アプリのセキュリティを第一に考える

マルウェアがデータを盗む仕組み

およびその対策方法

概要

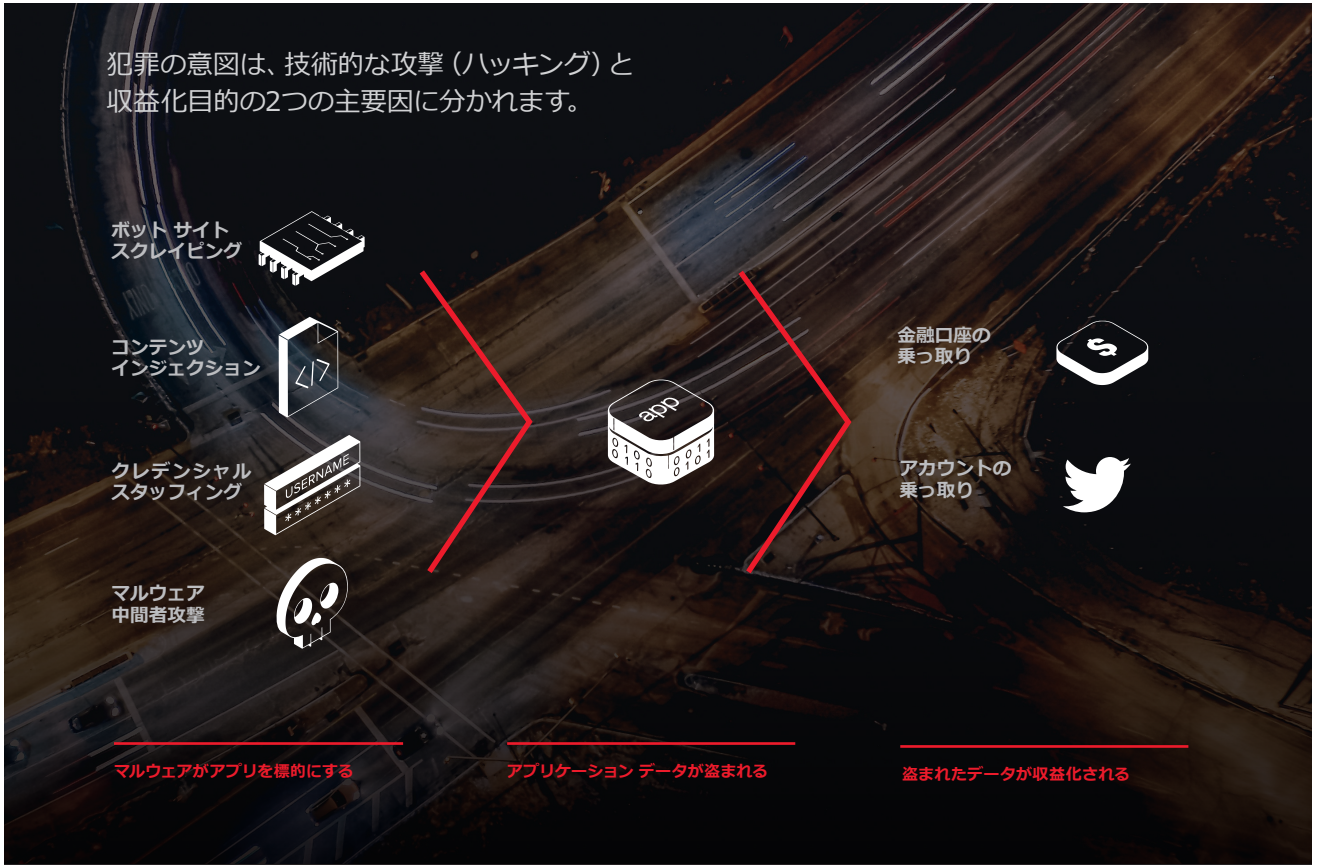
アプリケーションがビジネスを推進する中、ますます多くの機密情報がアクセスおよび取り引きされています。

サイバー犯罪者は、ソーシャル エンジニアリング、マルウェア作成、ボットネット ハーダー、クレジット カード不正利用、認証情報ロンダリング、盗んだデジタル情報の取引、企業の知的財産の販売など金銭目的でアプリのセキュリティを脅かそうとしています。

スキル レベル、時間の拘束、リソースおよび特殊化もさまざまで、犯罪の種類もさまざまですが、唯一不変の事実があります。攻撃者はアプリとそこに隠れているデータを虎視眈々と狙い、マルウェアを利用してデータを盗んでいます。

51%

情報漏洩にマルウェアが関与している割合 [1]

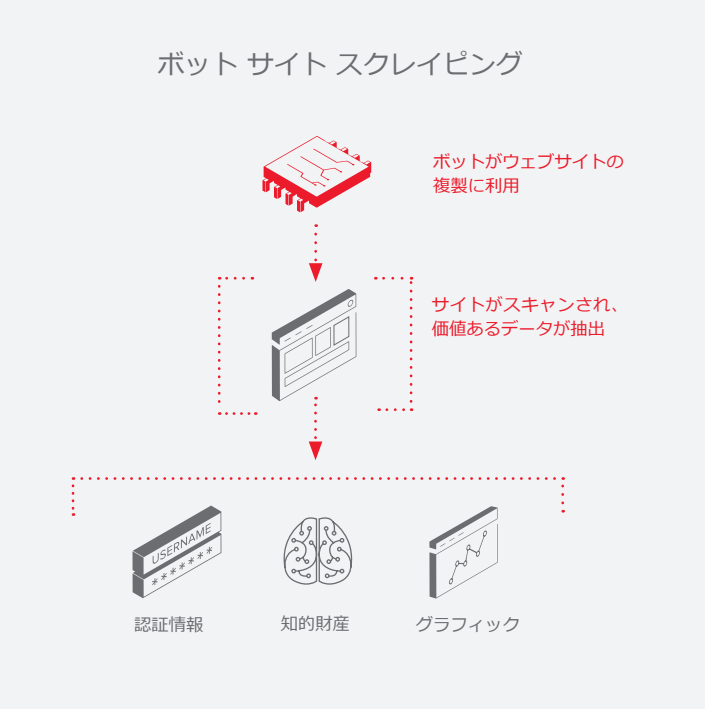


[1] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

攻撃：
マルウェアがデータを盗む仕組み

マルウェアは、ユーザに脅威をもたらすことを目的とした悪意のあるソフトウェア（ウイルス、ワーム、スパイウェア、ランサムウェア、トロイの木馬、ルートキットなど）を示す一般的な用語です。戦略、技術および方法は変わりますが、犯罪の意図は主に、技術的な攻撃（ハッキング）および収益化目的（データの悪用）の2つに分かれます。

サイバー犯罪者がマルウェアを利用し、アプリケーションの完全性を侵害して、個人データを盗む方法をいくつか説明します。



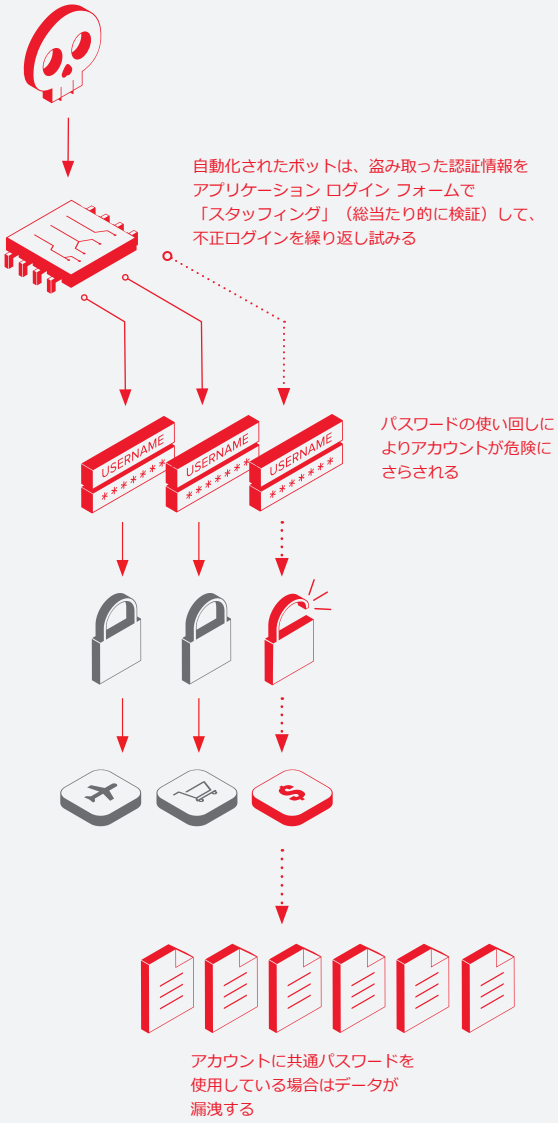
ボット サイト スクレイピング

2016年、インターネット上のトラフィックの半分以上は、人ではなく、ソフトウェアにより発信されました。[2]すべてのボットが悪いというわけではありませんが[3]、サイバー犯罪者はさまざまな悪意のある目的のために自律プログラムを利用します。たとえば、ボットを使用すると簡単にWebサイトを複製できます。複製したWebサイトは、価格情報（競合会社が利用）、ビデオやPDFなどの知的財産、Webコードに隠れていることがある電子メール アドレスやユーザ名、およびロゴやグラフィック（攻撃者がフィッシング サイトを設計するときに参考にできる）をスキャンできます。

攻撃者は、ボットを使用して、ログイン設計が不完全なウェブサイトからユーザ名を抽出することもできます。たとえば、あるサイトのログイン画面で、ユーザ名とパスワードの両方が正しくない場合は「ユーザ名が正しくありません」というメッセージが表示され、ユーザ名が正しくて、パスワードが正しくない場合は「パスワードが正しくありません」というメッセージが表示されるとします。このような場合、ユーザ名を検証および検出するボットを簡単に構築できます。また、攻撃者は、複数回のログインの失敗を検知できるWebアプリケーション ファイアウォールによる防御を回避するため、異なるIPアドレスを使用した大規模なボットを利用できます。

[2] https://www.recode.net/2017/5/31/15720396/internet-traffic-bots-surpass-human-2016-mary-meeker-code-conference
[3] http://botnerds.com/types-of-bots/

クレデンシャル スタッフィング



クレデンシャル スタッフィング

ユーザと認証情報のユーザが必ず一致するという考えは危険です。マルウェアベースの認証情報盗難は、現在組織が直面している最大のセキュリティ問題の1つとして急浮上しています。2017年上半期で、2,227件のデータ漏洩事件が報告され、60億件のレコードが漏洩し、膨大な数のアカウントが危険にさらされました。[4]犯罪者は漏洩したレコードを何に使うのでしょうか。クレデンシャル スタッフィングは、サイバー犯罪者がログイン認証情報を取得して、企業または個人のアカウントを乗っ取るSentry MBAなどのマルウェア ツールを利用した自動化攻撃です。[5]

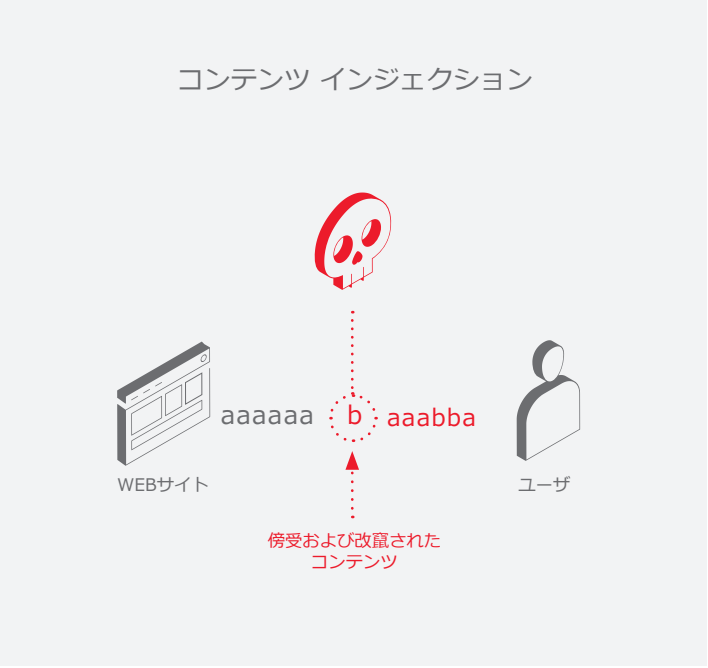
認証情報が漏洩した後でもパスワードを変更していれば、このような攻撃は成功していませんでした。しかし、管理するオンライン アカウントが大量にあるため、75%のユーザはその所有するアカウントで認証情報を使い回しています。[6] このような危険なパスワードの扱い方により、クレデンシャル スタッフィング攻撃が1~2%の確率で成功してしまいます。つまり、サイバー犯罪者が、盗まれた認証情報レコードを100万件入手できれば、10,000~20,000件のアカウントを簡単に乗っ取ることができます。さらに、ダーク ウェブでは、漏洩した数十億件の認証情報がわずかな金額で販売されています。[7]

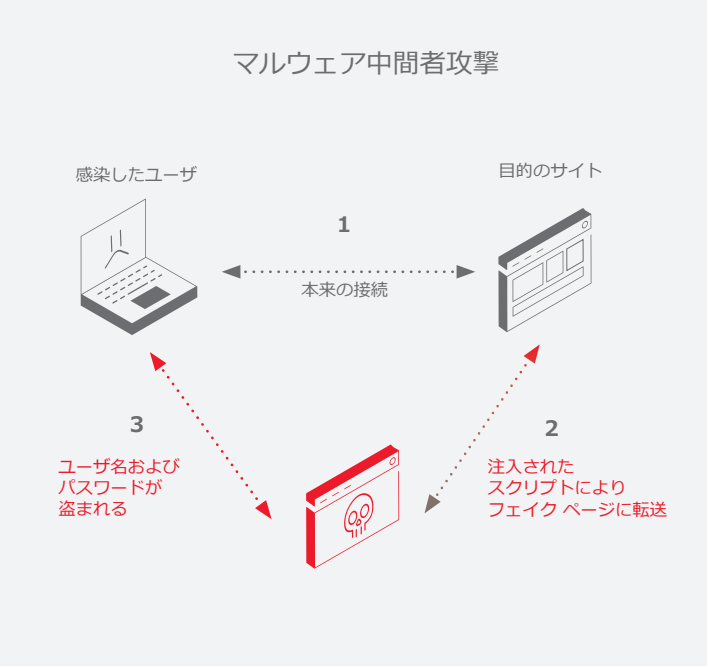
クレデンシャル スタッフィングが大きな脅威となる理由、およびその対抗策の詳細については、『クレデンシャル スタッフィング：セキュリティの蔓延』を参照してください。

3/4

4人中3人のユーザが複数のアカウントで同じパスワードを使い回している

[4] https://pages.riskbasedsecurity.com/hubfs/Reports/2017%20MidYear%20Data%20Breach%20QuickView%20Report.pdf
[5] https://www.infosecurity-magazine.com/news/sentry-mba-tool-used-in-attacks-on/
[6] https://www.entrepreneur.com/article/246902
[7] https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html?_r=0





コンテンツ インジェクション

プライバシに関する不安が高まり、暗号化のサポートが強化されたことで、2016年初めてインターネットの大部分が暗号化されました。[8]

これはデータ保護を心配する人には朗報である一方、オンライン トラフィックの半数近くが中間者 (MITM) 攻撃の危険にさらされ、脆弱であることを意味します。

MITM攻撃は、サイバー犯罪者が送受信間の通信を両者に知られることなく盗聴、傍受または改竄することです。暗号化されていないWebサイトは、サーバからブラウザに送信されるときに、ISPなどの転送、同じワイヤレス ネットワーク上のユーザまたはハッキングされたルータを参照できれば誰でも簡単に傍受および改竄できます。HTTPSによる暗号化の保証がない場合、ユーザは、閲覧 (およびデータを入力) しているページが、自分の意図するページであることを確信できません。

攻撃者は、マルウェア、悪意のあるスクリプトおよびフェイク メッセージをブラウザに注入することもできます。クロスサイト スクリプティング (XSS) に注意してください。これは、攻撃者が、個人情報を盗む、モバイル デバイスを乗っ取る、送金するなどのために、信頼できるWebサイトにスクリプトを注入する攻撃です。[9] 一部のISPでは、ユーザのトラフィックを監視し、独自の広告をブラウザに表示し始めています。[10]これに対しサイバー犯罪者は、クリックジャッキング (悪意のあるリンクを正常なコンテンツに隠すこと) を利用し、バナー広告詐欺を行う、またはユーザを騙してマルウェアをインストールさせようとしています。

マルウェア中間者攻撃

この特殊な攻撃では、マルウェアに感染したユーザがサイトを閲覧すると、マルウェアは、認証情報を盗むサイトとして、そのURLを認識して、悪意のあるJavaScriptを注入します。これは、コンテンツ インジェクションと非常によく似ていますが、ソフトウェア レベルでの動作です。注入されたスクリプトは、セッションをフェイク ページに転送し、ユーザのユーザ名およびパスワードを収集します。

[8] https://f5.com/labs/articles/threat-intelligence/ssl-tls/the-2016-tls-telemetry-report-24674
[9] https://f5.com/labs/articles/threat-intelligence/malware/webinject-analysis-newsidroncom-22441
[10] https://www.infoworld.com/article/2925839/net-neutrality/code-injection-new-low-isps.html

収益化：
犯罪者はどのようにして現金を得るか

犯罪者はアプリケーションからデータを盗んだ後、そのデータの収益化を考えます。その手口は、銀行口座の認証情報を盗んで漏洩させる、またはランサムウェアを使用して企業や個人から身代金を脅し取るといった単純な場合もありますが、知的財産、ユーザIDおよび電子メール アドレスを他の犯罪者やダークネット フォーラムの見知らぬユーザに売るといった場合もあります。[11]

ハッカーが盗んだデータを収益化するときの一般的な方法をいくつか説明します。

金融口座の乗っ取り

犯罪者は、大量に盗んだ認証情報を利用して、どのような方法で最も利益を得ることができるでしょうか。これが金融口座であれば答えは簡単です。金融口座を乗っ取り、金銭、株またはマイレージ サービス ポイントをリモート サーバに送信し、ここでマルウェアにより、犯罪者が盗んだアカウントで不正取引を処理します。

同時に、攻撃者（またはその利用するボット）が、盗んだアカウントからストアドバリュー、クレジット カード番号およびその他の個人を特定できる情報を収集します。

アカウントの乗っ取り

盗まれたすべての認証情報が、高額な金融口座へのアクセスに利用できるわけではありません。しかし、攻撃者は、このデータからも利益を上げることができます。

盗んだTwitterアカウントは、ダーク ウェブで1件10セント程度でしか販売できませんが、攻撃者がハイジャックしたコンピュータでボットを稼働させ、毎日数千のアカウントを盗んでいるとすれば、非常にいい儲け話です。[13]

11 https://darknetmarkets.co/corporate-bankers-stealing-own-company-data-to-sell-on-darknet/
12 https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/
13 https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/

$80

PAYPAL口座を1口座盗んでダーク ウェブで売れば$80の利益になります[12]

盗んだ口座で
何ができるか

盗んだ口座を収益化する最も簡単な方法は、不正入金です。攻撃者は、一連のeBayアカウントを使用して偽の買い手と偽の売り手のネットワークを作り、盗んだクレジットカードをロンダリングできます。ここでのすべての購入は最終的に攻撃者の利益になります。また、乗っ取ったアカウントを使用して、他のユーザにスパムを送る、クリック詐欺でバナー広告クリックを稼ぐ、なりすましのための個人情報（郵便番号、家族の名前、電子メールなど）を販売、または個人情報を利用して関連アカウントを不正利用できます。

攻撃者は、盗んだNetflixアカウントを数ドルで他のユーザに販売でき、アカウントを購入したユーザは、元の所有者に知られることなく映画を無料で見ることができます。[14] Uberアカウントは、盗んで販売するための標的として注目されつつあり、ダーク ウェブ フォーラムで1件2ドルで販売されています。[15]

プラットフォームの社会的な特性により特に価値のあるFacebookアカウントを不正利用するために攻撃者が利用できるマルウェアは数多くあります。Facebookユーザは個人を特定できるあらゆる情報（母親の旧姓、故郷、高校、子供の名前など）を投稿するので、Facebookアカウントはなりすましを狙う攻撃者にとっての宝の山となっています。また、Facebookアカウントから収集される情報は、偽装誘拐などに利用されています。この手口は、攻撃者が犠牲者を誘拐している振りをして、その友人や家族に身代金を要求するものです。[16]

[14] https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/
[15] https://nakedsecurity.sophos.com/2016/08/09/what-your-hacked-account-is-worth-on-the-dark-web/
[16] https://f5.com/labs/articles/threat-intelligence/cyber-security/virtual-kidnapping-the-latest-in-an-endless-stream-of-scams-25840

戦略：
多層防御による組織の保護

多くのサイバー犯罪者が大量のデータを盗み、そのデータを現金に換える方法はたくさんあります。こうした背景から、マルウェア問題の解決策があるか不安に思うかもしれません。このような攻撃を確実に防ぐことはできませんが、多層防御戦略により、マルウェアに対する脆弱性を劇的に軽減できます。

強力な認証

防御の最初の問題は、強力な認証システムです。認証情報はほぼ必ずマルウェア攻撃の標的となるため、強力な認証により、ユーザのIDおよび組織のデータのセキュリティを確保できます。

しかし現状は、強力な認証は非常に高価であるため、組織は、C レベル チーム メンバや価値のある企業情報にアクセスする従業員など、ハイリスクなユーザだけに多要素認証を実装せざるを得ません。

テクノロジは進化し続けています、同様に、サイバー犯罪者がお金を稼ぐための詐欺の手口も進化し続けています。

不正行為の監視

すべての業界の企業は、組織に年間数十億ドルの損害を与える多面的な脅威であるWeb不正行為のリスクにさらされています。不正行為を完全に防ぐことはできませんが、いくつかの方法を利用して、その影響を軽減できます。

不正行為の監視は、マシンベースの分析と、マシン ラーニングでは善悪を完全には分類できないアカウントの動作を評価する人間の専門家を組み合わせるものですが、[17]その実現とサポートにはコストがかかります。しかし、強力な不正行為監視サービスにより、マルウェアベースの盗難による壊滅的な被害を軽減できます。

WEBアプリケーション ファイアウォール

強力なWebアプリケーション ファイアウォールを使用することで、組織は、マルウェア攻撃からの防御を簡単に行うことができます。これにより、ボットによるサイト情報流出を防ぐことができ、その結果、知的財産を守り、フィッシング攻撃が成功する可能性を下げることができます。総当たり（ブルートフォース）攻撃およびクレデンシャル スタッフィング攻撃を検知および停止、ブラウザ セッション ハイジャック攻撃を特定およびブロック、不正行為の実行を防止できます。

これらのソリューションを使用しても、どこでも起こり得るマルウェア問題を完全に防ぐことはできませんが、多層防御戦略により、マルウェアによる組織への影響を軽減できます。

現在、そして今後の脅威から組織を守る方法の詳細は、F5 Labsをご覧ください。

[17] http://www.bankinfosecurity.eu/interviews/tips-for-fighting-fraud-big-data-i-2269

アプリのセキュリティを第一に考える

常時稼働、常時接続のアプリは、ビジネスを強化および変革する一方、
ファイアウォールに保護されないデータへのゲートウェイにもなり得ます。
ほとんどの攻撃はアプリ レベルで発生しているため、ビジネスを推進する機能を
保護することは、攻撃を受けるアプリを保護することにつながります。

F5ネットワークスジャパン合同会社

東京本社
〒107-0052 東京都港区赤坂4-15-1 赤坂ガーデンシティ19階
TEL 03-5114-3210 FAX 03-5114-3201

西日本支社
〒530-0012 大阪府大阪市北区芝田 1-1-4 阪急ターミナルビル 16 階
TEL 06-7222-3731 FAX 06-7222-3838

お問合わせ先：https://f5.com/jp/fc/

F5. EBOOK-SEC-169936955 1017