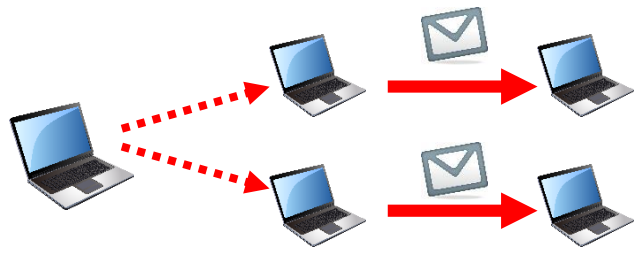
標的型攻撃とその対策

ソコ通信3月号

今回は昨年からマスコミで度々取り上げられるようになった「標的型攻撃」について特集します。

「標的型攻撃」はPCをウイルスに感染させ、外部からPCを遠隔操作して内部情報を窃取する諜報活動のこと。
2015年は６月に「標的型攻撃」による日本年金機構の情報漏えいが大きく報じられました。

標的型攻撃のよく知られている手口として、業務に関連するような内容のメールをターゲットに送り付けることによってメールを開封させ、「添付ファイルを開かせる」というものがあります。
不特定多数の対象にばらまかれる通常の迷惑メールとは異なり、攻撃者が「その組織に特有の業務を把握・想定して攻撃を仕掛けてくる」という特徴があります。
そのため、メールの内容も「実際の業務でやりとりされるものと非常によく似ている」場合が多く、つい添付ファイルを開いてしまうのです。
以前は省庁や大企業が狙われてきましたが、最近では地方自治体や中小企業もターゲットになってきました。



<標的型攻撃メールの特徴>

攻撃者の目的	・特定の組織の情報搾取 ・システムの妨害
言語	日本語
件名	自分に関係がありそうな用件
本文	・関心事 ・用件の説明が適切
送信者	官公庁、大企業を装う
添付ファイル	・PDFファイル ・Wordファイル
感染後のPCの症状	特に変わらない

調査
- 特定の企業や個人の情報を収集

感染侵入
- 標的に対し偽装メールなどを送付する

拡散拡大
- 感染したPCが遠隔操作され、感染を拡大。

情報奪取
- 通常のWebアクセスに紛れて、機密情報を奪取

発行日：2016.3.1
通算第51号

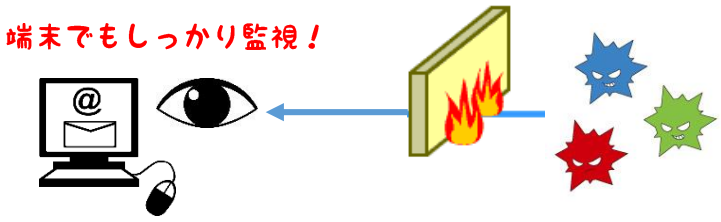
どんな人にもどんな時もどんな所にも
ソコロに出逢えた人にソコロのココロを届けます。

従来の対策の限界

多くの企業で行われている一般的なセキュリティ対策として、「ウイルス対策ソフトの定義ファイルを最新の状態にする」「各種ソフトウエアのアップデートを行う」という方法が挙げられるでしょう。これらは現在も変わらず必要ですが、「これだけでは防げない」というのが現状なのです。つまり、ウイルス対策ソフトや各種のソフトウエアが対応する前に、攻撃が完了してしまうのです。
「攻撃は受けるもの」「社内にある情報は外部に送信されてしまうもの」という前提で考える必要があるのです。

推奨する対策

- UTM（統合脅威管理）での通信の出口(入口)対策
- 端末でのウイルス対策
  特に端末でのウイルス対策は、「サンドボックス(砂場)」や「ヒューリスティック（未知のウイルス検知)」機能を提供する製品の導入をお勧め



※　サンドボックスとは、疑わしいメールを受け取った場合、仮想環境でメールを開封、疑わしい場合は隔離・削除・通報など対応を行う。
※　ヒューリスティックとは、過去の経験から、ウイルスソフトの振る舞いを参考に疑わしいと思われる動きをした場合、隔離・削除・通報など対応を行う。
※　UTMとは、ファイアウォール・ゲートウェイ・進入検知・進入防御・Webフィルタリング・URLフィルタリング・ウイルス・迷惑メールチェックなどをする機能を搭載した統合的なセキュリティ装置

まとめ

- 標的型攻撃メールでは、「添付ファイルを開く」または「本文のリンクをクリックする」ことにより、ウイルスに感染する。
- ウイルスに感染すると、コンピューターの遠隔操作などにより、情報を盗み取られてしまう。また、ネットワーク伝いに他のコンピューターにも侵入される可能性がある。
- 大企業だけでなく、中小企業も攻撃の対象になる。
- 標的型攻撃メールを全て見分けるのは、非常に難しい。「情報は流出するもの」という前提で対策を考える必要がある。

～セミナーのお知らせ～

＊1 時間程度の講習です

ホームページ作成

create HoPe

簡単・楽々・知識不要！

①ホームページを始めたい…でも知識がない！と、お困りの方いらっしゃいませんか？

当講習会では、ほとんどの操作はマウス操作で行える！クリエイトホープを使用します。

日時　３月　16 日(水) 19:00～　場所：益 田 本 社
　　３月　17 日(木) 19:00～　場所：浜田営業所

※受講料は無料ですが、テキスト代が 540 円(税込)必要となります。

ビジネスセミナー

受講料：無料
＊可能であれば、パソコンをご持参ください

日時　３月　９日(水) 16:00～　Office365 ハンズオンセミナー ～メール編
　　３月　23 日(水) 16:00～　Office365 ハンズオンセミナー ～グループウエアとデータ共有

お問合せ・お申込み ⇨ ■各セミナー　ソコロ益田本社へ　☎ 0856-22-5172　皆様のご参加心よりお待ちしております。

技術情報

LINE ～クローンの逆襲～

便利に
安全に
楽しもう

一連の某有名タレントとミュージシャンの不倫騒動で、LINE の会話の情報の流出経路が話題になりました。
なかでも有力視されているのがミュージシャンの『クローン iPhone』を何者かが入手していたのではないかという説です。
もともと LINE は情報を守るため、登録した１台のスマホからしか、やりとりを見られない仕組みになっています。
ところが、iPhone の中身を丸ごとバックアップして別の iPhone に移し替えると、新旧両方の端末からやりとりが見られていました。
これが「クローン iPhone」と呼ばれる抜け穴です。

＊クローン iPhone・・・iTunes のバックアップ機能を使用し、
iPhone を複製した iPhone のこと

そうした中、LINE 社は 2016 年 2 月 22 日にリリースされた iPhone 版アプリの最新版では、複数の iPhone 端末から同一アカウントにアクセスすることを不可能にしたと発表しました 。

LINE 社によると、最新版にしても、過去に既につくってしまったクローンからは、やりとりを引き続き見ることができるといいます。
個人情報を守る対策はしっかりしましょう。

LINE 覗き見対策

- 端末を放置しない
- iPhone と LINE にロック設定
  【設定】→【プライバシー管理】→「パスコードロック」をオン
- LINE のパスワード・PIN コードを変える
- ログイン許可をオフ

編集長のつぶやき。

たまには歩こうと思い、出先から徒歩での帰り道。
カワイイ娘に声をかけられました。
「チョッと…よろしいですか?」
「おっ!!」
色めき立つ私。アラフォーのラインが見えてきた所帯持ちのオトコにとっては、若い女性に声をかけられるなんて皆既日食よりも希な出来事です。
ですがよくよく話を聞いてみると、どうやら私に神の教えを説きたい様子。
まだまだ俗世での快楽に未練があるので、素晴らしい神の世界へのお誘いを丁重にお断りしました。
勧誘でもなければ、こんなおじさんに若い子が声をかけるわけありませんよね。
一瞬でもときめいた自分が憎いです(+O+)
あのガッツがあれば、いい営業になれるんだろうけどな。

今月の名言

無宗教…世界中の偉大な信仰の中で、いちばん重要な信仰。

（アメリカの作家、ジャーナリスト）アンブローズ・ビアス

私たちソコロは
「コンピューターやネットワークで元気になるビジネスを創っていく」をモットーに、企業様や個人様が求める様々な IT 技術を提供・サポートしております。

■トラブル対応・診断料
■個人講習(1 時間/内容要相談)

¥3,240～（税込）

まずは
ご相談を！

【お問合せ・お申込み先】
株式会社 ソコロシステムズ
FAX 0856-22-5165（共通）
■益田本社　益田市三宅町 1-19
電話 0856-22-5172
http://www.socorro.co.jp/
■浜田営業所　浜田市相生町 3905
電話 0855-28-7767
http://socorrohamada.createhope.jp/