Trellix | ABC Co.

ADVANCED THREAT RESEARCH レポート

2022 年 1 月

この Advanced Threat Research レポートは、
弊社パートナーの厚意により提供されるものです。

レポート

Trellix

ADVANCED THREAT RESEARCH レポート

2022 年 1 月

レポート

目次

新会社として初となる脅威レポートでは、世界的に大きな話題となり、サイバー セキュリティ会社や企業セキュリティ チームの注目を集めた Log4j の問題を明らかにしています。

レポートおよびリサーチ

Alfred Alvarado
Christiaan Beek
John Fokker
Douglas McKee
Tim Polzer
Steve Povolny
Raj Samani
Leandro Velasco

弊社チーフ サイエンティストからのご挨拶

新しい脅威レポート、そして新しい会社へようこそ。

この新しい年を前にして、私たちは、2021 年の特に困難な年末から私たちすべてを疲労困憊させている脅威の状況を認識しなければなりません。新会社として初となる脅威レポートでは、世界的に大きな話題となり、サイバー セキュリティ会社や企業セキュリティ チームの注目を集めた Log4j の問題を明らかにしています。2021 年の第 3 四半期と第 4 四半期についても振り返りますが、まずは Log4j の対策に利用できる豊富なリソースを詳しくご紹介します。

基本的に、Log4j の脅威の詳細が明らかになるにつれて、私たちの研究と最新のリソースにアクセスして助けを得ることが不可欠になります。本レポートでは、製品の状況だけでなく、この脆弱性を利用したキャンペーンを継続的に監視し、新しいペイロードの保護対応状況を詳しく説明しています。

Log4j の脆弱性の詳細が明らかになったとき、私たちは非常に迅速にネットワークベースの署名を提供し、脆弱性に関する記事を発表して対応しました。
本レポートで詳述している追加資産を速やかに追跡調査しました。

現在の Log4j の脅威活動や、その他の拡散している脅威についてさらに理解するには、弊社の貴重な 脅威ダッシュボードをご覧ください。

さらに、最新の脅威に関するコンテンツやビデオ、セキュリティ情報へのリンクが掲載された Trellix Threat Labs ブログも確認してください。

もちろん、企業のセキュリティに対する脅威は、Log4j だけではありません。
本レポートでは、ランサムウェアの迫り来る影と混乱や、その他の流行している一般的な脅威や攻撃についても取り上げています。

2022 年を迎えましたが、新しく生まれ変わった弊社をどうぞよろしくお願いします。

—Raj Samani

フェロー兼チーフ サイエンティスト

Twitter: @Raj_Samani

LOG4J: 知りすぎたメモリ

脅威の伝統となりつつある Log4j において、広く使用されている Log4j ライブラリに影響を与える新しい脆弱性が、ホリデーシーズンに合わせて発表されました。この数十年で最も深刻なサイバーセキュリティの欠陥と評されたため、2021 年の第 4 四半期に、Trellix とサイバーセキュリティ業界を対策へと促しました。Log4j の脆弱性は、Apple iCloud、Steam、Samsung Cloud ストレージなどの製品やサービスを含む、アプリケーションや Web サイトに Log4j ライブラリを統合している製品に甚大な影響を及ぼす可能性があります。

弊社チームは、Log4j の検出以来、その動向を詳しく追跡してきました。そして、Network Security Platform (NSP) をご利用のお客様向けに、ネットワーク シグネチャ KB95088 をリリースしました。このシグネチャは、LDAP 上で CVE-2021-44228 を悪用しようとする試みを検出します。これは、他のプロトコルやサービスに対応するように拡張される可能性があり、また、保護範囲を補完するために追加のシグネチャがリリースされる可能性があります。

Log4j のタイムライン

Log4j と弊社の研究のタイムラインを簡潔に紹介します。

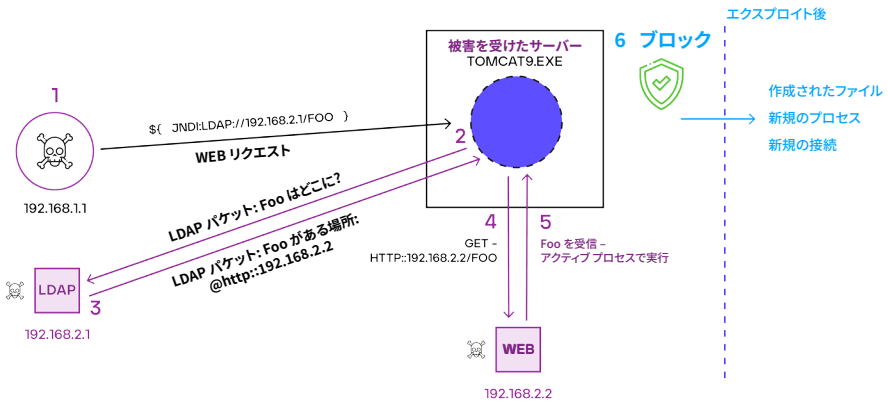
- 12 月 9 日 – Log4j の脆弱性 (CVE-2021-44228) が、Apache Log4j のロギング ライブラリに関する Github 上の POC とともに Twitter で公開されました。このバグが最初に明らかになったのは、11 月 24 日のことです。
- 12 月 10 日 – Steve Povolny と Douglas McKee が Log4j ブログに即時の調査結果の概要を投稿しました。当初の目的は、公開された PoC を使用して悪用のされやすさを判断することでしたが、それを再現し、確認するに至りました。これは、公開されている Docker コンテナーと、LDAP と RMI の両方を利用するクライアント サーバー アーキテクチャ、および Log4j バージョン 2.14.1 を悪用するための marshalsec を使用して行われました。
- 12 月 14 日 – Log4j バージョン 1.2 において JMSAppender コンポーネントを介した同様の攻撃に対する脆弱性が確認され、CVE-2021-4104 が発行されました。
- 12 月 18 日 – Log4j のバージョン 2.0-alpha1 から 2.16.0 に影響を与える新しいサービス拒否 (DOS) の脆弱性 CVE-2021-45105 が発見されました。

Log4j に対する防御に関する最新の調査については、Trellix Threat Labs ブログおよび脅威ダッシュボードを確認してください。弊社チームは、さまざまなオープン ソースとクローズド ソースから情報を収集および分析して、インテリジェンス レポートを発信しています。

Log4j 攻撃

弊社チームは、一般的な Web ベースの Log4j 攻撃の実行時に発生する事柄を迅速に調査し、流れをまとめました。

LOG4J の実行の流れ



- ステップ 1 – 攻撃者は、脆弱なアプリケーションをホストしている Web サーバーに、特別に細工した文字列を送信します。この文字列は、これまで見てきたところ、ネットワークベースのシグネチャをバイパスするために難読化されている可能性があります。
- ステップ 2 – アプリケーションはこの文字列の難読化を進めて、メモリに読み込ませます。メモリに読み込まれると、アプリケーションは LDAP 接続を開始し、悪意のある Class ファイルの場所のアドレスを要求します。
- ステップ 3 – 攻撃者が制御する LDAP サーバーは、悪意のある Class ファイルの場所を、それがホストされている HTTP URL アドレスを示すことで応答します。
- ステップ 4 – 脆弱なアプリケーションは、悪意のある Class ファイルのダウンロードを開始します。
- ステップ 5 – 脆弱なアプリケーションは、手順 4 で作成された悪意のある Class ファイルを読み込み、実行します。

Trellix ATR Log4j の防御策

Log4j のような攻撃から環境を保護するには、ネットワーク セキュリティと標的型エンドポイント メモリ スキャンで構成される多層型の戦略を採用することが効果的です。この戦略では、ネットワーク ベクトル経由で公開された、脆弱なシステムに対する攻撃の実行フローを効率よく検出し、防止することができます。弊社の ENS エキスパート ルールとカスタム スキャンによる対応は、こうした新たな脅威に対して的確な対応策を講じることができるように、防御側の能力を向上させる目的で設計されています。

また、CISA.gov は、Log4j の脆弱性の影響を受ける可能性のある Web サービスを組織が特定できるように、Log4j スキャナーを提供しています。

ランサムウェア

2021 年第 3 四半期に、知名度の高いランサムウェア グループは、姿を消しては再び現れ、改変を重ね、さらには名前まで変えながら、ますます多様化するセクターに対し、よく知られた破壊的な脅威として、影響力と蔓延性を保っています。

2021 年第 2 四半期にランサムウェアのアクティビティが多くのサイバー犯罪者フォーラムから非難され、禁止されたにもかかわらず、弊社チームは、いくつかのフォーラムで同じ攻撃者が別のペルソナを使用して活動しているのを観察しています。

Trellix はランサムウェア犯罪集団の逮捕と身代金の押収に協力

2021 年 12 月に、Trellix は、REvil の関連者を逮捕し、身代金 200 万ドルを押収するために FBI と欧州警察を支援する研究を提供しました。

2021 年第 3 四半期の注目すべきランサムウェアのトレンドとキャンペーンは以下のとおりです。

- BlackMatter – 2021 年 7 月末頃に発見されたこのランサムウェアの脅威は、米国に拠点を置く農業サプライチェーン企業 New Cooperative への強力な攻撃から始まりました。この攻撃により、同社は機密ビジネス データが漏洩する脅威にさらされました。New Cooperative は、サプライチェーンの管理機能と動物の給餌スケジュールがロックされたと報告し、米国内の穀物生産の 40% に悪影響が及ぶと推定しています。BlackMatter は、GandCrab、LockBit、DarkSide などの他のマルウェアの一部を利用しているとしていますが、このキャンペーンが新しい開発者グループによって実行されている疑いが高まっています。BlackMatter は、Colonial Pipeline 攻撃に関連する DarkSide マルウェアと非常に多くの共通点があります。
- Groove ギャングと Babuk ギャングが元関係者またはサブグループとして関連しているとの考えを発表しました。
- REvil/Sodinokibi は、マネージド サービス ソフトウェア プロバイダーの Kaseya VSA に対するランサムウェア攻撃により、100 万人以上のユーザーを感染させることに成功したと主張しました。REvil が報告した身代金要求額 7,000 万ドルは、これまで公表された身代金の金額として最大です。攻撃の結果、数百店舗のスーパーマーケットが数日間、強制的に閉鎖に追い込まれる事態となりました。
- 2021 年 7 月に表面化した LockBit 2.0 により 、最終的に 200 人以上の被害者がデータ流出サイトに掲載されました。

ランサムウェアの脅威に対する政府の対応

第 3 四半期に、米国政府はランサムウェアの蔓延を抑えるため、予防的キャンペーンを開始し、StopRansomware.gov ハブを立ち上げました。このキャンペーンは、米国の重要なインフラストラクチャに対するサイバー活動に関与する国家的な脅威を識別または特定する情報に対して、最高 1,000 万ドルの報奨金を提供するというものです。

これらのランサムウェアや新たなキャンペーンが今後どのように企業を脅かすかについては、Trellix 2022 Threat Predictions をご覧ください。

Trellix ランサムウェア調査

企業が脅威状況におけるランサムウェア攻撃の理解を深め、それを防御できるように、弊社チームは、ファミリー、手法、国、セクター、ベクトルなど、さまざまなランサムウェア脅威の流行に関する研究と調査結果を紹介しています。

各種ランサムウェアの検出状況

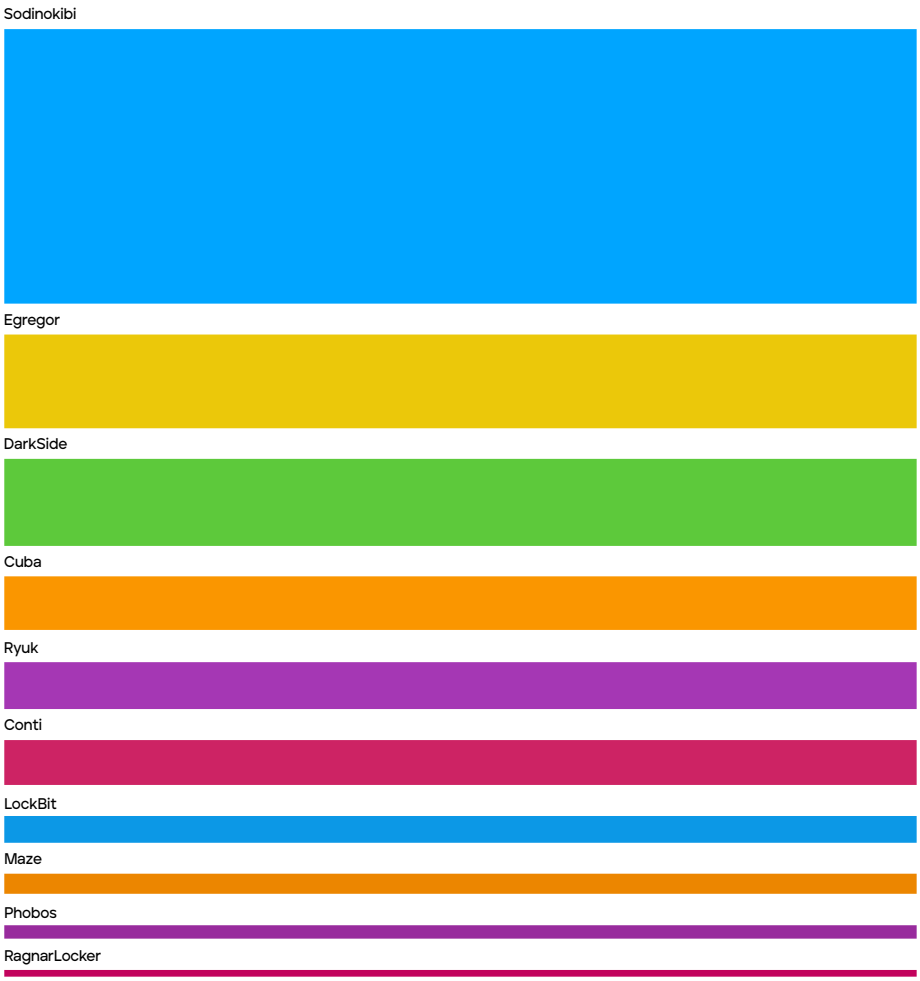


図 1. 2021 年第 3 四半期に検出された各種ランサムウェアは、Sodinokibi (41%) が最も多く、次いで DarkSide (14%) と Egregor (13%) となりました。

以下のランサムウェア クライアントの国、顧客セクター、および MITRE ATT&CK 手法をご覧ください。

攻撃パターン手法

チームでは、APT キャンペーンとそれに関連する指標や手法を追跡および監視しています。弊社チームは、2021 年第 3 四半期から、APT 脅威の主体、ツール、クライアントの国、顧客セクター、および MITRE ATT&CK 手法を反映しています。

APT 脅威の主体

図 2. 2021 年第 3 四半期に検出された APT 脅威の主体は、APT41 (24%) と APT29 (22%) が最も多く、監視された APT アクティビティのほぼ半分を占めています。

APT ツール

チームは、追跡された APT キャンペーンに属する侵害の指標と、それに関連する以下のツールを特定しました。APT グループは、一般的なシステム ユーティリティを使用して、セキュリティ制御をバイパスし、操作を実行することが知られています。

図 3. 2021 年第 3 四半期に検出された APT ツールは、Cobalt Strike (34%) が最も多く、次いで Mimikatz (27%)、Net.exe (26%)、PsExec (20%) の順でした。国家的な主体によって悪用された Cobalt Strike 攻撃スイートは、APT アクティビティの 3 分の 1 以上で検出されました。

以下の APT クライアントの国、顧客セクター、および MITRE ATT&CK 手法をご覧ください。

ADVANCED THREAT RESEARCH

弊社チームは、2021 年第 3 四半期に脅威のカテゴリを追跡調査しました。この調査では、使用された ATR マルウェアのタイプ、クライアントの国、顧客セクター、攻撃に使用された MITRE ATT&CK 手法、産業セクターでの検出率が反映されています。

ATR ツールの脅威

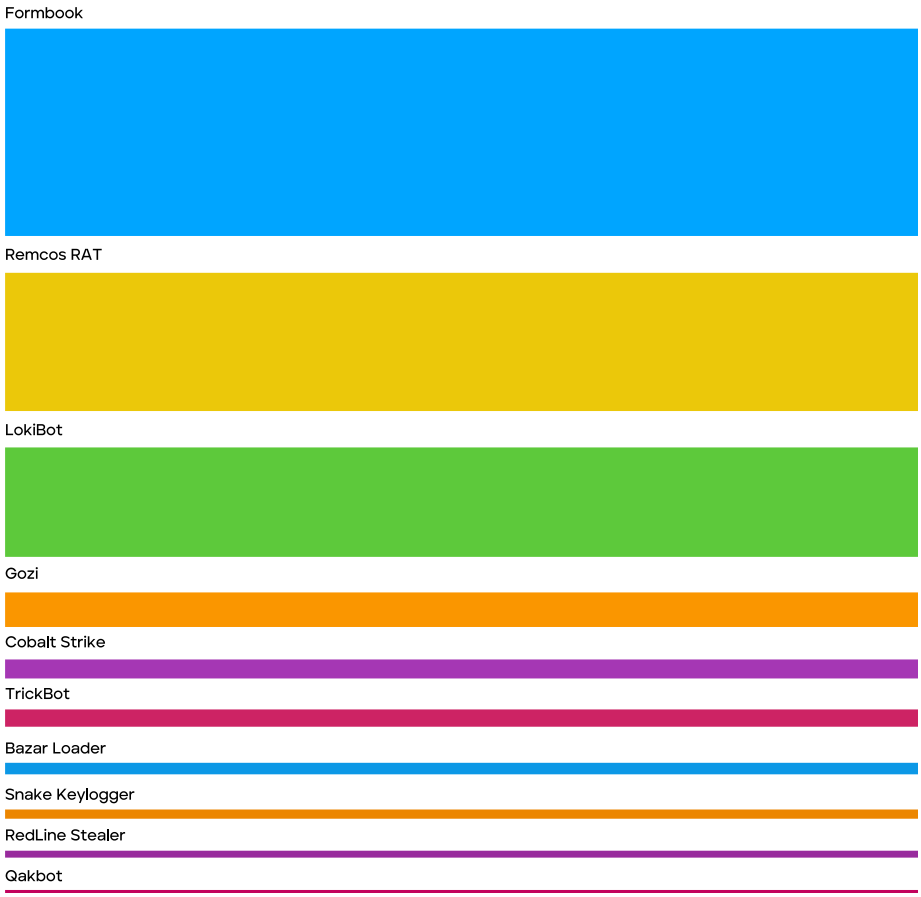


図 4. 2021 年第 3 四半期の ATR ツールの脅威の検出数は、Formbook (36%)、Remcos RAT (24%)、LokiBot (19%) で、ほぼ 80% に達しています。

以下の ATR クライアントの国、顧客セクター、および MITRE ATT&CK 手法をご覧ください。

国、地域、セクター、ベクトルへの脅威

国と地域 : 2021 年第 3 四半期

2021 年第 3 四半期に公表されたインシデントのうち、注目すべき国および地域の増加傾向は以下のとおりです。

- 北米は地域の中で最も多くのインシデントを記録しましたが、2021 年第 2 四半期から第 3 四半期にかけては 12% の減少が見られました。
- 米国では 2021 年第 3 四半期に最も多くのインシデントが報告されましたが、インシデントは 2021 年第 2 四半期から 9% 減少しています。
- 2021 年第 3 四半期に報告されたインシデントのうち、最も高い増加率 (400%) を記録したのはフランスです。
- 2021 年第 3 四半期のインシデントを 2021 年第 2 四半期と比較すると、ロシアが最も大きく減少しています (-79%) 。

攻撃セクター : 2021 年第 3 四半期

2021 年第 3 四半期に公表されたインシデントのうち、注目すべきセクターの傾向は以下のとおりです。

- 攻撃対象とされたのは、複数業種 (28%) が最も多く、次いで医療 (17%)、公共 (15%) となっています。
- 2021 年第 2 四半期から第 3 四半期にかけての注目すべきセクターの増加率は、金融 / 保険 (21%)、医療 (7%) などです。

攻撃ベクトル : 2021 年第 3 四半期

2021 年第 3 四半期に公表されたインシデントのうち、注目すべきベクトルの傾向は以下のとおりです。

- 2021 年第 3 四半期に報告されたインシデントで最も多く使用された手法はマルウェアでした。しかし、報告されたマルウェア インシデントは、2021 年第 2 四半期と比較して 24% 減少しました。
- 2021 年第 2 四半期から第 3 四半期にかけて増加したセクターは、分散型サービス拒否 (112%) および標的型攻撃 (55%) です。

LIVING OFF THE LAND (環境寄生)

サイバー犯罪者は、システム内の正規のソフトウェアや機能を利用し、そのシステム上で悪意のある行為を行う Living off the Land (LotL: 環境寄生) という手法を使用します。第 3 四半期の事象に基づいて、Trellix は、検知されずにいようとする攻撃者が使用するツールの傾向を特定しました。国家に支援された脅威グループや大規模な犯罪グループには、自社でツールを開発するためのリソースがありますが、多くの場合、明確な攻撃の段階を実行するために、ターゲットシステムの既存のバイナリや管理上インストールされているソフトウェアに注目します。

主な標的に対する偵察段階でネイティブ バイナリや管理上使用されるソフトウェアを特定するために、攻撃者は求人サイト、ベンダーが公開するお客様の声、または内部の共犯者から、使用される技術に関する情報を収集することがあります。

ネイティブ OS バイナリ		コメント
PowerShell (41.53%)	T1059.001	PowerShell は、スクリプトや PowerShell コマンドを実行するためによく使用されます。
Windows Command Shell (CMD) (40.40%)	T1059.003	Windows Command Shell は、Windows の主要な CLI ユーティリティであり、代替データ ストリームでファイルやコマンドを実行するためによく使用されます。
Rundll32 (16.96%)	T1218.011、T1564.004	Rundll32 は、ローカルの DLL ファイル、共有からの DLL ファイル、インターネットから取得した DLL ファイル、および代替データ ストリームを実行するために使用される可能性があります。
WMIC (12.87%)	T1218、1564.004	WMIC は、WMI のコマンドライン インターフェイスで、攻撃者がローカルに、代替データ ストリーム内で、またはリモート システムでコマンドや vpayload を実行するために使用される場合があります。
Excel (12.30%)	T1105	ネイティブにインストールされているわけではありませんが、多くのシステムには表計算ソフトが含まれています。攻撃者は悪意のあるコードやスクリプトを含む添付ファイルをユーザーに送信し、それが実行されると、遠隔地からペイロードを取得するために使用される可能性があります。
Schtasks (11.70%)	T1053.005	攻撃者は、持続性を維持したり、追加のマルウェアを実行したり、あるいは自動化されたタスクを実行したりするタスクをスケジュールする可能性があります。
Regsvr32 (10.53%)	T1218.010	Regsvr32 は、攻撃者によって DLL ファイルの登録、悪意のあるコードの実行、アプリケーションのホワイトリストのバイパスに使用される可能性があります。
MSHTA (8.78%)	T1218.005	MSHTA は、攻撃者が JavaScript、JScript、および VBScript ファイルを実行するために使用される可能性があり、ローカルに、および代替データ ストリーム内の HTA ファイルに隠されているか、リモートロケーションから取得される可能性があります。
Certutil (4.68%)	T1105、1564.004、T1027	Windows コマンド ユーティリティは、証明機関情報の取得や証明書サービスの設定に使用されます。また、攻撃者は certutil を使用して、リモート ツールやコンテンツを収集し、ファイルをエンコードおよびデコードするだけでなく、代替データ ストリームにアクセスすることもできます。
Net.exe (4.68%)	T1087 とサブ手法	攻撃者が脆弱なマシンのユーザー、ネットワーク、サービス機能を特定するなどの偵察タスクを実行できるようにする Windows のコマンド ライン ユーティリティ。

Reg.exe (4.10%)	1003.002、1564.004		Reg.exe は、攻撃者がレジストリ値の追加、変更、削除、および代替データ ストリームに保存される可能性のあるレジストリ値のエクスポートを行うために使用される可能性があります。さらに、reg.exe は SAM ファイルから認証情報をダンプするために使用される場合もあります。
管理ツール			**コメント**
リモート サービス (15.21%)	T1021.001、T1021.004、T1021.005	AnyDesk ConnectWise Control RDP UltraVNC PuTTY WinSCP	Windows にネイティブのリモート サービス ツールとサードパーティ ソフトウェアのリモート サービス ツールは、攻撃者によって、マシンやインフラストラクチャへのリモート アクセス、ツールやマルウェアの入力転送、データの漏えいなどに、有効なアカウントとともに使用される可能性があります。
アーカイブ ユーティリティ (4.68%)	T1560.001	7-Zip WinRAR WinZip	攻撃者は、アーカイブ ユーティリティを使用して、収集したデータを圧縮し、ファイルや実行可能ファイルを解凍して、漏えいさせる準備をする可能性があります。
PsExec (4.68%)	T1569.002		PsExec は、リモート システム上でコマンドやプログラムを実行するために使用されるツールです。
BITSAdmin (2.93%)	T1105、T1218、T1564.004		BiTSAdmin は、持続性の維持、成果物のクリーンアップ、設定された基準を満たした場合の追加アクションの起動によく使用されます。
fodhelper.exe (1.17%)	T1548.002		Fodhelper.exe は、攻撃者が脆弱なマシン上で昇格された特権を使用して悪意のあるファイルを実行するために使用される可能性がある Windows ユーティリティです。
ADFind (0.59%)	T1016、T1018、T1069 とサブ手法、T1087 とサブ手法、T1482		攻撃者が信頼できるドメイン、権限グループ、リモート システム、ネットワーク設定などの Active Directory 情報を発見するために使用される可能性のあるコマンド ライン ユーティリティ。

バグ レポート

フロントガラスに付いた「バグ」

(プリンシパル エンジニア兼シニア セキュリティ研究者である MDouglas McKee や他のブロガーが、毎月のバグ レポートで脆弱性を追跡および分析しています。)

世界が 2021 年の終わりまで全速力で駆け抜けようとしているとき、多くの「バグ」がいわばフロントガラスに飛び散りました。簡単に解決できるバグもあれば、染みのように残ってしまうものもありました。チームは、毎月、新しい脆弱性 (バグ) が公表されると、それらを追跡および評価し、その中から最も重要だと「思われる」ものを報告しています。重要なのは、CVSS スコアや OWASP ランキングではなく、長年の経験に基づく昔ながらの状況分析です。

これまでの振り返り

過去数か月で報告された中で上位にいるバグを見ると、いくつか際立っているものがあります。Apache では、その Web サーバー (CVE-2021-41773) と Log4j コンポーネント (CVE-2021-44228) の両方が影響力の強いバグの被害に遭い、困難な年となりました。また、Palo Alto の GlobalProtect VPN に発見されたバグ (CVE-2021-3064) は、世界的なパンデミック時に深刻な影響を及ぼし、注目に値します。では、現実を見てみましょう。Apache Log4j の脆弱性は、間違いなく 2021 年最大のバグであり、今後何年にもわたってその地位を譲らない可能性があるため、「影響力が強い」以上の評価に値します。これらの情報をご存じないなら、弊社の 12 月バグ レポートをお読みください。毎月、脆弱性に関する最新のニュースをお届けしていますので、ぜひご覧ください。

では、これらのバグが最悪と言えるのはなぜでしょうか。簡単に言えば、ネットワークの端にあるツールで認証を行うことなく、リモートで利用できるからです。これらのバグは、攻撃者がフィッシング詐欺を行うことなく、ネットワークへの最初の侵入口となり、それどころかより大規模な攻撃の玄関口ともなる可能性があります。

もし貴社の CISO がロシアン ルーレットで 1 つの製品にしかパッチを適用できないと言うのであれば、Log4j の脆弱性に優先的に適用することをお勧めします。なぜなら、これは実行が容易であり、悪意ある者によって積極的に悪用されているからです。Palo Alto の VPN の脆弱性は深刻で、2020 年以降 VPN での攻撃が増加しているものの、古いバージョンの VPN ソフトウェアに影響を与え、まだ攻撃が活発化していないため、Log4J や他の Apache の脆弱性に比べて目立たない存在となっています。

ターマイト

ターマイトのように、目立たないながらも壊滅的な影響を与えるバグがあります。

CVE-2021-41379 と呼ばれる Microsoft Windows Installer Service のローカル権限昇格バグは、11 月の Termite として知られています。Microsoft は、このバグがローカル アクセスを必要とすることを明らかにし、公式パッチで修正したとしましたが、パッチが予想どおりに機能しなかったため、この戦略は期待外れに終わりました。

Insights にあるように、失敗したパッチと公開された POC とともに、攻撃者は時を待たずにこれを彼らのプレイブックにまとめました。問題をさらに悪化させるものとして、このエクスプロイトの改造版がダーク ウェブで販売されています。

その他の顧客セクター、クライアントの国、および MITRE ATT&CK 手法

ランサムウェアの標的となったクライアントの国

図 5. 2021 年第 3 四半期に検出されたランサムウェア全体のうち、米国に拠点を置くクライアントが 3 分の 1 以上を占めています。

ランサムウェアの標的となった顧客セクター

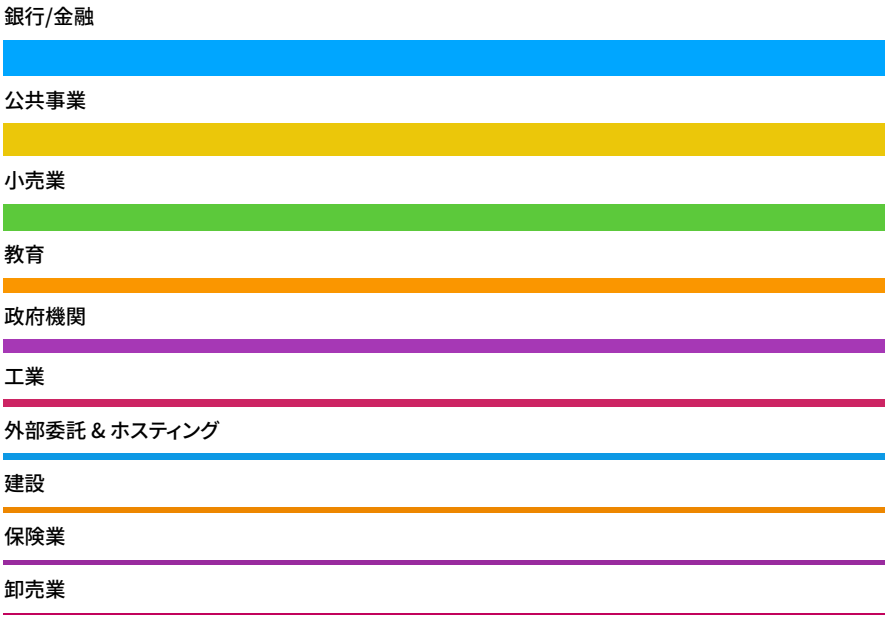


図 6. 銀行 / 金融 (22%)、公共事業 (20%)、および小売業 (16%) が、2021 年第 3 四半期に検出されたランサムウェア全体の約 60% を占めています。

ランサムウェア MITRE ATT&CK 手法

図 7. データ エントリ (2.6%)、ファイル / ディレクトリの探索 (2.5%)、および難読化されたファイル / 情報 (2.4%) が、2021 年第 3 四半期に検出されたランサムウェア MITRE ATT&CK 手法の上位を占めています。

APT の標的となったクライアントの国

図 8. 2021 年第 3 四半期に検出された攻撃パターン手法の件数では、トルコが全体の 17% を占め、次いで米国 (15%)、イスラエル (12%) となっています。

ATR 顧客セクター

図 9. 2021 年第 3 四半期に検出された APT の数が最も多かったのは、銀行 / 金融セクター (37%) で、次いで公益事業 (17%)、小売業 (16%)、政府 (11%) となっています。

APT MITRE ATT&CK 手法

図 10. 2021 年第 3 四半期に検出された APT MITRE ATT&CK 手法で最も多かったのは、スピアフィッシング用の添付ファイル (16.8%)、難読化されたファイル / 情報 (16.7%)、PowerShell (16%) です。

ATR クライアントの国

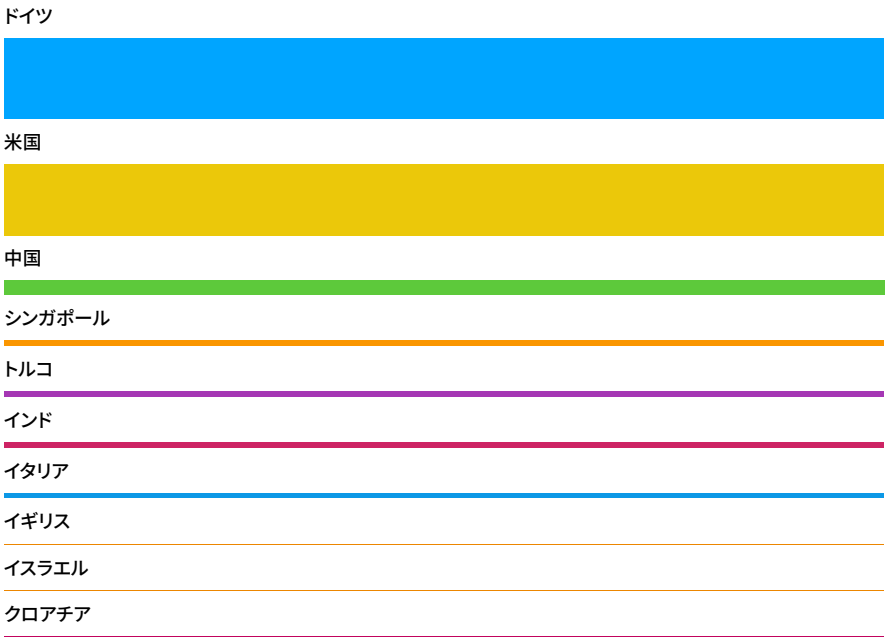


図 11. 2021 年第 3 四半期に検出された ATR ツールの脅威全体の半数以上をドイツ (32%) と米国 (28%) が占めていました。

ATR 顧客セクター

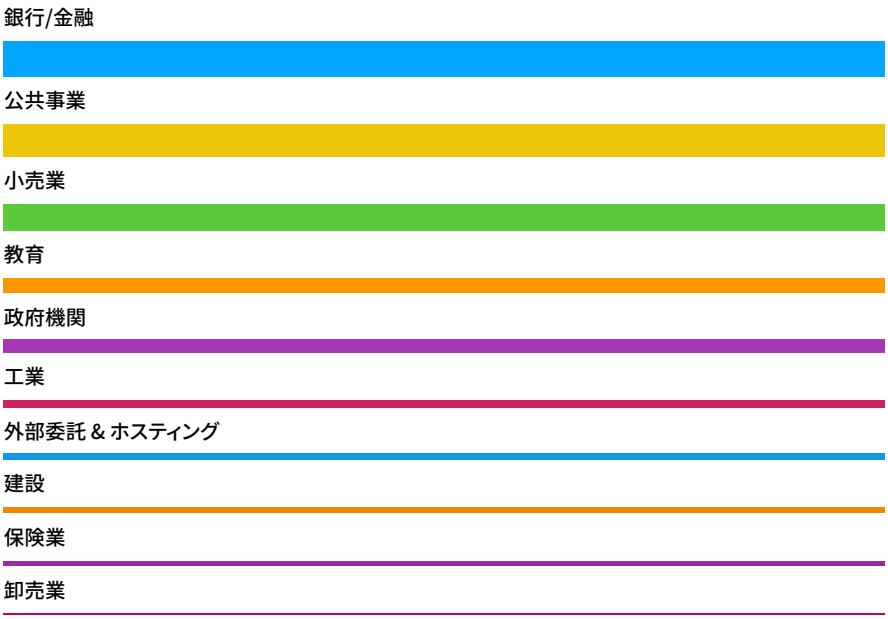


図 12. 2021 年第 3 四半期は、銀行 / 金融の ATR 顧客セクターの検出数 (45%) が最多でした。

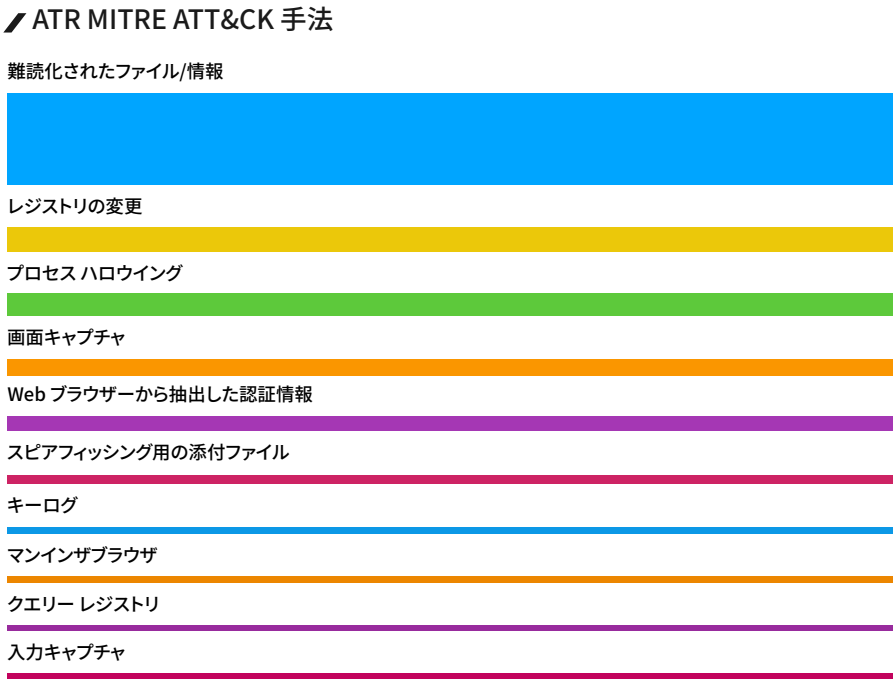


図 13. 難読化されたファイル / 情報が、2021 年第 3 四半期に検出された ATR MITRE ATT&CK 手法全体の 5% に相当します。

リソース

最新の脅威や研究については、弊社チームのリソースをご覧下さい。

脅威センター— 弊社チームが現在の影響力の強い脅威についてご説明します。

Twitter:

Trellix Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Douglas McKee

Trellix について

Trellix は、サイバーセキュリティの将来を再定義するグローバル カンパニーです。今日の最も高度な脅威に直面している組織は、弊社のオープンでネイティブな eXtended Detection and Response (XDR) プラットフォームを使用することにより、業務の保護と耐久性に自信を持つことができます。Trellix のセキュリティ専門家は、広範なパートナー エコシステムとともに、機械学習と自動化を通じて技術革新を加速させ、40,000 以上の企業や政府機関のお客様を支援しています。 詳細については、www.trellix.com をご覧ください。

Trellix Threat Labs

脅威情報を受け取るには購読登録をお願いします。

Trellix

6220 American Center Drive,
San Jose, CA 95002