お知らせ

2022 年 3 月 16 日

キヤノンマーケティングジャパン株式会社

2021 年サイバーセキュリティレポートを公開
～多発するランサムウェア攻撃、いまだ続く脆弱性を悪用した攻撃などを解説～

キヤノンマーケティングジャパン株式会社（代表取締役社長：足立正親、以下キヤノンMJ）は、“2021年サイバーセキュリティレポート”を公開しました。甚大な被害を及ぼすランサムウェア攻撃や、セキュリティアップデートが適用されていない古い機器やソフトウェアの脆弱性を悪用した攻撃など、2021年に発生したサイバーセキュリティの脅威動向や検出されたマルウェアについて解説します。

キヤノン MJ グループはセキュリティソリューションベンダーとして、サイバーセキュリティに関する研究を担うサイバーセキュリティラボを中核に、最新の脅威やマルウェアにおける動向の情報収集および分析を行い、セキュリティ対策に必要な情報を定期的に発信しています。

このたび、2021 年に国内で検出されたマルウェアや国内外で発生したサイバー攻撃事例について解説した“2021 年サイバーセキュリティレポート（以下、本レポート）”を公開しました。同年はランサムウェアを用いたサイバー攻撃が多数発生し、その手法の多様化・巧妙化が進み、企業規模を問わずさまざまな被害が報告されました。また、約 4 年前に明らかにされた脆弱性が悪用され続けているなど、適切なアップデートがされていない古い機器やソフトウェアの脆弱性をついた攻撃も確認されています。

本レポートでは、このような 2021 年に発生したサイバーセキュリティの脅威動向について、サイバーセキュリティラボ独自の視点で分析、考察し、対策を紹介しており、セキュリティ対策に役立つ内容となっています。

2021 年サイバーセキュリティレポート
【 https://eset-info.canon-its.jp/malware_info/special/detail/220316.html 】

● 報道関係者のお問い合わせ先：キヤノンマーケティングジャパン株式会社　広報部　03-6719-9093
● サイバーセキュリティ情報局ホームページ：canon.jp/cybersecurity

＜2021年サイバーセキュリティレポートの主な内容＞

■ 2021年マルウェア検出統計

国内のマルウェア検出数は 2020 年下半期をピークに減少傾向であるものの、2021 年は 2019 年以前に比べ依然として高い水準にありました。また、詐欺を目的としたマルウェアなどは 2020 年に比べても多く検出されています。2020 年以降は、新型コロナウイルス感染症の感染拡大をきっかけにリモートワークやオンライン学習などが普及し、多くの組織が対応に迫られました。このような IT 分野の変革期は、その隙を突くような攻撃やマルウェアが流行する傾向にあります。日頃から世間のセキュリティ動向を注視することが重要です。

マルウェア以外の脅威として、セキュリティアップデートが適用されていない古い機器や製品の脆弱性を悪用した攻撃の被害が確認されています。機器が正しく設定されていることやセキュリティアップデートが適用されているかを確認することが大切です。

■ 2021年に日本国内で検出されたダウンローダー

ダウンローダーは、攻撃に使うマルウェア本体をダウンロードし実行させることを目的とするマルウェアの 1 種です。2021 年の検出数は減少傾向でしたが、さまざまな種類のマルウェア感染を狙った攻撃は継続的に行われました。攻撃者はダウンローダーを量産し頻繁に攻撃を行うとともに、多数の亜種を作成することでセキュリティ製品の検出を避けようとしています。今後もセキュリティアップデートに対抗するため、その都度ダウンローダーに変化を生じさせる可能性があります。

ファイル形式別に分けると、悪意のある Office ファイルを使用する点で共通する VBA 形式と DOC 形式が 8 割以上を占めます。Office ファイルは、ビジネスメールの添付ファイルとして利用される機会が多く攻撃者に悪用されやすいため、検出割合が高いと考えられます。さらに、ダウンロードされるマルウェア別の統計では 2021 年 11 月頃に活動を再開した Emotet（エモテット）のダウンローダー検出数が下半期の 2 位に浮上しています。海外を狙った攻撃が日本にも届いたケースだけでなく、日本語で書かれたばらまきメールによる攻撃など、日本を標的とする攻撃も確認されています。今後の動向に注意が必要です。

■ 2021年のランサムウェア動向

2021 年にランサムウェア攻撃を受けた組織には、2020 年と同様、大規模・高収益の企業が多くありました。特に米国の石油パイプラインが 5 日間の操業停止に追い込まれた攻撃事例は、サイバー空間だけではなく実社会にも影響を及ぼした事例として印象的です。また、国内でも複数のランサムウェアによる攻撃事例がありました。ランサムウェアは被害を受けてから復旧するまでに多くの費用と時間を要するため、ランサムウェアへの対策はすべての組織にとって急務であると言えます。

ランサムウェアの感染経路にも変化が起きています。従来はメール経由の感染が多く確認されていましたが、2021 年は RDP（リモートデスクトッププロトコル）や VPN 機器を経由した攻撃が大半を占めています。多くの企業がリモートワークを導入し、社外から社内ネットワークにアクセスできる環境が増えた結果、リモートワークで使用するこれらの経路が狙われたと推測されます。

攻撃手法の多様化・巧妙化は進み、特に暗号化だけではなく機密情報の暴露を伴う「2 重の脅迫」と呼ばれる事例が多数発生しています。さらに、2 重に留まらず 3 重や 4 重の脅迫と呼ばれる事例も発生しています。それは「2 重の脅迫」に加えて、企業の公開サーバーの停止を狙った DDoS（複数の機器による大量のアクセス）攻撃や、ターゲット企業の顧客や取引先に対してその企業がサイバー攻撃の被害に遭ったことを周知するなどの嫌がらせを行うというものです。

本レポートでは、2021 年のランサムウェア攻撃の事例や感染経路・手法の変化、2021 年に活動が確認された 2 件のランサムウェアの詳細についても解説しています。

■ 国内最多検出数を記録した脆弱性を悪用するマルウェア

2021 年に国内で最も多く検出された、脆弱性を悪用するマルウェアは、「Win32/Exploit.CVE-2017-11882」でした。主な感染経路はメールで、ばらまきメールに添付されていることが大半を占めます。感染すると数式エディター（Microsoft 数式 3.0）に存在する脆弱性（CVE-2017-11882）が悪用され、攻撃者が設定したコードが実行されます。特に多く確認されているコードは、外部サーバーと通信することで別のマルウェアやスクリプトをダウンロードするものです。

CVE-2017-11882 を解消するセキュリティアップデートは 2017 年に公開されており、2018 年には数式エディターが削除されています。しかし、現在も数式エディターが使用されている端末の存在が推察できる点や CVE-2017-11882 の悪用が容易な点により、いまだに悪用され続けていることが考えられます。

本レポートでは CVE-2017-11882 の概要や悪用される様子、脆弱性が発生する要因なども解説しています。

■ Apache HTTP Serverの脆弱性（CVE-2021-41773、CVE-2021-42013）

Apache HTTP Serverは、Apache Software Foundationが管理するオープンソースソフトウェアで、HTMLファイルや画像ファイルなどの静的コンテンツを提供するWebサーバーソフトウェアです。2021年10月4日から7日にかけて複数の脆弱性の確認と修正バージョンのリリースが行われ、ESET製品においても関連する攻撃を検知しています。国内最初の検知は2021年10月26日で、11月中旬から12月中旬にかけて攻撃が多く検知されています。12月下旬から検知数は減少しましたが、依然として脅威が継続しています。

今回のApache HTTP Serverの例のように、数日の間に繰り返しソフトウェアの更新が行われることもあるため、一度の更新で安心することなく常に最新のバージョンにアップデートすることが大切です。取り扱っているソフトウェアの種類やバージョンを正確に把握し、関連するセキュリティ情報を日頃から収集して、懸念事項が生じた際にいち早く対応できる体制の構築も求められます。

本レポートでは、脆弱性の影響を受ける条件や脆弱性を悪用した攻撃の検証も紹介しています。

■ 新たな形態の個人情報漏えい事件と個人を特定しうる情報

2022 年 4 月 1 日の改正個人情報保護法の全面施行を控えた 2021 年は、個人情報が大きく注目を浴びる 1 年となりました。2021 年はこれまでに見られなかった新しい形態の「個人を特定しうる情報」に関する事件、事故が報告されています。その背景には、コロナ禍において導入が加速している、オンラインで本人確認手続きを行う仕組みである「eKYC（electronic Know Your Customer：電子本人確認）」や、貴重品の紛失防止や捜索を手助けする「スマートタグ」などの位置情報保存・発信デバイスの普及などがあります。

本レポートでは、2021 年に発生した従来とは異なる形態の個人情報の漏えい事件と、個人を特定しうる情報として位置情報に着目し、その活用例と悪用の可能性について解説しています。

＜本レポートを解説するウェブセミナーについてご案内＞

SB クリエイティブ株式会社（ビジネス＋IT）主催「Security Management Conference 2022 Spring」のウェブセミナーにおいて、サイバーセキュリティラボ　セキュリティエバンジェリストよる本レポートについての解説を行います。

〇イベント名称：Security Management Conference 2022 Spring
〇講演日時：2022 年 3 月 24 日（木）14：55～15：25
〇タイトル：2021 年を振返り備える！サイバーセキュリティ脅威動向と 2022 年の対策ポイント
〇参加費：無料（要事前登録）
〇開催概要：https://www.sbbit.jp/eventinfo/68721/