ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●件名「ご注文の確認」･･･ネットバンキングユーザを狙うマルウェア添付メールが確認

http://news.mynavi.jp/news/2015/09/11/135/
http://blog.trendmicro.co.jp/archives/12206

このニュースをザックリ言うと･･･

- 9月9日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、ネットバンキングを狙う新たなマルウェア添付メールが確認されたとして、同社ブログにて警告が出ています。

- メールは、件名が「ご注文の確認」という文字列を含むもので、PDFファイルに偽装したアイコンを持つマルウェア「WERDLOD」がzip形式で添付されています。

- 同社によれば、WERDLODに感染したと見られる国内PCは8月に約130台検出されていましたが、9月に入り、3日～7日の4日間だけで新たに150台以上の検出を確認したとのことです。

AUS便りからの所感等

- 実際にはWERDLOD自体は2014年12月から確認されており、メールや添付ファイルの形式を微妙に変えたものに過ぎないようですが、それでも数日間で急激に感染件数が増えるという現象がみられています。

- 幸いにも現時点でメールの内容は稚拙なものではありますが、今後感染率を上げるための工夫がなされることは容易に予想されますので、アンチウイルス・UTMによる防御は欠かさずに行う必要があるでしょう。

マイナビニュース

ネットバンキングを狙う新たなスパム、メールタイトルは「ご注文の確認」

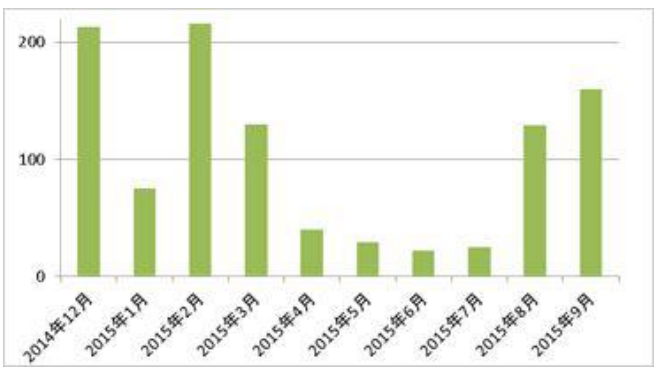
[2015/09/11]

トレンドマイクロは9月9日、同社のセキュリティブログにおいて、ネットバンキングを狙う新たなマルウェアスパム「ご注文の確認」を確認したと報告した。

2014年12月以降、有名ネット通販サイトからのメールを偽装し、オンライン銀行詐欺ツール「WERDLOD」を拡散しようとするマルウェアスパムが観測されている。トレンドマイクロでは、2015年9月に入りこのマルウェアスパムが、「ご注文の確認」という文字列を含む件名で、別の有名ネット通販サイトを偽装する新たな手口に変化したことを確認した。

PDFアイコン偽装を施した不正プログラムファイルの例

（アイコンはPDFファイルのものだが、拡張子が「.exe」になっている）



日本国内における「WERDLOD」の月別検出台数推移（2015年9月は 7日まで）

トレンドマイクロ セキュリティブログ
POWERED BY TrendLabs

ネットバンキングを狙う新たなマルウェアスパム「ご注文の確認」

投稿日: 2015年9月9日
脅威カテゴリ: 不正プログラム，スパムメール，サイバー犯罪
執筆: セキュリティエバンジェリスト 岡本 勝之

2014年12月以降、有名ネット通販サイトからのメールを偽装し、オンライン銀行詐欺ツール「WERDLOD」を拡散しようとするマルウェアスパムが観測されています。トレンドマイクロでは、2015年9月に入りこのマルウェアスパムが、「ご注文の確認」という文字列を含む件名で、別の有名ネット通販サイトを偽装する新たな手口に変化したことを確認しました。

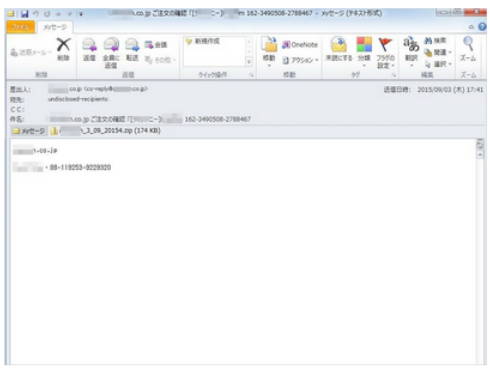


図1: 新たに確認された「ご注文の確認」スパムの例

■ネットバンキングを狙う新たなマルウェアスパム

本ブログでは、「WERDLOD」を拡散するマルウェアスパムとそのネットバンキングを狙う手口について、以下の記事によりその詳細を明らかにしてまいりました。

●千趣会、個人情報13万件が流出か･･･子会社ECサイトに不正アクセス

http://www.itmedia.co.jp/news/articles/1509/15/news123.html

このニュースをザックリ言うと･･･

- 9月15日（日本時間）、通信販売大手の千趣会より、同グループのECサイトが不正アクセスを受け、13万1096件の個人情報が流出した可能性があることが発表されました。

- 不正アクセスを受けたとされるのは、子会社のベルネージュダイレクトが運営する「ベビパラハッピーギフト」「Pre-moギフト」「TOMATOMAギフト」「ベビパラギフト」の4サイトのサーバで、サーバの管理会社が8月21日に不正アクセスの形跡を発見し、調査の末、9月3日にはベルネージュダイレクト社へ報告され、同日18時までに各サイトは利用停止の処置がとられました。

- 2012年9月20日～2015年8月26日に登録した会員21,994件とギフト送り先110,564件の氏名、住所、電話番号などが流出した恐れがあり、さらに会員情報のうち、13,713件にクレジットカード情報が含まれていたとのことです。


ITmedia ニュース

2015年09月15日 16時51分 更新

千趣会、個人情報13万件が流出か　子会社ECサイトに不正アクセス

千趣会の子会社が運営するECサイトが不正アクセスを受け、13万1096件の個人情報が流出した可能性。

[ITmedia]

千趣会は9月15日、子会社のベルネージュダイレクトが運営するECサイトが不正アクセスを受け、一部クレジットカード情報を含む13万1096件の個人情報が流出した可能性があると発表した。

ベルネージュダイレクトのトップページ

不正アクセスを受けたのは「ベビパラハッピーギフト」「Pre-moギフト」「TOMATOMAギフト」「ベビパラギフト」――の4サイトのサーバ。2012年9月20日～2015年8月26日に登録した会員2万1994人、送り先11万564件の氏名、住所、電話番号などが流出した恐れがあるという。会員情報のうち、1万3713件にクレジットカード情報が含まれているという。

AUS便りからの所感等

- 現時点での発表では具体的な不正アクセスの状況、例えば、不正アクセスが発生したとみられる正確な日時の情報が明らかにされておらず、それを把握するための何らかの機構が設置されていなかった可能性も考えられます。

- 不審なアクセス形跡の速やかかつ正確な検知により、不正アクセスの実態を正確に把握するためにも、IDSやそれを含むUTMといった機器の設置が重要となるでしょう。

●国勢調査インターネット回答用のパスワード入り用紙、無防備に郵便受けに

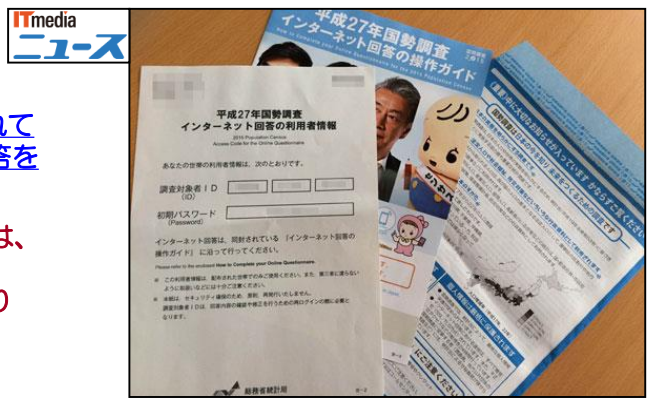
http://www.itmedia.co.jp/news/articles/1509/14/news095.html

このニュースをザックリ言うと･･･

- 今回より、PC・スマートフォンからのインターネット回答が可能になった国勢調査について、回答のためのアカウント情報が書かれた用紙が無防備に各家庭の郵便受けに投函されており、問題となりました。

- 用紙は9月10日～12日（日本時間）に、本来であれば各家庭に手渡しで渡されるとのことですが、封筒には封がされていないうえ、かつ、郵便受けに第三者が抜き取ることも可能な状態で差し込まれるケースが多発していました。

- なお、用紙に記載されたパスワードは初期アクセスのためのものであり、回答の入力に際してはパスワードの変更が要求されるため、もしパスワードが変更されてログインできないという場合は、統計局に連絡すれば、調査して対応するとのことです。


ITmedia ニュース

封筒に封はされておらず、中の紙には世帯ごとのID・初期パスワードが記されている。「第三者に渡らないよう取り扱いなどには十分ご注意ください」とも書かれている

AUS便りからの所感等

- 前述のとおり、もし誰かに初期パスワードを盗み見られていたとしても、先に回答していれば、攻撃者が後から回答を改ざんすることは理論上不可能です。

- 9月20日までにインターネット回答をしなかった場合は、26日以降従来通りの手書き調査票が配布されるとのことですが、用紙を受け取らなかった場合、もしくは受け取りながら回答しなかった場合、運悪く第三者に不正に回答されている可能性に注意し、やはり念の為に連絡・確認することを推奨致します。