暗号化された

攻撃の現状

2021年版レポート

zscaler™

目次

HTTPSトラフィックは安全でしょうか？

企業のデータセキュリティにおいては、この問題に対する誤解が広まっているようです。HTTPS（＝TLS、旧SSL）は暗号化の業界標準であり、転送中のデータを保護します。その機能は、コンテンツを誰にも見られないようにすることです。しかし、このプロトコルはあくまでも手段であり、暗号化したからといってコンテンツ自体が安全になるわけではありません。マルウェアは、正規のファイルと同じように簡単に暗号化して送信することができ、実際にマルウェアの80%以上がこのような経路で送信されています。

この考えは当たり前なことのように思われますが、ほとんどの組織は、暗号化されたトラフィックを全部は検査していないということを考えてみて下さい。多くの場合、暗号化されたトラフィックは一切検査されていません。トラフィックの大半が暗号化されたチャネルを経由しているのに、なぜ企業は検査しないのでしょうか？さらに一歩進んだ疑問としては、彼らは何に気付いていないのでしょうか？

気付いていないどころの騒ぎではありません。2021年の1月から9月の間に、ゼットスケーラーはHTTPSを介して207億件の脅威をブロックしました。2020年にブロックされた66億の脅威から314％以上の増加を示しており、それ自体は前年からほぼ260%の増加でした。

サイバー犯罪者の攻撃手法はますます巧妙になっており、ダークウェブ上で利用できるアフィリエイトネットワークやサービスツールを活用しています。これにより、セキュリティチームが一瞬たりとも油断できない巧妙な攻撃が爆発的に増加しています。特にランサムウェアは、世界中の企業に影響を与えており、有名な攻撃では数千万ドルの損害が発生しています。マルウェアの暗号化は、攻撃シーケンスの中では些細なステップです。

ランサムウェアをはじめとする数多くの脅威が増加し、ハイブリッドモデルや場所を選ばない仕事のモデルが続出する中で、企業は組織を保護する可能性を最大限に高めるために、オンプレミスおよびオフプレミスのすべてのトラフィックを検査する必要があります。しかし、このような検査には膨大なリソースが必要です。次世代ファイアウォールなどの従来のハードウェアベースのセキュリティツールでこれを大規模に行おうとするのはほぼ不可能であり、パフォーマンスを低下させることなく効果的に行うためには、5 ～ 7倍の数のデバイスが必要となります。その結果、多くの組織は、少なくとも一部の暗号化されたトラフィックを検査しないで通過させています。これは大きな問題ですが、具体的にどのくらいの深刻度なのかをご紹介します。

暗号化されたチャネルを利用した攻撃は、2020年から2021年にかけて、**314%増加しました。**

主な調査結果：

ゼットスケーラーのZero Trust Exchangeには、300兆以上のシグナルと1,600億以上の日々のトランザクションから収集された世界最大のセキュリティデータセットが保管されています。これは、一日のGoogle検索の15倍以上の量です。ゼットスケーラーのThreatLabz脅威研究チームは、2021年前半の9 ヶ月間のデータを分析し、その期間の暗号化トラフィックにおける脅威を評価しました。次の分析は、暗号化された攻撃の状況に関する重要な洞察を示しています。主な調査結果は次のとおりです：

- **HTTPS を介した脅威が増加：** ゼットスケーラーは、2年連続で暗号化トラフィック内の脅威が前年比314%以上増加していることを確認しました。
- **テクノロジ企業は巨大なターゲット：**テクノロジ企業への攻撃は前年比で2,344%増加、小売・卸売企業への攻撃は841%増加しました。
- **重要なサービスに猶予：** 2020年の最大の標的はヘルスケアでしたが、政府機関に対する攻撃とともに脅威は急激に減少しています。コロニアルパイプラインに対する攻撃のような大規模な攻撃を受けて、法執行機関の注目度が高まり、これらの業界が標的としての魅力を失ったのです。
- **暗号化された攻撃のトップターゲットは英国と米国：** インド、オーストラリア、フランスがトップ 5に入っています。
- **攻撃傾向の変化：** マルウェアは212%、フィッシングは90%増加しているのに対し、クリプトマイニング系マルウェアは20%減少しており、ランサムウェアが人気を集めるなど、攻撃の傾向が大きく変化していることが反映されています。
- **ゼロトラストで組織を守る** 暗号化された脅威を防御する最善の方法は、クラウドプロキシベースのゼロトラストアーキテクチャを使用することです。これにより、攻撃対象を減らし、すべてのインバウンドおよびアウトバウンドのトラフィックをインラインで大規模に検査することができます。

テクノロジ企業への
攻撃は **20倍に増加**

SSL (Secure Sockets Layer) やその後継であるTLS (Transport Layer Security)などの最新の暗号化技術は、インターネットトラフィックの大半を保護するために世界中で使用されています。合法的トラフィックの暗号化率が高まると、悪意のあるトラフィックも同様に暗号化されます。ゼットスケーラーは、2021年の9ヶ月間に207億件以上の脅威をブロックしました。

暗号化されたトラフィックは、セキュリティチームが検査する可能性が低いだけでなく、暗号化されたファイルはフィンガープリントが非常に困難であるため、マルウェアが検出されずにすり抜けることができるといった、攻撃者にとっては都合のいい状態となります。

犯罪者が暗号化されたトラフィックに隠すことができる攻撃の種類はさまざまです。マルウェアが圧倒的に多く、攻撃の約91%を占めています。

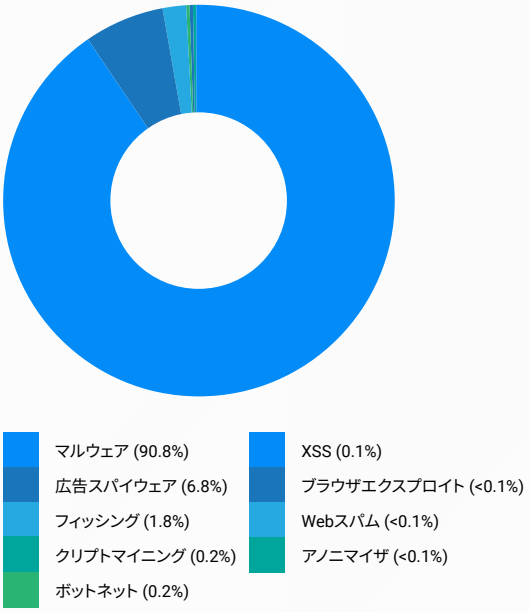

図 1: 暗号化されたチャネルを介した攻撃の頻度

マルウェアが占める攻撃の割合:91%

しかし、他の攻撃タイプも増加しています。広告スパイウェア、ブラウザエクスプロイト、マルウェア、フィッシング、ボットネット攻撃はすべて、2020年と比較すると2021年は増加しています。減少した攻撃タイプは、クリプトマイニング（コンピュータを乗っ取って暗号通貨をマイニングする）、クロスサイトスクリプティング、すなわちXSS（正規のWebサイトに悪意のあるコードを注入する）、アノニマイザ攻撃（プロキシを使って攻撃者を追跡しにくくする）の3つだけでした。 ここ数年、ランサムウェアがより収益性の高い選択肢となっているため、クリプトマイニング攻撃の人気は低下しています。ランサムウェアは、このレポートのマルウェアカテゴリーに含まれています。

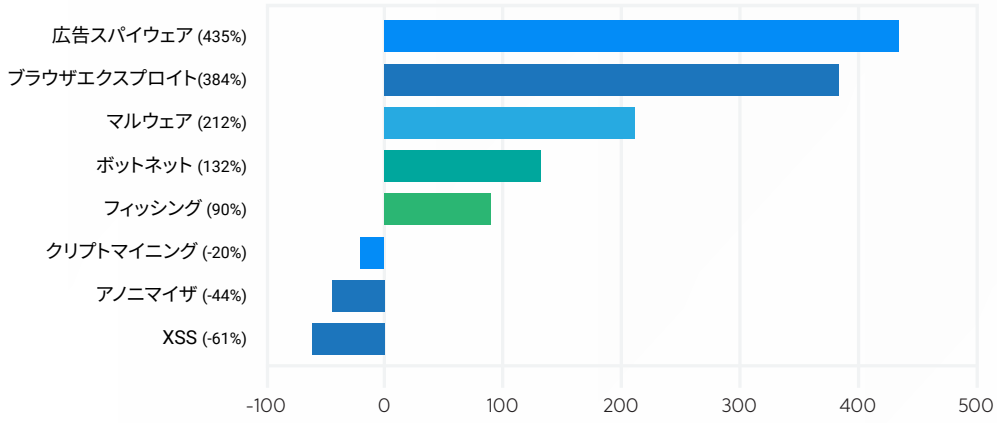

図 2: 暗号化されたチャネルを介した攻撃の年次変化

Web攻撃

Webには、HTTPSプレフィックスが付いたサイトなど、悪意のあるサイトがたくさんあります。インターネットの衛生状態が悪いため、脅威が長引く可能性があります。ゼットスケーラーは、Coinhiveが2年以上シャットダウンされているにもかかわらず、Coinhiveに感染したサイトからの13,000を超える攻撃を観察しました。HTTPSを利用する最も一般的なWeb攻撃カテゴリの1つは、ウェブの支払いデータを盗むために使用されるMagecartのような JavaScript ベースのスキマーです。

ファミリ	ヒット	タイプ
Nicehash	5,644,273	クリプトマイニング
Magecart	2,573,304	支払いのスキミング
Adload	1,626,905	Webスパム
Covid19	972,223	マルウェア
Webシェル	934,873	マルウェア
Coinhive	13,670	クリプトマイニング

感染したウェブサイトは、その後**何年も**残存することがあります。

フィッシング

フィッシングは依然として最も一般的な手口であり、ユーザは隠されたマルウェアを含むメール内のリンクをクリックするように仕向けられます。すべての電子メールおよびファイル共有サービスは攻撃に対して脆弱ですが、Microsoft 365の人気により、2021年には圧倒的に上位のターゲットとなり、9か月の監視期間中に1,500万件を超える攻撃の試みがゼットスケーラーのプラットフォームによってブロックされました。

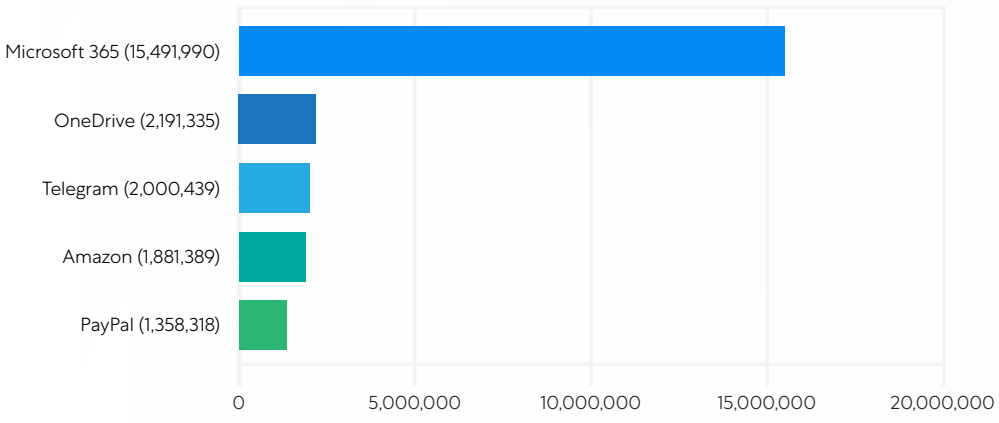

図 3: 暗号化されたフィッシング攻撃

マルウェア

2021年にはマルウェアが攻撃のトップカテゴリでした。マルウェアは通常、感染したリンクから電子メールまたはWebサイトでダウンロードされます。ほとんどの企業が何らかの形でマルウェア対策を行っていますが、攻撃者はその技術を高め、フィンガープリント技術を回避できる新たなマルウェアの変種を作成しています。もちろん、暗号化されたトラフィックを検査していない組織は、マルウェアがシステムに侵入するまで、たとえそれが有名なマルウェアであっても可視化することはできません。以下は、2021年に流行したマルウェアファミリの一部です。このレポートの後半で、これらのファミリのうち4つのファミリについて、その攻撃手順を示す技術的な事例を紹介をします。

ファミリ	マルウェアの攻撃
njRAT	355,753
Ursnif	336,540
Azorult	199,334
Hancitor	137,421
Emotet	58,867
QakBot	30,199
Smokeloader	4,269

個人識別情報（PII）は、情報窃盗の試みの**最大の標的です。**

情報窃盗

攻撃者は暗号化されたチャネルを使ってシステムに侵入するだけでなく、暗号化されたチャネルを使ってデータを流出させることもあります。最もよく流出するデータタイプは、Aadhar（インド）、TFN（オーストラリア）、Social Security（米国）、BSN（オランダ）の番号などの、国家および税務上の識別子です。次いで、クレジットカードや金融情報、そして知的財産や医療データが狙われています。次のグラフは、わずか3ヶ月分の情報窃盗の試みを示しています。

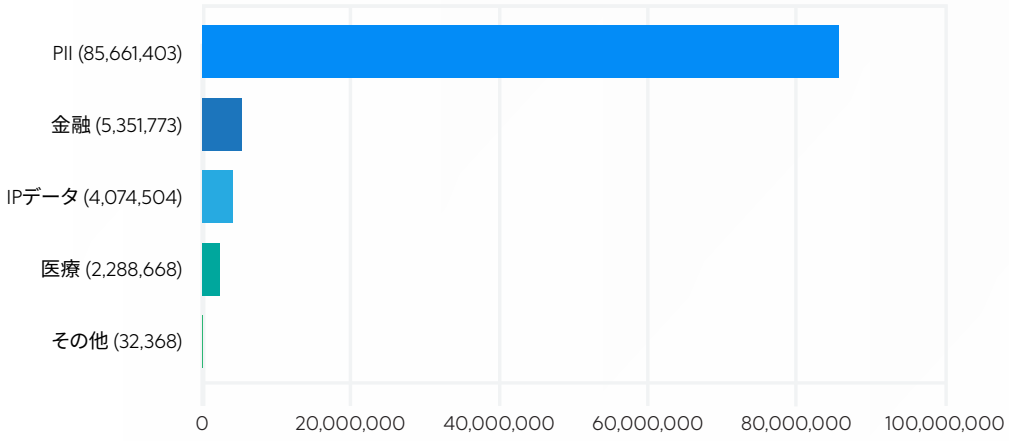

図 4: 情報窃盗の試み

コマンド&コントロール活動

コマンド&コントロール (C&C) サーバは、標的型攻撃での第2段階のペイロードの実行、データの盗用、ボットネットで使用するマシンの制御など、さまざまな理由で使用されます。 ボットネットは、攻撃者の制御下にあるデバイスのネットワークであり、大規模な協調攻撃を可能にします。 ボットネットは、分散型サービス拒否 (DDoS) 攻撃、金融データの侵害、暗号通貨のマイニング、標的型侵入などに利用されてきました。

攻撃者は、さまざまなツールを使用してC& Cサーバにコールバックします。Smoke LoaderやGumblarなどは、この目的のために特別に設計されたボットです。 その他、 CobaltstrikeやPoshc2などは、攻撃者によって再利用されている侵入テストツールです。以下は、これらのツールを使用したコールバックの試行率です。

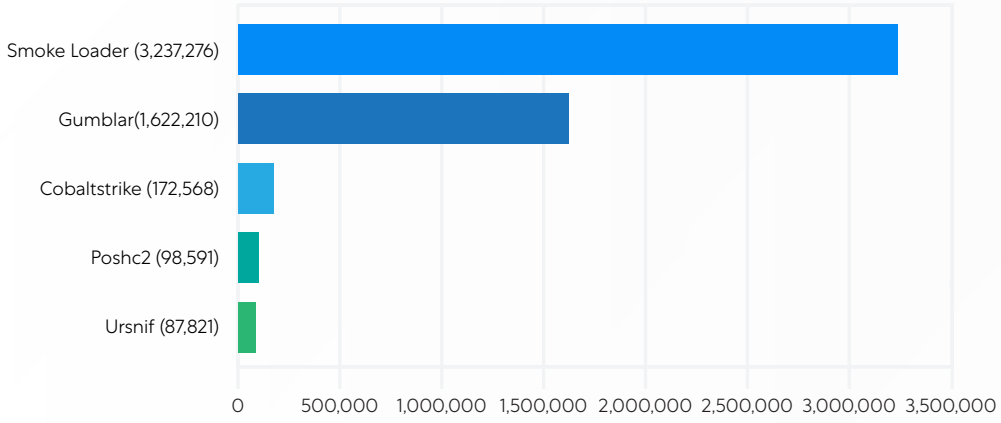

図 5: コマンド&コントロール活動

攻撃者は、暗号化されたWeb上のアプリケーションの約**70%**に影響を及ぼします。

認証スタッフィングとエクスプロイト活動

暗号化されたトラフィックに拡散するのはマルウェアだけではありません。攻撃者はまた、これらのチャネルを使用して、暗号化されたアプリケーションを悪用することにより、人間による攻撃を試みます。

Threatlabzチームは、また、ゼットスケーラーのディセプション技術を用いてグローバルに展開された網状の「おとり」から情報を収集し、攻撃者の戦術、技術、手順 (TTP) も研究しています。「おとり」アセットは攻撃者の餌として使用され、正規ユーザーによって操作されることはないため、「おとり」アセットとの関与は悪意のある活動の兆候となります。ThreatLabzが発見したのは次の通りです。

1. すべてのSSL対応アプリケーション「おとり」の約70%が相互作用を持っていました。これは、SSL対応アプリケーションの70%に攻撃が試みられている可能性があることを示しています。
2. インターネット向けの「おとり」Webアプリケーションのコンテキストでは、認証情報攻撃の約48%が電子メールとVPN「おとり」に対するものでした。
   - 電子メールの「おとり」は、盗んだ認証情報をスタッフィングするのによく使われるターゲットでした。
   - VPN「おとり」は、VPN製品で最近公開されたCVEの悪用の対象となっていました。
3. 最もよく観察された手法は、「.git」ファイルの検索で、ソースコードを公開するために誤って設定されたWebサーバを検索する目的で行われたと考えられます。この手法は以前からありましたが、今でも侵入前の偵察では非常に一般的なものです。

モバイル攻撃

スマートフォンやタブレット端末は、攻撃者が偽のアプリケーションを使用して悪用する人気のターゲットであり続けています。初期の頃の感染以降、新しく流行になったモバイルマルウェアの亜種の多くは、SSLネットワーク通信を使用して、コマンド&コントロール活動をするもので、ペイロードの取得や、悪意のある活動やデータ盗用を行うためのコマンドの受信などをします。Hydra、Joker、そして新たに発見されたGriftHorseなどのマルウェアファミリは、感染後の活動にSSLを活用していることがわかっています。

GriftHorseマルウェア

最近表面化したAndroid向けマルウェア「GriftHorse」は、全世界で1,000万人以上の被害者を出し、数億相当とも言われるユーロを盗んでいました。感染すると、賞品を受け取るために電話番号を送信するように誘導されます。被害者が知らないうちに、その電話番号はプレミアム SMSサービスに加入しており、被害者の電話料金は毎月30 ユーロ以上も請求されていました。このトロイの木馬は、3つの段階でC&Cサーバと通信し、感染後の活動にSSLを活用していることが判明しました。

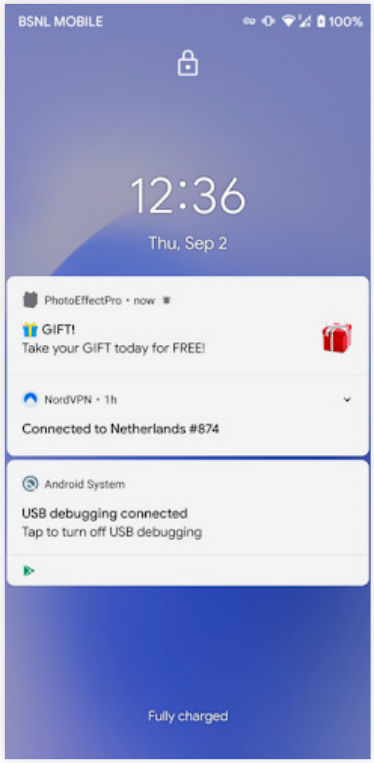

図 6：GriftHorseマルウェア

Jokerマルウェア

Jokerは、GooglePlayストアを通じてAndroidデバイスを標的とする最も著名なマルウェアファミリの1つです。**ゼットスケーラー**は、Jokerマルウェアがコマンド&コントロール活動に使用するTLS経由のコールバック試行を約22,000回ブロックしました。このマルウェアは一般に認識されているにもかかわらず、コード、実行方法、ペイロード取得技術の姿を変貌させながら、Googleの公式アプリケーション市場への侵入をし続けています。Jokerは、スパイウェアの一種であり、SMSメッセージ、連絡先リスト、デバイス情報を盗み、被害者をプレミアムワイヤレスアプリケーションプロトコル (WAP) サービスに登録するように設計されています。

Hydraマルウェア

Hydraは、バンキングマルウェアの中でも最も一般的で強力な例の1つです。その機能の代表的なものには、ユーザの画面上で行われている活動を時間の経過とともに動画化するスクリーンキャストがあります。Hydraは、攻撃者が感染したデバイスを監視・制御できるリモートアプリをインストールすることもできるため、深刻な脅威になります。Hydraは、SSL証明書を利用してコマンド&コントロール活動を行います。

業種別

2021年と2020年を比較すると、業界によって大きな違いがありました。当社による調査では、暗号化されたチャネルでの攻撃率が上昇した業界が7つありましたが、昨年度に最大のターゲットとなったヘルスケアを含め、2つは実際に攻撃率が減少しました。

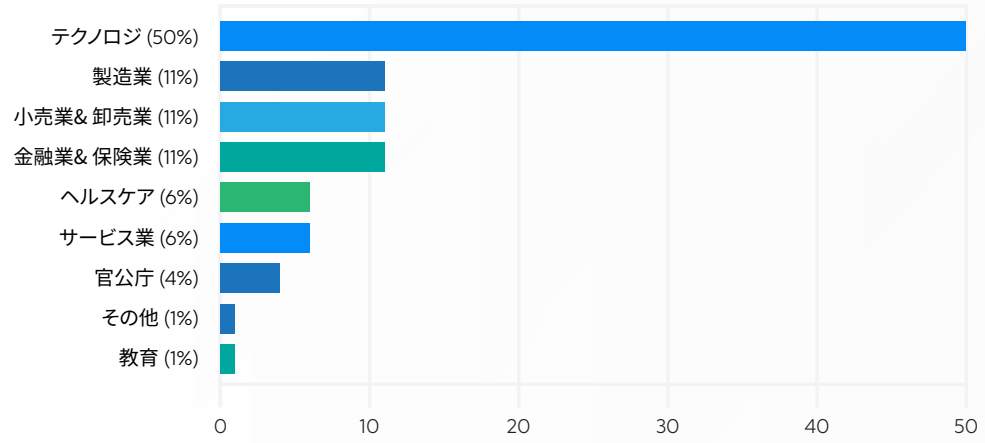

図 7: 業界別の攻撃量

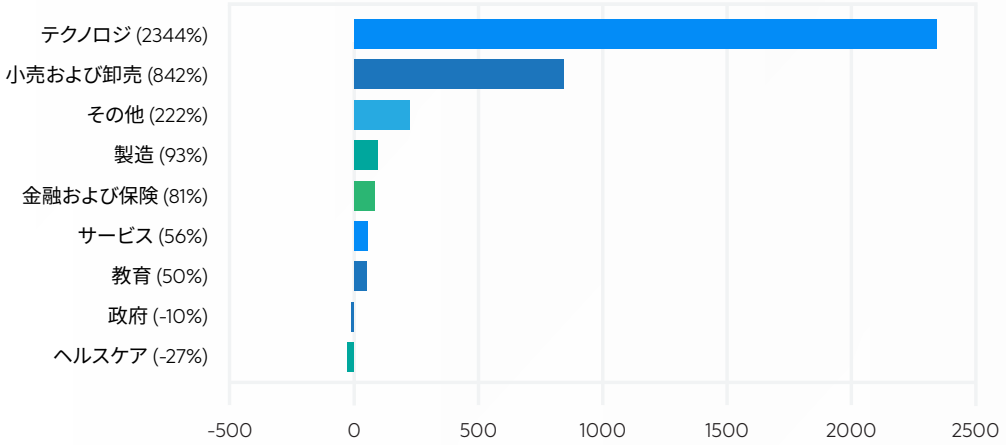

図 8: 2021年業界別攻撃量対2020年

テクノロジと小売業では攻撃率が大幅に増加しています

テクノロジ企業への攻撃は驚異的な23倍の増加を見せ、現在、観察されている攻撃の半分以上を占めています。テクノロジ業界は、他の業界よりもはるかに高い割合でマルウェアに悩まされています。ほぼすべてのビジネス機能がテクノロジに大きく依存しているため、攻撃者は多くの攻撃対象領域を悪用できます。これは、リモート接続から電話会議、SaaSベースのアプリ、パブリッククラウドワークロードまで、あらゆるものでリモートワーカーをサポートする必要性が急増したことで悪化しました。

テクノロジ企業は、他の企業のサプライチェーンの中で重要な役割を担っているため、魅力的なターゲットとなります。サプライチェーン攻撃が成功すれば、KaseyaやSolarWindsなどの事例に見られるように、攻撃者は何百人、何千人もの下流の被害者にアクセスできるようになります。

小売および卸売部門もまた、攻撃率が8倍以上増加するという、非常に悪い年でした。2020年は攻撃の3.5％しか占めていませんでしたが、2021年には攻撃の11％を占めていました。TLSチャネルを介して小売業者やeコマース業者を狙うスキマー、悪意のあるJavaスクリプト、マルウェアのペイロードなどの悪意のあるコンテンツが大幅に増加しました。

世界が正常な状態に戻り始め、ビジネスや公共のイベントが世界中で開かれるようになっても、多くの従業員は、いまだに比較的安全ではない環境で働いています。重要なPOSシステムにアクセスすることは、サイバー犯罪者にとって非常に魅力的ですが、これはサイバー犯罪者に莫大な利益をもたらす可能性の扉を開くからです。

ヘルスケア業界や政府機関への攻撃が減少

2020年に最大の標的となったものの、ヘルスケア業界への攻撃は2021年に27％減少しました。同様に、政府機関への攻撃は10％減少しました。SolarWinds社への攻撃、Colonial Pipeline社への攻撃、アイルランドのHealth Service Executive社へのランサムウェア攻撃など、重要なサービスに影響を与えた大規模なランサムウェア攻撃は、法執行機関の最高レベルから注目されており、これらの重要な産業は、手出しをするには危険が大きすぎるわけです。さらに、多くのランサムウェアファミリーは、パンデミックの際に医療やその他の重要なサービスを攻撃しないことを宣言していますが、これらの約束は、完全には守られてはいません。

地域

暗号化攻撃で最も狙われている国は、英国、アメリカ、インド、オーストラリア、フランスの5 ヶ国です。

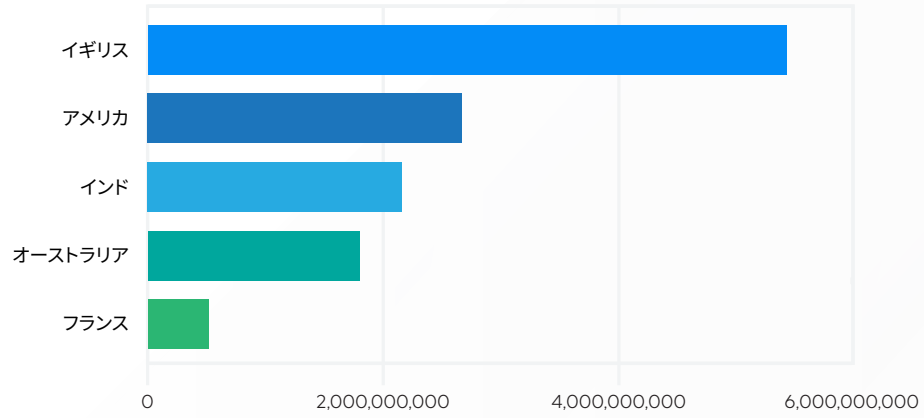

図 9: 最も攻撃された国

これらの国はいずれも大規模な技術拠点であり、その分野を標的とした攻撃の全体的な増加に伴い、攻撃率も増加しています。ThreatLabzは、一般的なターゲットではない小国を含む世界中の255の異なる国で攻撃を観測しました。 その中には、カリブ海の全域の島々、フェロー諸島、サン・バルテルミー島、フォークランド諸島などでの750万件以上の攻撃が含まれていました。 これは、「場所を選ばない仕事」ポリシーの増加により、従業員が遠隔地で仕事をするようになったためです。

英国での大規模な攻撃率を筆頭に、ヨーロッパ全体では、暗号化されたチャネルを介して最も多くの攻撃が試みられました。

地域	回数
ヨーロッパ	7,234,747,361
APAC	4,925,542,601
北アメリカ	2,778,360,051
南アメリカ	226,320,069
アフリカ	146,865,982
中東	137,494,862
中央アメリカ	127,354,294
カリブ	7,543,056
南極大陸	16,144

「場所を選ばない仕事」の浸透により、サイバー攻撃の地理的な範囲が広がりました。

デジタル化された新しいワークモデルをサポートするために組織が移行するにつれ、資産とその資産へのアクセスの安全性を確保することがますます重要になっています。さらに、暗号化だけではセキュリティを確保できないことを認識しておくことも重要です。暗号化されたチャネルは、暗号化されていないチャネルと同様に、敵に頻繁に使用されます。

基本事項：**トラフィック全てを検査する**

従来のツールでは、完全な検査を行うにはコストがかかり、パフォーマンスも低下してしまいます。また、データタイプごとに異なるポリシーを要求する規制も、この作業を困難なものにしています。幸いなことに、システムのパフォーマンスに悪影響を与えたり、コンプライアンス上の悪夢を引き起こしたりすることなく、大規模に暗号化されたトラフィックを検査することができる、実践証明された戦略があります。具体的には次を推奨します。

- すべてのユーザのすべてのトラフィックを検査できるクラウドネイティブなプロキシベースのアーキテクチャにより、HTTPSトラフィックの全脅威を解読、検出、防止。
- ファイアウォールベースのパススルーアプローチとは異なり、疑わしいコンテンツを分析のために保持するAIドリブンのサンドボックスにより、未知の攻撃を隔離し、マルウェアによるPatient Zero（最初の感染）を阻止。
- すべてのユーザ、すべての場所に一貫したセキュリティを提供することで、自宅、本社、外出先など、誰もが常に同じ最高のセキュリティを利用できるようにする。
- 水平移動ができないゼロトラストの状態からスタートすることで、攻撃対象領域を瞬時に減らす。アプリが攻撃者に公開されることはなく、ネットワーク全体ではなく、必要なリソースへのダイレクトアクセスが、認証されたユーザに許可されます。

このソリューションには、ゼットスケーラーのZero Trust Exchange™のようなクラウドネイティブなプロキシベースのアーキテクチャでしか実現できないスケーラビリティとパフォーマンスが必要です。クラウドベースのセキュリティプラットフォームは、コンピューティングリソースを弾力的に拡張することで、復号化と検査の要求に応え、複数の場所で一貫したポリシーの施行を可能にします。企業を確実に保護するためには、攻撃対象を減らし、隠れた脅威を発見するための HTTPS 検査を完全にサポートする、多層的で徹底した防御戦略が不可欠です。

暗号化された脅威を阻止する最善の方法は、全体的なゼロトラストセキュリティ戦略の一環として、暗号化されたトラフィックを検査することです。

ゼットスケーラーのZERO TRUST EXCHANGEは、暗号化された脅威をどのように防止するのか

ゼロトラスト戦略とアーキテクチャは、急速に進化するサイバー攻撃から組織を守るための最も効果的な手段です。ゼロトラストとは、どの時点でも実際に攻撃を受けていること、そしてインフラがすでに侵入されていることを想定するものです。想定した攻撃が成功しないように、この想定に基づいてセキュリティ管理を行います。

最も進んだ攻撃には、3つの異なるステージがあります。攻撃は、インターネットに接続されたエンドポイントや資産を最初に侵害することから始まります。侵入した攻撃者は、横方向に伝播し、偵察を行い、ネットワークの足場を確立します。最後に、攻撃は目的を達成するために行動を起こしますが、その目的には通常、データ盗用が含まれます。ゼットスケーラーのZero Trust Exchangeは、これらの3つの攻撃段階のそれぞれにおいて、複数のセキュリティコントロールを提供することで、総合的にリスクを低減します。

侵入の防止

攻撃対象領域を最小化し、すべてのトラフィックを検査することで、ユーザ、サーバ、ワークロード、IoT/OTを保護します。

水平移動の防止

攻撃者がネットワーク上を移動し価値の高いターゲットを見つけることを阻止します。

情報窃盗を防ぐ

インターネットに接続されているすべてのデータを検査し、インターネットへのデータ流出や管理されていないデバイスの悪用を防ぎます。

最初の情報漏洩: 最初のアクセスを停止するためのステップは、エコシステムへのエントリポイントの数を減らすことです。攻撃対象領域を監査し、セキュリティパッチを最新の状態に保ち、存在する可能性のある設定ミスを修正します。また、インターネットに直接接続するアプリケーションを削除し、代わりに接続を仲介するクラウドプロキシの背後に配置する必要があります。これにより、攻撃者には1つの入り口と1つの出口のみとなり、監視をすることができます。次に、繰り返し推奨しているように、すべてのトラフィックを検査します。何でも信頼できると思い込まないでください。ゼットスケーラーは、サービスのプラットフォームの一部としてHTTPS検査を大規模に行います。トラフィックが増加すると、容量は即座にオンデマンドで追加されます。アプライアンスの導入検討や注文、出荷の必要はありません。

水平方向への移動: ゼロトラストでは、「信頼されたネットワーク」というものは存在しません。どのアプリケーションにアクセスしている人も敵対的であると仮定するため、その人が引き起こすダメージを制限する必要があります。マイクロセグメンテーションを使用して、認証されたユーザであってもアクセスを制限します。ゼットスケーラーのゼロトラストアクセスソリューションであるZscaler Private Access™は、ネットワークを公開することなくユーザを必要なアプリケーションに直接接続し、Zero Trust Exchangeによって仲介・認証された1対1のセグメントを作成します。これは純粋なゼロトラストのセグメント化であり、従来のテクノロジで使用されているルールベースのネットワークセグメント化よりも複雑さがはるかに少ないものです。また、ゼットスケーラーでは、戦略的に配置された「おとり」で攻撃者をおびき寄せ、攻撃者が横方向に移動しようとしたり、偵察を行おうとするとセキュリティチームに警告するデセプション技術を採用しています。

コマンド&コントロール (C&C) のコールバック: マルウェアがインストールされると、通常、コマンド&コントロール (C&C) サーバとの接触を試みます。この接触により、攻撃者はマシンを乗っ取ったり、追加のコマンドを発行したり、追加のマルウェアをダウンロードしたり、データを盗んだりすることができます。このような通信を遮断し、機密データを保護するためには、northbound (発信) トラフィックの検査は、southbound (着信) トラフィックと同様に重要です。ゼットスケーラーは、暗号化されたデータを双方向で検査し、悪意のある送信トラフィックを特定して停止させる洗練されたデータ損失保護機能を展開します。

ゼットスケーラーのZero Trust Exchange は、攻撃の一連の流れを止め、インラインの脅威検査、サンドボックス、データ損失防止、および幅広い追加の防御機能を備えたマルチレイヤのアプローチを用いて、大規模な HTTPS検査を実施します。さらに、ゼットスケーラーのクラウド効果により、グローバルプラットフォーム全体で特定されたすべての脅威は、ゼットスケーラーのすべてのお客様の保護機能を自動的に更新します。そのため、世界中のお客様からの情報に基づいて、セキュリティ体制が常に改善されています。世界最大のセキュリティクラウドであるゼットスケーラーのZero Trust Exchangeは、コンテキストベースのIDとポリシーの適用を使用して、場所に関係なく、ユーザーとアプリケーションによるビジネスのトランスフォーメーションを加速します。

次は、ThreatLabzが2021年に見て取ることができた、TLSを活用した新しく普及しているマルウェアファミリです。

njRAT

TLSを介したダウンロードで355,753回のブロックが観測されました。

まとめ

njRATは、Bladabindiとも呼ばれ、.Netフレームワークで記述されたリモートアクセスのトロイの木馬 (RAT) であり、感染したシステムを完全に制御しつつリモートの攻撃者にさまざまな機能を提供するものです。ユーザのキーボード操作を記録したり、侵入したマシンからデータを盗んだり、リモートサーバにデータを流出させたりすることができます。初めて観測されたのは2013年6月でした。

検出を回避するために、マルウェアは、次のような技術の一部または全部を使用することができます。

1. ConfuserXなどの既知のパッカーを使った難読化。
2. 仮想化防止：次の存在を確認する：vboxservice.exe、vboxtray.exe、vmtoosd.exe、SDBIE.DLL、など。
3. 分析ツールのチェック：次のプロセスチェックをする：processviewer.exe、processhacker.exe、など。

配布戦略

攻撃者は、電子メールやWebの攻撃ベクターなど、さまざまな戦略を用いてnjRATを実際に配布しています。一般的な攻撃ベクターとしては、次のようなものがあります。

- LordEKやRigEKなどのエクスプロイトキットを使用する。
- マクロベースのMS Officeファイルを、電子メールの添付ファイルとして送信する、またはURLでホストする。

パーシステンス

パーシステンスを確保するために、マルウェアは次のメカニズムのいずれかまたは両方を使用することができます。

1. 自動実行のレジストリエントリをHKCUSoftware®Microsoft®Windows®CurrentVersion®Runまたは HKCUSoftware®Microsoft®Windows®CurrentVersion®RunOnceに作成する。
2. 自身をスタートアップフォルダにコピーする

ネットワーク

njRATは、コマンド &コントロール (C&C) サーバに対してダイナミック DNSを利用し、構成可能なポートを介してカスタム TCPプロトコルを使用して通信します。njRAT v2.0では、HTTPSプロトコル上で機能するペイロードをドロップするためにcdn.discordapp.comを使用していることが最近確認されています。同じくHTTPSを使用しているFilebin.netも、クラックされたゲームを装うために使用されています。

Smoke Loader

ThreatLabzは、TLS経由のダウンロードで4,269回のブロック、コールバックで3,237,276回のブロックを記録しました。

まとめ

Smoke Loaderは、2011年にロシアのサイバー犯罪闇組織から最初に出現しました。今年、Smoke Loaderは10年目になり、現在も活動を続けています。Smoke Loaderは、追加のマルウェアをダウンロードして実行するためのダウンローダとして広く使用されています。Smoke Loaderは、ボットとPHPベースのC&Cパネル、およびユーザーマニュアルが付属する犯罪キットです。このマルウェアはダークウェブで販売されることが多く、完全なマルウェアパッケージが1,650ドルで販売されています。

回避技術

Smoke Loaderは、多くの場合プロセスリストを繰り返し処理して注入するプロセスを見つけ、プロパゲート注入メソッドを使用してexplorer.exeに注入します。また、複数のアンチVMトリックで武器化されています。たとえば、実行可能ファイルのパスに文字列 [A-F0-9] {4} .vmtが含まれているかどうかを確認し、実行中のすべてのプロセスを確認して次のような文字列を検索します。qemu-ga.exeqga.exe、windanr.exe、vboxservice.exe、vboxtray.exe、vmtoosd.exe、pr_toos.exe、vbox、およびvmmemc。 そしてどれかを見つけた場合、バイナリは終了します。 また、次の実行中のプロセス名も検索します：procmon.exe、ProcessHacker.exe、Wireshark.exe、などその他多数。そしてこれらのプロセスの1つが見つかると、バイナリが終了します。

パーシステンスメカニズム

これは、コンピュータ名、ハードコードされた静的な番号 (キャンペーンによって異なる)、システムドライブのボリュームシリアル番号の連結に基づいて、被害者のマシンごとに一意のIDを生成します。次に、IDは連結された文字列のMD5 ハッシュとして生成され、ボリュームシリアル番号のMD5が再度追加されます。マルウェアは、この一意のIDをいくつかの目的で使用しますが、具体的には2つのドロップされたファイルのランダムなファイル名を作成します。1つ目はSmoke Loaderの実行可能ファイルのコピーであり、2つ目はスタートアップフォルダに作成されスケジュールされたタスクとして起動されるlnkファイルです。

ネットワーク通信

C& Cドメインは、単純なXOR操作を使用して暗号化されます。次に、Smoke Loaderは、POSTリクエストをC& Cサーバに送信します。ペイロードは、RC4を使用して送信前に暗号化されます。POSTリクエストは「404 Not Found」レスポンスを返しますが、レスポンスの本文にペイロードが含まれています。Smoke Loaderは、いくつかの異なるマルウェアファミリで人気のあるダウンローダで、pastebin.comでホストされているAvemariaなどのマルウェアのダウンロードが確認されています。これは、HTTPSを介して機能します。また、HTTPSを使用する他のドロップ型マルウェアでも同様の通信が確認されています。

QakBot

TLSを介したダウンロードで30,199回のブロックが観測されました。

まとめ

QakBotは、QbotまたはPinkslipbotとも呼ばれるバンキング型トロイの木馬であり、2007年から活動を続けています。その主な目的は、銀行の認証情報を盗むことです。スパムメールによって配布され、悪意のある添付ファイルをダウンロードしたり、悪意のあるリンクをクリックしたりするようにユーザを誘導します。ダウンロードされたドキュメントまたはスクリプトファイルは、感染したシステムのメインのQakbotペイロードをさらにダウンロードします。一部の事例では、エクスプロイトキットを通じて配布され、TrickBotなどの他のマルウェアによってダウンロードされています。経時的に開発され、クレジットカード番号、社会保障番号、電子メールアドレス、キーストロークだけでなく、認証情報を盗むWebインジェクション技術などの機能が追加されていて、バックドア機能も備えています。

パーシステンスメカニズム

QakBotは、自動起動場所にRUNキーを作成し、ログインするたびにマルウェアを実行することでパーシステンスを確立します。また、午前5時33分にペイロードを1回実行するようにスケジュールされたタスクを作成すると、実行後にスケジュールされたタスクを削除します。

```
HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run\{Random}
C:\Windows\SysWOW64\schtasks.exe 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn {Random}/tr '\'% AppData%\Roaming\Microsoft\{Random}\{Random.exe}\' /I {Random}' /SC ONCE /Z /ST 05:33 /ET 05:45
```

ネットワーク通信

キャンペーンの中には、JavaScriptが更新された QakBotを、ebook[.]w3wvg.com/datacollectionservice.php3からダウンロードして実行するものがあります。ダウンロードしているペイロードは暗号化されて、スクリプトはそれを復号してからシステムにドロップし、次の情報を被害者のマシンから盗みます。

- IPアドレス
- ホスト名
- ユーザ名
- OSバージョン
- 銀行の認証情報

WebInjectを使用して、被害者のマシンと銀行のWebサイト間の通信を改ざんし、認証情報を盗みます。次のスクリーンショットに示すように、トランスポート層セキュリティを介してコマンド &コントロールサーバと通信するために、QakBotは、Secure Sockets Layerの代わりにTLSハンドシェイクを使用しています。

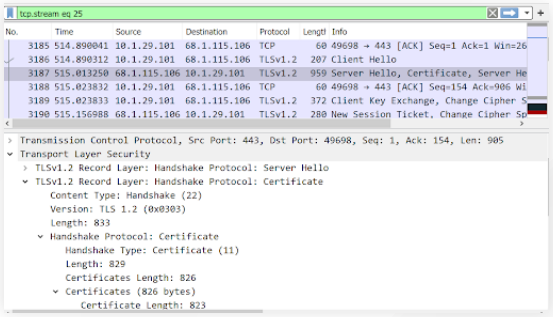

図 10：QakBot が TLS ハンドシェイクを使用する場合

Solarmarker

まとめ

Solarmarker / Jupyter Infostealer / Yellow Cockatoo / Polazertとして知られるマルウェアは、高度にモジュール化された情報収集型ハッキングツールおよびキーロガーです。マルウェアは通常、PDFSamなどの既知の潜在的に望ましくない可能性のあるアプリケーション (PUA) をパッケージ化し、ほとんどの場合、Innopackを使用して正規のプログラムファイルとしてパッケージ化します。Solarmarker感染は、通常、被害者にインターネットからファイルをダウンロードさせるための誘惑として使用される古い手法であるSEOポイズニングを使用して実行されます。マルウェアパッケージのダウンロードはHTTPS経由で行われます。

回避技術

このマルウェアは、MSIやInnopackなどのインストーラを使用して配布されます。これは、初期ベクトルのサイズを50 MBより大きくするために行われます。これは、一部のマルウェアリポジトリやサンドボックスの送信サイズよりも大きくなります。MSIは、エンドポイント検出やウイルス対策ソリューションを回避するためにも使用されます。というのは、PowerShellを実行しているMSIは、PowerShellスクリプトを実行しているEXEよりも不審度が低いためです。

パーシステンスメカニズム

最近のキャンペーンでは、マルウェアはユーザーのスタートメニュー \プログラム \スタートアップディレクトリにある.lnkファイルをドロップします。.lnkファイルがこのディレクトリに配置されると、起動時に実行され、バックドアが起動します。

ネットワーク通信

SolarmarkerはTLSプロトコルを使用して提供され、SEOポイズニングを使用して配布されます。このマルウェアは、通常、他のインストーラと一緒にパッケージ化されているため、そのネットワーク通信は、正規パッカー通信によって多少難読化されています。ほとんどのプログラムはTLSとHTTPSを使用しますが、悪意のある通信はPOSTリクエストを使用してHTTP経由で発生します。IPアドレスはバイナリに存在します。ユーザデータは、次に示すようにJSONを使用して送信されます。

```
"{\"action\":\"ping\",\"",
Deimos.a.a(new char[]
{
    'h',
    'w',
    'i',
    'd'
}),
"\":\"",
A_0.g,
"\",\"pc_name\":\"",
Deimos.a.h(),
Deimos.a.b(),
"\",\"os_name\":\"",
Deimos.a.e(),
Deimos.a.b(),
"\",\"arch\":\"",
Deimos.a.f() ? "x64" : "x86",
Deimos.a.b(),
"\",\"rights\":\"",
Deimos.a.d() ? "Admin" : "User",
Deimos.a.b(),
"\",\"version\":\"",
A_0.a,
"\",\"",
```

図 1: JSON を使って送信されるユーザデータ

BlackMatter

まとめ

BlackMatterは、2021年7月に配信を開始しました。BlackMatterランサムウェアのオペレータは二重恐喝の手法を用いており、身代金が支払われない場合には、被害者から盗んだ機密データをWebサイトで公開することが知られています。BlackMatterは、RaaS (サービスとしてのランサムウェア) を投稿しており、フォーラムに広告を掲載して、侵害された大規模ネットワークへの初期アクセスを提供してくれるブローカーを募集しているのが確認されています。「BlackMatter」の運営者はブローカーにネットワークへのアクセス料を支払っています。BlackMatterランサムウェアは、暗号化プロセスでRSA + Salsa20の組み合わせを使用しています。このランサムウェアは、暗号化した後のファイルに「.{ランダムな英数字 }」拡張子を追加しています。身代金を要求する文書として「{ランダムな英数字 }.README.txt」を残しています。

回避と難読化

BlackMatterランサムウェアは、システムの復元を防ぐために、被害者のマシン上のシャドウコピーを削除します。ランサムウェアがより多くのファイルを暗号化できるように、Outlook、Oracle、Notepadなどの生産性に関連するプロセスを終了させます。また、実行後はCOMインターフェイスを介して特権の昇格もさせます。文字列の難読化と動的なWin32API解決手法を使用しています。

ネットワーク通信

BlackMatterは、ボットバージョン、ボット ID、ホスト名、ユーザ名、ディスク情報、オペレーティングシステム、システムアーキテクチャ、暗号化されたファイル情報などの情報を収集します。次のスクリーンショットに示すように、HTTPSを介して通信し、暗号化にTLSを使用します。ペイロードがHTTPSとの通信に失敗した場合、HTTPを使用してコマンド&コントロールサーバと通信します。

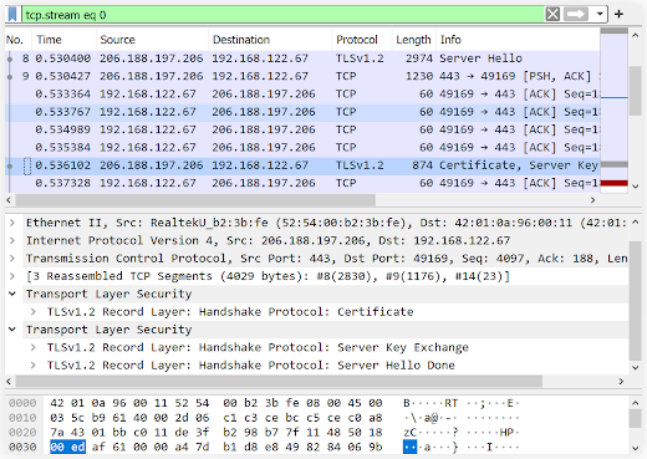

図 12：BlackMatterは暗号化にTLSを使用

REvil/Sodinokibi

まとめ

Sodinokibiとしても知られるREvilランサムウェアは、2019年4月に最初に発見され、スパムメール、エクスプロイトキット、および侵害されたRDPアカウントを通じて配布されました。 Sodinokibiは、Oracle WebLogicの脆弱性も頻繁に悪用します。Sodinokibiは全てのファイルを暗号化し、拡張子に「.{ランダムな英数字 }」を付けています。暗号化の過程では、Salsa20とECDHベースの鍵交換アルゴリズムの組み合わせを使用します。身代金を要求する文書として「{ランダムな英数字 }-readme.txt」を残し、感染したシステムの壁紙を変更します。

回避と難読化

REvilは、UACバイパス技術を使用して、現在のプロセスのコンテキストで昇格された特権を持つ機能を実行する機能を備えています。REvilは、また、さまざまなWindows APIを使用して、マシンにインストールされているデフォルトのシステム言語を判断し、そのシステム言語が事前に設定されたホワイトリストに存在しない場合にのみ、悪意のある活動を実行します。このような言語チェックは、特定の地理的地域への被害者への感染を防ぐために、ランサムウェア媒体によって実行されることがよくあります。

ネットワーク通信

REvilは、被害者のシステムからユーザ名、ホスト名、ドメイン名、キーボードレイアウト、オペレーティングシステム、ドライブ情報、CPUアーキテクチャ、および暗号キーの詳細を収集し、HTTPSを使用してこの情報をコマンド&コントロールサーバに送信します。ドメインのリストは、ペイロードに埋め込まれた設定に存在します。

Microsoft Office 365

フィッシングコンテンツをホストするために、合法的なホスティングサイトや、glitch.me、CodeSandbox、Cloudflare Workersなどのオンラインコードエディタが悪用されていることが確認されています。これらのサイトは、HTTPSを介してフィッシングページを提供し、迅速なWeb開発に一役買っています。これらのフィッシングサイトのいくつかの例を次に示します。

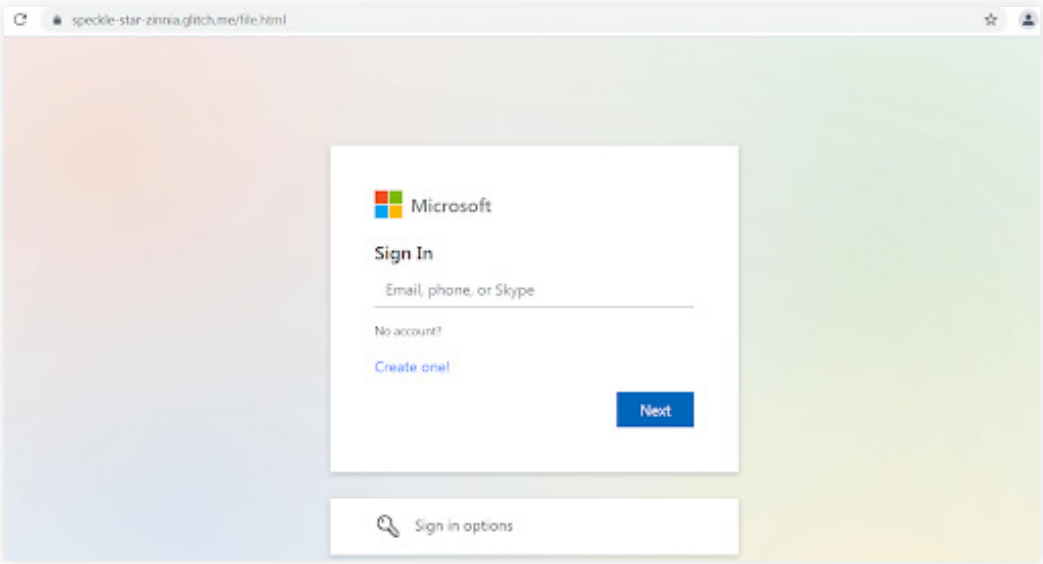

図 13: フィッシングサイトの例

これらのフィッシングページは、多層難読化を使用しており、ソースコードの一部は、JavaScript難読化ツールとBase64 エンコーディングを組み合わせて難読化されています。

図 14: 多層難読化の例

多層難読化の別の例を次に示します。

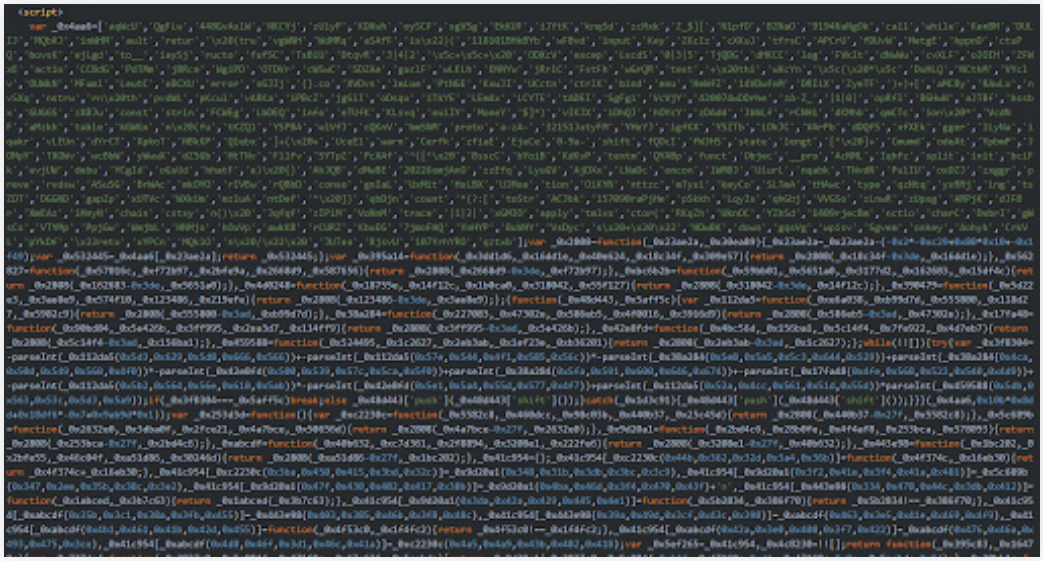

図 15: 多層難読化の例

これらのフィッシングサイトは、IPアドレスのフィンガープリントも作成し、そのIPが、次に示すスクリーンショットに示されている企業一覧に属している場合は、Microsoftの正規サイトにリダイレクトします。

```
$.ajax({
        type: "GET",
        url:'https://pro.ip-api.com/json/?key=tPiZVEq18Ne6eQ1&fields=66846719',
        dataType: "json",
        success: function (res) {
        var e833200 = res.as + " " + res.asname + " " + res.isp;
          if (
          e833200.toLowerCase().indexOf("phish".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Paypal".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("namecheap".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Google".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Amazon".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("M247".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("AVAST".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Kaspersky".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("BullGuard".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Wintek Corporation".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("McAfee".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("commodo".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bitdefender".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Contina".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Symantec".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("fireeye".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("NetCraft".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("YandexBot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("barracuda".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mimecast".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("appriver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("proofpoint".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlscan".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlredirectresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bingbot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("trendmicro".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("spam".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("crawler".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mozilla".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("msnbot".toLowerCase()) >= 0
```

図 16: 企業一覧

Amazon

HTTPSを介したAmazonフィッシングの事例が確認されています。その一例を、次のスクリーンショットでご紹介します。配信地域が米国にあらかじめ設定されていることがわかります。これにより、このフィッシングキャンペーンのターゲットに関する見識が得られます。

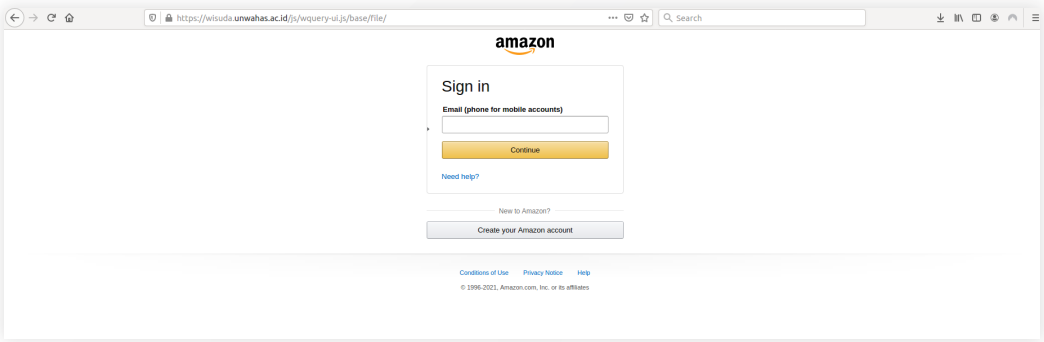

図 17: HTTPS を介したAmazonフィッシングのインスタンス

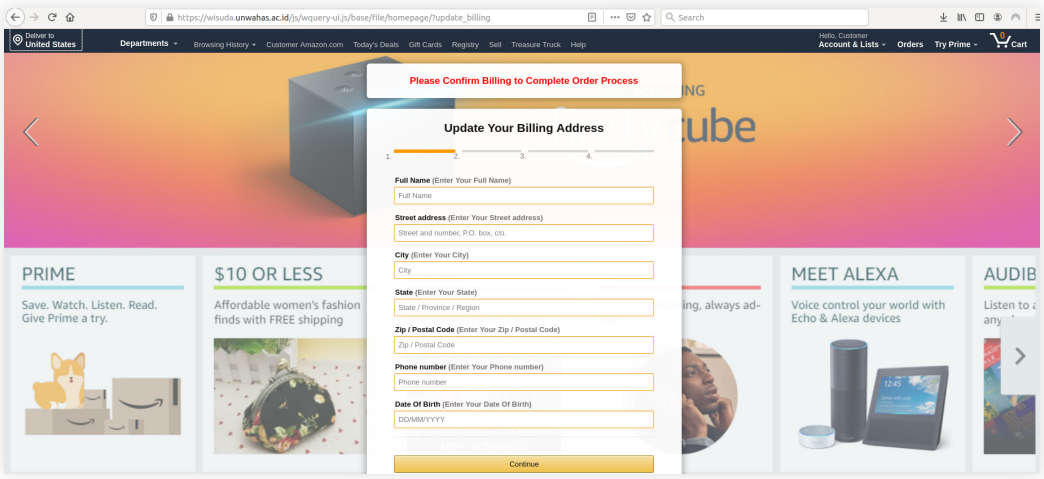

図 18: HTTPS を介した Amazonフィッシングのインスタンス

次に示すのは、Amazonフィッシングホスティング Webサイトの場所にある、攻撃者が改ざんしたページです。

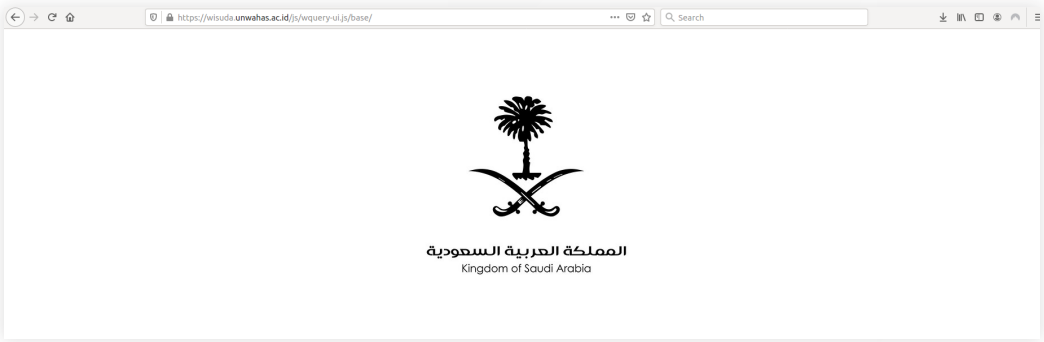

図 19: 攻撃者が改ざんしたページ

OneDrive

攻撃者がHTTPS経由でOneDriveフィッシングページを提供しているのを確認しました。これらは、フィッシングコンテンツを掲載している危険なウェブサイトから提供されていました。ソースコードは基本的な16進数でエンコードされており、フィッシングコンテンツのスキャナーによる検出を免れています。

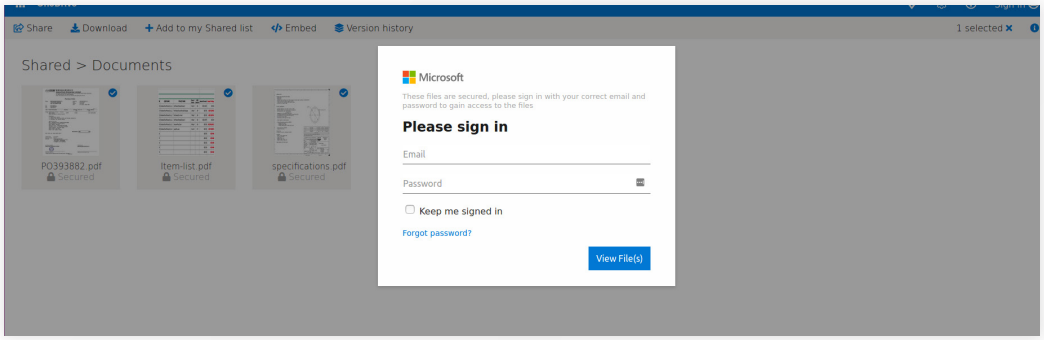

図 20: HTTPSでのOneDriveフィッシングのインスタンス

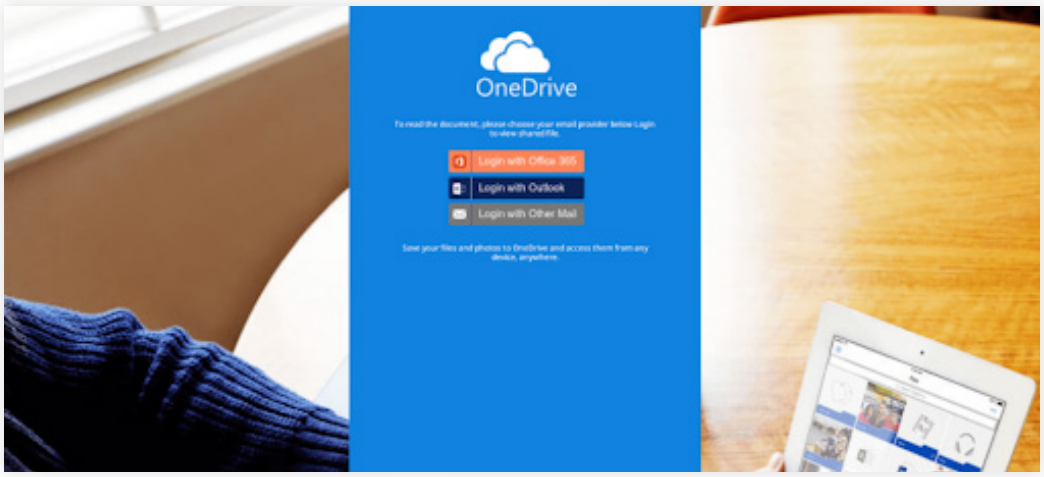

図 20: HTTPSでの OneDriveフィッシングのインスタンス

図 22: ソースコードのコード化された部分

Telegram

非公式のTelegramウェブクライアントがHTTPSを使用している例が見られています。これらのWebクライアントは、セキュリティを保証するものではありません。これらのフィッシングページは、ユーザの電話番号を要求し、ユーザの電話番号にワンタイムパスワードを送信します。ユーザが非公式サイトでワンタイムパスワードを入力すると、Webクライアントは、TelegramのAPIを使ってユーザのコンテンツを取得し、ユーザに提供します。それを実行している間、ユーザのメッセージ、連絡先リスト、その他の詳細情報が悪意のあるWebクライアントによってどのように使用されるかについては保証されません。そのようなWebサイトの例を次に示します。

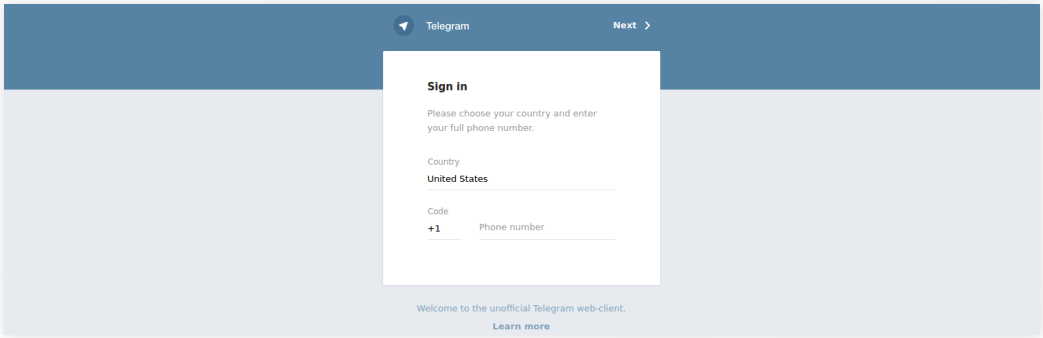

図 23: HTTPSを使用した非公式Telegram Webクライアントのインスタンス

Telegramの創始者は、セキュリティを確保するためにTelegramの公式アプリの使用を推奨していました。

図 24: HTTPSでのOneDriveフィッシングのインスタンス

PayPal

HTTPSを利用したPayPalのフィッシング活動を確認しました。次の例では、あるショッピングサイトで、PayPalによる支払い方法が被害に遭っています。

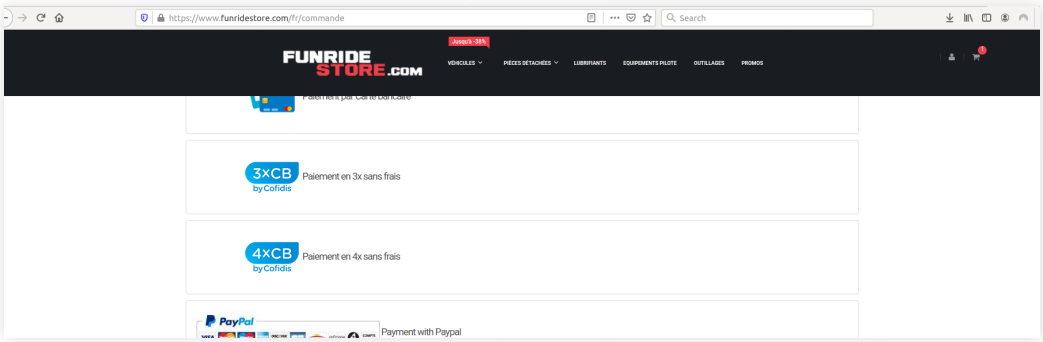

図 25: HTTPSでのPayPalフィッシング活動のインスタンス

ユーザがショッピングカートに商品を追加すると、配送と連絡先情報のリクエストがされます。詳細を入力すると、ユーザーにはさまざまな支払いオプションが提供されます。ここに表示されているPayPal支払いリンクは危険にさらされています。ユーザーがPayPalオプションを選択すると、次に示すフィッシングページに移動します。

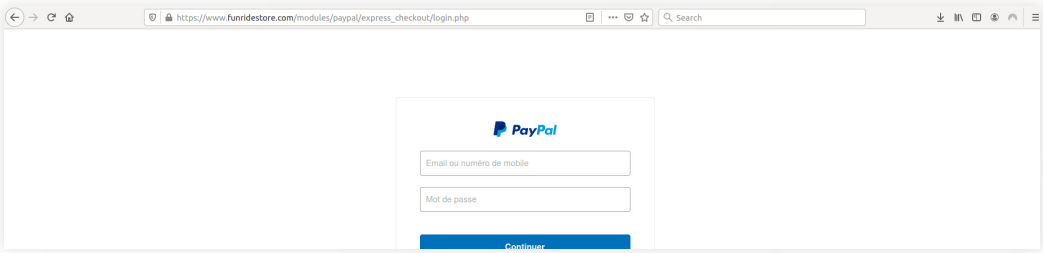

図 26: PayPalのフィッシングページ

PayPalの認証情報が入力されると、ユーザは正規のPayPal URLにリダイレクトされ、そこでログインして購入を完了することができます。

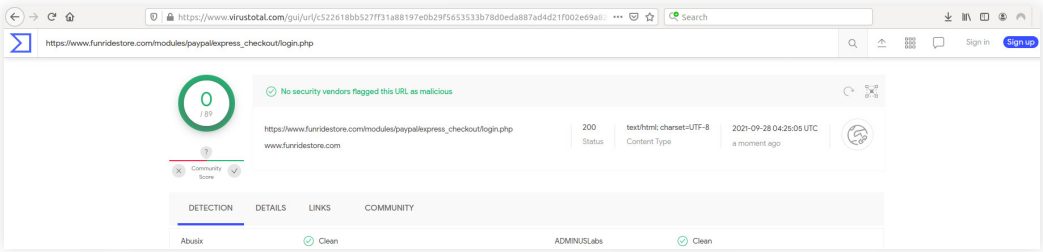

図 27: PayPalのフィッシングページ

この例は、ソーシャルエンジニアリングの興味深い例です。このページでは、正規のショッピングページと、お客様が正規のリンクを期待するであろう場所にPayPalのフィッシングリンクが配置されています。クレジットカードの支払いリンクは正規のURLを指していますが、PayPalリンクのみが侵害されています。

標的型攻撃の実行者は、Cobalt Strike、Mimikatz、LaZagneなどのツールを使用して、水平方向の伝播、データの漏えい、その他のC& C活動を実行するのが一般的です。Cobalt Strikeは、このような標的型攻撃の多くで最も一般的に使用されているツールの1つです。

Cobalt Strike

ダウンロード用に24,410回のブロック、TLSを介したコールバック用に172,568回のブロックが観測されました。

まとめ

Cobalt Strikeは、敵のシミュレーションとレッドチームの運用のための商用ツールです。これは、事前に定義された設定可能なコマンド&コントロール (C&C) プロファイルを備えたフル機能のソフトウェアで、その振る舞いやネットワーク指標を変更して、実際の攻撃で使用されるさまざまなマルウェアファミリーの戦術、技術、手順 (TTP) をシミュレートすることができます。これは正当な商用ツールですが、実際の攻撃では敵によって繰り返し使用されています。次のようなさまざまなAPTグループが、Cobalt Strikeフレームワークを使用することが知られています。

- APT19
- DarkHydrus
- CopyKittens
- APT32
- Cobalt Group
- APT29
- Leviathan
- FIN6

Cobalt Strikeはファイルレスマルウェアであり、複数の目的に使用できる多段階シェルコードをサポートしています。

ネットワーク通信

Cobalt Strikeは、影響されやすいC& Cプロファイルと呼ばれる機能を使用して、1つまたは複数のプロトコルを介して通信するように設定できます。

- DNS (TXT、A、AAAAレコード)
- HTTP/HTTPS
- SMB (名前付きパイプ)
- TCP

回避技術

Cobalt Strikeは、プロセス間またはホスト間での通信を可能にするソケットである名前付きパイプも使用する最終段階のペイロードとしてドロップされることがよくあります。Cobalt Strikeでの攻撃後に使用される機能としては、キーロガー、Mimikatz、スクリーンショットモジュールなどがあります。

盗まれた認証情報を使用する横方向の動き

Cobalt Strikeは、盗んだ認証情報を使って、SMB (Server Message Block) を使用しているリモートネットワーク共有へのアクセス、RDP (Remote Desktop Protocol) を使っているコンピュータへのログイン、Telnet、SSH、VNCなどのリモート接続を受け付けるために特別に設計されたサービスへのログインなどを行っています。

PoshC2

TLSを介したコールバックで98,591回のブロックが観測されました。

PoshC2は、レッドチーム、ポストエクスプロイト、および横方向の動きで侵入テスターを支援するために使用されるプロキシ対応のC& Cフレームワークです。

PoshC2は主 にPython3で書 かれています。 すぐに使 用 できるPoshC2には、 PowerShell v2およびv4、C ++およびC#ソースコードで記述されたペイロードを備えたPowerShell/C#およびPython2/ Python3のインプラントが付属しています。これらにより、Windows、* nix、OSXなどのさまざまなデバイスやオペレーティングシステムでC& C機能が有効になります。

PoshC2は、 SharpSocksで使用できます。これにより、 C#リバース HTTPSトンネリング Socksプロキシが可能になり、 C& CトラフィックをHTTPS経由で実行できるようになります。

Ursnif

ダウンロード用に336,540回のブロック、 TLSを介したコールバック用に87,821回のブロックが観測されました。

まとめ

Ursnif (Goziとも呼ばれます) はバンキング型トロイの木馬ですが、バックドア、スパイウェア、ファイルインジェクタなどのコンポーネントを含む亜種があります。初めて存在が確認されたのは2006年で、以降継続的に稼働しています。このマルウェアは、国別のフィッシングキャンペーンを使用して配布されます。

パーシステンスメカニズム

Ursnifは、 2つのメカニズムを使用してパーシステンスを作成します。

1. 新しいスケジュールタスクを作成します (名前は「Power<random_word>」(例：PowerSgs))
2. 何らかの理由でこれが失敗した場合は、「HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run」レジストリキーを使用して、システムの再起動時にもパーシステンスを維持できるようにします。

ネットワーク活動

マシン上に足場を確立すると、メインのワーカースレッドを開始し、C& Cサーバでコマンドを継続的にポーリングします。このマルウェアは、「ユーザ」、「サーバ」、「ID」などのユーザ情報をハッシュ値として収集します。「稼働時間」は、デバイスの実行時間の時間値です。「DNS」はコンピュータ名、「whoami」は完全なユーザ名です。マルウェアは、 HTTPSを使用して、 C& Cに連絡し、情報を中継している場合があります。

Dridex

ダウンロード用に50,088回のブロック、TLSを介したコールバック用に11,167回のブロックが観測されました。

まとめ

BugatおよびCridexとしても知られるDridexは、銀行の認証情報を盗むことを専門とするトロイの木馬です。2011年に初めて登場し、何年にもわたって進化し、Microsoft WordやExcelドキュメントをペイロードとして使用するいくつかのフィッシングキャンペーンで取り上げられました。

回避技術

Dridexは、CutwailボットネットまたはRIGエクスプロイトキットによって配布されます。Dridexは、たとえばSpaceXの打ち上げなど、現在の社会情勢に基づいたフィッシングキャンペーンを使用することでも知られています。

ネットワーク通信

Dridexドキュメントペイロードには、次の段階のC&Cが含まれています。HTTPSを使用してC&Cに接続し、ダイナミックリンクライブラリ (DLL) ファイルをダウンロードします。これは、ユーザに感染し、さらにC&Cに接続するという最終的なペイロードです。Dridexの亜種は、最近のキャンペーンではDoppelDridexとも呼ばれ、cdn.discordapp.comとSlackをC&Cとして使用し始めており、DLLファイルが含まれています。

Zscalerがパフォーマンスに影響を与えたり、コンプライアンスの懸念を引き起こしたりすることなく、すべての SSLトラフィックを検査する方法を確認してください。 また、**インターネット脅威エクスポージャ分析ツール**を使用してSSL/TLSトラフィックを検査する機能をチェックすることもできます。

ThreatLabZについて

ThreatLabZは、Zscalerのセキュリティ研究部門です。このワールドクラスのチームは新しい脅威を発見し、グローバルなZscalerプラットフォームを使用する何千もの組織が常に保護されていることを保証する責任があります。マルウェアの研究や行動分析に加えて、チームメンバーは、Zscalerプラットフォームの高度な脅威対策のための新しいプロトタイプモジュールの研究開発に携わり、Zscalerの製品やインフラがセキュリティコンプライアンス基準を満たしていることを確認するための内部セキュリティ監査を定期的に実施しています。ThreatLabZは、新たに出現した脅威の詳細な分析結果をポータル（**research.zscaler.com**）で公開しています。

Zscalerについて

Zscaler (NASDAQ：ZS) は、デジタルトランスフォーメーションを加速させ、敏捷性、効率性、耐障害性、安全性の向上を可能にします。ゼットスケーラーのZero Trust Exchange™ は、あらゆる場所のユーザ、デバイス、アプリケーションを安全に接続することで、サイバー攻撃やデータ損失から何千ものお客様を保護しています。SASEベースのZero Trust Exchangeは、世界中の150以上のデータセンタに分散する、世界最大のインラインクラウドセキュリティプラットフォームです。詳細は、zscaler.comをご覧いただくか、**Twitter @zscaler**をフォローしてください。