2020 年 8 月 19 日

報道機関各位

ソニックウォール・ジャパン株式会社

SonicWall 2020 年上半期サイバー脅威レポートが悪意のある Microsoft Office ファイルの増加、ランサムウェアの米国および世界的な増加を報告

- *ランサムウェアは世界中で 20%増、米国では 109%急増*
- *マルウェア攻撃は世界中で 24%減*
- *フィッシング攻撃の 7%が新型コロナウイルス（COVID-19）のパンデミックを利用*
- *悪意のある Microsoft Office ファイルは 176%増*
- *23%のマルウェア攻撃は非標準ポートを利用*
- *IoT マルウェア攻撃は 50%増*
- *レポートは、215 以上の国と地域における 110 万個のセンサーから収集した脅威インテリジェンスデータを分析*

カルフォルニア州ミルピタス（米国時間 2020 年 7 月 23 日配信のプレスリリース抄訳）— SonicWall Capture Labs の脅威調査チームは本日、2020 年上半期 SonicWall サイバー脅威レポートを発表しました。このレポートでは、ランサムウェアの増加、新型コロナウイルス（COVID-19）パンデミックの日和見的利用、システムの弱点、サイバー犯罪者による Microsoft Office ファイル利用の高まりが指摘されています。

「サイバー犯罪者は機知に富み、自然災害時の人々の優しさ、危機時のパニック、そして日々使用されるシステムへの信頼を利用した罠を仕掛けてくることがよくあります」と SonicWall の社長兼 CEO のビル・コナーは述べています。「最新のサイバー脅威データによると、サイバー犯罪者は、不確実な時代にも、自分たちに有利になるように戦術を変化させ続けていることがわかります。これまで以上にリモートやモバイルが利用されるようになったことで、ビジネスは危険に常にさらされており、サイバー犯罪者業界はそのことを強く認識しています。組織は、その場しのぎのセキュリティ戦略や従来のセキュリティ戦略から脱却し、この新しいビジネスの常態はもはや新しいものではないことを認識することが不可欠です」

環境の変化によるマルウェア量の減少

2020 年の上半期、世界のマルウェア攻撃は、2019 年の上半期合計である 48 億件から 32 億件（24%減）に減少しました。今回の下落は、昨年 11 月に始まった下落傾向の継続です。

マルウェアの量と割合の変化には地域差があり、サイバー犯罪者の注目度の変化が浮き彫りになっています。例えば、米国（24%減）、英国（27%減）、ドイツ（60%減）、インド（64%減）では、いずれもマルウェアの量が減少しました。しかし、マルウェアの減少は必ずしも安全性の増加を指すわけではありません。それを示すように、ランサムウェアによる攻撃は同じ期間に急増しています。

ランサムウェア攻撃者による危険度の増加

世界的にマルウェアの量が減少しているにもかかわらず、ランサムウェアが企業にとって最も懸念される脅威かつサイバー犯罪者に好まれるツールであり続けており、2020 年上半期には世界全体で 20%（1 億 2,140 万件）の増加という驚異的な数字を示しています。

The Chertoff Group の創設者兼 CEO であるチャド・スウィート氏は、「リモートワークやモバイルワークフォースは、セキュリティの問題で転換期にあります」と述べています。「企業や組織がオンラインセキュリティを優先し、これまでは贅沢と見なされていたものを必須の安全や保護へと変化させ、普及させています」

また、米国と英国では対照的な結果が見られます。SonicWall Capture Labs の脅威研究者は、米国で 7,990 万件のランサムウェア攻撃（109%増）を記録したのに対し、英国では 590 万件のランサムウェア攻撃（6%減）を記録し、俊敏なサイバー犯罪者ネットワークの行動をもとにした風変りな傾向を認めました。

マルウェアを搭載した新型コロナウイルス（COVID-19）関連電子メール

世界的なパンデミックと社会工学的なサイバー攻撃の組み合わせは、フィッシングやその他の電子メール詐欺を利用するサイバー犯罪者にとって効果的な組み合わせであることが証明されています。2 月 4 日までさかのぼり、SonicWall の研究者は新型コロナウイルス（COVID-19）に特化した攻撃、詐欺、エクスプロイトの増加を検知し、第 1～第 2 四半期の間に新型コロナウイルス関連のフィッシングが 7%増加したことを報告しています。

予想されたように、新型コロナウイルス関連のフィッシングは 3 月に増加し始め、3 月 24 日、4 月 3 日、6 月 19 日に最も大きなピークを迎えました。これは、フィッシング全体とは対照的で、全体では 1 月に堅調な増加を見せますが、新型コロナウイルス関連のフィッシングが流行し始めた頃には、世界的にフィッシングはわずかに減少傾向にありました（15%減）。

Office を用いた攻撃は今も健在

現在、何百万人もの作業者がリモートで作業を行う必要性に迫られていることから、人々はビジネス生産性のアプリケーション群に依存しており、Microsoft Office は必須のものになっています。サイバー犯罪者はこうした環境の変化にいち早く対応し、SonicWall の脅威研究者は、信頼できる Microsoft Office のファイルタイプを装った新しいマルウェア攻撃が 176%増となったことを観測しました。

SonicWall Capture Advanced Threat Protection（ATP）と Real-Time Deep Memory Inspection™（RTDMI）テクノロジーを活用することで、SonicWall は 2020 年に、Microsoft Office ファイルの 22%と PDF ファイルの 11%で新たに確認されたマルウェアの 33%を占めていることを発見しました。特許出願中の RTDMI™テクノロジーは、この間に記録的な 120,910 個の「いまだかつて見られなかった」マルウェアの亜種を識別しました。これは、2019 年の上半期と比較して 63%の増加です。

「サイバー犯罪者は、既知のマルウェアの亜種を使用するにはあまりにも洗練されているため、従来のサンドボックス技術のようなセキュリティ制御を破るために、マルウェアを再定義したり書き換えたりしています。そして、それが功を奏しているのです」とコナーは述べます。

マルウェアで最もリスクの高い米国の州とは？

世界中に散らばる 110 万個以上のセンサーが 24 時間体制で脅威の情報を収集している SonicWall の新しい「マルウェア拡散」データは、マルウェア攻撃のリスクが最も高い米国の州を示しています。

米国では、シリコンバレーのあるカリフォルニア州が 2020 年のマルウェア総量で 1 位となっています。しかし、カリフォルニア州はリスクの高い州の上位半数に含まれておらず、最もリスクの高い州ではありませんでした。マルウェアの拡散状況に基づいた上位 5 位までの最もリスクの高い州は、バージニア州（26.6%）、フロリダ州（26.6%）、ミシガン州（26.3%）、ニュージャージー州（26.3%）、オハイオ州（25.3%）でした。

興味深いことに、カンザス州の企業はマルウェアに遭遇する可能性が高く、同州のセンサーのほぼ 3 分の 1（31.3%）がマルウェアを検知しています。対照的に、ノースダコタ州のセンサーの 5 分の 1 強（21.9%）がマルウェア攻撃を記録していました。

マルウェアの拡散を追跡するこの方法は、マルウェア攻撃を検知したセンサーの割合を計算することで行われ、その結果、組織が位置する地域でマルウェアが見られる可能性があるかどうかについて、より有用で正確な情報を得ることができます。マルウェアの拡散率が高いほど、特定の地域でマルウェアが見られる確率が高いことを示しています。

非標準ポートを使った攻撃の検知率が再上昇

全体では、2020 年のこれまでのところ、平均 23%の攻撃が非標準ポートを経由して行われており、SonicWall が 2018 年に攻撃元区分の追跡を開始して以来、最高となっています。

マルウェアを非標準のポートに送信することで、攻撃者は従来のファイアウォール技術を迂回することができ、ペイロードの成功率を高めることができます。「非標準」ポートはデフォルトの割り当て以外のポートで実行されているサービスで利用されます（例：ポート 80 と 443 は Web トラフィックの標準ポート）。

2020 年の第 1 四半期から第 2 四半期までの間に、2 件の月次記録を更新しました。2 月の非標準ポート攻撃が 26%に達した後、5 月には前例のない 30%に増加しました。その月の間に、VBA Trojan Downloader など、特定の攻撃が急増しており、それが検知率の増加の一因となっている可能性があります。

IoT が依然として脅威の要因に

リモートワークに従事する従業員やリモートワークフォースにより、冷蔵庫、ベビーモニター、ドアベル、ゲーム機などの IoT（Internet of Things）デバイスなどが、多くの新たなリスクの引き金になる可能性があります。IT 部門は、企業の領域が従来の境界線を超えて拡大しているため、ネットワークやエンドポイントに群がる無数のデバイスに取り囲まれています。

SonicWall の研究者は、IoT マルウェア攻撃が 50%増加していることを観測しました。これは、個人や企業が自宅で作業を導入するようになるにつれ、オンラインに接続されているデバイスの数が増えていることを反映しています。未確認の IoT デバイスは、通常は安全性の高い組織へのサイバー犯罪者にとっての入り口を提供することになりかねません。

2020 年上半期 SonicWall サイバー脅威レポートは、こちらをご覧ください。
https://sonicwall-pub.snwl.jp/files/whitepaper/SonicWallThreatReport-20200814.pdf
また、要約のスライド版は、こちらをご覧ください。
https://sonicwall-pub.snwl.jp/files/whitepaper/SonicWallThreatReport-summary-20200814.pdf

SonicWall について

SonicWall は、Boundless Cybersecurity を提供することにより、誰もがリモート／モバイルで危険にさらされながら仕事をするという超分散化時代のビジネスの現実に対処します。SonicWall はシームレスな防御を提供し、非常に巧妙なサイバー攻撃を阻止します。これによって、無限に存在する脆弱性ポイントすべてを保護し、リモート勤務やモバイル化、クラウド利用を活発に進める人員を守り、ひいてはビジネスのニューノーマルに対応すべくモバイル化を進める組織のセキュリティを確保します。未知の領域を探求し、リアルタイムの可視性を提供しながら経済の大躍進を実現している SonicWall は、サイバーセキュリティ業務上の課題を解決して世界中の企業や政府、SMB をサポートします。詳細については、https://www.sonicwall.com/ja-jp/ をご覧いただくか、Twitter、LinkedIn、Facebook、Instagram で当社をフォローしてください。

広報担当の連絡先

ソニックウォール・ジャパン株式会社
マーケティング 白畑　mshirahata@SonicWall.com