
ISC
2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
威胁情报论坛

X-Force Exchange

The Concrete Value of Threat Intelligence Sharing and IBM X-Force Practice

Ron Williams, STSM
Chief Architect, Infrastructure Security
IBM Security

Agenda

Threat Analyst Operations - ‘Getting to Go’

The Power of Community

Analyzing, Mitigating, and Sharing Active Threats

The Internet is Really – REALLY BIG

4.2 Billion IPv4 Addresses (Research indicates visibility to ~1.2 Billion < 25%)
7x1038 IPv6 Addresses

Systematic Scanning & Site Analysis is mathematically infeasible.

Effective Internet Threat Data starts with observables associated with questionable activity.

Effective Internet Threat Intelligence starts with intranet observables correlated with Internet Threat Data.

IBM Daily Analyzes 12+ Million Malicious Emails, 10+ Million Web Sites, Generating and updating new threat data across ~1 Billion IPs & URLs

Effective Threat Intelligence

Starts with a trigger (observable)

- Malicious Mail (SPAM) -> Dropper URLs, Associated IP's, Actual Malware
- Detected Malware Beaconing to Unknown IP
- Network Observable (Suspicious Destination Address)

Further Analysis

- IP/URL – Have other's seen malicious activity? Multi-hoster? New Domain?
- Has malware been found? Has it's C2 infrastructure been identified
- Can other's confirm the 'Three-Legged Stool: IP, URL, Malware'

Of Observables and Indicators

Q: When does an ‘observable’ become an ‘indicator’

Of Observables and Indicators

A: When it’s associated with other known malicious observables

Collecting the data – making the correlation

True 0-Days may be confirmed in one of two-ways

1. Human Analysis
2. Automated Behavioral analysis of one or more of the observables (IP, URL, Malware, Compromised System)

The ‘holy grail’ of Threat Mitigation is ‘Automated Action’ based on ‘Actionable Intelligence’

We have technical examples of this today in Next Generation Firewalls, Intrusion Prevention Systems, Malware Sandboxes, Security Information and Event Management Systems.

But there is yet to be an end-to-end and automated system that can start with a zero-day threat and end with automated and actionable threat intelligence.

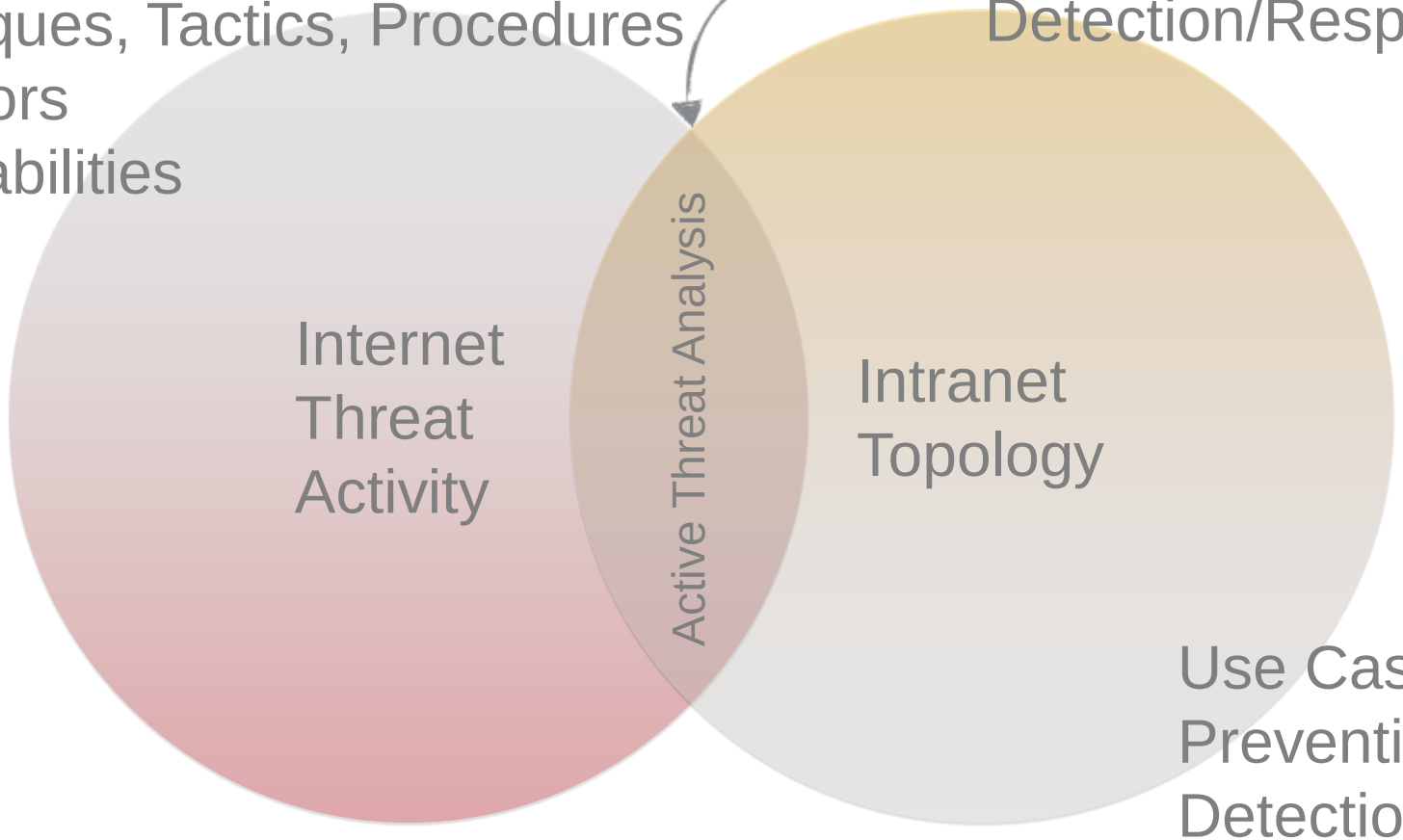
Getting to ‘go’ – the role of the threat analyst

Until a Watson or Hal takes over the internet – The Human Security Analyst remains the most important part of any Threat Protection System. His or her role is to:

1. Understand a threat and how to mitigate it
2. Apply business metrics to prioritize threat mitigation
3. And Increasingly – how to apply tools to continuously shorten the time from identification to validation to prioritization to mitigation (or risk acceptance)

Analyst's Scope: Detection/Response

Actors
Techniques, Tactics, Procedures
Indicators
Vulnerabilities



Use Cases
Prevention
Detection
Response

infiltrating an enterprise (darkhotel)

A. At hotel, I want WiFi access in Lobby

B. Presented with ‘Hotel’s’ WiFi Finder App and promise of Free WiFi

C. Select ‘Connect’ - authenticate to O/S to permit installation

Powned

D. Urgent phone call - close laptop - leave town

back home in SOC

1. SIEM Alert - SRC 172.10.34.17 DEST **216.158.85.49**
2. Identified C2 Communications
3. Response
    1. Identify SRC Machine from Asset Repository/Network
    2. Institute Malware Scan
    3. Found Suspicious File MD5: 560d68c31980c26d2adab7406b61c651

IBM X-FORCE EXCHANGE

Search

AlertCon™ Threat Level 1

216.158.85.49

Search

Current Threat Activity

Malicious IP addresses in the last hour

Activity

Timeline

ip-198.206.133.79

ip-2.115.68.148

Schneider Electric InduSoft Web Studio Remote Agent code execution

NVIDIA Graphics Driver privilege escalation

Security Intelligence Blog

Shifu Officially Spreads to the UK: Banks and Wealth Management Firms Beware

The Mobility Minute, Sept. 21–25: Are Your Travel Apps Secure?

The Importance of a Security Culture

Collections

My Collections

+ New collection

XCodeGhost

Bogus 'Dear Apple Customer" Spam

CryptoWall Sender

"Quote" SPAM delivers Malware

Shared with me

No collections are shared with you yet

Public

The Dukes - Report on Russian Cyberespionage

Black Vine / Deep Panda APT

IBM X-FORCE EXCHANGE | 216.158.85.49

Risk
7.1

X-Force IP Report

216.158.85.49

Details

Categorization Malware (43%)
Botnet Command and Control Server (71%)
Application No known application
Location United States

18
Timeline
view all

Category	Reason	Location	Date
▼ Malware (43%) Botnet Command and Control Server (71%)	Content found on multihoster	United States	Sep 25, 2015 6:00 PM
▲ Malware (57%) Botnet Command and Control Server (71%)	Content found on multihoster	United States	Sep 25, 2015 11:35 AM
▼ Malware (43%) Botnet Command and Control Server (71%)	Content found on multihoster	United States	Sep 18, 2015 5:45 PM
▲ Malware (57%) Botnet Command and Control Server (71%)	Content found on multihoster	United States	Sep 18, 2015 11:34 AM

11
Passive DNS
view all

Name	Category	Type	Location	Date
216-158-85-49.static.webnx.com	Shopping, Software /	PTR		Sep 29, 2015 4:03

IBM X-FORCE EXCHANGE

Search

My Searches

23.27.192.115

222.178.229.66

80.78.251.161

Trending

tcp_cisco_implant_cnc

vulnerabilities

134.0.9.93

Activity

Timeline

malware-e90c7bcf645c38f00db4e838157

ip-2.115.68.148

NVIDIA Graphics Driver privilege escalation

Git for Windows ssh-agent.exe buffer overflow

Security Intelligence Blog

Shifu Officially Spreads to the UK: Banks and Wealth Management Firms Beware

The Mobility Minute, Sept. 21–25: Are Your Travel Apps Secure?

The Importance of a Security Culture Across the Organization

Collections

My Collections **4** | Shared with me **0** | Public **69**

Dark Hotel

First | Previous | 1 | 2 | 3 | 4 | Next | Last

Darkhotel 2015

22 URL **15** MAL **2** VUL
2 IP

Doug Franklin
Aug 24, 2015

Darkhotel 2015

Public Collection

H1 H2 H3 pre

Darkhotel APT (2015)

This threat actor has been active since at least 2008 and appears to focus on compromising hotel networks in order to surveil or compromise guests. This report focuses on the most recent attacks (at the time of writing this Collection), which often involve misuse of stolen certificates. This actor also has a history of deploying their tools as .hta files. Recent attacks use the one of the 0-day vulnerabilities revealed in the Hacking Team breach, but some reports indicate that Darkhotel was using the exploit prior to the Hacking Team leak. In addition, the latest attacks shows expansion of the geographic reach of Darkhotel's targets. Recent attacks also use (lightly) obfuscated .HTA downloaders. Multiple sources describe their spearphishing attacks as "relentless".

This actor appears to maintain a stockpile of stolen certificates and signs their downloaders (droppers) and backdoors with them. Some recent revoked certificates belong to Xuchang Hongguang Technology Co. Ltd. As time passes, Darkhotel's implants employ additional layers of encryption and obfuscation to avoid detection, helping to reduce the rate at which their stolen certificates are identified. These implants also employ additional checks for analysis and defensive technologies on the victim machines. The actor also seems to modify compilation and linkage timestamps embedded in the executable files to indicate origins in 2013. The actor reacts to security researcher pressure, and has tightened their control over the contents of their CnC servers.

Attack Flow

The actor pursues a consistent attack flow, probably due to their success with it. Recent attacks tend to use one of three chains:

- downloader -> hta checkin -> info stealer -> additional components
- dropper -> wsh script -> wsh script -> info stealer -> additional components
- spearphish -> dropper -> hta checkin -> downloader -> info stealer

Additional Indicators

- 021685613fb739dec7303247212c3b09
- 1ee3dfce97ab318b416c1ba7463ee405

Reports (41) view all

IP 216.158.85.49
Report captured on Aug 25, 2015 4:38:46 PM by Ron Willia

IP 111.90.144.225
Report captured on Aug 25, 2015 4:29:59 PM by Ron Willia

VUL Adobe Flash Player code execution (CVE-2015
Report captured on Aug 22, 2015 12:25:48 AM by Doug

URL thewordusrapid.com
Report captured on Aug 21, 2015 11:51:50 PM by Doug

Version History (15) view all

Bruce Wynn
Last modified: Aug 24, 2015 7:37:32 PM

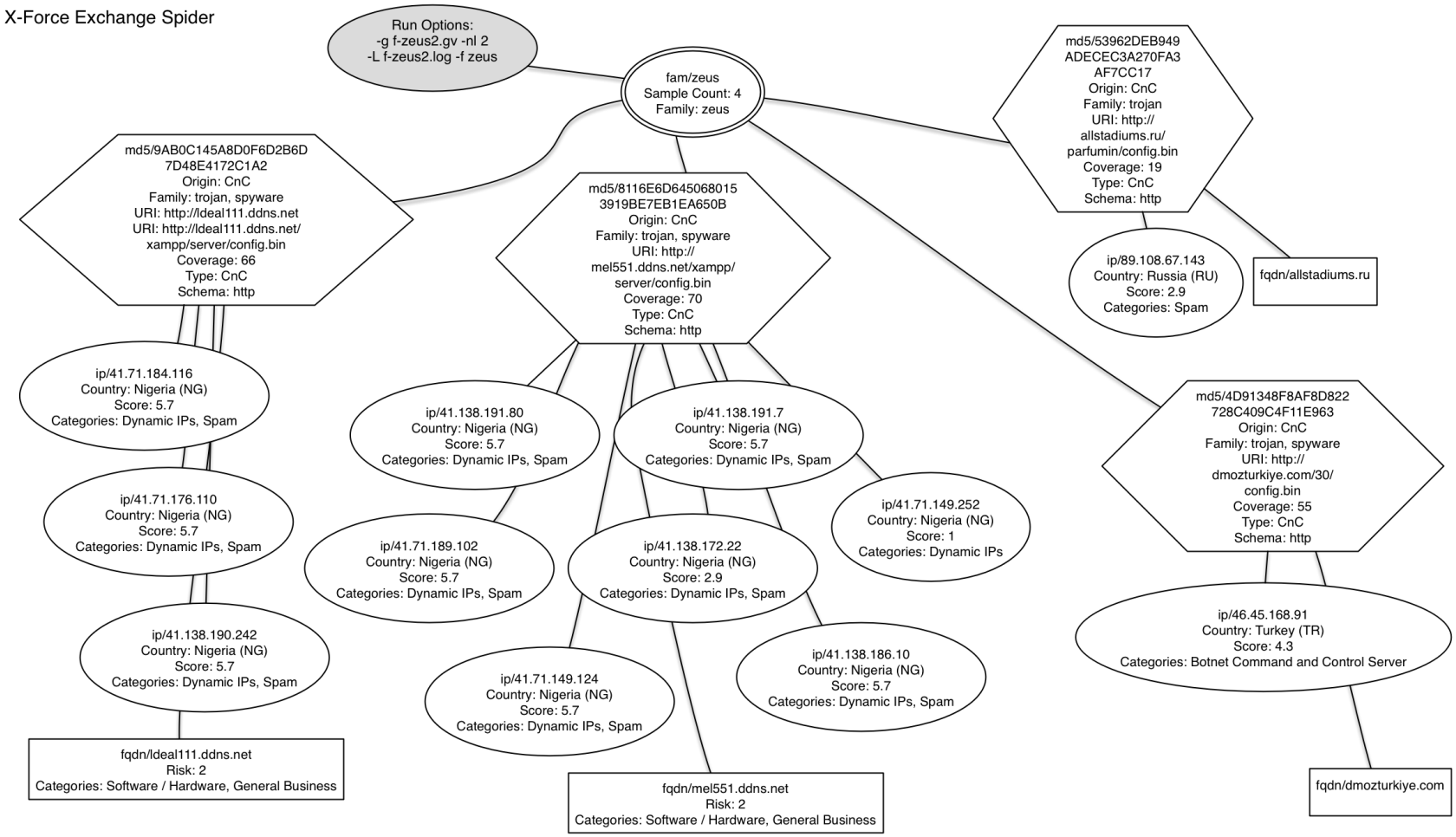
Doug Franklin
Last modified: Aug 22, 2015 1:56:11 AM

Doug Franklin
Last modified: Aug 22, 2015 12:53:52 AM

Doug Franklin

threat data -> intelligence

X-Force Exchange Spider



what we can share

Attack Flow

Suspect Internet IP's & URLs

Identified Malware Signatures

Other IOC's (Registry Keys, dropped files, command files, executables, etc.)

Meaningful Correlations

Significant data to assist the 2nd analyst

what we (typically) don’t share

internal infrastructure (internal networks, ip’s)

0day application and system vulnerabilities (unpublished)

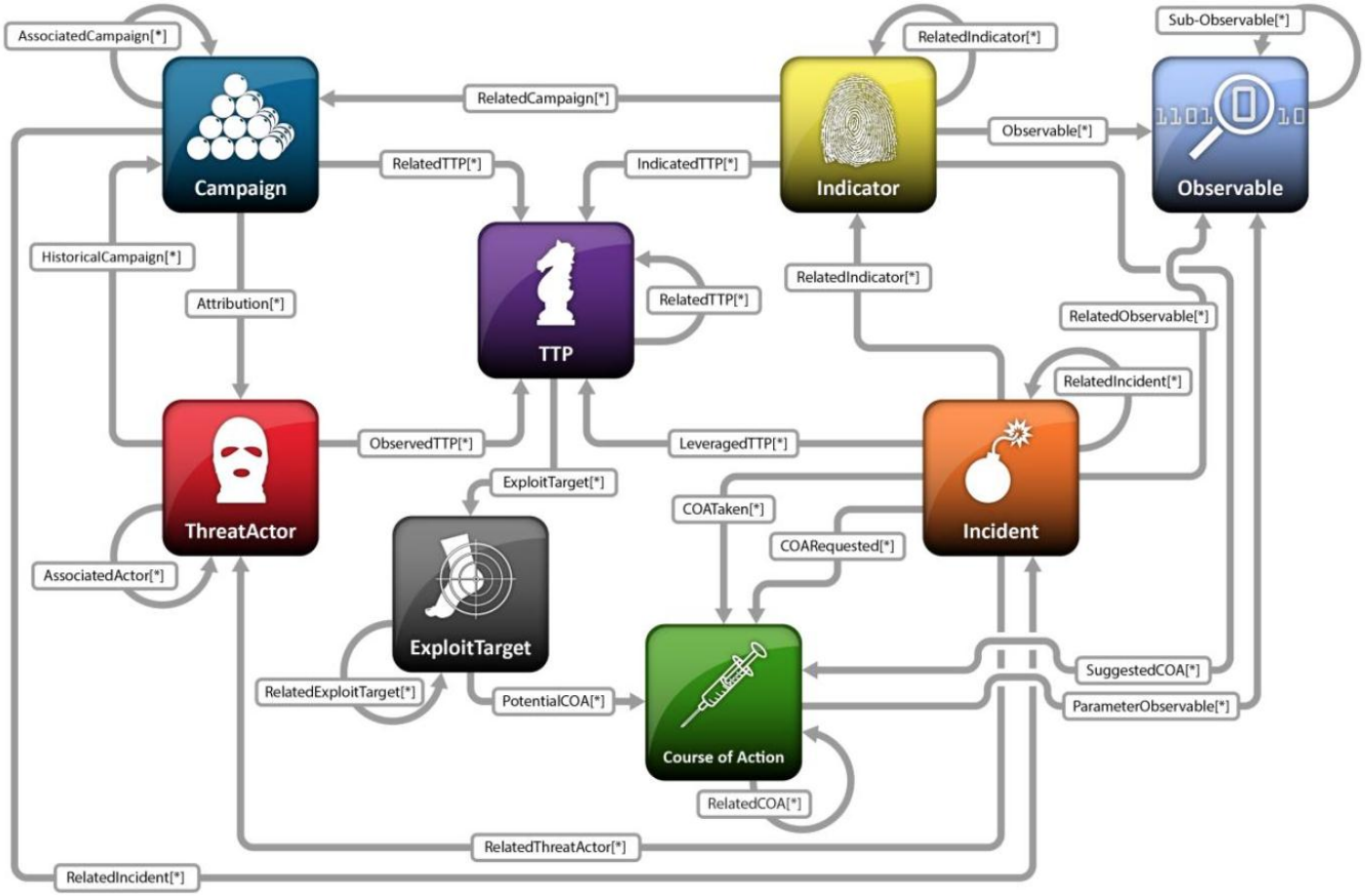
target specific data (individuals, accounts, ip addrs, etc)

Threat Intelligence – Enabling Machine Processing

Making Threat Data and Intelligence Available

- For the Human Analyst
- For the Human Analysts Tools
- Building and Threat Intelligence Ecosystem

Structured Threat Information eXpression (STIX) v1.1 Architecture



Accessing X-Force Exchange API

Public (free) Access

X-Force Exchange

https://exchange.xforce.ibmcloud.com

X-Force Exchange API

https://api.xforce.ibmcloud.com/doc

Who's Using X-Force Exchange?

Threat Researchers – Aggregating IP, URL, Malware, and Vulnerability reports into Collections

Customers in Finance, Banking, Retail, and Energy

Managed Security Services Analysts – Using Collections to create report with historical threat information for operations.

3rd Party Developers building SDK's to integrate X-Force Exchange Data with their own offerings (GitHub)

Accessing the API

IBM X-Force Exchange | IBM X-Force Exchange API

swagger

https://api.xforce.ibmcloud.com/doc/swagger.yaml

eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9

Explore

IBM X-Force Exchange API Documentation

Check out the Gentle Introduction to the X-Force Exchange API first!

To get started, you can try out all the endpoints interactively here. To use the XFE api from other http clients, refer to the authentication endpoint section on how to obtain an access token.

Most endpoints require the 'Accept-Language' header, including the language you would like the response in.

Some endpoints are authenticated endpoints, and will require a valid user owned token to use. Your token can be obtained from the Exchange within your User Dropdown. Copy and paste that key into the box in the upper right corner of this documentation to use your authenticated user token.

Your use of the IBM X-Force Exchange is governed by the IBM Cloud Services Agreement and the accompanying Service Description. You can find a copy of the Cloud Services Agreement by clicking on https://www.ibm.com/terms, and selecting your region, then your country, then the 'IBM Cloud Services Agreement' link. You can find a copy of the Services Description by clicking on Service Description. By using these services you agree to the terms of the IBM Cloud Services Agreement and Service Description. If you do not agree with these terms, do not use the IBM X-Force Exchange

Created by X-Force API Support

Contact the developer

Authentication	Show/Hide | List Operations | Expand Operations
Collections	Show/Hide | List Operations | Expand Operations
DNS	Show/Hide | List Operations | Expand Operations
Internet Application Profile	Show/Hide | List Operations | Expand Operations
IP Reputation	Show/Hide | List Operations | Expand Operations
Malware	Show/Hide | List Operations | Expand Operations
Signatures	Show/Hide | List Operations | Expand Operations
TAXII	Show/Hide | List Operations | Expand Operations
URL	Show/Hide | List Operations | Expand Operations
User	Show/Hide | List Operations | Expand Operations
Version Information	Show/Hide | List Operations | Expand Operations
Vulnerabilities	Show/Hide | List Operations | Expand Operations

Authentication

GET /auth/anonymousToken

Request (curl)

```
curl -X GET --header "Accept: application/json”
      "https://api.xforce.ibmcloud.com/auth/anonymousToken"
```

Response Body:

```
{
  "token”: <jwt>
}
```

The <jwt> goes into Authorization Headers for subsequent requests like this:

```
curl -X GET --header "Accept: application/json”
      --header “Authorization: “Bearer <jwt>”
```

IP Reputation

Show/Hide | List Operations | Expand Operations

GET /ipr/{ip} — Returns the IP report for the entered IP.

```
curl -X GET --header "Accept: application/json" --header "Authorization: Bearer <jwt>"
                                        https://api.xforce.ibmcloud.com/ipr/1.2.3.4"
```

Response (partial) in JSON Format


```
[ {
     "ip": "1.2.3.4",
     "cats": {
       "Anonymisation Services": 43,
       "Malware": 71,
       "Botnet Command and Control Server": 71
     },
     "reason": "Content found on multihoster",
     "created": "2015-06-16T09:48:00.000Z",
     "score": 7.1,
     "subnet": "1.2.3.4/32"
   },
  "cats": {
    "Anonymisation Services": 43,
    "Malware": 71,
    "Botnet Command and Control Server": 71
  },
  "geo": {
    "country": "Australia",
    "countrycode": "AU"
  },
  "score": 7.1
}]
```

TAXII Interface (for STIX Formatted IP, URL, VULN, and User Collections)

TAXII

Show/Hide | List Operations | Expand Operations

POST /taxii — Trusted Automated eXchange of Indicator Information version 1.1

Implementation Notes

Single endpoint for taxii over https. Start with a discovery request.
Available feeds: xfe.default, xfe.ipr, xfe.url, xfe.collections.public, xfe.vulnerabilities

Reference: https://taxii.mitre.org/.

TAXII requests must be made with an anonymous authentication token, available from https://xforce-api.mybluemix.net/auth/anonymousToken

Example queries

Click the buttons below to pre-populate example queries.

A TAXII discovery request lists all available TAXII services.
Discovery
A TAXII data collection request lists all available TAXII data collections.
Data Collections
A Poll IPR query returns a TAXII IPR report. The IP address in the query can be modified.
IPR
A Poll URL query returns a TAXII URL report. The URL in the query can be modified.
URL
A All Public Collections query returns a list of all TAXII public collections.
All Public Collections
A Public Collection query returns a TAXII public collection. The value parameter is the object ID in the database.
Public Collection
A Poll Vulnerability query returns a TAXII Vulnerability report.
Vulnerability

Parameters

Parameter	Value	Description	Parameter Type	Data Type
message	`<taxii_11:Discovery_Request xmlns="http://taxii.mitre.org/messages/taxii_xml_binding-1.1" message_id="551"></taxii_11:Discovery_Request>`	**taxii 1.1 message**	body	string

Parameter content type: application/xml

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	TAXII Response		

Try it out! Hide Response

Curl

Curl

```
curl -X POST --header "Content-Type: application/xml" --header "Accept: application/xml" --header "Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJ1c2
```

Request URL

```
https://api.xforce.ibmcloud.com/taxii
```

Response Body

```
<taxii_11:Discovery_Response xmlns:taxii_11="http://taxii.mitre.org/messages/taxii_xml_binding-1.1" message_id="56180" in_response_to="551">
  <taxii_11:Service_Instance service_type="POLL" service_version="urn:taxii.mitre.org:services:1.1" available="true">
    <taxii_11:Protocol_Binding>urn:taxii.mitre.org:protocol:http:1.0</taxii_11:Protocol_Binding>
    <taxii_11:Address>https://api.xforce.ibmcloud.com/taxii</taxii_11:Address>
    <taxii_11:Message_Binding>urn:taxii.mitre.org:message:xml:1.1</taxii_11:Message_Binding>
    <taxii_11:Content_Binding binding_id="urn:stix.mitre.org:xml:1.0"></taxii_11:Content_Binding>
  </taxii_11:Service_Instance>
  <taxii_11:Service_Instance service_type="DISCOVERY" service_version="urn:taxii.mitre.org:services:1.1" available="true">
    <taxii_11:Protocol_Binding>urn:taxii.mitre.org:protocol:http:1.0</taxii_11:Protocol_Binding>
    <taxii_11:Address>https://api.xforce.ibmcloud.com/taxii</taxii_11:Address>
    <taxii_11:Message_Binding>urn:taxii.mitre.org:message:xml:1.1</taxii_11:Message_Binding>
    <taxii_11:Content_Binding binding_id="urn:stix.mitre.org:xml:1.0"></taxii_11:Content_Binding>
  </taxii_11:Service_Instance>
  <taxii_11:Service_Instance service_type="COLLECTION_MANAGEMENT" service_version="urn:taxii.mitre.org:services:1.1" available="true">
    <taxii_11:Protocol_Binding>urn:taxii.mitre.org:protocol:http:1.0</taxii_11:Protocol_Binding>
    <taxii_11:Address>https://api.xforce.ibmcloud.com/taxii</taxii_11:Address>
    <taxii_11:Message_Binding>urn:taxii.mitre.org:message:xml:1.1</taxii_11:Message_Binding>
    <taxii_11:Content_Binding binding_id="urn:stix.mitre.org:xml:1.0"></taxii_11:Content_Binding>
  </taxii_11:Service_Instance>
</taxii_11:Discovery_Response>
```

Response Code

```
200
```

The Importance of Threat Intelligence Sharing

Research estimates indicate less than 20% of the IPv4 namespace is analyzed and categorized.

Increasingly, attacks use dynamic ip addresses and dynamically generated domain names to direct victims to command and control servers. This means that internet scanning and analysis by itself is not sufficient to protect against attack.

For IPv4 alone – there are over 4 billion possible endpoints. It is not possible to understand the state of all endpoints instantaneously. IPv6 renders random internet scanning a very low yield activity.

The ability to share active attack information with trusted colleagues and communities provides the most current information from which active attacks might be thwarted.

The Unthinkable or Unacceptable is not the same as the Impossible.

Plan for it - or it will plan for you.

– Anonymous

https://exchange.xforce.ibmcloud.com

ron williams, senior technical staff member
ibm security