Secureworks®

脅威インテリジェンス エグゼクティブレポート

Volume 2022, Number 1

カウンター・スレット・ユニット™（CTU）
リサーチチーム

エグゼクティブサマリー

セキュアワークスのカウンター・スレット・ユニット（CTU™）リサーチチームは、セキュリティの脅威を分析し、組織によるシステム保護を支援しています。2021年11月から12月にかけて観測された脅威のふるまい、グローバル規模の脅威状況、セキュリティトレンドをもとに、注目すべきポイントをCTU™のリサーチャーがまとめました。

- **Log4j の脆弱性により、サードパーティコードにおけるセキュリティの問題が浮き彫りに**
- **戦術を共有し、巧妙化する中国のサイバー攻撃グループ**
- **ランサムウェア攻撃グループの動向：新興勢力、活動を続ける勢力、活動を再開した勢力**

Log4jの脆弱性により、サードパーティコードにおけるセキュリティの問題が浮き彫りに

世間を騒がせるような脆弱性でも、すべての組織が被害を受けるわけではありません。しかし各組織のセキュリティ部門は何かあった時すぐに、自社における影響範囲（とくにサードパーティコードを使用しているシステム）を特定し、パッチ適用ができる態勢を整えておく必要があります。

2021年12月に判明したLog4jの脆弱性 CVE-2021-44228（通称Log4Shell）は、簡単に攻撃に利用できると考えられたため、各組織のサイバーセキュリティ部門はこの月多忙を極めました。Log4jを実行するJavaアプリケーションは、ほぼすべての組織で利用されています。その後公表された4つの脆弱性（CVE-2021-45105、CVE-2021-45046、CVE-2021-44832、CVE-2021-4104）はLog4Shellに比べて深刻度は低いとされていましたが、さらなる作業負担となりました。

12月9日に脆弱性が公表されると、攻撃者たちによる広範囲なスキャンがたちまち開始されました。しかしスキャン活動の活発さに比べ、実際の侵害件数は低水準にとどまっています。つまり、たとえ「簡単に攻撃できる」とされている脆弱性であっても、実際の企業のシステム構造はテスト環境に比べて複雑なため、攻撃の達成ははるかに困難であることがわかります。

侵害件数が少ないからといって慢心はできません。特にサードパーティのコードでLog4jライブラリを使っているシステムを特定し、脆弱なサーバーが侵害されていないかチェックして、対象システムにパッチを適用する、という一連の作業は影響を受ける組織にとってどれも大変な負担です。しかし脆弱性の深刻度を考えると、これだけ細かい作業を徹底する必要がありました。

そして問題はまだ終わっていません。脆弱なシステムをすべて特定し、更新を終えるまではLog4j関連リスクは消えることはなく、攻撃者から狙われ続けるでしょう。

今回に限らず、影響を受ける社内システムを簡単に特定できない脆弱性への対処が求められるようなケースは、今後も発生するでしょう。組織としての対応力を強化するには、社内システムが使用しているサードパーティコードを特定し、その結果をリスク評価に反映するための仕組みが必要です。また、バックエンドサーバーによるインターネット通信の制限/禁止、ネットワークとエンドポイントの包括的な監視などのリスク緩和策も整備する必要があります。

上記を踏まえ、ぜひ実行してほしいアクション：
インシデント対応の手順を見直し、人員が手薄で攻撃が発生しやすい休日や祝日などの時期でも計画通り機能するかどうかを確認しましょう。

戦術を共有し、巧妙化する中国のサイバー攻撃グループ

中国政府を後ろ盾とする攻撃グループは引き続き攻撃作戦の機密保全を強化し、攻撃技術を高度化しています。ネットワーク防御のためには、「同じ地域を標的とする攻撃グループは、諜報ノウハウを共有していることが多い」ということを念頭に置いたうえで、ますます複雑化する攻撃に対応しなければなりません。

2021年11月から12月にかけての中国政府を後ろ盾とする攻S撃グループの活動を分析した結果、地政学的な活動を追跡することでサイバー活動を予測、あるいは手がかりを得られることが改めてわかりました。2015年に発表された中国人民解放軍（PLA）の機構改革によって、5つの戦区（北部、西部、中部、東部、南部）が発足しました。インフラやマルウェアの共通性、および近隣諸国を狙う中国の特定の攻撃グループ同士の協力関係をこれらの戦区と照らし合わせると、両者が重なり合っていることがわかります。

たとえば、モジュール型マルウェアShadowPadが関与する活動が進化しているという事実から、ShadowPadが全戦区に浸透していることがわかります。中国政府を後ろ盾とする攻撃グループBRONZE ATLASはShadowPadを少なくとも2017年から使用しています。2019年には、中国の他の攻撃グループも世界各地の様々な業界の組織を狙った攻撃にこぞってShadowPadを使い始めました。ShadowPadが用いられたサイバー活動を当社CTUリサーチャーが分析した結果、北部、南部、西部の戦区との関連が疑われる活動が確認されています。

11月～12月に確認された中国の攻撃グループによるサイバー攻撃を見ると、諜報ノウハウに磨きがかかっていることが裏付けられます。なかには何段階ものステップを経て攻撃を実行する複雑な攻撃チェーンも見つかっています。攻撃発生元が特定されないよう偽装するために、標的国のインフラを攻撃基盤として活用するケースも増えています。また、ゼロデイ攻撃よりも既知の脆弱性を狙った攻撃が多いという傾向も変わりません。ネットワーク防御の担当者がこうした脅威に対処するには、複雑な攻撃チェーンを用いたサイバー攻撃の予防・検知・修復に対応できる可視性と多層防御機能を備えたセキュリティ統制を実装する必要があります。

これまで特定のグループだけが用いていた攻撃の戦術、テクニック、手順（TTPs）が中国の複数の攻撃グループに広がり、標的組織の攻撃に使われる恐れがあります。つまり、攻撃グループ別の脅威対策モデルを作成する際は、同じ戦区にある別のグループのTTPsも考慮しておく必要があります。たとえ中国の攻撃グループが諜報ノウハウを強化し、手口を巧妙化したとしても、ネットワーク境界のデバイスにパッチを迅速に適用することで、そうした活動から自社を保護することができます。

上記を踏まえ、ぜひ実行してほしいアクション：
自社が事業展開する地域に影響を及ぼす地政学的な情勢を注視しましょう。

ランサムウェア攻撃グループの動向：新興勢力、活動を続ける勢力、活動を再開した勢力

ランサムウェア業界の勢力図は常に変化しています。ある攻撃グループが一時的に後退しても、攻撃数の全体的な増加傾向は変わりません。

2021年5月、ランサムウェア Darksideの運営グループが Colonial Pipeline社に対する攻撃を仕掛けました。その後しばらくの間は、あたかもランサムウェア攻撃の動きが停滞し、多くのグループが身を潜めているかのように見えました。しかし、11月から12月に発生した暴露型（Name and Shame）攻撃の件数の結果を見れば、そんな考えは覆ります。11月には、当社CTUリサーチチームが監視する暴露サイト全体で、名前が掲載された被害組織の数は2021年のピークに達しました。12月には、暴露を行う攻撃グループの数が過去最高となりました。もちろん暴露サイトの状況は、ランサムウェア攻撃全体のごく一部を反映したものにすぎません。被害を受けても社名が暴露される前に身代金を払う組織や、暴露サイトを開設していない攻撃グループも多数存在します。

11月から12月にかけて、最も活発な動きを見せた暴露型攻撃グループはLockBitとContiです。11月にはSabbath、Entropyなどの新たなグループが姿を現したほか、12月にはALPHV（別名Blackcat）、Bl@ckt0r、RobinHood、ROOKといったグループも登場しました。

「新興」とされるこれらの勢力のなかで最も活発なのが、ファイル暗号化を行わない脅迫攻撃を専門に行っていると見られるKarakurtです。Karakurtは12月に33の組織名を暴露サイトに掲載しましたが、攻撃自体は9月には行っており、12月になって暴露サイトを新設したと見られます。

2021年11月、暴露型攻撃グループSnatchが活動を再開しました。Snatchは暴露サイトを初めて開設したグループであり、2019年5月に6つの組織名を掲載した後に活動休止状態になっていましたが、2021年12月末までに23に上る組織が掲載されています。一方、活動休止状態が続くグループもあります。ランサムウェア REvilの運営元GOLD SOUTHFIELDのサイトには10月以降、新たな被害組織が掲載されていません。

ランサムウェアは、ヒュドラー（ギリシャ神話に登場する9つ首の不死身の怪物）のような存在です。個々のグループが消滅・休止状態になっても、新たなグループがたちまち出現します。司法・捜査当局による厳しい取り締まりにもかかわらず、2021年、暴露サイトに掲載された被害組織の月ごとの数が2021年1月の数を下回ることはありませんでした。さらに、2021年に暴露された被害組織の数は2020年の倍以上に増えました。ランサムウェアの拡散手段として長年出回っていたEmotetが11月に復活したことで、2022年には被害組織の数がさらに拡大する恐れがあります。まだまだ警戒の手を緩めることはできません。

上記を踏まえ、ぜひ実行してほしいアクション：
インターネット接続サーバーへのアクセスすべてに多要素認証を適用し、
ランサムウェア攻撃リスクを防ぎましょう。

結論

ランサムウェア攻撃グループや、国家を後ろ盾とする攻撃グループの手口はますます巧妙化し、検知を逃れるステルス性、攻撃の有効性も高まっています。そのため、脆弱性が注目されるたびに今後とも積極的に攻撃を仕掛けてくるでしょう。また、至るところでサードパーティコードが使われているため、組織における脆弱性管理やネットワーク防御の作業負担は増大しています。こうした攻撃グループによる侵入の検知・阻止だけでなく、できれば予防機能も備えた検知システムやセキュリティ統制対策を活用することが、これまで以上に重要になります。

CTUリサーチチームについて

CTUのリサーチャーは、メディアでも頻繁に取り上げられ、セキュリティコミュニティ向けの技術分析を公開し、セキュリティカンファレンスでは新たな脅威について説明しています。セキュアワークスの高度なセキュリティテクノロジーと、業界でのネットワークを活用して、CTUリサーチチームは脅威アクターを追跡し、異常なアクティビティを分析して、新しい攻撃手法と脅威を追跡しています。このプロセスにより、CTUのリサーチャーは、脅威をすぐに識別し、損害が生じる前にお客様を保護する対策を開発します。

リサーチ

お客様が直面する脅威の根本を理解し、対処・保護するための対策を作成

インテリジェンス

ネットワークエッジを超えて、脅威の可視性を強化する情報を提供

統合

CTUによるリサーチとインテリジェンスを、セキュアワークスのマネージド・セキュリティ・サービスとコンサルティングに投入

Secureworks®

Secureworks®（NASDAQ: SCWX）は、サイバーセキュリティにおける世界的な先進企業です。当社ソリューションをご活用いただくことにより、お客様やパートナーは攻撃者よりも常に先手を打ち、マーケットに迅速に対応し、ビジネスニーズを満たすことができます。クラウドネイティブのSaaSセキュリティプラットフォームとインテリジェンス主導のセキュリティソリューションの独自の組み合わせにより、20年以上の脅威インテリジェンスと分析から得た深く広い知見を提供しております。このように、長年にわたるサイバー攻撃の最前線で蓄積した実践経験に基づく知見を提供するセキュリティプラットフォームは、唯一無二のセキュアワークスだけです。

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest,
Sydney NSW Australia 2086

日本
東京都千代田区大手町一丁目2番1号
Otemachi Oneタワー17階
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

緊急のインシデント対応に関するご相談は、こちらまでご連絡ください。

03-6848-9760

