Symantec

INTERNET SECURITY THREAT REPORT

概要

インターネットセキュリティ脅威レポート

2019年インターネットセキュリティ脅威レポート

ISTR

第24号

概要

フォームジャッキング、標的型攻撃、ツールの現地調達が企業を脅かす。

ハエが蜜にたかるように、犯罪者は確実に手っ取り早く稼げる最新のエクスプロイトに群がります。ランサムウェアとクリプトジャッキングは全盛期を過ぎ、今やフォームジャッキングが注目されています。

『シマンテックインターネットセキュリティ脅威レポート第 24 号』では、グローバルな脅威活動、サイバー犯罪の傾向、および攻撃者の動機に関する最新の分析結果をお届けします。

このレポートでは、全世界 1 億 2,300 万の攻撃センサーから送られるイベントを記録し、1 日に 1 億 4,200 万件もの脅威をブロックし、157 を超える国で脅威活動を監視する世界最大の民間脅威インテリジェンスネットワーク、シマンテック Global Intelligence Network のデータを分析しています。

{FORMJACKING}

フォームジャッキング

フォームジャッキングで手っ取り早く稼ぐサイバー犯罪者

フォームジャッキング攻撃はシンプルで効率的です。サイバー犯罪者は小売業者の Web サイトに悪質なコードをロードし、買い物客のクレジットカード情報を盗みます。毎月平均して 4,800 社以上の Web サイトが侵害されています。

攻撃対象には、Ticketmaster 社や British Airways 社をはじめとする有名企業のほか、中小規模企業も含まれ、控えめに見ても前年だけで数千万ドルが犯罪者の手に渡りました。

闇取引市場ではカード 1 枚分の情報が最大 45 ドルで取引されるため、侵害した Web サイト 1 つあたり 10 個のクレジットカード情報を盗むとして、1 カ月で最大 220 万ドルを簡単に稼ぎ出すことができます。38 万枚以上のクレジットカード情報が盗まれた British Airways 社に対する攻撃だけで、犯罪者たちは 1,700 万ドルを超える利益を上げたと見られています。

RANSOMWARE

ランサムウェア

CRYPTOJACKING

クリプトジャッキング

減少したものの、いまだ健在

ランサムウェアとクリプトジャッキングは人気のある攻撃手法でしたが、2018 年は利益が少なくなった結果、活動が下火になりました。

ランサムウェアは 2013 年以降初めて、全体で 20 パーセント減少しました。ただし、企業を狙ったものは 12 パーセント増加しています。

暗号通貨の価格が 90 パーセント急落したため、2018 年にはクリプトジャッキングが 52 パーセント減少しました。とはいえ、クリプトジャッキングは、手間がかからず簡単に参入できるため、いまだ人気があります。シマンテックが 2018 年にブロックしたクリプトジャッキング攻撃の件数は前年比 4 倍となっています。

TARGETED ATTACKS

標的型攻撃

破壊的な性質を持つ標的型攻撃

サプライチェーン攻撃と「ツールの現地調達」手法がサイバー犯罪の主流となっています。サプライチェーン攻撃は 2018 年に 78 パーセントの急増を見せています。

「ツールの現地調達」手法により、攻撃者は正規のプロセス内に身を隠すことができます。たとえば、悪質な PowerShell スクリプトの使用は、前年比で 1,000 パーセントも増加しました。

シマンテックは毎月 11 万 5,000 件の悪質な PowerShell スクリプトをブロックしていますが、この数字は PowerShell の使用量全体の 1 パーセントにも達しません。すべての PowerShell 活動をブロックするような厳格な対策は業務の中断をもたらすため実際には導入できません。このことも、多くの標的型攻撃グループが攻撃の検出を回避するために「ツールの現地調達」手法をよく使用する理由となっています。

MORE AMBITIOUS
より大掛かり

AND STEALTHIER
しかも気づかれにくい

攻撃者が、スピアフィッシングなどの確実な手法を使用して企業に侵入する傾向も強まりました。攻撃者の主な目的がインテリジェンスの収集であることに変わりはありませんが、それと同時に破壊活動を目的とするグループも存在します。現在、標的型攻撃グループの 10 分の 1 近くが、企業の事業活動を破壊したり中断したりするためにマルウェアを使用しています。これは前年から 25 パーセントの増加です。

たとえば、2 年間の沈黙の後、再び中東の企業を標的に姿を現した Shamoon は、ワイパーマルウェアをばらまいてコンピュータ上のファイルを削除する重大な脅威です。

クラウド

クラウドの難しさ: クラウド内のセキュリティは各企業の責任

クラウドワークロードやストレージインスタンスの設定に 1 つでも誤りがあると、企業に何百万ドルものコストやコンプライアンス上のリスクをもたらす原因になりかねません。2018 年には、7,000 万件を超える情報が、不適切な設定の S3 バケットが原因で盗難に遭ったり漏えいしたりしました。攻撃者は、Web 上の既存のツールを使って、設定が不適切なクラウドリソースを特定できます。

侵入者が、Meltdown、Spectre、Foreshadow などのハードウェアチップ脆弱性を利用して、同一の物理サーバーでホストされているクラウドサービス上の企業各社の保護メモリ領域にアクセスすることも可能です。悪用に成功すると、通常はアクセスが禁止されているメモリ上の場所にアクセスできるようになります。

これはとりわけクラウドサービスでは重大な問題です。クラウドインスタンスは独自の仮想プロセッサを備えていますが、メモリプールは共有しているため、1 つの物理システムへの攻撃が成功すると、複数のクラウドインスタンスからデータが漏洩するおそれがあるのです。

IoT

ユーザーのお気に入りの IoT デバイスは攻撃者にとってもお気に入り

感染した IoT デバイスの 90 パーセントはルーターとネットワークカメラですが、ほとんどすべての IoT デバイス(スマート電球、スマートスピーカーなど)に脆弱性があります。

標的型攻撃グループは、デバイスを破壊したりデータを消去したり、資格情報やデータを盗んだり、あるいは SCADA 通信を傍受したりするために簡単に利用できる侵入経路として、ますます IoT に注目しています。

さらに、産業用 IT が、運転制御システムや産業制御システムを侵害する能力を持つ Thrip や Triton などの脅威グループとのサイバー戦争の場を提供しています。

ELECTION INTERFERENCE 2018

2018 年の選挙干渉

ソーシャルメディアフィードの選挙への影響力

幸いにも、大いに注目された 2018 年米国中間選挙に大きな混乱はありませんでした。ただし、ソーシャルメディアでは、相変わらず派手なバトルが繰り広げられました。

正規の政治 Web サイトを模倣した悪質なドメインが発見されて閉鎖されたかと思えば、ロシアに関連したアカウントが第三者を使ってソーシャルメディア広告を買い占めたりもしました。

ソーシャルメディア各社は、選挙干渉との闘いで積極的な役割を果たしました。Facebook 社は選挙干渉に取り組むための司令室を設立し、Twitter 社は人々の投票意欲を削ぐメッセージを投稿していた 10,000 以上のボットを削除したのです。

詳しくは、シマンテックの『2019 年インターネットセキュリティ脅威レポート(ISTR)』
https://symc.ly/APISTR をダウンロードしてください。

シマンテックについて

シマンテックコーポレーション（NASDAQ: SYMC）はサイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るために、ノートンと LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。詳しくは www.symantec.com/ja/jp をご覧ください。

〒 107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ

www.symantec.com/ja/jp/

ISTR