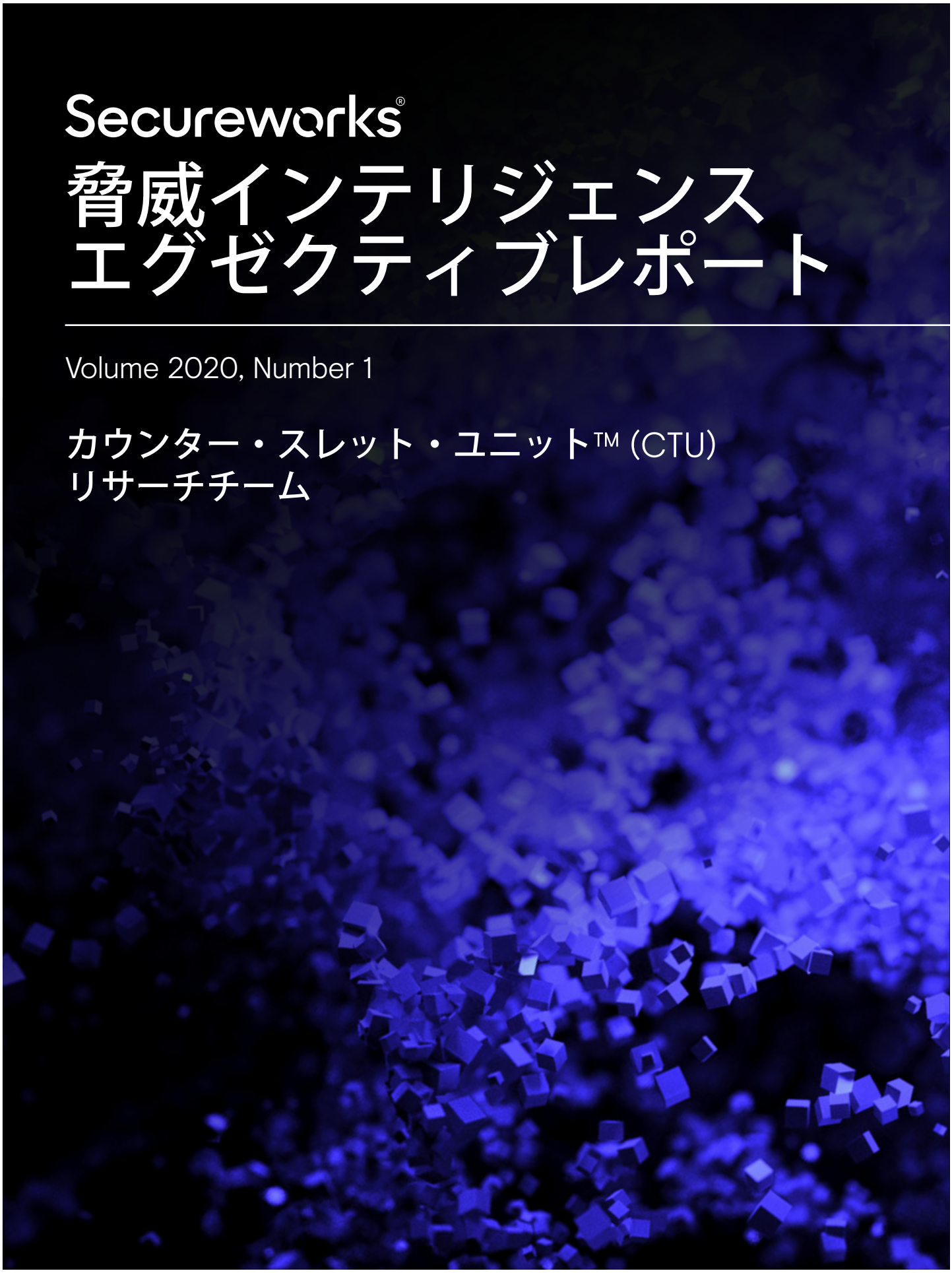
Secureworks®

脅威インテリジェンス エグゼクティブレポート

Volume 2020, 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。2019年11月から2か月にわたり、CTU™ のリサーチャーは、脅威のふるまい、グローバル規模の脅威状況、そしてセキュリティトレンドの観測から、注目すべきポイントをまとめました。

- 継続するイランのスパイ活動
- カスタマイズされたMagecart攻撃が有名な小売ウェブサイトからの顧客データを搾取
- 中国を拠点とする脅威グループは、NGOとアジア政府のネットワークを標的化

継続するイランのスパイ活動

同じのテーマを繰り返し利用することは、攻撃者がこれらの手法で成功したことを示唆する

CTUのリサーチャーは2019年11月上旬、イランに拠点を置くCOBALT TRINITY脅威グループ（APT33およびElfinとも呼ばれる）によって実行された恐れのある、明らかなフィッシングキャンペーンとパスワードスプレー攻撃を発見しました。2つのフィッシングキャンペーンにはそれぞれテーマと標的があり、それらは広範に及ぶパスワードスプレー攻撃と同時に発生しました。そのうち1つのキャンペーンでは、脅威アクターは標的となるメールサーバーを模倣したインフラストラクチャを構築しました。もう1つのキャンペーンは、米国国防省が契約する求人Webサイトを模倣して、公開かつ一般的に利用可能なPoshC2フレームワークを配信しました。2018年と2019年に観測されたCOBALT TRINITYキャンペーンの多くは、「職」をテーマにしたキャンペーンプレイブックに準じています。具体的に9月のキャンペーンでは、米国国防省が別の契約業者のドメインを模倣して、感染したホストにPoshC2およびKoadicマルウェアを配信しました。同時多発的なアクティビティは、COBALT TRINITYが利用できるリソースのレベルを示しています。CTUのリサーチャーは、脅威グループが「職」をテーマにしたキャンペーンを継続することを予測しており、このテーマとテクニックを2年以上利用していることから、成功率が高いと推測されます。

CTUによるCOBALT TRINITYのアクティビティ分析では、このグループの主な動機は、おそらくイラン政府を代表して、戦略的利益獲得のためのスパイ行為であることを示しています。CTUのリサーチャーは、同じ動機を持つイランの脅威グループを多数特定しています。この種の通常行われるスパイ活動は、米国のドローンによるガーセム・ソレイマーニーを殺害したストライキに対する報復作戦と混同すべきではありません。本レポートの公開時点では、CTUのリサーチャーは、イランに拠点を置く脅威アクターからのソレイマーニー関連の報復を観測していません。

カスタマイズされたMagecart攻撃が有名な小売ウェブサイトからの顧客データを搾取

基本的なセキュリティ対策は、小売組織がeコマースWebサイトの侵害を緩和に効果あり

2019年11月と12月、CTUのリサーチャーは、米国デパートメントチェーンMacy'sのWebサイトに影響を与えたMagecartによるWebサイトスキミング攻撃を調査しました。Magecartによる攻撃では、脅威アクターがWebサイトにコードを挿入して、Webサイトの訪問者から個人情報や支払い情報を搾取します。11月14日に被害を受けたユーザーへの声明により、Macy'sは10月7日から10月15日の間に発生したmacys.comのチェックアウトページとマイアカウントウォレットページで送信された顧客の住所と支払い情報に脅威アクターがアクセスできる状態であったと述べました。スキミング手法は、Macy'sのオンライン小売サービス向けにカスタマイズされており、脅威アクターは技術的に洗練され、かつこの標的に対して焦点が向けられていることを示唆しています。

著名な小売Webサイトは、一般的な攻撃の標的となります。悪意のあるクライアント側のスクリプトをeコマースWebサイトに挿入されると、組織の評判が損なわれ、経営にも影響を与える可能性があります。CPUのリサーチャーは、eコマースWebサイトを運営する組織は、適切なセキュリティアップデートをタイムリーに適用し、サードパーティのスクリプトの数を確認し最小限に抑え、ネットワークトラフィックの異常なアクティビティを確認し、Webサイトの変更を監視するプロセス（例：変更管理、コンテンツ管理、ファイルの整合性監視など）を確立することを推奨しています。

中国を拠点とする脅威グループは、NGOとアジア政府のネットワークを標的化

ある脅威グループの既知の手法を監視すると、これらのツールと手法を利用する他のアクティビティを検知できる

2019年11月、CTUのリサーチャーは、中国に拠点を置くBRONSE PRESIDENTが、悪意のあるベトナム語の添付ファイルを含むフィッシングメールを配信するサイバースパイグループを標的としていることを観測しました。添付ファイルには、情報セキュリティの専門家の履歴書と法執行機関のトレーニング文書が含まれていました。脆弱なシステムでドキュメントを開くと、公開されているペネトレーションテストツールであるCobalt Strikeがインストールされました。2019年12月、CTUのリサーチャーは、非政府組織（NGO）を標的としたBRONSE PRESIDENTのアクティビティの分析を公開しました。

このグループは、プロプライエタリで公開されているツールを利用して、東南アジアの法執行機関および政治ネットワーク、ならびにグローバルNGOをターゲットにしています。中国を拠点とする脅威グループはツールを共有し、同様の手法を利用することが多いため、CTUのリサーチャーは中国を拠点とする脅威に遭遇する可能性のある組織に対して、BRONSE PRESIDENTが利用する手法を確認し、この知識を生かして現状の防御対策を評価することを推奨しています。

結論

高度な攻撃の数が増え、脅威のアクターがより高い適応力を実証する一方、多くのサイバーセキュリティインシデントはよく知られているマルウェアとツールを利用していることを認識しておくことが重要です。CTUのリサーチャーは、これらの既知の脅威に対する防御態勢を継続的に見直し、すべてのシステムに基本的なセキュリティコントロールを実装することを推奨しています。例えば、インターネットに面したシステムで多要素認証を利用すると、多くの攻撃を軽減できます。また組織は、高度な脅威グループからのリスクを高める可能性のある世界各国の出来事に対して、常に注意を払う必要があります。

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研究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越えて、脅威の可視性を拡張する情報を提供

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®

グローバルのサイバーセキュリティ・サービス業界をリードする Secureworks®（NASDAQ: SCWX）は、デジタル化が進む社会において、企業組織をサイバーの脅威から保護し続けています。当社は、数千社におよぶお客様から集積したデータと人工知能（AI）、そして独自のカウンター・スレット・プラットフォーム（Counter Threat Platform™：CTP）の自動化による可視性と、お客様の環境を保護する強固なネットワーク効果を創出する当社の卓越したリサーチャーとアナリスト集団から提供される実践的な分析結果を統合してサービスに反映させます。データの種別や出所を問わず集積・分析を行うことで、セキュリティ侵害の防御、悪意ある活動のリアルタイムによる検知、深刻化する脅威の迅速な対応と予見を実現し、サイバーの脅威への対抗策をお客様に提供します。
もっと上手に組み合わせれば、セキュリティは飛躍できる https://www.secureworks.jp/

Corporate Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
www.secureworks.com

Europe & Middle East France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center, Unterschweinstiege 10
60549 Frankfurt am Main
Germany
069/9792-0

United Kingdom
One Creechurch Place, 1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111
00971 4 420 7000

Asia Pacific Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817

日本
212-8589
川崎市幸区堀河町580
ソリッドスクエア東館20階
03-6893-2317
www.secureworks.jp

