マルウェア取扱い
ヒヤリハットQUIZ

2020/10/28 MWS企画セッション①

荒木 粧子（株式会社ソリトンシステムズ）

※本資料に記載の内容は所属企業・団体とは関係ありません。

Q1：悪性サイトURLの受け渡し

悪性サイトのリストを部署内で情報連携する際、
なるべく使いやすく、かつ、元のURLそのままで
提供すべきと考え、ExcelにURLを列挙して受け渡した

A：OK

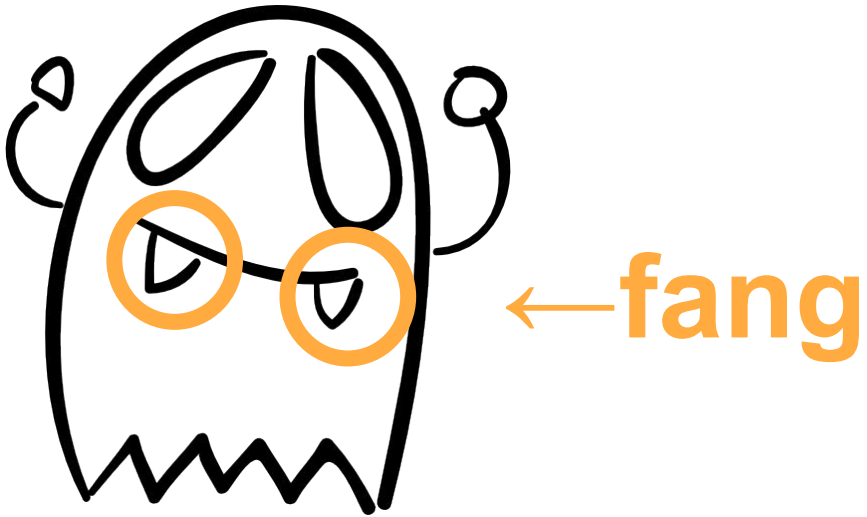
B：NG

Q1の答え

B：NG

URLをそのままExcelに記載するとリンク化され、うっかりクリックしてアクセスする事故につながります。

無害化（Defang（デファング））しましょう。



Icons made by Freepik from www.flaticon.com

Defang（デファング）例

Original	Defang
https://	https[:]//, hxxps://
www.iwsec.org	www.iwsec[.]org
192.168.0.1	192.168.0[.]1
test@test.com	test[at]test.com

参考）https://isc.sans.edu/forums/diary/Defang+all+the+things/22744/
https://ninoseki.github.io/2018/11/07/ioc-extraction-techniques.html

Q2：古いフリーソフトの調査

調査のために古いバージョンのフリーウェアを
ダウンロードする必要があったので、
G〇〇GLEで検索してヒットしたページから入手した

A：OK

B：NG

Q2の答え

B:NG

フリーウェアにマルウェアが仕込まれ公開されるケースも増えています。

信頼できるサイトから入手し、ウイルスチェックしたうえで調査環境でのみ利用しましょう…

信頼できるサイト

- 開発者のサイト
- 窓〇杜
- VECT〇R

…実は大変難しいので、感染してもOKな解析端末で調査し、業務端末では行わないよう配慮するのが良いです。

Q3：ウイルス対策ソフトによる駆除

マルウェア解析環境でマルウェアを動作させた後、
停止させていたウイルス対策ソフトを起動してマルウェアを駆除した。「駆除完了」と表示されたので、環境がクリーンになったと判断できる。

A：OK

B：NG

Q3の答え

B：NG

ウイルス対策ソフトで「駆除完了」となっても駆除されていないケースもあるので要注意。

解析環境はベース環境を作ってリフレッシュ（再構築）を基本とするのがおすすめ。

参考）https://isc.sans.edu/forums/diary/Antivirus+Multiple+Detections/26134/

ヒヤリハットQUIZ 終わり