脅威インテリジェンスを共有する革新的なプラットフォーム
「IBM X-Force Exchange」と「Exchange API」

Technologist
X-Force Research
IBM Security
Doug Franklin

X-Forceのリサーチ・テクノロジストとして、広範囲に及ぶ脅威、エクスプロイテーション、ディフェンス技術を担当。これまでに不正侵入防止/防御システム(IDS/IPS)や、アンチウイルス・システム、文書画像処理システムの開発などに従事。

将来2015年は、「脅威インテリジェンス共有の年」として語られるようになるでしょう。セキュリティー脅威情報の共有については、1990年代に関心を集めるようになってから今日に至るまでさまざまな取り組みが行われており、近年増加を続ける情報漏洩事件によりその注目度が急激に高まっています。2015年2月にオバマ米大統領が「サイバー・セキュリティーと消費者保護に関するホワイトハウス・サミット」[1]を主催し、大統領令13691号「民間企業におけるサイバー・セキュリティー情報共有の促進(Promoting Private Sector Cybersecurity Information Sharing)」[2]を発令したことも注目が高まっている大きな契機となっています。攻撃者である"Bad Guys"は自らの成功と失敗だけでなく、私たちの防御策と脆弱性に関する情報も共有しています。私たち"Good Guys"も同じように情報を共有しなければ、サイバー空間という戦場は攻撃者の手に落ちてしまいます。

こうした気運を受けIBMは、2015年4月に「X-Force Exchangeポータル」(以下、Exchange)を開設しました[3]。Exchangeでは、リアルタイムのセキュリティー脅威情報に加えて、IBM Securityが1990年代から収集してきた膨大な脅威情報を、ブラウザー・ベースのUI[3]とAPI[4]を通して提供しています。X-Force脆弱性検索による脆弱性情報や、X-Force AppLoupeポータルからのIP/ドメイン/URLレピュテーションなど、「攻撃によって観測された事象(以下、観測事象)」に関する幅広い情報が公開されています。Exchangeのユーザーは、インシデントやサイバー攻撃活動、攻撃者などの情報をまとめるコレクションを作ることが可能で、特定の個人や世界中の人々と共有したり、更新できることが特長です。

Exchange APIとは

Exchangeは、セキュアでREST(Representational State Transfer)原則に従っているJSONベースのAPIを提供しています。このAPIを使用することで、クエリを自動化して、Exchangeに蓄積されているセキュリティー脅威情報をシステムや製品に取り入れることができます。Exchange APIは、次の3つのカテゴリーに大別されます(**表1**)。

Exchange APIの各クエリの詳細は、API資料ページ(https://xforce-api.mybluemix.net/doc/)を参照してください。このページには各クエリの構文とレスポン

表1. Exchange APIのカテゴリーとクエリ・タイプ

カテゴリー	リクエスト・タイプ
アクセス管理	Version Information:バージョン情報 User:ユーザー情報 Authentication:認証情報(APIキー)
インジケーター・クエリ	DNS:最新および過去のDNS情報
	IAP:インターネット・アプリケーション・プロファイル(IAP)
	IP Reputation:最新および過去のIPアドレスのレピュテーションおよびアソシエーション
	Malware:ハッシュまたはファミリー名によるマルウェア・サンプルのリスクと対処
	Signatures:IBMセキュリティー保護シグネチャーの詳細
	URL:最新および過去のURLのレピュテーションおよびアソシエーション
	Vulnerabilities:脆弱性(リスク、製品、保護シグネチャーなど)
コレクション・クエリ	Collections:Exchangeコレクションおよび添付ファイルの参照および検索
	TAXII:TAXIIプロトコルによるSTIX形式情報のアップロード/ダウンロード

ス結果のデータ・モデルが掲載されており、対話形式でクエリをテストすることもできます。

■フル・テキスト検索

Exchange APIでは、コレクション(Collections)、インターネット・アプリケーション・プロファイル(IAP)、シグネチャー(Signatures)、および脆弱性(Vulnerabilities)に関するクエリにて、フル・テキスト検索機能を提供しています。これらのクエリでは、大文字と小文字を区別せずワイルド・カードを用いた任意の文字列を検索できます。またLuceneクエリ言語もサポートしているため、次のような機能もあります。

- ●ブール演算子(AND(+)、OR、NOT(-))
- ●括弧を使用したグループ化による優先順位制御
- ●ファジー検索(ティルデ(~)記号を検索語句の最後に付加)
- ●特定語句の強調(カレット(^)演算子を使用)

例えば、次の検索を実行すると、

```
email and (phish*^ or spam*)
```

emailという単語を含み、かつphish(フィッシュ)またはspam(スパム)のいずれかの文字列を含む(ただしphishの強調度を2倍として検索)観測事象のレポートとコレクションが返されます。この検索は、自然言語テキスト(コレクションのWiki部分、項目の説明、およびタイトル)を含むすべてのExchangeのデータベース・フィールドが対象となります。言語構文の詳細は、Apache Software Foundationの「Query Parser Syntax」文書に記載されています[5]。特に、検索語句はクエリ実行時のリクエストURLの一部になるため、特殊文字は正規表現に基づいて設定する必要があります。文書内の「Escaping Special Characters」セクションをよく確認してください。なお、フル・テキスト検索の結果として返されるのは最大200項目のため、検索語句を追加してこの最大数を超えないようにしてください。

■ライブラリーの活用

以下に示すように、Exchange APIクライアントを対象としたいくつかのオープン・ソース・プロジェクトが、GitHubで立ち上がっています。同じ言語のライブラリーを使用すれば、一部のインターフェース作業が不要となります。

- ●Go言語/Golangライブラリーを提供するgoxforceプロジェクト[6]
- ●Pythonライブラリーを提供するibmxforceex.checkerプロジェクト[7]
- ●R言語の制限付きサポートを提供するxForceプロジェクト[8]

注:これらのプロジェクトは、いずれも公式のIBMプロジェクトや、IBM公認のものではありません。

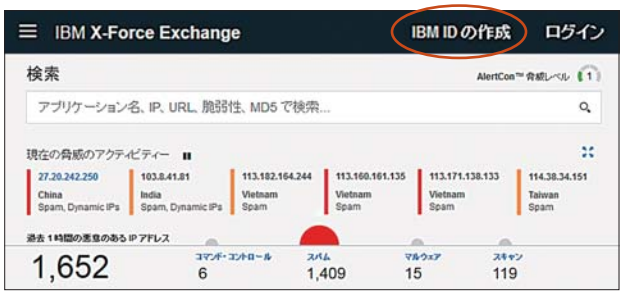
goxforceプロジェクトではExchange APIのほとんどを対象としており、対象範囲の広さではibmxforceex.checkerプロジェクトが続きます。xForceプロジェクトは、IAPにおけるリスクのスコア分析とグラフ化に特化しています。

■Exchange APIの使い方(基礎)

ここでは、Exchange APIの基本的な使い方について説明します。Exchange APIは、IBM Bluemixプラットフォーム[9]のxforce-api.mybluemix.netドメインにて提供されており、HTTPS(ポート443)を経由して利用することができます。クエリはHTTP GET/POSTリクエストを使用し、APIはJSON形式のHTTPレスポンスを生成します。

多くのWebベース・アプリケーションと同様、値のないレスポンス・フィールドは省略されるので、API資料ページで各リクエストの「Model」および「Model Schema」タブを参照しながら、必要なフィールドすべてを埋めてください。詳細はIBM developerWorksのxforce-exchangeタグにて確認できます[10]。

Exchange APIにアクセスするためには、認証済みのAPIキーとパスワードが必要です。これらを取得するには、Exchangeのメイン・ページ(https://exchange.xforce.ibmcloud.com/)にアクセスし、まずウインドウの右上の「IBM IDの作成」をクリックして指示に従います。

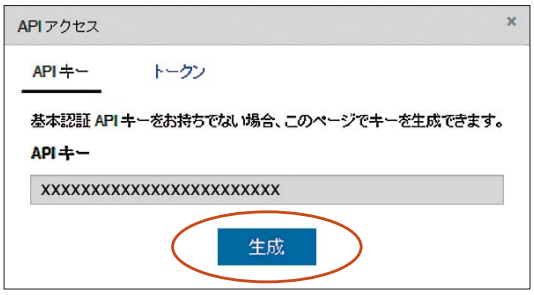


IBM IDが認証されたら、「ログイン」リンクをクリックしサインインします。認証が済んだら、ブラウザー・ウインドウの右上に表示されている肩から上の人間のアイコン(右図)をクリックしてプロファ

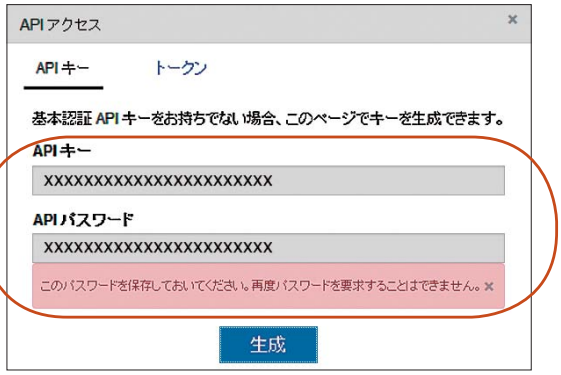
イルにアクセスします。

表示されるパネルの左下にある「API アクセス」をクリックします。

別のパネルがポップアップします。下部にある「生成」ボタンをクリックして認証済みのAPIキーとパスワードを生成します。



なお、APIパスワードは、キー/パスワードを生成するときにのみ表示されますので、APIキーおよびパスワードの値を保存しておいてください。



ここで生成されたAPIキーとパスワードを使用してExchange APIにアクセスできます。なお、APIキーを使ってクエリを実行する際には、以下の通り「Basic 」(スペースに注意)に続けてBase64でエンコードしたAPIキーとパスワードを記載したAuthorizationヘッダーを含める必要があります。

```
Authorization: Basic $BASE64_KEY_AND_PASSWORD
```

なお、APIキーとパスワードに期限はありませんが、新しいAPIキー/パスワードを生成すると古いキー/パスワードは無効になります。

Exchange APIの使い方(実例)

この章では、実際のクエリを使って、ドメイン名またはURLに関するDNSデータを検索してみます。DNSクエリのレスポンス結果には、IBM Securityのセンサー・ネットワークによって収集された情報が組み合わされます。このクエリには、以下のように単純な構文を使用します。

```
/resolve/{domain}
https://xforce-api.mybluemix.net:443/resolve/{domain}
```

{domain}を検索語句に置き換えます。例えば、schneider-electric.comドメインに関するクエリは、以下のようになります。

```
/resolve/schneider-electric.com
https://xforce-api.mybluemix.net:443/resolve/schneider-electric.com
```

このドメインを選択したのには、理由があります。後述するように興味深い結果となるためです。

レスポンス・フィールドにはDNSレコード・タイプの情報が表示され、パッシブDNSレコードがある場合には追加されます。レスポンスには、TXTレコード、AおよびAAAAレコード(IPv4およびIPv6アドレス)、MXレコードが表示されます。レスポンスは、これらをDNSレコード・タイプに関連した名前のオブジェクトで表し、例えばIPv6アドレスに対応しているドメインについては、AAAAオブジェクトが返されます。

各オブジェクトは配列になっています。例えばMXオブジェクトはMXレコードの配列となっており、それぞれにexchangeとpriorityという文字列が含まれています。これらは、DNSクエリの場合と同じようにメール・サーバーの名前とその優先順位を表しています。例示したドメインでは以下のようなレスポンスが返ってきます。

```
{
  "A" : [ "159.215.33.174" ],
  "TXT" : [ "uzeY…" , "MS=ms…" , "MS=…" ],
  "MX" : [
    { "exchange" : "cluster3.eu.messagelabs.com" , "priority" :10 },
    { "exchange" : "cluster3a.eu.messagelabs.com" , "priority" :20 }
  ],
  "total_rows" : 6
}
```

なおこのレスポンスにはパッシブDNSデータは含まれていませんが、レスポンスによってはpassiveフィールドが含まれることもあります。/resolveクエリは、Exchange APIの最もシンプルなレスポンスの一つです。多くのクエリでは、入れ子になっているようなより複雑

なレスポンスが返されますので、APIを利用する際にはAPI資料ページに掲載されている各クエリの「Model」および「Model Schema」タブをよく確認してください。

また、特定のURLやドメインに関連するマルウェアの情報を検索する場合は、次のようなクエリを使用します。

```
/url/malware/schneider-electric.com
https://xforce-api.mybluemix.net:443/url/malware/schneider-electric.com
```

この結果には、発見されたマルウェア・サンプルの数を示すcountオブジェクトと、各マルウェア・サンプルのオブジェクトを保持するmalwareという配列が含まれます。各オブジェクトには、マルウェアとドメインのアソシエーションを記述した複数のフィールドが含まれます。例えば、type値が“SPM”であれば、ドメインを偽装したメール・アドレスからのeメールにマルウェアが添付されていたことを示します。md5値はマルウェア・インスタンスのMD5ハッシュを、firstseenオブジェクトとlastseenオブジェクトは、そのマルウェアに関する最初の検出日時と最新の検出日時を提供します。

```
{
"malware": [
{
"type": "SPM",
"md5": "58BA175F6B837E30FCAA6ABF70D58BCD",
"domain": "schneider-electric.com",
"firstseen": "2015-05-26T15:45:00Z",
"lastseen": "2015-05-26T15:45:00Z",
"ip": "24.243.102.12",
"count": 1,
"filepath": "499193-.zip",
"origin": "SPM",
"uri": "499193-.zip",
"family": [
"Spam Zero-Day"
]
},

・・・※4つのマルウェアに関する情報を中略。
      2015-05-07に最初のマルウェアが検知された。
],
"count": 5
}
```

Schneider Electricのチームは驚くことでしょう。この記事の執筆時点（2015年11月）で、このクエリは5個のマルウェア・サンプルを返したからです。それはどれも2015年5月7日から5月26日の間に検出されたもので、この企業を標的とする攻撃者が5月にSchneider Electricのドメインを偽装してスパム・メールを送り付けていたのは明らかです。

今日、どんな差出人メール・アドレスも偽造できますが、差出元のIPアドレスをチェックすればこの偽装は判明します。クエリの実行結果にあるように、5個のマルウェア・サンプルの攻撃元は、異なる4つのIPv4アドレスでした。これらのマルウェアが本当にSchneider Electricに関係するのであれば、広く散らばったサブネットに属する異なるIPv4アドレスが使われることは通常考えられません。実際に、これらのIPアドレスを個別にチェックしてみると、やはりいずれもSchneider Electricとは無関係なアドレスでした。

終わりに

API資料ページでは、すべてのクエリとレスポンスの詳細を確認できるほか、本稿で説明した各クエリを含めすべてのクエリを対話形式でテストできます。Exchangeは2015年4月に立ち上げたばかりですが、提供するデータとサポートするクエリの両面を迅速に拡充させています。また、クエリ機能の拡張に応じて、API資料ページの内容も追加、変更していきます。

IBM X-Force Exchange APIを利用して、過去および現在のセキュリティー・インテリジェンスを運用されているセキュリティー製品などにインポートすることで最新サイバー脅威に対峙できます。ぜひIBM X-Force ExchangeとExchange APIをご活用ください。

[参考文献]

[1] The White House：Summit on Cybersecurity and Consumer Protection, https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/summit

[2] The White House：Executive Order -- Promoting Private Sector Cybersecurity Information Sharing, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

[3] IBM Security：IBM X-Force Exchange, https://exchange.xforce.ibmcloud.com/

[4] IBM Security：IBM X-Force Exchange API Documentation, https://api.xforce.ibmcloud.com/doc/

[5] Lucene：Package org.apache.lucene.queryparser.classic Description, http://lucene.apache.org/core/4_2_1/queryparser/org/apache/lucene/queryparser/classic/package-summary.html#package_description

[6] GitHub：Golang library to access IBM X-Force Exchange, https://github.com/demisto/goxforce

[7] GitHub：Python based client for IBM XForce Exchange https://exchange.xforce.ibmcloud.com, https://github.com/johestephan/ibmxforceex.checker.py

[8] GitHub：R client for retrieving security intelligence data from IBM xForce Exchange, https://github.com/bmatthie/xForce

[9] IBM Bluemix：http://www.ibm.com/cloud-computing/bluemix/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

[10] IBM developerWorks：Questions tagged with "xforce-exchange", https://developer.ibm.com/answers/topics/xforce-exchange/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US