CONFIDENTIAL

KELA インテリジェンス
レポート

Conti から流出した内部データの分析

2022 年 3 月 15 日

エグゼクティブサマリー

ランサムウエアグループ Conti が、ロシアのウクライナ侵攻を支持する声明を発表しました。これを受けて 2022 年 2 月 27 日、ウクライナ人研究者と思われる人物が、同グループのメンバー間で交わされたやり取りをリークしました。KELA はこのグループの進化と TTP（戦術、技術、手順）、組織体制を理解するべく、このリーク情報を分析しました。

主な調査結果：

- リークされたグループ内のやり取りから、**当初は特定のランサムウエアグループに所属していなかったランサムウエア攻撃者たちの集団が進化していった**流れが明らかとなりました。彼らは様々なランサムウエアを扱っており、Ryuk や Conti、Maze をそれぞれ別個のプロジェクトとして話し合っていました。そして彼らの活動が、最終的に現在の Conti のオペレーションを形成するにいたりました。
- Conti は様々なマルウエアやツールを使用していました。我々は、**Conti と TrickBot や Emotet、BazarBackdoor（初期アクセスを入手するために使用）に強いつながり**があったことを裏付ける証拠を発見しました。また**ランサムウエア Diavol は、Conti の「サイドプロジェクト（本業とは別のプロジェクト）であると思われます。**合法ツールについては、Conti が **VMware CarbonBlack や Sophos の製品をテストしようとしていたことが明らかとなりました。**
- Conti は、**初期アクセス・ブローカーのサービス**を利用して初期アクセスを入手していました。
- リークされた会話の中では、**約 100 の被害者（組織）が言及されていましたが、Conti のブログではその約半分が公開されていませんでした。**この点を調査する中で、ランサムウエア展開前後の様々なステップをはじめとする**攻撃プロセスが明らかとなりました。**
- Conti のメンバーは、**米国の公的セクターを攻撃することに興味を示していました。**
- Conti のグループは高度に組織化されており、**ハッカー、コーダー、テスター、リバースエンジニアリングスペシャリスト、クリプター、OSINT スペシャリスト、交渉者、IT サポート、HR** などのチームで構成されています。

- KELA は、**アクターの上位 15 人（やり取りされたメッセージの件数に基づく）に関する詳細な説明と、彼らの相関図**を作成しました。

背景

2022 年 2 月 25 日、ランサムウエアグループ Conti は、ロシアのウクライナ侵攻を支持することを宣言しました。その後の 2022 年 2 月 27 日、この宣言に反応してウクライナの研究者と思われる人物[1]が、Conti のメンバー間で交わされたグループ内のやり取りを Twitter アカウント「ContiLeaks」を使ってリークしました。リークされたやり取りには、以下の内容が含まれていました。

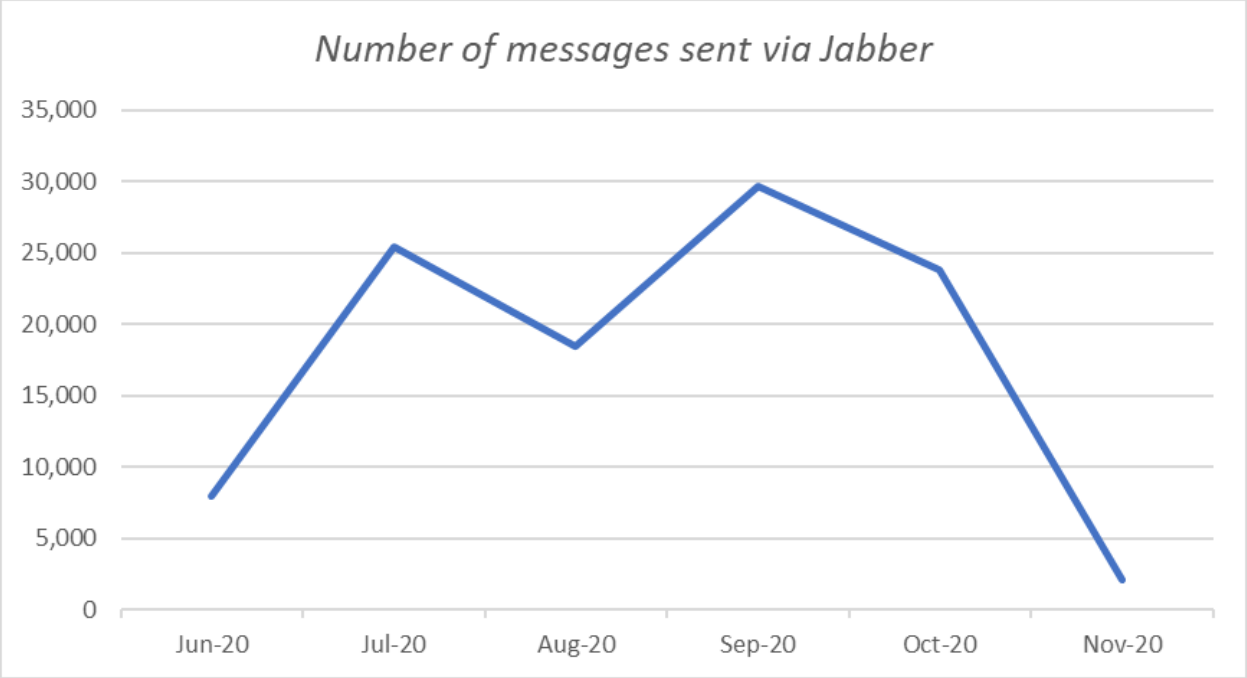
- Jabber のログ（ContiLeaks が複数に分けて Twitter に投稿）。この時投稿されたログは、q3mcco35auwcstmt[.]onion でホストされた Conti の Jabber サーバーから発信されたものと思われます。また Jabber を使って行われたチャットの大半は、各メンバーが他のメンバーと 1 対 1 でやり取りしていた個別チャットであると思われます。まず第 1 部には 2020 年 6 月 21 日から 2020 年 11 月 16 日までのメッセージが含まれており、第 2 部には一部空白期間があるものの、2021 年 1 月 29 日から 2022 年 2 月 27 日までのアーカイブが含まれていました。
- Rocket.Chat のログ（こちらも ContiLeaks によるリーク）。リークされたログは 6 台の Rocket.Chat サーバーから収集されており、2020 年 8 月 31 日から 2022 年 2 月 26 日までの情報が含まれていました[2]。

今回のレポートを作成するにあたり、我々は Jabber ログから抽出したアクターの会話を分析し、また Rocket.Chat のログの内容を一部使用して調査結果の裏付けを行いました。当初 Jabber は、当時展開中であった攻撃をはじめとするあらゆる類のやり取りに使用されていたものと思われます。しかし 2021 年が近づくにつれ、「技術的に関するやり取り（特定の企業に対する不正アクセスや、コーディング作業の割り振りなど）」が Rocket.Chat へと移

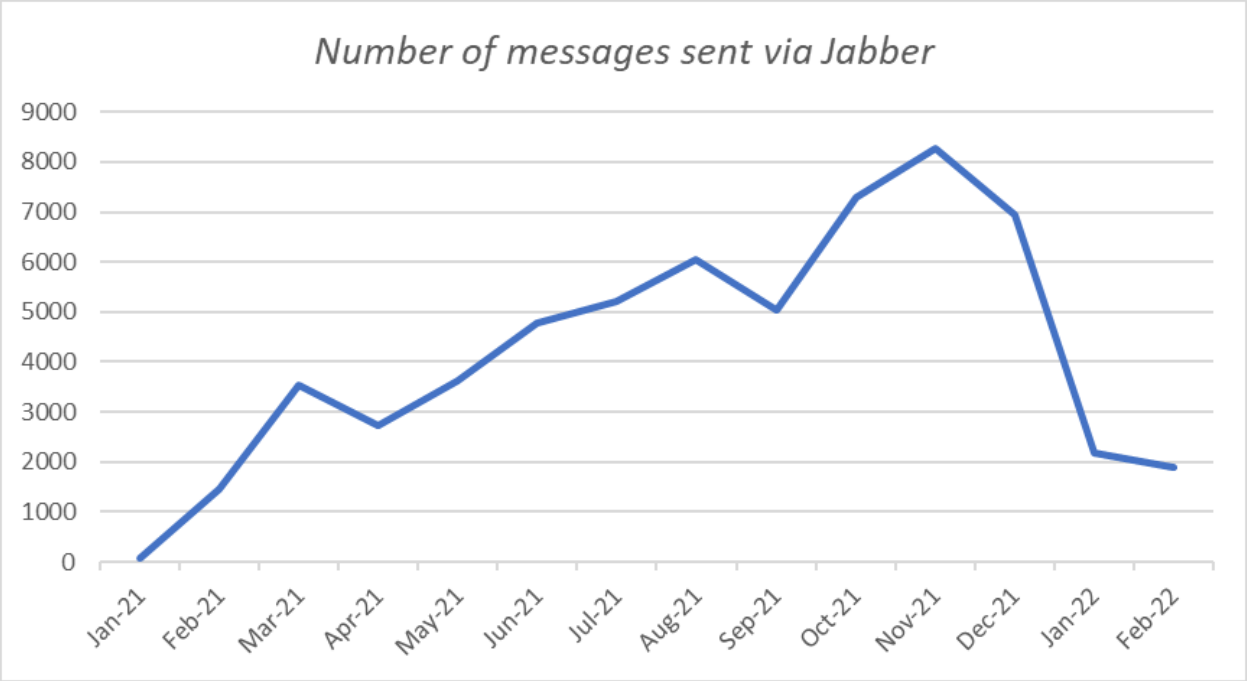
[1] https://www.databreachtoday.com/ukrainian-researcher-leaks-conti-ransomware-gang-data-a-18620
[2] DARKBEAST のクローラー：ContiJabberLeaks 及びクローラー；ContiRocketChat*でご確認いただけます。

行されるようになりました。我々はより多くの知見を得るため、引き続きこのリーク情報の分析を続けています。

また Twitter アカウント「Trickbotleaks」と「trickleaks（アカウント「Trickbotleaks」が禁止された後に登場した２つ目のアカウント）」からは、TrickBot のオペレーターとその関係者間のやり取りで発生したと思われる Jabber のログと、TrickBot のメンバーであるとされている 21 人の情報を含んだファイルがリークされました。我々がこのリークデータを分析した結果、その中のチャットデータと ContiLeaks によるリーク情報の一部が重複していることが明らかとなりました。そのため、本レポートでは TrickBot のリークデータも補足情報として活用しています。



2020 年 6 月 21 日から 2020 年 11 月 16 日のデータに基づく



2021 年 1 月 29 日から 2022 年 2 月 27 日のデータに基づく

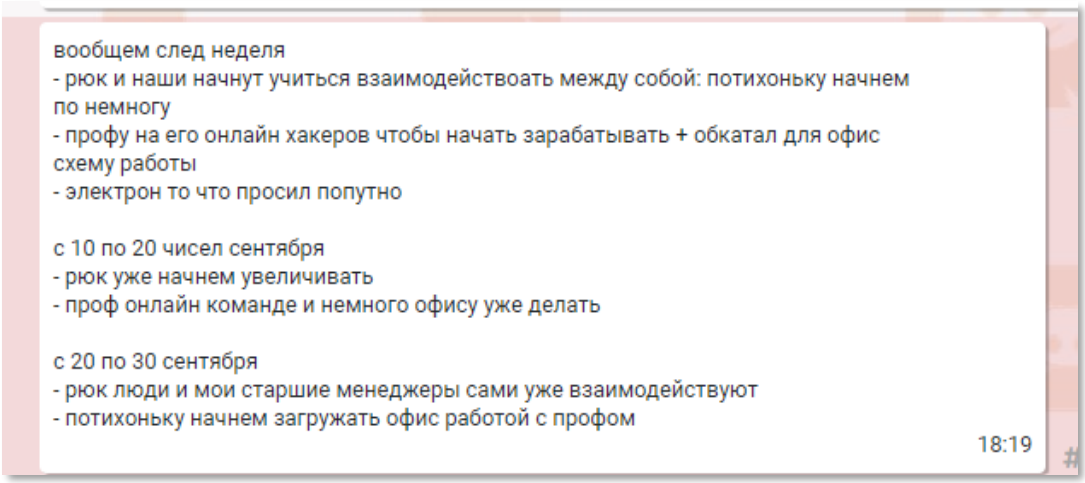
Conti の進化

かつて Conti は、ランサムウエアグループ「Ryuk」との共通点（両グループのコードに類似点があったことや、身代金メモに同じテンプレートを使用していたこと）から、Ryuk の後継者である可能性が疑われていました[3]。またブロックチェーン調査企業 Chainalysis も、「金銭面と運用面が実質的に一致していることを裏付けるブロックチェーンのトランザクション」が新たに確認されたと主張していました。これを示唆する一例として、Conti の上位メンバーの 1 人である stern が、Conti と Ryuk の両方からコミッションを受け取っていたことが挙げられます[4]。

しかし我々がデータを調査した結果、少なくとも一部のやり取りの中では、Ryuk はあくまで個別のプロジェクトとして語られていました。例えば、我々が観察したこの「グループ」が自分達独自のランサムウエアを開発していた時、アクター**stern** はオンライン上で Ryuke

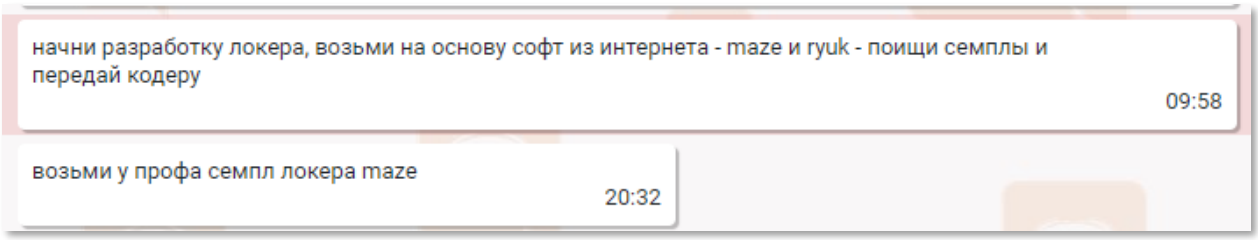
[3] https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/
[4] https://twitter.com/JBurnsKoven/status/1498679108812877824

のサンプルを見つけて利用するよう **buza** に提案していました。また、Ryuk と Conti の関係について混乱が生じるもうひとつの原因として、**рюк**（ryuk）と呼ばれるサイバー犯罪者の存在が挙げられます（この人物も攻撃者のチームを持っているとされています）。Conti のメンバーは рюк（ryuk）と交わした会話の内容を共有していますが、今回リークされた内容には рюкs（ryuk）からのメッセージが含まれていなかったことから、Conti のメンバーと рюк（ryuk）は、別のプラットフォームを介してやり取りを行っているものと思われます。なお、рюк（ryuk）がランサムウエア Ryuk とつながっている場合は、рюк（ryuk）と Ryuk のチームが実際に協力体制をとっており、最終的に団結している可能性があるものと思われます。ただし、рюк（ryuk）が単にランサムウエアグループ Ryuk と同じ名前を使っている個人であるという可能性も考えられます。

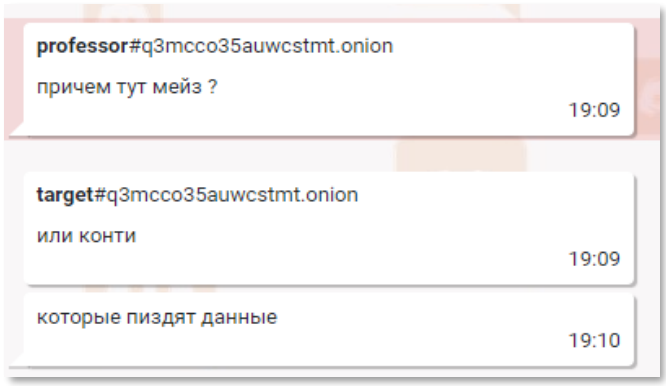


*2020 年 8 月 27 日：**target** が **stern** に対し、Conti と **ryuk** の「従業員」が 9 月から一緒に働くと告げているメッセージ*

リーク情報のうち最初の頃に交わされていたやり取りから、このグループのメンバーが Maze を使用していたことが明らかとなりました。Maze は別グループのランサムウエアの亜種ですが、彼らは独自のランサムウエアを開発するため、そして企業を攻撃するためという 2 つの目的で Maze を使用していました。また彼らは、2020 年から 2021 年初めにかけては Conti のことさえも別のプロジェクトとして説明しており、「自分達は独自のロッカー（ランサムウエアを指すスラング）」を使用していると発言していました。



*2020 年 7 月 9 日：**stern** が **buza** に「インターネットでソフトウエア（Maze と Ryuk）」のサンプルを探し、そのサンプルをベースにロッカーを開発するようコーダーに依頼するよう頼んでいるメッセージ*



*2020 年 10 月 9 日：**professor** と **target** が Maze と Conti を別々のオペレーションとして議論しているメッセージ*

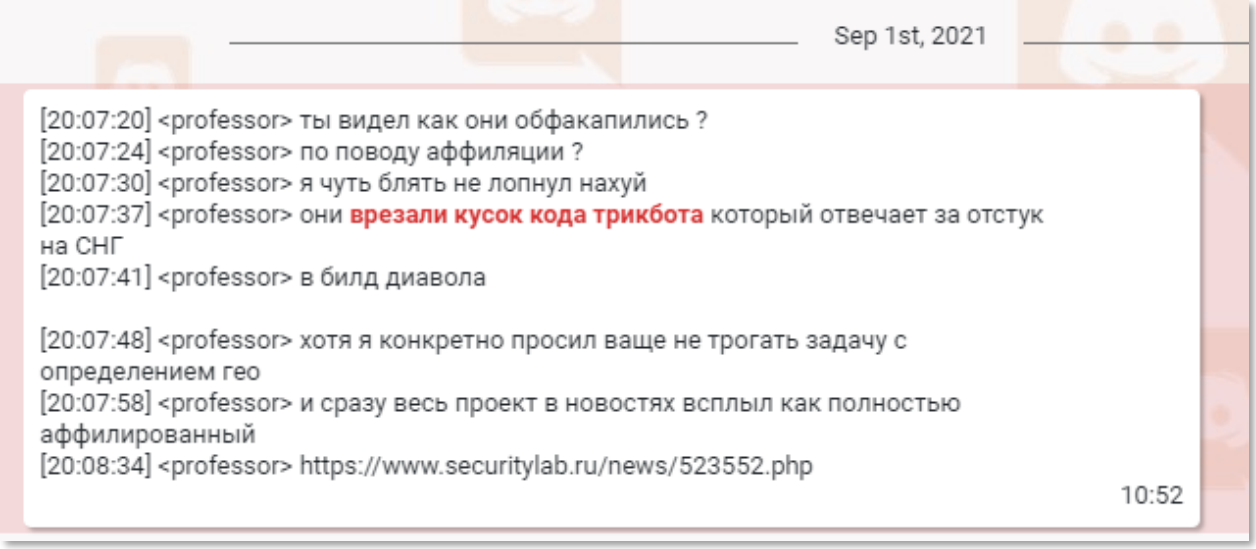
従って我々は、この Jabber サーバーは本来、「特定のランサムウエアグループのメンバーではないサイバー犯罪者たち」の集団に属していたものであると考えています。この集団のメンバーは様々なランサムウエアの亜種を使用し、他のサイバー犯罪者たちと連携していたようですが、そういった彼らの活動がやがて、近年その名を知られるようになった Conti のオペレーションを形成するにいたったものと思われます。また、初期の頃に活躍していたアクターの一部は、現在 Conti の上級マネージャーになっているようです。その一方で我々は、2021 年から 2022 年においても Conti グループ内の一部のアクターが複数のオペレーションに同時進行で携わっていることを示唆するメッセージや、Conti のことを第三者として言及しているメッセージも発見しています。

TTP（戦術・技術・手順）

マルウエアとツール

我々は、Conti が TrickBot や Emotet と強いつながりがあるという証拠を発見しました。TrickBot も Emotet も、サイバー犯罪者がランサムウエアを最初にインストールする際に利用する悪名高いマルウエアです。その他にも、今回のリークで確認された会話の中で、BazarBackdoor が企業のネットワークにリモートでアクセスするための手段のひとつとして言及されていました。

また Conti は、「baget」と呼ばれるユーザーが開発したランサムウエア Diavol を、サイドプロジェクトとして所有しているようです。



*2021 年 9 月 1 日：**professor** が「Diavol の開発者が TrickBot のコードの一部をランサムウエア（Diavol）のビルドの一部に使用した」と不満を述べているメッセージ（これにより Diavol と TrickBot が公に関連付けられました）*

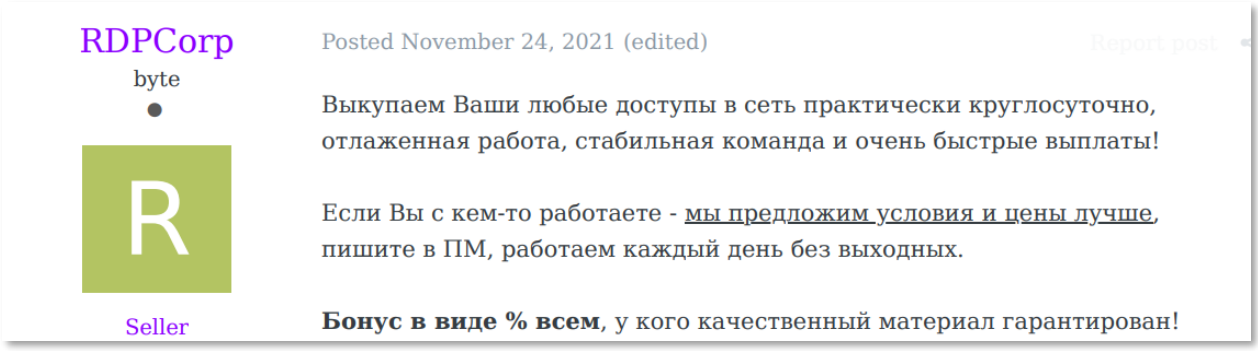
同グループは合法的なツールも広範に悪用しており、その一例として、彼らがセキュリティ企業 VMware CarbonBlack 社や Sophos 社とデモを設定して、2 社の製品をテストしようとしていたことが挙げられます。なお、少なくとも CarbonBlack 社については、彼らは同社から製品を購入することに成功しました。このような戦術をとることで、サイバー犯罪者は既存のセキュリティソリューションに対して自らのマルウエアと手法を実行し、それらのソリューションをいかに回避すべきかを学ぶことができるのです。

その他にも、ポストエクスプロイトツールの Cobalt Strike、資格情報を収集するオープンソースアプリケーションの Mimikatz、Metasploit や Poverview のフレームワーク、Cookie Grabber（もともとは TrickBot のモジュール）など、ランサムウエア攻撃者の間で人気のあるツールの一部が、このグループの武器として使用されていることが改めて確認されました。また彼らが特定の脆弱性（CVE-2020-5135：SonicWall 社の VPN 製品に存在するスタックベースのバッファーオーバーフロー）やゼロディ脆弱性のエクスプロイト、またそれらの脆弱性をスキャンするツールを購入・開発する方法について議論していることも確認されました。

初期アクセス・ブローカーとの連携

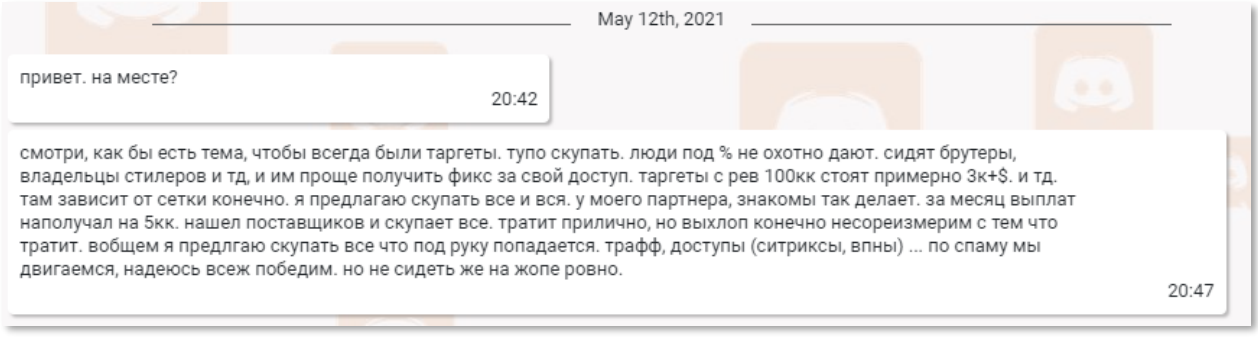
初期アクセス・ブローカー（IAB）[5]は、Conti のオペレーターにとって初期アクセスの供給元のひとつとなっています。Conti と連携している初期アクセス・ブローカーの大半は、身代金を一定の割合で受け取っているようです。リークで確認されたやり取りの一部から、ロシア語話者用サイバー犯罪フォーラム XSS や Exploit、RAMP で活動している某アクターと、Conti の間で行われた交渉が明らかになっています。このアクターは「rdpcorp_@thesecure[.]biz」という Jabber アカウントを使用しており、我々の調査の結果、XSS や Exploit で **RDPCorp** として活動しているユーザーとつながりがあることが確認されています。この RDPCorp と名乗るユーザーは、XSS や Exploit で「あらゆるネットワークアクセス」を定価で購入して Conti へ転売し、身代金の一部をその代金として受け取っていました。RDPCorp は Conti と「労働条件」を話し合う中で、ドメイン管理者権限を持つアクセスの場合は身代金の 35%、ユーザー権限のアクセスの場合は 15%を支払うよう要求していました。そして交渉の結果、Conti は非特権アクセスのみ購入することに合意していました。

[5] 初期アクセス・ブローカーは、不正アクセス先の組織が所有するコンピューターへのリモートアクセス（ネットワークへの初期アクセス）を販売しており、彼らの活動がネットワークへの侵入を著しく容易にしていると同時に、無作為に行われる場当たり的なキャンペーンを標的型攻撃につなげる役割を果たしています。ネットワークアクセスがランサムウエア攻撃に発展するまでの流れを 5 つの実例で解説した弊社ブログ「https://ke-la.com/ja/from-initial-access-to-ransomware-attack-5-real-cases-showing-the-path-from-start-to-end/」をご参照ください。



RDPCorp が Exploit に掲載した声明：「我々はどんなネットワークアクセスでもほぼ 24 時間週 7 日対応で買い取ります。我々には確立されたプロセスがあり、しっかりしたチームが迅速に支払い対応します！」

2021 年 5 月 12 日、**kevin** と名乗るアクターが、新たな戦略を採用し、利用できるすべてのネットワークアクセスを定価で購入するよう **stern** に持ちかけていました。この時 kevin は、「私のパートナーはそうしている人物を知っている。彼（その人物）は 1 カ月で 500 万米ドル（身代金：KELA 補足情報）を受け取った。彼は『サプライヤー』を見つけていて、そのサプライヤーたちからすべてのアクセスを購入している。彼の払っている額は大きいが、彼が得ている利益は払った額とは比べ物にならないほどだ」と発言していました。この提案の前後には、kevin が Conti のハッカーチームのために「標的を準備」しているところが観察されており、これは kevin が同チームに潜在被害者の初期アクセスを提供していたことを意味しています。



2021 年 5 月 12 日：利用できるネットワークアクセスをすべて購入するよう提案している kevin の投稿。「皆、歩合で売るのは好きじゃない。彼らの中にはブルートフォース攻撃を実行する奴やスティーラー（情報窃取型マルウエア）のオーナーがいるし、彼らにとってはアクセスの代金を定額で受け取る方が楽なんだ」

Conti による攻撃の分析

Conti のリークに関する調査で、我々は Conti から攻撃を受けたにもかかわらず、ブログで公開されなかった被害者（組織や企業）が 50 件以上存在することを発見しました。これらの被害者については、身代金を支払った可能性が非常に高いと考えられます[6]。また、リークされた会話の中に登場した被害者のうち 40 件超はブログに登場していますが、そのうちの一部の被害者も身代金を支払った後に投稿を削除されています。これまでに発見されて分析されてきた被害者は氷山の一角であると思われ、我々は Conti リークの分析を引き続き行ってゆく過程で、さらなる被害者が判明するものと予想しています。

Conti のメンバーが被害者について交わした会話から、以下の攻撃のプロセスが明らかとなりました。

1. ハッカーチームが企業のネットワークに不正アクセスし、ランサムウエアを配備し、データを窃取します。Rocket.Chat のログにあった「manuals_team_c」という名称のチャンネルからは、Conti が偵察からデータの抜き取りにいたるまでのプロセスで使用していた 16 のマニュアルの存在が明らかとなりました[7]。またこれらのマニュアルの一部は、かつて同グループから流出したマニュアルの一部と重複していました[8]。
2. OSINT チームが、今後被害者を脅迫する際に利用可能な情報（被害者の連絡先や上級管理職の情報など）を収集します。
3. OSINT チームと他のメンバーは、被害者から窃取したデータを分析し、パスワード保護されたフォルダやファイルにブルートフォース攻撃を試み、データをもとに Conti が被害者の名前を公開する「ネイミング＆シェイミング」ブログの投稿内容（非表示の投稿）を作成します。また、被害者企業の従業員やマネージャーに電話をかけて脅迫する際に使用できるレポートも作成します。

[6] Darkbeast のタグ："Conti leak" と カテゴリ："Ransom Event"でご確認いただけます。

[7] https://github.com/Res260/conti_202202_leak_procedures

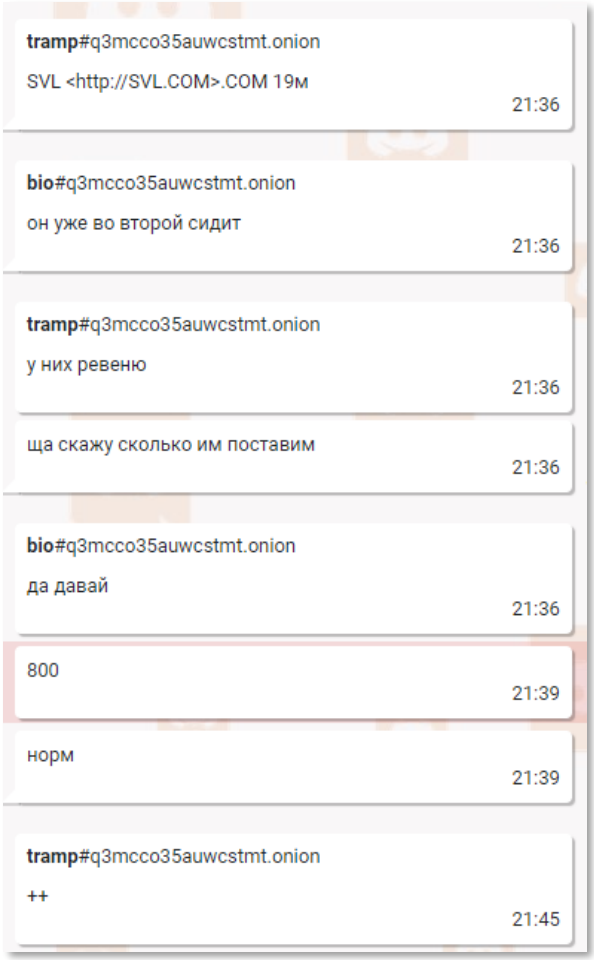
[8] 弊社は 2021 年 8 月 5 日、脅威アクターm1Geelka が、ランサムウエアグループ Conti のマニュアルであると主張してフォーラム XSS でファイルを公開したことを確認しました。m1Geelka は、Conti がアフィリエイトに対し月 1,500 米ドルを支払うと約束したにもかかわらず、速やかに支払いを行わなかったことに失望してこの行為に及んだものと思われます。

4. OSINT チームと交渉者が、ZoomInfo や D&B Hoovers などの企業データベースから被害者企業の収益情報を入手し、その情報をもとに身代金の額を決定します。
5. 交渉が行われます。ブログ投稿の作成担当者が被害者と交渉します。
6. 被害者が身代金の支払いに応じた場合は復号化ツールを提供しており、場合によってはネットワークへの不正アクセスの際に使用した方法に関するレポートも提供しています。ブログで情報を公開された後に被害者が身代金の支払いに応じた場合、ブログから投稿が削除されます。

その一例を挙げてみましょう。2021 年 12 月 12 日、暖房や換気、空調設備を提供する SVL 社（svl.com）が、被害者の 1 社として会話の中で言及されていました。その中でアクター **bio** と **tramp** は、同社の収益が約 1,900 万米ドルであると記載している ZoomInfo の情報をもとに、身代金を 80 万米ドルに設定することに同意しました。

その後彼らは交渉について話し合い、同社のマネージャーに圧力をかけるべく、電話をかけて脅迫しようとしていました。その際、**tramp** は **bio** に対し次のように依頼していました。「彼 [企業の交渉者宛て（KELA 補足）] に対し、あなたは私達と交渉するだけの資格がない、我々は会社の経営陣に毎日電話するつもりである、と書いてくれ。彼らが問題を起こしたくなければ、そして自社の従業員から訴えられたくなければとにかく身代金を支払うだろう」

その後の 2021 年 12 月 20 日、bio は SVL 社が 50 万ドルの支払いに同意したと述べており、同社は身代金を支払ったものと思われます。このアクターたちのやり取りによると、その後の 2022 年 1 月、SVL 社でファイルの復号化にトラブルがあり、アクター**cybergangster** がその対応にあたりました。



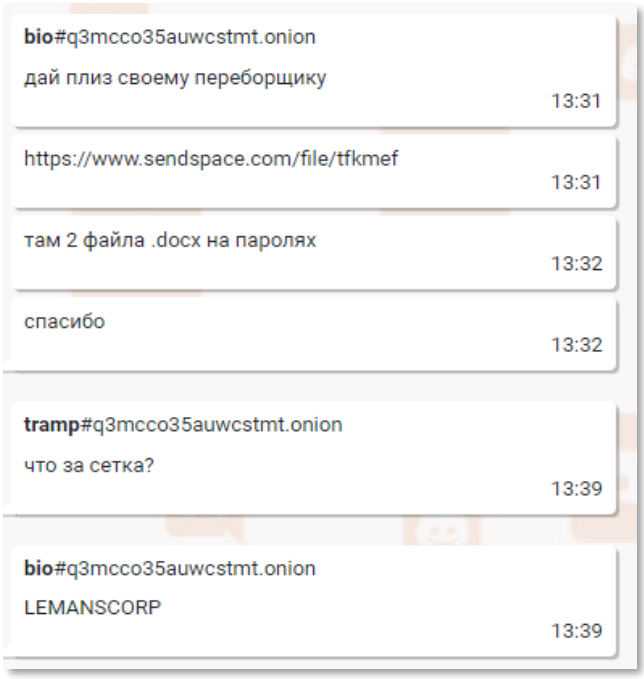
*2021 年 12 月 12 日：**bio** と **tramp** が SVL 社に要求する身代金の額について議論しているメッセージ*

我々が検証した会話の中では、被害者企業は通常、収益の 1%から 3%に相当する額を身代金として要求されており、その大半は 80 万米ドルから 830 万米ドルの範囲内となっていました。なお交渉の際には、身代金の額が引き下げられる場合もあります。例えば法律事務所 BSCR（bscr-law.com）の場合、当初は 100 万米ドルの身代金を要求されていました。同社と交渉を行う中で、bio は tramp に対し、価値のあるデータを窃取できていなかったと不満を述べていました（同社から窃取した大半のファイルは 2016 年から 2018 年のものであり、そのデータ量も小さいものでした）。その後 Conti と BSCR は、最終的な支払額を 30 万米ドルから 40 万米ドルの間とすることで合意しました（実際の身代金の最終額は明らかにされていません）。

ただし、Conti が常に少額の身代金を受け入れていたわけではありません。2021 年 11 月には、米国とカナダでモール向け小売事業を展開する Spencer Gifts 社（spencersonline.com）が攻撃を受けました。その後の 2021 年 12 月 2 日、bio と skippy は Spencer Gifts 社が支払に合意した身代金の額（45 万米ドル）が少なすぎると話し合っており、その話し合いの後、彼らは同社のデータをブログで公開しました。

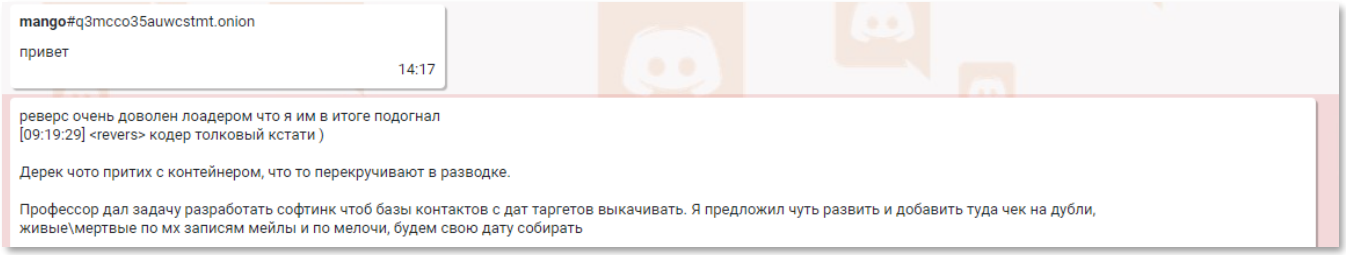
盗んだデータの処理

Conti が窃取したデータを処理する方法は、個別に取りあげて議論だけの価値がある興味深いトピックです。彼らは、身代金を支払うよう被害者を説得する際に利用可能な機密情報をより多く手に入れるべく、パスワード保護されたファイルにも不正アクセスしようと試みています。例えば、**bio** と **tramp** がモータースポーツをはじめとするパワースポーツ製品を販売する LeMans Corporation 社（lemanscorporation.com）について話し合っている時、**bio** は同社から窃取したパスワード保護付ファイルにブルートフォース攻撃を行うために、もう 1 人メンバーを割り当てることができるかと **tramp** に尋ねていました。



*2021 年 12 月 10 日 **bio** が **tramp** に、パスワード保護されたファイル 2 本のパスワードを破るために手助けが必要であることを伝えているメッセージ*

また彼らは、窃取したデータから被害者企業の従業員や提携先、その他第三者の電子メールアドレスや連絡先情報を抽出する際、特定のツールを使用している可能性があります。2021 年 3 月に彼らの間で交わされていたやり取りの中では、このタスクに関する話し合いが行われていました。その内容によると、彼らが使用している可能性のあるツールは、重複データを削除して電子メールがアクティブであることをチェックするためのものであると思われます。



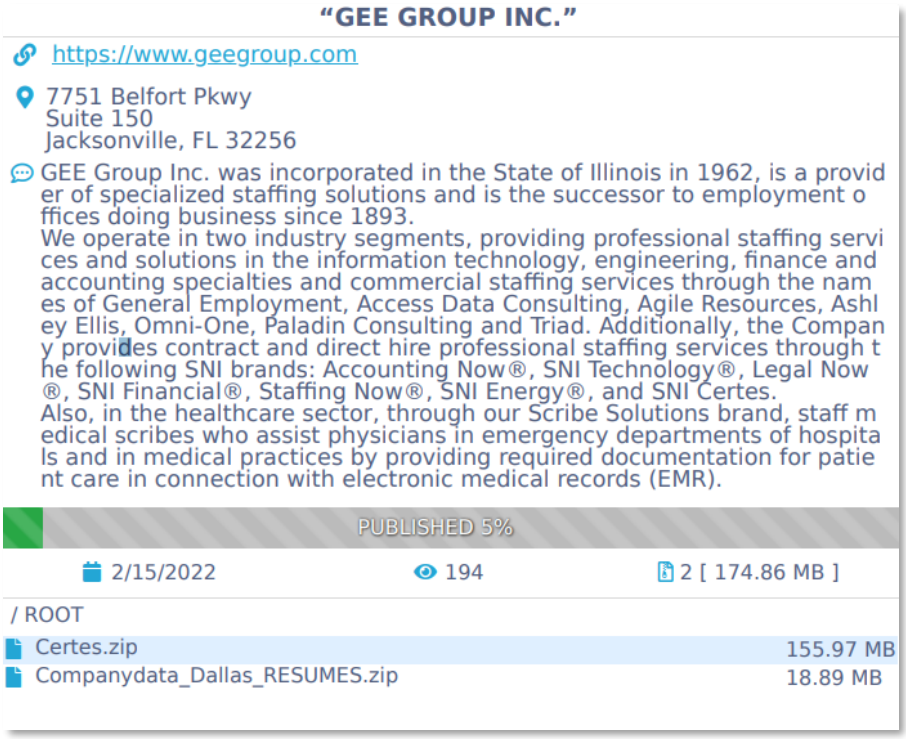
*2021 年3 月 16 日：**mango** が**professor** に「被害者のデータから連絡先情報を含むデータベースを抽出する」ためのソフトウエアを開発するタスクがあると説明しているメッセージ。mango が、電子メールの有効性や重複部分をチェックする機能を追加するよう提案している*

非公開のブログと交渉

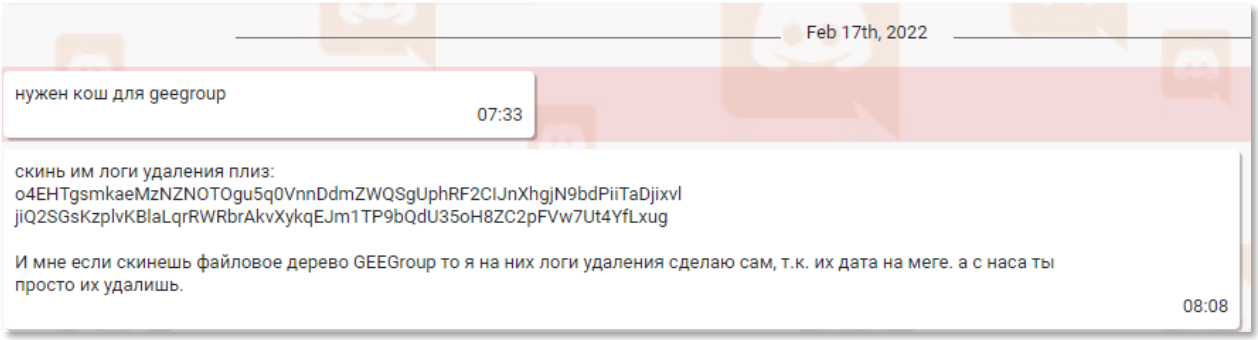
Conti のメンバーは、ブログ内で被害者に関する非公開の投稿を作成しており、この投稿は特定の URL でのみ閲覧することができます。この非公開の投稿を被害者に公開することで、被害者のデータがいかに簡単に閲覧できる状態にあるかを理解させて脅迫します。被害者が身代金の支払いに合意した場合は、非公開の投稿が公開されることはありませんが、交渉が不成立に終わった場合は投稿が公開され、被害者の名前も公表されます。2021 年 11 月 10 日、**bio** はこのやり方が被害者に対して大きな影響力を持っていることを説明していました。「あんたが好きなように言えばいい。けど、非公開のブログは本当にクールなんだ。被害者に対して効果を発揮しているよ」。

また、ブログの投稿が非公開であった時点では Conti の説得に応じなかったものの、すべての人々に向けて公開された時点で身代金の支払いに応じた被害者もいました。その一例として、米国の人材派遣会社 Gee Group（geegroup.com）の事例が挙げられます。同社は 2022 年 2 月 15 日、Conti のブログで被害者として公開されました。しかしその 2 日後、**pumba**

（**bio**）が「geegroup」用のビットコインウォレットを提供し、「削除ログ」を送信するよう **tramp** に依頼していました。また我々が Conti のサイトを確認したところ、Gee Group 社に関する投稿が同サイトで閲覧不可能になっていることが判明しました。これらの事実から、pumba（bio）がビットコインのウォレットを要求したのは Gee Group からの支払いを受け取るためであったと思われ、また同社は実際に身代金を支払っていました。

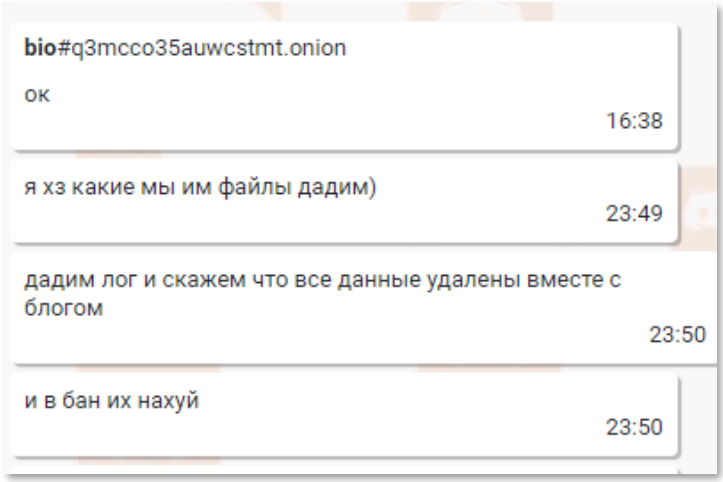


Gee Group に関する Conti の投稿（現在は削除済み）



*2022 年 2 月 17 日：Gee Group の削除ログを提供するよう **bio** が **tramp** に依頼しているメッセージ*

興味深いことに、Conti は被害者に対して窃取データに関する嘘を頻繁についており、実際よりも大量のデータを窃取したと主張しています。例えば、**bio** と **skippy** がカナダの電気工事請負企業である Houle 社（houle.ca）について話し合っている中で、**bio** は **skippy** に対し、被害者から特定のファイルツリー内にあった特定のファイルを提出するよう要求されたものの、該当するファイルを見つけられなかったと不満を述べていました。**bio** は、Houle 社のネットワークを攻撃したチームが、後に同社から指定されたファイルツリーにあった全ファイルをダウンロードしていなかったと主張していました。その他にも、世界的保健機関である Helen Keller International（「HKI：ヘレンケラー国際財団」、hki.org）に関するやり取りの中で、**bio** は同財団から窃取したのはたった 8 GB のデータであったと **skippy** に伝えていましたが、同財団との話し合いの中ではそれよりも大きな規模のデータを窃取したと主張していました。その後 HKI は、115 万米ドルを支払うことに同意しました。



*2021 年 11 月 30 日：**bio** が窃取ファイルを HKI に渡す方法について検討しているやり取り。最終的に HKI へ「ログ（恐らく削除ログ）」を渡すと決定し、HKI の全データをブログ投稿データとともに削除すると伝えているメッセージ。*

政府関連機関に対する攻撃と課題

Conti のリークにより、米国当局及びロシア当局について交わされた多数のやり取りが明らかとなりました。特に興味深いのは、この「グループ」が米国の公共セクターを重点的に攻撃しようと計画していたということです。2020 年 7 月、**target** が、米国の公共セクター攻撃を担当するチームを結成するよう提案していました。このチームには、すでに不正アクセ

スされた被害者から窃取した文書を調査して、興味深い標的となりうる政府関連機関を特定するという役割が想定されていました。target は、被害者の支払情報やその他通信関連文書をもとに、すべての取引先企業を特定してプライオリティ毎に分類するよう提案しており、この公共セクター担当チームの主要部門がネットワークへの不正アクセスと攻撃の準備を担当することとなっていました。

target は、現在の作業計画には一貫性もなければ米国の公共セクターをコントロールできるようなものでもなく、もしこのミッションが重要なのであれば、専用の体制を構築するべきだと述べていました。この会話が交わされたのは 2020 年のことであり、当時は Conti のオペレーションも安定していなかったため、この計画が実行されたか否かについては、定かではありません。

米国の公共セクターについての会話から 1 カ月後、**stern** と **electronic** は、米国当局が彼らに反撃している可能性を疑っていました。2020 年 8 月 21 日、**stern** はある人物が彼のサーバーに不正アクセスして、そこに自らの Jabber アドレスを記載したメモを残していったと語っていました。stern がこの Jabber アドレスに連絡したところ、この人物は stern に対し、Conti は特定のネットワークに不正アクセスしてほしいといったリクエストを受け付けているのか、また Conti は「米国で発生した不正アクセス」とどのように関係しているのかといった質問をしてきたとのことです。**stern** は、この人物のことを研究者か政府関連のハッカーではないかと推測していました。一方 **electronic** は、以前何者からか連絡があり、選挙（恐らくは米国の選挙）について質問されたと語っていました。

組織

構成

現在の Conti のグループは高度に組織化されており、複数のチームに分かれています。

- ハッカー。ネットワークに直接不正アクセスしているメンバー。このメンバーが特権昇格を行い、ネットワーク内を水平移動し、データをダウンロードし、ランサムウエアを展開します。複数のハッカーチームがあり、**revers** や **hors** がチームリーダーを務めています。

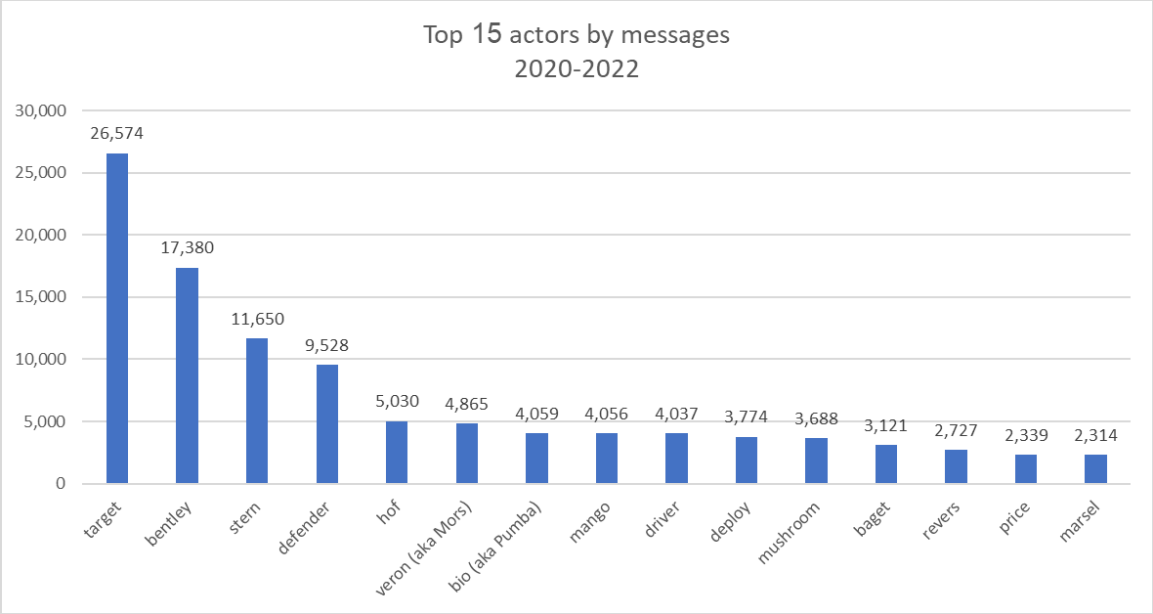
- コーダー。マルウエアの開発を担当するメンバー。一部のメンバーは、合法的な求職サイトを通じて採用されており、自分達が何の製品のコードを書いているのかを正確に理解していません。**buza** が彼らのチームリーダーを務めています。
- リバースエンジニアリングスペシャリスト。リバースエンジニアリングのスキルを有するメンバー。マルウエアの開発者を支援しています。
- クリプター。セキュリティソリューションによる検出を回避するため、マルウエアのビルドの難読化に携わっているメンバー。**bentley** がクリプターの 1 人に該当します。
- テスター。セキュリティソリューションによるマルウエアの検出をテストしているメンバー。
- OSINT スペシャリスト。窃取したデータを処理し、被害者（企業）に関するさらなる情報を発見し、被害者に関するブログ投稿を作成しているメンバー。**bio/pumba** や **buza** は OSINT スペシャリストに該当します。
- 交渉者。被害者との交渉にあたり、身代金の額について話し合い、他のチームメンバーに対するリクエスト（復号化のテストや、削除ログの取得など）の支援も行っているメンバー。
- 電話担当者。被害者（企業）の従業員やマネージャーに電話をかけ、OSINT チームが入手したデータを使って脅迫するメンバー。
- IT サポート。オペレーションのインフラをサポートし、システム管理者の役割を果たすメンバー。
- HR。様々なソース経由でメンバーを採用する部門。Conti はサイバー犯罪フォーラムの他に、様々な合法求職サイトも利用しており、その大半はロシアに特化したサイト（HH.ru や SuperJob.ru など）です。**Salamandra** が HR の 1 人に該当します。

2021 年 7 月には Conti は 100 人以上のメンバーを雇用しており、チームメンバーへの給与分配を担当していた mango の発言によると、同月の給与の予算は 16 万 4,800 米ドルとのことでした。また、2021 年 7 月におけるメンバー1 人当たりの平均給与は約 1,800 米ドルとなっていました。リークされた情報では食事の注文や実生活の場で行われた会議に関する会

話が確認されており、それらの情報をもとにすると、少なくとも同グループの一部のメンバーが、ロシアに構えたひとつの事務所に「出勤」していたものと思われます。

上位アクター

我々は Conti のリーク情報を分析して、やり取りに深く関与していたアクターの上位 15 人を特定し、各アクターの活動に関する説明を記載しました。



ソース：Jabber のログ

#1 - target

メッセージの件数	26,574
活動期間	2020 年 6 月 22 日 - 2021 年 10 月
役割	マネージャー
最も関連のあったアクター	bentley、stern、troy

target はマネージャーとして、日々の作業と様々なチーム間のコミュニケーションを担当しています。2020 年 10 月 9 日、target はオペレーションが成功した後に彼らが受け取る身代金の割合について、**stern** と話し合っていました。また彼らは、ハッキングチーム内の変更点やメンバーの採用プロセスを拡充する意向についても話し合っていました。

#2 - bentley

メッセージの件数	17,380
活動期間	2020 年 6 月 22 日～
役割	技術リーダー
最も関連のあったアクター	deploy、target、marsel

bentley はテクニカルリードであり、セキュリティソフトウエアによる検出を困難にするために、Conti のマルウエアの暗号化や難読化、操作を担当しているクリプターです。2021 年 7 月 27 日のチャットの内容から、bentley が TrickBot や様々なマルウエアローダー、Cobalt Strike や PowerShell ベースのマルウエアなど、様々な種類のマルウエアの暗号化を担当していることが明らかとなっています。

bentley は、「TrickBot ドキシング」でリークされた情報の中でも名前が挙げられています。我々は、TrickBot ドキシングのリーク情報内で確認された bentley の Jabber アカウントをもとに、bentley が volhvb とのユーザー名でフォーラム Exploit に掲載しているスレッドを特定することができました。bentley は、コードサイニング証明書の購入も担当しているようです。

#3 - stern

メッセージの件数	11,650
活動期間	2020 年 6 月 22 日 - 2021 年 12 月
役割	上級マネージャー
最も関連のあったアクター	target、 bentley、 mango

stern は重要なリーダーとして同グループのオペレーションを管理しており、「ビッグボス」と見なされています。そのため彼は様々な部門に対し、割り当てた日々の作業に関する最新情報を頻繁に問い合わせていました。また stern は、採用プロセスや新人研修プロセスにも直接関与しており、様々なメンバーに対する給与支払いの責任者でもあったようです。

2020 年 7 月 17 日、stern は給与を担当する「ボス」として言及されていました。また 2020 年 9 月 15 日には、stern が **mango** に「テスター」を 3、4 人採用するよう依頼しており、その際、給与は 1,200 米ドルであると伝えていました。stern はメンバーの状況や彼らのタスクの進捗状況をチェックしており、積極的にプロジェクトに関与していると思われます。それを表す一例として 2021 年 3 月、stern が **hof** に対し、ボットが正しくロードされないことを伝え、TrickBot に関する問題を修正するよう依頼していたことが挙げられます。

#4 - defender

メッセージの件数	9,528
活動期間	2020 年 6 月 22 日
役割	コーダーのリーダー
最も関連のあったアクター	driver、veron（別名 mors）、hof

defender は、コーダー数人（**zulas** や **ttrr**、**flip**、**driver**、**steller** など）の技術リーダーである可能性が最も高いと思われます。また技術リーダーとして、自分の仕事に利用できるツールを探していたことが確認されています。2020 年 9 月 24 日、defender は **ganesh** に対し、フォーラム Exploit からアクセスを購入するよう依頼しており、またブルートフォース攻撃を実行したり不正アクセスされたルーターを販売する人物を探すよう依頼していました。defender は、2021 年において送信メッセージの件数が最も多く、最も有力なアクターでした。

#5 - hof

メッセージの件数	5,030
活動期間	2020 年 6 月 22 日 - 2021 年 12 月
役割	ハッカーチームのヘッド
最も関連のあったアクター	defender、 bentley、 driver

hof は、マルウエアのコーダーチームの責任者と考えられています。2020 年 8 月 24 日、**stern** は新しいプログラマー**dark** に対し、最初の作業の件で hof に連絡を取るよう伝えていました。また 2020 年 9 月 4 日には、**stern** が **viper** に対し、特別な言語知識を持つコーダー募集の件で、hof をサポートするよう依頼していました。

#6 - veron （mors）

メッセージの件数	4,865
活動期間	2020 年 6 月 26 日～
役割	コーダー
最も関連のあったアクター	defender、deploy、marsel

veron（別名 mors）は、スパムからトラフィックを提供するという話の流れの中でその名が言及されており、またあるチャットの中では、「Emotet からロードしている」人物として具体的に自己紹介していました。2020 年 9 月 21 日、**stern** は **mango** に対し、「mors は我々にとって最も重要な人物だ」と語っており、これに対して mango は「最も重要なコーダーという意味で？それとも一般的な意味で？」と返していました。

#7 - bio

メッセージの件数	4,059
活動期間	2021 年 11 月 2 日～
役割	OSINT スペシャリスト兼交渉人
その他の名称	pumba
最も関連のあったアクター	tramp、 skippy、 cybergangster

bio（別名 pumba）は、2021 年 11 月にチームに加わりました。bio は、ブログに投稿する文書のレビュー、ブログの作成と公開を担当しているものと思われ、場合によっては身代金額の決定も担当しているようです。彼のメッセージは **tramp** 宛てのものが一番多く、大抵は被害者やブログ公開までの期間について tramp に相談している内容でした。

#8 - mango

メッセージの件数	4,056
活動期間	2020 年 6 月 21 日～
役割	ジェネラルマネージャー
その他の名称	khano
最も関連のあったアクター	stern、bentley、dollar

mango は、ジェネラルマネージャーとして **stern** とチームをサポートしています。mango は「業務」の一環として、不正アクセスされたネットワークへのアクセスを探していました（ランサムウエアを展開するため）。mango は、「traffers（感染用にトラフィックを提供するアクター）」とコーダー間の問題を解決するとも主張していました。2021 年 8 月 3 日、mango は **elvira** に対し、チームに加わった新たなメンバーのニックネームや雇用開始日、所属するチームのリーダー、Jabber のバックアップアカウント、合意した給与額などを記載したレポートを作成するよう依頼していました。また 2021 年 12 月 3 日、mango は新たな従業員の 1 人に対し、「ここでは私は、地域担当の保安官のようなものです：）」と発言していました。

会話を分析した結果、mango の会話の大半（69%）は 2021 年に発言されたものであること、また 2021 年における mango の会話の 45%は **stern** に宛てたものであることが判明しました。2021 年 2 月 1 日、この 2 人の間で交わされたやり取りの中で mango は、「私が様々なアクセス（ボットや RDP、VPN）を歩合で買い取るということを、全てのフォーラムで発表した」と報告していました。我々が監視しているサイバー犯罪フォーラムで類似の投稿を探したところ、khano と名乗るアクターが同日、フォーラム XSS と Exploit で上述の言い回しを用いた投稿を公開していたことを確認することができました。khano がこれまでに「市場で最も優れたソリューションのひとつ」との提携（affiliation）について言及し掲載してい

た投稿から、我々は高い確信をもって、khano は mango がこれらフォーラムの中で使用している別名のひとつであると結論付けます。

#9 - driver

メッセージの件数	4,037
活動期間	2020 年 10 月 28 日～
役割	コーダー
最も関連のあったアクター	defender、specter、hof

driver はバックエンドの php コーダーであり、**defender** が指揮するコーダーチームのメンバーである可能性が高いと思われます。driver は 2020 年 10 月に採用されており、彼自身、付加の高いプロジェクトに参加する意思を表明していました。driver は 2021 年 7 月にはすでに日々の業務で経験を積み重ねており、他の新入りコーダーを支援するようになっていました。

#10 - deploy

メッセージの件数	3,774
活動期間	2020 年 6 月 22 日 - 2020 年 11 月
役割	クリプター
最も関連のあったアクター	bentley、veron（mors）、hof

deploy はクリプターの 1 人であり、**stern** からは「クリプターのチーフ」と呼ばれています。論理的には、deploy のメッセージの大半（58%）は、**bentley**（Conti のマルウエアの難読化に関与しているテクニカルマネージャー）に送信されていました。

#11 - mushroom

メッセージの件数	3,688
活動期間	2020 年 6 月 22 日 - 2021 年 9 月
役割	ローダーのビルダー
最も関連のあったアクター	bentley、price、frog

mushroom はマルウエアのローダーの構築及び開発、ローダーの実行時間の改善における責任者であると思われます。2020 年 9 月 16 日 mushroom は、マルウエアが数回検知されたことを受けて実行時間を短縮するよう **stern** が依頼してきたと発言しており、またその困難な作業について不満を述べていました。mushroom のメッセージの約 1/3 は **price** に宛てたものであり、彼らの間で交わされたチャットのひとつでは、「ボットローダー」のテストについて話し合っていました。mushroom については、彼の連絡先情報やソーシャルメディアアカウントをはじめとする情報が「TrickBot ドキシング」の中でも言及されています。

#12 - baget

メッセージの件数	3,121
活動期間	2020 年 6 月 22 日～
役割	コーダー
最も関連のあったアクター	braun、hof、stern

baget はコーダーの 1 人です。2020 年 9 月 8 日、**buza** は baget がバックドア（マルウエアの一種）を書き終えたと発言していました。baget は「TrickBot ドキシング」でリークされた情報の中でも、プログラミング言語「C/C++」に精通したコーダーであり、かつランサムウエア Diavol を開発した人物であることが言及されていました。

#13 - revers

メッセージの件数	2,727
活動期間	2020 年 6 月 22 日 - 2022 年 1 月
役割	ハッキングチームのリーダー
最も関連のあったアクター	target、stern、taker

reverse はハッキングチームのリーダーです。2021 年 5 月 11 日、採用プロセスに関与していると思われるアクター**viper** が新入コーダーの **cheesecake** に対し、チームリーダー兼 cheesecake の監督者を務める revers に連絡をとるよう指示していました。

#14 - price

メッセージの件数	2,339
活動期間	2020 年 6 月 21 日 - 2021 年 10 月
役割	コーダー
最も関連のあったアクター	mushroom、target、hof

price は、バックドアやローダーなどを開発しているコーダーです。主に活動していたのは 2020 年であり、2021 年に関与していたは 3 件のチャットのみでした。

#15 - marsel

メッセージの件数	2,314
活動期間	2020 年 6 月 22 日 - 2021 年 10 月
役割	クリプター
最も関連のあったアクター	bentley、veron（mors）、green

marsel はクリプターであると思われ、主に 2020 年にチャットに参加していたことが確認されています。

我々は、Conti リークでその名が挙げられていたものの、上位 15 人に入らなかった重要なアクターを特定しました。そのうちの 1 人である **buza** は、OSINT チームのヘッドとコーダーのチームリーダーを兼務していました。buza は、2020 年 6 月から 2022 年 1 月まで活動していました。

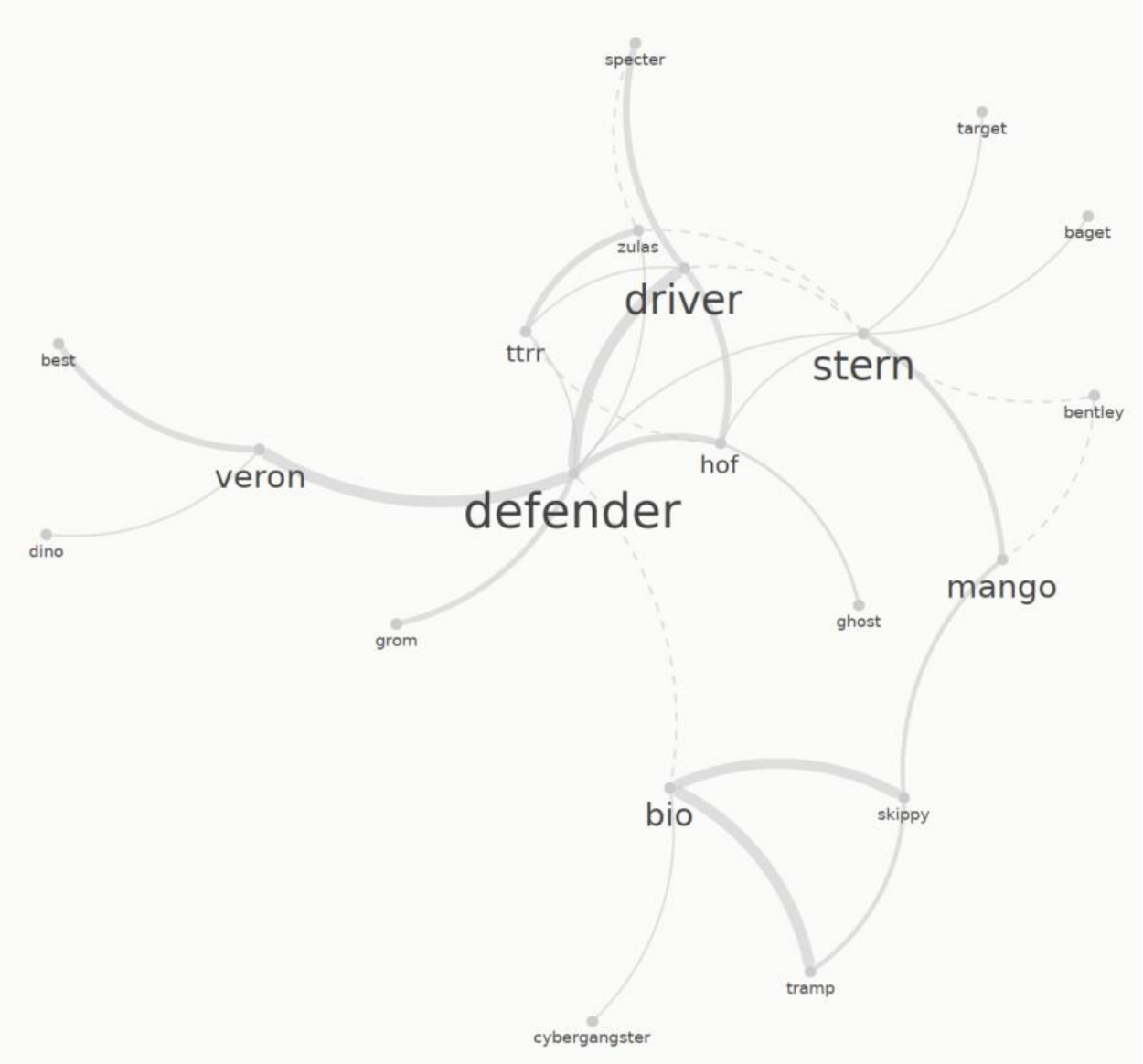
professor は、Conti のツール管理について責任を負っていた上級マネージャーであると思われ、2020 年 6 月から 2021 年 12 月まで活動していました。2020 年 7 月 9 日、professor は stern に対し、Maze の開発者と連絡をとっていると発言していました。

tramp も上級マネージャーであり、このハンドル名で 2021 年 11 月から活動していますが、最近グループに入ったばかりの人物には到底任せられないであろう重要な役割を果たしています。そのため、tramp は以前から別のハンドル名を使って活動していた可能性が考えられます。この可能性を裏付ける情報として、tramp が bio とのやり取りの中で自分は「第 2 の管理パネルと第 2 のチーム」も運営していると発言していたことが挙げられます。またもう 1 人の重要なアクターとして、その他の開発タスクの調整を支援していたシニアマネー

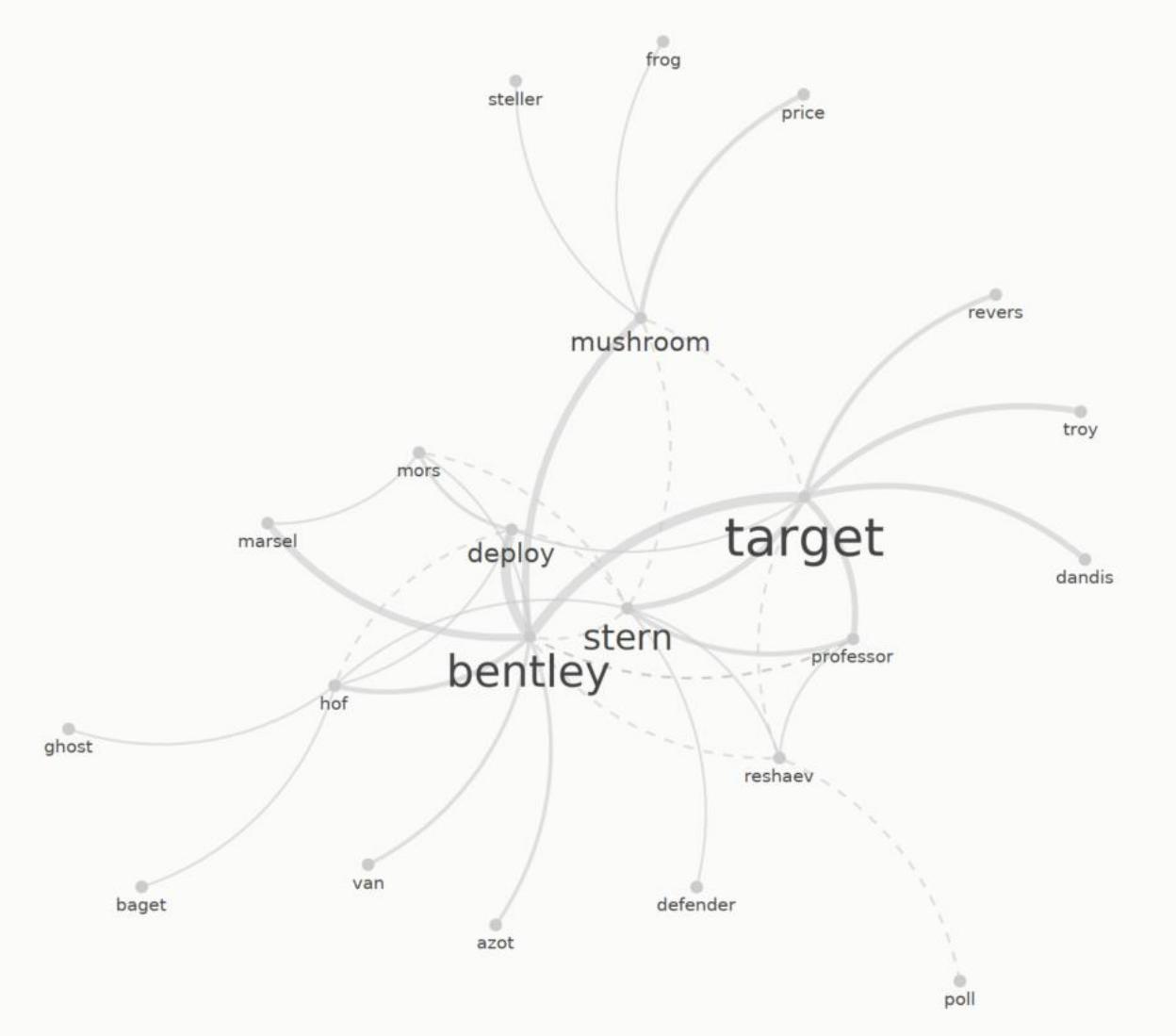
ジャーの **reshaev** が挙げられます。reshaev は、2020 年 6 月から 2021 年 11 月まで活動していました。

上位アクター間の交流

我々がアクター同士のやり取りを調査した結果、最も活発に活動していたアクターや最も人気のあったチャットが、2020 年の 1 年間と、2021 年から 2022 年にかけての期間では大きく異なっていることが判明しました。我々はこの違いについて、2020 年以降に Conti のグループ内に変化が生じたこと、そして Rocket.Chat の使用頻度が増加したことが原因であると考えています。以下の図は、両期間における上位アクター間のやり取りを表したものであり、太線になるほど強いつながり、点線になるほど弱いつながりを示しています。またアクターの名前の大きさは、そのアクターが送信したメッセージの件数と比例しています。



アクター間のやり取り（2021 年～2022 年）



アクター間のやり取り（2020 年）

結論

リークされた Conti の内部情報には、膨大な量のデータが含まれていました。その内容はすでにパナマ文書[9]とも比較されているほどであり、新たな IOC が多数確認されました[10]。Conti が高度に組織化された合法的な事業のようなやり方で運営されていることは既に明らかとなっていますが、今回のリーク情報をさらに分析してゆくことで、同グループの TTP やその作業の進め方についてより多くの知見を得ることが可能となります。また今回の Conti リークに続いて、他のサイバー犯罪者についてのさらなる情報がリークされる可能性も考えられます。例えば Twitter アカウント「f_0_r_e_v_e_r_」は、LockBit の TOX メッセージがリーク予定でありうることをほのめかしていました[11]。ランサムウエアグループ同士の競争が激しさを増し、政治情勢が緊迫している現在、企業の防御者であられる皆様には、サイバー犯罪関連のサイトやソースを注意深く監視し、こうしたリーク情報を素早く検知して、自らのセキュリティ対策の一助として活用されるよう強く提言いたします。

[9] 2016 年 4 月に財務・法務に関する記録 1,150 万件超が流出した事件で、犯罪や汚職を可能にするシステムが暴露されました。
[10] 本レポートと併せて Excel シートにて公開しております。IoC のソースは以下のとおりです。
https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
https://www.forescout.com/resources/analysis-of-conti-leaks/
https://www.breachquest.com/conti-leaks-insight-into-a-ransomware-unicorn/
[11] https://twitter.com/f_0_r_e_v_e_r_?t=ssOLFBJ88U-ZyrGjiO75MA&s=09


KELA
TARGETED CYBER
INTELLIGENCE