proofpoint

Proofpoint Threat Report

March 2015

本レポートは、Proofpoint が注目し、お客様および一般企業に対して注意を喚起したいと考えている様々な脅威に関する情報、詳細、トレンドなどをまとめたものです。

Threat Models (手法)

システムのハッキングから人のハッキングへ

「ビジュアルハッキング」または「ショルダーサーフィン」は、人の肩越しに PC やデバイスをのぞき込んでパスワードなどを盗む手法を指す言葉です。人のプライバシーを狙う、非常に単純で直接的なやり方です。

ビジュアルハッキングは時と場所を選ばずに行えますが、オフィスでは非常に成功率が高い攻撃になります。本人を確認してから攻撃しますから、これは理想的な標的型攻撃であり、またオフィスでは公開の場所よりも人々は無防備になりがちだからです。

このローテクな攻撃手法に対抗するためには、データのプライバシーを大切にするセキュリティ環境や、自己管理の文化が必要です。

企業内の誰もがデジタル機器を利用しているにも関わらず、日々生み出され、複製され、消費される膨大なデータを守るのは、これまではー握りの IT セキュリティチームに任されていました。そのため、高度な技術を駆使して企業のネットワークやシステムを狙うハッカーに対抗するための複雑な防御ソリューションは、データセキュリティの専門家によって開発されてきました。しかし、防御技術がどんどん洗練されてきた結果、ハッカー達は新たな攻撃ポイントを見つけなければならなくなったのです。それでは、システムのハッキングから人のハッキングへのシフトは始まっているのでしょうか? それについては、もう少し様子を見る必要がありそうです。

しかし、過ちは人の常と言いますし、人間はデータセキュリティのパイプラインの中でも、最も脆弱な部分のひとつであることは確かです。最近の研究では、ビジュアルハッキングは非常に簡単に実行できることが明らかになりました。

3M が行った Visual Hacking Experiment (http://solutions.3m.com/wps/portal/3M/en_US/3MScreens_NA/Protectors/Industries/VisualHackingExperiment/?WT.mc_id=www.3Mscreens.com/visualhacking) という研究では、全米の 8 つの企業に一時雇用やパートタイムの従業員を装ってホワイトハットハッカーを送り込み、ビジュアルハッキングの手法を使って重要情報を取得しようと試みました。取得できた情報の中には、従業員リスト、顧客情報、企業財務、従業員のアカウント情報、クレデンシャル (認証情報) などが含まれていました。

この調査により、ハッキングの新しい可能性が見えて来ました。ホワイトハットハッカー達は 88%のケースで、従業員のコンピュータ画面やドキュメントから重要情報を視覚的に取得することに成功したのです。この驚くべき調査結果から、企業はこれまで以上にデータ流出のリスクに晒されているということがわかります。さらに気になることに、これらのハッキングは一般的に極めて短時間 (63%が 30 分以内) のうちに完了し、しかもほとんど気づかれなかったということです。70%の事例で、誰にも見とがめられなかったのです。

また、従業員がモバイルからアクセスする率は上がっています。公共の場から企業内へのデータアクセスが行われれば、そこでのビジュアルハッキングはほとんど追跡できません。ビジュアルハッキング以外にも、ソーシャルエンジニアリングやスピアフィッシング等の、比較的ローテクな攻撃が従業員を狙っていますし、内部関係者によるデータ流出もまた、懸念事項の一つです。

これらの脅威に対抗するためには新しい発想が必要であり、さらにはデータセキュリティとプライバシーに対する従業員からの強力なコミットメントが必要です。安全な環境を作り上げるためには、セキュリティとデータプライバシーに価値を置く企業文化を築き上げる必要があります。企業データを守ることを、従業員一人一人の責務としなければなりません。

また、安全を目指す企業は、正直さを推奨すべきです。従業員が自らの失敗を打ち明けた場合に、責めるのでは無く、褒めるくらいでなければなりません。

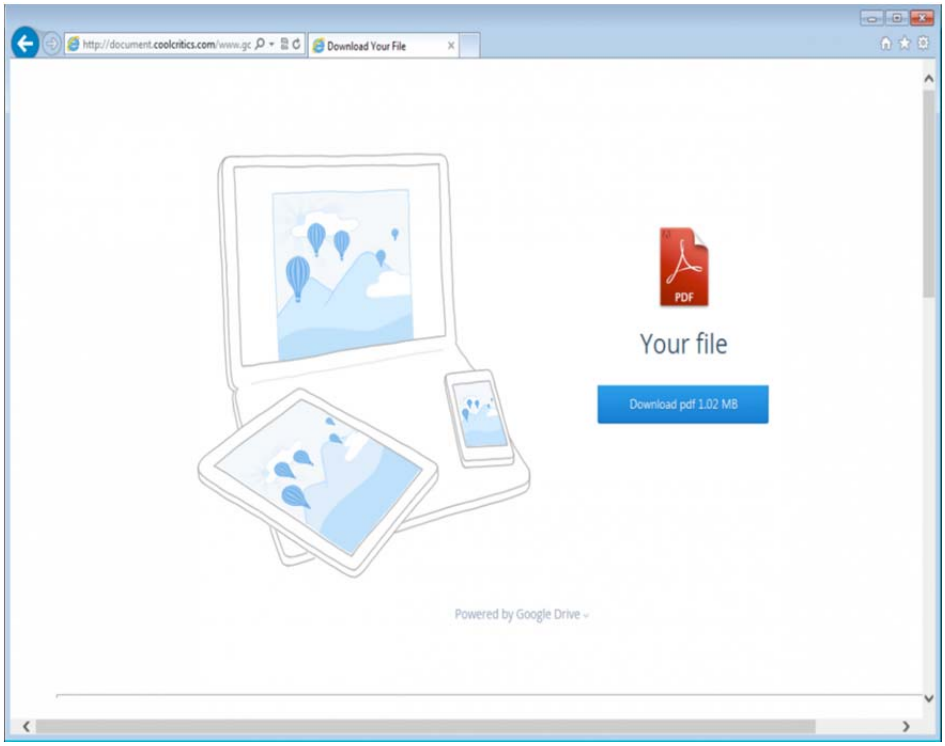
そのファイルは大丈夫?：クラウド上のドキュメントを使ったクレデンシャルフィッシング

クレデンシャル (認証情報) を狙ったフィッシング攻撃は依然としてポピュラーで、Outlook Web Access のクレデンシャルが他の Web メールのアカウントと結び着いて攻撃対象となっていることから、最近ではさらに増えています。さらに、クラウドベースのドキュメント活用が広がっていることから、犯罪者はこの新しい利用パターンをユーザーを騙す餌に使おうとしています。

Proofpoint の研究者は最近、この種の攻撃の典型的な例を解析しました。この例は、犯罪者の一部がさらに知的に進化していることも浮き彫りにしました。

Proofpoint が日々検知している E メールベースの脅威の中でも、最も多いもののひとつが Google Apps のクレデンシャルフィッシュです。Google Apps を導入している組織はこれらのタイプの攻撃に特に注意しなければなりません。

この例では、被害者を偽のログインページに誘導するのでは無く、リンクをクリックすると、あたかも本物の Google docs のドキュメント共有ページに誘導します。



このページは本物の Google サイトの完璧なコピーですが、配信のモードが違います。HTTPS ではなく、HTTP を使って配信されているのです。受信者がこの点に気がつかないと、ファイルをダウンロードしてしまうことになります。そして本物そっくりの Google のログインページが現われます。専門家で無いと見分けるのは不可能です。

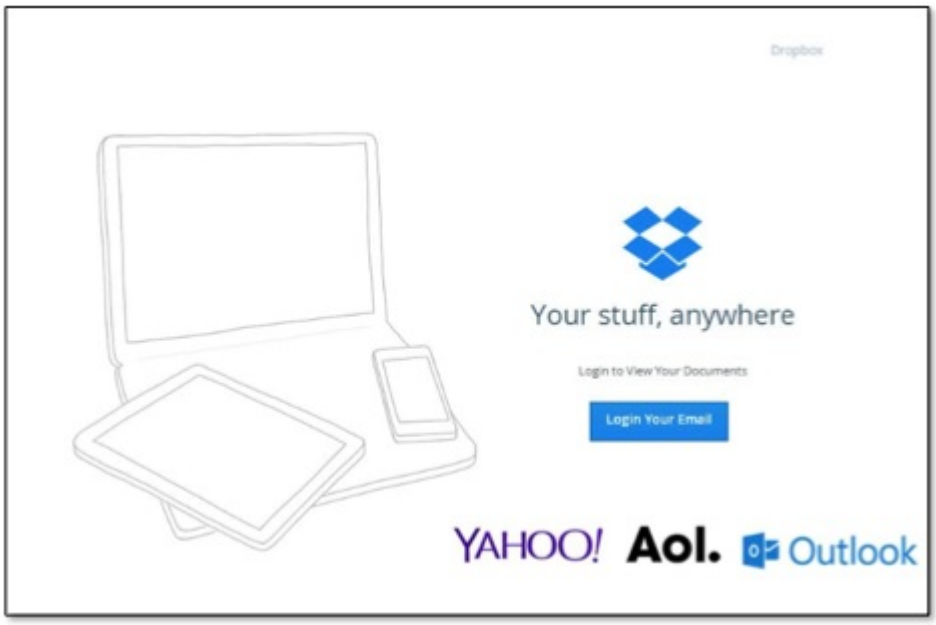
この偽のドキュメントは Yahoo、Hotmail、AOL などのその他の Web メールサービスへのログインもサポートしており、さらに「その他」も用意されているため、企業内部のクレデンシャルも集めることができます。

一般的には、こういった偽サイトはクレデンシャルを取得した後のことまで考えてはいません。しかし今回のケースでは、攻撃者はクレデンシャルを取得した後に、実際のドキュメントを表示しています。これは、ユーザーが「何か変だ」と感じて攻撃に気づくリスクを減らすためと考えられます。盗んだクレデンシャルを使う時間を稼げるわけです。

侵害された Google アカウントを使ったクレデンシャルフィッシングが有利な点は、他にもあります。被害者のコンタクトリストから入手したアドレスに対して、比較的簡単に、信憑性のある標的型フィッシングを仕掛けることができ、次の攻撃ステップのための受信者リストにも使うことができるのです。

これと似た攻撃で、偽の Dropbox ドキュメントを使って、クラウドベースのドキュメント共有サービスからクレデンシャルを取得しようとするものがあります。

ログインページは本物のように見えます:



クラウドベースのドキュメントサービスおよびアプリケーションアカウントを用いたハッキングをうまく利用すると、ハックした価値の高いメールアカウントを使った、効果的で収益の見込める新しい標的型攻撃を作り出すことができます。

クラウドベースのドキュメントを使ったクレデンシャルフィッシングは、防御システムを出し抜こうとする攻撃者達によって、今後も増えることは間違いないでしょう。

Threat News (ニュース)

Woollen Goldfish と GHOLE を使った Rocket Kitten フィッシング

「Rocket Kitten」は、イスラエルおよびヨーロッパで見られるスピアフィッシング攻撃で、マイクロソフト製品によってホストされる「GHOLE (malware)」と「(Operation) Woolen-GoldFish」が使われています。

今の所、Rocket Kitten は二つの攻撃を行ったと見られています。

GHOLE は 2011 年から活動していると言われており、トレンドマイクロによると、Rocket Kitten の悪意のある活動は、イスラエル及びヨーロッパの公的・私的組織を狙ってきたということです。GHOLE マルウェア攻撃に特有のマクロを含むファイルを解析した結果、主に防衛産業、IT セクター、政府関係機関、学術機関に関心を持っていることがわかりました。

トレンドマイクロのサイバーセキュリティスペシャリストの Bharat Mistry によると、この攻撃の注目すべき点は、攻撃の実行に必要な「洗練されたスキル」が明らかに欠けているということだそうです。「ハッカー達はもはや自分でスクリプトを書く必要はありません。販売されているツールをそのまま使えば良いのです。」

これにより、最終的には犯罪者を特定することが難しくなります。「彼らはオンラインに足跡を残さないため、追跡は難しくなります。過去のどのグループとも関係を持ちません。コード中のパターンを見つけ出さない限り、特定は難しいのです。」

こちらで詳細をご確認下さい: http://www.scmagazineuk.com/rocket-kitten-phishing-with-woollen-goldfish-ghole/article/404693/.

同じ RSA 暗号鍵が 28,000 回使われていたことが判明

あなたの家の鍵が、他の 28,000 件の家の鍵と同じものだったとしたらどうでしょうか?

ロンドン大学 Royal Holloway の研究者がインターネットをスキャンして、FREAK と呼ばれる Web セキュリティホールに対する脆弱性をもつサーバーがどれだけあるかを調べました。

FREAK は 3 月 3 日に発見された脆弱性で、攻撃者は SSL/TLS (Secure Sockets Layer/Transport Layer Security) 暗号化プロトコルを使った接続の強度を弱めることができます。これにより、暗号化通信を解読し、トラフィックの中を覗くことが容易になります。これは、広く使われているオープンソースソフトウェアで昨年見つかった一連の脆弱性につながるものです。

発見当時、インターネット上の 1/4 のホストが FREAK に対して脆弱だったと言われています。Royal Holloway の研究者は、その後も修正されていないホストがどれだけあるのかを調べようと考えたのです。

このプロジェクト (セキュアな接続を確立するために、ホストに 512bit の RSA 鍵を要求する) は、驚くべき結果をもたらしました。2,300 万台近くのホストのうち 9.7%、約 220 万台のホストが未だに 512bit 鍵を許容していたのです。(この長さの暗号鍵は、10 年以上前から安全では無いと認識されています) FREAK の危険度と、発見から数週間が経過していることを考え合わせると、この数字は大きな衝撃です。

しかし、恐らく研究者達にとってもっと衝撃的だったのは、多くのホスト (サーバーまたはその他のインターネットに接続されたデバイス) が「同じ」512bit の公開鍵を使っていたことでしょう。

こちらで詳細をご確認下さい: http://www.pcworld.com/article/2897772/researchers-find-same-rsa-encryption-key-used-28000-times.html.

Microsoft は Windows10 でパスワードを止め、生体認証に移行

Microsoft はもうすぐリリースされる Windows 10 CS でデバイスへの新しいログインオプションを提供し、パスワードを廃止したがっているようです。「Windows Hello」と呼ばれる生体認証技術は、指紋、顔、虹彩を使ってラップトップ、タブレット、スマホその他のデバイスへの不正なアクセスを阻止します。

パスワードは不便で、安全でないにも関わらず、未だに個人情報を守るための方法として広く使われています。Microsoft は、生体認証はパスワードよりも安全であると言っています。生体情報はデバイスのみで処理され、外部のサーバーに送られることはありません。

Microsoft が発表したところでは、生体情報はネットワーク認証には使われず、必要であれば生体認証を使わないことも可能だと言うことです。Microsoft の生体認証はまず、Intel の技術を使った顔のスキャンをサポートします。

こちらで詳細をご確認下さい: http://www.computerworld.com/article/2898654/microsoft-wants-to-kill-passwords-with-biometric-authentication-in-windows-10.html.

Dridex バンキングトロージャンが XML ファイルでも広がっている

Microsoft Office のマクロを使ってシステムに感染するバンキングマルウェアの Dridex は、最初はスパムメールに添付された Microsoft Word や Excel ドキュメントとしてエンドユーザーに到達します。ユーザーがドキュメントを開くと、マクロが起動し、Dridex バンキングマルウェアをひそかにダウンロードします。こうしてオンラインバンキングのクレデンシャルを盗み出し、次にそれを使って不正な取引を行います。ハッカー達はこのマルウェアを現在も強化し続けており、今では餌として XML ファイルを使ったものが出てきました。

Trustwave の研究者は先頃、ユーザーの Office ドキュメントへの信頼を悪用しようとするメッセージが、先月だけで数百通も「捕獲された」と発表しました。これらのメッセージはユーザーにマクロを有効にするようあからさまに求めており、そのため、バンキングマルウェアがダウンロードされてしまいました。不正な XML ファイルは、送金指示や支払い通知などを装ってユーザーを騙し、悪意のあるコードを実行させるために戦略的に作られています。

こちらで詳細をご確認下さい: https://threatpost.com/dridex-banking-trojan-spreading-via-macros-in-xml-files/111503.

Threat Insight Blog (ブログ)

Proofpoint のセキュリティブログである Threat Insight から、興味深い記事をピックアップしました。皆様も Threat Insight のディスカッションに是非ご参加ください。
http://www.proofpoint.com/threatinsight.

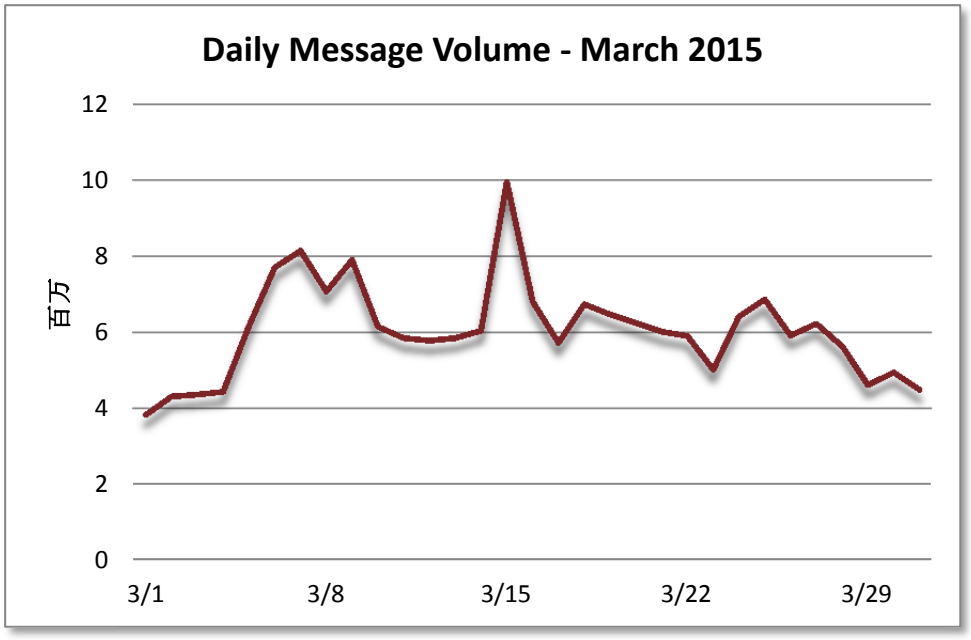
今後ブログの内容には、上の URL からアクセスしてください。ブログのセクションは、今後 Threat Model に統合されます。

Threat Trends (トレンド)

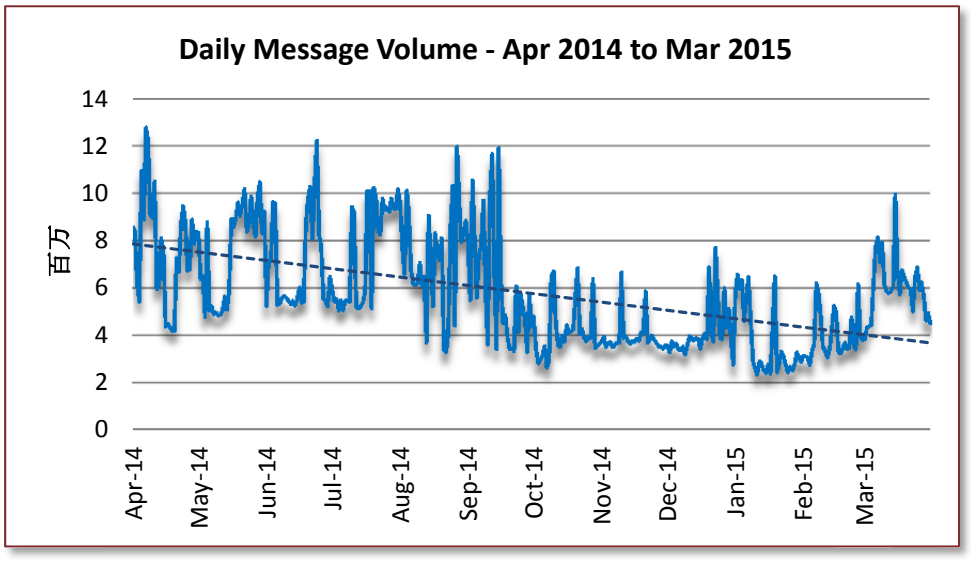
Spam Volume Trends (スパム量のトレンド)

Proofpoint では、スパム量についてハニーポットを使って追跡していますが、この値は Proofpoint のお客様からの報告ともほぼ一致します。

3 月のスパム量の推移も先月と同じ傾向でした。400 万通未満で始まり、800 万通まで上昇した後、第 1 週の終わりには 700 万通に落ちました。第 2 週はまた 800 万通から始まり、600 万まで落ちてしばらく安定しました。第 3 週の初めに突然 1,000 万通に急増し、今度は 600 万通まで急落しました。その後は月末まで穏やに上下を繰り返し、450 万通で月を終えました。



2 月と 3 月を比較すると、2013 年 12 月以来最大の増加 (54.37%) となりました。対前年比では 41.04%の減少です。



Spam Sources by Region and Country (スパム発信源)

EU は首位の座を守り、アメリカも第 2 位をキープしました。3 位にはロシアが入り、4 位は久しぶりにインドです。中国は 5 位に後退しました。

以下は、過去 6 ヶ月間のスパム配信量上位 5 カ国の表です。

		Oct '14	Nov '14	Dec '14	Jan '15	Feb '15	Mar '15
Rank	1st	China	China	EU	EU	EU	EU
	2nd	EU	EU	China	USA	USA	USA
	3rd	Russia	USA	USA	Vietnam	Vietnam	Russia
	4th	Vietnam	Russia	Russia	Argentina	Argentina	India
	5th	USA	Argentina	Vietnam	China	Russia	China

以下の表は、各国が総スパム量に占める発信量の割合を比較したものです。EU の数値はすべての加盟国を含んでおり、より正確な比較ができます。EU は全世界のスパムの 30.89%を生成しました。2 位以下の 4 ヵ国を足しても 23.02%にしかなりません。

February 2015			March 2015		
1	EU	35.30%	1	EU	30.89%
2	USA	6.67%	2	USA	9.75%
3	Vietnam	3.64%	3	Russia	5.24%
4	Argentina	2.85%	4	India	4.97%
5	Russia	2.46%	5	China	3.06%

以下は、EU 内の過去 6 ヶ月間のスパム配信量上位 5 カ国の表です。

February 2015			March 2015		
1	Germany	4.45%	1	France	3.56%
2	Spain	4.10%	2	Italy	3.28%
3	Italy	3.48%	3	Germany	3.19%
4	Romania	2.21%	4	Spain	2.54%
5	Bulgaria	1.97%	5	UK	1.62%

この他の情報については以下をご覧ください
www.proofpoint.com/threatinsight

proofpoint

Proofpoint, Inc.
892 Ross Drive, Sunnyvale, CA 94089
Tel: +1 408 517 4710
www.proofpoint.com

