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 3

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、企業や組織のシステム保護を支援しています。2022年3月から4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。

- **ランサムウェア攻撃やハック・アンド・リーク（意図的なデータ漏えい）攻撃の勢いは止まらず**
- **ロシアおよびウクライナ：局地的な脅威**
- **Spring4Shellによる影響は、当初の懸念ほど深刻ではなかった**

ランサムウェア攻撃やハック・アンド・リーク（意図的なデータ漏えい）攻撃の勢いは止まらず

サイバー犯罪集団は、内部情報の流出、司法・捜査当局の措置、活動ノウハウの蓄積不足などの逆境を乗り越え、勢力を拡大しています。引き続き警戒を怠らないようにしましょう。

Conti leaksの内情暴露投稿は3月まで続き、攻撃グループGOLD ULRICKにおける高度な分業体制およびランサムウェアContiの運営スキームが暴露されました。これを受け、同グループが活動休止に追い込まれるのではないかという憶測が飛び交いましたが、4月末現在も活動を続けています。当社CTUの分析によると、4月30日時点でのContiの活動レベルは最盛期（2021年）と同水準となっています。

全般的に、ランサムウェア攻撃の勢いは依然として衰えを見せていません。ロシア正教会のクリスマス時期である1月に小休止があったものの、当社CTUリサーチャーが追跡管理するランサムウェア攻撃の暴露サイトの多くでは活動レベルが着実に増えています。また、2021年10月に米国の司法・捜査当局によるテイクダウン（攻撃インフラの停止）措置を受け、2022年1月には構成員がロシアで逮捕された攻撃グループGOLD SOUTHFIELDが4月に入ってランサムウェアREvilの運営を再開しました。

さらに、脅迫特化型の攻撃（別名：ハック・アンド・リーク攻撃）を行うLapsus$など、比較的新しい攻撃グループも順調に活動しています。同グループは経験の浅い10代の若者を中心に構成されていると見られますが、ソーシャルエンジニアリング攻撃の手法でMicrosoft社などのグローバル企業を次々に侵害しています。

個々の構成員、攻撃グループ、マネーロンダリングサービス、アンダーグラウンドフォーラムに対する司法・捜査当局の措置をもってしても、ランサムウェア攻撃のリスクは依然として高い状況です。攻撃の技術的な複雑度にかかわらず、パッチ未適用のシステムを有する組織、および多要素認証などのアイデンティティ管理手段、サプライチェーンにおけるセキュリティ監視、多層型セキュリティ対策に不備がある組織は攻撃リスクにさらされ続けることになります。ランサムウェア攻撃やハック・アンド・リーク攻撃から自社を守るために、基本的なセキュリティプラクティスを踏襲し、セキュリティ対策を隅々まで徹底的に実装しましょう。

上記を踏まえ、ぜひ実行してほしいアクション：
リスクを評価する際は「ランサムウェア」を最大の脅威と考えて優先的に対応しましょう。

ロシアおよびウクライナ：局地的な脅威

ウクライナとの接点がない組織のネットワーク防御担当者は、今般の紛争に気を取られて長期的なセキュリティ課題への対応がおろそかにならないよう気を付けましょう。大半の組織にとっては、ウクライナ戦争に関連した攻撃よりもランサムウェア攻撃によるリスクのほうが圧倒的に大きな懸念材料です。

ロシア政府を後ろ盾とする攻撃グループによるウクライナ侵攻関連の攻撃活動は、3月～4月にかけてもこれまでと変わらずウクライナ国内が集中的に狙われました。4月8日に実行されたウクライナのエネルギー事業者に対する攻撃は失敗に終わりましたが、この攻撃で使われた産業用制御システムに対するマルウェアは、2016年12月にウクライナで停電を引き起こしたマルウェアのコードと類似していました。2016年12月の攻撃はロシア連邦軍参謀本部情報総局(GRU)の特殊部隊「Unit 74455」の仕業であることが、米国政府によって確認されています。また、民間事業者Viasat社の衛星通信機器が標的となった今年2月の攻撃もロシアの攻撃グループによるものでした。この攻撃は、ウクライナへの侵攻中に同国内の通信を妨害することが目的でしたが、付随的な被害は広範囲に及び、欧州各地の一般世帯向けブロードバンド回線数万件が一部サービス停止に陥ったほか、ドイツで稼働する風力発電機のリモートアクセスおよび監視機能が停止する、などの被害が出ました。本レポート作成日時点で公表されている「ロシア政府傘下の攻撃グループが紛争に乗じて仕掛けた攻撃」のなかで、ウクライナ以外の国や地域のシステムに影響が及んだ攻撃は上記以外にはありません。

ウクライナ以外の国や地域の組織にとってのリスクはこうした付随的な被害だけにとどまりません。ロシアとつながりのある組織を狙う親ウクライナ派の攻撃グループ、もしくはウクライナとつながりのある組織を狙う親ロシア派のハクティビスト（政治的思想をもつハッカー）の標的となるリスクもあります。ハクティビストの常套手段である分散型サービス拒否(DDoS)攻撃の件数が大きく増えている理由は、今回の紛争に起因すると見られます。自社が標的組織に該当すると思われる場合は、DDoS対策サービスを実装しましょう。

優秀なハクティビストによる攻撃が一定規模の混乱を引き起こすとはいえ、脅威動向を分析する限り、脅威の規模はサイバー犯罪には遠く及びません。ランサムウェア攻撃は世界規模で増加の一途をたどっているため、ウクライナ以外の国や地域の組織はこうしたサイバー攻撃への備えを最優先に考えるべきです。

上記を踏まえ、ぜひ実行してほしいアクション：
机上演習のシナリオにランサムウェア攻撃のシミュレーションを組み入れましょう。ランサムウェア攻撃グループが使う攻撃手法の多くは、国家を後ろ盾とする攻撃グループやハクティビストの手法と共通しているため、こうした演習を行うことで様々な攻撃に備えることができます。

Spring4Shellによる影響は、当初の懸念ほど深刻ではなかった

大きく報道される脆弱性のすべてが当初の想定どおりのダメージをもたらすわけではありません。脅威インテリジェンスの最新情報を入手し、自社の資産を適切に管理することで、新たな脆弱性が現在進行形で悪用されているのか、理論上のリスクにすぎないのかを見極められるようになります。

3月29日、Spring Framework Coreコンポーネントにリモートコード実行（RCE）を引き起こすゼロデイ脆弱性が存在する、という噂が流れました。Springは世界各地で広く利用されているJavaアプリケーションフレームワークです。3月30日の未明、ある人物が悪用攻撃の概念実証（PoC）コードのリンクをTwitterに投稿しましたが、このアカウントはすぐに削除されました。当該脆弱性（dCVE-2022-22965）の深刻度を表すCVSSv3のスコアは10点満点中9.8となっており、広範囲にわたり悪用されたLog4Shell（Javaのログ出力ライブラリLog4jに影響を及ぼしたCVE-2021-44228）にちなんでSpring4Shellという名称が付けられました。。

Log4Shellと同様、Spring4Shellも多くの組織に影響を及ぼす恐れがありました。しかし実際の影響範囲は予想に比べてはるかに限定的だったようです。Log4Shellを使った悪用攻撃が当初考えられていたほど簡単ではなかったように、Spring4Shellを使った悪用攻撃も一定の条件が揃わなければ実行できず、デフォルト構成どおりに実装されていれば脆弱性の問題はありません。当社CTUのリサーチャーおよびインシデント対応者が実際に遭遇したSpring4Shellの悪用事案は数件のみでした。

こうした脆弱性を見ると、細部にわたって注意を怠らないことの重要性が改めてわかります。ネットワークセキュリティ担当者は、脆弱性が悪用される可能性を常に頭に入れて悪用手法を評価し、「自社環境への影響度」を具体的に把握しておく必要があります。ランサムウェアをはじめとするサイバー攻撃を防ぐにはパッチ適用がきわめて重要です。そのため当社のインシデント対応チームは日頃から「注目度の高い脆弱性へのパッチ適用」を推奨しています。最新の脅威インテリジェンスと適切な資産管理を組み合わせ、各種推奨策の優先順位を自社環境に応じて分類し、適用しましょう。

上記を踏まえ、ぜひ実行してほしいアクション：
脅威インテリジェンスの進化に後れを取らないように社内リソースを更新し、充分な信頼性、妥当性、包括性を備えているかどうか確認しましょう。

結論

注目度の高い脆弱性や国家的な敵対グループによるリスクは、当初の見立てほど深刻ではない可能性があります。一方ランサムウェアなどによる脅威は深刻であり、驚くほど高い回復力や永続力を備えています。憶測にもとづく報道に右往左往せず、最新の脅威インテリジェンスをもとに対応策を判断することが、自社環境の適切かつ効率的な防御につながります。

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
〒100-8159
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

