

Computer Virus の検出

クラウド資源利用による脅威判定

総合情報基盤センター

沖野 浩二

1. メールを取り巻く環境

本学には、平日には2万通を超えるメールが届いています。本学に届くメールは、

- ・ SPAM サイトからのメール 20%
(このメールは学内に配送されない)
- ・ 内容等から SPAM と判断されるメール 15%
(サブジェクトに[SPAM]を付加し配送)
- ・ 通常のメール 65%
(通常の配送)

となっています。この割合は、誤検知(正当なメールを SPAM と判断すること)を防ぐため、判断を一番安全(誤検知を防ぐ設定、代わりに SPAM も通常と判断される)な設定としているため、実際には、SPAM の割合は、40%以上であることは間違いないと思います。

感覚としては、サブジェクトに[SPAM]が追加されているメールと同数以上の SPAM がシステム側にて排除されています。これらの SPAM 判断には、本学に届くメールだけでなく、クラウド側にある SPAM 情報を利用し、多くのサイトの情報を相互に利用しあうことでその効率を上げています。

また、ユーザがメールを取り込んだ時に、Antivirus ソフトウェアが Virus 警告を上げることがあると思います。本学では、ユーザがメールを読むまでに3回 Virus 検査を行っています。1回目はメールが学外から学内のサーバに送信されたときにサーバで、2回目はユーザがメールを取り込むとき FW で、3回目はユーザがメールを開くときクライアントの Antivirus ソフトウェアで検査しています。

メールの安全性を確保するため、怪しいメールを排除し、何回も Virus 検査を行っていますが、実際には、ユーザの PC まで SPAM や Virus 付きメールが届いています。

Google 等のクラウドベンダでは、この数兆倍以上のメールを処理することで、重複しているメールや Virus の検出、悪性あるサイトからの通信を遮断することで、悪意あるメールの対策を行っています。

本学においてもクラウド上のデータおよび資源を利用し、2018年3月から新たな対策を開始しました。これは、1回目の検査において、Virus とは確定できないが怪しそうな添付ファイルを外部クラウドで実行し、その解析結果を受け取るシステムを導入しました。

2. 攻撃者の現状

本学に送信される SPAM やフィッシングメール、Virus 付きメールにはどのような背景があるのでしょうか。実際に送信する人に会うことは難しいため想像になりますが、送信することでなんらかの利益（または本学に恨みがあり損失を願う）が発生することは間違いありません。攻撃者側は、SPAM の場合には、SPAM に書かれている物品を購入することでお金が入ったり、フィッシングメールの場合には ID/パスワードやクレジットカード番号が入手でき、Virus 付きメールの場合には PC 内の情報を盗んだり PC 自体を乗っ取りすることが目的とされます。これらはもちろん一例であり、その他、お金以外の利益が目的の場合もあるかもしれません。さらに、攻撃側が不特定多数ではなく、ある一定の人を狙って行った場合には、標的型攻撃と呼ばれます。

現在の攻撃側は、作成したプログラムやシステムなどを、自分だけで利用するのではなく、それぞれの攻撃行為をサービスとして（悪意ある）他のユーザに提供し利益を得ています。さらに、防御側のシステムと同様のものを手元に準備し、その仕様等を解析することで、サービスの質の向上を行っています。もちろん、お仕事として行っているため、ユーザサービスも行っており、攻撃の実行する前には、成功確率の向上のため、ブラックリストに載ってないサイトを準備し、Antivirus が反応しないことを確認します。

攻撃側にとって必要な資源が必要な時に利用でき、これも一種のクラウド利用といえるかもしれません。

3. 実際に守るためには

では、どうやって、自分の身を守ればよいのでしょうか。攻撃が広く行われている場合には、だれかがその攻撃に気が付いて、その情報をインターネットに公開することや、Virus 対策ベンダーが攻撃に気が付き、対応することが考えられます。攻撃開始からの時間の経過は、情報の流通という点で、ユーザには有利になり、攻撃者には不利となります。メールの場合には、おかしいなと感じる添付メールは処理を翌日に回し、その時に Virus 検査やメール本文を検索することを行えば、被害に会う可能性を低減することが可能です。また、情報の裏付けを取るという観点から、情報元の正規サイトに必ずアクセスし、内容を確認してから作業を開始してもよいと思います。（例えば、あるサイトで情報漏洩が発生したのならば、メールのリンクからではなく、その情報を検索して、内容を確認してからアクセスすることはセキュリティの観点から有用です。）

まずは、自分の身を守るためには、慌てて対応するのではなく、

- ・検索等を利用し、届いたメール以外の方法で情報確認すること
- ・メールのリンクは利用しないこと
（メールソフトは TEXT 形式で利用すること）
- ・添付ファイルの実行は注意すること

を意識してください。

4. 更に身を守るために

実際に自分に届いている添付ファイルや Download したファイルが安全かどうか確認したことがあると思います。このような場合には、どうすればよいのでしょうか。

手元にあるファイルの安全性を調べる方法として有効な方法は、VirusTotal 等のマルウェア共有サイトを利用してその危険度を判断することです。これらのサイトでは、手元のファイルを UPLOAD することで、そのファイルを複数の Antivirus ソフトで検査を行ったり、実際に実行しその時の特徴をまとめてその結果を返したり、してくれます。

ただし、これらのサイトを利用するときに、注意することが2点あります。

- ・パスワード付き ZIP 等の暗号化されたファイルは解析することができない
- ・UPLOAD されたファイルは他のユーザが DOWNLOAD できる

特に、2点目の他人がファイルを DOWNLOAD できることは注意が必要で、機密を含む(可能性がある)ファイルを検査することは絶対にしないでください。

それでも、標的型攻撃を受けた場合など、機密を含むかわからないが、そのファイルの危険性を判断したい場合には、そのファイルの Hash 値と呼ばれるものが利用できるサイトもあります。その場合には、ファイル自体を提出する検査ではなく、過去の検査状況を確認することができます。

Hash 値とは、そのファイル内部のビットの並びに応じて生成される文字列であり、方式(生成される文字列の長さが異なる)により複数の方式 (MD5,SHA-1,SHA-256 など) があります。Hash 値は、Windows ではコマンドラインから

```
>certutil -hashfile ファイル名 方式
```

で計算できます。具体的には、ファイル (例えば、情報システム.docx) があるフォルダで SHA-1 を計算する場合には、

```
C:¥Users¥okino¥Documents>certutil -  
hashfile 情報システム.docx SHA1  
SHA1 ハッシュ (対象 情報システム.docx):  
edd712127d3f7b1c435c347f3a5a9d9c34c  
7bcb2  
certutil: -hashfile コマンドは正常に完了  
しました。
```

と出力されます。Mac の場合には、

```
$shasuum -a 1 ファイル名
```

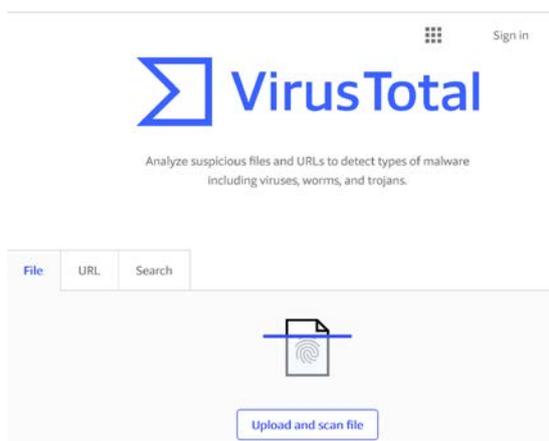
で計算することができます。

HASH 値が同値のファイルを作ることはかなり難しいことが知られています。そのため、普通の利用においては HASH 値が同値であるファイルは、同じ内容と判断して構いません。

5.VirusTotal の利用

具体的なクラウド利用の事例として、VirusTotal を利用した場合の説明を行います。

<https://www.virustotal.com>



今回利用するファイルは、「1.メールを取り巻く環境」で説明した新しい検査にて怪しいと判断された2018/4/13夜に学内に配送されたメールに添付されていたファイルである DOCXXXXXXXX.doc(Xの部分は、ランダムな数字)を利用しました。

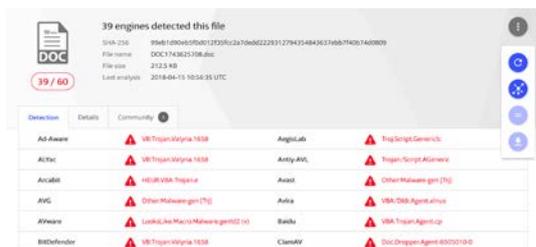
このファイルの Hash 値は

SHA1:

878f05a0ddc78db92cd844b5d13be93e7b25f343
でした。

この Word ファイルは実行コードを含み、実行した場合には、Virus 本体を海外にあるサイトから DOWNLOAD します。

このファイルを VirusTotal に upload し、検査したら、2018/4/15 19:56 現在で 60 種類の Antivirus ソフトのうち 39 種類で悪性と判断されました。



また、ファイルに機密を含む可能性がある場合など、UPLOAD をためらうときには、Search に HASH 値を入力することで、過去に同一の HASH 値を持ったファイルの検査結果を確認することができます。



HASH 値が同値ということはファイルの文字列の並びが同じであると判断して問題ないので、誰かが UPLOAD した手元と同一ファイルの検査結果となります。

自分宛のファイルと同一のものがあるということは怪しいといえるかもしれません。また、だれも UPLOAD していない場合(同一の HASH 値がない場合)には、なしと表示されます。

さらに VirusTotal ではウイルス配布等に利用された URL 等の検索もできます。

6.gred の利用

もう一つ別のサイトとして、ワンクリック詐欺サイトやフィッシングサイトであることを判断する gred を利用した場合を説明します。

<http://check.gred.jp/>



gred は、検査したいと思う URL を入力すると、そのサイトに実際にアクセスし、そのサイトを解析することで、ワンクリック詐欺サイトやフィッシングサイトの可能性を判断します。

今回、調査するサイトは、本学では 2018/4/13 に配送された Apple ID のフィッシングメールの URL を利用します。このメールは HTML 形式では、以下のように表示されました。

お客様のApple ID が、ウェブブラウザから iCloud へのサインインに使用されました。
日付と時間: 2018年4月13日 14:57 JST
のブラウザ: Microsoft Edge
オペレーティングシステム: Windows 10 IoT Enterprise
IP: 220.38.268.190 (岐阜)
上記が問題でない場合は、このメールを無視してください。
あなたのアカウントの安全性を守るために、セキュリティ質問を再設定して頂く必要があります。再設定することができません。
この問題を解決するには [こちら](#)
今後ともよろしくお願致します。
Apple サポートセンター

本メール中の「この問題を解決するにはこちら」をクリックすると、次のサイトが表示されます。



このページは、Apple のページを模して作成されていますが、本当の Apple のページとは異なり、ID と Password を盗むために攻撃者が準備したページです。

実際の動作は、メールのリンクをクリックすると、まずは、メール中に記載された URL にアクセスします。その後、ユーザに情報を入力させるフィッシングサイト本体である `http://securityprotection-support-apple-apple.com/` に飛ばされます。

実際に、メールのリンク先を確認するには、メールを TEXT 形式で表示します。するとクリックするとアクセス URL が分ります。

IP: 220.38.268.190 (岐阜)
上記が問題でない場合は、このメールを無視してください。
あなたのアカウントの安全性を守るために、セキュリティ質問を再設定して頂くことが、ワード及び元のセキュリティ情報を知っているとしても、それを使用することができません。
この問題を解決するには <http://gdr3-support-redirect-apple.com/> はこちら
今後ともよろしくお願致します。
Apple サポートセンター

今回のメールは、

http://gdr3-support-redirect-apple.com/ ということが確認できました。ユーザが文字列を確認しても間違えるように、support-redirect-apple.com と本当のドメインと似たドメインを利用しています。またフィッシングサイト自体も support-appleid-apple.com と本当のドメインと似ていることがわかります。

では、メールで届いているこの URL が本当に安全であるかを確認するために、gred を利用してみましょう。

gred のページに http://gdr3-support-redirect-apple.com/ を入力し、Check をクリックすると、ページに実際にアクセスし、内容を解析して、危険性が判断されます。今回の検査では、

「このウェブサイトは危険な可能性があります。

Apple Phishing」と判断されました。



7. まとめ

現在、攻撃者はそのパワーを集約し、日々、その能力は向上しています。その中で、私たちがネットワークを利用するうえで必要なことは、いかに安全にいろいろなクラウドサービスを利用するかにかかっています。

適切にクラウドサービスを利用することで、より安心してネットワークにアクセスすることができます。

今回は、本学のセキュリティ向上のために利用しているクラウドサービスと、個人がネットワークを安全に利用するために使えるサイトを紹介しました。今回、紹介したサイトをより安全なネットワーク利用のために活用ください。また、これらのサイトを利用して、まったく検出されないようなファイルや極端に検出数が少ないことなどがあつた場合には、標的型等の高度な攻撃の可能性もありますので、総合情報基盤センターまで相談してください。

最後に、注意していただきたいことがあります。これ以外にもいろいろな利用価値の高いサイトがありますが、利用時には、ただ闇雲にクラウドサービスを利用するのではなく、自分から提供してよい情報かを確認したうえで、それらの情報が半永久的に蓄積されることを忘れずに利用してください。相手側に蓄積された情報がどのように利用されるかは自分ではコントロールできないことを覚えておいて下さい。