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 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。2020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。

- サイバー犯罪集団による企業脅迫型 DDoS 攻撃
- Microsoft、法的措置を用いて TrickBot を阻止
- 米国による敵対的 APT 攻撃グループへの締め付け強化

サイバー犯罪集団による企業脅迫型 DDoS 攻撃

身分を偽る脅威アクター

2020 年 8 月 28 日、米国連邦捜査局 (FBI) は、数千にのぼる世界各国の組織に対する分散型サービス妨害 (DDoS) 攻撃についてのレポートを公表しました。この攻撃では、DDoS 実行直後に「身代金を払わなければ第二弾としてさらに大規模な攻撃を仕掛ける」という脅迫メールが送りつけられました。送信者は、ロシアの国家的脅威グループ Fancy Bear の一員だと名乗っていましたが、当社 CTU リサーチャーの追跡調査により、実際には IRON TWILIGHT の一員であることが判明しました。2017 年と 2019 年にも同様の攻撃が発生しており、同一の脅威アクターによる犯行とみられています。

最初の DDoS 攻撃は標的組織のシステム障害を起こすことが目的で、平均持続時間は 20 ～ 90 分間ほどでした。的を絞った攻撃のため、単なる総当たり攻撃より効果が出やすくなります。さらに攻撃時の通信量も大きかったため (20～180GB/秒)、DDoS 制御・緩和策を整備していない大半の組織のシステムが容量不足に陥る恐れがあります。

攻撃直後のメールは、6 日以内に身代金およそ 30 万ドルをビットコイン (BTC) で支払うよう要求するものでした。脅威アクターは「応じなければ、身代金の額を吊り上げ、第二弾としてさらに大規模かつ長時間にわたる DDoS 攻撃を仕掛ける」と脅迫しています。多くの場合、第二弾の攻撃発生には至らなかったものの、少ないながらも二次的攻撃に発展したケースでは、攻撃時間が長く、比較的大規模かつ標的組織がピンポイントで狙われました。つまり、脅迫を無視すると攻撃を実行するという意図が読み取れます。

実行犯である脅威アクターは、Fancy Bear や Lazarus Group をはじめとする標的型攻撃 (APT) グループの一員と称していますが、実際は違います。当社 CTU リサーチャーによる調査で、今回の犯行は金銭目的の脅威グループ「GOLD FLANDER」によるものと結論付けられました。

重要なポイント

被害に合った組織は、敵対する国家主体の脅威グループの標的になったわけではありません。数件ではあるものの二次的な攻撃も発生しているため、攻撃リスクを受け入れるのか、DDoS 緩和策を整備するのか、組織として検討する必要があります。最も効率的な DDoS 攻撃防御方法は、あらかじめ緩和策を実装しておくことです。DDoS 攻撃を「業務への脅威」と捉えているのであれば、ネットワークプロバイダーと協力のうえ、基幹データの可用性を保護しておくべきです。

Microsoft、法的措置を用いて TrickBot を阻止

ボットネットの再編が進むも、威力のフル回復には時間を要する見込み

TrickBot は、2016 年 8 月からサイバー犯罪の脅威グループ GOLD BLACKBURN が拡散しているモジュール型の多機能マルウェアファミリーです。同グループは、金融詐欺や脅迫を実行するためのマルウェア開発やボットネット運用のあらゆる側面を熟知しています。ボットネットのアフィリエイト型ビジネスモデル（同グループが一元運用する TrickBot を他のサイバー犯罪脅威グループに貸し出す方式）により、世界的な金融被害が増大しています。

10 月 9 日付のワシントンポスト紙は、米国サイバー軍が TrickBot 撲滅に向けた大規模かつ重要な作戦を実行したと報じています。これとは別に、Microsoft を筆頭にした民間企業同盟は 10 月 12 日、米国の裁判所命令によるTrickBot 阻止に向けた法的措置を講じたことを発表しました。両者の公表タイミングが近いため、米国政府と民間企業との間で何らかの調整が行われていた可能性もあります。Microsoft の 10 月 20 日付更新情報では、同社が TrickBot のインフラであると特定した世界各地のサーバー 128 台のうち 120台 を停止したと発表しています。

米国サイバー軍の措置を受けた GOLD BLACKBURN は、別のコマンド & コントロール (C2) サーバー群を使って TrickBot のサンプルをデプロイするという反撃に出ました。その結果、ボットネットが独立した機能をもつセグメントに分割されました。同グループは、Microsoft による措置が実施された後も新たなセグメントを使ってボットネットの再構築を続けました。

重要なポイント

ボットネット TrickBotの原型は、2020 年 11 月上旬には消滅したとみられています。新たなボットネットセグメントでの活動が低下していることから、実行グループ GOLD BLACKBURN が TrickBot から戦略的に撤退している可能性があります。これに比例して、同グループが運用するマルウェア BazarLoader の件数が増加していることが当社 CTU リサーチャーの調べで判明しました。

これまでボットネット TrickBot の攻撃規模は増減を繰り返していました。このマルウェアは自動で水平移動できるため、ランサムウェア Ryuk や 777 の初期感染ベクトルとしても活用されています。撲滅措置が講じられたものの、TrickBot は今後ともあらゆる組織に対する長期的かつ大きな脅威として残る可能性が高いと見られます (本レポートの公表日現在) 。適切なセキュリティ統制や対策を実行することで、自組織のネットワークを保護できます。さらに、法的手段に訴えた Microsoft の成功例に追随する動きが他社にも広まり、ボットネット撲滅が進む可能性もあります。

米国による敵対的 APT 攻撃グループへの締め付け強化

一連のアラートにより、APT 攻撃グループによる大統領選前の工作活動が露呈

2020 年 9月から 10 月にかけて財務省、司法省 (DOJ) 、FBI 、サイバーセキュリティ・インフラセキュリティ庁 (CISA) を含む複数の米国政府機関から発令された、国家主体の脅威アクターによる敵対的活動に関するアラートおよび制裁措置の件数は異常ともいえる多さでした。この 2 ヶ月間で政府が発動した措置の数は、例年の件数を上回っています。

具体例: 財務省はマルウェア Triton に関与するとして、ロシアの研究機関を制裁対象に指定しました。司法省は、ロシア連邦軍参謀本部情報総局 (GRU) の諜報員 6 名を破壊的マルウェアによる攻撃に関与した疑いで起訴しました。他にも、ロシアの主な国家的攻撃グループすべてによる敵対的活動への措置が講じられました。また、中国の APT 攻撃グループ BRONZE ATLAS (別名APT41) のメンバー 5 名がコンピューターへの侵入容疑で起訴されました。FBI と CISA は共同で、イランの APT 攻撃アクターが有権者登録データを入手したとして、注意を呼びかけました。さらに、イランのイスラム革命防衛隊 (IRGC) が使用したドメイン名が差し押さえられたほか、9 月には司法省がイランの脅威アクターに対する容疑を明らかにしました。

米国による一連の措置は、大統領選を控えた時期における敵対的な APT 攻撃活動けん制を意図したものでした。2020 年前半には、中国の脅威グループ BRONZE VINEWOOD やイランの脅威グループ COBALT ILLUSION が、大統領選への介入や投票結果のかく乱、選挙プロセスに対する米国民の信頼失墜を目的に、選挙活動への攻撃を仕掛けた疑いが報じられています。

こうした脅威アクターは常に、自国の優先課題をもとに色々なセクターの組織を標的にして、大量の個人情報や知的財産、機密情報を収集しています。コロナウィルス関連の研究活動は 2020 年度のサイバースパイ活動の格好のターゲットとなりました。悪質なサイバー活動は、米国と他国との地政学的緊張が高まる時期にも増える傾向があります。

重要なポイント

米国の諜報機関や関連団体による脅威グループの報告件数および司法省による措置件数の増加は、「米国政府には、国家主体の敵対的脅威アクターを追跡し、工作活動を究明する手腕があり、調査結果の一部を公表する用意がある」という米国政府からのアピールであると解釈できます。この傾向をみると、米国政府がリスク算定基準を変え、「限定的な開示だけでは脅威グループの活動監視能力を強化できない」というスタンスにシフトしていると解釈することもできますが、政府による戦略転換を示す根拠はありません。

米国政府による情報開示や制裁措置にもかかわらず、国家主体の敵対的脅威グループは大きなダメージを受けることなくそれぞれの国で活動を続けると予想されます。こうした脅威グループに関する公開情報を確認して脅威の状況を把握し、APT の標的にならないためのサイバーセキュリティ戦略を策定することが、各組織に求められるアクションです。

結論

脅威に関する個々の攻撃活動や活動主体 (アクター) がもたらすリスクレベルは、様々な理由によってその都度変動します。脅威アクターは集団を変えて舞い戻ってくるケースが多いため、活動が小康状態であっても油断できません。脅威の最新動向への注意を怠らず、予期せぬ事態が生じても影響をしっかり見極め、迅速に対応できるようにしておくことが重要です。

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 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戦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。

www.secureworks.com

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
川崎市幸区堀川町 580
ソリッドスクエア東館 20 階
044-556-4300
www.secureworks.jp

