proofpoint™

Proofpoint Threat Report

October 2014

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)

忘れられたサブドメインがビジネスのセキュリティリスクに

多くの企業が、社外にサービスを提供するためにサブドメインを設定していますが、サービスを停止した際にサブドメインを無効化することを忘れてしまい、そこを攻撃者に狙われることがあります。

これは、サービスプロバイダーの多くが、そのサービスにリンクされているサブドメインの所有者のチェックを適切に行っていないために起こることです。攻撃者は新しいアカウントを利用することで、これらの忘れられたサブドメインが自分の所有であることを主張し、悪用することができるのです。

使われなくなったサブドメインについては、DNS エントリを削除するかアップデートするのが通常の対応ですが、ストックホルムの Web サイトセキュリティスキャンサービスの Detecify の研究者によると、こういった見逃しはよく見られるということです。

Detecify は、サブドメインの所有権について適切な確認を行っていないサービスプロバイダーを 17 社も発見しました。多くの場合、有名なドメインだったということです。研究者によると、これによって少なくとも 200 以上の組織が影響を受けているということです。

Web サイトの所有者にとってのリスクは、そのドメインがサードパーティのサービスからリンクされた際にそこで何ができるかによります。サービスがユーザーに対して Web ページやリダ

イレクトの作成を許している場合、攻撃者はエクスプロイトを使って Web サイトのコピーを作成してログイン情報を盗むフィッシング攻撃を仕掛けることができます。
Detecify によると、この乗っ取りに対して脆弱だったいくつかのサブドメインは様々なタイプの企業のものであり、政府機関、ヘルスサービス、保険・銀行などが含まれていました。
同社では、この攻撃に対する脆弱性をチェックすることができるツール (https://redoctober.detectify.com/) を用意し、組織がサブドメインをチェックできるようにしました。このツールを使う際には、ユーザーが確実にそのドメインの所有者であることを証明しなければならないことに注意して下さい。

ハッカーはロシア・東欧の ATM を狙っている

サイバー犯罪者の狙いは、大手銀行のコンピュータシステムだけではありません。最近では、ロシア及び東欧の ATM を狙った攻撃が増えています。

セキュリティ企業の Kaspersky Lab とインターポール (国際刑事警察機構) は、犯罪者がキャッシュマシンを空にしてしまえるような悪意のあるソフトウェアを発見したと発表しました。ある金融機関から依頼されたフォレンジック調査の一貫として、ロシア及び東欧の複数の ATM をハックした際に発見したということです。(この金融機関の名前は明らかにされていません)

捜査の段階 (今年の 3 月頃) では、マルウェアはロシア及び東欧の 50 を越える ATM に感染していました。Kaspersky によると、このマルウェアはアメリカ、イスラエル、マレーシア、フランス、インド及び中国にも広がっているということです。ATM はインターネットに接続されているわけではありませんから、被害を被った銀行がそれを発表しない限り、攻撃は表面化しないと考えられます。

感染した ATM を監視していたセキュリティカメラの映像を分析すると、ハッキングは日曜日と月曜日の夜間に行われていたことがわかりました。さらに、このマルウェアは日曜日と月曜日の特定の時間にのみコマンドを受け付けることがわかりました。
犯罪者は悪意のあるソフトウェアを含んだブート可能なディスクを、システムに読み込ませていました。ATM はリブートされ、その時点でソフトウェアが読み込まれます。ATM が 2 回目にリブートさると、犯罪者は ATM のキーボードでユニークな組合せの数値を毎回打ち込み、その後、現場からオペレータに電話をかけ、違う組合せの数値を入力します。
数分後、ATM は現金の払い出しを開始します。

Kaspersky 氏は、ロシア警察に協力していると話しており、インターポールは関連国に警告を発しました。捜査は継続中です。

Threat News (ニュース)

たったひとつの犯罪者グループが 80 万人分の銀行アカウントを盗んだ方法とは

Proofpoint の新しいレポートには、サイバー犯罪インフラが洗練の度を高めていることが示されています。Proofpoint のレポートには、ロシア語圏のサイバー犯罪組織がサードパーティのサービスを活用してブラウザの脆弱性を調べたり、難読化して攻撃を隠蔽しようとしていたことが示されています。犯罪組織はまた、自らの技術を販売することにより別の収益源を確保することまで行っていました。

攻撃組織はまず、盗まれた WordPress サイトの管理者ログイン情報を発注し、その後それらのサイトに対してマルウェアをアップロードします。その後何が起こるのか、こちらからご確認下さい:

http://www.darkreading.com/cloud/how-one-criminal-hacker-group-stole-credentials-for-800000-bank-accounts/d/d-id/1316484.

Windows のゼロデイ脆弱性 (CVE-2014-4114) がロシアのスパイグループ「SandWorm」に利用されていたことが判明

iSIGHT Partners は Microsoft の協力の下、すべてのサポート中の Windows および Windows Server 2008/2012 にゼロデイ脆弱性が存在することを発見し、公表ました。この脆弱性に対するパッチは 10 月 14 日に公開されました。

SandWorm がロシア政府の意を受けて活動していたのか、捜査当局を混乱させるために行ったことなのかは別として、その活動は「政府として、あるいは国家としてのミッション」に関連づけられるように見えると、Lieberman Software の Philip Lieberman は述べています。国家の持っている「最高のリソースを使って最重要な標的を狙った」ということです。この脆弱性を狙われると、標的システム上で攻撃者のプログラムをリモートで実行されてしまいます。

狙われた組織名などはこちらでご確認下さい: http://www.tripwire.com/state-of-security/incident-detection/microsoft-windows-zero-day-exploit-sandworm-used-in-cyber-espionage-cve-2014-4114/.

金融サービス業界の最大の懸念はサイバー攻撃

米 Depository Trust & Clearing Corporation (証券保管振替機関などの持株会社) が最近発表した 2014 年第 3 四半期のレポートによると、金融関連企業の 84%が、懸念事項のトッ

プ 5 のひとつとしてサイバー攻撃をあげており、第 1 四半期の 59%から大幅に増加しています。他の 4 つは以下の通りです。

- 新規の規制 (64%)
- 地政学的リスク (62%)
- 金融取引市場の突然の移転 (43%)
- 主要な市場参加者の破綻 (32%)

また、76%の金融関連企業が、過去 1 年間のうちにシステムリスクに対抗するための検知・復旧ソリューションのために投資を行っていると述べています。
詳しくはこちらからご確認下さい: http://www.darkreading.com/attacks-breaches/financial-services-ranks-cyberattacks-top-industry-worry/d/d-id/1316917?

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.

カレンダースパムが問題を引き起こす

過去に流行ったフィッシングやスパムのテンプレートが度々復活することは、よくあることです。最新のセキュリティフィルタなら簡単に防げるような古い技術と思える攻撃が復活することもあります。最近復活したカレンダースパムがその例です。
このスパムおよびその亜種が依然として有効なのは、多くのフィルターでカレンダーへの招待 (*.ics) が適切にブロックされていないためです。また、正規のドメインからルーティングされてきたメッセージは送信者レピュテーションベースのフィルターをくぐり抜ける可能性もあります。
最近観測されたカレンダースパムの実例をご覧ください。
http://www.proofpoint.com/threatinsight/posts/calendar-spam-invites-trouble.php

Dyreza が通信を傍受

“Dyreza” または “Dyre” と呼ばれるマルウェアは、man-in-the-middle (中間者) 攻撃によってオンラインバンキングとユーザーの間の暗号化された (ユーザーは安全と信じている) Web トラフィックを傍受します。
このマルウェアは最近観測された複数の大規模なフィッシング攻撃に使われましたが、これらの攻撃は Salesforce のようなクラウドサービスのユーザーを狙って拡大しています。Dyreza は「ブラウザフッキング」という手法を使って、暗号化された Web トラフィックを傍受します。コ

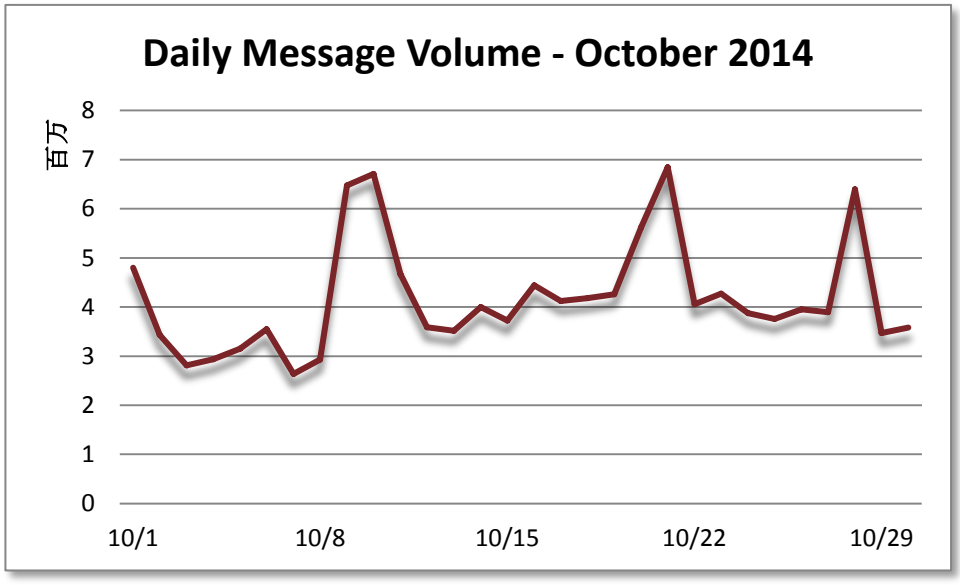
ンピュータを侵害し、暗号化されていないトラフィックを傍受し、ユーザーが SSL による通信をはじめようとしたときに入り込むのです。
Dyreza は最近数回変更が行われましたが、Proofpoint ではすでにそれらを解析しています。新しい機能については以下をご参照下さい:

http://www.proofpoint.com/threatinsight/posts/dyreza-takes-stock.php

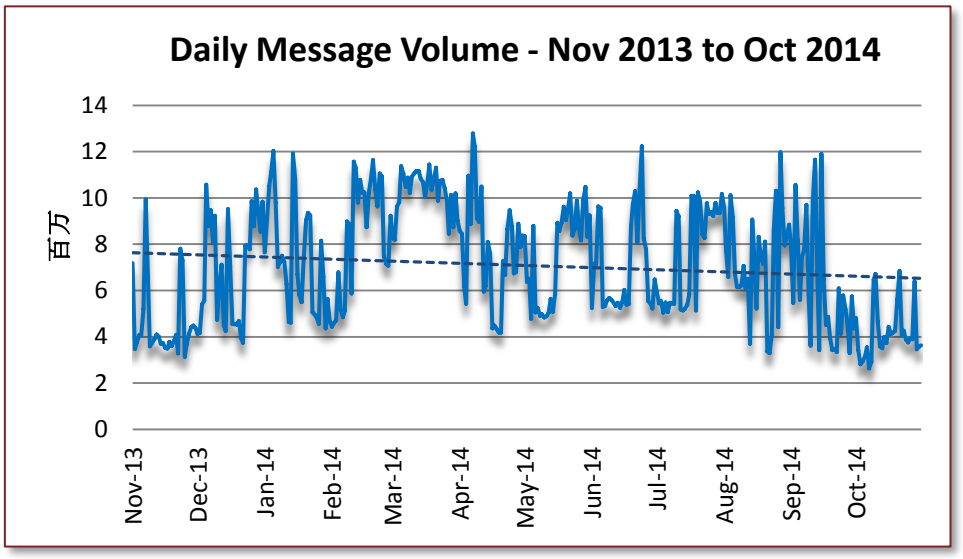
Threat Trends (トレンド)

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。10 月のスパム量は一定しませんでしたが、極端では無い増減を月末まで繰り返しました。500 万通/日で始まった後に徐々に 300 万まで下降し、第 2 週の始まりには急激に 600 万通まで上昇、週中には 400 万に下がりました。そこから徐々に増加し、第 3 週の終わりに月中最高値の 700 万に達しました。第 4 週は 400 万前後を推移し、月末に 600 万まで急増し、その後 300 万に急減しました。



9 月と 10 月を比較すると、昨年の 11 月 (38.17%) 以降最大の減少(32.38%) を記録しました。前年比 43.10%の大幅な減少です。



Spam Sources by Country (スパム発信源)

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。EU は 2013 年 5 月以降初めて 2 位に下がりましたが、1 位との差はわずかです。(そのと EU は 3 位でした) ロシアは 1 ヶ月ぶりに上位 5 カ国にランクインし、3 位に入りました。4 位と 5 位はベトナムとアメリカです。
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。

		May '14	Jun '14	Jul '14	Aug '14	Sep '14	Oct '14
Rank	1st	EU	EU	EU	EU	EU	China
	2nd	US	Vietnam	US	US	Vietnam	EU
	3rd	Argentina	US	China	Argentina	China	Russia
	4th	Russia	China	Argentina	Russia	Argentina	Vietnam
	5th	China	Russia	Russia	China	Korea	USA

以下の表は、各国が総スパム量に占める発信量の割合を示したものです。EU の数値は全加盟国を含んでおり、以前よりも正確に傾向をつかむことができます。中国が 18.82%を占め、1 位になりました。それ以下の 4 カ国の合計は 33.61%で、中国の 2 倍程度です。

September 2014			October 2014		
1	EU	24.99%	1	China	18.82%
2	Vietnam	13.36%	2	EU	15.61%
3	China	4.51%	3	Russia	9.25%
4	Argentina	3.68%	4	Vietnam	5.10%
5	Korea	3.66%	5	US	3.65%

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