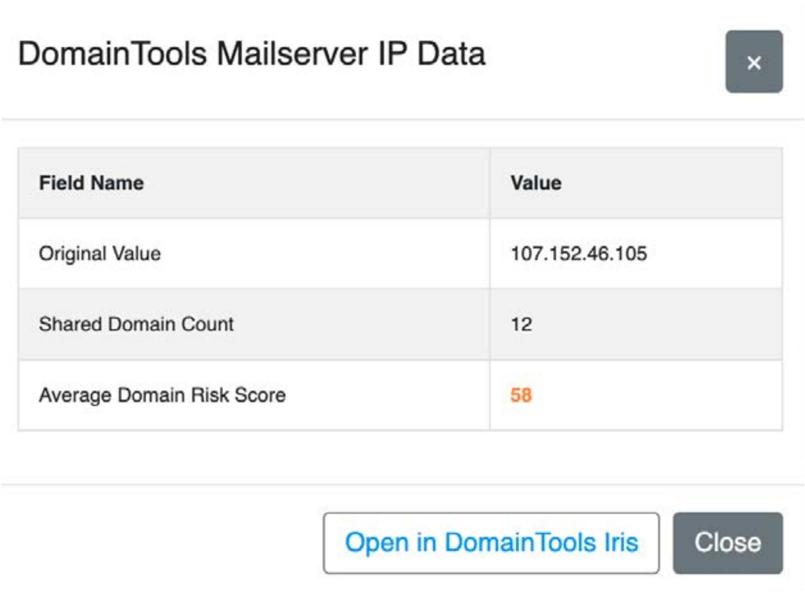
Guided Pivots

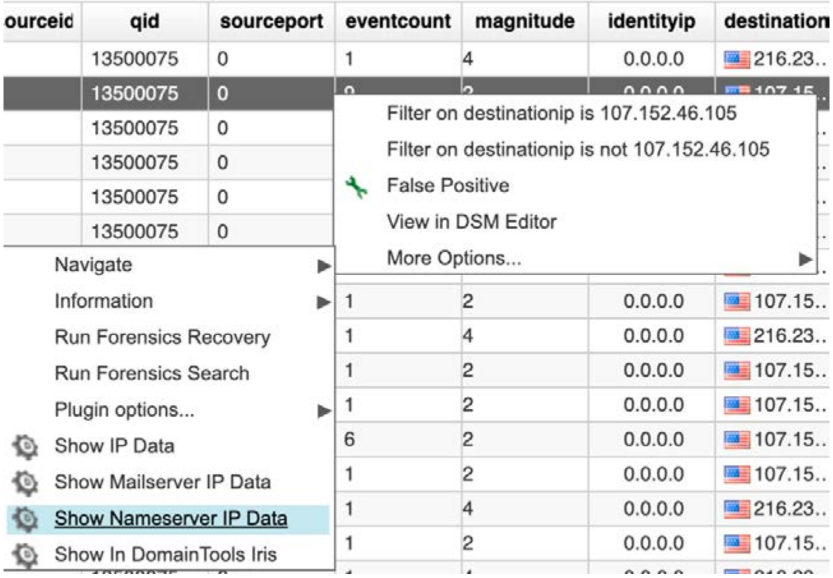
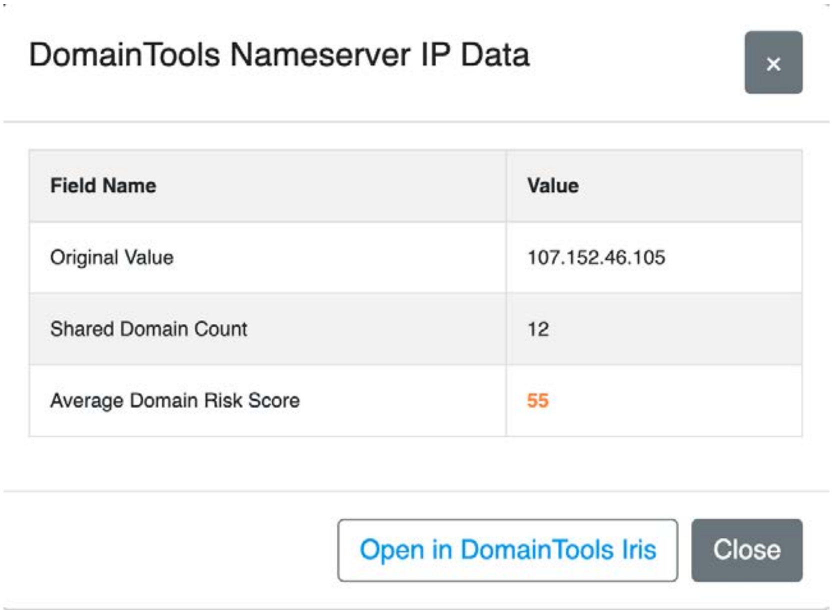
Field Name	Value	Associated Domain Count
REGISTRANT CONTACT ORG	WMD Cleaning	39
REGISTRANT ORG	WMD Cleaning	39

Open in DomainTools Iris Close

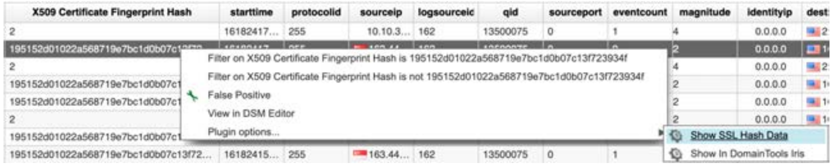
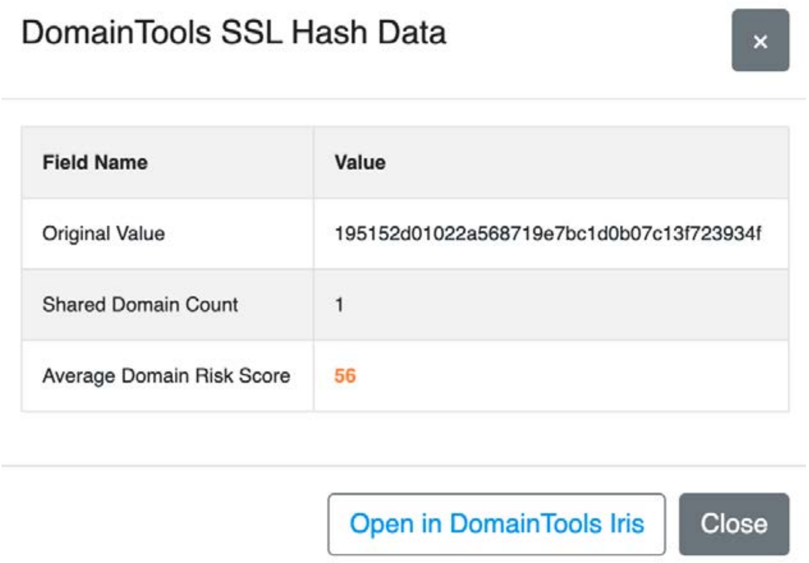
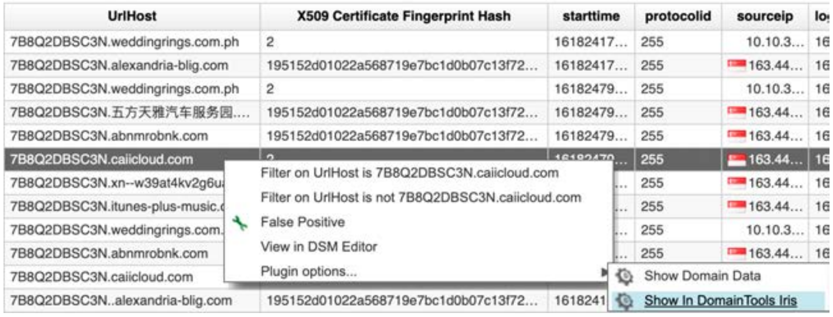
sourceip	logsourceid	qid	sourceport	eventcount	magnitude	identityip
10.10.3…	162	13500075	0	1	4	0.0.0.0
163.44…	162	13500075	0	9	2	0.0.0.0
10.10					4	0.0.0.0
163.4					2	0.0.0.0
163.4					2	0.0.0.0
163.4					2	0.0.0.0
163.4						
163.44…	162	13500075	0	1		
10.10.3…	162	13500075	0	1		
163.44…	162	13500075	0	1		
163.44…	162	13500075	0	1		
163.44…	162	13500075	0	6		
163.44…	113	13500075	0	1		
10.10.3…	113	13500075	0	1		
163.44…	113	13500075	0	1		
10.10.3	113	13500075	0	1	4	

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

		 logsourceid qid sourceport eventcount magnitude identityip destination 162 13500075 0 1 4 0.0.0.0 216.23. 162 13500075 0 162 13500075 0 162 13500075 0 162 13500075 0 162 13500075 0 162 162 1 2 0.0.0.0 107.15. 162 1 4 0.0.0.0 216.23. 162 1 2 0.0.0.0 107.15. 162 1 2 0.0.0.0 107.15. 162 6 2 0.0.0.0 107.15. 113 1 2 0.0.0.0 107.15. 113 1 4 0.0.0.0 216.23. 113 1 2 0.0.0.0 107.15. 113 13500075 0 1 4 0.0.0.0 216.23 Filter on destinationip is 107.152.46.105 Filter on destinationip is not 107.152.46.105 False Positive View in DSM Editor More Options... Navigate Information Run Forensics Recovery Run Forensics Search Plugin options... Show IP Data Show Mailserver IP Data Show Nameserver IP Data Show In DomainTools Iris  DomainTools Mailserver IP Data × Field Name: Value Original Value: 107.152.46.105 Shared Domain Count: 12 Average Domain Risk Score: 58 Open in DomainTools Iris · Close
Nameserver 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 the selected Nameserver IP including: ● Original Value ● Shared Domain Count (number of domains associated with the Nameserver IP) ● Average Domain Risk Score for domains associated with the Nameserver IP

<table>
<tr><td></td><td></td><td>

<table>
<tr><th>ourceid</th><th>qid</th><th>sourceport</th><th>eventcount</th><th>magnitude</th><th>identityip</th><th>destination</th></tr>
<tr><td></td><td>13500075</td><td>0</td><td>1</td><td>4</td><td>0.0.0.0</td><td>216.23..</td></tr>
<tr><td></td><td>13500075</td><td>0</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>13500075</td><td>0</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>13500075</td><td>0</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>13500075</td><td>0</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>13500075</td><td>0</td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>2</td><td>0.0.0.0</td><td>107.15..</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>4</td><td>0.0.0.0</td><td>216.23..</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>2</td><td>0.0.0.0</td><td>107.15..</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>2</td><td>0.0.0.0</td><td>107.15..</td></tr>
<tr><td></td><td></td><td></td><td>6</td><td>2</td><td>0.0.0.0</td><td>107.15..</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>2</td><td>0.0.0.0</td><td>107.15..</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>4</td><td>0.0.0.0</td><td>216.23..</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>2</td><td>0.0.0.0</td><td>107.15..</td></tr>
</table>
Filter on destinationip is 107.152.46.105
Filter on destinationip is not 107.152.46.105
False Positive
View in DSM Editor
More Options...
Navigate
Information
Run Forensics Recovery
Run Forensics Search
Plugin options...
Show IP Data
Show Mailserver IP Data
Show Nameserver IP Data
Show In DomainTools Iris

DomainTools Nameserver IP Data
<table>
<tr><th>Field Name</th><th>Value</th></tr>
<tr><td>Original Value</td><td>107.152.46.105</td></tr>
<tr><td>Shared Domain Count</td><td>12</td></tr>
<tr><td>Average Domain Risk Score</td><td>55</td></tr>
</table>

</td></tr>
<tr><td><b>SSL Hashes</b></td><td>X509 Certificate Fingerprint Hash</td><td>Shows a summary of key data points for the selected SSL Hash including:
● Original Value
● Shared Domain Count (number of domains associated with the SSL Hash)
● Average Domain Risk Score for domains associated with the SSL Hash</td></tr>
</table>

		 
Iris Investigation Opener	UrlHost	Opens up a new tab in the DomainTools Iris for further investigation. This action will be available to all entities previously discussed. 
	urlhost	
	url_host	
	Url_Host	
	urlHost	
	URLHOST	
	URL_HOST	
	Url	
	url	
	URL	
	Domain	
	domain	
	DOMAIN	

X509 Certificate Fingerprint Hash	starttime	protocolid	sourceip	logsourceic	qid	sourceport	eventcount	magnitude	identityip	dest:
2	16182417...	255	10.10.3...	162	13500075	0	1	4	0.0.0.0	2
195152d01022a568719e7bc1d0b07c1								2	0.0.0.0	1
2								4	0.0.0.0	2
195152d01022a568719e7bc1d0b07c1								2	0.0.0.0	1
195152d01022a568719e7bc1d0b07c1								2	0.0.0.0	1
2								2	0.0.0.0	1
195152d01022a568719e7bc1d0b07c1										
195152d01022a568719e7bc1d0b07c13f72...	16182415...	255	163.44...	162	13500075	0	1			

Filter on X509 Certificate Fingerprint Hash is 195152d01022a568719e7bc1d0b07c13f723934f
Filter on X509 Certificate Fingerprint Hash is not 195152d01022a568719e7bc1d0b07c13f723934f
False Positive
View in DSM Editor
Plugin options...

Show SSL Hash Data
Show In DomainTools Iris

DomainTools SSL Hash Data ×

Field Name	Value
Original Value	195152d01022a568719e7bc1d0b07c13f723934f
Shared Domain Count	1
Average Domain Risk Score	56

Open in DomainTools Iris | Close

UrlHost	X509 Certificate Fingerprint Hash	starttime	protocolid	sourceip	lo
7B8Q2DBSC3N.weddingrings.com.ph	2	16182417...	255	10.10.3...	16
7B8Q2DBSC3N.alexandria-blig.com	195152d01022a568719e7bc1d0b07c13f72...	16182417...	255	163.44...	16
7B8Q2DBSC3N.weddingrings.com.ph	2	16182479...	255	10.10.3...	16
7B8Q2DBSC3N.五方天雅汽车服务園....	195152d01022a568719e7bc1d0b07c13f72...	16182479...	255	163.44...	16
7B8Q2DBSC3N.abnmrobnk.com	195152d01022a568719e7bc1d0b07c13f72...	16182479...	255	163.44...	16
7B8Q2DBSC3N.caiicloud.com	2		255	163.44...	16
7B8Q2DBSC3N.xn--w39at4kv2g6u		...	255	163.44...	16
7B8Q2DBSC3N.itunes-plus-music.c		...	255	163.44...	16
7B8Q2DBSC3N.weddingrings.com.		...	255	10.10.3...	16
7B8Q2DBSC3N.abnmrobnk.com		...	255	163.44...	16
7B8Q2DBSC3N.caiicloud.com					
7B8Q2DBSC3N..alexandria-blig.com	195152d01022a568719e7bc1d0b07c13f72...	1618241			

Filter on UrlHost is 7B8Q2DBSC3N.caiicloud.com
Filter on UrlHost is not 7B8Q2DBSC3N.caiicloud.com
False Positive
View in DSM Editor
Plugin options...

Show Domain Data
Show In DomainTools Iris

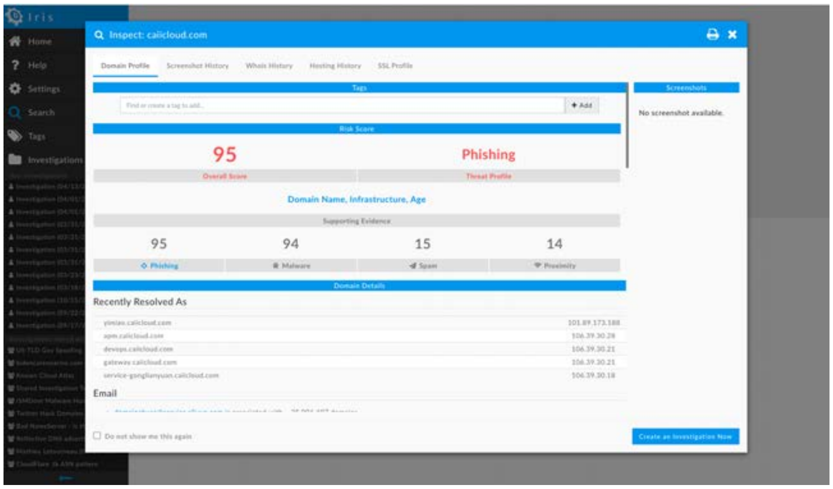
	Destination Host Name	
	Hostname	
	Source Host Name	
	URL Path	
	URL Query String	
	Referrer URL	
	Originating Host	
	Recipient Host	
	Remote Host	
	DNS Query	
	DNS Domain Name	
	DNS Response	
	X509 Certificate Fingerprint Hash	
	Due to how QRadar handles IPs, all data with the IP data type have this action.	

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 IBM App Exchange. 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 sales@domaintools.com. Account rate limits apply.

Firewall Rule

Ensure you can reach https://api.domaintools.com/ 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 *Uninstalling Prior Versions* 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 enterprisesupport@domaintools.com for assistance with the app installation.

QRadar Credentials to Install App

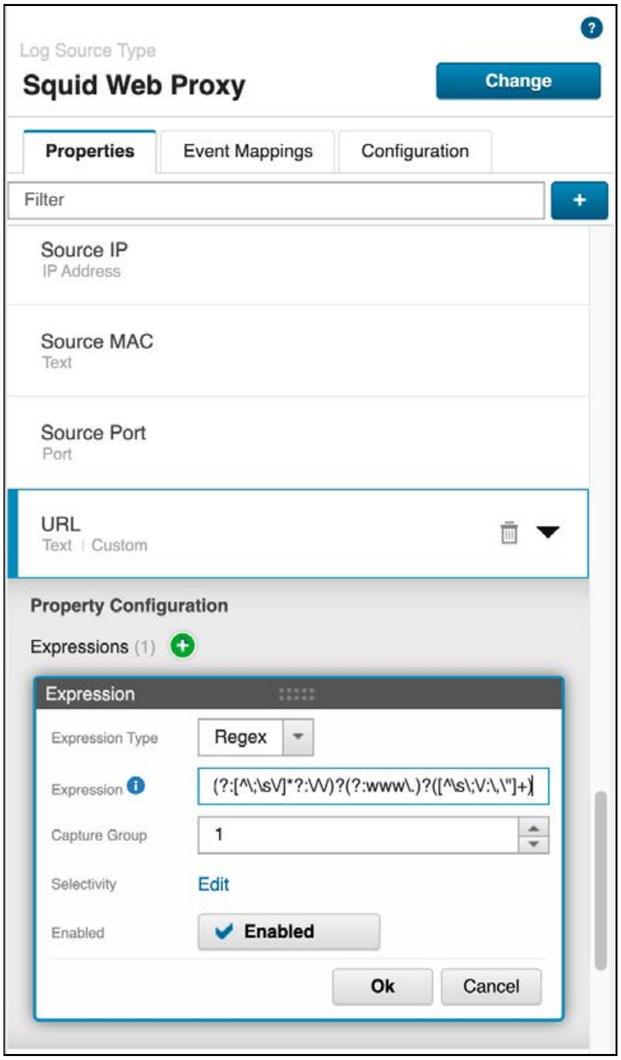
A QRadar account with `admin` access is required to successfully install and configure the app. After installation, user functions should be available with any account.

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** → **DomainTools** → **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** → **Data Sources** → **Events** → **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



Log Source Type

Squid Web Proxy

Source IP
IP Address

Source MAC
Text

Source Port
Port

URL
Text | Custom

Property Configuration

Expressions (1)

Expression

Expression Type: Regex

Expression:

```
(?:[^\;\s\/]*?:\/\/)?(?:www\.)?([^\s\;\/:\,\"]+)
```

Capture Group: 1

Selectivity: Edit

Enabled: ✓ Enabled

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 QRadar documentation.

App Installation

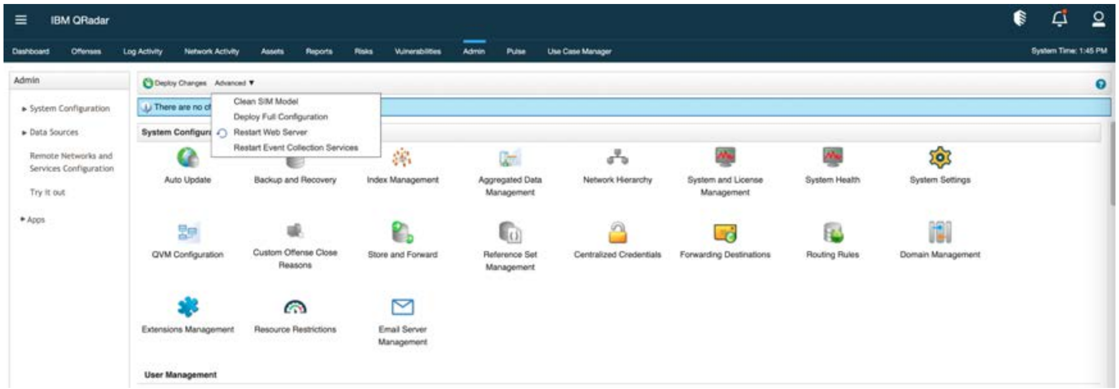
Uninstalling Prior Versions

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.

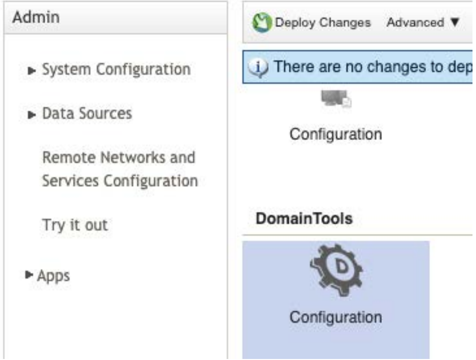
For best results, use the QRadar web UI to uninstall any previous versions of the DomainTools App.

Installation Steps

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

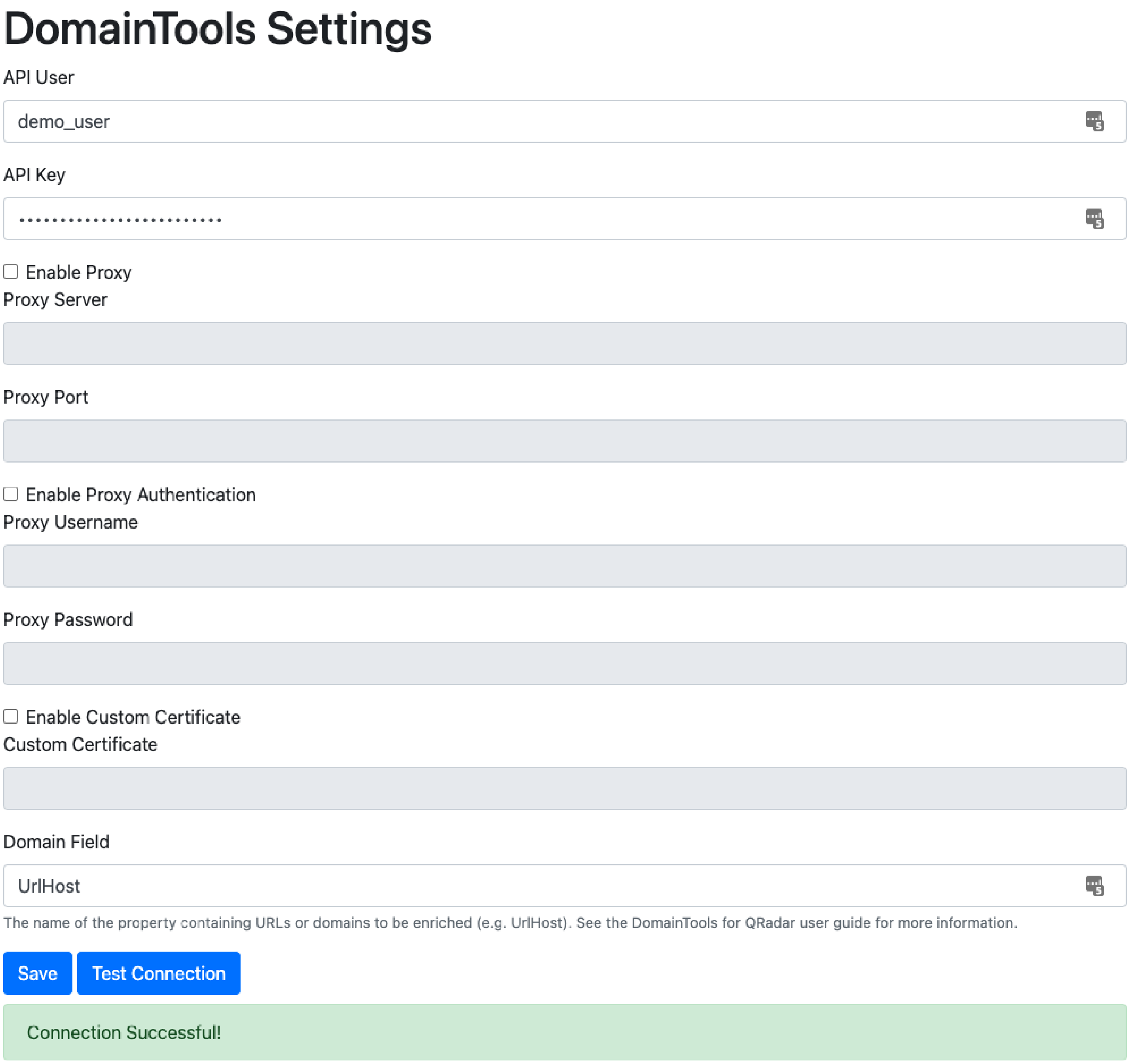


5. Log in to one of the search head members and verify the setup and configuration.
   a. Navigate to **Admin** → **DomainTools** → **Configuration**.



   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 Username

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.

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:

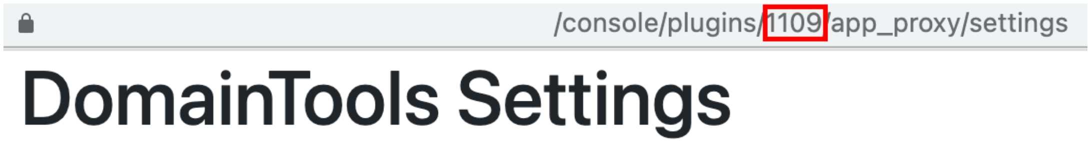
1. Navigate to **Admin** → **DomainTools** → **Configuration**.
2. Add the *API Credentials* - the *API Username* and *API Key*.
3. Click the **Test Connection** button to validate the connection.
4. Once validated, click **Save** *to* save the settings.

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

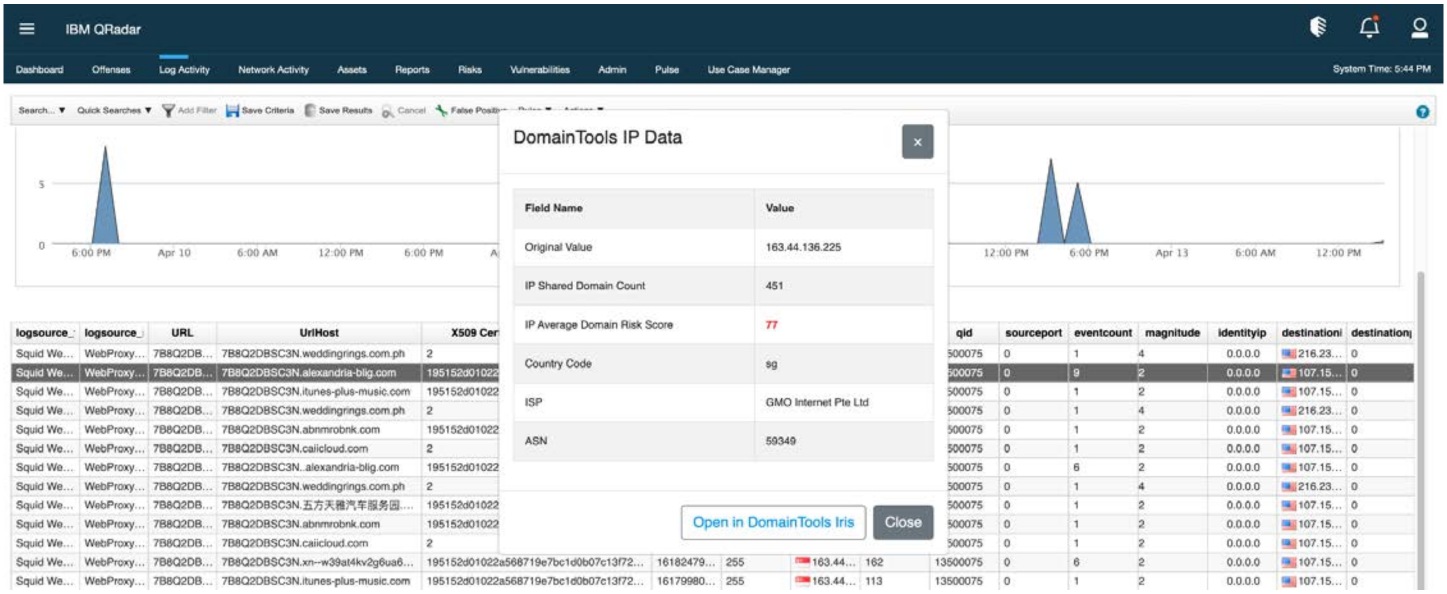
Throughout the QRadar App, anywhere one of the designated properties described in the Right Click Actions Table is presented, the user can right click to gain a brief overview of DomainTools data about that entity. This contextual information on Domain, IP, Mailserver IP, Nameserver IP, and SSL Hashes 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 "Guided Pivot" 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.



DomainTools IP Data

Field Name	Value
Original Value	163.44.136.225
IP Shared Domain Count	451
IP Average Domain Risk Score	77
Country Code	sg
ISP	GMO Internet Pte Ltd
ASN	59349

logsource_	logsource_	URL	UrlHost	X509 Cer					qid	sourceport	eventcount	magnitude	identityip	destinationi	destination
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					500075	0	9	2	0.0.0.0	107.15...	0
Squid We...	WebProxy...	7B8Q2DB...	7B8Q2DBSC3N.itunes-plus-music.com	195152d01022					500075	0	1	2	0.0.0.0	107.15...	0
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.abnmrobnk.com	195152d01022					500075	0	1	2	0.0.0.0	107.15...	0
Squid We...	WebProxy...	7B8Q2DB...	7B8Q2DBSC3N.caiicloud.com	2					500075	0	1	2	0.0.0.0	107.15...	0
Squid We...	WebProxy...	7B8Q2DB...	7B8Q2DBSC3N..alexandria-blig.com	195152d01022					500075	0	6	2	0.0.0.0	107.15...	0
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.五方天雅汽车服务图....	195152d01022					500075	0	1	2	0.0.0.0	107.15...	0
Squid We...	WebProxy...	7B8Q2DB...	7B8Q2DBSC3N.abnmrobnk.com	195152d01022					500075	0	1	2	0.0.0.0	107.15...	0
Squid We...	WebProxy...	7B8Q2DB...	7B8Q2DBSC3N.caiicloud.com	2					500075	0	1	2	0.0.0.0	107.15...	0
Squid We...	WebProxy...	7B8Q2DB...	7B8Q2DBSC3N.xn--w39at4kv2g6ua6...	195152d01022a568719e7bc1d0b07c13f72...	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	195152d01022a568719e7bc1d0b07c13f72...	16179980...	255	163.44...	113	13500075	0	1	2	0.0.0.0	107.15...	0

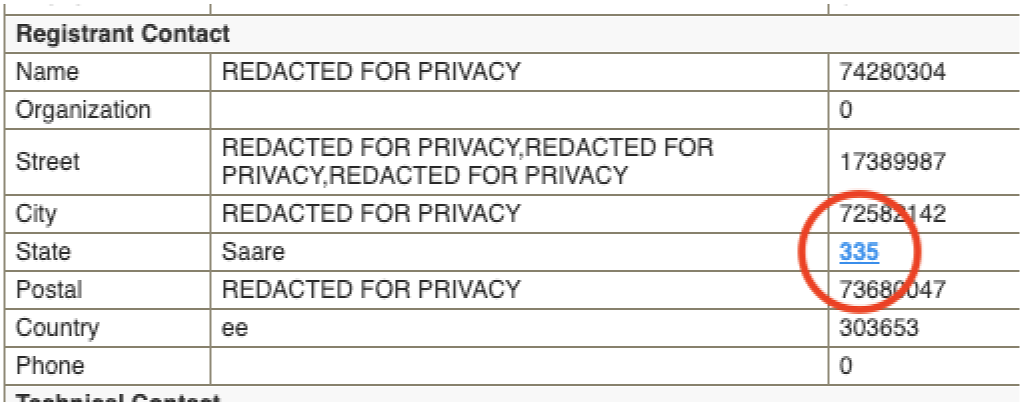
Fig 3: DomainTools summary panel for an IP

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.

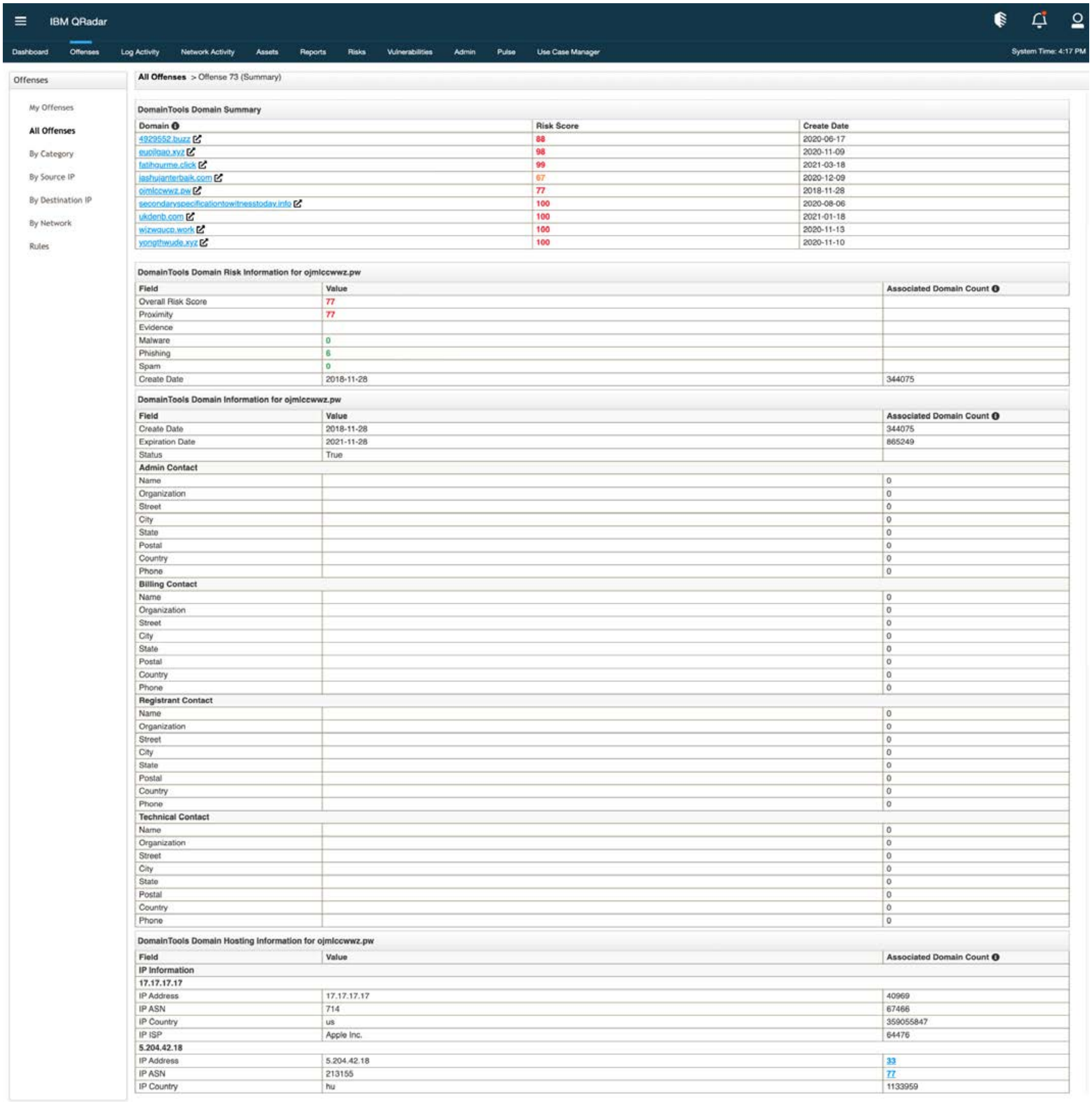


Registrant Contact		
Name	REDACTED FOR PRIVACY	74280304
Organization		0
Street	REDACTED FOR PRIVACY,REDACTED FOR PRIVACY,REDACTED FOR PRIVACY	17389987
City	REDACTED FOR PRIVACY	72582142
State	Saare	335
Postal	REDACTED FOR PRIVACY	73680047
Country	ee	303653
Phone		0
Technical Contact		

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 Iris User Guide for more information.



All Offenses > Offense 73 (Summary)

DomainTools Domain Summary

Domain	Risk Score	Create Date
4929552.buzz	88	2020-06-17
eupilgao.xyz	98	2020-11-09
fatihgurme.click	99	2021-03-18
jashujanterbaik.com	67	2020-12-09
ojmlccwwz.pw	77	2018-11-28
secondaryspecificationtowitnesstoday.info	100	2020-08-06
ukdenb.com	100	2021-01-18
wizwqucp.work	100	2020-11-13
yongthwude.xyz	100	2020-11-10

DomainTools Domain Risk Information for ojmlccwwz.pw

Field	Value	Associated Domain Count
Overall Risk Score	77	
Proximity	77	
Evidence		
Malware	0	
Phishing	6	
Spam	0	
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	
Admin Contact		
Name		0
Organization		0
Street		0
City		0
State		0
Postal		0
Country		0
Phone		0
Billing Contact		
Name		0
Organization		0
Street		0
City		0
State		0
Postal		0
Country		0
Phone		0
Registrant Contact		
Name		0
Organization		0
Street		0
City		0
State		0
Postal		0
Country		0
Phone		0
Technical Contact		
Name		0
Organization		0
Street		0
City		0
State		0
Postal		0
Country		0
Phone		0

DomainTools Domain Hosting Information for ojmlccwwz.pw

Field	Value	Associated Domain Count
IP Information		
17.17.17.17		
IP Address	17.17.17.17	40969
IP ASN	714	67466
IP Country	us	359055847
IP ISP	Apple Inc.	64476
5.204.42.18		
IP Address	5.204.42.18	33
IP ASN	213155	77
IP Country	hu	1133959

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 the official QRadar documentation. 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

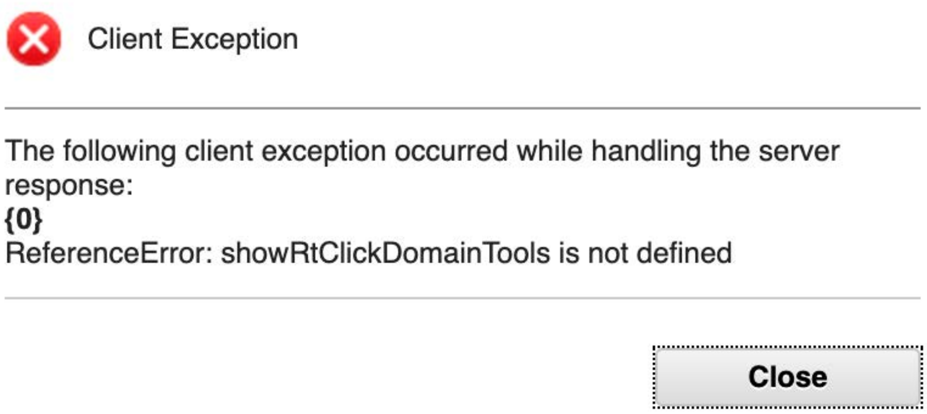
The list below contains all known issues and each contains a workaround or resolution step as appropriate

ID	Issue Overview
1	showRtClickDomainTools is not defined
2	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:



Client Exception

The following client exception occurred while handling the server response:
{0}
ReferenceError: showRtClickDomainTools is not defined

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

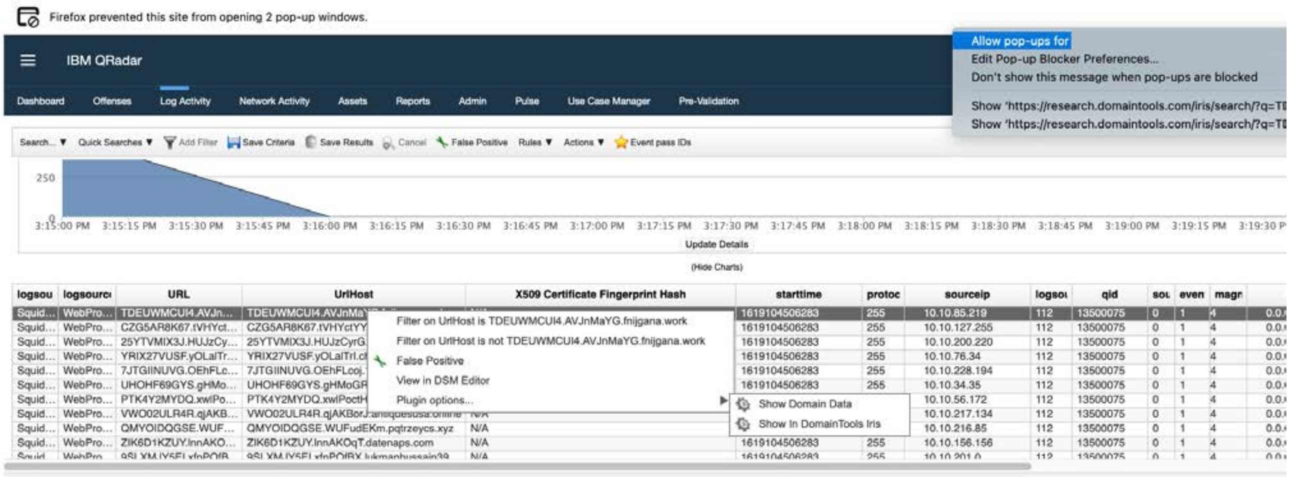
QRadar caches lots of the resources it loads so sometimes a newly installed app's resources don't get loaded.

Workaround

Restart Web Server from the Admin panel and hard refresh 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:



Firefox prevented this site from opening 2 pop-up windows.

logsou	logsourc	URL	UrlHost	X509 Certificate Fingerprint Hash	starttime	protoc	sourceip	logsou	qid	sou	even	magr	
Squid...	WebPro...	TDEUWMCUI4.AVJn...	TDEUWMCUI4.AVJnMa		1619104506283	255	10.10.85.219	112	13500075	0	1	4	0.0.
Squid...	WebPro...	CZG5AR8K67.tVHYct...	CZG5AR8K67.tVHYctYY		1619104506283	255	10.10.127.255	112	13500075	0	1	4	0.0.
Squid...	WebPro...	25YTVMIX3J.HUJzCy...	25YTVMIX3J.HUJzCyrG.		1619104506283	255	10.10.200.220	112	13500075	0	1	4	0.0.
Squid...	WebPro...	YRIX27VUSF.yOLalTr...	YRIX27VUSF.yOLalTrl.cl		1619104506283	255	10.10.76.34	112	13500075	0	1	4	0.0.
Squid...	WebPro...	7JTGIINUVG.OEhFLc...	7JTGIINUVG.OEhFLcoj.		1619104506283	255	10.10.228.194	112	13500075	0	1	4	0.0.
Squid...	WebPro...	UHOHF69GYS.gHMo...	UHOHF69GYS.gHMoGR		1619104506283	255	10.10.34.35	112	13500075	0	1	4	0.0.
Squid...	WebPro...	PTK4Y2MYDQ.xwlPo...	PTK4Y2MYDQ.xwlPoctH				10.10.56.172	112	13500075	0	1	4	0.0.
Squid...	WebPro...	VWO02ULR4R.qjAKB...	VWO02ULR4R.qjAKBorJ.antiquesusa.online	N/A			10.10.217.134	112	13500075	0	1	4	0.0.
Squid...	WebPro...	QMYOIDQGSE.WUF...	QMYOIDQGSE.WUFudEKm.pqtrzeycs.xyz	N/A			10.10.216.85	112	13500075	0	1	4	0.0.
Squid...	WebPro...	ZIK6D1KZUY.lnnAKO...	ZIK6D1KZUY.lnnAKOqT.datenaps.com	N/A	1619104506283	255	10.10.156.156	112	13500075	0	1	4	0.0.
Squid	WebPro	9SLXMJY5FI.xfnPOfB	9SLXMJY5FI.xfnPOIBX.lukmanhussain39	N/A	1619104506283	255	10.10.201.0	112	13500075	0	1	4	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.