GLOBAL APPLICATION & NETWORK SECURITY REPORT 2015-2016 日本語速報版

本ドキュメントは、Radware が発行する「2015-2016 年版グローバルアプリケーション＆ネットワークセキュリティレポート」の簡易版です。本ドキュメントは、2015 年のセキュリティ業界における気づきおよび分析内容と、Radware のセキュリティ専門チームである Emergency Response Team (ERT)が日々直面するサイバー攻撃との闘いの中で得た知見、そして第三者視点として 2 つのサービスプロバイダの意見をベースにしており、ビジネスおよび技術の両方の側面から、包括的かつ客観的な内容となっています。2016 年度に向けたサイバー攻撃対策計画の参考資料としてお役立ていただければ幸いです。

まとめ：「攻撃対象の『例外』はない。しかし、対策ができている企業組織は少ないということ。」

近年の猛攻とも言えるサイバー攻撃の結果、誰もが攻撃対象となりえる中、対策ができている企業組織は少ないという事実がわかっています。この事実は弊社実施のアンケート結果にも如実に現れ、業種に関わらず、金融業界やインフラ業界からクラウドサービス事業者に至るまで広がっています。

➢ 2015 年中に攻撃を受けた企業組織は 90%

弊社実施のアンケートでは、90%を超える企業組織が 2015 年中に攻撃を受けたと回答しています。

➢ 教育およびホスティングサービスに対する攻撃が増加傾向に

類似性を持つ業種/組織が攻撃を受ける傾向にあります。前年と比較し脅威数がさほど増加しなかった業種がある一方で、2015 年には教育およびホスティングサービスにおいて、危険度が「中」から「高」に上がっています。この事実は、2016 年これらの業種が他業種と比較し、DoS/DDoS 攻撃をはじめとするさまざまなサイバー攻撃の標的になりやすいことを示します。

➢ サイバー攻撃対策の変化

60%を超える企業組織が不正アクセスやウイルス、ワームに対する対策を実施している一方で、同じ 60%が標的型攻撃および情報漏えいに対する対策は「やや不十分」としています。DDoS 攻撃に対しては、対策している企業組織と、していない企業の割合が、ほぼ半々でした。

➢ 全面的に見られる対策のギャップ

回答者の 1/3 が、「ネットワーク飽和型攻撃」に対する弱さを、また 1/4 が「ネットワーク脆弱性」や「HTTPS/SSL 攻撃」に対する弱さを自覚していると回答しています。「全体的な対策」の弱さは平均的となっており、これは今日の企業組織におけるセキュリティ対策のギャップを表しています。

動機と影響の変化

➢ サイバー攻撃の主なる影響は「遅延」

過去、セキュリティ投資の主なる目的は、サービスの停止を防ぐことでした。しかし、今回の調査の回答者の半分は、攻撃の怖さは、サービスの完全停止よりもむしろ、遅延にあると指摘しています。この事実と、オーバープロビジョニングを考慮すると、サービス停止対策は二の次とされている傾向が見て取れます。

➢ DDoS は相変わらずサイバー攻撃の中心的存在

2014 年同様、回答者の半数が DDoS 攻撃を大きな脅威と捉えていると回答しています。不正アクセスはその次点です。

➢ ランサム攻撃の増加がサイバー攻撃を変える

本年のサーベイ結果では、ランサム(身代金)を目的とした攻撃者の増加が目立ち、2014 年の 16%から 25%にまで増加しています。さらに、1/3 の回答者がランサム攻撃もしくは SSL/TLS ベースの攻撃を受けたと回答しています。
スイスに拠点を置く暗号化メールプロバイダ、ProntonMail は、2015 年 11 月に Armada Collective(アルマダ・コレクティブ)と名乗る新手のハッカーグループによる身代金脅迫を受けた後、一連の攻撃被害を受けました。脅迫内容は、「攻撃を止めて欲しければ身代金を払え」というもので、攻撃は回線飽和型攻撃およびアプリケーションとネットワークの両方を狙うものでした。

➢ 攻撃がもたらすであろう影響の拡大

本年のサーベイ結果では、企業組織が恐れる攻撃による影響が、「評判の悪化」から、「SLA の継続性」に変化しています。攻撃がもたらす企業の評判悪化は依然大きな問題であるものの、2014 年の 47%から 26%へと大きく減少しました。多くの企業組織は、それよりも、お客様へサービス提供ができなくなることをより大きな懸念事項と捉えています。

➢ セキュリティ自動化の必要性

今回のレポートでは、”APDoS” (Advanced Persistent DoS/標的型持続性 DoS) の存在が明らかになりました。この攻撃の登場により、より高度な検出と攻撃緩和技術(ミティゲーション技術)が早急に求められるようになり、今までにないレベルで DDoS ミティゲーションサービスプロバイダとの関係を密にする必要が生ることとなりました。
APDoS 攻撃は非常に大規模なネットワーク層を対象とした回線飽和型 DDoS 攻撃と、アプリケーション層フラッド(HTTP flood) を伴い、ランダムな間隔で SQL 攻撃やクロスサイトスクリプティング攻撃で追い討ちをかけます。攻撃者は 1 秒に数千万リクエストを発するような 5～8 の異なる攻撃手法を同時に用います。SYN フラッドが用いられることも多いですが、この場合、攻撃対象の企業組織だけでなく、ISP にも攻撃の影響が及ぶ場合もあります。

➢ 現在の対策における課題：「マルチベンダ」と「マニュアル制御」

昨今の攻撃に対応していくために、自動防御と迅速な脅威分析および攻撃緩和が早急に求められます。しかし、未だ多くの企業組織では、多大なマニュアル操作を伴うパッチワーク的対策が中心となっているのが現状です。91%がマルチベンダソリュ

ーションを利用していると回答しており、さらに 6%はサイバー攻撃に対してたった 1 つのソリューションによる対策しかしていないとしています。また、約 3/5 は、マニュアル設定を含むある程度のマニュアルチューニングが必要であると回答しています。

- **ハイブリッドソリューションへの必要性は、継続して増加傾向に**

クラウドベースの対策とオンプレミスの対策を統合したハイブリッドソリューションの導入は加速を続けています。ハイブリッド対策を行っていると回答した企業組織は、2014 年には 21%であったのに対し、2015 年には、41%に増加しています。

- **短期集中的な攻撃の増加**

短期集中的攻撃(60 秒以内)は増加傾向にあります。3 大攻撃の経験者の半数以上が、攻撃は 1 時間以内で終わったと回答しています。2014 年での回答は 27%でした。攻撃者は、ボットネットを用いた自動攻撃により、短期間に大量のトラフィックを生み出す攻撃を行う一方で、そのボットネットを APDoS のような長期攻撃キャンペーンにも利用しているのです。

- **ネットワーク同様に狙われるアプリケーション**

本年は、ネットワークとアプリケーションの両方に対する攻撃の頻度の観点からも調査を行いました。攻撃手法にいくらかのバリエーションは見られますが、全般的に、ネットワークを対象にした攻撃もアプリケーションを対象にした攻撃も、頻度については類似点が見られます。これはつまり、今日のサイバー攻撃のキャンペーンにおいて、特に APDoS の場合、ネットワークとアプリケーションを同時に攻撃する傾向があることを意味しており、企業組織はその両方を守る必要があるといえます。
本レポートはまた、米国の某航空会社が受けた、自動的かつ進化した攻撃についても説明しています。攻撃ボットが偽の航空券購入者に成りすまし、不正なブッキングを行いました。その結果、搭乗者のいない飛行機が複数機飛び立つ、という事態を招いたのです。この事例は、この航空会社が最近のボットに対してどういったアプリケーションセキュリティを実施しすべきだったか、そして Web オペレータが本物のユーザとボットが成りすました偽のユーザを見分け、本来の、守るべきお客様の予約を受けるべきだったかを考えるいい事例です。
この事例およびその他の類似した被害事例を考慮すると、新たなレベルのセキュリティが求められ始めているといえます。セキュリティの自動化と、ボットネットに対抗するための「よいボット(white hat bot)」の開発を行うことができるセキュリティ専門家という新たな課題です。

2015 年、セキュリティは何が変わったか

2015 年は APDoS 出現の年であったといえます。複数の攻撃を同時実行する攻撃キャンペーンは、攻撃対象となる企業の情報基盤のネットワーク、サーバ、アプリケーションなど、あらゆるレイヤを狙ってきます。攻撃はより、しぶとく長期化する傾向が見られ、その背景には、ネットワークリソースを消費させる “low and slow” 攻撃技術が活用されていると思われます。さらに攻撃者側は、SSL ベースの攻撃や、HTTP フラッド攻撃で異なるページリクエストを行うなどの、攻撃検出の回避策をあみ出しています。
数年前、DoS といえばネットワーク層を狙うものであり、SYN, TCP, UDP, ICMP フラッドなどが有名でしたが、2010 年から 2012 年にかけ、さらに巧妙なアプリケーションレベル攻撃や SSL 暗号を用いた攻撃などが増加し始めました。最近では、アンプリフィケーション・リフレクティブ・フラッド(Amplification Reflective Flood)といった特定のタイプの DoS 攻撃手法が、ネットワークのみならず、アプリケーションを狙う攻撃者にも利用され始めています。2013 年により活発な動きを見せ始めた

DNS や NTP, CHARGEN などを悪用したリフレクティブ攻撃は、2014 年にかけても継続的に発生し続けました。リフレクティブ攻撃の増加の結果、インターネットパイプが、エンタープライズセキュリティの弱点のひとつとなってしまいました。
こういったサイバー攻撃を仕掛けるのは実に簡単であり、攻撃ツールも容易に入手が可能であるため、どの企業組織も DDoS のような脅威に晒されやすくなります。もはや、攻撃の回避は不可能であることを認識し、攻撃を受ける前提で考える必要があります。今早急に求められるのは、「早期発見、早期対処」なのです。

複数手段による攻撃への対策

進化し続ける脅威に直面する企業組織に求められるのは、新たな、そしてあらゆるタイプの攻撃に対する強固なセキュリティソリューションの実施です。
企業システムの脆弱性を探すため、ネットワークの異なるレイヤを狙ったり、データセンタを狙ったり、と、攻撃者はさまざまな攻撃を同時展開します。そのひとつでも成功すれば、攻撃者の勝ちです。企業組織への影響は甚大なものとなるでしょう。
あらゆるタイプの DDoS 攻撃の対策を効果的に行うために企業組織に求められるのは、ネットワークからアプリケーションに及ぶ幅広い攻撃に対策できる、単一ベンダによるハイブリッドソリューションです。ハイブリッドソリューションとはつまり、オンプレミスでのリアルタイムな検出と、大規模なボリューメトリック攻撃に対するクラウドベースのオンデマンドな対策の統合です。本来の意味での統合ソリューションとは、DDoS 対策をはじめ、ふるまい検知、IPS, 暗号化を用いた攻撃への対処および WAF (Web Application Firewall) など、求められるあらゆる技術の統合を意味します。
クラウドへの移行や IoT デバイスの普及、セキュリティの効率性の低下といった直近の傾向を考慮し、今年のレポートでは、攻撃がいかに、より複雑化してきているかに焦点を当てています。本レポートでは、攻撃における動機や手段、効率性などが確実に高まっていると同時に、進化を続ける脅威に対して迅速な対応が求められることを指摘しています。

著者について

Radware (NASDAQ:RDWR)は、仮想環境、クラウド、およびソフトウェア・デファインドによるデータセンタにおけるアプリケーションデリバリおよびサイバーセキュリティソリューションにおけるグローバルリーダーです。数々のアワードを受賞したソリューションポートフォリオは、IT 効果を最大化しながら、クリティカルなアプリケーションに対するサービスレベルを保証します。Radware のソリューションは全世界 10,000 を超える企業およびキャリアのお客様に採用され、低コストを保ちつつ、ビジネス継続性や生産性の最大化を実現しています。詳細は、www.radware.com(英語)もしくは www.radware.co.jp(日本語)をご参照ください。