SOPHOS
Cybersecurity delivered.

ソフォス脅威レポート 2023 年版

サイバー犯罪者向けのマーケットの成熟が、防御側の組織に新たな課題を突き付ける

提供：Sophos X-Ops

目次

Joe Levy からのメッセージ 2

ウクライナ戦争によるサイバー環境の変化 4
- 地域紛争が世界に波及する 4
- ウクライナ国内の状況 5

マルウェアを中心とした経済圏 6
- 9 つのサービスとしてのサイバー犯罪 6
- テキストベースの広告からグラフィックを多用した広告への進化 11
- 情報窃取マルウェア 13

ランサムウェアの進化 17

攻撃ツール 20

オフェンシブセキュリティツールの悪用 21
- 悪用されているその他のセキュリティツール 24
- RAT の攻撃目的への転用 24
- LOLBin と正規の実行ファイル 25
- 脆弱性の意図的な持ち込み 26
- エンドポイントセキュリティのアップグレードを標的とするランサムウェア 28
- 暗号通貨を採掘するマイニングマルウェア 28

Windows だけが狙われていた時代の終わり：Linux、Mac、モバイルの脅威環境 30
- Linux の脅威 30
- Mac の脅威 32
- モバイルの脅威 33

まとめ 34

Joe Levy
Sophos CTO

Joe Levy からのメッセージ

サイバーセキュリティ業界の人々は、毎年年末になると今年はセキュリティ史上最も重要な一年であったと振り返ることがあります。2022 年は、Aurora、Stuxnet、WannaCry、Colonial Pipeline のような大規模なサイバー攻撃はありませんでしたが、残念ながらヨーロッパでは過去半世紀で最大の戦争が勃発し、サイバーセキュリティの歴史にもこの戦争の影響が刻まれました。

この戦争がサイバーセキュリティに及ぼした影響は甚大でした。サイバー犯罪活動を世界的に助長し、犯罪者の安全な避難場所としてよく知られ、国家的な産業としてランサムウェアビジネスを最初に確立したロシアが、隣国のウクライナに侵攻したからです。

ウクライナへの侵攻に伴って、ロシア政府はサイバー攻撃者を兵役に召集したわけではありませんが、ロシアの大規模なサイバー犯罪組織を強力にバックアップし、世界的な世論をロシアに有利な方向に誘導し、ウクライナの大統領が目指した世界各国との外交成果を妨害しようとしたことは必然でした。ランサムウェア、マルウェア、偽情報を操るサイバー犯罪組織がロシアの侵略を支持するための行動を起こしました。

しかし、それらの努力は、今のところ成果を得ることなく失敗に終わっています。ランサムウェアの犯罪者は、あらゆる国ですでに忌み嫌われていますが、新型コロナウイルスのパンデミックでは、ヘルスケア業界、医療研究機関、サプライチェーンや食料・エネルギー事業の維持に関連する企業、さらには教育システムなど、コロナ渦において重要な役割を果たしていた基幹産業の最も脆弱な部分までも標的にしました。ランサムウェア組織がロシアの侵略に揺るぎない支持を表明し、ロシアに反対する国や組織を攻撃したことから世界中から怒りを買うことになり、これらの組織の評判はさらに地に落ちました。

ウクライナを拠点とするランサムウェア組織が起こした行動は、ロシアの組織とは方向性が異なっていました。ランサムウェア組織の活動に関する最も機密性の高い情報を暴露し合う、リークの応酬が始まったのです。この戦争によって、ウクライナのサイバー犯罪組織とロシアおよびベラルーシの組織の関係性は、おそらく永久に断ち切られることになったと考えられます。

一方、ロシアが侵略戦争を続けていたときに、中国は近隣諸国や「一帯一路」構想において重要とされる国々、そして、セキュリティ業界を標的としてサイバー攻撃を激化させました。情報やネットワークを保護しなければならない企業に対する攻撃はさらに大胆になっています。中国を拠点とし、中国政府の支援を受けていると考えられているサイバー犯罪組織は、サイバーセキュリティおよびインフラストラクチャ業界のほぼすべての企業が製造するハードウェアセキュリティ関連の製品を攻撃しています。

2022 年のサイバー攻撃は、グローブが外され素手で本気で殴り合うような状態になったと私は感じています。世界の多くの国にサイバーセキュリティの脅威をふりまいてきたロシアと中国の 2 つの大国は、大規模なセキュリティ侵害、インフラへの重大な攻撃、教育、グローバル企業、ヘルスケア組織への妨害についてこれまでは自らの関与を隠ぺいすることもありましたが、今では大々的に活動するようになりました。「我々の攻撃に本当に抵抗できるのか？」と言わんばかりに、その攻撃力を誇示するようになっています。

ソフォスがサイバーセキュリティの問題にこれまで取り組んできたこと、そしてこれから取り組んでいくことは、顧客とソフォス自身を守るために、これまでの取り組みを着実に強化していくことです。ソフォスは、ランサムウェアの挙動を検出して自動的に防止するための対策を、長年段階的に改善し、攻撃を防ぐことで、大きな成功を収めてきました。そのため、現在攻撃者は防衛側による検出を回避することにさらに注力するようになりました。

中国やロシアとつながりのあるサイバー犯罪組織によるセキュリティインフラへの攻撃が続いています。そのため、取り引きするベンダーを信頼できることが、これまで以上に重要となっています。特に、サイバーセキュリティに関連するサービスや製品を提供しているベンダーが信頼を獲得し維持するためには、ベンダーがセキュリティに対して何をどのように投資しているのかを明確に伝え、透明性を確保しなければなりません。ソフォスの Trust Center では、アドバイザリーや脅威情報、セキュリティテストの結果、バグ報奨金制度、インシデント分析および対応計画に関するソフォスの取り組みを紹介しています。ソフォスは今後も APT グループによる標的型攻撃からソフォスのインフラを保護し、顧客の環境で稼働するハードウェアとソフトウェアを強靭化するための投資を継続していきます。このアプローチが重要である理由は、攻撃者は常に脆弱性を見つけ出して攻撃に転用しようとしており、実際、あらゆるベンダーのファイアウォール、スイッチ、ネットワークアクセスポイントのセキュリティを崩壊させるための活動を強化しているためです。また、ソフォスは引き続き、デフォルトの設定で安全が確保される「セキュアバイデフォルト」を製品に反映し、ヘルスチェックやポリシー修正などの便利な機能を製品やサービスに導入し、正しい設定でセキュリティ製品を運用し、衛生状態を改善していきます。

脅威が今後も進化し続けることは間違いありません。しかし、ソフォスも脅威の進化に絶え間なく適応し、サイバーセキュリティにおいて優れた成果をもたらし続けます。

ウクライナ戦争によるサイバー環境の変化

クラウゼウィッツがその著書『戦争論』の中で述べているように「戦争とは他の手段をもってする政治の継続」であり、サイバー紛争が戦争の 1 つの形態とするならば、ウクライナ紛争におけるオンラインの戦争も、陸海空での戦争と共通点があることが分かります。本レポートを執筆した時点では、ウクライナ国内における脅威環境は極めて悪化しています。西側世界の他の国ではそれほど脅威は広がっていませんが、広範な紛争、偽情報の拡散、および混乱を引き起こす活動が行われる可能性は依然として高いままです。

地域紛争が世界に波及する

2 月 24 日に発生したロシアによるウクライナへ軍事侵攻に端を発して、予想通り、世界の人々の悲しみと懸念に付け込んで利益を得ようとする詐欺師の活動が活発になりました。

3 月上旬、ソフォスはウクライナを支援するために国際的な寄付を求める偽のチャリティーメールが増加していることを確認しました。戦争が始まった当初、ウクライナ当局は世界に向けて防衛費の寄付を呼びかけており、暗号通貨を国庫に寄付してほしいという要請もありました。詐欺師はすぐに暗号通貨という切り口に飛びつき、何百万通ものスパムメールを一斉に配信しました。このスパムメールでは、暗号通貨のウォレットのアドレスが、政府やその他の正規の慈善団体や非政府系の救援機関とは関係のないアドレスにすり替えられていました。3 月 5 日から 6 日の週末にかけて、このような暗号通貨ウォレットへの偽の寄付を募るスパムメールが大量に発生し、この期間に受信したスパムメールの半分を占めるという衝撃的な検出数を記録しました。幸い、このキャンペーンは数日で沈静化しました。

1 日に検出されるスパム数に占めるウクライナでの詐欺の割合、2022 年 3 月

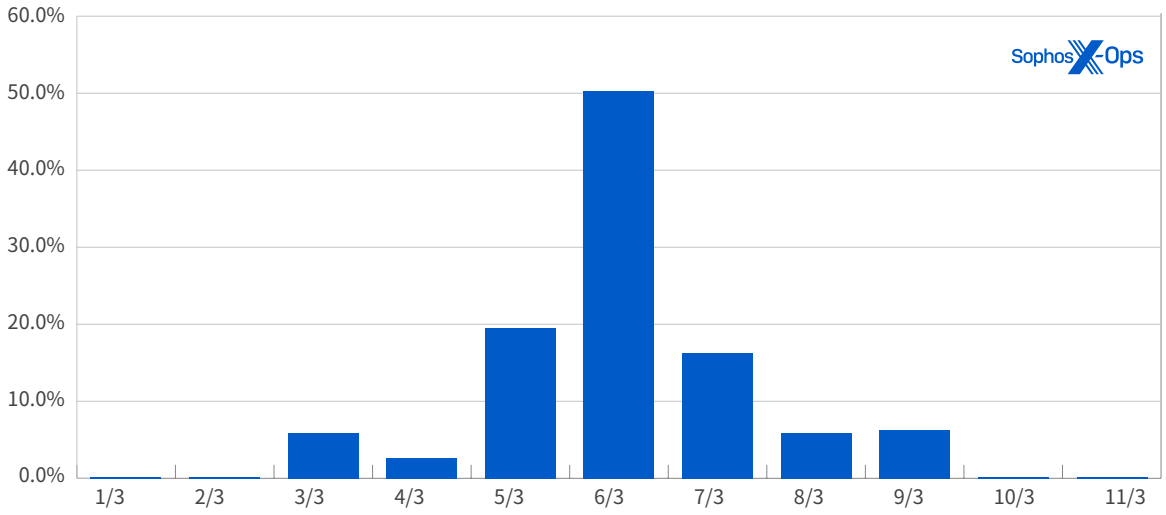

図1. 偽のアドレスへの暗号通貨の寄付を募るスパムメールが一時的に急増した。

5 月までに数百の偽サイトが「寄付」を要求していましたが、最初のスパムメールでは財務情報が共通していたことから、比較的少数の組織によってスパムメールが運用されていた可能性があります。これらの攻撃では、それほど高度な技術は使用されていませんでしたが、国名や影響力の大きな人物の名前を使用するソーシャルエンジニアリングが使用されており、比較的古い脆弱性を悪用する攻撃も見られました。

たとえば、5 月に発生したスパムキャンペーンは注目が必要であり、Emotet マルウェアの組織が、「US and Allies provide chemical weapons to Ukraine's military.doc (米国と同盟国、ウクライナへ化学兵器を供与)」といったロシアのプロパガンダをそのまま使用した挑発的なファイル名を付けた悪意のある Word 文書を配布し、マルウェアを拡散していました。この攻撃で使用された悪意のあるドキュメントは、CVE-2021-40444 の脆弱性を攻撃するエクスプロイトを利用しており、前年の秋に公開された Office パッチをインストールしていないマシンでこのファイルを開いたユーザーのコンピュータを感染させました。

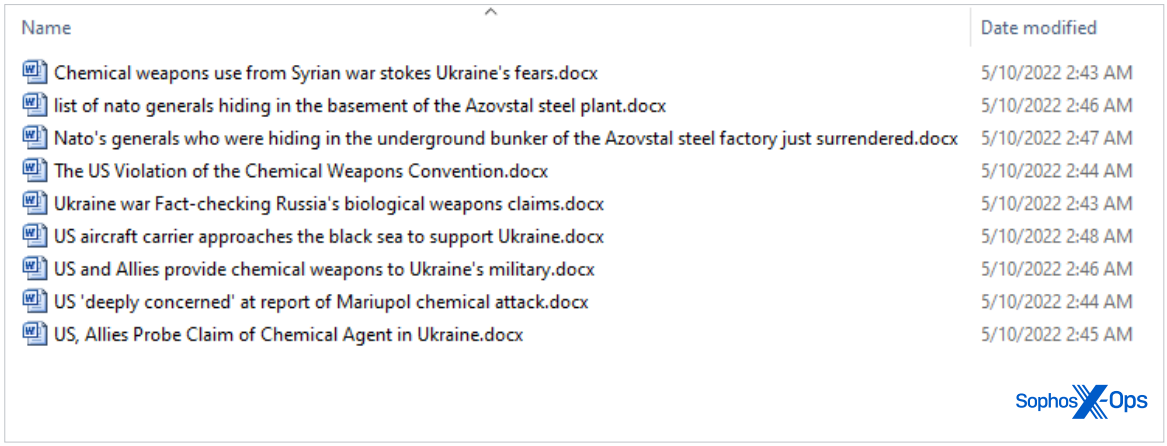

図2. 悪意のある Emotet のスパムメールに添付されていた文書のタイトルでは、ウクライナ戦争を題材とした恐怖を煽る虚偽の主張が使用されていた。

ウクライナ国外での国家レベルのサイバー攻撃については、2 件の重大なインシデントがありました。本レポートの執筆時点では、そのうちの 1 件の攻撃元は不明なままです。衛星通信サービスを提供している ViaSat への攻撃は、ロシアによる侵攻が始まる数時間前に開始され、ウクライナとヨーロッパの顧客向けの衛星サービスに影響を及ぼしました。当局者によると、これはロシアによる攻撃とされています。しかし、10 月に欧米で起きた空港の Web サイトの改ざんについては、攻撃者の特定が困難になっています。これはウクライナの同盟国を威嚇するための国家による仕業だったのか、特定の国家に所属していないサイバー犯罪組織による攻撃だったのかは明らかになっていません。

実際、後者であるかのように振る舞って攻撃した可能性もあります。技術力の低い改ざんや DDoS 攻撃 (空港サイトの改ざんや、ユーロビジョンへの投票を妨害) もこの戦争当初に見られましたが、紛争が長引き再び厳冬期が近づき、世界の緊張が高まる中、親ロシア派のハッカー組織である KillNet によるサイトへの妨害行為が発生したことで、この戦争がまだ何も解決していないことを改めて思い起こさせる結果になりました。

ウクライナ国内の状況

ウクライナ国内は、さらに陰鬱で奇妙な様相を呈しています。ウクライナ政府を標的とするいくつかの攻撃は、ソーシャルエンジニアリングメール、コモディティマルウェア、攻撃に転用可能な商用セキュリティツールの悪用など、多くのサイバー犯罪に見られるパターンを踏襲しています。偽造されたメールに「アンチウイルスアップデート」へのリンクが含まれており、リンクをクリックすると代わりに Cobalt Strike のビーコンがドロップされるケースもありました。また、このレポートの後半で紹介しますが、ウクライナの市民や政府組織に関する大量のデータを販売しており、身代金を要求することはなく、ただデータを公開するために侵入していた攻撃も報告されています。

一方、ウクライナとロシアは異なる国でありながら、両国のサイバー犯罪組織はこれまで長年協力関係を築いており、いくつものランサムウェア組織は両国に拠点を置く提携者を利用してきました。戦争の勃発により、国家主義によっていくつかの組織のこれまでの良好な関係が瓦解したと見られています。

たとえば、ランサムウェア組織のチャットログがダンプされ、Conti グループの内部情報が漏えいしましたが、これは、ランサムウェア組織とその提携者であるロシア人とウクライナ人のメンバー間の分裂によって引き起こされた可能性があります。その後、@TrickbotLeaks というツイッターアカウントが短期間利用され、Trickbot、Conti、Mazo、Diavol、Ryuk、および Wizard Spiders の犯罪組織の一員とされる人物の個人情報やプライベートな情報が晒されました。

漏洩した情報からさまざまな事実が明らかになりました。多くの欧米の研究者が何年も前から指摘してきたように、ロシア連邦保安局 (FSB) が多くのランサムウェア組織と密接に関係していることが証明され、Conti を悪用したいくつかのインシデントについては、これらの組織と契約を締結していた可能性もあることが明らかになりました。

しかし、このような内部闘争は、世界的なランサムウェアの活動を大幅そして長期的に減少させることにはつながりませんでした。2022 年には、ロシア連邦保安局がサービスとしてランサムウェアを提供していたサイバー犯罪組織「REvil」の複数のメンバーを 1 月に、無名のクレジットカード犯罪組織のメンバーを 2 月に逮捕し、さらに、3 月初旬には、REvil のメンバーを裁判のために米国に引き渡しましたが、今年の半ばには、このような犯罪撲滅のための国際的な協力体制がすでに失われ、REvil あるいは REvil l のサービスを提供しているように装っている組織が、すでに復活しています。この戦争の終わりは今も見えないままです。

マルウェアを中心とした経済圏

この 1 年で脅威環境はさまざまな方向に進化しましたが、おそらく最も注意すべきことは、サイバー犯罪者向けのマーケットが発展を続けていることでしょう。このマルウェアを中心とするこのエコシステムは、犯罪を助長するサービスのネットワークや、専門的なマルウェアの運用方法などを提供しており、1 つの産業へと変貌を遂げつつあります。

情報テクノロジー企業が、多くの業務を「XaaS」モデルに移行しているように、サイバー犯罪向けのエコシステムも変化しています。アクセスブローカー、ランサムウェア、情報窃取型マルウェア、マルウェアの配信など、サイバー犯罪を簡単に運用できるようにする製品やサービスが登場し、誰でも簡単にサイバー犯罪者に手を染めることが可能になっています。

この傾向を後押ししている要因の 1 つは、サイバー犯罪のためのマーケットの登場です。Genesis などの犯罪者向けのマーケットでは、高度なスキルを持たないサイバー犯罪者でもマルウェアやマルウェアを配信するサービスを購入し、盗んだ認証情報やその他のデータを大量に販売できます。アクセスブローカーは、脆弱なソフトウェアを悪用するコモディティエクスプロイトを利用して、数百のネットワークに攻撃のための足がかりを築き、他の犯罪者に販売しています。多くの場合、同じ企業へのアクセス情報は繰り返し販売されます。ランサムウェアの提携者や他の攻撃者は、さらにリスクが高く、高額な報酬を得る可能性が高い犯罪を行うために、認証情報やアクセス権限を購入しています。

ランサムウェアが産業化したことで、ランサムウェアの「提携者」による専業化が進み、脆弱性の攻撃に特化した組織も登場しました。専門的なオフェンシブセキュリティのツール、管理やテクニカルサポートのための正規のソフトウェア、サービスとしてのマルウェアが使用され、地下マーケットではさまざまなエクスプロイトやマルウェアが入手できるようになっています。サイバー犯罪者が多くのツール、戦術、手法を利用できるようになっており、これらは特定のランサムウェアのオペレーションや国家によるスパイ活動などの目的に限定されておらず、さまざまな攻撃が展開されています。企業や組織へのアクセス情報を獲得または購入することを専業とする組織が存在し、これらのアクセス情報をさまざまな攻撃のために購入する意欲の高いサイバー犯罪者に売りつけています。

これらの組織は、クラウドや Web サービスビジネスの多くの要素を模倣しています。企業の IT 部門が「XaaS」モデルを採用して業務範囲を拡大しているように、サイバー犯罪で利用されるツールキットの多くの要素も、地下マーケットの Web 掲示板で宣伝されている「サービスとしてのサイバー犯罪」のプロバイダーにアウトソースすることが可能です。以下に、これらのサービスとしてのサイバー犯罪の 9 つの例について簡単に紹介します。

9 つのサービスとしてのサイバー犯罪

サービスとしてのアクセス：リモートデスクトッププロトコル (RDP) や VPN の認証情報、アカウント、データベース、Web シェル、攻撃に利用できる脆弱性など、侵害されたアカウントやシステムにアクセスするための情報が個別にまたはパッケージングされて、地下マーケットでサービスとして販売されています。

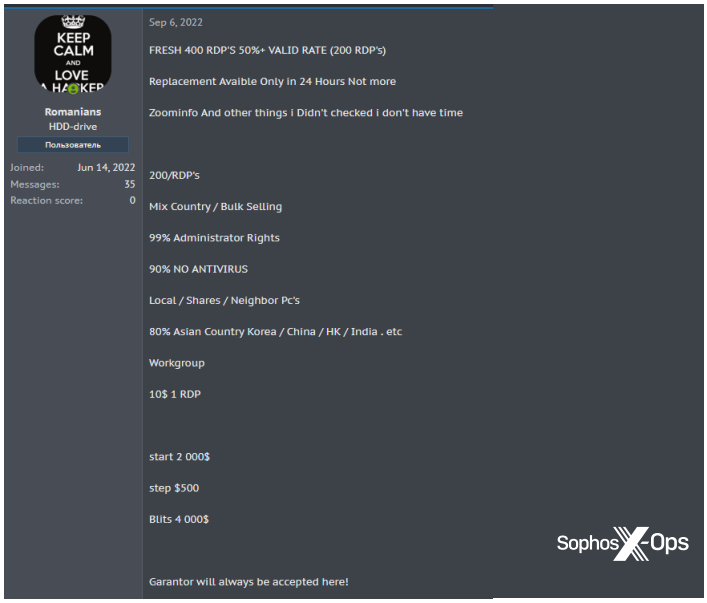

図 3. アクセスブローカーが掲載しているアクセス情報と価格

図 4. オークションに出品された EU 企業のデータ

サービスとしてのマルウェア配信 / 拡散：特定の地域や業界、また、さらに広い範囲にマルウェアを配信するサービスが提供されています。ソフォスが確認しているこれらのサービスの広告では、水飲み場攻撃、脆弱性の攻撃、AaaS (サービスとしてのアクセス) リストと組み合わせた攻撃手法などが掲載されていましたが、これらの攻撃が実際にどこでどのように実行されているのかは不明です。

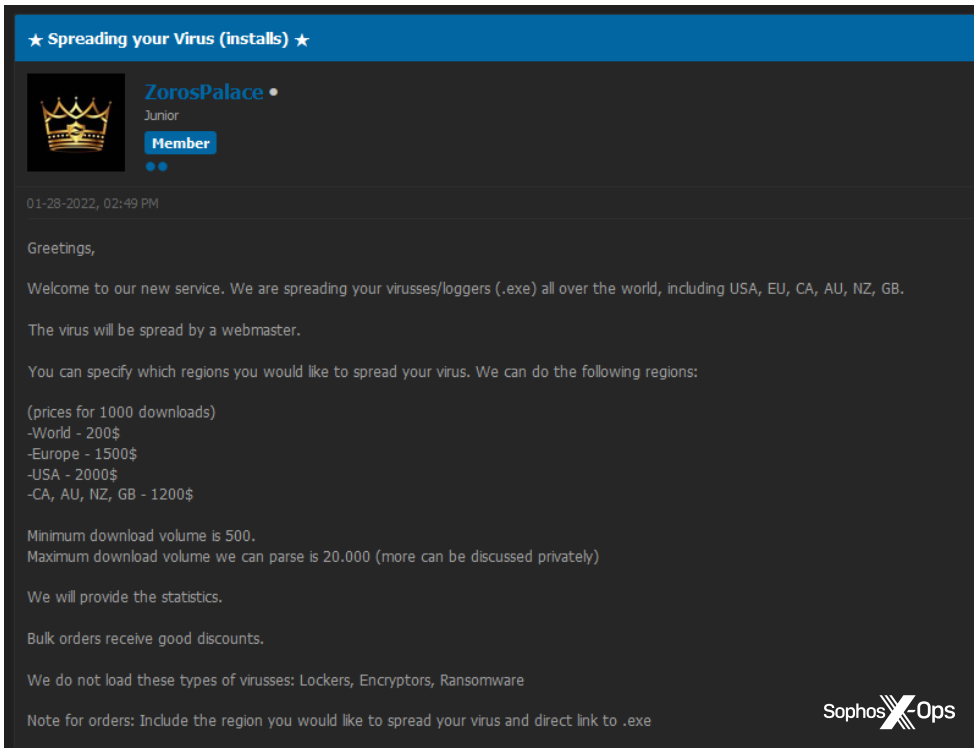

図 5. マルウェアを拡散する新しいサービスの広告。

サービスとしてのフィッシング：フィッシングキャンペーンのための偽装サイト、ホスティング、スパムフィルターを回避する巧妙なメール、結果を監視する画面など、サイバー犯罪者は包括的なサービスを提供しています。

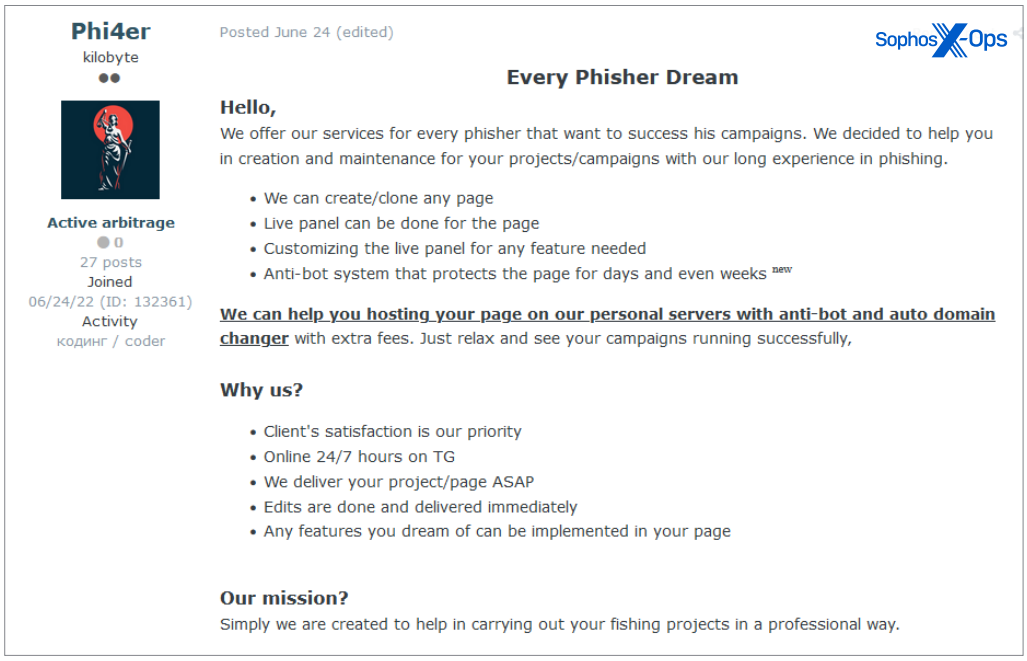

図 6. さまざまなカスタマーサービスが受けられるフィッシングサービス。

サービスとしての OPSEC：特に注意が必要なのは、犯罪者フォーラムで確認された攻撃シミュレーションツール「Cobalt Strike」がバンドルされているケースです。販売者は、Cobalt Strike に感染していることを隠ぺいし、検出されて攻撃元を特定されるリスクを最小化するように設計された OPSEC サービスを 1 回限り利用するサービスや月額のサブスクリプションサービスとして提供し、サイバー犯罪を支援しています。

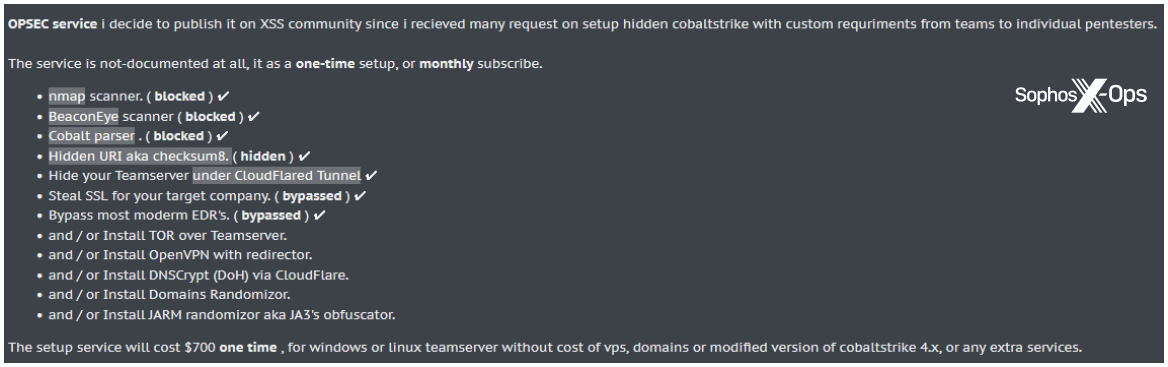

図 7. 専門性の高いサービスプロバイダーが、攻撃の痕跡を隠ぺいできるように支援している。

サービスとしての暗号化：サービスとしての暗号化は、多くのフォーラムで販売されている一般的なサービスです。これは、マルウェアを暗号化し、特に Windows Defender や SmartScreen、またその他のアンチウイルス製品による検出を回避するように設計されています。以下の事例では、サービスを 1 回利用する場合の購入額が 75 ドル、1 カ月間無制限で利用する場合には 300 ドルになっています。

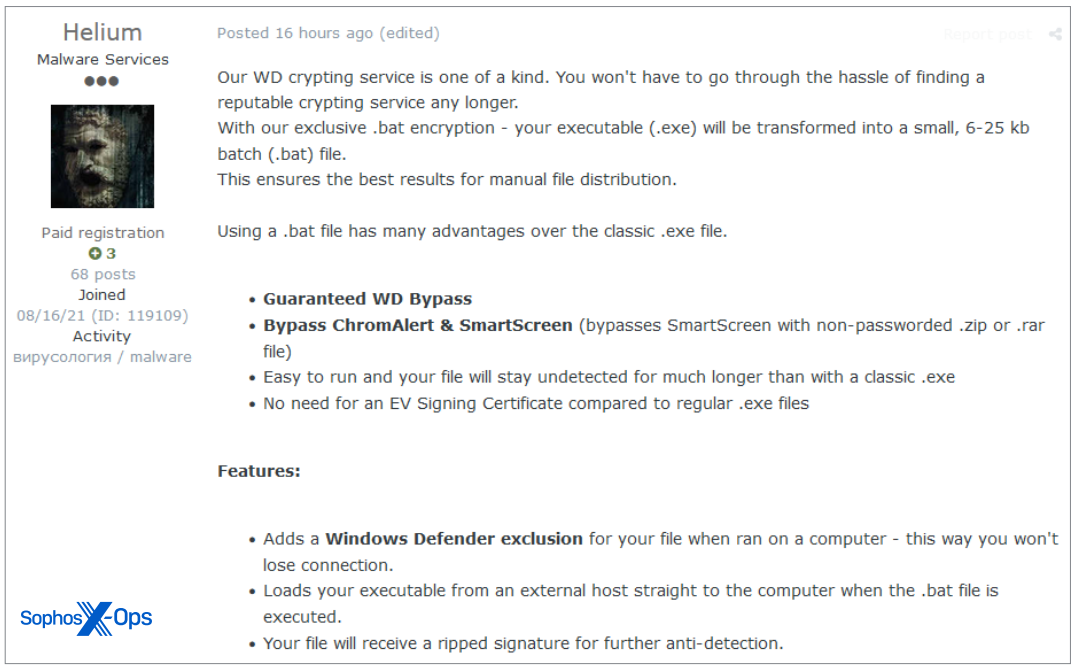

図 8. 検出を回避するために、.exe ファイルを .bat ファイルに変換する専門的なサービス。

サービスとしての詐欺：特に暗号通貨詐欺に関連した「詐欺用キット」が犯罪者向けフォーラムで宣伝されている例もいくつか確認されています。販売される内容の詳細は明らかになっていませんが、「イーロンマスクがビットコインをプレゼントする」という詐欺キャンペーンのサービスは 450 ドルで提供されています。これは少なくとも 2018 年から流行している詐欺であり、Twitter、Medium、またはディープフェイクビデオを利用して拡散されています。

サービスとしてのビッシング：ボイスフィッシング (ビッシング) サービスでは、電話を受けるための音声システムをレンタルし、標的ユーザーが人ではなくボットと対話することを選択できる「AI システム」を提供します。

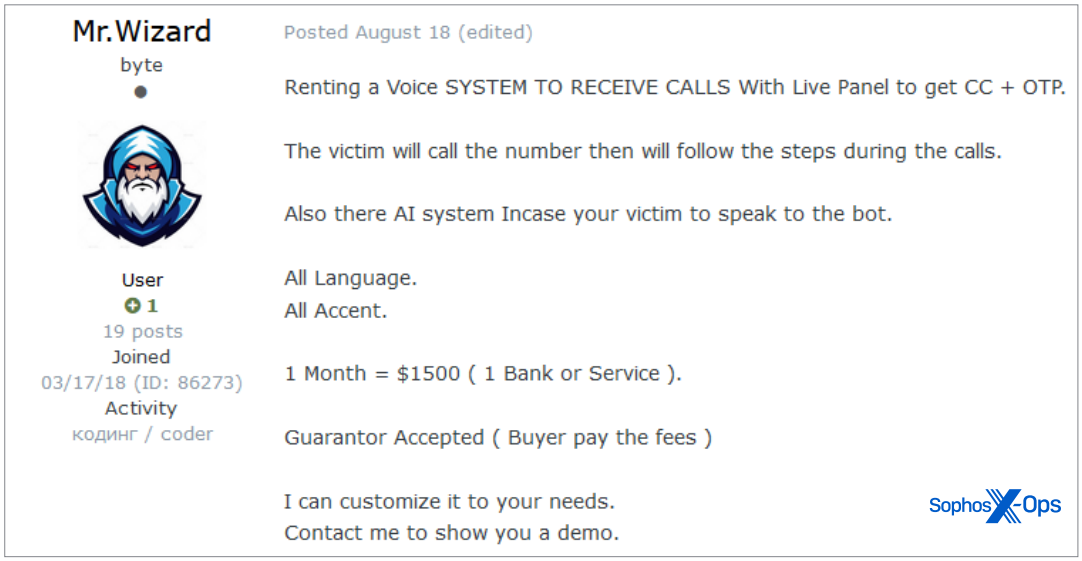

図 9.「すべての言語およびアクセント」に対応するサービスとしてのビッシング。

サービスとしてのスパムメール：サービスとしてのスパムメールは、古くから人気の高いサービスであり、今でも犯罪者フォーラムで広く販売されています。これは、SMS やメールなどのさまざまな方法で大量のスパムメールを送信するサービスです。これらのサービスを提供するサイバー犯罪者は、インフラストラクチャ全体をゼロから構築するように提案するケースもあれば、インフラストラクチャを運用しており、カスタマイズしたスパムメッセージを送信しているケースもあります。

サービスとしてのスキャン：最後のサービスは特に注意が必要です。これは、脆弱性を特定して攻撃するために、Metasploit、Invikti、Burp Suite、Cobalt Strike、Brute Ratel などの正規の商用ツールをユーザーに提供するサービスです。図 10 にあるように、販売価格が大幅にディスカウントされています。すべてのインフラストラクチャは販売者が構築および維持していると考えられます。この販売者は、「スキャンの結果がメールで送信されるのを待つだけ」と説明していました。

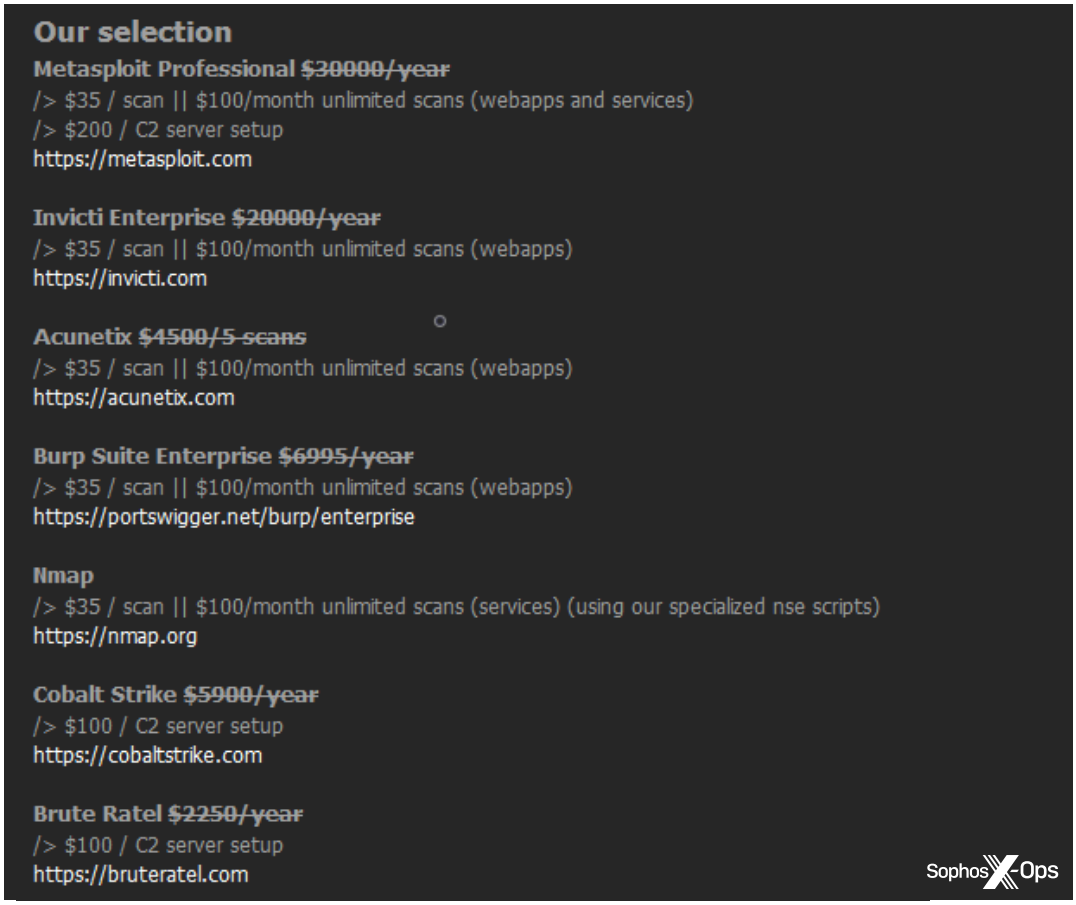

図 10. サービスとしてのスキャンのプロバイダーは、一般的なさまざまな商用ツールを利用できると述べている。

テキストベースの広告からグラフィックを多用した広告への進化

XaaS 産業が成長し、犯罪者向けのマーケットのコモディティ化が進むにつれて、これらのマーケットのルックアンドフィールも変化しました。たとえば、人気の高いフォーラムでは、広告スペースを支払うことで、フォーラムの数千人のユーザーに対してアニメーションのバナー広告を表示できます。なお、以下の例は、既出の Genesis という人気のある地下マーケットに掲載されている広告です。

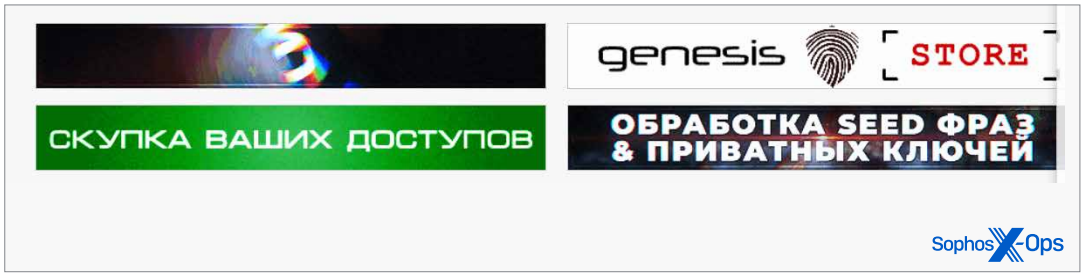

図 11. さまざまなマーケットやサービスの広告を掲載する犯罪者向けフォーラム。

また、サイバー犯罪者も、プロフェッショナルなグラフィックデザインやレイアウトにする効果を認識するようになりました。数年前までは、マルウェアやサービスのリストは、機能や性能が一覧表示されるテキストベースの簡易な投稿が一般的でしたが現在では、目を引く画像が利用されることが多く、プロフェッショナルな雰囲気やブランドの差別化、権威性を高めていることが多くあります。

図 12. Zed Pointのサービスは、個人情報の改ざんや窃取を助長する情報を提供している。

図 13. NoCryi は、セッション Cookie を盗み出し、特定のマシンにアクセスするための情報を収集して保持している。

地下マーケットで宣伝されるのは、製品やサービスだけではありません。犯罪者向けのマーケットの成長と専門化が進むにつれ、仕事のオファーや求人投稿も増加しています。人気の高いいくつものマーケットで、求職者 (通常、ランサムウェアの提携者を婉曲に表現した「ペンテスター」) および採用スタッフを募集する専用の求人ページが用意されています。

0

[JOB - BTC/XMR] I operate dozens of phishing websites of all kinds. Looking for some "marketers" who can bring people in for a 50/50 split

by **/u/carderman** · 1 week ago in **/d/Jobs4Crypto**

Like the title states, I've got a bunch of different custom-built phishing websites, ranging from fake darknet markets, fake crypto exchanges, email templates with fake giveaways & crypto promos, fake carding sites, simple landing pages, and so on.

I'm looking for someone or someones who'd like to bring people in, via spamming, social engineering, whatever method works for you... and if they take the bait, we split their generous donations 50/50.

I've had some of these up for anywhere from over a year to some I just created this week. These sites bring in a decent chunk of change as they are, but I've never been opposed to more money.

If interested in getting started, or simply learning more about them, just DM me and I can send you some links and you can choose which ones you think you might be able to do something with.

We can keep track of which ones are yours using a coupon code or custom "referral" url. I have a couple ideas for making sure we're on the same page when it comes to keeping track of which "sales" are yours. I'm keen to ensure you're compensated fairly for the hits you bring in because that's just good business - this shit is already passive AF and basically free money for me at the end of the day. But If you can bring in more free money then I'm more than happy to keep you happy if that means you'll keep selling.

Hell, if you're really good, I'd be more than happy to give you the lions share.

Let's make some money, ladies!

SophosX-Ops

図 14. さまざまなスキルを有する組織が連携することで、犯罪の効率化が進んでいる。

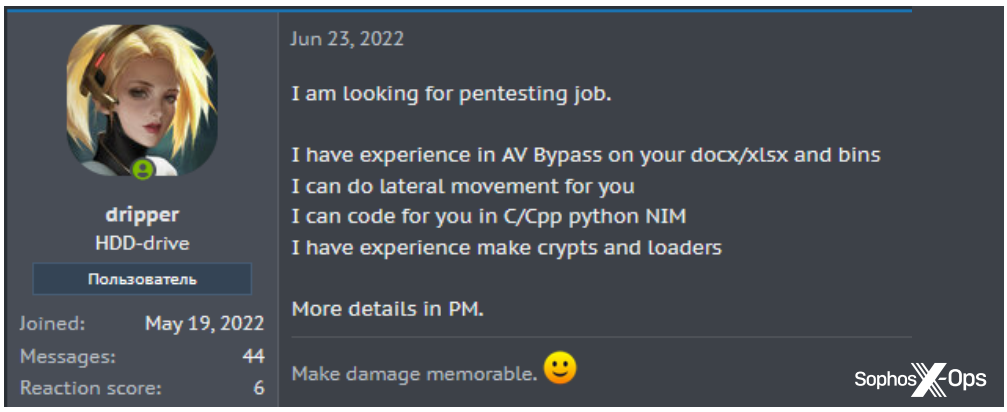

図 15. 実績のある組織のジョブを求めている経験豊富なペンテスター。

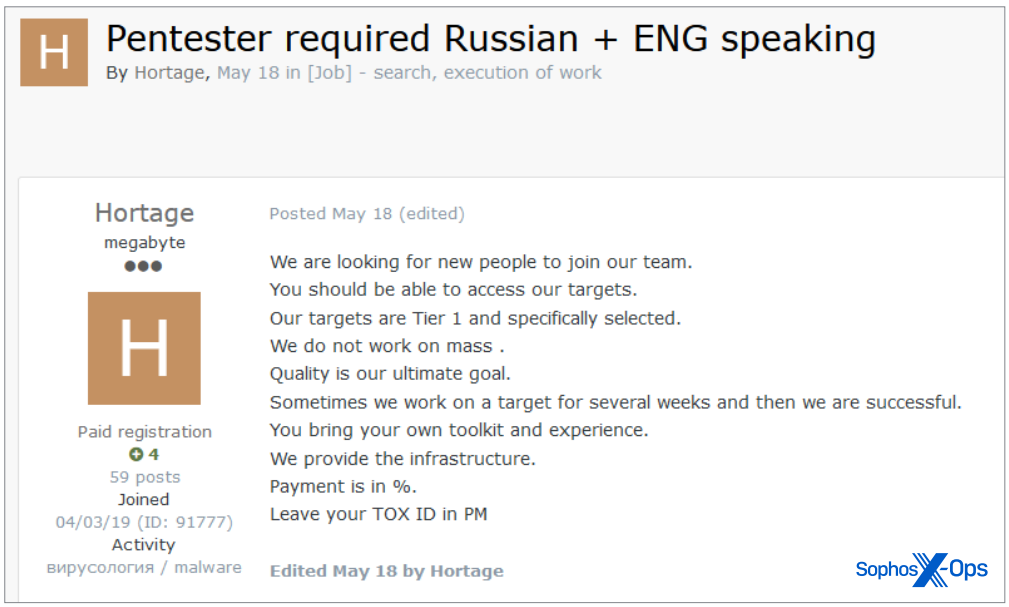

図 16. 新しいメンバーを募集するサイバー犯罪組織

情報窃取マルウェア

情報窃取のサービスは、マルウェア経済圏を支えるインフラストラクチャの一部であり、先ほど列挙した「XaaS」モデルにも似ていますが、さらに大規模なサービスです。サービスとしてのマルウェアやサービスとしてのマルウェア配信により、わずかな投資で誰でも犯罪行為を開始できるようになっています。必要とされるのは、Web コントロールパネルにログインして、認証のマーケットにアクセスする能力だけです。

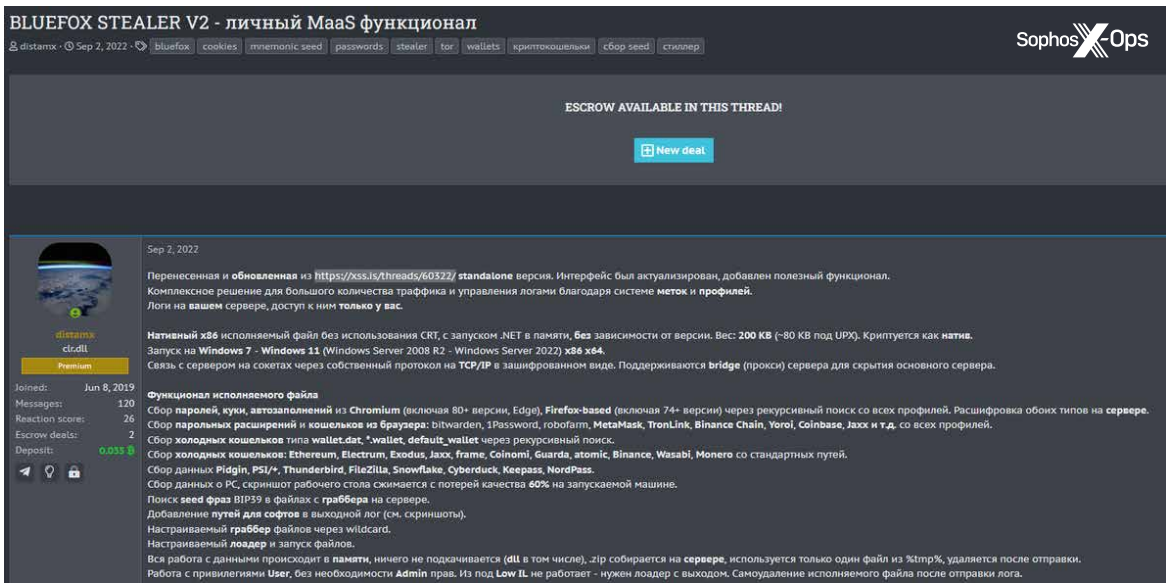

図 17. サイバー犯罪エコシステムの専門化が進む中で、拡大する情報窃取サービス

起業家精神のあるサイバー犯罪者は、盗んだ認証情報を多くの地下マーケットで転売する場合もあります。取引される暗号通貨を窃取したり、マルウェアをマネタイズする手法を実施したりする過程で、認証情報が二次的に取得される場合があります。

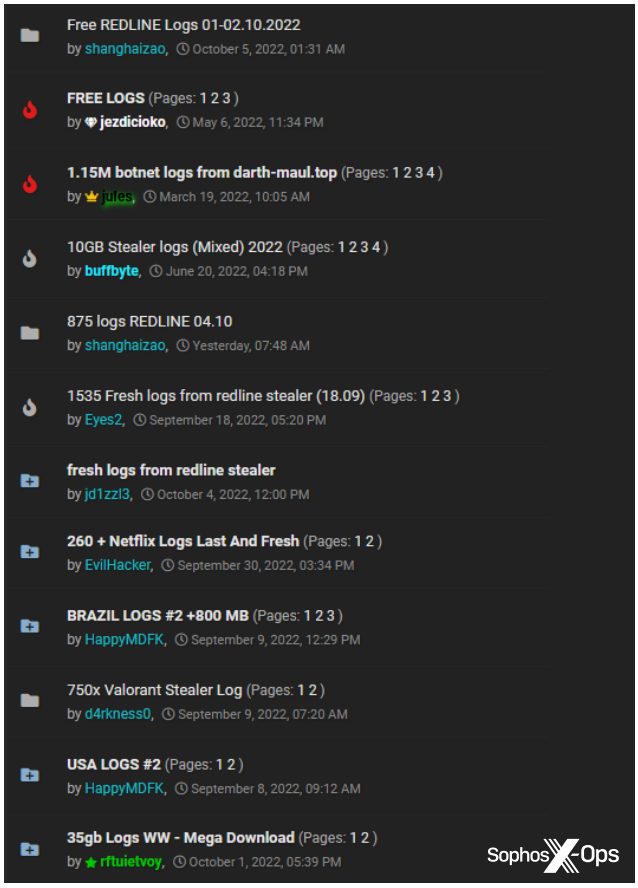

図 18. パスワードなどの認証情報を含む「ログ」が盗まれ販売されている

最後に、情報窃取マルウェアのエコシステムは、防衛側が関心を持っていることを強く意識しており、いつものように、利益を得る機会を探っています。最近、地下フォーラムの 1 つである「XSS」は、2000 ドルのサブスクリプション費用を年間で支払えば、無制限にアクセスしてデータを収集できると謳い、ホワイトハットがフォーラムをスクレイピングしようとする労力を金銭に変えようとしていました。

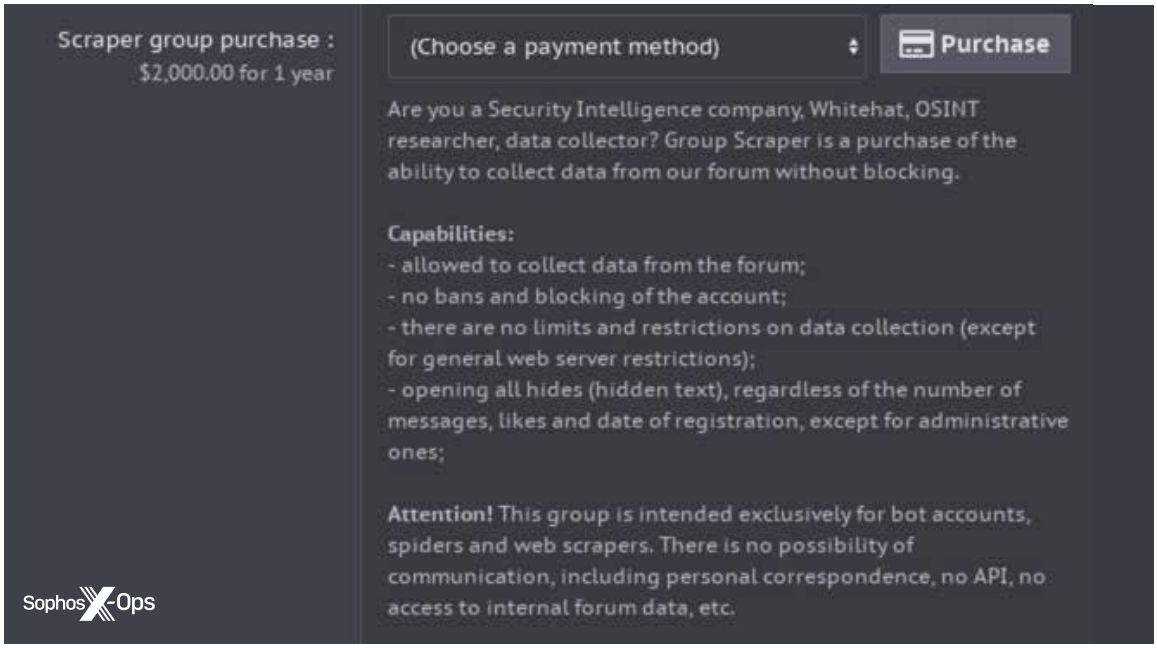

図 19. あるフォーラムでは、犯罪行為を監視するホワイトハットスクレイパーにアクセス権限を有料で販売している。(2 枚目の画像の文章は、ロシア語から英語に翻訳されています)。

情報窃取型マルウェアは広義で使用されます。これらのマルウェアには、リモートアクセスツール (RAT)、キーロガー、仮想通貨を盗み出すマルウェアである「クリッパー」、認証情報、ブラウザ Cookie、暗号通貨取引、また、簡単に盗むことができ販売や悪意のある目的のために再利用できるデータを取得する他のマルウェアなど、このレポートでも説明している多様なマルウェアが含まれます。

情報窃取型マルウェアを使用するサイバー犯罪組織は Slack の Cookie を提供していましたが、2021 年に Lapsus$ 組織はこの Cookie を使用してエレクトロニック・アーツ社のネットワークにアクセスしています。また、最近では、Web アプリケーションのセッショントークンが盗み出され、ビジネスメール詐欺 (BEC) からランサムウェア攻撃まで、持続的で広範な悪意のある活動にも利用されています。

ユニークマシンで見た情報窃取型マルウェアの検出数

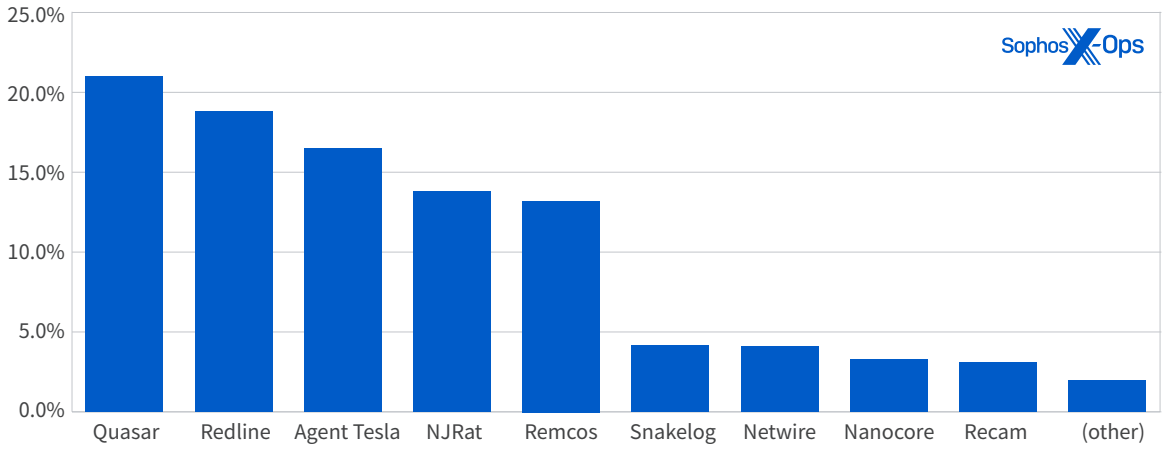

図 20. Quasar、Redline、Agent Tesla は、検出された情報窃取型マルウェアの大部分を占めており、Quasar は 6 ヶ月間に感染したマシンの 5 分の 1 以上で検出されている。

情報窃取型マルウェアに詳しい方であれば、上の図に悪名高い Raccoon Stealer が表示されていないことに気が付いたのではないでしょうか。Raccoon Stealer は、ウクライナで開発され 2019 年に登場した Windows 向けのマルウェアであり、オランダやイタリアの捜査当局と連携した FBI の活動により、2022 年初めに一時的に姿を消しましたが、その後、新たな体制の元で再び登場しました。6 月に新バージョンの開発を開始し、9 月に完成した新バージョンを開発者の Telegram チャンネルで公開しました。しかし、新バージョンが公開されたことが周知されているにもかかわらず、新しい Raccoon Stealer が悪用されているケースはほぼ確認されていません。10 月下旬、米国司法省は、現在オランダに拘束されているウクライナ人を、このサービスの運営を共謀した罪で起訴したことを公表しました。

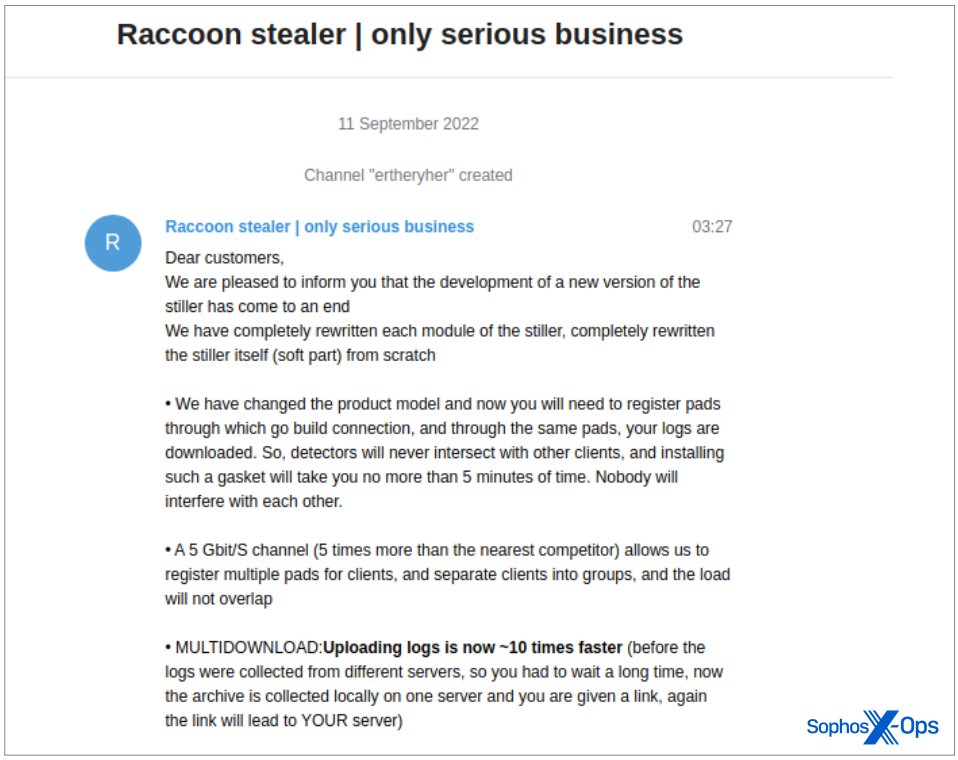

図 21. Raccoon Stealer を開発した組織が、Telegram チャンネルで最新版を発表した。

情報窃取型マルウェアは、さまざまなチャンネルで配信されます。最も一般的なチャンネルは、ソーシャルエンジニアリングを利用するダウンローダーサービスであり、正規のソフトウェアインストーラが含まれていると謳ったアーカイブファイルやディスクイメージを取得するようにユーザーを誘導します。これらのファイルやイメージは通常、ライセンスを取得する必要がない海賊版として宣伝されています。また、ダウンロードされるファイルには、いくつものマルウェアパッケージのインストーラが含まれています。これらのダウンロードサイトは、SEO (検索エンジンの最適化) 技術を使用して、「海賊版」ソフトウェアを検索するときに、検索リストの上位に表示されるようにしています。その他、Emotet や Qakbot/Qbot などのボットネットを利用し、対価を払って配信される場合も多くあります。

Agent Tesla などの一部の情報窃取型マルウェアは通常、悪意のあるメールを作成し、標的を絞り込んで送信しています。これらのメールには、緊急の文書を装ったファイルが添付されていますが、このファイルはマルウェアのインストーラになっています。

しかし、さらに標的を絞って情報窃取型マルウェアが展開される場合もあります。ソフォスは、ネットワークに侵入した攻撃者が、Cobalt Strike から展開されたバックドアを使用して、ネットワークから Cookie や他の認証情報を窃取するマルウェアを実行したインシデントを追跡しています。サーバーが存在するシステムからブラウザ Cookie を大量に収集し、盗んだ Cookie を使用してこの組織の Web ベースのリソースに正規ユーザーとしてアクセスし、ラテラルムーブメントによって組織の深部への侵入を試みていました。

ソフォスは、情報窃取型マルウェアをブロックするさまざまな対策を導入しており、セッション Cookie を大量に取得して情報を盗み出す攻撃を防止するために、Cookie の窃取を防止する機能を追加しています。

ランサムウェアの進化

昨年、地政学的な混乱やランサムウェア組織のメンバーの起訴があったことで、ランサムウェア組織の活動が中断することがありました。しかし、古いグループから新しいグループが生まれており、ランサムウェアが組織にとって最も重大なサイバー犯罪の脅威の 1 つであることに変わりはありません。ランサムウェアのオペレーターは、検出を回避するため、また新しい手法を取り入れるために、その活動の内容やその仕組みを進化させ続けています。

一部のランサムウェア組織は、検出をより困難にするため、ランサムウェアの実行ファイルをさまざまな OS やプラットフォームで実行できるようにコンパイルしやすくするため、あるいはマルウェアペイロードの開発者のスキルやツールを取り入れるために、新しいプログラミング言語を使用したランサムウェアを利用するようになりました。プログラミング言語「Rust」は、BlackCat および Hive ランサムウェアの開発者によって採用されており、BlackByte のマルウェアは Go (別名、GoLang) で記述されています。

2022 年 10 月までに Sophos Rapid Response が確認している最も悪用されたランサムウェアは LockBit であり、BlackCat と Phobos の検出が僅差で続いています。しかし、他のランサムウェアも 5 分の 1 以上を占めており、ランサムウェアは注目を集めている特定の系統に限定されているわけではありません。以下に示すランサムウェアの分布は、世界全体におけるランサムウェア攻撃の実際の分布を正確に反映していると考えられます。

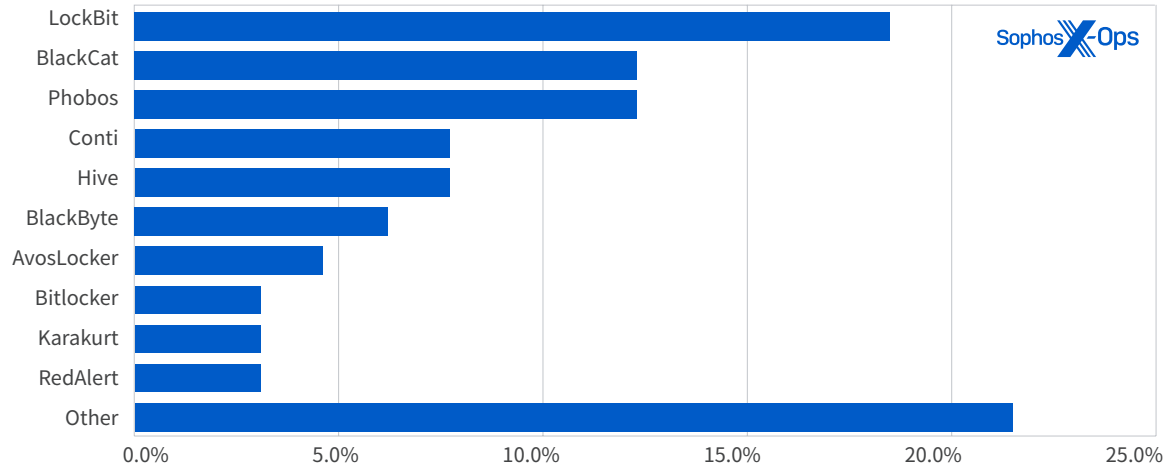

図 22. LockBit、BlackCat、Phobos など知名度の高いランサムウェアも存在するが、ランサムウェアの種類は多岐にわたる。

ランサムウェアで使用される言語も多様化し、標的も広がっており、Windows 以外のオペレーティングシステムも攻撃を受けるようになっています。RedAlert (別名、N13V) は、Luna (Rust ベースの別のランサムウェア系統) と同じように、Windows と Linux の ESXi サーバーも暗号化します。しかし、Linux を標的としているのはマイナーなランサムウェアだけではありません。年初には、Linux-ESXi を攻撃する LockBit の亜種も研究者によって発見されています。攻撃の対象となるプラットフォームの変化は、サイバー犯罪者にとって攻撃機会の増加につながっています。攻撃対象領域が広がったことで、組織に圧し掛かるプレッシャーも増大しています。多くのランサムウェア対策は Windows に集中しているため、検出されるリスクも低くなっています。Linux、Mac、モバイルの各プラットフォームの脅威については、本レポートの後半で詳しく説明します。

また、侵害されたシステムにランサムウェアを展開する方法も進化しています。今年初めに SophosLabs チームが分析した 2 つのランサムウェアインシデント (1 件は Darkside、もう 1 件は Exx ランサムウェア) では、正規のアプリケーションを使用した DLL サイドローディングの手法が用いられました。Darkside のケースでは、通常のアンチウイルスユーティリティプログラムが使用され、Exx の場合は、Google アップデーターが使用されていました。DLL サイドローディングは、一部の業界を標的とする攻撃者によって長年にわたって多用されてきた手法ですが、現在では、正規のプロセスを装って悪意のあるペイロードを実行することでセキュリティ製品による検出を回避できることから、サイバー犯罪者の間で急速に普及しつつあります。

ランサムウェアの配信と拡散についても、サイバー犯罪者は新たな手法を取り入れています。ソフォスでは、ネットワークプロトコルを操作するためのオープンソースの Python モジュールのコレクションである Impacket が、ネットワークのラテラルムーブメントに悪用されていることを確認しています。Impacket のツールセットには、リモートからのコード実行機能、認証情報を傍受してダンプするスクリプト、既知の脆弱性に対するエクスプロイト、そしてエニュメレーションモジュールが含まれており、ランサムウェアを使用するサイバー犯罪者にとって、非常に好都合なパッケージとなっています。このツールは正規のセキュリティテストツールとして開発・提供されているものですが、Metasploit や Cobalt Strike と同様に、その機能

や能力は、好ましからざる顧客を惹きつけています。同じように、侵入テストツールの Brute Ratel がペイロードを配信するために使用されていることも確認されています。攻撃者が正規のセキュリティツールを攻撃に悪用するケースが増加しているため、ネットワーク上で何がどのような目的で稼働しているのか、これらのツールを実行する権限があるユーザーが誰かを、防衛側の組織は細心の注意を払って確認しなければならなくなっています。

また、ランサムウェア組織は、金銭を取得するためにさらに多くの機会を探っており、活動を多様化させています。その最たる例が、被害を受けた組織の情報を掲載するリークサイトの増加です。従来は、組織が金銭を払えばリークサイトにデータを公開しないという分かりやすいモデルが採用されていました。金銭を支払わなければ、データはリークサイトに公開されることになります。しかし、今年はリークサイトの運用について興味深い動きがありました。

先陣を切って新たなタイプのリークサイトを運用したのは、最大のランサムウェア組織の 1 つである LockBit です。このランサムウェアの新バージョン LockBit 3.0 の公開に伴って、新たなリークサイトが登場しました。このサイトにはいくつもの新機能が含まれています (LockBit 3.0 の多くの機能とコードの大部分が BlackMatter ランサムウェアをベースにしているように見えることから、これは LockBit Black とも呼ばれます)。たとえば、このランサムウェア組織が考案した金儲けの方法の 1 つは、リークサイトにアクセスした組織つまり被害を受けた組織に、盗まれたデータを消去または購入したり、一般に公開するまでの期間を延長したりする選択肢を提供することでした。

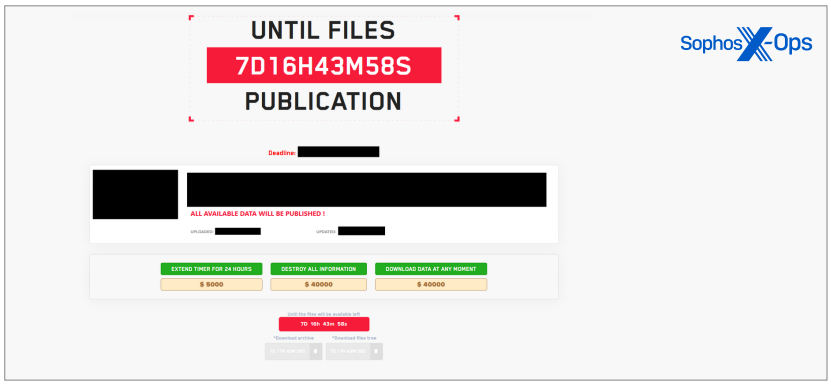

図 23. LockBit の被害を受けた組織には、ランサムウェアのタイマーを延長したり、データをダウンロード または消去する選択肢が提示される。

Karakurt や AvosLocker など、他のランサムウェア組織もこの手法を模倣し、窃取したデータをオークションにかけています。さらに、Snatch のように、リーク行為をサブスクリプションモデルに移行している組織もあります。被害を受けた組織がお金を払えば、情報が公開されないだけでなく、情報漏洩の事実も公開されないようにするなど (つまり、被害を受けたことがリークサイトに公開されていた場合、その言及も削除される)、組織の情報を公開した後に、独自の対応を行っているサイトもあります。多くの国ではセキュリティ侵害が発生した場合に規制当局への報告が義務付けられており、被害者が侵害の事実を隠蔽すると、犯罪の共謀と見なされる恐れもあります。

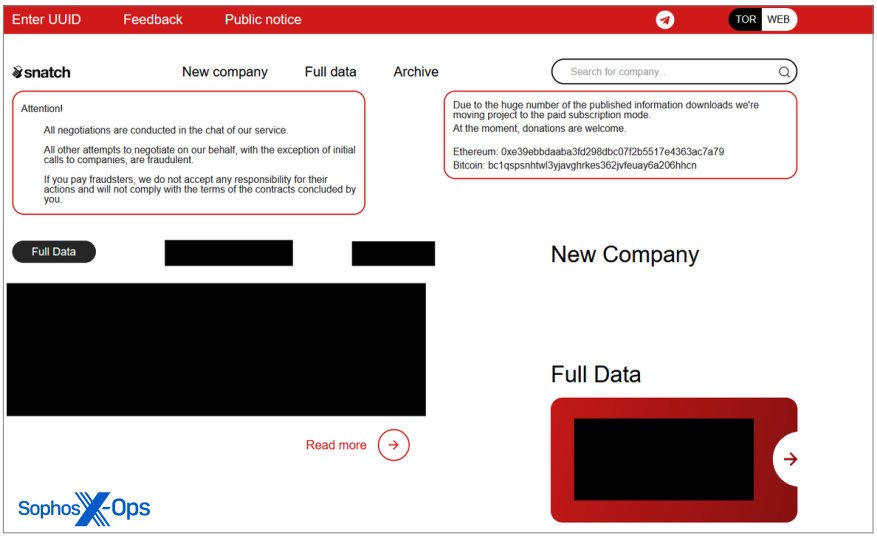

図 24. サブスクリプションモデルに移行している Snatch ランサムウェア。

しかし、LockBit はさらに一歩進んでおり、ランサムウェアという主力製品だけではなく、犯罪者コミュニティの交流や連携のための場所を提供するなどの新たな取り組みを行っています。たとえば、LockBit の新しいリークサイトでは、バグ報奨金制度を提供しており、最終的にサービスを強化することにつながる以下のようなさまざまな活動に対して「1000 ドルから 100 万ドル」の報酬を提供しています。

- LockBit の Web サイトやマルウェアに存在するバグを特定して秘密裏に報告すること。
- LockBit の提携プログラムの関係者の個人情報の窃取に成功し、その方法について詳しく説明すること。これは、LockBit が OPSEC を強化することを目的としています。この報奨金は 100 万ドルになっています。
- サイバー犯罪者が多用しているインスタントメッセージングサービスである Tox メッセンジャーの脆弱性
- LockBit ランサムウェアを改善するためのアイデア
- オニオンドメインや Tor ネットワークにおける情報漏えいの脆弱性

バグ報奨金制度を提供しているサイバー犯罪組織は、LockBit が初めてではありません。2021 年 11 月には、複数のロシア語のサイバー犯罪フォーラムで活動している主要なカード犯罪組織である All World Cards が、組織のストアで見つかった脆弱性に対して最大 1 万ドルの報奨金を提供しています。恐らくこのような取り組みは今後も続くでしょう。これは、クラウドソーシングの手法により侵入テストや脆弱性評価を効果的に行う方法であり、発見された脆弱性は、調査した協力者とサイバー犯罪者だけで共有されることになります。

図 25. All World Cards は、2021 年末にバグ報奨金プログラムを発表した。

最後に、知名度が低いランサムウェア組織や情報漏えいを中心に行っている組織をいくつか紹介します。これらの組織は、有名なサイバー犯罪組織とは異なり、政治的な動機を持っていると考えられます。まず、ウクライナの市民や政府組織を侵害して得た資料を共有することに特化したリークサイトが見つかっていますが、データの出所やランサムウェアが関与しているかどうかは不明です。

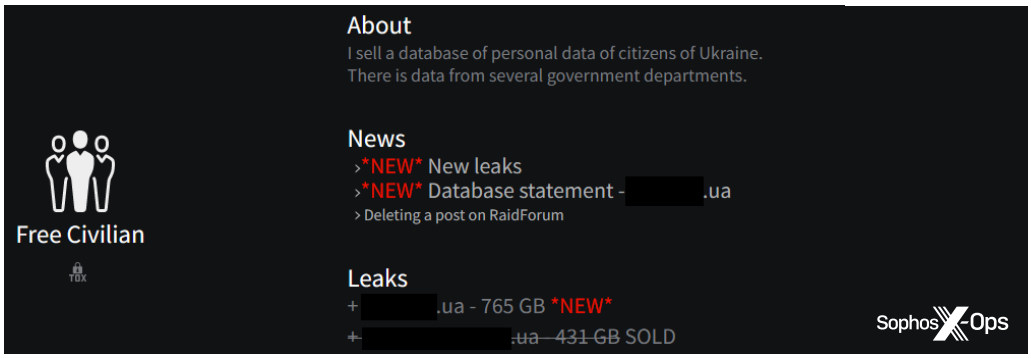

図 26. ウクライナの一般市民を標的とする攻撃者

また、Moses Staff として知られる組織は、身代金を実際に要求しておらず、ランサムウェアのような手法を用いてイスラエルの組織を標的としていると考えられています。

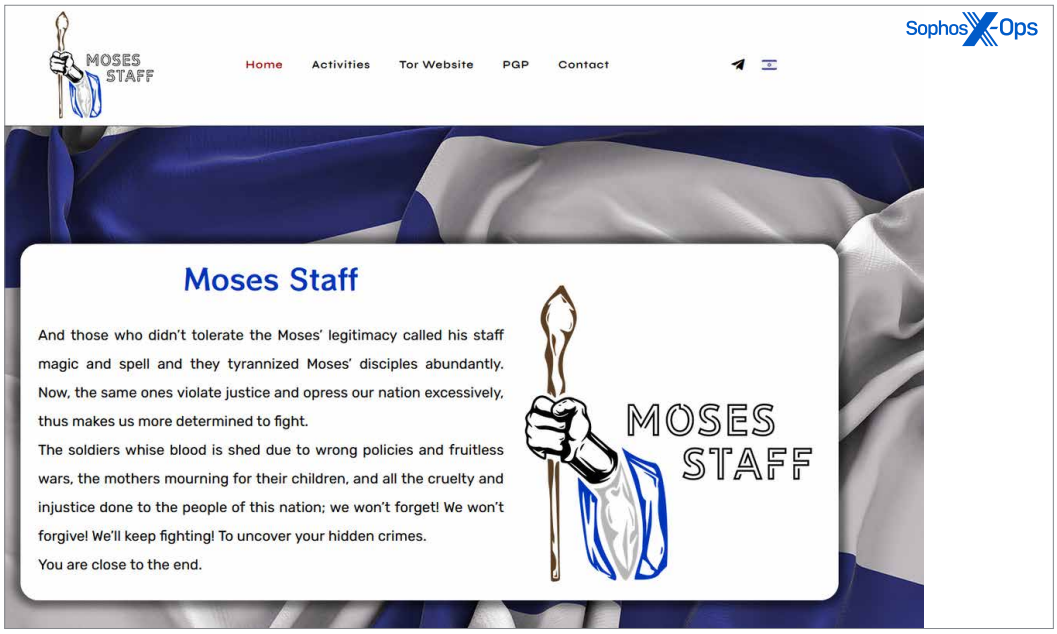

図 27. ランサムウェアのような手法を用いて攻撃を行うイスラエルに敵対する組織

攻撃ツール

防衛側の多くの組織にとって、攻撃者が誰であるかを特定することに比べると、攻撃の方法を示す情報は比較的簡単に入手できる場合があります。このセクションでは、攻撃者が現在、その目的を達成するためにセキュリティツールをどのように転用しているかを見ていきます。悪用されるケースが多くなっているのは侵入テストツールだけではありません。他の正規のセキュリティツールも攻撃に転用されています。ここでは、正規のリモートアクセスツール (RAT) が使用されているケースなど他の手法について簡単に説明します。その後に、標的のシステムにすでに存在するバイナリを悪用する、環境寄生型バイナリ (LOLBin) と呼ばれる手法や、サードパーティのドライバや DLL を利用して不正コードを潜り込ませる攻撃者が最近増加している状況とその対策について説明します。最後に、2022 年の特に注意すべきマルウェアとして、エンドポイントセキュリティのアップグレードを狙うランサムウェアと、暗号通貨を採掘するためにユーザーのリソースを利用するマイニングソフトウェアの 2 つについて詳しく説明します。レポートの最後のセクションでは、Linux、Mac、およびモバイルの脅威環境について説明します。

オフェンシブセキュリティツールの悪用

情報セキュリティチームが現在の攻撃をシミュレートするために使用しているオフェンシブセキュリティツールが、多くのランサムウェアキャンペーンで悪用されるようになりました。昨年のレポートでも説明したように、商用の侵入テストツールである Cobalt Strike の海賊版が、ランサムウェアの提携者などによって利用されるケースが増加しています。たとえば、認証情報の収集ツールである Mimikatz (ソフォスのテレメトリで検出されたユニーク攻撃ツールの約 4 割を占める)、PowerSploit などの PowerShell ベースの攻撃ツール、オープンソースの MetaSploit 攻撃プラットフォームに接続する「Meterpreter」コンポーネントなど、オフェンシブセキュリティのコミュニティによって開発されたオープンソースツールは、検出される攻撃ツール全体の中でも最も多くなっています。

しかし、市販のオフェンシブセキュリティツールの海賊版は、複雑で高度な攻撃で標準的に使用されるようになっています。上記のように、サイバー犯罪組織の中には、このようなツールに関するスキルを有する人材を採用するための広告を出しています。また、Cobalt Strike や商用版の Metasploit の海賊版も拡散しており、地下サイトには無料版へのリンクが頻繁に貼られています (これらの中には実際にはマルウェアである場合もあります)。

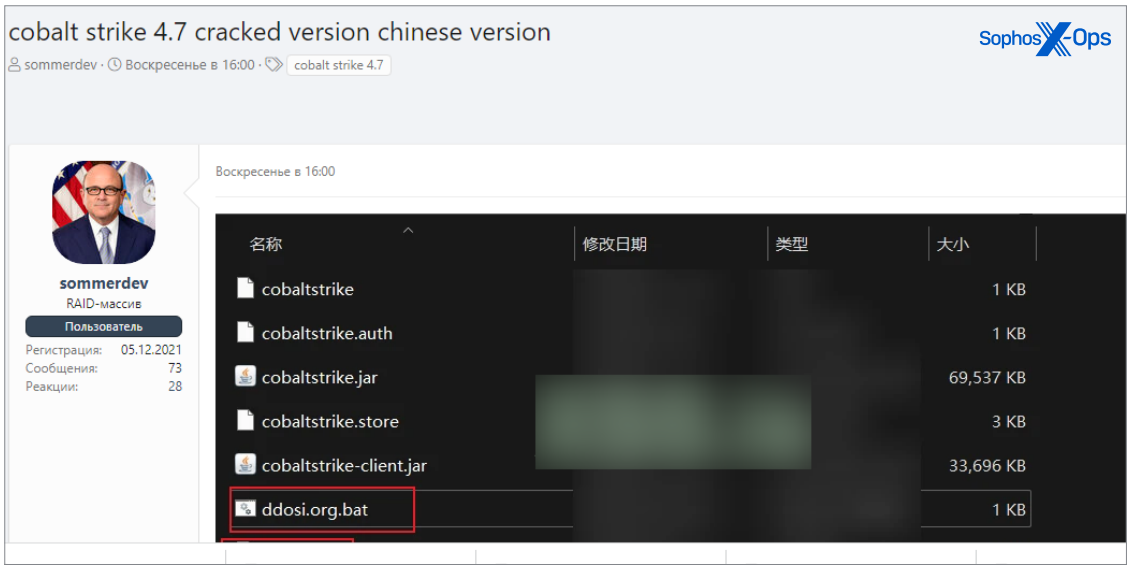

図 28. 転売される海賊版の Cobalt Strike 4.7 (中国語版) 。

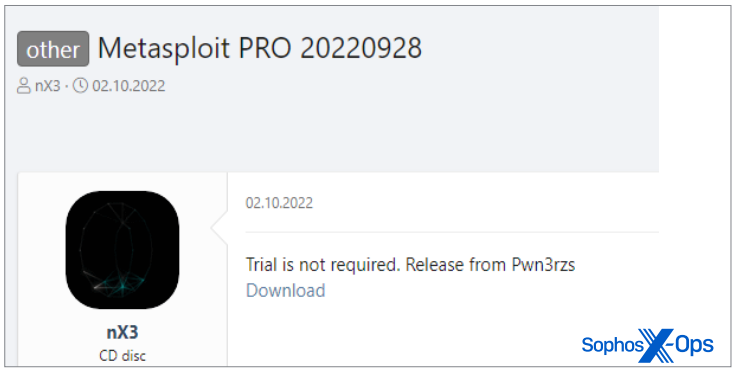

図 29. Metasploit の有料版が海賊版として提供されておりダウンロードできる。

Cobalt Strike は、2022 年の第 1 ～ 3 四半期にソフォスの Rapid Response チームが担当した顧客のインシデントの 47% で使用されていました。これらの多くのケースで Cobalt Strike は、ランサムウェア攻撃や、ランサムウェア攻撃の前段階の操作で使用されていました。これらの攻撃試行は、ランサムウェア攻撃を防ぐための TTP (手法、ツール、手順) を使用して検出されています。Cobalt Strike は、2020 年の SolarWinds キャンペーンや、ロシアの支援を受けているサイバー犯罪組織によるウクライナを標的とした攻撃など、国家を対象とした攻撃でも観測されています。

Cobalt Strike 単体が、検出されるユニーク攻撃ツールの 8% を占めています。また、Cobalt Strike の通信プロトコルは、攻撃者が開発した他のツールにも取り込まれています。たとえば、TurtleLoader のいくつかのバージョンは、Metasploit や Cobalt Strike の通信プロトコルのいずれかを介して、コマンドアンドコントロール (C2) ネットワークに接続しています。このように複数のツールを攻撃者が使用している場合、防御側の組織では多層防御が求められることになります。

そして、さらに注意が必要なことがあります。たとえば、本レポートを執筆している時点で、Brute Ratel ツールキットが新たに利用可能になっており、悪用されるケースが増加しています。ソフォスのインメモリ検出で見つかった Brute Ratel はこれまで 1% にも満たず、これまではほぼ検出されていませんでしたが、2023 年には、Brute Ratel 製品の海賊版が急増し、状況が大きく変化することになるはずです。

注意が必要な攻撃ツールの検出数 (6 ヶ月間におけるユニークマシン数)		
攻撃ツール	**感染したマシンの割合**	**注**
Mimikatz	24.7%	ネットワークに侵入された後に使用されるオープンソースの認証情報ダンプユーティリティ
Apteryx	14.5%	Mimikatz のコンパイル版
PowerSploit スイート	11.7%	オープンソース。2020 年 8 月に公式サポート終了
SrpSuite	8.3%	FuzzySecurity によるオープンソースの PowerShell スイート。
Cobalt Strike	8.0%	プロプライエタリソフトウェア。海賊版として悪用されることが多い。
Meterpreter	7.8%	オープンソースの Metasploit 攻撃ペイロード。商用サポート版もある
Nishang	6.8%	PowerShell で使用するためのフレームワークとスクリプト / ペイロード
TheFatRat	6.2%	オープンソースの Metasploit バックドア / ペイロード自動化
TurtleLoader	5.4%	Metasploit や Cobalt Strike と組み合わせて使用するバックドア。
JMeter	5.1%	Java ベースの Metasploit
Juicy Potato	5.0%	オープンソースの BITS (バックグラウンドインテリジェント転送サービス) エクスプロイト (権限昇格ツール)
winPEAS	4.8%	権限昇格と情報窃取のためのスクリプト
Swrort	4.6%	Metasploit ベースのバックドア
Empire	4.5%	PowerShell Empire と Python EmPyre を統合したオープンソースのポストエクスプロイトフレームワーク。2019 年 7 月以降は正式なサポートなし

図 30：感染したマシンをソフォスが分析した結果を基準としています。これらのツールが存在した割合と、ツールの説明を掲載。半年間（2022年4月～9月）のデータで、ユニークマシンの 4.5% 未満で検出されたツールはスペースの関係で省略しています。

Sophos X-Ops

2022 年 9 月まで、Brute Ratel の開発元は、ライセンス規定によりツールへのアクセスが厳格に管理されていると主張していました。それでも、Conti ランサムウェアとつながりのあるサイバー犯罪者が、このプラットフォームを購入するためにダミー会社を設立したと見られており、ライセンスを購入した正規の顧客の従業員によってライセンスが流出したケースが少なくとも 1 件確認されています。9 月現在、最新版の Brute Ratel の海賊版が、地下マーケットで広く出回っています。

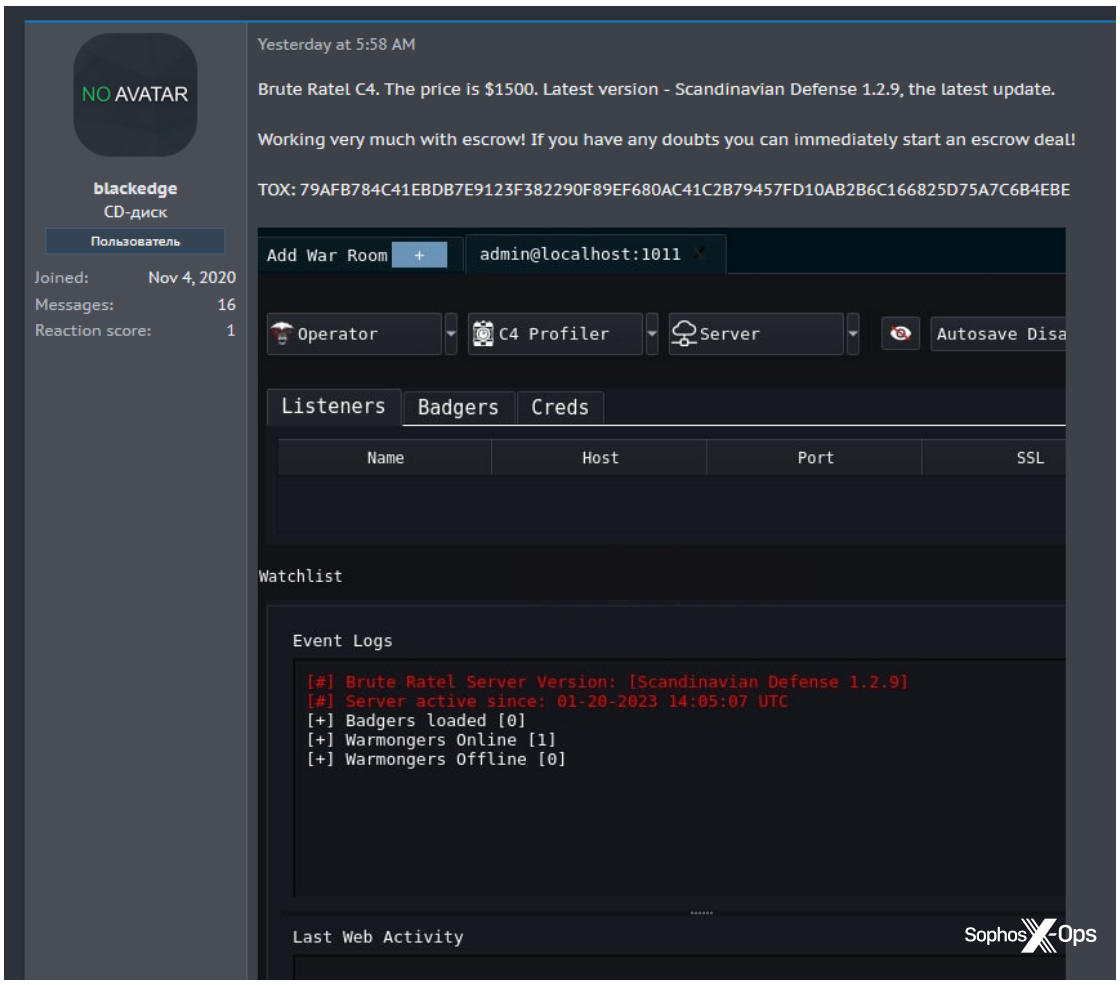

図 31. 地下マーケットで初めて販売された Brute Ratel の海賊版。

これまでソフォスは、Brute Ratel のコンポーネントを利用した散発的な攻撃を記録しています。Sophos MDR が実施したインシデントトリアージでは、攻撃者が最初に Cobalt Strike の使用を試みていました。Cobalt Strike が検出されブロックされたため、次に Brute Ratel を展開しようとしていましたが、これもブロックされました。

しかし、今後は Brute Ratel を使用する多くのインシデントが発生する可能性が高いと考えられます。最近の調査では、過去に Cobalt Strike ビーコンが拡散されたのと同じように、Brute Ratel のエージェントが Qakbot によって拡散されています。これは Brute Ratel が広く利用できるようになった結果だと考えられます。

悪用されているその他のセキュリティツール

正規のツールが悪意のある目的に「転用」されることは、Brute Ratel に限ったことではありません。サイバー犯罪者は、犯罪者向けのマーケットで、他の多くの正規のセキュリティツールを販売しています。たとえば、侵入テストのフレームワークである Core Impact、脆弱性スキャナの Nexpose、VirusTotal Enterprise、エンドポイント保護プラットフォームの Carbon Black などが販売されています。

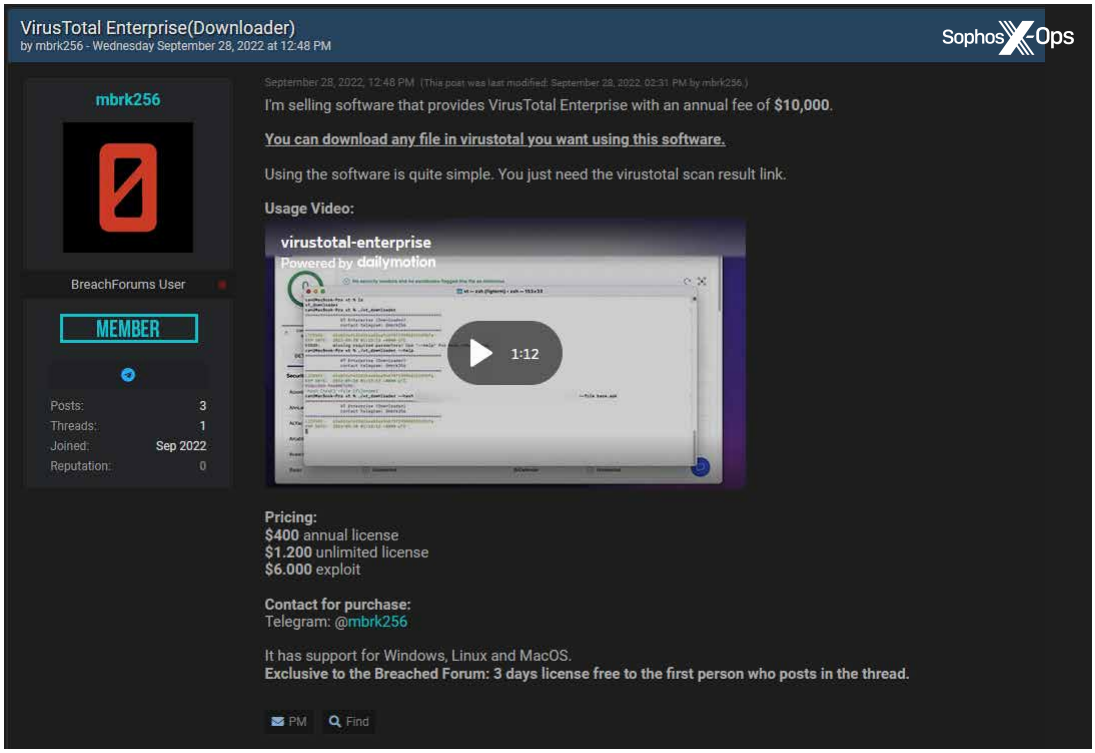

図 32. データスクレイピングに悪用される VirusTotal Enterprise

サイバー犯罪者は、正規のツールをさまざまな目的に使用しています。EDR やエンドポイント保護プラットフォームを分析して脆弱性や回避策をテストしたり、侵入テストやエクスプロイトフレームワークによって脆弱性のスキャンや攻撃を自動化したり、VirusTotal などのツールを使ってマルウェアの検体やスパイ防止活動の情報を入手したりしています。

RAT の攻撃目的への転用

セキュリティツールの不正利用や悪用が後を絶ちませんが、特に注意すべきなのはリモートアクセスツールです。これらの正規のツールが非合法な目的に転用されることが多くなっており、防御側の組織はこれらのツールが不自然に利用されているケースや、攻撃が疑われる兆候を常に監視しなければなりません。

リモートアクセスツールは、侵害したシステムで持続的な接続を確立し、新たな攻撃を仕掛けるために使用されます。代表的なリモートアクセスツールには、以下があります。

- NetSupport Manager (NetSupport)
- TeamViewer リモートアクセス (TeamViewer)
- ConnectWise Control / Screenconnect Remote Access (ConnectWise)
- AnyDesk (AnyDesk Software)
- Atera (Atera Networks)
- Radmin (Famatech)
- Remote Utilities (Remote Utilities)
- Action1 RMM (Action1)

これらのツールは、攻撃者によって展開されることもあれば、侵害したネットワークへの持続的なアクセスを販売しているアクセスブローカーによって展開されることもあります。これらのツールを使用してセキュリティが侵害された組織にアクセスするよう、地下マーケットで公然と勧誘しているサイバー犯罪者もいます。

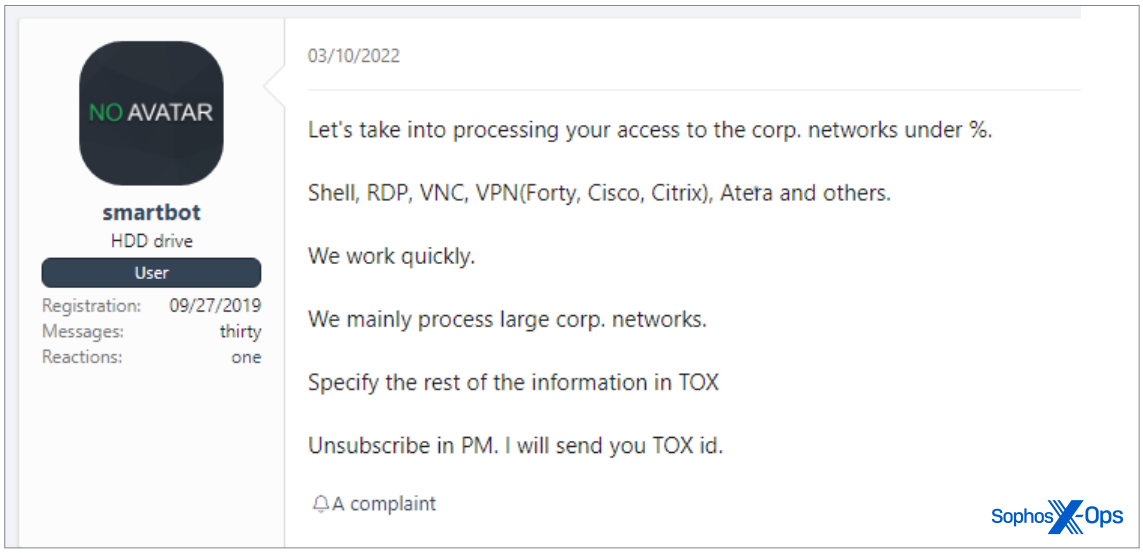

図 33. 侵害された正規のツールが、ネットワークへのアクセスに利用されている。

Atera は、Log4J の脆弱性を悪用してマルウェアを展開する攻撃や Sophos Rapid Response が調査したいくつものランサムウェアの事案など、ソフォスが調査した複数の侵入の試みで検出されています。VMWare Horizon サーバーを狙った Log4J エクスプロイトによる攻撃では、リモートで PowerShell スクリプトを実行し、トライアル版のライセンスを使用して、Atera エージェントを秘密裏にダウンロードしてインストールしようとしていました。このケースでは、別の正規のリモートアクセスツールである Splashtop Streamer も一緒にインストールしようとしていました。Rapid Response が担当したインシデントでは、脆弱な Microsoft Exchange Server が悪用されて、Atera がインストールされていました。また、Rapid Response が調査した最近のインシデントでは、BlackCat ランサムウェアが TeamViewer と AnyDesk を悪用しています。

多くの場合、これらの正規のツールの悪用は、たとえば、NetSupport のバージョンが PowerShell によって通常とは異なるディレクトリにインストールされるなど、不審なコンテキストとして検出およびブロックされることがあります。さらに、トライアル版のライセンスが展開に使用されていることから、これらのツールが悪用されていることを検出できるケースもあります。ソフォスは、Atera のトライアル版ライセンスの不正使用を検出する動作ルールを導入しています。このパッケージや他のリモートアクセスパッケージの不正使用に対する動作検出ルールの開発を今後も続けていきます。

LOLBin と正規の実行ファイル

サイバー犯罪者による進行中の攻撃や、完全に自動化されている攻撃の大きな特徴は、「環境寄生型バイナリ (LOLBin)」が使用されていることです。これらのネイティブの Windows コンポーネントは攻撃者により、システムコマンドの実行、セキュリティ機能の回避、リモートからの悪意のあるファイルのダウンロードと実行、ネットワークでのラテラルムーブメントに利用されています。

Windows コマンドシェル (cmd.exe) は、代表的な LOLBin です。多くのバックドアやシェルがシステムコマンドの実行やマルウェアの起動にこのコマンドシェルを使用しており、何らかの形で実質的にすべてのマルウェア攻撃に介在しています。PowerShell、Microsoft HTML アプリケーションホスト (mshta.exe)、Windows Scripting Host (wscript.exe) の Windows の各スクリプトプラットフォームは、Windows API コールの実行、他の悪意のあるコンテンツのダウンロードと実行、システムコマンドの実行、データ収集ツールとして使用されています。また、PowerShell は、サイバー犯罪者の攻撃ツールでも多用されています。

Rundll32.exe もランサムウェアで悪用されることが多い Windows コンポーネントの 1 つであり、ダイナミックリンクライブラリ (DLL) 形式でドロップされるマルウェアをロードするために頻繁に使用されています。同じように悪用され、バックドアやランサムウェアを実行するために持ち込まれる署名付きの正規の実行ファイルも他に存在します。

攻撃であるかどうかが曖昧な LOLBin もあります。リモートの Web サーバーからコンテンツを取得する Windows の証明書ユーティリティ (certutil.exe) は、ランサムウェアオペレーターなどのサイバー犯罪者が悪意のあるファイルをダウンロードして復号化するために頻繁に悪用されています。Bitsadmin.exe は、バックグラウンドインテリジェント転送サービスのコマンドラインユーティリティであり、転送を開始したプロセスを稼働させたまま、標的ネットワークとの間でファイルを移動させるために使用されています。これは、マルウェアのラテラルムーブメントやデータの外部送信を実行するときに好都合のツールになっています。

これらの動作は、さまざまな方法で検知してブロックできます。PowerShell や他のスクリプトエンジンを使用する悪意のある挙動は、マイクロソフトのマルウェア対策スキャンインターフェイス (AMSI) を監視して検出できます。また、システムコールやコマンドラインから LOLBins を実行する挙動を解析して、このような不正を検出することも可能です。

感染したコンピュータで利用されていたの割合が高い LOLBin トップ 10		
LOLBin	**検出数に対する割合**	**注**
cmd	92.26%	デフォルトのコマンドインタプリタ
powershell	1.79%	高度なコマンドラインとシェルスクリプト
certutil	1.09%	証明書サービスの一部としてインストールされるコマンドラインプログラム
mshta	1.01%	Microsoft HTML アプリケーションホスト。.HTA (HTML アプリケーション) の実行を許可します。
bitsadmit	0.95%	バックグラウンドインテリジェント転送サービス。Windows Update の一部としてファイル転送に使用されます。
wscript	0.93%	JScript と VBScript の実行をサポートする Windows Script Host
bcdedit	0.83%	ブート構成データを管理するコマンドラインツール
rundll32	0.52%	32 ビットのダイナミックリンクライブラリ (DLL) をロードして実行するために使用されます。
nltest	0.39%	診断情報を提供するツール
procdump	0.21%	システムプロセスに関する情報を提供するコマンドラインアプリケーション

図 34. Windows システムでは、cmd.exe がさまざまな目的に利用されており、LOLBin の対象として悪用されるケースが圧倒的に多い (2022 年 4 月～9 月)。 Sophos X-Ops

脆弱性の意図的な持ち込み

LOLBins 以外にも、ランサムウェア攻撃やその他のサイバー犯罪の一部として、正規の実行ファイルが使用されることが多くあります。悪用されるアプリケーションが攻撃者によって意図的に持ち込まれる場合もあります。脆弱な実行ファイルが持ち込まれ、悪意のあるコードをサイドローディングするために使用されるケースもあります。昨年、AtomSilo ランサムウェアの攻撃では、McAfee の署名が付けられた古いコンポーネントが使用され、Cobalt Strike のバックドアが展開されています。

「Bring Your Own Vulnerable Driver (独自のドライバの持ち込み)」という似た手法もあります。これは、悪用可能な脆弱性がある正規の署名付きドライバを利用して、オペレーティングシステムへの下位レベルのアクセス権限を取得する手法です。たとえば、ソフォスの研究者は BlackByte ランサムウェアを展開するサイバー犯罪者が、広く使用されているグラフィックカードである Micro-Star MSI AfterBurner 4.6.2.15658 のオーバークロックユーティリティが使用するドライバ RTCore64.sys および RTCore32.sys を悪用していることを特定しました。これらのドライバには CVE-2019-16098 の脆弱性が存在し、認証されたユーザーであればメモリを自由に読み取り / 書き込みできるようになります。ソフォスが検出したケースでは、一部のセキュリティソフトウェアを迂回および無効化するためにこれらのドライバが使用されていました。

脆弱なドライバが持ち込まれた最近のインシデントとしては、7 月にゲーム「原神」の脆弱なチート対策用のドライバが悪用されたケースがありますが、この攻撃者は明らかになっていません。5 月には Avast の脆弱なルートキット対策ドライバを悪用するランサムウェアの亜種が報告されています。両方のケースで脆弱なドライバが攻撃されており、セキュリティソフトを回避したり停止したりしていました。ソフォスの

Rapid Response チームは、システム環境におけるランサムウェア攻撃を示す兆候を慎重に観察し、警告しています。2022 年 1 ～ 9 月に対応したインシデントの調査では、少なくとも 83% のランサムウェア攻撃で、何らかの攻撃の兆候が見られていました。ランサムウェア攻撃の兆候として、MITRE ATT&CK の分類で最も多かったのは、以下の 5 つです。

- T1003 – 認証情報へのアクセス - OS 認証情報のダンプ
  - 平文またはハッシュ化された認証情報をダンプし、標的のオペレーティングシステムやソフトウェアからアカウントログイン情報や認証情報を取得します。
- T1562 – 防衛回避 - 防御策の妨害
  - 標的となった組織の環境のコンポーネントを変更または無効化し、予防措置および監査 / ログ機能を含む既存の防御策を回避または減退させます。
- T1055 – 権限昇格 - プロセスインジェクション
  - 信頼されるプロセスのアドレス空間にコードを挿入し、攻撃者コードが防御策を回避し、権限を昇格できるようにします。
- T1021 – ラテラルムーブメント - リモートサービス
  - 有効で保護されていないアカウントからリモートサービスを利用し、システムにログインして、先に説明した攻撃のために転用された RAT を使用して、ログオンユーザーとして操作を実行します。
- T1059 – 実行 - 一般的なインタープリタおよびスクリプトインタープリタ
  - コマンドやスクリプトのインタープリタを悪用してコマンド、スクリプト、およびバイナリを実行したり、対話型ターミナルやシェル、または上記のようなリモートサービスからこれらを実行したりします。

他にも、MITRE ATT&CK のカテゴリには明確に分類できませんが、セキュリティ担当者が注意すべきパターンがいくつか見つかっています。

- ランサムウェア攻撃の 64% (具体的にはランサムウェアの展開) が、現地時間の午後 10 時から午前 6 時の間に開始されています。
- 攻撃が開始された時間帯は、月曜日の夜から火曜日の朝 (夜勤型) が最多になっています。
- ランサムウェアによって身代金が要求される約 2 日前にデータが流出しています。
- 攻撃者が組織に侵入して滞在している平均期間は 11 日です。

エンドポイントセキュリティのアップグレードを標的とするランサムウェア

上記で説明したランサムウェア攻撃の兆候にある「T1562 - 防衛回避 - 防御策の妨害」は、さらに詳細に把握すべき重要な問題です。2022 年にソフォスの Rapid Response がランサムウェアの被害を阻止することに成功し、その成功がランサムウェア組織や提携者に認識されていることが最近の攻撃の傾向にも顕著に表れています。ランサムウェア攻撃では、ファイルを暗号化するマルウェアを展開する前段階として、システムのセキュリティ環境を制御する管理コンソールへのアクセスを試みることが一般的になっています。

前のセクションで説明したように、ランサムウェアの「アクティブアドバーサリ」、つまり実際にキーボードを操作してリアルタイムで操作する攻撃者は、管理者の認証情報を取得するためにパスワードの傍受やスクレイピングツールを日常的に使用しています。Mimikatz のようなユーティリティを使用すれば、攻撃対象のネットワークからユーザーのパスワードを傍受して抽出できます。

これらの管理者のパスワードを使用して、Windows ドメインコントローラーなどの管理ツールを乗っ取り、ランサムウェアを展開するケースは過去にありましたが、最近の攻撃では、これらの認証情報を使用して、エンドポイントセキュリティ製品の管理に使用される管理コンソールにアクセスするケースが増えています。場合によっては、攻撃者は窃取した認証情報を使用してすぐに管理ツールにログインし、エンドポイントセキュリティツールの改ざん防止機能を無効にしたり、場合によってはエンドポイントセキュリティを完全に無効にしたりするケースもあります。

このような攻撃を防止するため、ソフォスなどのセキュリティベンダーは、管理コンソールのログインページや、管理者がログインして設定を行うファイアウォールなどの物理デバイスに多要素認証 (MFA) 機能を追加しています。しかし、これらの製品を使用するセキュリティ管理者や IT 管理者は、脅威を阻止するために、これらの MFA の機能を有効にして使用する必要があります。ソフォスは、すべてのお客様がこれらの保護機能を速やかに有効にすることを推奨しています。

暗号通貨を採掘するマイニングマルウェア

クリプトマイニングソフトウェアは、新しい「コイン」(トークン) を獲得するために、暗号通貨の取引に必要となる複雑な計算処理を行います。通常、ネットワーク化されたプロセッサまたはマシンのプールがこの処理に参加します。多くの暗号通貨では、採掘を行うために、処理負荷の高い作業に特化したグラフィックス処理ユニットを搭載した専用のハードウェアが必要になります。しかし、一般的なハードウェアを悪用して暗号通貨を採掘する攻撃はまだ存在しており、脆弱なシステムを悪用し、その処理能力を無断で使用して利益を上げるために広大で自己拡散型の採掘ボットのネットワークを構築しています。

このようなマルウェアは、組織のデータには影響を与えませんが、コンピューティングリソースが消耗し、電気代や冷却費が増加します。マイニングマルウェアは、通常、簡単に悪用できるネットワークやソフトウェアの脆弱性を利用して展開されることが多いことから、他のマルウェアが悪用される兆候となることも多くあります。

マイニングマルウェアの多くは Monero (XMR) を採掘していますが、これにはいくつかの理由があります。XMR を採掘するためには、必ずしも専用のグラフィックスカードが必要ではなく、グラフィックスハードウェアを搭載していないサーバーでも採掘が可能です。また、XMR は他の多くの暗号通貨に比べて追跡が困難であることから、犯罪者にとって魅力的な暗号通貨になっています。

マイニングボットは、新しく公開された脆弱性を最初に悪用するマルウェアであることが多くあります。Java の脆弱性である Log4J と Microsoft Exchange Server の ProxyLogon/ProxyShell のエクスプロイトは、いち早くマイニングボットネットで利用されました。ソフォスの Rapid Response が対応したランサムウェアの多くの事例では、ランサムウェアと同じ最初の侵入口をマイニングマルウェアが使用している証拠が発見されています。ランサムウェア攻撃の数ヶ月前にマイニングマルウェアによって侵入されている事例もあります。

また、マイニングマルウェアは、さまざまなプラットフォームを標的としています。ソフォスが検出している多くのマイニングマルウェアのボットは、PowerShell などの Windows スクリプトエンジンを利用してインストールし、システムに常駐して Windows システムを攻撃していますが、Linux を攻撃するボットネットも存在します。多くの場合、パッチが適用されていない Linux のネットワークアプライアンスや Web サーバーが標的になっています。

XMR を採掘するマイニングマルウェアは依然として広く悪用されていますが、多くの暗号通貨が急落したことが、マイニングマルウェアのオペレーターにも影響を与えています。XMR の価値が下落するにつれ、マイニングマルウェアのボットネットの収益性が低下しており、ボットのオペレーターがマイニングボットを拡散する意欲に影響を及ぼしていると考えられます。XMR の価値の変動に追随するように、展開されたマイニングマルウェアの検出率も以下のように変動しています。特に 6 月中旬は XMR の価値とマイニングマルウェアの検出数ともに急減しています。

2022 年 4 月から 9 月までの Monero マイニングマルウェアの検出と価格変動

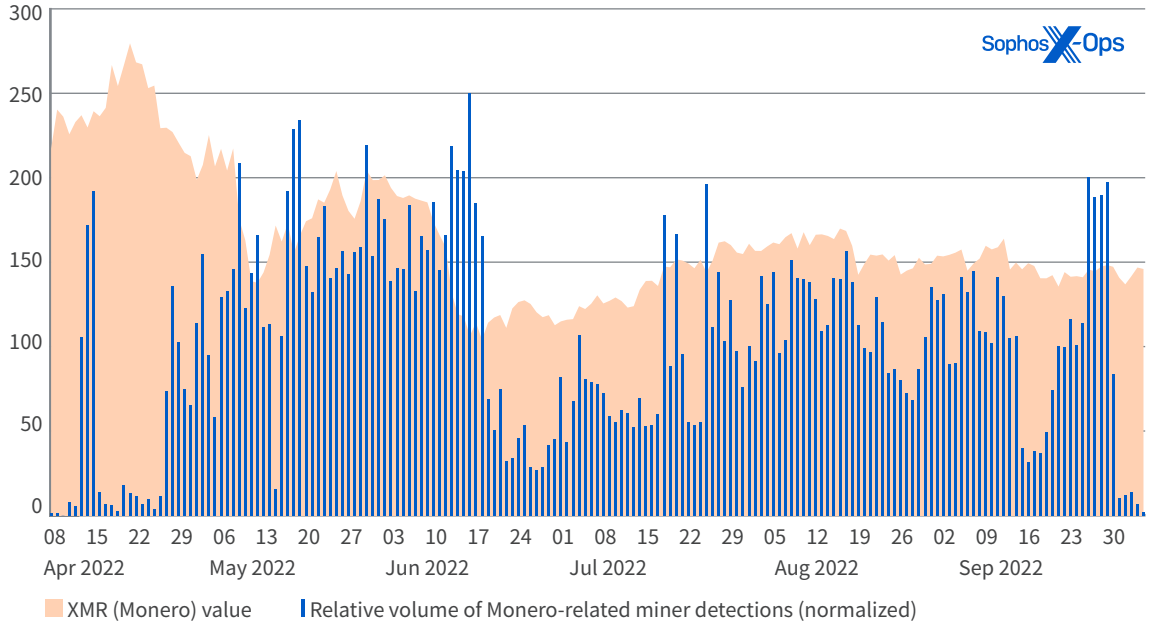

図35. 過去 1 年間の Monero を採掘するマルウェアの検出数 (青色、縮尺のため合計数が正規化されています) は、その期間の Monero の価値 (オレンジ色) とある程度一致している。

しかし、マイニングマルウェアを操る攻撃者の収益は、採掘する暗号通貨の価値だけでなく、マイニングマルウェアがどれだけ長期的に活動できるかにも影響されます。マイニングマルウェアを利用する多くの攻撃者は、自分のマイニングマルウェアをインストールしたサーバーから同様の攻撃者を探し出し、排除しています。また、これらの攻撃者は、他のマイニングマルウェアがインストールされることがないように、マルウェアをインストールするために使用した脆弱性を修正するパッチを適用し、組織が脆弱なシステムをスキャンした場合でも、採掘を継続できるようにしているケースもあります。

Windows だけが狙われていた時代の終わり：Linux、Mac、モバイルの脅威環境

このレポートでは、多くの攻撃者の標的となっている Windows に影響するマルウェアや攻撃ツールを中心に説明してきました。しかし、企業で標的となるプラットフォームは Windows だけではありません。複数のプラットフォームに対応するペイロードを使用する攻撃キャンペーンが増加しています。これらの攻撃キャンペーンは、Go や Python などのマルチプラットフォーム対応の言語 (多くの場合 pyinstaller でラップされています) や Electron などのフレームワークを使用しているか、主要なフレームワークのバイナリを準備して構築されています。本レポートの最後のセクションでは、Linux、Mac、およびモバイルプラットフォームの脅威について簡単に説明します。

Linux の脅威

Linux システムは、組織の Web サイト、仮想マシンサーバー、ネットワークアプライアンス、ストレージサーバー、エンタープライズアプリケーションのインフラストラクチャなどのサービスに展開されることが多く、長い間利用されています。犯罪者は、複数のプラットフォームを攻撃できるランサムウェアやその他のマルウェアを開発しており、これらの Linux システムのリソースも攻撃して利益を得るようになっています。ソフォスが Linux 向けの保護機能を発表してから半年間で、ランサムウェアの標的となった Linux サーバーを 14 台検出しています。

Linux システム (および他のサーバープラットフォーム) に影響を及ぼすマルウェアの多くは、暗号通貨の採掘を目的として構築されています。ソフォスの検出したすべてのマルウェアの 40% 以上、マルウェアが検出された Linux デバイスの 72% は、マイニングマルウェアが占めています。

Linux で検出された脅威の割合

脅威	検出率	注
マイニングマルウェア	43.0%	一般的なマイニングマルウェアの検出
DDoS	27.1%	Mirai 関連の検出
Tsunami	12.3%	IRC ベースの DDoS クライアント
Gognt	11.5%	Go で記述されたマルウェア全般の検出
Rst	1.3%	20 年前のファイルに感染するウイルス
Loit	1.1%	ローカルエクスプロイト
Swrort	0.9%	Linux 版の Mettle (Meterpreter の実装)
SSHDoor	0.7%	SSH バックドア
XpMmap	0.6%	メモリ関連のエクスプロイト
DrtyCoW	0.6%	Dirty COW (CVE-2016-5195) エクスプロイト
ProcHid	0.4%	プロセスを隠ぺいするトロイの木馬
Ngioweb	0.2%	プロキシボットネット
Psdon	0.1%	Mythic レッドチームフレームワークの Poseidon エージェント
GoScan	0.1%	脆弱なマシンを探す Go スキャナ

図 36. 2022 年の暗号通貨を取り巻く環境は混沌としているが、残念ながら、マイニングマルウェアは Linux 環境で確実に広がっている。

今年の Linux で検出されたマルウェアの中ではマイニングマルウェアは大きな割合を占めており、このグラフのデータよりも圧倒的な存在感を示しています。図の「Miner」は、ソフォスが検出したマイニングマルウェア全般を示しています。しかし、別のカテゴリでもマイニングマルウェアが検出されている場合があります。たとえば、「Gognt」は、Go で記述されたマルウェアの検出結果です。つまり、この表で「Miner」として検出されている以外にも実際には多くのマイニングマルウェアが検出されている可能性があります。

Linux で検出された脅威の割合 (ユニークマシンを基準とする)		
脅威	ユニークマシンの割合	注
マイニングマルウェア	74.3%	一般的なマイニングマルウェアの検出
Gognt	5.1%	Go で記述されたマルウェアファミリー全般の検出
DDoS	4.3%	Mirai 関連の検出
Swrort	3.2%	Linux 版の Mettle (Meterpreter の実装)
DrtyCoW	3.1%	Dirty COW (CVE-2016-5195) エクスプロイト
Ngioweb	2.8%	プロキシボットネット
Tsunami	2.7%	IRC ベースの DDoS クライアント
Roopre	0.9%	Web サーバーを標的とするバックドア
SSHBrut	0.9%	SSH ブルートフォースパスワードクラッカー
Loit	0.8%	ローカルエクスプロイト
Shell	0.8%	攻撃者によるシェルアクセスを可能にするマルウェア
Bckdr	0.6%	一般的なバックドアの検出
Ransm	0.6%	ランサムウェア

図 37. 影響を受けたユニークマシン別にみると、Linux 環境におけるマイニングマルウェアの影響がより明確になる。

侵害された Linux システムで検出されたマルウェアとしてマイニングマルウェアの次に多いグループは、Gognt と分散型サービス拒否 (DDoS) ツールキットに関連するマルウェアです。これらのマルウェアで悪用されているほぼすべての脆弱性は、Linux の最新バージョンで解決されていますが、相当数のデバイスやアプライアンスに未だにパッチが適用されないままとなっています。

他の重要な Linux の脅威には、いくつかのバックドアやボットネットがあります。しかし、企業から見た場合、Linux プラットフォームに対する他の上位の脅威の中で最も注意が必要なのは、長年にわたって活動している Linux バックドアであり、最近では Jenkins と WebLogic アプリケーションサーバーを標的として進化している Tsunami です。

Mac の脅威

2022 年には、macOS に対応するオープンソースの攻撃ツールやポストエクスプロイト /C2 フレームワークが GitHub などで多く見つかっています。リポジトリにコードが存在するだけで Mac への大規模な攻撃が発生することを示唆するものではありませんが、少なくとも Mac への攻撃への関心が高まっていることは間違いないでしょう。

macOS プラットフォームの主要な脅威は引き続き、Apple の Safari ブラウザ (および他のブラウザ) 向けのプラグインをインストールするアプリなどの、PUA (不要と思われるアプリケーション) です。これらのアプリは、Web ページにコンテンツを挿入して、不正または悪意のあるコンテンツにユーザーをリダイレクトします。

macOS の PUA（不要と思われるアプリケーション）、2022 年 4 月～ 9 月		
検出	**ユニークマシンの割合**	**注**
Adloadr	16.2%	一般的なアドウェアの検出
Genieo	8.9%	ブラウザ (検索) ハイジャック
Bundlore	8.4%	アドウェア
Dynji	4.6%	ブラウザ (ツールバー) のハイジャック
Pirrit	3.7%	アドウェア
アドマック	3.2%	アドウェア
HistColl	3.0%	ブラウザデータの収集
Keygen	2.3%	ソフトウェア著作権侵害ツール

図 38. Adloadr の検出は、2022 年の Mac PUA のリストで、2 位に大きな差を付けている。

Adloadr アプリケーションは、アドウェアとしての特徴があり、拡散している PUA の 1 つであり、2022 年の Mac テレメトリの統計で 2 位となったブラウザをハイジャックする Genieo の約 2 倍の感染数 (ユニークなマシンを基準とした感染) を記録して第一位になりました。

マルウェアに目を向けると、NukeSped、VSearch、Dwnldr (それぞれ、リモートアクセスのためのトロイの木馬、アドウェアパッケージ、多目的のダウンローダー型のトロイの木馬) の検出が多く確認されています。Adloadr ファミリーに関連する 2 つのヘルパーアプリである Chropex と ProxAgnt も、多く検出されています。

macOS でのマルウェア検出数、2022 年 4 月～ 9 月		
検出	**ユニークマシンの割合**	**注**
NukeSped	22.2%	リモートアクセスを可能にするトロイの木馬
VSearch	15.6%	アドウェア / ブラウザハイジャック
Dwnldr	10.8%	一般的なトロイの木馬の検出
Agent	10.8%	一般的なマルウェアの検出
Keygen	6.4%	コピープロテクトを回避するキージェネレーター
FkCodec	6.2%	アドウェア。ビデオコーデックのインストーラを偽装
Chropex	5.0%	アドウェア。ブラウザをハイジャックする場合もあり
ProxAgnt	1.9%	トロイの木馬
Swrort	1.5%	リモートアクセスを可能にするトロイの木馬

図 39. NukeSped、VSearch、Dwnldr が macOS で検出されるマルウェアのリストで上位を占める。

ソフォスは、10 月までに 2022 年に登場した新しい macOS の脅威を 5 つ発見しています。これらの脅威は macOS マルウェアの上位リストには入っていませんがその詳細をお伝えします。

2022 年に新たに検出された macOS の脅威			
月	名前	検出	注
1 月	SysJoker	OSX/SysJoker	macOS に対応するマルチプラットフォームバックドア
1 月	DazzleSpy	OSX/DazzleSpy	香港の民主化を推進する運動家を標的とするバックドア「MACMA」と関連する感染手法
3 月	Gimmick	OSX/Gimmick	Google Drive API 経由で通信し、監視システムからネットワークトラフィックを隠蔽。
5 月	pymafka/CrateDepression	Troj/Pymaf、OSX/Cobalt	pypi でホストされているパッケージへのサプライチェーン攻撃、最終的に Cobalt Strike ビーコンをドロップ
10 月	Alchimist	Exp/20214034-D	Go で記述されたマルチプラットフォームに対応する攻撃フレームワーク

図 40. 2022 年の最初の 10 ヶ月間で、5 つの新しい macOS の脅威が出現した。

モバイルの脅威

モバイルアプリケーションは、インターネットを利用する主要な方法となっており、モバイルデバイスは、新しいタイプのサイバー犯罪が急成長している場所にもなっています。Android プラットフォームには、偽のアプリケーションや情報窃取型マルウェアが依然として多く存在します。しかし、Android と iOS の両方が、不正な偽のアプリケーションの標的となるケースが増えており、サイバー犯罪者は、ソーシャルエンジニアリングの手法を使用して、Apple のモバイルデバイスのウォールドガーデンにも侵入する方法を見つけています。

マルウェアインジェクター、スパイウェア、バンキングマルウェアは、偽の広告クリックを生成するアプリとともに、依然として悪意のある Android の APK パッケージの検出数でトップを占めています。しかし、ユーザーから「アプリ内課金」を秘密裏に収集する手段としてのみ機能するアプリケーションなど、PUA (不要と思われるアプリケーション) はモバイルユーザーを脅かす存在としてその存在感を増しています。そして昨年は、偽アプリを使用する巧妙な金融詐欺集団が出現し、東南アジアで 1 つのビジネスとして確立されるようになりました。

ソフォスは 2021 年に組織的な犯罪キャンペーンの追跡を開始し、このキャンペーンを CryptoRom と命名しました。このキャンペーンは、「杀猪盘」と呼ばれるサイバー詐欺の一種であり、詐欺用の Web やアプリケーションの開発者、偽のソーシャルプロファイルの作成者、ソーシャルメディアや出会い系アプリを介して、特定のシナリオによるソーシャルエンジニアリングによって詐欺行為を行う組織的なシンジケートによって実施されています。

2021 年 10 月、ソフォスは、このキャンペーンがグローバルに展開していることを報告しています。このキャンペーンの手法は、暗号通貨への偽の投資詐欺から、偽の暗号資産を用いたデリバティブ取引、そして別の偽金融マーケットへと変遷し、変異を繰り返しています。これらの詐欺の手口は、正規の金融機関を装った偽のアプリケーションやモバイル Web サイトを作成し、正規の金融機関に見せかけるものです。これらのアプリの多くは、Apple App Store や Google Play ストアで見つかった「流動性マイニング」アプリのように、アプリストアに検出されずに紛れ込んでいます。

一方、詐欺師は iOS も悪用する方法を見つけ、Web クリップやアプリケーション開発者のテストデプロイプログラムを活用して、開発した不正なアプリケーションを iOS デバイスに取り込むことに成功しています。これらの方法には、Apple のアドホック配布方式を悪用し、「Super Signature サービス」と呼ばれる手順を使用するものや、ベータテストツールである「Test Flight」の利用、App Store のセキュリティ審査を回避するエンタープライズアプリケーション向けのスキームを利用するものがあります。iOS を標的とする他のマルウェアでも同様の手法が用いられている可能性がありますが、インストールを許可するためには、何らかのソーシャルエンジニアリングが必要となります。

これらのアプリケーションによる被害額は数億ドルに達しており、ロマンス詐欺から、Facebook、Twitter、LinkedIn などのプラットフォームで広範なソーシャルエンジニアリングを試みるものまで、拡大し続けるサイバー犯罪のエコシステムの一部になっています。詐欺は進化し続けています。犯罪組織は手法を模倣しながら、それぞれ独自の工夫を凝らしています。

また、Android と iOS の両方が、システムからの警告のように見せかけた悪意のある広告キャンペーンの標的になっています。多くの場合、ユーザーをアプリストアに誘導して、ユーザーが気づかないうちに、サブスクリプション料金を支払わせる、また、他のマルウェアをインストールする、あるいはその両方を行うアプリケーションを購入させています。

ソフォスは、これらの脅威をブロックする方法について継続的に取り組んでおり、アプリストアにおける不正な行為が新たに発見された場合には、モバイル OS の開発元に注意喚起しています。

まとめ

現在の脅威を俯瞰したときに最も注意しなければならないことが 2 つあります。1 つは、誰でも簡単にサイバー犯罪に手を染めることができるようになっていること、そして、かつては高度な APT グループが使用していたツールや戦術がコモディティ化していることです。ハッキングツールやマルウェア、脆弱なネットワークへのアクセス情報を売買するマーケットは以前から存在し活況を呈していましたが、ランサムウェア組織や資金力のあるサイバー犯罪組織の最近の活動を観察していると、犯罪者のコミュニティが急速に広がっており、防御策を回避するように設計された商用セキュリティツールの攻撃への転用も進んでいることが分かります。

地政学的なさまざまな状況から、サイバー犯罪との戦いがより困難になっています。今年、中国は米中関係が緊迫化する中で、サイバー犯罪対策における米国司法当局との協力を打ち切っています。一方、中国政府は国内の暗号通貨詐欺などのサイバー犯罪の取り締まりを強化したため、中国の犯罪者はこれらの犯罪行為の標的を海外の組織へと急速に移行しています。また、ロシアとウクライナの戦争により、一時的にロシア語圏の犯罪組織の活動が中断されましたが、すぐに再開されています。

これらすべての脅威を確実な防止する方策はありません。侵入による被害を防ぐためには、積極的な防御が求められますが、多くの組織に、防御にかかるコストの負担が重く圧し掛かっています。ソフォスは、エンドポイントやネットワークの防御、マネージド型のセキュリティオペレーションサービスを提供し、絶えず進化する脅威に対して、あらゆる規模の組織を保護できるように、今後も機能を強化する取り組みを進めていきます。

ソフォス株式会社営業部
sales@sophos.co.jp

22-11-17 EN (NP)

SOPHOS