PCフォーラム

ＪＡ水郷つくばパソコン研究会会報　　2022 年 7 月号
編集・発行 JA 水郷つくばパソコン研究会
事務局：ＪＡ水郷つくば　営農部営農企画課
住所：土浦市田中１－１－４　電話：823-7001
ホームページ　https://www.dappe.com/
ブログ　http://dappe.chicappa.jp/japc/
メールアドレス　japc2@dappe.com
FACEBOOK　JA 水郷つくばパソコン研究会
Instagram　#JA 水郷つくばパソコン研究会

定例会予定　学習のテーマ:パソコン簿記、エクセル、スマホ、SNS

◆7 月 05 日　12 日定例会　19 日 WEB、
26 日　PC フォーラム発行、農業簿記講座

◆8 月 2 日、9 日 WEB、16 日休み、23 日定例会、
28 日 PC フォーラム発行、農業簿記講座など

※定例会予定は変更になる場合があります。HP、SNS 等で連絡します。

定例会お知らせ

皆さん、毎日暑い日が続きますがいかがお過ごしですか。この PC フォーラムを発行する前日になって梅雨が明けたというニュースが飛び込んできました。連日 35 度を超す日々が続いたのではたまったものではありませんね。どうぞお体に気を付けて仕事頑張ってください。

さて、役員会で検討したところ 7 月から隔週で定例会を再開することとなりました。質問等ある方はご参加ください。その場合は、ラインやメール等でご連絡いただけるとありがたいです。この PC フォーラムの定例会予定でご確認ください。

同じく青色申告をパソコンで行いたい方の講座を始めました。既会員の方でも希望者がおりましたら、最終週のPCフォーラム発行の時間に並行して行っていますので申し込んでください。今月は 4 ページに増刷しました。定例会で使ったノートパソコン処分もご覧ください。新品 SSD を取り付けメモリー増設し再調整しました、サブ機などにご検討ください。

今月の特集

「なりすましメール」から数億円の被害まで

（ZDNetJAPANより）

サイバー攻撃は増加の一途をたどっており、大きな被害をもたらしているのが「EAC」(Email Account Compromise：電子メールアカウント侵害）や「BEC」(Business Email Compromise：ビジネスメール詐欺）といったメール詐欺・攻撃です。

なりすましメールの手口

①表示名 (Display Name)詐欺

「from」フィールドの表示名は正規の名前だが、
実際のアドレスは攻撃者のもの

②タイポスクワッティング

類似ドメインを装ったドメイン
例) yamadashoji.co.jp -> yamadash0ji.co.jp

実は、これらの攻撃が世の中で大きく騒がれているランサムウェア以上に多額の被害をもたらしています。

メール詐欺・攻撃では、手口自体は非常に単純です。

例えば、数万ドル規模の金銭を詐取したと言われる攻撃者グループ「TA2519」が展開したBECでは、受け取った人物の興味を引きそうな話題を盛り込んだメールを送りつけてマルウェアを仕込み、そのマルウェアを用いてIDとパスワードといった、ユーザーの認証情報を盗み取り、その後は、盗んだ認証情報を用いて本人になりすまし、頻繁にやりとりしている同僚や上司、取引先に偽のメールを送り、金銭を支払うよう仕向けました。

既に大半の認証システムやメールシステムでは、セキュリティ対策として数回続けて認証に失敗すると不正アクセスと見なし、アカウントをロックする仕組みを備えているので、攻撃者が総当たり攻撃でアカウントの侵害を試みても、成功率は26%程度です。これに対し、フィッシングなどでアカウント情報の詐取を試みた場合、成功率は65%に高まるというのです。

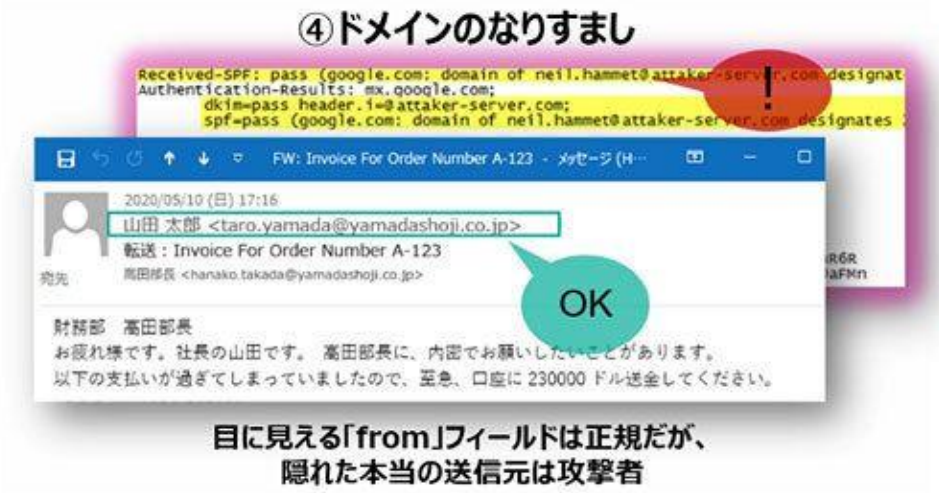
では、なぜメール詐欺・攻撃の成功率は高いのでしょうか？ユーザーをだまし、本物のメッセージらしく見せかける幾つかのなりすまし手法が使われていることが大きな理由と考えられます。主な偽装手法を説明します。

表示名（Display Name）詐欺

メールを受信すると、メールアドレスとともに名前が表示されますが、その名前がメールアドレスを保有している人物の名前であることに疑いを抱かない人は多いのですが、実際には、メールの仕様上、任意の名前を定義できてしまうのです。

これは、通常の利用で「会社名・部署名を表示したい」といった場合に便利な機能なのですが、サイバー攻撃者はこれを悪用し、なりすましメールの送信元であるメールアドレスとは全く別の名前を受信側に表示させ、相手をだますことに使っています。例えば、「TA2520」と呼ばれる攻撃グループが2020年のBEC詐欺では、この表示名を偽装してある会社の経営幹部になりすまし、「企業買収に必要な資金だから」と、従業員に送金を指示して多額の金銭を詐取したのです。

表示名詐欺は、メーラーの表示やヘッダーを確認すれば見破ることのできる非常に単純な手口ですが、いまだに多く使われています。それでもユーザーが焦っていたり、大量のメールを処理しなければならなかったりした場合には見落とすこともあるのです。サイバー攻撃者は、「たとえ受信者の0.01%でもいいから、一定数引っかかればいい」という考え方をするのです。それでECサイトや金融機関、クレジットカード会社などに見せかけた大量のなりすましメールをいまだに送り続けているというわけです。



タイポスクワッティング、類似ドメイン

タイポスクワッティングは、なりすましの対象によく似たドメイン名を使ってメールを送り、受け手側が見間違いをするように誘う手口です。例えば、本来は「mail@zdnet.co.jp」というメールアドレスから送られてくるはずのメールを、「mail@zdmet.co.jp」というドメインから送りつけるイメージ。メール詐欺・攻撃で送信元を偽装するためだけでなく、本文にこうしたURLを記して、フィッシングサイトや悪意あるサイトへの誘導を促す手口としてもよく使われています。

なお、前述の「zdmet」の例なら、コンピューターで利用している文字フォントにもよるが、一見しただけで「n」と「m」の違いに気付ける人も多いでしょうが、実際

の手口には、「o」（オー）を「0」（数字のゼロ）に、「l」（エル）を「1」（数字のイチ）に置き換えるなど、非常に見分けの付きにくい文字列が使われがちなのです。

「Reply-to」詐欺

メールの仕様では、返信メールの宛先を指定する「Reply-to」という機能が用意されています。本来はメーリングリストなどで返信先を指定するために使われるものですが、「Reply-to」詐欺はこれを悪用し、画面に表示されている送信元に返信したつもりが、実際には攻撃者が用意した別のメールアドレスに送られてしまうのです。これは、何度かやりとりを交わして標的を信用させた上で、送金を指示するBECでよく使われる手口です。

より巧妙な「ドメインのなりすまし」

ここまで紹介した3つの手口に加え、ユーザーが見抜くことが最も難しい手口が「ドメインのなりすまし」です。

この手法では、攻撃者がメールアプリに表示される送信者のメールアドレス（header-fromフィールド）を改ざんし、いつもやりとりをしている信頼しているメールアドレスを記載する。実は、メールアプリに表示されるメールアドレスは、簡単に改ざんできるのです。

例えば、ロシアのサイバー犯罪集団である「Cosmic Lynx」は、この手法を用いて標的とする企業の経営陣になりすまし、M&A（合併・買収）絡みのテーマを用いたビジネスメール詐欺によって合計200以上の企業を狙い、それぞれから平均して127万ドルの大金を窃取していました。

こうした手口に対処するには、まず受信者一人一人がさまざまな手口の存在を理解することが第一歩で、「もしかするとだまされる可能性があるかもしれない」という意識を常に持つことが重要です。　　（みやざき）

★★　研究会の定例会で使用したノートパソコンの販売　★★

①LENOVO　B590

￥22，000

本体、ACアダプタ、バッテリー

②LENOVO　Z575

￥22，000

本体、ACアダプタ、バッテリー

①

Celeron Dual-Core 1005M(Ivy Bridge) 1.9GHz/2コア
画面サイズ　15.6 型(インチ)
解像度 WXGA (1366x768)ワイド画面
メモリ容量 8GB　メモリ規格　　DDR3 PC3-12800
メモリスロット(空き) 2(0)
SSD 256GB m.2 SATA
詳細スペック
OS　Windows 10 プロ64bit
ドライブ規格　DVD±R/±RW/RAM/±RDL
ビデオチップ　Intel HD Graphics ビデオメモリ　　1740MB
その他Webカメラ HDMI端子 VGA端子 テンキー USB3.0 SDカードスロット
ネットワーク
無線LAN　　IEEE802.11b (11Mbps),IEEE802.11g (54Mbps),IEEE802.11n
LAN 100/1000Mbps
サイズ・重量 重量　2.5 kg 幅x高さx奥行 378x33.4x252 mm
カラー カラー ブラック

SSD新品にしましたのでサクサク動いています。
ソフトウェア；MS　office　2021pro　、Xnview、リサイズ超簡単proなど

②
AMD Quad-Core A8-3520M　1.6GHz/4コア
画面サイズ　15.6　型(インチ)
解像度　WXGA (1366x768)　ワイド画面
メモリ容量　8GB　メモリ規格 DDR3 PC3-10600
メモリスロット(空き)　2(0)
SSD 480GB
詳細スペック
OS　Windows 10 pro 64bit
ドライブ規格　DVD±R/±RW/RAM/±RDL
ビデオチップ　AMD Radeon HD 6620G　ビデオメモリ　2048MB
その他　Webカメラ　HDMI端子　Bluetooth eSATA　テンキー
ネットワーク
無線LAN　IEEE802.11b (11Mbps),IEEE802.11g (54Mbps),IEEE802.11n
LAN　10/100Mbps
サイズ･重量　重量　2.6 kg　幅x高さx奥行 376x34.5x250 mm
カラー　カラー ガンメタルグレー

SSD新品にしました。HDD(ハードディスクドライブ)よりも高速です。
ソフト類は①と同様です。
SSDにつきましては、JA水郷つくば広報紙、パソコン研究会の記事6月号をご覧ください。

サブ機、3台目などにいかがですか。パソコン教室で現物確認できますのでお問い合わせください。
事務局電話　営農部TEL　、メール　japc2@dappe.com　小林まで

※なお、売約済みになってしまった場合はご容赦ください。

写真　(みやざき)　(こばやし)

■編集後記

今月の特集記事はいかがでしたか？気を付けましょう。以前からドメインなどのお話はしてきましたが、もっと勉強しましょう。研究会で使用していたノートパソコン、ディスプレイ等、この次第2弾もありますのでよろしくお願いします。暑さに負けずに定例会ご参加ください。ウクライナが早く集結しますように。

(みや、こば)