セキュリティ脅威動向

2020年 総まとめ

2021年 予測

AhnLab

2020年
セキュリティ脅威動向

2020年セキュリティ脅威動向総まとめ TOP5

AhnLab

01
ランサムウェア：周知の攻撃、被害は依然として深刻

ランサムウェアは数年前から、脅威総まとめおよび来年度の予測に必ず登場してくるキーワードである。すでに広範囲にわたり拡散され、人々にとっては周知の脅威だが、その被害は依然として深刻だ。2020年には、ファイルの暗号化前に内部情報を先に窃取した後、外部への公開を脅し文句に「二重脅迫」という手法を使用する、標的型ランサムウェアグループの拡大が特に目立った。2020年に起こった世界的に注目すべきランサムウェアの被害例は以下の2つである。

A. 世界的な攻撃敢行、Maze ランサムウェア

一つ目に挙げる Maze ランサムウェア (Maze Ransomware) は、世界中の企業を対象に標的型攻撃を行ってきた。攻撃組織は企業の内部データを窃取した後、金銭の要求とともに脅迫を行い、被害企業が要求に応じない場合は自身の Web サイトに窃取したデータを公開した。さらに、11月初めに活動停止を発表しながら、資料の削除を条件に期限内に自分達へ連絡するよう要求した。

B. 患者の命を奪った DoppelPaymer ランサムウェア

2020年9月、ドイツのデュッセルドルフ大学病院がランサムウェア攻撃を受け、医療システムが麻痺したことで救急患者が死亡する事件が発生した。病院内のサーバー30台がランサムウェアに感染し、多数の医療サービス提供が困難に陥ったことで、治療が遅れ救急患者が死亡したのである。その後ドイツの捜査機関は、病院を攻撃したランサムウェアが「DoppelPaymer ランサムウェア」であることを発表した。攻撃組織が患者の死亡を意図したわけではないにせよ、主要インフラがランサムウェア等のマルウェアに感染すると、最悪の場合命を脅かす可能性もあることを示唆した事件だった。

02
国家支援によるハッキング組織の全方位型攻撃

2020年も、自国の利益のためにいくつものハッキング組織が国内外の企業、政府機関、大学、個人等を対象にハッキング行為を行った。一部の企業は職員のアカウント情報および内部資料が流出し、個人の場合保有している仮想通貨を窃取されたりもした。

新型コロナは、国家支援によるハッキング組織の動向を探る上で必ず言及されるべきキーワードだ。世界的にコロナ感染者が急増し、多国籍製薬会社が競って新型コロナウイルスのワクチンを開発している中、複数のハッキング組織が政府機関および製薬会社を相手に攻撃を仕掛けてきた。

新型コロナワクチンに関する文書を保管している欧州医薬品庁 (European Medicines Agency、EMA) は、関連情報の窃取を狙ったハッカーの標的となってきた。また、特定国家から体系的な支援の授受が疑われる攻撃組織が、新型コロナワクチン技術、研究結果、コールドチェーン (低温流通体系) に不正アクセスした事例が相次いで報告されている。

これまで継続的にグローバルハッキング組織の標的となってきた hwp (ハングル) 形式文書の脆弱性は、昨年度に比べ減少した。その理由として、攻撃者が利用していたハングル文書内のゴーストスクリプトの脆弱性が、ハングルプログラムのセキュリティアップデートにより除去され、時間の経過とともにユーザーのハングルセキュリティアップデートの設置が拡大したことで、これ以上の攻撃に効果が期待できないと判断したものと推測される。しかし、代替的な攻撃手段として、マクロ (Macro)、パワーシェル (PowerShell)、WSF (Windows Script File)、VBS (Visual Basic Script) 等のスクリプト形態のマルウェア使用が拡大した。

03
より巧妙化したフィッシング攻撃

2020年に発見されたフィッシング (Phishing) 型のマルウェアは、ユーザーがいとも簡単に騙されるほど巧妙に進化した。正常なポータルサイトを装った不正 Web ページは、正常なサイトに類似したログイン画面を作成することでユーザーを騙し、アカウント情報の窃取を図った。以前は画面構成に多少の違和感があったが、現在は専門家でさえ見分けるのが困難なほど精巧になっている。こうしたフィッシング型の不正 Web ページは、ユーザーがアカウント情報を入力するとサーバーに情報を転送し、その後正常サイトにリダイレクト (redirect) するため、ユーザーが疑いすら抱かないように作られている。

メールにおいても同様のことが言える。主に「システムメンテナンス案内」、「アカウントアクセス制限」、「発注書」等の業務に関する内容で、ユーザーが深く疑うことなく不正リンクやメール内の不正添付ファイルを実行するよう仕向けている。以前は不特定多数を対象に拡散される英文のスパムメールが多かったが、最近ではハングルで作成され、ユーザーにパーソナライズ化された内容も多く発見された。マルウェア制作者が攻撃成功率を高めるため、より巧妙なフィッシング型マルウェアを制作・拡散していることが分かる。

04
ボットネット (Botnet) マルウェアの世界的な大量拡散

Emotet (エモテット) に代表されるボットネットマルウェアが、世界的に大量に拡散された。ボットネットマルウェアは多くのユーザーを感染させた後、攻撃者の命令に従い作動するマルウェアであり、機能としてはユーザー情報の流出、不正ファイルの追加ダウンロード等が行われている。

Emotet マルウェアは金融情報流出型のマルウェアとして始まったが、次第に進化を重ね、TrickBot、QBot のような金融情報流出型のマルウェアを追加ダウンロードし実行する形態に変化した。2020年に確認されたほとんどのボットネットマルウェアは、不正メールを介して流布された。メールの添付文書ファイルに挿入されたマクロを実行すると、不正ファイルがダウンロードされる仕組みだ。

ボットネットマルウェアは、ビルダー (Builder) を通して制作される場合が多く、添付文書ファイルや実行ファイルの外形変更が数時間単位の早さで行われた。また、攻撃者の命令を受けてから機能が作動するため、マルウェアの最終目的を把握するのが困難で、作動時間ごとにユーザー別の被害状況が変わってくる特徴もあった。

05
Google Play 等のサプライチェーンを介した不正アプリの拡散増加

2020年は、Google Play を介して拡散した不正アプリの種類と数が大幅に増加した。こうして配布された不正アプリは、主に金融情報の搾取、購読サービスへの加入、広告流布等の機能を果たしていることが確認された。

2020年、WAP (Wireless Application Protocol) 決済サービスを利用する国で、有料課金サービスへの加入がユーザーの知らない間に行われる「Trojan/Android.Joker」が初めて確認されて以来、文書スキャナーやフォトエディター等に偽装し、Google Play を介して絶えず配布されていたことが判明した。マルウェア制作者がソースコードを公開したケルベロス (Cerberus) という不正アプリも同様に、Google Play から継続的に拡散されていた。

広告露出型の不正アプリは、まずゲームやユーザーに有用なその他機能を提供し、多くのユーザーを集客する。その後、攻撃者のサーバー (C2) から送られた命令に従い、一斉に攻撃的な広告を露出させた。このように、Google Play から拡散した不正アプリは、悪意ある機能が作動するまで一定期間待機 (潜伏) するため、多くの被害者が発生する特徴がある。

2021年
セキュリティ脅威予測

2021年セキュリティ脅威予測 TOP5

AhnLab

01
Maze ランサムウェアに代わる新たなランサムウェアの登場および高度化

これまで盛んに拡散されてきた Maze ランサムウェアが、11月初旬に活動停止を発表した。しかし、これは数えきれないほどのランサムウェア脅威の一つが消えただけに過ぎない。その空席は間違いなく他のランサムウェアが取って代わり、引き続き被害も発生することが予想される。特に、標的型ランサムウェアグループは相互提携からその領域を広げ、攻撃を高度化させていく可能性が高い。サイバー犯罪組織にとってランサムウェアは、重要な金儲けの手段であるからだ。

昨今、企業は資源管理の利便性と効率性向上のため、様々なソフトウェアを使用している。しかし、ソフトウェアに脆弱性が存在する場合、攻撃者がこれを悪用することで企業内部を掌握し、不正行為を実行する環境が作られてしまう。攻撃者は侵入、掌握、窃取等、段階別の攻撃を効果的に成功させるため、継続的にその方法を高度化させている。

過去にメディアを通じて伝えられた韓国国内のハッキング事例を見てみると、ハッカーが企業用ソフトウェアの脆弱性を悪用した例も存在する。ランサムウェア攻撃においてもシナリオとしては十分可能であり、2021年はより高度化し、かつ活発なランサムウェアの拡散が予測できる。

また、前述したランサムウェア攻撃による医療システム麻痺が原因の救急患者死亡事件が、国内では絶対に起こらないという保証はない。これに対抗できるセキュリティシステムの強化、セキュリティ守則の遵守、および認識改善が必要である。

02
新型コロナが変化をもたらした業務環境、そしてセキュリティ脅威

新型コロナの発症が確認されてから、いつの間にか一年の月日が過ぎた。2020年、私たちの生活パターンは新型コロナにより大きく変化した。例えば、オンラインでの購入や配達サービスの利用が急増し、ビジネスにおいても場所に限らずリモートで業務を行う「アンタクト (非接触・非対面)」の導入が大幅に増えた。

企業のセキュリティポリシーによって保護されている時とは違い、非対面式の業務環境では構成員である一人一人が主体となったセキュリティへの配慮が必要となるが、コスト、人材等の理由から容易でないのが事実だ。セキュリティ面から見た新型コロナは、企業にとって新たな挑戦課題であり、同時に攻撃者にとっては絶好の機会でもある。2021年は非対面式の業務環境を狙ったフィッシング、標的型攻撃などのハッキングが相次いで発生することが予想される。

そのため、企業はアンタクト環境下のセキュリティを「推奨」ではなく「必須」項目として認識し、関連環境セキュリティの優先順位を明確に設定する必要がある。さらに、VPN (Virtual Private Network) 使用時の適正なポリシー設定やユーザー検証の強化が必要であり、別途のセキュリティ専門人材がいなくても、安全な業務環境を効率的に整備できる SaaS (Software as a Service、サービスとしてのソフトウェア) 型セキュリティソリューションの導入も考慮するべきである。

03
マルウェア作動方式のモジュール化

2021年は、EXE、DLL等の実行ファイル形式のマルウェア制作方法がさらに多様化するものと予想される。今までも相当数のPE (portable executable) ファイルが、C / C++ / Visual Basic / Delphi / C# 等の言語で制作されてきたが、ここ最近ではパイソン (Python) やGo言語 (Golang) 等のプログラミング言語を用いて制作されたマルウェアも複数登場している。

攻撃者側が、手軽なコンパイルやバイナリ作成が可能な点、さらにライブラリやモジュールの追加が比較的簡単というメリットを十分に利用していることが確認できる。また、今までのアンチウイルス製品のシグネチャパターンとは完全に違う形態と構造をもったファイルであるため、攻撃者はこの点を狙いマルウェアを制作することが予想される。

04
マルウェア作動方式のモジュール化

マルウェアの作動方式はすでにモジュール化されている。一つのファイルが攻撃者のC2サーバー通信、ダウンロード、情報流出、ファイル作成等すべてを行うのではなく、その機能を複数のファイルに分け作動させるのだ。これはアンチウイルス検知を最大限迂回するだけでなく、不正機能をより長期間持続させる目的もある。例えば、攻撃者のサーバーからエンコードされたファイルをダウンロードした後これをデコードするファイルが別にある場合、単一ファイルの情報を見ただけでは正確な機能や不正行為の流れを把握するのが容易ではない。

2021年は、このようにモジュール化したマルウェアのさらなる増加が予想される。特に、ユーザーが不正サーバーにアクセスしてファイルをダウンロードするよう誘導し、植え付けたファイルを継続的に交換する形で被害を与えることが予想される。

05
不正アプリの攻撃対象国拡大が加速化

モバイル端末機を対象にした不正アプリは、言語および文化的な差や決済システムの多様性などの理由から、主に一つの国でのみ攻撃が効果的に行われる傾向にある。韓国国内のスマートフォンユーザーを攻撃するフィッシングアプリ (Dropper / Android.PhishingApp) は、宅配、招待状、新型コロナのような社会的問題に関するフィッシングメッセージを介して拡散された。こうした不正アプリは、ユーザーのスマートフォンに保存されている情報を漏洩し、ボイスフィッシングと連携することで金銭的搾取に利用された。

2020年、同一制作者によるものと思われる不正アプリの配布事例が様々な国で確認された。攻撃者は各国の代表的な宅配業者を装う手法を用いた。
また、Netflix (ネットフリックス) やディズニーなど、有名コンテンツの供給企業や認知度の高いゲームなどを詐称することで拡散し、ブラウザのアラーム広告を購読するよう仕向けるマルウェアも確認された。

このようなマルウェアは、広告提供企業が端末機で作動する国別の言語に対し広告を提供するため、複数の国のユーザーを対象に広まっていった。過去、限られた収益性が理由で局地的に作動していた不正アプリが、今や複数の国のスマートフォンユーザーを攻撃対象とし始めており、こうした傾向は次第に加速化することが予測される。

セキュリティ脅威動向

2020年 総まとめ
2021年 予測

アンラボとは
株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。
今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

発行所　株式会社アンラボ
発行者　AhnLab Security Emergency Response Center
編集　アンラボ・コンテンツ企画チーム

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315　(代)

A AhnLab.com　B ASEC Blog　F Facebook

AhnLab