アンラボ・セキュリティレター

Press Ahn

2022.12　Vol.108

振り返る「2022 年サイバー脅威トレンド Top 10」

振り返る「2022年サイバー脅威トレンドTop 10」

2021年 12月に触発された Log4j の脆弱性の余波が残る状態で迎えた 2022年は、全世界的に政治と文化イベントが多数予定され、サイバー領域でのセキュリティ脅威がいつにも増して多く予想された年だった。毎年どのグローバル行事よりも先駆けて開催され、様々な企業が技術力と一年間の戦略の方向性を公表して全世界の人々の耳目を集中させる CES でも、2022年の 5つの話題の一つとしてサイバーセキュリティが挙げられた。これはサイバーセキュリティ領域での活動により没頭させる動機になったのではないかと思われる。また、誰も予想できなかったロシア ・ ウクライナ戦争とサイバー攻撃者たちの熾烈な活動は、これまで経験できなかった新たな局面をもたらした。

慌ただしく過ぎ去った 2022年の一年間に韓国国内外で発生した主なサイバーセキュリティ脅威を振り返り、我々のセキュリティ現況を確認して問題を解決、または緩和していくための対策を考えてみようと思う。

#1. Log4j の脆弱性の登場と余波、そして残ったのは…

Log4j は人気のオープンソースであり、長い間多様なバージョンが登場した。Log4j の脆弱性が発見された後、Log4j が必須要素として活用されたアプリケーションが多かったため、メーカーと使用企業は現状を把握すること自体が大変だった。また、悪用可能なセキュリティ脆弱性が登場し続け、関連対応を行う組織の不眠不休の業務が続いた。

Log4j の脆弱性が存在するセキュリティが脆弱なサーバーに仮想通貨マイニングおよび関連したマルウェアが設置された事例は多くはないが、一部確認されたケースがある。その中で最も注目すべきは、標的型ランサムウェアグループ「ナイトスカイ (NightSky)」の Log4j の脆弱性の悪用だ。

ナイトスカイは企業の内部情報を窃取して全て暗号化した後、復号化の条件として金銭的な要求をすることで一度脅迫し、さらに企業が侵入されたという事実と内部情報をダークウェブ (Dark Web) に公開するという二重脅迫をすることで有名だ。これは、仮想通貨マイニングやインフォスティーラー (InfoStealer) のように PC ユーザーの情報を収集し流出する程度のマルウェアが設置されるのとは規模が異なるサイバー攻撃だ。

ナイトスカイは他の標的型ランサムウェアグループとは異なり、活発な活動は見せなかったが、Log4j のセキュリティ脆弱性を悪用したという点と被害企業との連絡にトーア（Tor）ではなくロケットチャット（Rocket .Chat）を利用したという特徴が注目されている。他の標的型ランサムウェアの展開に影響力を与えるほどのランサムウェアではないが、比較的深刻なランサムウェアが Log4j を悪用した事例に該当する。

再び Log4j の脆弱性に話を戻すと、ほとんどは最終的にマルウェアの設置まで進まず、文字列処理後に悪意のあるサーバーとの通信までしか進んでいなかったが、これはむしろセキュリティ担当者の負担を増やす結果となった。これは攻撃者の意図が把握できないだけでなく、セキュリティパッチを完了するまで、いつどんなセキュリティ問題が発生するかわからないという不安が続くためである。

個別のセキュリティパッチに対するガイドは完了しており、関連モニタリングも国家と企業レベルで徹底的に行われている現時点においては、各アプリケーションレベルでの問題点がないか再点検すべきである。今では企業が脆弱な文字列を継続的に送ってくるサーバーとの通信を果敢に遮断するポリシーも上手く適用しているため、その現況と変化の推移を共に分析して結論を導き出し、今後類似したサイバーセキュリティ脅威が登場した際の意思決定に活用すれば役に立つだろう。

そして、Log4j の脆弱性に渾身を尽くして対応し、現在も各自の位置で黙々と任務に従事している全てのセキュリティ担当者および関係部署に感謝の気持ちと拍手を送る。

#2. 標的型ランサムウェアのマスターキー公開と復号化ツール作成

まず、マスターキーを公開した主な標的型ランサムウェアグループと活動期間は［表1］のとおりである。

ランサムウェアグループ	活動期間
メイズ（Maze):	2019.05 ~ 2020.10
エグレガー（Egregor)	2020.09 ~ 2021.02
セクメト（Sekhmet)	2020.03 ~

［表］マスターキー公開ランサムウェアグループおよび活動期間

標的型ランサムウェアグループの第一世代とも言えるランサムウェアグループ「メイズ（Maze)」は、複数のグローバル企業（国内企業を含む）を標的攻撃し、内部情報を自分たちの公式ウェブページに公開して二重脅迫をすることで有名だ。活発な攻撃で金銭的利益と名声を築いてきた彼らは、2020年 10月に突然引退を宣言し、姿を消した。ただし、彼らが消える直前にランサムウェアグループ「エグレガー（Egregor)」が登場したこともあり、一部のアナリストはメイズの一部がエグレガーに合流したと推定している。

エグレガーは、大型書店チェーン「バーンズアンドノーブル（Barnes & Noble)」、ソフトウェア開発会社「クライテック（Crytek)」や「ユービーアイソフト（Ubisoft)」などを攻撃し標的型ランサムウェアの流行りに便乗した。以後 2021年 2月、欧州捜査機関の共助によりランサムウェアグループ「ネットウォーカー（Netwalker)」と共に検挙され、サービスが強制終了された。セクメト（Sekhmet) ランサムウェアはランサムノートがエグレガーと同じで、同じランサムウェアグループであると判断される。

上記で述べたランサムウェアのマスターキーと、これを活用した復号化ツールが、作成および公開された。公開者はこれらランサムウェア作成者グループに属していた人物であると推定されており、欧州と東欧圏で進行中のランサムウェア作成者グループの検挙とは関係ないと明らかにしている。

数学的に暗号を見つけてランサムウェアを解くのは、現在の技術では限界がある。最近話題になっている量子コンピューティングが特別な制約もなく、日常的に利用可能な環境になれば話は変わるだろうが、現時点では残念だが不可能と考えるのが正しい。だからと

いって今回の例のように作成者グループあるいは捜査機関によるマスターキーの公開を待つことが、必ずしも肯定的とは言えない。今回のマスターキーの公開は、標的型ランサムウェアグループが引退または退場して、ある程度時間が経った後に誰かの善意によって行われたものであり、現在までマスターキーが公開された例は指折り数えられる程度しか存在しない。

いずれにせよ、全世界的に大きな被害をもたらした第一世代の標的型ランサムウェアグループメイズのマスターキーの公開と復号化ツールの作成は、その事実だけをとってみても十分に有意義な事件である。もしこれらのランサムウェアから被害を受けて復号化が必要な企業 / 機関があれば、復号化ツールを利用した復旧を試みることを勧める。ちなみに、復号化のためにはランサムノートファイルが必要である。

#3. ランサムウェアの両極化

活発な攻撃で猛威を振るう名の知れたランサムウェアがある。そのうちの一つがまさにロックビット（LockBit）ランサムウェアだ。進化を重ねたロックビット 3.0 はファイルの暗号化、窃取した情報の公開、そしてDDoS（ディードス）攻撃に至る三重脅迫を行う標的型ランサムウェアへと発展した。

「標的型」ランサムウェアという単語からもわかるように、今やランサムウェアが誰かを偶発的に攻撃するケースはほとんどない。彼らは常に緻密に計算された意図を持ち、徹底的に準備された攻撃を敢行するという事実を忘れてはならない。

アンラボが ASEC ブログを通じて公開したLockBit 3.0 の攻撃事例を見れば、攻撃者はエントリーシートを装った不正な word ドキュメントを拡散し、拡散ファイル名は「イム ・ ギュミン.docx」や「ジョン ・ チェリン.docx」などのように、人の名前を使って巧妙に偽装してある。

公開された攻撃パターンを見ただけでも、彼らの攻撃が偶発的なものではないことがわかる。このようなタイプの攻撃は、ほとんどが「組織内部ネットワーク、または被害者コンピュータに侵入 > マルウェアのインストール > 意図に合わせて追加のマルウェアまたは攻撃ツールを配布 > 管理者アカウント盗用 > システム復旧妨害目的の復元イメージ削除およびサービス終了 > 目標達成」の順に展開される。彼らが企業や組織内部へのアクセスに成功した後の行動を見ても、意図的に接近したということを十分に類推できる。

一つ注目すべき点は、新規ランサムウェアの作成比率は年々減少していることだ。今や一般的なランサムウェアの作成 & 拡散は大きな利益をもたらすことができず、ランサムウェア市場でも一種の両極化が進んでいるのだ。有名で大規模な標的型ランサムウェアは積極的に政府機関と主要企業を攻撃して利益を得ている反面、他の数多くのランサムウェアは 1、2度の活動の後に姿を消してしまうこともある。全体的なランサムウェアの数が減少する様相を呈しているが、実際に脅威となっている上位圏の標的型ランサムウェアは攻撃のレベルを下げていないことを忘れてはならない。

#4. セキュリティシステムの無力化に本気を出す攻撃者たち

PC とサーバーで稼動中のセキュリティシステムを無力化することは、映画でもよく観る、侵入者が歩哨を排除するのと同じ原理だ。歩哨の役割も未確認あるいは疑わしい相手を防ぐことであるため、その部分も類似した面がある。

サイバーセキュリティの領域でも攻撃者と防御者の攻防は続いており、技術も発展し続けて今日に至っている。アンチウイルス（AV）製品は正常な OS 環境でマルウェアと認識されるファイルを除外し、攻撃者は自分を妨害する AV 製品が正常に作動できぬよう、様々な試みがなされている。

これまでは攻撃者がアンチウイルス（AV）製品の削除（uninstall）を試みる場合、CAPTCHA（キャプチャ）認証をする過程を適用してこれを防御してきた。しかし、最近は攻撃者が直接介入するなど様々な方法で防御システムを無力化するための試みが確認されている。二つの例を見てみよう。

まず、アンラボが今年 9月に発刊した「ラザルス攻撃グループの BYOVD を活用したルートキットマルウェア分析レポート」によれば、攻撃者はイニテック（INITECH）社の旧バージョンのプロセスを悪用して企業に初期侵入を行った後、攻撃者のサーバーからルートキットマルウェアをダウンロードして実行した。ルートキットマルウェアは脆弱なドライバカーネルモジュールを悪用し、直接カーネルメモリ領域に対して読み取り / 書き込み行為を行いアンチウイルス（AV）製品を含むシステム内の全てのモニタリングシステムを無力化させた。

また、最近「韓国型」ランサムウェアとして名を馳せている「クィシン（Gwisin）」ランサムウェア」は、セーフモードで再起動させてからファイルを暗号化する方法で AV 製品を迂回する。セーフモードでは最小限のサービスだけが作動するため、Windows の基本ドライバを除いてはローディングされず AV 製品の監視も迂回できるようになる。

このように、攻撃者がセキュリティシステムの無力化に力を入れている状況で防御者が選択できる最善の対策は、自分のセキュリティシステムをモニタリングし、これを積極的に管理して攻撃者に隙を与えないことだ。攻撃者の攻撃動向を注視することはもちろん、自分の現状を積極的に把握して対処することが重要である。我々のセキュリティシステムを破壊することに本気を出す攻撃者に、我々も「抜かりなく」本気で立ち向かうべきだ。

#5. 国際協力によるサイバー脅威攻撃者の検挙

サイバー脅威攻撃者の検挙ニュースは、1年前に韓国内でクロップ（CLOP）ランサムウェア共助者の検挙から出発したと言っても過言ではない。この事件は主導勢力検挙の出発点となり、以後ウクライナでの国際協力による検挙にまでつながった。この他にも、2021年 10月にロッカーゴガ（Locker Goga）ランサムウェア関連者とその他多数のサイバー攻撃を行った関連者検挙のニュースまで確認することができた。

最近はランサムウェアグループの名前は明確ではないが、50か国以上で約 100万ドル規模の被害を出したサイバー脅威攻撃者を検挙したというニュースまで出るなど、韓国だけでなく西側主要国との積極的な協力を通じてサイバー犯罪に加担した人々を探し出し検挙している。

一方、1月には国内でブルークラブ（BlueCrab）ランサムウェア、海外ではソディノキビ（Sodinokibi）ランサムウェアとして知られているランサムウェアグループ「レビル（Revil）」の関連者を検挙したというニュースがロシアで伝えられた。ロシアでサイバー犯罪者検挙のニュースが伝えられたのは非常に異例のことだ。自国民の保護より国際社会との共助を選択するほうが戦略的に良いという判断の可能性もあるが、ランサムウェアグループ「ダークサイド（Dark Side）」およびレビルの背後とロシアは関係ないということを主張するための「アクション」の可能性もある。

アメリカとロシアの相互間のサイバー脅威については認めも協力もしなかった前例を踏まえると、今回のロシアの選択は今後どのような戦略的選択をしていくのかを注意深く観察させる手がかりを提供したといえる。

#6. 背後に国家を持つサイバー攻撃グループの展開

今年 3月、韓国では第 20代大統領選挙が行われた。当時「ビッグイベント」がある韓国を巡り、各国のサイバー攻撃がどのように展開されるのか各自の領域で注視したことだろう。

現在は韓国と政治的あるいは軍事的に対立している国家がこのように特定時期に直接的なサイバー攻撃を敢行する場合、実際に利益を得られる部分はほとんどない。ただし、間接的には様々な状況に備え、各分野にて自分たちが必要としている情報があるか探す方法を講じてきたものと見られる。

その一環として、悪意のあるスクリプトが挿入された文書ファイルを制限された受信者だけに送信する攻撃を続けている。この攻撃に

使われる悪意のあるスクリプトは、基本的に一般ユーザーが読めないように難読化（Obfuscation）されている。文書ファイルを閲覧して悪意のあるスクリプトが作動すれば、ユーザーの PC に保存されたセンシティブ情報を収集および流出し、PC 自体に対する情報も一緒に収集していく形式だ。これは攻撃者が目標対象を明確に区分するための手段であると解釈される。

一つの事例を挙げると、最近アンラボは「ニュースのアンケートに偽装して拡散している不正な word ドキュメント」という投稿を ASEC ブログにて公開した。不正な word ドキュメントのファイル名は「CNA [Q].doc」で、対北朝鮮関連の特定人物を対象に、CNA シンガポール放送のインタビューに偽装したものだった。ユーザーがタイピングを始めると「マクロを実行してください」というメッセージボックスが表示される。ユーザーは文書作成のために「コンテンツの有効化」ボタンをクリックし、文書に含まれた悪性 VBA マクロが実行される形だ。

このようなタイプの攻撃は、ユーザー情報を収集して流出するインフォスティーラー（InfoStealer）とも類似していると考えられる。しかし、上記の事例のように背後に国家を持つサイバー攻撃グループは、明確な目的を持って動くという決定的な違いが存在する。現在、攻撃の主要ターゲットとなっている産業群は、政治、統一、外交、航空宇宙、防衛産業、エネルギー & 再生可能エネルギーなどがある。したがって、国家関連の主要技術あるいは企業の核心技術および資料を扱う組織は、警戒をさらに徹底しなければならない。

#7. 注目されるマルチファクタ認証、我々に残された課題は ？

2021年 5月、非政府組織（NGO）で基本マルチファクタ認証（MFA）プロトコルを設定したが、ロシアのサイバー犯罪者が誤った構成のアカウントを利用してMFA 用の新しい装置を登録し被害者のネットワークにアクセスする事件が発生した。この過程で、攻撃者は Windows 印刷スプーラー（spooler）の脆弱性である「Print Nightmare（CVE-2021-34527）」を悪用し、システム権限で任意のコードを実行した。

MFA は許可された 2つ以上の機器を通じてユーザーを確認するため、明らかに攻撃者が手こずる防御システムの一つだ。ただし、これを迂回する問題が発生したため、様々な悩みが生じている。もちろん MFA が全ての攻撃を防ぐ 100% 完璧なセキュリティシステムとは言えないが、正しく活用すれば攻撃者に不都合を招き、容易に彼らの思い通りにすることはできない。

したがって、上記のようなセキュリティ問題が発生したという理由で MFA そのものを疑って適用しないよりは、これを積極的に適用しつつ、構成ポリシーをきちんと検討して誤用 · 乱用される余地をなくすことが正しいアプローチだ。また、組織内のユーザーアカウントのうち、すでに存在しないアカウント情報は定期的に点検して削除し、知られているセキュリティ脆弱性に対してパッチを迅速に適用すれば、危険要素を最小化することができる。このような措置を継続的に行えば、MFA の効果も極大化でき、ひいてはより安全な環境でビジネスに集中することができるだろう。

#8. インフォ（Info）をスティール（Steal）せよ

インフォスティーラー（InfoStealer）は情報窃取型マルウェアで、ウェブブラウザやメールクライアントのようなプログラムに保存されているユーザーアカウント情報や仮想通貨のウォレットアドレス、ファイルのようなユーザー情報を窃取することを目的とする。2022年第 3四半期の ASEC レポートによれば、当該期間中に拡散されたマルウェアのうちインフォスティーラーが 55.1% を占めるほど活発に攻撃へ活用されている。

最近のインフォスティーラーのマルウェア動向を見ると、互いの連携と変化が活発に行われている。代表的な事例として、オンラインバンキング（Banking）型マルウェアの一つであるエモテット（Emotet）がある。これまで、登場しては姿を消すことが多かったエモテットは、トリックボット（Trickbot）との連携を通じて急速に拡散されたが、2021年初めにインフラが捜査機関に押収され静かになった。

それから 9ヶ月後の 2021年末に再び復活したエモテットは、従来のボット（bot）型マルウェアとの連動を止め、自発的なスパム発送機能を搭載して自ら拡散する能力を備え、再び姿を現した。ここに、エモテット本来の情報収集 & 流出機能が高度化された。

今やエモテットは昨年から主要なマルウェア型に急浮上したインフォスティーラーに含まれても不思議ではなく、アンラボでも今後の展開を注視している。

#9. IoT 機器の脆弱性攻撃

ネットワークにつながる各種 IoT 機器に対する脆弱性攻撃が絶えない中で、全世界的に多くの顧客が使用している無線 LAN ルーターの脆弱性を悪用したサイバー攻撃が猛威を振るっている。ルーター1台で有線 / 無線インターネットに接続される機器を全て操縦できるという点を考慮すれば、相当な影響があると見られる。

攻撃者は無線 LAN ルーターを掌握することで、何の利益を得ることができるだろうか？ユーザーが入力する各種個人情報を横取りすることができ、ユーザーの目には正常なサイトであるかのように偽装したフィッシングサイトを作って接続するよう誘導することもできる。また、掌握されたルーターはネットワークに接続された不特定多数を相手に DDoS 攻撃を敢行するのに活用することもできる。IoT 機器を対象に攻撃を敢行する代表的なマルウェアとしては、ミライ（Mirai）やツナミ（Tsunami）などがある。

このような攻撃に対するセキュリティのためには、一次攻撃対象となるルーター（または有線 / 無線 LAN ルーター）に対するセキュリティ脆弱性パッチを実行し、掌握されたルーターによって敢行される DDoS 攻撃およびログインアカウントに対する Brute Force 攻撃の有無に注意を払う必要がある。また、ログインアカウントを継続的に管理し、ログイン可能な未使用アカウントはできる限り適時に削除しなければならず、機器へのアクセスを制限されたユーザーにのみ許可するセキュリティポリシーを適用してこそ、脅威による被害を最小限に抑えることができる。

#10. マイナー（Miner）、彼らだけの経済

「マイナー（Miner）」は仮想通貨マイニング目的で作られたアプリケーションの通称で、正式名称は「コインマイナー（Coin Miner）」、略して「マイナー」と呼ぶ。

仮想通貨に対する関心が高かった 2018年初めには、ウェブブラウザを通じたクリプトジャッキング（Crypto Jacking）マルウェアが莫大な被害を発生させた。今年は経済の低迷が加速して注目度が落ちたが、仮想通貨マイニング関連マルウェアは関心度の差が存在するだけで、着実に作成・拡散されている。

むしろ、最近のマイナーは領域を拡張するための動きを見せながら、ユーザー情報を収集して流出するインフォスティーラー（InfoStealer）と連携する姿まで見せている。先に説明したように、インフォスティーラーが窃取する情報にはウェブブラウザや応用プログラムに保存されたユーザーアカウント情報と仮想通貨のウォレットアドレスも含まれるが、ここで、非常に長い仮想通貨のウォレットアドレスを攻撃者のウォレットアドレスに置き換えるクリッパー（Clipper）機能まで搭載したマルウェアが登場し始めた。

ちなみに、仮想通貨のウォレットアドレスを置き換える機能を持つマルウェアとしては、2017年に活動したクリプトシャフラー（Crypto Shuffler）があったが、これがクリッパー（Clipper）に生まれ変わり、機能が補強された。ウォレットアドレスがマルウェア内に含まれており、ファイルサイズが数十メガバイトに達していたクリプトシャフラーとは異なり、クリッパーは内部の演算構造を通じて関連仮想通貨を判断し攻撃者のアドレスに置き換える機能を通じて、サイズを大幅に縮小した。攻撃者の立場ではサイズの負担を減らしながら多様な仮想通貨ウォレットを狙うことができ、情報を流出するインフォスティーラー機能だけでなくコインマイナーのマイニング機能まで、多様なマルウェアの長所を総合的に享受できるマルウェアだ。

今まで、マイナーは組織と企業の資源を枯渇させる程度の危害だけを与えると認識されてきた。しかし、彼らだけの経済構造の中で継続的に生産され活動しており、単純な機能だけを実行していた過去から抜け出し、主要情報を収集および流出し仮想通貨のウォレットアドレスまで窃取するなど、直接的な打撃を与えることができるようになった。組織はこのような変化を認知し、内部インフラにおけるマイナー活動に対する点検を継続的に行わなければならない。

http://jp.ahnlab.com/site/main.do

http://global.ahnlab.com/site/main.do

http://www.ahnlab.com/kr/site/main.do

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。

AhnLab

〒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)