Secureworks®

脅威インテリジェンス エグゼクティブレポート

Volume 2019, 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、組織によるシステム保護を支援しています。2019年9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。

- **永続的に続くマルウェアと脅威グループ**
- **政治的情勢に伴い、イランの脅威アクターの活動が継続**
- **侵入済みのランサムウェアは、既存の感染を活用して長期間潜伏**

“APT”の“P”とは – 永続的な脅威例

一部の脅威アクターは、運用上の過失や法的措置にも回避する永続性を確立

政府による支援や反社会的企業の資金提供の有無に関係なく、標的型脅威アクター（Advanced Persistent ThreatやAPT）は、永続性の確立に多大な時間と労力を費やしています。運用面における継続的な成功には、永続性が必要不可欠です。時間と労力による「投資」は一般的に、フォールトトレランスと、リーガルトレランスの2つのカテゴリに分類されます。

フォールトトレランスとは、ミッションを脅かすことなく、運用における障害に耐えうる機能です。これには、既存の検知を回避するカスタムツールの開発や、複数のアクセスベクターを導入、ボットネットをプロキシした悪意のあるアクティビティを阻止する「堅牢な」ネットワークの構築などの技術が含まれます。

Cutwailスパムボットネットは、フォールトトレランスの成功を実証しています。Cutwailマルウェアが2007年に登場して以来、脅威グループはさまざまなバージョンを利用してスパムメール配信ボットネットを構築してきました。現存するCutwailボットネットは、2012年以降、GOLD ESSEX 脅威グループによって継続的に運用されています。CTUのリサーチャーは10月、日本語を標的にして、アップル、アマゾン、および楽天ブランドを悪用して、アカウントの紛失、ロックアウト、不正行為になりすますことで、ユーザー名とパスワードを搾取を試みるボットネットを発見しました。GOLD ESSEX は、セキュリティコミュニティが何度もCutwailの遮断を試みたにもかかわらず、ボットネットを維持できるため、過去10年間で最も永続的な脅威としてランクされています。

リーガルトレランスとは、拘留と起訴を回避する機能です。これには、防弾ホスティングプロバイダーの使用、官庁などに対する贈賄行為や、「見て見ぬふり」といった、テクニカルな領域にとどまらない手法が含まれます。最適化されたリーガルトレランスによるサイバー業務は、政府主導で行われます。

9月、ウクライナ外務省の職員が受け取ったとされるフィッシングメールがVirusTotalのパブリックマルウェアリポジトリにアップロードされました。このメールにZebrocyダウンローダーをドロップするMicrosoft Officeドキュメントが添付されており、CTUのリサーチャーは、ZebrocyはIRON TWILIGHT（APT28、Fancy Bear、Sofacyとも呼ばれる）脅威グループと関連があるとしています。CTUは、IRON TWILIGHTはロシア連邦軍における情報機関であるGRUのインテリジェンスサービスによって運営されていると分析しています。この脅威グループの犯行として有名なものには、2016年の民主党全国委員会（DNC）ネットワーク侵害と、ヒラリー・クリントンのキャンペーン陣営のメールアカウントへの侵害が有名です。米国司法省（DOJ）は、2018年7月に12人のグループメンバーを起訴しました。しかし、今年9月のメールキャンペーンやその他の報告されている活動を振り返ると、IRON TWILIGHが国際規模での法的圧力に持ちこたえる永続性と、継続的な運用を確保できる技術力があることを象徴しています。

イランの脅威アクターによる活動は、国家の緊張状態と一致

政治的緊張はサイバー活動を促す傾向にある

イランからの挑発的なサイバー攻撃と軍事活動は、タンカー戦争や、地域に特化したサイバー攻撃を経て、2019年9月と10月まで続きました。CTUのリサーチャーは、イランのCOBALT KATANA脅威グループが中東の政府機関のWebサイトを侵害し、政府の運営に関連する資格情報を収集していることを発見しました。さらに、イランの脅威グループが、サウジのインターネットサービスプロバイダと、米国の兵役経験者コミュニティを標的にするためにSysKitマルウェアを利用し、さらにTortoiseShellマルウェへと連携させていることが、CTUのリサーチャーにより発見されました。
イラン政府が後押ししていると思われる西側諸国へのサイバー活動の激しさは、9月と10月を通じて一貫して続きました。CTUによる分析では、2019年に発生した複数のキャンペーン通じて、イランは軍事、政治・国政、金融に関する情報に関心があることを示唆しています。CTUによる観測を通じて、イランの経済に対する米国の制裁の影響や、オマーン湾とペルシャ湾での挑発を鑑みると、イラン政府による地域支配の確立という戦略目標と一致しています。

侵入済みのランサムウェアは引き続き、影響度の高い脅威

感染の修正と、脆弱性パッチで、侵入後のランサムウェアのリスクを減らすことができる

CTUのリサーチャーは、侵入済みのランサムウェアの活動が、9月と10月に増加していることを観測しました。2019年全体を通して同じ傾向が続いています。侵入済みのランサムウェアに関連する、セキュアワークスのインシデント対応は2018年から2019年に2倍へと増加しました。同じスキームを使うグループの数も増加しており、その多くが成功を収め、手口がマニュアル化されています。

 © 2020 SecureWorks, Inc. All rights reserved.

脅威グループは、主に2つの手法を利用して足場を確立します。最初の手法には、既存のコモディティマルウェア感染を活用します。たとえば、Ryukランサムウェアは TrickBot感染を利用し、BitPaymerはDridex感染を利用します。通常、最初のマルウェアは大規模なスパムキャンペーンによって配信されます。ランサムウェアはすぐには展開されず、長期間潜伏することがあります（図1を参照）。

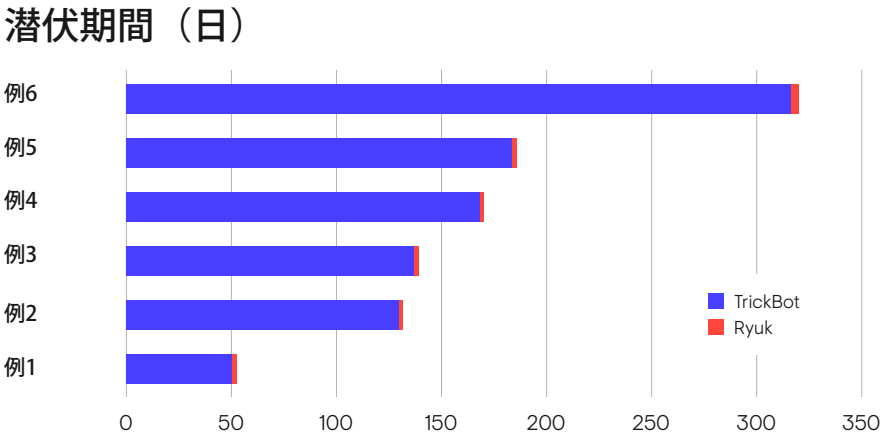

図1: *TrickBot感染からRyukの展開まで、長期の潜伏期間が存在する（出典：セキュアワークス）*

次の手法には、インターネットに接続された脆弱なサーバーへのスキャンと侵入が行われます。脅威グループは通常、リモートデスクトッププロトコル（RDP）を利用して、被害者のインターネット側のネットワークへアクセスします。その後、既知の脆弱性を悪用してシステムへ侵入します。侵入されたシステムは、他のネットワークにアクセスするための足場として利用されます。CTUのリサーチャーは、侵入済みのランサムウェアによる脅威が収益性が高いことから、今後も増加すると予測しています。組織は、最初の侵入を防ぐことにより、リスクを大幅に削減できます。組織が侵入を検知した場合、すべてのマルウェアを排除すること、そしてすべてのアクセスベクトルを削除することが重要です。

結論

高度な攻撃の数が増加し、脅威アクターがより高い適応力を実証する一方、ほとんどのサイバーセキュリティインシデントでは、よく知られているマルウェアとツールを活用しています。CTUのリサーチャーは、これらの既知の脅威に対する保護体制を継続的に見直し、すべてのシステムに基本的なセキュリティ制御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。組織は、地理的・政治的な背景を元に、高度な脅威グループによるリスク増加を考慮することも必要です。

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

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp

 © 2020 SecureWorks, Inc. All rights reserved.