



WEBROOT®

ウェブルート 脅威レポート

2015

脅威インテリジェンスによるインサイト

2014年を通して、ウェブルートでは数え切れないほどのマルウェアやいわゆるPUA (Potentially Unwanted Applications) と呼ばれる不要なアプリケーションの収集、数十億のIPアドレスやURLの監視、数百万の新種およびアップデートされたモバイルアプリの不正な振る舞い分析、何百万ものエンドポイントから取得したデータにもとづくマルウェアのトレンド分析を行ってきました。このレポートでは、脅威インテリジェンスを利用して進化した攻撃から企業が身を守る方法について、弊社独自のインサイト、分析結果および有益な情報を提供します。

CONTENTS

まえがき.....	3
はじめに.....	4
BrightCloud Threat Intelligenceの機能（収集、分析、分類、相関分析、公開）	
85,000：1日に発生する新しい不正IP	7
Webroot BrightCloud IP レピュテーション	
IPアドレスに関する重要事項	
55%以下：「信頼できる」とみなされるURLの割合.....	10
Webroot BrightCloud Web クラシフィケーションとWeb レピュテーション	
URLに関する重要事項	
30%：フィッシングサイトにアクセスしたインターネットユーザーの割合.....	14
Webroot BrightCloud リアルタイム アンチフィッシング	
フィッシングに関する重要事項	
15%：新しく作成されるファイルのうち、悪質な実行ファイルの割合.....	17
Webroot BrightCloudファイル レピュテーション	
実行ファイルに関する重要事項	
わずか 28% のモバイルアプリが「信頼できる」または「安全」	19
信頼できるアプリの割合は2013～2014年の間に52%から28%に減少	
モバイルアプリに関する重要事項	
まとめ	23

まえがき

ウェブルートは、データの盗難やサービス妨害を目的とした数多くの不正URL、IPアドレス、マルウェア、モバイルアプリが絶えず発生する状況を目の当たりにしてきました。2014年には中小企業のみならず、大企業や金融機関、IT企業を狙った侵害も増加し、その件数はとどまるところを知らません。

Hal Lonas,
(ハル・ロナス – Webroot, Inc. 最高技術責任者)

被害に遭った企業は当然何かしらのセキュリティインフラを保持していたはずですが、それなのに侵害が発生してしまった理由はどこにあるのでしょうか。原因の一つとして考えられるのは、効果が薄い時代遅れのセキュリティ手法への依存です。これは、今日の能動的な脅威に対する理解や対策、未知の脅威をブロックする能力、そして被害を実際に検知するまでの時間を最小限におさえる機能がすべて不足していることを意味します。

ウェブルートは、各企業のIT担当部署やユーザーにとって必要不可欠なのは、常に最新の状態でアップデートされた脅威インテリジェンスであると考えています。常にその姿を変化させる脅威に対して、セキュリティ対策も同様に適応していかなくてはなりません。そのためには、不正IPやフィッシング攻撃に使用されるWebサイト、不正アプリが最も多く存在するカテゴリなどに関する最新情報の取得が重要になってきます。

今日の脅威に対抗するため、データの相互関係まで把握した上で脅威を事前にリアルタイム検出する脅威インテリジェンスが求められます。様々な脅威に対応するためのリアルタイムに複数要素を相関分析する予測型の脅威インテリジェンスは、企業が未知と既知両方の脅威に対抗していくにあたって必要不可欠な要素といえるでしょう。



はじめに

この2015年版脅威レポートでは、2014年に企業や個人が経験した様々な脅威の概要についてまとめています。データは、ウェブルートのエンドポイントソリューションと脅威インテリジェンスサービスのバックボーンとして機能するビッグデータ分析セキュリティエンジンであるBrightCloudが自動収集、分析した結果である脅威インテリジェンスに基づきます。

2014年を通して、ウェブルートでは数え切れないほどのマルウェアやいわゆるPUA (Potentially Unwanted Applications) と呼ばれる不要なアプリケーションの収集、数十億のIPアドレスやURLの監視、数百万の新種およびアップデートされたモバイルアプリの不正な振る舞い分析、何百万ものエンドポイントから取得したデータをもとづくマルウェアのトレンド分析を行ってきました。

このレポートでは以下のようなウェブルートの脅威分析チームの見解も併せて紹介します。



不正な動作に関連づけられたIPアドレスの分析



URLの分類や評価に関する詳細



フィッシング検出における統計



マルウェアとPUAに関するインサイト

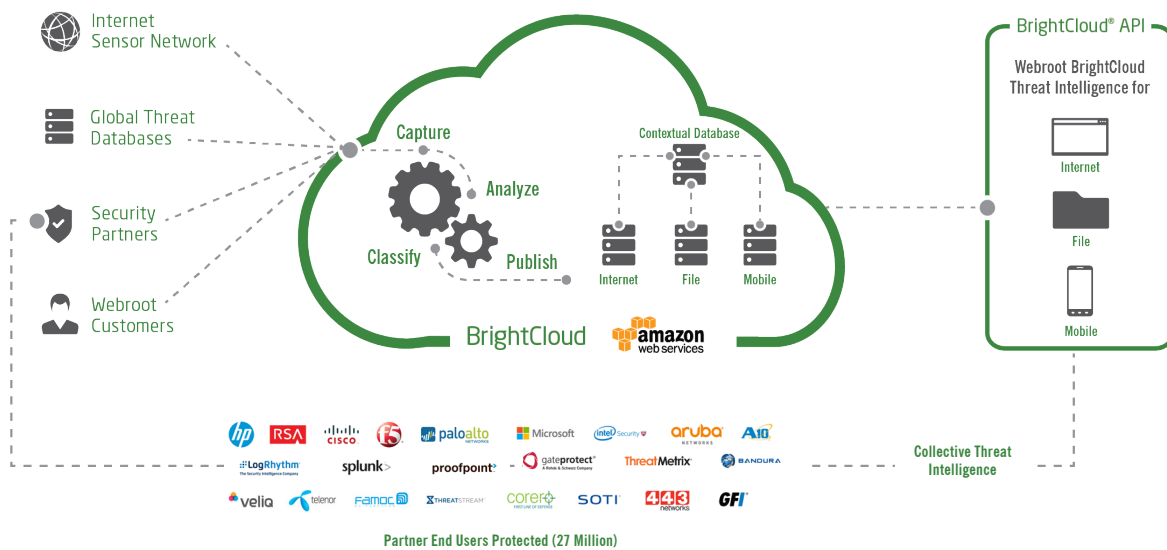


Androidデバイス向けアプリのセキュリティに関する情報

BrightCloud Threat Intelligenceの機能 (収集、分析、分類、公開)

ウェブルートが提供する エンドポイントおよび脅威インテリジェンスソリューションは、次世代の脅威対策の最先端技術として構築されたBrightCloudがベースとなります。このBrightCloudには世界規模のマルウェア検出ネットワークを構成する何百万ものセンサーから取得された膨大なデータが集約されており、ウェブルートのパートナー企業は

BrightCloud®Threat Intelligence サービスを経由して自社の顧客に既知と未知どちらの脅威にも対応可能な次世代の脅威インテリジェンスを提供しています。また、本サービスはURLの分類や判定、IPやファイルの評価、フィッシング対策、モバイルセキュリティなどをすべてカバーしています。



グラフ1:BrightCloud

このレポートでは、上記サービスに組み込まれたリアルタイム脅威分析エンジンを通してみえてきた様々な脅威の全容がまとめられています。ウェブルートは、膨大なデータ処理能力と最先端の自動機械学習機能および強力な相関分析エンジンの組み合わせにより、以下を実施します。



さらに、ウェブルートではこのようなデータをURL、IP、ファイル、モバイルアプリなどの様々な要素間で関連づけ、その相互関係にもとづいたより正確で詳細な評価を提供しています。たとえば、単独では正常と判断されるURLでも、不正なIPやファイル、モバイルアプリと関連している場合は、ウェブルートシステム内での評価は低くなります。このシステムの本来の目的は脅威の急激な広がりから企業やユーザーを守ることですが、今回のレポート発行にあたり、ウェブルートでは以下のようなデータを分析し脅威の全容をまとめました。



85,000



1日に発生する新しい不正IP

Webroot BrightCloud IP レピュテーション

攻撃を防止する最も効果的な手法の一つに不正なIPアドレスからの通信のブロックがあげられます。ウェブルートでは40億以上ものIPアドレスを継続的に監視した結果をデータベース化し、リスクの高いIPアドレスについて5分ごとに（※設定で頻度の変更が可能です）更新しています。最新の脅威を正確に識別し効果的な防御を実施するには、頻度の高い更新が必要不可欠です。また、ホストが感染状態から回復しIPアドレスを変更した場合など、再評価を繰り返し実施してリアルタイムな状況を把握することが重要になってきます。

BrightCloudでは、様々なアプローチからデータの分析と関連づけを行い、より正確なリスク判定スコアの算出を目指しています。このスコアは「信頼できる」ものから「不正」まで、5つのレベルに分かれます。カテゴリへの分類は、BrightCloud® IP Reputation Indexで各IPアドレスにつけられた1から100までのスコアにもとづいて実施されます。数値が低いほどリスクが高いことになり、これらのIPアドレスはスコアの高いものと比較してより高い頻度でモニタリングされます。

グラフ2: BrightCloud IP Reputation Index

01-20 高リスク		リスクが高いとみなされるIPアドレスです。不正ペイロードやDos攻撃などの攻撃に使用される可能性が高く、企業インフラやエンドポイントに影響を与える恐れがあります。
21-40 疑わしい		疑わしい動作をするとされるIPアドレスです。攻撃に使用される可能性は平均値より高いとみなされます。
41-60 中リスク		一般的に良性と考えられるが、リスクになり得る可能性を持つIPアドレスです。攻撃に使用される可能性も一定程度存在します。
61-80 低リスク		良性と考えられ、リスクと判断される特徴も持たないIPアドレスです。攻撃に使用される可能性も低いとされます。
81-100 信頼できる Trustworthy		セキュリティリスクと関連づけられたことが一度もない、クリーンなIPアドレスです。攻撃に使用される可能性は非常に低いとされます。

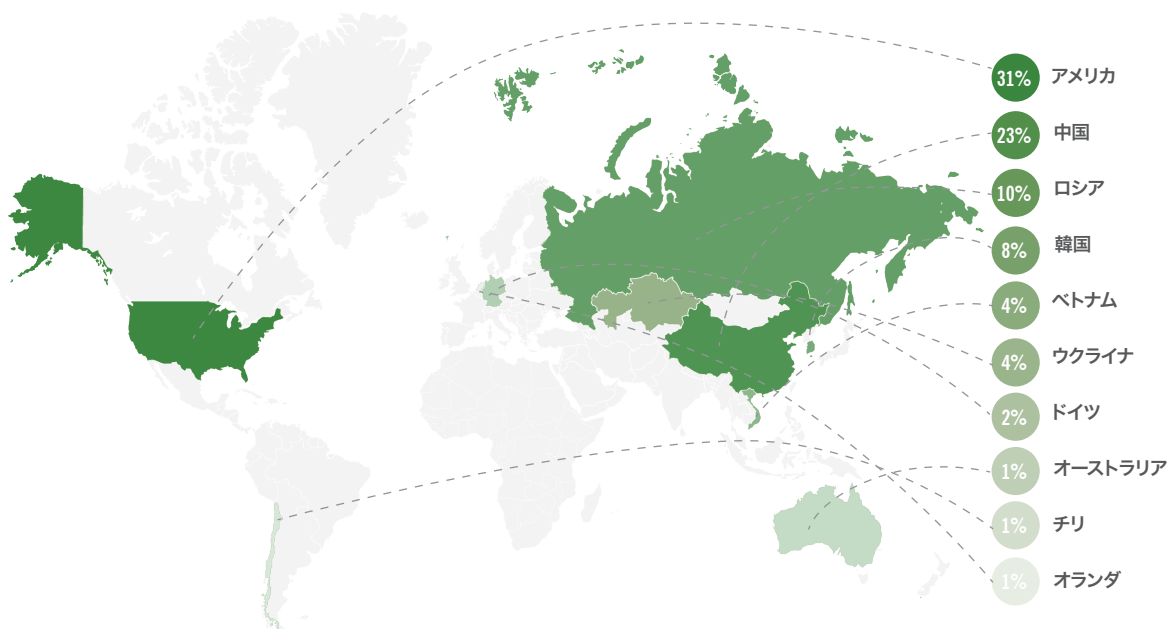
IPアドレスに関する重要事項

ウェブルートが保持する既知の不正IPアドレスのリストには、約1200万ものIPアドレスが登録されています。そのうち約36%のIPアドレスは毎日入れ替わり、この傾向は年間を通してほぼ変わりません。マルウェア作成者は、あるIPアドレスは不正と判定されるまでのわずかな時間しか、攻撃の開始や制御に使用できないことを知っています。不正な動作が確認された数分後にブラックリストに登録されるため、攻撃者はホストやIPアドレスを頻繁に変えます。しかし、常に最新の状態にアップデートされるウェブルートのIPブラックリストは、このような急速な変化にも対応し、被害が広がる前にその動きを食い止めることができます。

ブラックリストから外されたIPアドレスが再度リストに現れることはあまりないものの、一部のIPアドレスに限っては不正な動作と何度も関連づけられ、リストに再登録されることもあります。特に、リストの上位1万までに登録されたIPアドレスは再利用される率が高く、1ヶ月のうちにリスト除外と再登録を平均4回も繰り返します。ま

た、それまで不正な動きがまったく見られなかったIPアドレスが新規で登録されることも多いのがウェブルートのリストの特徴です。2014年には一日平均85,000以上の新しいIPアドレスがリストに追加されました。この数値から、こうしたリストが日常的に更新され続けることがスパムやDDoS攻撃対策において、いかに重要か改めて分かります。各企業での設定の例として、たとえばセキュリティ意識の高い銀行であれば前述のスコアが80より低いIPアドレスはすべてブロックするように選択できます。一般企業では、パートナー企業と関連したサイトであればスコアが60以上のIPアドレスまで許可することもあるかもしれません。

不正IPアドレスは世界中に存在しますが、一定の国や地域に集中していることも事実です。以下のグラフ3が示すとおり、不正IPアドレスの30%はアメリカに存在し、その後に次いで多いのが中国とロシアです。また、不正IPの半数がアジアに存在します。

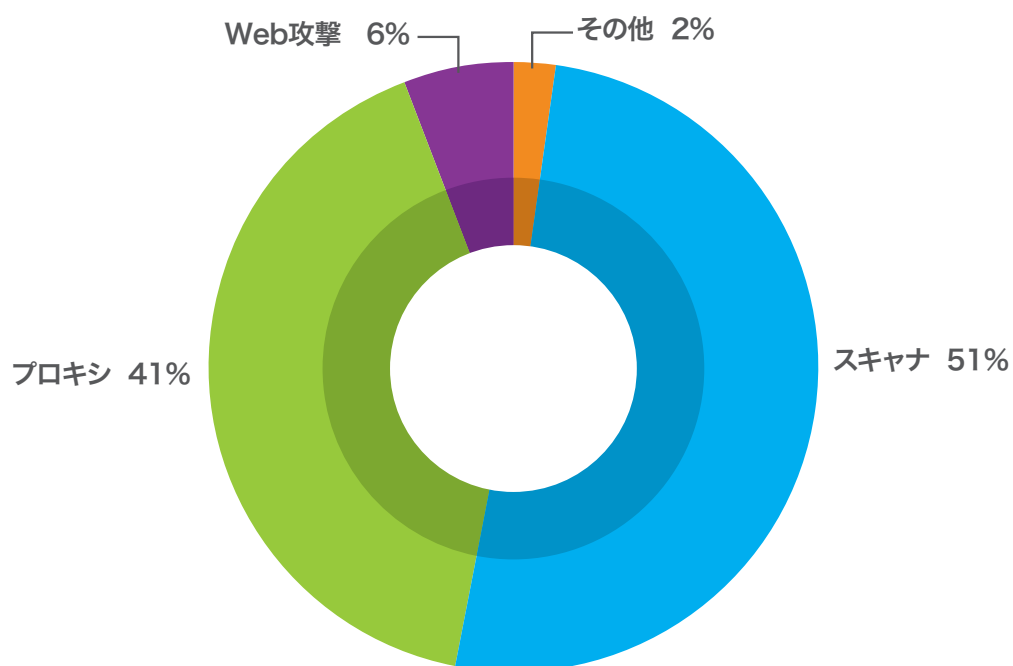


グラフ3：不正IP発生国トップ10

不正IPアドレスに関するもうひとつの興味深い点として脅威のタイプが挙げられます。これは各IPが関連する不正行為の性質に応じてスパム、スキャナー、プロキシ、Web攻撃、フィッシングなどに分かれます。個々のIPが関連する不正行為に基づき、主要な脅威タイプでカテゴリー分けされています。そのうち、脅威タイプ別では最も割合が高いのはスパムであり、全体の90%におよびます。これらの脅威は活動期間が非常に短く、数時間もしくは数分のもものもあります。

しかし、企業側で既存のブラックリストを使用して関連IPアドレスをブロックし、スパムやボットネットを阻止することは不可能ではありません。

グラフ4では、脅威のタイプごとに分けられた不正IPの割合をまとめています（スパムおよびボットネットを除く）。半数を占めるのはスキャナーで、プロキシが僅差でそれに続きます。



グラフ4：脅威タイプ別不正IPの分布（2014年、スパムを除く）

55%以下

「信頼できる」と
みなされるURLの割合



Webroot BrightCloud Web クラシフィケーションとWeb レピュテーション

ウェブルートでは200億以上のURLを分類、監視し、その結果をBrightCloud®Web クラシフィケーションとBrightCloud® Web レピュテーションを通して提供しています。Webroot BrightCloud Web クラシフィケーションはWebサイトを83のカテゴリに分類したインテリジェンスをベースにオンライン脅威からユーザーを守り、ポリシーを経由した効率的なインターネット利用の制御を行います。

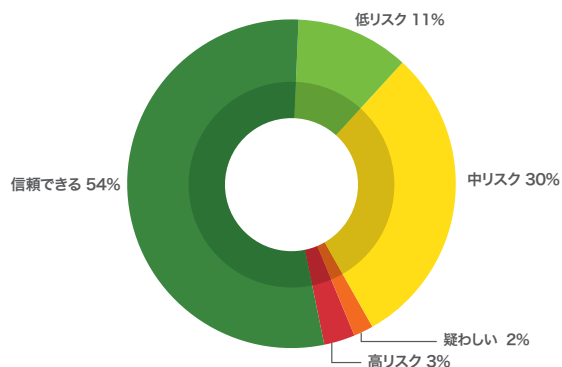
BrightCloud®Web レピュテーション では各URLの履歴、存在期間、ランク、場所、ネットワーク、リンク、リアルタイムな動作などにもとづいて、IP レピュテーションと同様に5つにレベル分けされたスコア判定システムを利用しています。本サービスを導入することでカテゴリ別ではなく単独のURLにおける評価を反映し、Web攻撃に対する正確でリアルタイムな防御を実行することができます。

BrightCloud分析エンジンは現在、1秒ごとに2,500以上のURLに対する分類とスコア判定を人間よりも高い精度で実施することができます。このスピードと正確性はウェブルートの大きな強みとなっています。

URLに関する重要事項

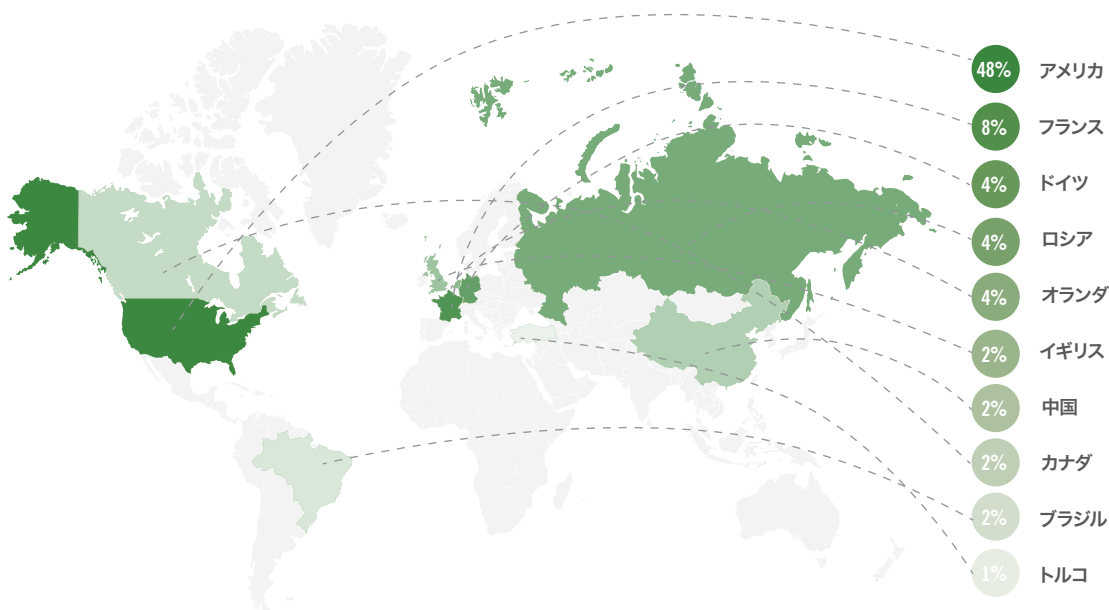
一言でリスクのあるURLといっても、そのレベルは多岐にわたります。グラフ5では、BrightCloud上でスコア判定されたURLのリスク度の内訳をまとめています。判定対象となったURLの半数は信頼がおけると判定され、リスクが低いと判断されたものも11%あったことは特筆すべき内容でしょう。多少のリスクがあると判定された30%に関しては、新規Webサイトなど内容を識別するために十分なデータがなかったものも含まれます。そのため、このカテゴリに分類されたURLがすべて悪質なものであるとは言い切れません。Web上に存在するサイトの多くは正当なものです。企業にとっては避けた方が無難なサイトも数多くあります。

また、URLが作成された地域についても注意が必要です。グラフ6では、検出された不正URLを国ごとにまとめています。グラフ3や5と比較すると、分布の割合が大きく異なることがわかります。不正IPの発生源で大きな割合を占めていたロシアや中国は、URLの分布ではそこまでの数値を出していません。原因の一つとして考えられるのは、リスクの高い地域にいる攻撃者がフィルタリングによる自動ブロックの回避する



グラフ5：カテゴリ別URLリスクの分布（2014年）

ために、アメリカなどの地域フィルタリングサービスでは自動的にブロックされない国にマルウェアURLをホストします。これで、企業ネットワーク側で「高リスク」の国のURLを含むアクセスをすべて拒否する設定がされていた場合でも影響されません。このような状況をふまえると、IPアドレス単独に対するフィルタリングだけではなく、URLの性質にもとづいた評価スコアを確認することが重要であることがわかります。



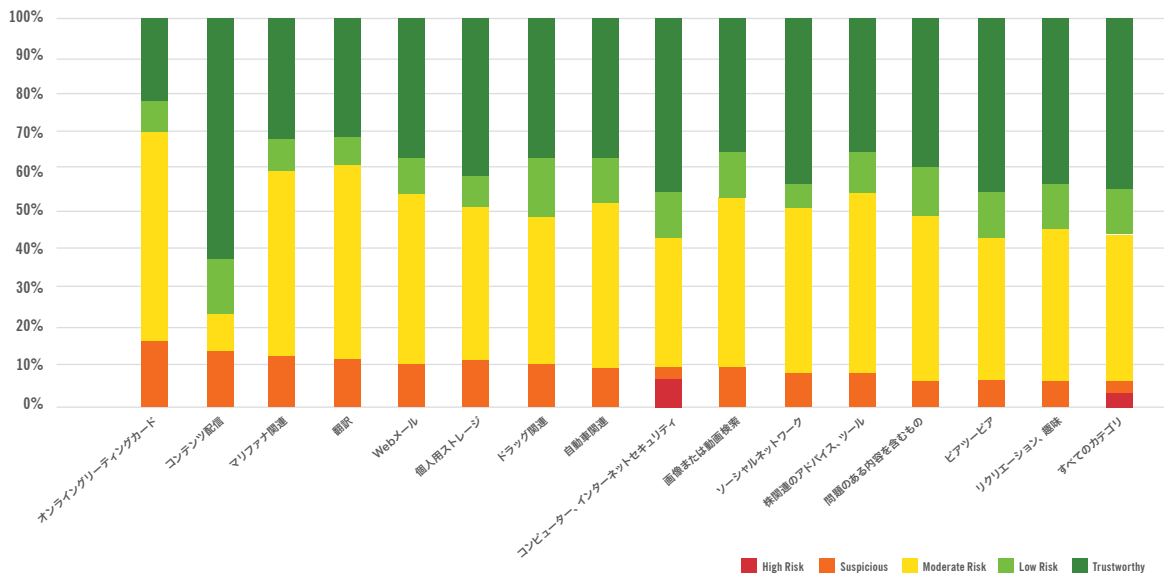
グラフ6：不正URLのホスト国トップ10

数億もの不正なサイトからのユーザーとネットワークの保護

インターネット上に存在する数多くの不正なサイトからユーザーやネットワークを守ることは非常に重要です。URLに関するデータをさらに詳しく分析するため、ウェブルートでは83個のURLカテゴリをもうけています。例として、コンテンツ配信ネットワーク、オンラインگریティングカード、翻訳サービスなどが挙げられます。また、BrightCloud Web クラシフィケーションでは高リスクのURLをさらに「既知のスパムURL」、「マルウェアサイト」、「フィッシング」、「プロキシ回避、アノマイザー」、「スパイウェア、アドウェア」、「ポットネット」の6つのカテゴリに分類しています。グラフ7では、リスクが高い、もしくは疑わしい動作が確認されたURLが多く確認されたカテゴリのうち上位15位をまとめています。これらのサイトには感染後に回復していないものや、不正URL、IPアドレ

ス、ファイル、モバイルアプリなどとの関係性が確認されたものが含まれます。

最も疑わしいとされたのはオンラインگریティングカードのサイトで、一般的には信頼できるとみなされがちな定期的に更新されるコンテンツ提供サイトが次に続きます。コンピューターやインターネットセキュリティ関連のWebサイトが上位に位置しているのは、不正URLに言及することが多かったり、セキュリティブログ上でそういったリンクを直接紹介することもあるためです。なお、「すべてのカテゴリ」は前述したような比較的高いリスクを示す、不正に関連したカテゴリを含めた83すべてのカテゴリの平均です。



グラフ7: 疑わしいまたはリスクが高いとされるカテゴリトップ15 (悪質なカテゴリを除く)

リスクの高い国の攻撃者は信頼度の高い国に不正なサイトをホストする

グラフ8では、左列が訪問回数の多いURLカテゴリ上位10位、右列がリスクが高いURLカテゴリ上位10位を表しています。不正に関連したカテゴリに含まれるURLは必然的にリスクが高くなります。これらの直接不正に関連したカテゴリを除外すると、ビジネス、経済、社会、ショッピング、旅行、健康、医療関連のものなどが疑わしいカテゴリとして挙げられることが分かります。

URLカテゴリトップ10

1	ビジネス、経済	21.2%
2	社会	12.8%
3	旅行	6.4%
4	アダルト、ポルノ	5.7%
5	ショッピング	5.4%
6	個人サイト、ブログ関連	4.8%
7	アート、エンタテインメント	4.0%
8	健康、医療関連	2.7%
9	コンピューター、インターネット関連	2.5%
10	ニュース、メディア	2.3%

疑わしい、または高リスクのURLカテゴリトップ10

1	スパム関連URL	30.9%
2	マルウェアサイト	13.7%
3	ビジネス、経済	7.8%
4	プロキシ回避、アノニマイザー	6.7%
5	フィッシングや他の不正	6.4%
6	社会	5.1%
7	ショッピング	5.1%
8	旅行	2.7%
9	健康、医療関連	1.8%
10	アート、エンタテインメント	1.8%

グラフ 8: 2014年におけるURLカテゴリトップ10の内訳

また、一見疑わしかったり望ましくないと見られがちなカテゴリでも、平均値と比較すると評価が高い場合もあります。たとえば詐欺関連のカテゴリに分類されたURLのうち85%が「信頼できる」または「低リスク」と判定され、これは全カテゴリの平均値である65%を上回ります。他にもヘイト、人種差別関連 (82%)、グロテスク系 (81%) 暴力関連 (77%)、違法な内容 (67%)、アダルト、ポルノ (65%)、ヌードを含むもの (65%) が「信頼できる」または「低リスク」の評価割合が高いカテゴリとして挙げられます。企業や家庭においては、上記のようなカテゴリは好ましくないと考えており、アクセスや制限を行う場合にはカテゴリ分けも考慮に入れるべきです。なぜなら評価スコアだけでは、こうしたサイトを内容を踏まえた上での判定ができないためです。

ウェブルートが使用するURLカテゴリの一覧は以下のURLより参照可能です。

www.brightcloud.com (英語)

30%



フィッシングサイトにアクセスしたインターネットユーザーの割合

Webroot BrightCloud リアルタイム アンチフィッシング

ウェブルートのBrightCloud リアルタイム アンチフィッシングはアクセス先のWebサイトに不備がないか、フィッシングサイトではないかの分析をミリ秒単位で実行します。フィッシングサイトは一定のサイト訪問が得られる数時間の間だけオンラインであることが多いため、いかにリアルタイムな分析を実施するかが重要になってきます。静的なブラックリストではこのようにダイナミックに活動するサイトに對抗することはできないのに対し、リアルタイム検出ではサイトが作成されてから数秒で検出が可能であるためです。

さまざまなセキュリティベンダーが自社の顧客を保護し、フィッシングサイトに対抗するためにBrightCloud リアルタイム アンチフィッシングを活用しています。2014年、ウェブルートは英語以外の言語サポートを増設し、エンドポイント向けのセキュリティ製品であるWebroot SecureAnywhereにリアルタイムのフィッシング対策機能を統合しました。その結果、2014年最後の3ヶ月間にウェブルート全体で検出されたフィッシングサイトの平均値は大きな増加をみせました。それにともない、このレポートでは2014年の10月から12月にかけてのデータにもとづいた分析を紹介します。

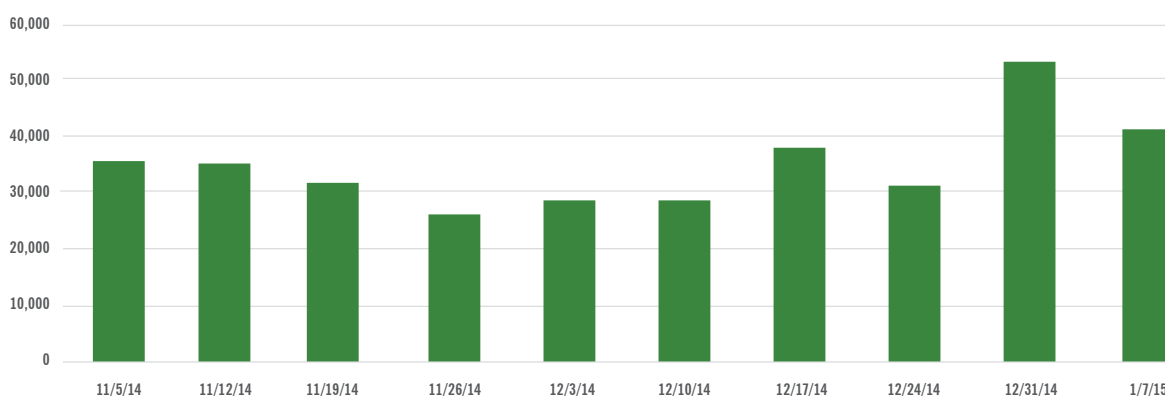
フィッシングに関する重要事項

2014年最後の3ヶ月間、ウェブルートの保護下にあるユーザーのうち、毎月およそ2.5%においてゼロデイ攻撃をしかけるフィッシングサイトへの初回アクセスが確認されていたことが分かりました。(2回目以降のアクセスはすべて自動でブロックされています) 2.5%という数値自体は少なくみえますが、年間に換算するとユーザー全体の30%がゼロデイURLを経由したフィッシング攻撃に遭遇する可能性があるということになります。この数値から、リアルタイムなフィッシング対策を事前に用意しておくことがどれだけ重要かが分かります。

また、フィッシング攻撃は世界規模のイベントが発生する時期に集中して増加する傾向があります。たとえば、2015年の始めにフランスでシャルリー・ヘブド襲撃事件が発生した際には、データに大きな変動がみられました。また、2014年最後の週には、その四半期における他の週と比較して50%以上のフィッシング攻撃の増加が確認されました。これは、この時期がちょうどホリデーシーズンにあたり、プレゼントなどで新しいデバイスを使い始めるユーザーが多いことが原因と考えられます。



年間でユーザー全体の30%がゼロデイURLを経由したフィッシング攻撃に遭遇する可能性あり

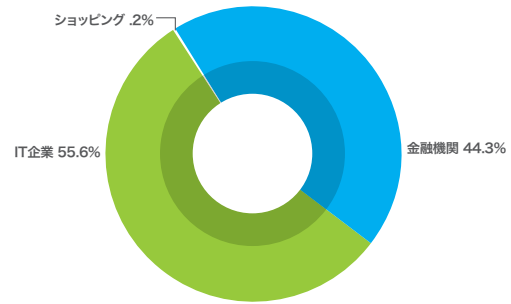


グラフ9：2014年の10月から12月にかけて週単位で確認されたフィッシングURL

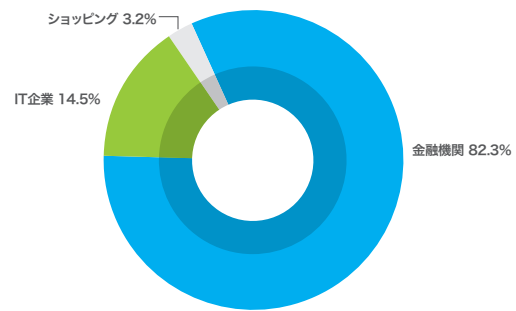
ゼロデイ攻撃で使用されたフィッシングデータから具体的にどのようなWebサイトがねらわれていたのかを分析すると、興味深い結果が得られました。調査対象は、2014年の間になりすまし被害にあったトップ60の企業です。グラフ10のデータから、フィッシングサイトのターゲットが金融機関もしくはIT企業のいずれかにほぼ同じ割合で集中していることが分かります。

しかし、実際に攻撃の対象となった企業の数と比較するとその割合は変化します。グラフ11で分かるように、なりすましの被害にあった企業のうち、80%以上が金融機関でした。ただし、1企業に対するフィッシング攻撃の総数では、IT企業が金融機関を上回っています。平均値では、1金融機関につき攻撃総数が900回だったのに対し、IT企業においては1社に対して実に9,000回もの攻撃が確認されています。

60企業のうち、なりすまし被害に遭った総数が上位5位だった企業をカテゴリ別に以下に示します。



グラフ10: 産業カテゴリ別フィッシングサイトの割合



グラフ11: フィッシングサイトによりなりすましにあった企業の割合

フィッシングの標的とされたIT企業トップ5

1位	Google	35.6%
2位	Apple	23.8%
3位	Yahoo	18.6%
4位	Facebook	13.3%
5位	Dropbox	6.6%
その他: Microsoft, Blizzard, Adobeなど		

フィッシングの標的とされた金融機関トップ5

1位	PayPal	52.2%
2位	Wells Fargo	17.9%
3位	Bank of America	12.2%
4位	Chase	4.6%
5位	Lloyd's Bank	4.5%
その他: NatWest, Royal Bank of Canada, Navy Federalなど		

グラフ12: なりすましの被害にあったIT企業と金融機関

国ごとのフィッシングサイト分布を見ると、アメリカが全体の75%を占めトップに立っています。しかし、これはあくまでアメリカを中心に展開するウェブルートユーザーから取得したデータのため、どうしても偏りがあることも述べておきます。また、フィッシング攻撃は経済的な見返りが大きいターゲットが狙われやすいため、必然的に発展途上国よりも先進国での発生率が高くなります。

15%

新しく作成されるファイルのうち、悪質な実行ファイルの割合



Webroot BrightCloudファイル レピュテーション

ウェブルートでは、パートナー企業向けに分単位で自動更新されるファイル評価サービスを提供しています。この不正またはホワイトリスト化されたファイル指標に対するリアルタイムな検索サービスを利用することで、IT管理者は企業ネットワークに侵入しようとする脅威ファイルを種類、ファイル名、プラットフォーム、暗号化やパスワード保護の有無に関わらずブロックすることができます。

ファイルの特徴から、不正実行ファイルは「マルウェア」と「PUA」の2種類に分けられます。後者は性質上不正と断言はできないものの、企業にとっては不適切または不必要とみなされるアプリケーションです。これにはスパイウェアやアドウェア、ハッキングツールなどが含まれます。

実行ファイルに関する重要事項

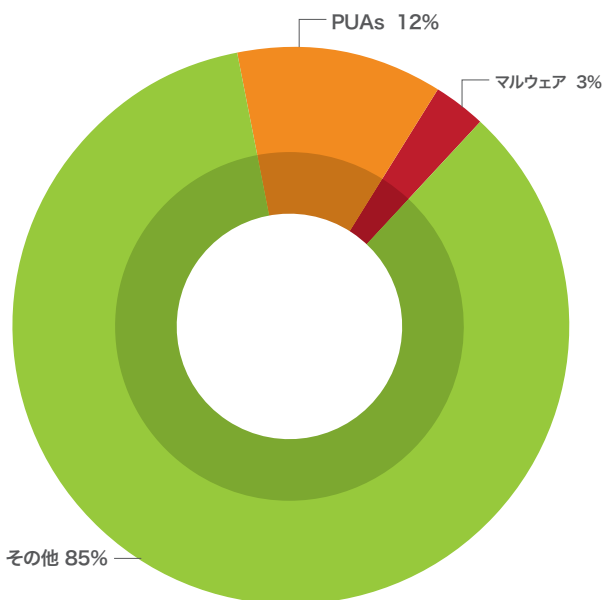
2014年、ウェブルートを数億におよぶ実ユニークな実行ファイルを新しく確認しました。これらのファイルのうち、約3.4%がマルウェア、12%がPUAとみなされています。

2014年を通して、各ウェブルートユーザーは平均1.3個のマルウェア、4.6個のユニークなPUAに遭遇したことになります。この数値から実行ファイルを利用した脅威がいかに急速に広まっているかや、その内容もカスタム化が進み、よりピンポイントなターゲットを狙ったねらったものに進化していることがよく分かります。

また、マルウェアやPUAはその数だけでなく、種類の豊富さも注目すべき点といえます。2014年、ウェブルートではひとつのマルウェアファミリーにつき平均して約700、PUAファミリーに関しては約30,000もの実行ファイルを検出しました。これらの実行ファイルから特定されたマルウェアファミリーの数は14,000以上、PUAファミリーは1,000以上におよびます。これはマルウェアよりもPUAの方がユーザーに広まる率が高いということです。その原因として考えられるのは、多くの環境においてPUAの方がはっきり「不正」ではなく、「疑わしい」という判定のみで、検出やブロックまではされないこともある点です。

そして、このような高い発生率に加え、2014年は身代金要求型ウイルス（ランサムウェア）の爆発的な増加および複雑化が見られた年といえます。全体で15のファミリーと広く蔓延したCTB/CritroniやCryptowall 3.0を含む何百もの亜種が確認されました。各ファミリーは、ソーシャルエンジニアリングを利用した新しく画期的な手法と複雑な仕組みを暗号化の手法に導入しています。Twitterを利用して「身代金」を支払ったユーザーのリストを作成する、暗号解除用と偽って感染のきっかけとなるツールを配布する、暗号解除が可能であることを示すためファイルをひとつだけ無料で解除する、ゲーマーやゲームMODを狙うなど、さらなる身代金を狙ってその手法は多岐におよびます。

また、2014年はPC感染において新手の手法が目立ちまし



グラフ13: 2014年ファイル評価カテゴリ分布

た。中でも最も注目すべきなのがWindowsのレジストリを悪用し、新種のウイルスに感染させるPoweliksと呼ばれるマルウェアです。このマルウェアの強みはレジストリ下に完全におさまる点と、新しい感染を引き起こす際にファイルコンポーネントをまったく必要としない点です。主に暗号化ランサムウェアに使われたことにより、Poweliksが大々的に注目されたのは2014年8月でしたが、ウェブルートでは、2014年3月からPoweliksを確認し、直ちに顧客の保護を開始していました。早期バージョンのサンプル分析を通して、レジストリに感染するためのテクニックは2種類のパターンが識別され、WindowsのPowerShellを経由するものが最終形態として確認されています。

わずか 28%

のモバイルアプリが「信頼できる」または「安全」



Webroot BrightCloud モバイルアプリ レピュテーション

BrightCloud モバイルアプリ レピュテーションサービスは、モバイル管理やセキュリティのソリューションを提供するベンダーが、流動性の高いモバイルデバイスにおける脆弱性を把握するのに役立ちます。このサービスでは、アプリストアやその他の提供元で公開されるアプリを継続的に分析し脅威の識別を実施しているため、IT担当者側で個別に設定したポリシーやリスク耐性にもとづいて特定アプリへのアクセスを制限し、ユーザーに悪質なアプリが配布されることを未然に防ぐことができます。

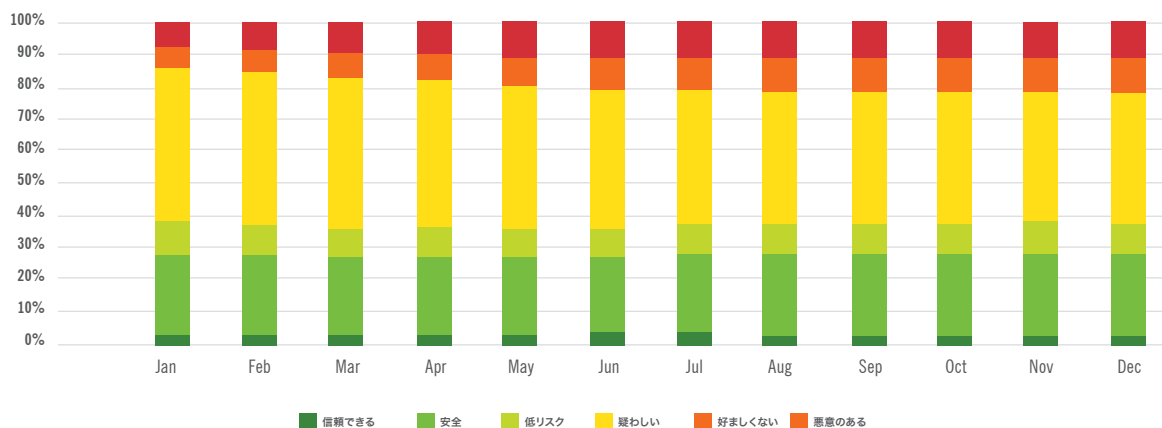
ウェブルートではこのプロセスを一本化することで、正確な分類やモバイルアプリにおける情報の提供を実現しています。パートナー企業は6層に分けられた分類カテゴリにもとづいて効果的なポリシーを作成することができます。アプリの情報を実際にどのように判断し適用するかをフレキシブルに設定できるため、各企業のニーズに応えた環境を作り出すことができます。

信頼できるアプリの割合は2013～2014年の間に52%から28%に減少

モバイルアプリに関する重要事項

2014年、ウェブルートではアプリ レピュテーションに700万以上の新しいAndroidアプリのデータを追加し、その総数は1,500万を超えました。グラフ14では、これらのアプリの評価の内訳を月別で表しています。「信頼できる」または「安全」と判定されたアプリの割合はあまり変わらないのに対し、「好ましくない」または「悪意のある」とされたアプリの数は増加し、「疑わしい」とされたアプリの数は逆に減少しています。平均値を見ると「信頼できる」または「安全」と判定されたのはアプリ全体の28%で、ほぼ半数が「低リスク」または「疑わしい」、そして22%以上が「好ましくない」または「悪意のある」と判定されたこととなります。この結果からアプリの大半が良性ではないと考

えてしまいそうになりますが、対象データの取得源にマルウェアが多く含まれていることを念頭に置いておくことは必要です。とはいえ「信頼できる」または「安全」と判定されるアプリ（※2013年には52%だったのが、2014年には28%に減少）が「疑わしい」または「悪意のある」アプリに取って代わられたことは事実です。この原因として考えられるのは、既存のアプリと機能が重複する新規アプリの市場が縮小していることです。また、「悪意のある」、「疑わしい」、「好ましくない」アプリが、より多くのデバイス、特に新興国向けのデバイスに、工場出荷時にインストールされていることが考えられます。



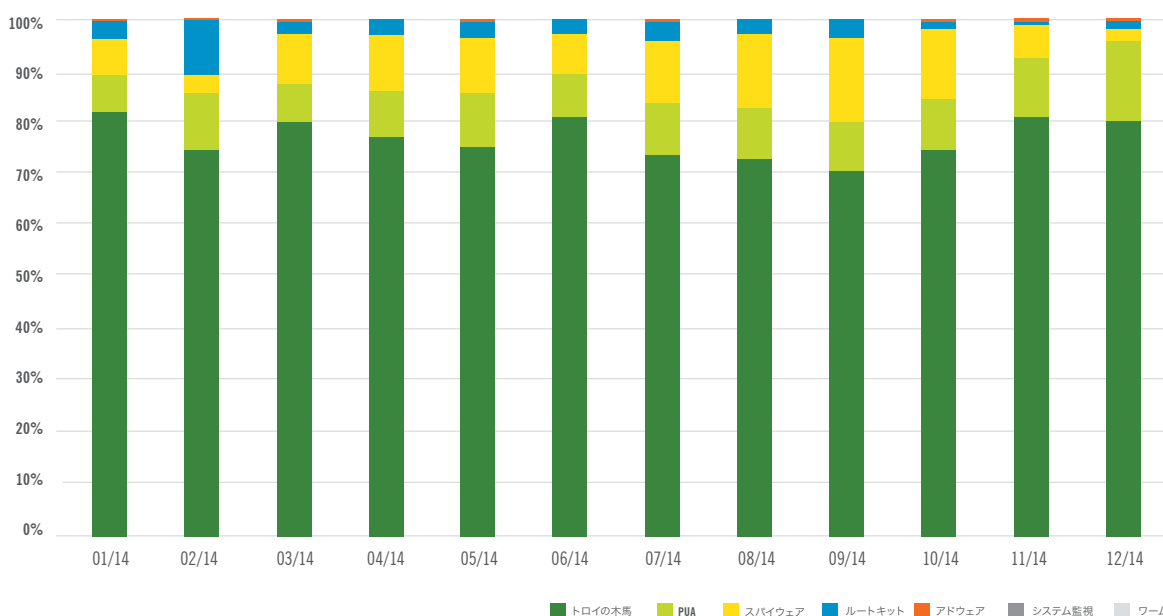
グラフ14：モバイルアプリ評価の年間変移（2014年）

グラフ15では、「悪意のある」カテゴリに含まれる脅威（アドウェア、PUA、ルートキット、スパイウェア、システムモニター、トロイの木馬、ワームなど）の相対度数をまとめています。マルウェア脅威で大多数を占めるのは「トロイの木馬」で、2014年は77%でした。これには、Androidにおける不正アプリの大半を占めるSMS感染から偽インストーラまで、幅広い内容が含まれます。他にもPUA（10%）、スパイウェア（9%）、ルートキット（4%）などが挙げられています。

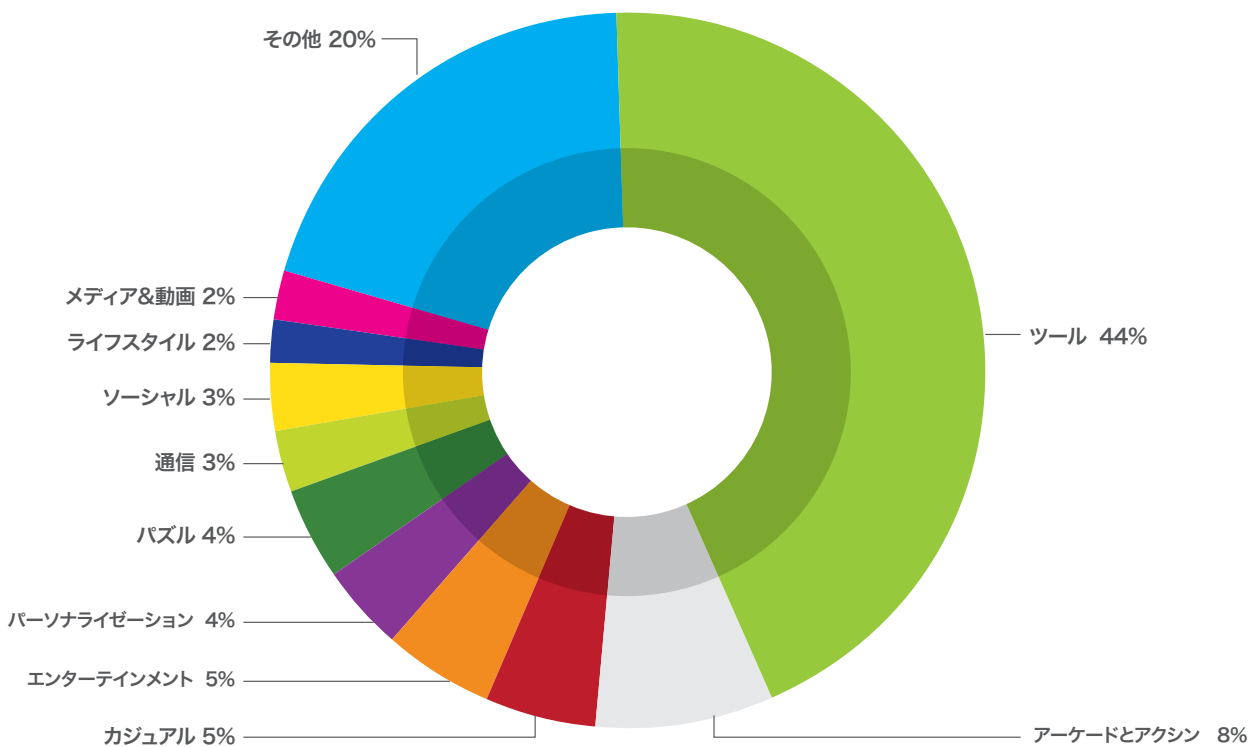
また、2014年12月においては、ルートキットの割合が11月と比べてほぼ9倍になっています。これは、ホリデーシーズンでさまざまなデバイスの新モデルが発表されたことに起因するとみられます。こういった新機種が発表されるとすぐそれに対応したルーティング

ツールも公開されます。数字が示すほどの大きなインパクトはないものの、ルートキットによるアプリへのアプローチは今後も開発が続くと考えられます。

Androidアプリは、Google Playストアで設定された45カテゴリに基づいたアプリの使用目的ごとにも分析することができます。ウェブルートでは、すべてのカテゴリにおいて不正アプリを検出しましたが、その割合はカテゴリによって異なりました。グラフ16で分かるように、計算機からバッテリー管理までさまざまな機能を持ったアプリが含まれる「ツール」カテゴリが、現時点で不正アプリを最も多く含むカテゴリと判明しました。



グラフ15：月別Android不正アプリの分布



グラフ16：カテゴリ別「悪意のある」Androidアプリの分布（2014年）

このカテゴリに分類されるアプリには、デバイスになんらかの追加アクセスを要求するものが多いのも特徴です。これはアプリを不正利用する際に悪用されがちな要素といえます。他に上位10位に入ったカテゴリは、「アーケードとアクション」（8%）、「カジュアル」（5%）、「エンターテインメント」（5%）、「パーソナライゼーション」（4%）、「パズル」（4%）、「通信」（3%）、「ソーシャル」（3%）、「ライフスタイル」（2%）、「メディア&動画」（2%）でした。

残りの35のカテゴリが不正アプリの総数において占める割合は合計してもわずか20%でした。しかし、これらの数値からだけではマルウェアの本質はみえてきません。補足情報として、以下にウェブルート分析担当者のAndroidに対する脅威の見解をまとめます。

1 Android向けに作成されたマルウェアのうち、ほとんどすべてがデバイス管理機能に干渉することで自身の権限をより強く設定し、アンインストールも非常に難しくする能力を持ちます。デバイス管理機能の確認画面はほとんどの場合特定のアプリに対して表示されるため、マルウェアでは他のアプリ名を騙ってこういった画面を表示したり、ソーシャルエンジニアリング手法を通してユーザーに自身が適正なアプリだと信じこませるケースがほとんどです。

2 今日、Android上でPC向けのマルウェアが模倣されることは珍しくありません。例として挙げられるのは、何年も前からPCを対象に発生しているランサムウェアです。これらの脅威は近年SimplelockerやSvpengの最新形態であるKohlerなどの形でAndroidにその矛先を向けています。また、デジタル仮想通貨の発行もこういったソフトウェアの例のひとつです。2014年、Google Playストア上で公開されているAndroid向けアプリの中でも、マイニングソフトウェアを秘密裏に搭載したものが多く発見されました。

3 SmsForw、Smsreg、Sms.Fakeinst、Sms.Thief など、Android向けに作られたSMS関連のマルウェアの数は増え続けています。また、ShastroSms やYzhcsmsなどの旧型マルウェアが最近またその勢力を増してきています。

4 2013年末ごろ、Secapkと呼ばれる難読化ツールが広まりました。これはコードの盗難防止など正当な目的にも使用されますが、悪質な内容を隠すために悪用されることもあります。このSecapk を使用したアプリの数は減ることがありません。ウェブルートのモニタリングにおいても、毎週何百ものSecapkで難読化されたアプリが確認されています。

まとめ

ウェブルートで取得、分析したデータは、脅威が世界のあらゆる場所で発生していること、そしてこれらの脅威が非常にダイナミックな性質を持つことを示しています。IPアドレスを何度も変更して検出をかくぐろうとする新種の攻撃に対抗するには、継続的にブラックリストを更新していくことが必要不可欠です。また、フィッシング攻撃もその動きが非常に速いことが特徴です。年間約30%のユーザーがゼロデイフィッシングサイトの被害に遭っているという数値からも、リアルタイムなフィッシング対策がいかに重要かが分かります。

また、サイトが良性なのか悪性なのかの判断についても一定の傾向がみられました。URL評価サービスで取得されたデータによると、URLカテゴリの評価だけでは個々のサイトの性質を判断することはできないことが分かります。さらに、膨大な数の実行ファイル（全体の15%以上）がマルウェアもしくはPUAと判定されました。平均すると、各ユーザーが6つの新しくユニークな疑わしいアプリケーションに遭遇していることとなります。これは、システム侵害のためのアプリのカスタム化が進み、狙いもピンポイントになってきていることを示しています。

Android向けアプリにおいては、「安全」、または「信頼できる」アプリの数が2013年から2014年にかけてほぼ半数に落ちこみ、「疑わしい」、あるいは「悪意のある」とされるアプリの数は逆に3倍になったことが分かりました。Androidのユーザーにとっては、今までよりも脅威のリスクが高まったということです。

結論として、企業がサイバー攻撃から身を守るには、リアルタイムかつ正確性の高い脅威インテリジェンスの導入が重要であるといえます。そうすることで脅威を事前に自動検出するポリシーの設定が可能になり、ネットワーク、エンドポイント、ユーザーを幅広く保護することができます。これは、企業が自身をターゲットにした攻撃を詳しく分析するのに加え、脅威の全体像をつかむためにも重要なことといえます。ユーザー側でも、訪問するWebサイトやEメールに記載されたURL、使用するアプリケーションやモバイルアプリに対して今まで以上に注意を払う必要があるでしょう。

(ウェブルート脅威分析チーム)

脅威インテリジェンスの詳細については、以下URLをご覧ください。

www.webroot.co.jp

サイバーセキュリティ ソリューションの詳細については、ウェブルートまでお気軽にお問い合わせください。

ウェブルートについて

ウェブルートは保護下にあるエンドポイントをインテリジェンスを構成する重要なデータとして活用し、インターネット上に存在する様々な脅威からユーザーを防御しています。ウェブルートが提供するクラウドベースのインテリジェンスネットワークの保護対象となるユーザーは、コンシューマー、ビジネスユーザー、セキュリティソリューションを提供するベンダーなど多岐に渡ります。アワードを受賞したSecureAnywhere*と BrightCloud*ソリューションでは、コンピューター、タブレット、スマートフォンなどの様々な種類のデバイスが保護され、その台数は3000万台以上におよびます。また、セキュリティインテリジェンスを活用したサービスはCisco、F5ネットワークス、HP、Microsoft、ハロアルトネットワークス、RSAセキュリティなどの名高いセキュリティ企業が提供するサービスの強化に貢献しています。本社はコロラド州にあり、北アメリカ、ヨーロッパ、日本、アジアパシフィックなどの幅広い地域に展開しています。サービスの詳細は以下URLをご覧ください。 URL: www.webroot.co.jp

ウェブルート株式会社

東京都港区南青山3-13-18 313南青山18F
03-4588-6500