Secureworks®

脅威インテリジェンス エグゼクティブレポート

Volume 2021, Number 6

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。2021 年 9 月から 10 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。

- Qakbotが復活し、ランサムウェア攻撃を再開
- ペネトレーションテスターだけでなく攻撃者にとっても便利なCobalt Strike
- ランサムウェアー掃を見据える司法・捜査当局

Qakbotが復活し、ランサムウェア攻撃を再開

ランサムウェア攻撃は、初期アクセスの確立から最終的なランサムウェア展開まで、いくつもの段階を経て行われます。複数の攻撃者が多岐にわたる手法を駆使したり、ツールやマルウェアを組み合わせた複雑な攻撃チェーンが用いられることもあります。Qakbotをはじめとするダウンロード用マルウェアやボットネットはランサムウェア攻撃チェーンで重要な役割を担っているため、これらの活動を監視することがセキュリティ対策上不可欠です。

当社CTUのリサーチャーは2021年9月9日、2ヵ月にわたり休止状態であったボットネットQakbot（別名QbotまたはPinkslip）の活動再開を確認しました。Qakbotは認証情報の窃取、スパムメールの配信、Webトラフィックの傍受や操作などを実行可能なモジュール型のマルウェアフレームワークです。感染したホストがQakbotのボットネットに追加されることから、ボットネットだけでなくマルウェアそのものもQakbotと呼ばれています。攻撃グループのGOLD LAGOONは2007年以降、ほぼ休みなくQakbotの運営を続けてきました。これまでにもQakbotのインフラの一部が休止状態になり通信が停止したことはありましたが、今回の休止期間中は重要なインフラが完全に停止状態となっていました。

ローダーマルウェアやボットネットは、ランサムウェア攻撃の「イネーブラー」または「前兆」の一つで、更なる攻撃活動をもたらすものです。これらはランサムウェアの運営組織や加盟メンバーとは異なるグループが実行していることもありますが、マルウェアやボットネットサービスのレンタルや販売を通じて、ランサムウェア攻撃グループやサイバー犯罪グループと連携している可能性もあります。また、自らが活動の幅を広げ、ランサムウェア攻撃に手を染めることもあります。たとえばGOLD DRAKEはボットネットDridexおよび複数のランサムウェア亜種（BitPaymer、PayloadBinなど）を運営しています。

前述のGOLD LAGOONがランサムウェア攻撃に手を広げるという確証はありませんが、ランサムウェア配信に関する活動がますます増えていることは確かです。2021年を通じて、Qakbotを使う複数の攻撃グループによって、侵害されたホストにマルウェアが配信されていますが、これらがランサムウェア展開の前兆であることは当社のCTUリサーチャーによって確認済みです。Qakbotの存在をいち早く検知して対応できるように、あらかじめ備えましょう。

上記を踏まえ、ぜひ実行してほしいアクション：
ランサムウェア攻撃の初期段階によく使われるマルウェア（Qakbotなど）を検知可能な対策を実装しましょう。

ペネトレーションテスターだけでなく攻撃者にとっても便利なCobalt Strike

攻撃者は、商用製品を悪用することで多くのメリットを享受します。システム上に存在しないはずのCobalt Strikeが発見された場合は、攻撃者の存在が疑われます。

Cobalt Strikeはペネトレーションテストのフレームワークとして広く普及している商用製品です。セキュリティ診断ツールとして開発された製品ですが、近年ではサイバー犯罪者や国家支援の攻撃グループの間で人気が高まっており、ランサムウェア攻撃チェーンでもCobalt Strikeが使用される事例がますます増えています。たとえば9月には、他の正規ツールとCobalt Strikeを併用したランサムウェア、Hiveを使った攻撃が行われました。

攻撃者が商用製品を使うと、複数のメリットを得られます。たとえば、Cobalt Strikeはクラックされたものや、正規ライセンスが流出したものがインターネット上から入手できるため、攻撃元の特定が難しいという点があります。多数の機能を持ち、マニュアルも完備され、追加で必要な開発もほとんど必要ないため使い勝手が良く、汎用性が高いため攻撃の様々な側面に応用できます。

そのままでも充分便利ですが、ある攻撃グループがCobalt StrikeをカスタマイズしたVermilion Strikeというツールを開発しました。Linux、Windowsそれぞれに完全対応するバージョンに加え、単一の通信形態に的を絞った「簡易」バージョンもあります。この攻撃グループはエンドポイント対策ソリューションによるCobalt Strikeのコードチェックを回避しつつ、Cobalt Strike本来の機能も享受したいという動機でVermilion Strikeの開発に至った可能性があります。両ツールはよく似ているため、Vermilion Strikeを使った活動がCobalt Strikeによるものと誤検知され、攻撃者の隠れ蓑として使われる恐れがあります。

システム上でCobalt Strikeによる活動が突然検知されても、ランサムウェア攻撃によるものと断言はできません。しかし正規のペネトレーションテスト以外の活動が検知された場合は何らかの攻撃である可能性が高いため、即座に対応できるように備えましょう。

上記を踏まえ、ぜひ実行してほしいアクション：
侵入の兆候を検知するために、Cobalt Strikeをはじめとする商用製品が不正使用されていないか監視しましょう。

ランサムウェアー掃を見据える司法・捜査当局

司法・捜査当局は、ランサムウェアの運営組織や加盟メンバーとの戦いに勝利を収めています。しかしセキュリティ担当者はまだ安心できません。ランサムウェア攻撃グループは状況に合わせて姿を変え、粘り強く活動を続けます。

9月から10月にかけて、司法・捜査当局はランサムウェア運営組織の大々的な摘発作戦に乗り出しました。アイルランド警察は9月上旬、ランサムウェア攻撃グループGOLD ULRICKを解散に追い込みました。同グループは、2021年5月にアイルランドの公的医療サービス提供母体 (HSE) に対してランサムウェアContiによる攻撃を仕掛けたグループです。この摘発作戦は欧州刑事警察機構 (Europol) と国際刑事警察機構 (Interpol) による捜査協力を得て、ContiのITインフラを狙い撃ちするというものでした。

各国の司法・捜査当局による合同作戦の結果、ランサムウェアREvilを運営するRansomware-as-a-Service (RaaS) グループのGOLD SOUTHFIELDが10月17日をもって活動を停止しました。REvilは、加盟メンバーの1つが7月13日にリモート監視・管理(RMM) 製品のKaseya VSAへの攻撃を実行してKaseya社の顧客を次々にランサムウェアに感染させた後、突然停止状態になりましたが、9月上旬には活動を再開しています。10月は活動停止中と思われますが、油断はできません。

米国連邦捜査局 (FBI) の副長官Paul Abbate氏は9月、「今年に入ってバイデン大統領がロシアのプーチン大統領に再三警告したにもかかわらず、米国組織に対するランサムウェア攻撃の阻止に向けてロシア政府が対処している兆しは一切見られない」と話しています。ランサムウェア運営組織と加盟メンバーは、ロシアを筆頭に多くの旧ソ連諸国で自由に活動しています。ただし、ウクライナのような例外もあります。ウクライナは、あるRaaS加盟メンバーを壊滅させるために10月末に実施された多国間当局の合同作戦に参加しました。このRaaS加盟メンバーはLockerGoga、MegaCortex、Dharmaなどのマルウェアを使った複数の攻撃の首謀者であり、これまで被害を受けた国は71ヵ国、被害組織の数は1,800を超えると見られています。

ロシアおよびその周辺諸国が国際社会の法執行機関への協力に消極的だったことが、捜査の難航を招いたと考えられます。ロシアが迅速かつ断固とした行動を取れることはすでに証明されており、9月には半官半民の長距離通信事業者RostelecomがDDoS（分散型サービス拒否攻撃）ボットネットMerisの一部をシンクホールで検知しました。Merisはロシア最大手のWebサイト運営企業Yandexに対する大規模攻撃に用いられたボットネットです。

当社CTUのリサーチャーは、米国およびその同盟国によるランサムウェア運営組織の一掃作戦（攻撃インフラの壊滅や資産の押収など）がさらに続くものと予想しています。しかし、ランサムウェア攻撃グループはこれまでのように手を変え品を変え舞い戻ってきます。9月から10月にかけて、少なくとも9つの新たな攻撃グループの暴露サイトに被害組織の名前が追加されています。既存の攻撃グループの動きも引き続き活発です。手を変え品を変え、犯罪収益を積み上げるランサムウェア攻撃グループから自組織を守るためには充分な対策を講じる必要があります。

上記を踏まえ、ぜひ実行してほしいアクション：
厳戒態勢を維持し、サイバー衛生を良好な状態に保ちましょう。司法・捜査当局が勝利を収めたものの、ランサムウェア攻撃者による脅威は弱まっていません。

結論

ランサムウェア展開の前兆となる攻撃は、いくつもの段階を経て、多数のツールを用いて行われます。自組織を守るためには、初期段階で用いられるQakbotなどのマルウェアやCobalt Strikeなどの攻撃フレームワークの存在を検知できる包括的な監視機能が不可欠です。司法・捜査当局はランサムウェア攻撃者との戦いに勝利しているものの、戦いはまだまだ終わりません。引き続き、セキュリティ対策を万全に備えましょう。

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
03-4400-9373
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

