M|B|S|D®

Know your enemy
Defense leadership

ContiLeaksの概要まとめ Rev. 3

※本資料は「ContiLeaks」の
概要を簡易的にまとめたものです

※バージョン履歴：2022/3/4 Rev1 作成
※バージョン履歴：2022/3/8 Rev2 作成
※バージョン履歴：2022/3/8 Rev3 作成
（以降更新のたびに追記）

三井物産セキュアディレクション株式会社
サイバーインテリジェンスグループ
吉川 孝志
菅原 圭

■はじめに

2022 年 2 月 28 日に ContiLeaks という SNS アカウントが突如出現し、Conti の内部情報とされるデータを SNS 上で連日暴露し始めた。

以降では流出したチャットログの概要と、チャットの内容からいくつかピックアップして掲載した内容を記載する。

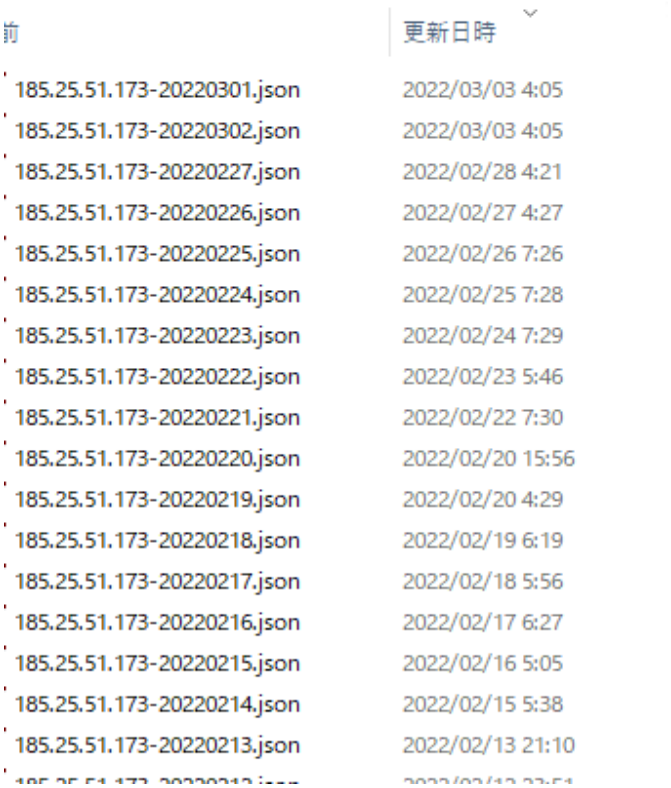
なお本レポートの趣旨は、あくまで大量に流出した一連のデータについて、詳細では無く概要や大枠を知りたいというようなケースにおいて、流出データの入手や確認にかかる手間や工数、リスクを減らしていただくことを目的としており、ホワイトペーパーやブログに属するものではないため、それぞれの情報に関する見解やコメント等はあえて掲載していない。またロシア語の翻訳に機械翻訳を用いている点など併せてご了承頂きたい。

※【注意】なお、SNS で暴露されている一連のデータやファイル、配布サイトなどは、マルウェアやランサムウェア、その他不正なコードを含む可能性があるため不用意な入手は推奨しない。

■流出したデータの種類と概要

流出が確認されているのは以下に列挙する各種ファイルやデータ類となる。

- Conti 攻撃グループのメンバー間の内部チャットログ約 2 年分(詳細は後述)



前	更新日時
185.25.51.173-20220301.json	2022/03/03 4:05
185.25.51.173-20220302.json	2022/03/03 4:05
185.25.51.173-20220227.json	2022/02/28 4:21
185.25.51.173-20220226.json	2022/02/27 4:27
185.25.51.173-20220225.json	2022/02/26 7:26
185.25.51.173-20220224.json	2022/02/25 7:28
185.25.51.173-20220223.json	2022/02/24 7:29
185.25.51.173-20220222.json	2022/02/23 5:46
185.25.51.173-20220221.json	2022/02/22 7:30
185.25.51.173-20220220.json	2022/02/20 15:56
185.25.51.173-20220219.json	2022/02/20 4:29
185.25.51.173-20220218.json	2022/02/19 6:19
185.25.51.173-20220217.json	2022/02/18 5:56
185.25.51.173-20220216.json	2022/02/17 6:27
185.25.51.173-20220215.json	2022/02/16 5:05
185.25.51.173-20220214.json	2022/02/15 5:38
185.25.51.173-20220213.json	2022/02/13 21:10

図 1 公開された 546 の json ファイル（一部）

- 複数のスクリーンショット:

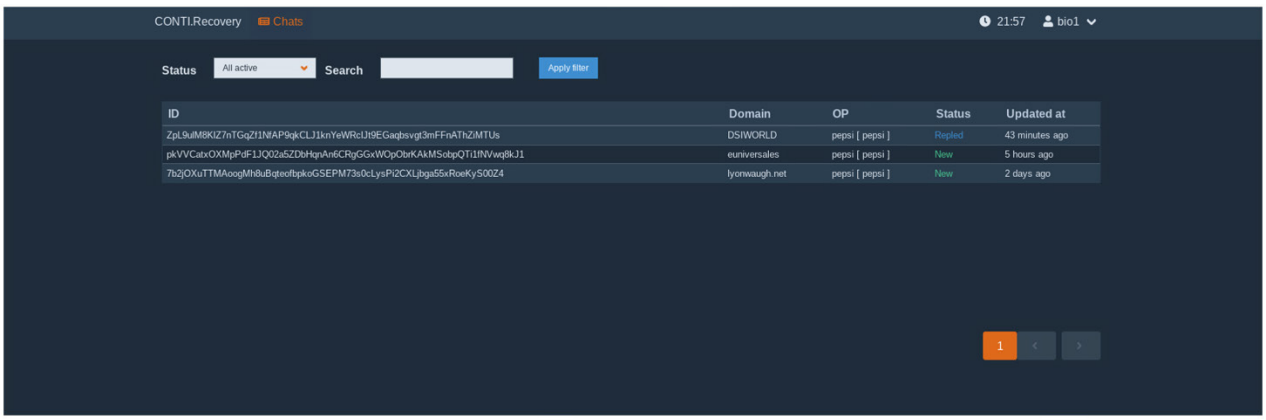


図 2 被害組織との交渉の管理画面（どちらがボールを持っているのかのステータスなどが確認できる）

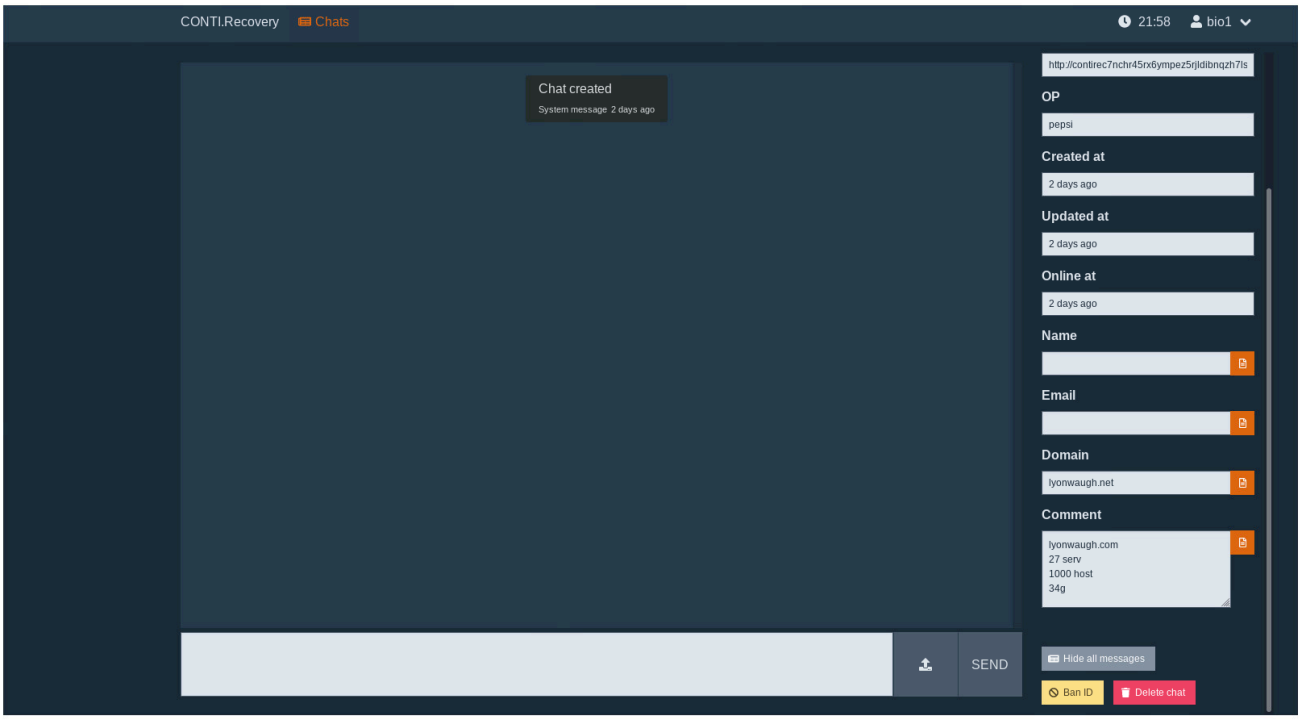


図 3 被害組織との交渉に使用されるチャット画面

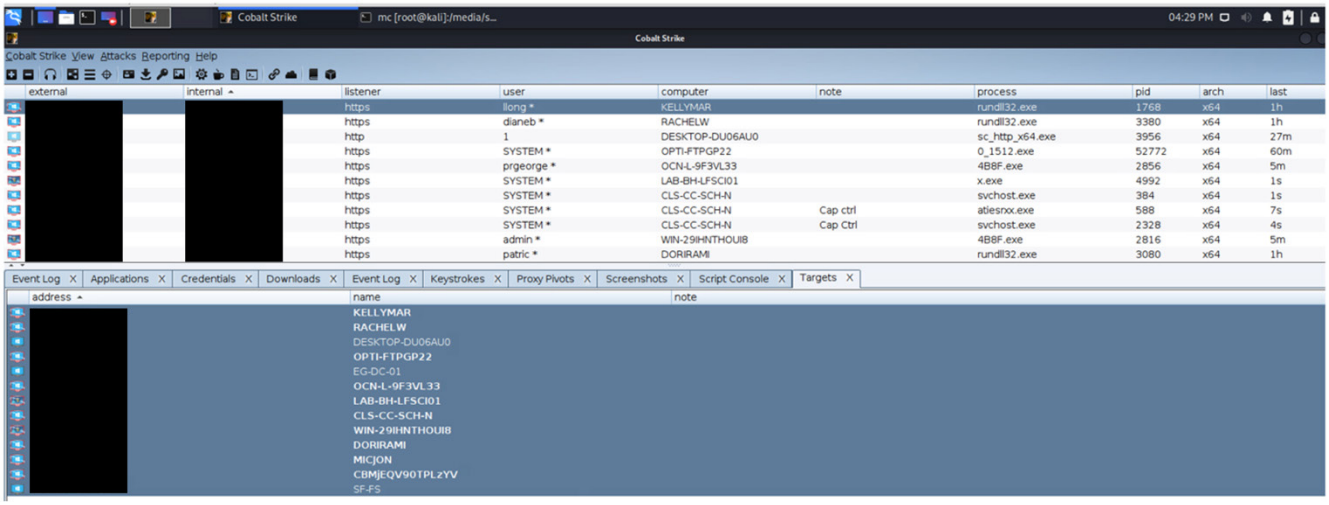


図 4 CobaltStrike の管理画面（既に多数の端末が感染し管理下にあることがわかる）

- BazarLoader（Conti の初期アクセスブローカーが使用するマルウェア）の関連データ
- Conti ランサムウェアのソースコード一式
- バックドアやツール等のソースコード
- TrickBot 関連のデータ
- Conti/Trickbot 攻撃グループの内部フォーラムログ（Conti 攻撃マニュアルの元となった書き込み）
- 役割担当ごとに分かれたマニュアル一式

```
│ エクスプローラーのクイックスタート.txt
│ ハッカーズ・クイックスタート.txt
│ オールドスクール魂.txt
│ スピードコンピューティング.txt
│
├────bot
│ cs2 proto.rtf
│ doc-lero.docx
│
├── インジェクター
│ inj.rtf
│ Logs60.rtf
│ module.rtf
│
├鞁マネジメント
│ マネジメントマニュアル.txt
│ テクニカルマネージャーへの指示.txt
│ コードとアセンブリの設計.txt
│ エラー報告ルール.txt
│ 安全対策.txt
│ タスク会計.txt
│ AB クリーニング.txt
│
├──misc
│ tor.txt
│ cryptopanel.txt にあるグループテスト自動化のための TOR
│ インジェクターテスト自動化のための ToR.txt
│ 暗号テストの TOR 自動化.txt
│ DPOST パスワード奪取のための ToR.txt
│ インジェクターテスト用 ToR.txt
│ TK メールアカウント再計算.txt
│ cryptopanel.txt の TOR チェック状況
│
└────モジュール
        バックドアオペレーターマニュアル.txt
        module_HOWTO.txt
        バックドア起動.txt
```

日刊 crypts.txt
軽量モジュラーボット.txt
テスト計画書 bk.txt
スーパーブラウザ マニュアル.txt
クリプトパン・オペレーター・マニュアル.txt
apache tomcat.txt
バックコネクト サーバ.txt
TK VPN クライアントと admin.txt
クリーニングオートメーション ToR.txt
管理者スキャナー.txt
OWA ブルートフォース.txt
バックドアレクイエム.txt
Windows と AD のユーザー dump.txt
ToR refine ディストリビューションモジュール.txt
クリプトロッカーToR.txt
Cryptolocker.txt
Cookies.txt モジュールの ToR を取得する。
VPN モジュールとブリッジの ToR.txt
coincidence.txt でファイルやフォルダを検索するモジュール。
サーバーの ToR ファイル検索.txt
キーワードによる ToR ファイル検索.txt
Asm ポリモーフ・プロセッサ ToR.txt
ToR ポーティング masscan.txt
ToR simple cryptolocker.txt
ToR 常駐ローダー.txt
ToR rdp スキャナー.txt
ToR sql injection scanner2.txt
ローカルネットワークスキャナ ToR.txt
プリンタスキャナ ToR.txt
Spambot.txt
ボット要件.txt
loader.txt の要件

図 5 マニュアルのタイトル一覧（機械翻訳）

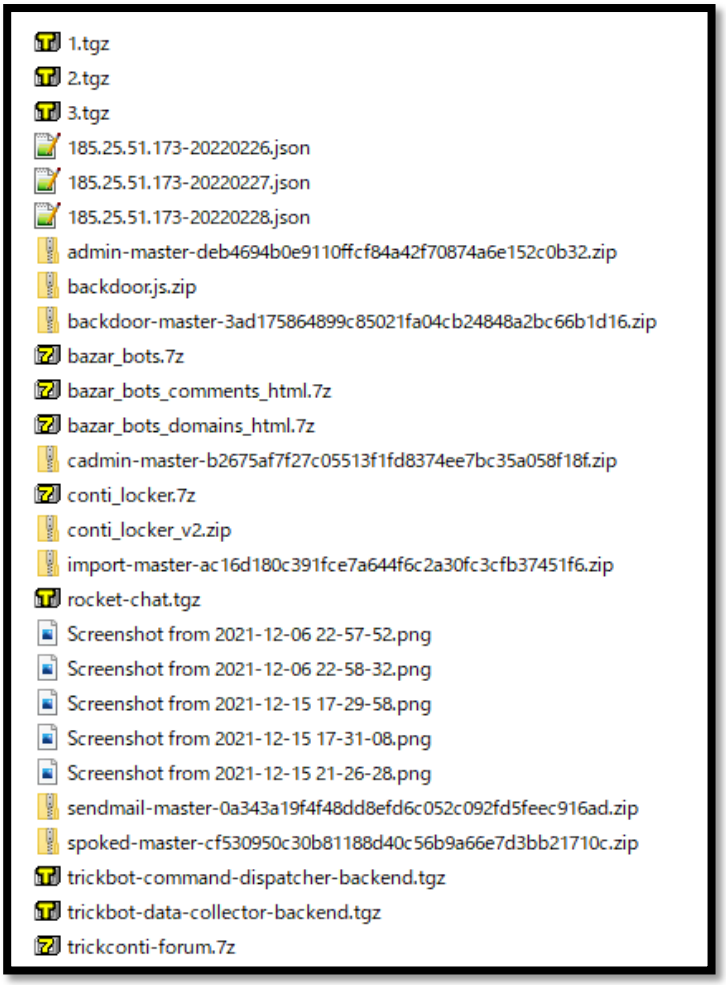


図 6 連日に渡り暴露されたデータを一つにまとめた様子

■チャットログの概要と内容

- **概要**

本資料作成までの間に確認された流出データは以下の項目となる。

- 流出したチャットログの期間：2020/6/21～2022/03/2
- チャットログの形式：json 形式（Jabber(XMPP)のログと推測されるデータ）
- Json ファイル数：546 ファイル
- メッセージ数の合計：約 17 万弱(168,777)
- メッセージ内のユーザー数（重複削除）：465 ユーザー

- **内容**

チャットの総メッセージ数は（本執筆時点で）約 17 万弱あることもあり全てを列挙する現実的では無いため、以下はその中からいくつか興味深いものをピックアップして抜粋（順不同）したものとなる。

なお注意点として、これらチャットの原文はスラングなども用いられたロシア語で記述されているため、一部機械翻訳からの意訳を含むものや、意味が不明なものは機械翻訳のまま掲載しているものもある。

- **新しい従業員の採用・内定について／送られてきた履歴書に関して会話している様子**

「すでにオファーを送ったのに、この履歴書を見たということが書かれていない というコーダーからの不満は多い」
「履歴書を見たという印がないのに、もう内定を出したというコーダーの苦情がたくさん来ている」

（※ある人物の履歴書を話し合っている様子↓）

[13:29:39] <buza>こんにちは。
[16:34:40] <salamandra> 彼は 200 の給料を要求している。
[13:30:00] <buza>そういえば、マネージャーの視点からも候補者を見るというお話がありましたね。
[13:30:03] <シュテルン> うん。
[13:30:05] <Stern> わかりました。

[13:30:18] <buza>履歴書を見てみると、IT 業界で 20 年ほどの経験があり、最近はすべて上級職に就いています。
[13:30:21] <Stern> しかし、そのためには、その人が 1.ハイレベルなコーダーであることを証明する必要があります。
[13:30:23] <シュテルン> 2.安定している。
[13:30:28] <buza>まったくその通りです。
[13:30:36] <buza>誰も 20 万円あげろとは言ってない。
[13:30:38] <スターン> 3.管理できる、忠実である。
[13:30:56] <シュテルン> ok
[13:31:00] <Stern> それから最初の 2 ヶ月間 150
[13:31:00] <buza>ここで彼がすべてを見せ、コーダーのプロであることを示し、6 ヶ月のうちに管理職と給料を得ることに同意すればいいのです。
[13:31:01] <シュテルン> さらに 200
[13:31:28] <buza> サラマンダーには、彼をつけるように言ってください。
[13:32:03] <シュテルン> ok

（※人材派遣の就活サイトで従業員を探している話題↓）

"XX でレジュメを検索し、そこから相手のメールを取り、手紙を書く。"
"レジュメ検索がありますね"
"履歴書は 1 日 30 通まで"
8 月 1 日よりアクセス料金を変更しました。
2020 年 8 月 1 日、hh.ru（ロシア・モスクワの人材捜しや採用活動をサポートしてきたサービス／履歴書検索サービス）はこれまでで最大の変化を遂げました。履歴書データベースの運用を新しいモデルに切り替えたのです。つまり、履歴書の枚数が激減したのです。今、会社には 1 ヶ月に 1280 通の履歴書が送られてくるが、全ての管理職で、1 日あたり 45 通である。従来は 1 日 8000 枚の CV を付与していました。料金の詳細はこちら

（※新しい求人広告に関する話題↓）

「昨日の履歴書はどうした？」
「夏も終わりですから、そろそろ履歴書も増えると思います。」
“こんにちは、.....のチームの仕事を紹介します。
孤立無援の中、私たちのチームはあなたに完全なリモートワークのための現在の欠員を提供します。
職務内容
電話の取次ぎ、お客様とのコミュニケーション
必要なスキル：英会話の知識、18 歳～25 歳

利用規約
-給与は 450 ドルから 500 ドル（スーパーバイザーのポジションにより 100 ドルから 200 ドル、300 ドルの昇給あり）。
-完全リモート勤務、スケジュール 18:00 - 2:00 MSK . 週休二日制。
-有給休暇制度あり
興味のある方は、このメールに履歴書を送ってください。"

"履歴書を見せてください"
"履歴書をお持ちですか？"
"履歴書を見ています"
"履歴書を見てみよう" "ストレスを与えないように"
"日曜に面接と面談のレポートを送ってくれ" "履歴書もだ"

（※面接を受けにきた人物との会話↓）

「レジュメに githab があるんだけど、こんな感じで、ほとんどのプロジェクトが NDA で、画面やスクリーンショット以外、何を見せればいいんだろう？」
「履歴書や経験についてもっと具体的な質問がありますか？」
「私は今、11 月 4 日に退社する予定です。その日の夕方には仕事の最終決断ができ、いろいろなことを終わらせ、9 日にはもう出社できます。」
「オファーを出す準備ができていて、私の経験に満足し、マリアとの取り決めに基づいて、カードに 10 万円という理解で合っていますか？」
「あなたは私の履歴書、電話（まあ、一般的に）、その一方で私は誰と働いているのか分からないでしょうし、これは我々の契約の一部として、私が同意するかしないかです。」

「私の立場は、もし候補者がそのお金に見合う価値があると説得力を持って証明できれば、給料を希望通りに上げる用意がある、ということです。」

（※おそらく履歴書の貼り付け↓）

親愛なる、自分自身について、ミニレジュメ。
2010 年から Win システムで管理者レベルの業務に従事、WinServer 2003 からスタート
AD、DNS、DHCP、GP、デプロイメント、サポート。
VMWare、ESXi、Hyper-V の仮想化。

nix のようなシステムで作業する。
例えば、4,000 台ものホストからなる大規模な工場を管理するチーム。
酒を飲まない、麻薬もやらない、行方不明にならない、仲間とのコミュニケーション。

- **一般開発ベンダーのようにテスターの役割の人物が QA テストを行っている様子が窺えるやりとり**

「こんにちは、明日はすでにビルドを発行できます。今日は xp と 2003 でテストしています。」

- **Windows11 のリリースに備えて調査が必要だと指示するやりとり**

「コーダーに探索させる」
「Win11 が間もなくリリースされます。準備が整い、調査を開始する必要があります。ベータ版はすでにオンラインになっています。正式にダウンロードして作業できます。」
「わかりました」

- **雇われ開発者の参入と挨拶**

「こんにちは。私は新しいプログラマーです。割り当てを依頼するように言われました。」

- **VMware から Carbon Black を割引価格で購入しているやりとり**

（※以下は CarbonBlack の返事の貼り付けと想定される文面）
「こんにちは、すばらしいニュースがあります。お伝え頂いた価格に割引できるか確認中です。
CarbonBlack のインストールガイドはこちら。＜URL＞。製品使用ガイドはこちら＜URL＞。
CarbonBlack のライセンスを購入いただくと、次の URL にある無料のトレーニングにアクセス可能です。＜URL＞明日までに販売代理店から見積もりを受け取っていただければ幸いです。カーボンブラックを信頼していただきありがとうございます。よろしくお願いいたします。」

（以下は攻撃グループ側の購入担当者と想定される文面）
請求書は明日発行され購入の準備ができました。

- **新しいポジションの募集要項の書き込み**

・給与：450-500 $（スーパーバイザーの位置に応じて、給与が 100 $ -200 $ -300 $増加します）
・勤務時間：18：00-2：00（モスクワ時間）。週休二日。
・英語上級中級
・年齢：18 歳から 25 歳まで
・主な業務：電話を受けてクライアントとコミュニケーションをとるお仕事です。

・オペレーター1 人あたりの 1 日あたりの電話数は 10～40 までです。
・スムーズな交渉時の通話時間はおよそ 15～16 分です。

● ランサムウェアの開発を示唆するコメント

「兄弟、財布を渡せ」
「ああ 今買おうとしてるんだけど、夏だからみんなイライラしている」
「Maze の開発者とオーナーと話したが...詳しくは行ってからのお楽しみだ。」
「バ、シャイン、マーカス.....彼らはすでに解体されているが、悪い時に落ちたので、作り直さなければならない。」
「ロッカー（ランサムウェア）の開発を始める、ネットから Maze と Ryuk のサンプルを探し、コーダーに渡す」

● SIM カードの手配に関するやりとり

「彼らはまだ SIM カードを持ってきていないが、週末までにそれを持ってくるはずだ、まあ、私は月曜日から始めることができると思う」
「CIS 以外の SIM カードが必要です。または、それ以外の方法を教えてください。」

● 支払い期限を過ぎても支払わない被害会社に対してどう対応するかを会話しているやりとり

「アメリカの会社、どうしますか？」
「私たちはすでにあなたに十分な日付を与えていると彼らに書いてください」
「私には小さな考えがあります」
「4 つの会社に攻撃を行い、パネルに来たのは（交渉してきたのは）そのうち 2 つだけで、他の 2 つは電話を切り、最も興味深い金融業者の会社も電話を切りました」
「とにかくどうしますか？彼らを茶番で絞め殺すか、それともまだ返事を待ちますか？」
「ファイルを取り出すのに時間がかかりますが、窃取データはアーカイブで分割されており 650GB あると書いてください。それから、すでに十分な日付を指定しており、あなたがお金を払わなければ明日アップロードを開始します、などを追加してください。彼らはリスクを冒したくないのでお金を払うと思います。」

● メディアが書いた記事が自分達の攻撃なのか把握できてないことがわかる

（※以下はランサムウェア被害を報じたあるメディア記事の貼り付けと推測される文面）
「Apple、Tesla、HP、Dell の請負業者である台湾の電子機器会社 Delta Electronics は、ランサムウェアのサイバー攻撃の攻撃を受けた。・・・ランサムウェアグループは、ファイルの復号とデータ流出を防ぐため 1,500 万ドルの身代金を要求しました。」

（※以下は上記の記事に対するコメントと思われる文面）
「これは本当に私たちのチームの 1 つがやったことですか？彼らはネット上で何を書いていますか？」

- **交渉時の金額について最初はふっかけるものだという助言**

「金額はどうしますか？」「3.5kk？」
「最低 4」「少なくとも 2 を拾うには 4 から始める」「$ 4,000,000」
「OK、わかりました、ありがとう」
「あなたは今彼らにその金額を伝えるつもりか？」
「要求に応じて」
「わかった」
「今日は聞いてくれると思います」
「財布が来る」
「ありがとうございます」

- **メディアの記事になっていることを嘆いている様子**

「ここで？」
「（Ryuk が医療機関サービスプロバイダーを攻撃したと報じるメディアの記事へのリンク 1）」
「ああ、くそ」
「ネットで話題になっている」
「くそ」
「お前が台無しにしたんだ」

「ググれ」
「全てはここにある」
「“5 千万ドルの身代金要求“とある」
「（Ryuk が医療機関サービスプロバイダーを攻撃したと報じるメディアの記事へのリンク 2）」

- **結果が出ない時に感じる苦労を話す様子**

「午後 8 時までにソフトウェアとアシスタントを準備するように」
「結果が出ない日が続くと、とても悲しくなる」
「白髪になりそうだ」

- **Conti のあるメンバーが Ryuk に自身が作ったコードが再利用されていることを知って驚く様子**

「（メディアによる Ryuk の解析記事へのリンク）」
「（これを読むと）我々の動きと大差ないな」
「実はほとんど同じなんです」
「adf.bat – あれ、それは私の（私が作成した）バッチだ」
（※Ryuk と Conti が同じ幹部によって利用されている事を知らないメンバーの可能性↑）

- **ランサムウェアを改良しテストで問題なければ実戦に進めるという趣旨のコメント**

<reshaev> 「こんにちは、私のロッカーのアルゴリズムを AES の何倍も速い chacha20 に変え、暗号化をスポットで行うことでスピードアップ、バズはランダム化を助け、昨日スキャンし、今日は手動ですべてチェックします。crypt-decrypt を徹底的にチェックして、問題なければ明日出陣します。」

- **被害組織側のランサムウェアの交渉人からの交渉コメントを共有する書き込み**

「あなたのチームからのオファーは 50 万ドルです。 しかし私のクライアント（被害企業）は最大で 20 万ドルしか支払うことができず、データだけが欲しいようです。 この件に関して何ができるか考えてください、さもなければこの取引は成立しません。」

- **2 人の従業員同士がもめており、最終的に違うチームに移動してくれといって終わるやりとり**

"[23:43:40] <pumba> まあ、全額ではないですが。
[23:43:49] <プンバ> ハーフのみ
[23:44:15] <pumba>不逞の輩、正直者だと思ってた。
[23:44:25] <tramp> -0.746645
[23:44:30] <pumba>何のために？
[23:44:35] <tramp> はい、でももう 1%もありません。
[23:44:46] <tramp> ブログの場合は 0.5 となる予定です。
[23:44:55] <pumba> でも、ダメならダメで、新しい会社で行こう。
[23:44:57] <tramp> tramp さん、あなたは正直者だと思っていましたが、そうなんですか？
[23:44:58] <プンバ> そして、これらは私が運転したものです。
[23:45:07] <pumba>あなたと一緒に
[23:45:30] <tramp> いや、入り方が気に入らない。
[23:45:37] <tramp> そこで私はこう決断した。
[23:45:44] <tramp> 議論しませんか？
[23:46:08] <pumba>お前は間違っている、この 2 社に金を払う直前に俺を追い出したのはお前だ。
[23:46:26] <pumba>そして最後の 1 つは、4850 という金額を交渉したのは私です。
[23:46:30] <tramp> あなたは正しいブログの書き方を学んだのだから、それを続けてください。
[23:46:52] <プンバ> 正直なところ、この前の会社の分くらいは払えよ。
[23:47:02] <pumba>そして、0.5 で作業します。
[23:47:10] <tramp> そして最後の 1 つは 4850 で交渉しました - まあ、誰がそんな割引をするように頼んだのですか？ 彼らはもっと請求してきたでしょう
[23:47:24] <pumba> x3 入れたんですね。
[23:47:29] <pumba>5km でした。
[23:47:35] <pumba> 150k 落とした。
[23:47:41] <pumba>私たちがあなたと決めたように
[23:47:49] <tramp> 友達は今すぐやめなさい。

[23:47:57] <tramp> または、今すぐすべての作業を停止する。
[23:48:08] <tramp> 自分のブログは自分でできる。
[23:48:19] <tramp> そこで何度か失敗したので、0.5 としたのです。
[23:48:24] <tramp> それは論外です。
[23:48:46] <tramp> とにかく、あと一言で終了です。
こちらも同様です。
[23:55:18] <pumba> なぜ？
[23:55:23] <tramp> 1%。
[23:55:29] <tramp> その後の消費
[23:55:42] <pumba> as you soot.
[23:55:56] <tramp> それで仕事は終わりです。
"まあ、だいたいのことはわかったから、他のチームにしてくれると助かるんだけど。"

- **新年の挨拶と雑談をするメンバー間の会話**

「新年おめでとう、兄弟」
「マクガズに行ってきます」
「ショップ」
「サバが食べたい」
「スモーク」
「冷燻されたサバの朝食ほど美味しいものはない」
「私も店に行くが 7 時から 12 時だ、酒は売ってないぞ」
「12 時以降は酒も売らないと」
「うらやましい..」
「12 時過ぎでも気にしない...」
「少なくとも酒を買うには森の反対側までドライブが必要だ」

- **休暇の申請が認められたことを喜ぶ従業員の会話**

「よーし」
「やあ！ 02/23 に休日を申請したら 許可が出ました。」
「素晴らしいね」

- **バンク・オブ・アメリカをはじめとしてアメリカを狙っている会話**

「銀行への攻撃をトライしているが、すべてが悲しいことに失敗している。私は個人的にバンクオブアメリカを狙っている。しかしこれまでのところ結果はない。」
「アメリカ全体をロックする必要がある」「協力して、アメリカを一緒にやろう」

- **攻撃グループの給料がフォーラムで安すぎと言われているということに関する会話**

「ハッカーフォーラムで広告を出して新しいメンバーを募集していますが、給与が 2,000 ドルであるという発表では、ガレー船の奴隷を募集しているものだというコメントがたくさんあります。どうやって異議を唱えることができますか？」

「結果を出せばより多くの給与を得られるなど。」

「5-10k の給与を稼ぐ開発者の例はありますが、全員と給与交渉することは困難ではあります。」

- **フランス被害企業の交渉人からの連絡を貼り付けた書き込み**

（※以下はフランス被害企業の交渉人からと思われる文面を貼り付けたと想定される文面）

「こんにちは。私はフランスの企業/機関に関する身代金の公式交渉者です。私にメールを送ってください。Jabber を介し任意のチャネルで交渉できます。時間とお金を節約してください。」

- **日本に関する雑談**

「ずっと行きたかった日本行きの飛行機のチケットを予約した。」

「おお」「本当に？」「自分の？」「どのくらい飛ぶの？」

「4 時間で」

「本当に？」

「いいえ、私は真夜中に私を起こすような人たちのためにそのような冗談を言っているんだ。」

- **日本に関するやりとり（一部、意味不明）**

「unicode を使うのは致命的だ」

「マルチバイトは止められているのか？」

「いいえ」

「使いたいものを使ったらいい」

「日本ではマルチバイトはパスが悪いと言われている」（？）

「Unicode はサイズだけでなく、プログラムも大きい」

「ANSI を使えば、立ち上がるのが遅くなるのでは？」

「VPN が必要です。VPN がないとブロックされます」

「そして、どの VPN が必要ですか？火星か別の VPN ですか？」

「わからない」

「自分で見つけましたが、日本語でブロックすることもできます」

「どんなアメリカ人」

「それなら火星で十分かもしれない」

- **給与の管理がうまくいっていないことが窺える以下のような書き込みが目立つ**

「ちなみに、給料はいつになりますか？」
「VPN の有効期限が切れています。料金を支払う必要があります。」
「人々に給料を払う必要があるでしょう」
「給料を出してください」
「こんにちは、給料を送ってください」
「給料をくれませんか？」
「こんにちは、今日は給料日です。このウォレットに送信してください」
「給料にフォークはありません」
「雑草としての給料についてはそうです」
「こんにちは。今日は給料をくれませんか？」
「給料について話してもいいですか？」
「今日は給料をもらえますか？」
「こんにちは、この住所に給料を送っていただけませんか？」
「こんばんは。今日は給料がもらえるの？」
「給料はもらえますか？」
「彼は 4 ヶ月間給料をもらっていませんでした」
「1 年も給料がもらえなくても脱落しない」
「こんにちは、あなたはいつ労働者と給料を支払うつもりですか？私はすでに自分でサーバーの代金を払っています・・・。」
「こんにちは、給料がはっきりしないのはなぜですか？もう一ヶ月経ちました」
「今、開発者の 1 人が自分の給料を 2 から 2.5k にアップしたという状況が発生しました。誰が給料を上げたのですか？」

- **ゼロディエクスプロイトの売買の可能性や提案に関するやりとり**

「Windows10 でのみ機能する IE11 の 0Day エクスプロイトとサンドボックスエスケープがあります。
Excel2007-2019／365 の 0Day エクスプロイトも。ただ完全サイレントではなく、「編集を有効にする」必要があります。IE エクスプロイトと Excel エクスプロイトは Windows10 でのみ機能します。
エクスプロイトには dll ペイロードが必要です。」
「私は開発者です。2 月からこのエクスプロイトがあります。。私の手にあるエクスプロイトは、すでに多くの「パッチチューズデー」を生き延びています。」「ハッカーフォーラムで販売しています」
「今は買わない」「それに、IE11 はあまり使用されていない。」
「了解しました」

「こんにちは。WIDFRD.sys ドライバーに解放後使用の脆弱性に対するゼロデイ特権昇格エクスプロイトがあります。このエクスプロイトは、Windows 10 x64 1607、1703、1709、1803、1809、1903、1909 に実装されています。この脆弱性は 2004 年以降にも存在しますが、ドライバーの対応するコードが書き直され、OS が

BSOD にクラッシュしてから、ターゲットの null ポインターの逆参照の脆弱性がトリガーされます。必要であり、ターゲットプロセスのトークンをシステムのものに置き換えるコードを実行します。」

「購入したいという希望を表明しましたが、誰も答えません。価格-60k、交渉可能。希望する人のために、ユーティリティを作成して発行できます。対象のシステムで起動すると、OS が脆弱かどうかがわかります。最初に PM で連絡し、次にジャバーで連絡します。　追加します： エクスプロイトは片手で販売されます。 」

- **証明書の購入に関するやりとりもいくつか見られる**

「証明書を購入しましたか？」
「割引で買えました、2600 ドルの代わりに 1500 ドルで」
「1500 で証明書を購入しました。」
「私たちは証明書を買いました。」

- **Emotet や Dridex などのマルウェアに関する会話（一部、意味不明）**

「dridex は何年も聞いていない」
「インターネット上にマルウェア解析者によって解析された emotet の情報がある」

「もちろん、多くの質問があります。TrickBot はどのようにして始まったのですか？何がそれを促したのですか？」
「それは銀行のボットから始まり、ログ、ログイン、パスワードを収集しました。それはお金が目的です」
「まあ、個人的な願望があったの違いないとしても、あなたは成功した会社をゼロから育てたと思う。もしそれが合法的なビジネスだったら、あなたはすでに海外でヨットを買っているだろう」
「そして今、私はあなたが Conti と、そして Ryuk と一緒に働いているのを見ています」
「ちなみに、Dridex はどうですか？彼と一緒に働いていますか？」
「よろしければ、ここから追い出さないでください。まだ話せるかもしれません」
「dridex は約 3-5 年前に聞いた」
「まぁ彼らもロッカーにいます」
「Trickbot は本当に面白い」
「Emotet も面白いけど、何も知らない」
「emotet、はい、作者は美しく、彼女は安定してサポートしています」
「あなたはロシア出身ですか？」
「ロシアと呼ぶのは難しい：D」

- **TrickBot が検知されてしまったということに対する検出回避部署のサポートのやりとり**

「ono54.exe は Win32 / Trickbot.L として検出されてしまいました」
「購入直後ですか？」
「レポートを送ってもらえますか？」
「WindowsDefender は、マルウェアまたはその他の望ましくない可能性のあるソフトウェアを検出しました。詳細については、以下を参照してください。」
「はい、すぐに」

- **マルウェアの検知について技術的な会話をする様子**

「カスペルスキーはどうですか？反応しない？」
「プロセスハローウィングでは、ResumeThread に反応します。ResumeThread はさまざまな方法で試しましたが、役に立ちません。」
「ResumeThread は難読化されていますか？」
「それはプロセスハローウィングですか、それともドッペルギャンギングですか？」

- **「CrowdStrike」の購入に苦慮している様子**

「こんにちは、2 つのアンチウイルスを他のアンチウイルスに置き換えることは可能ですか？CrowdStrike について話しているのですが、実際、彼らは営業担当者を通じてオフラインでのみライセンスを販売しています。私は彼らに連絡しました。月曜日、昨日メールに書いたのですが、今のところ返事がありません。どうしても購入できない場合は、トライアルで再度アクティベートを試みますが。Crowdstrike は別として、トレンドマイクロだけが残っており、残りはすでにディフェンダーに送られています。」

- **様々なアンチウイルス製品のライセンス価格や購入に関するやりとり**

「こんにちは、ESET のライセンスを確認できますか？」
「5 台のデバイスのクラウド管理付きのライセンスが 239 ドルまたはその場で 190 ドル必要ですか？」
「トレンドマイクロの 5 台のデバイスのライセンス 299.35 ドル？」
「ソフォスアカウントは更新する場合、電話でオフィスに連絡するか、徒歩でオフィスに行く必要があります。」
「パネルに正しい「購入」ボタンが表示されない場合がありますか？」
「クラウドを介した 5 台のデバイスの ESET ENDPOINT PROTECTION は高価ですが、それだけの価値があります」
「トレンドマイクロのビジネスセキュリティサービスアドバンスト 2 ユーザーは 1 年間 119.74」
「SymantecEndpointProtection-ノートン」
「Sophos」
「ここで買えます」

「こんにちは、トレンドマイクロのライセンスを購入しました。詳細を確認するためにサポートにメールしました。取引は銀行で確認されましたが、ありました。カードなしでの払い戻しはありません。まだ回答はありません。」
「わかりました。トレンドにマイクロを貼り付けます」
「ノートン、ソフォンは進行中ですか？」
「はい、少なくともあと 1 つは十分なはずです」
「他に CrowdStrike を買う方法...」

「ESET のライセンスは購入されていません」
「Bitdefender のライセンスを購入しました」
「こんにちは。念のために言っておきますが、彼がキットをテストできるように、本番サーバーでグループのアカウントを作成する必要があります」
「ソフォスのライセンス、購入されていません」
「トレンドマイクロ、ライセンスを購入しました」
「マカフィー、ライセンスを購入しました」
「シマンテック、ライセンスは購入されていません」
「アバスト ライセンスを購入しました。」
「ウェブルート、ライセンスは購入されていません」
「前回の購入以来、自宅のライセンスを含む企業ライセンスの一部を購入しました。問題は、eset、Norton、Sophos、Trend micro、Webrut の企業バージョンで発生しました。」

- **セキュリティ製品による検知テストに関するやりとり**

「彼が言う唯一のことは、一部の AV がブロックされているということです。現在、トレンドマイクロと ESET からの検出除外を行っています。」
「トレンドマイクロとウェブブリュットはウイルスを発見しませんでしたか？」
「トレンドマイクロとウェブルートは間違いなく検出している」

- **Conti ギャングの雇用に関する情報（一部意味不明）**

「ギャングの給料明細
総額 85k
99947 コアチーム 62 名
33847 – リバースエンジニア 23 名
8500 - 新しいコーディングチーム 6 名、今のところ 4 名しか給料をもらっていない
12500 侵入テスター6 名
10000 OSINT 部門 4 名

3,000（ソフトウェアテスター/サーバー）
月総額 164.8k」

- **100 人のエンコーダーを雇いたいという書き込み**

「結局、私は新しい人々からすべてを正しく理解しましたか？夏の終わりまでに最大 100 のエンコーダーを雇いたい」

- **Conti の従業員が様々な諸経費に資金が足りないと訴えている書き込み（一部意味不明）**

「こんにちは、ビットコインが不足しています、合計 8 つの新しいサーバー、2 つの VPN サブスクリプション、および 18 の拡張。2 週間先の更新はビットコインでわずか 1240 ドルです。0.025 は、Felipe のオーダーのために早く出てきました、彼は悪用サーバーを必要とし、グリーンは支払うために約 10 アドレスを送っていました、今 Manuel も 2 つのウイルス対策製品のライセンスを要求しています。ビットコインをこのウォレットに送ってください。」

- **新入に先輩が日々の仕事を語る様子**

「組織の詳細はありますか？オンラインのとき、どのくらいの時間働きますか？」
「はい、明確にしましょう。あなたのタイムゾーンは何ですか？」
「+0」
「MSK」（モスクワ標準時）
「よかった。8 時間の勤務日がある」
「私たちはモスクワ時間の 20-21 まで働く必要があります」
「これは恒久的な仕事ですか、それとも一時的な仕事ですか？」
「常に」
「素晴らしい」
「ええ、そしてキャリアアップは可能です」
「最初はテスターとして始めましたか？」
「ええ」
「1 年以上前に」
「営業日は正確に何時に始まりますか？フォーラムの書き込みを見たとき、9 時から 18:00 まで表示されていました。」
「まあ、9 時から 18 時は完全には正しくありません、11 時から 20-21 時が良いでしょう」
「わかりました、素晴らしい」

- **ウイルス対策製品に検出されないようにする業務を行う先輩が新入に作業を教える様子**

「マシンはテストの準備ができていますか？」
「はい、スナップショットから復元する必要があります」
「AV（ウイルス対策製品）を更新」
「そして、10 と 2019 の新しいスナップショットを作成します」
「わかりました」
「テストサイクルはウイルス対策製品のアップデートごとに繰り返します。Windows Defender のデータベースのアップデートは約 4 時間ごとにリリースされますので。」
「了解しました」

- **ウイルス対策製品に検出されないようにどうすべきかを会話している様子**

「時間があれば、答えを教えてください」。
「例えば、プログラムがレジストリに書き込むと、ウイルス対策ソフトはそれに気づきます。それに気づかれないようにするには、例えば別のプログラムにレジストリを調べさせて、そこに別のプログラム、例えば BITS を書き込むなど、動作を変える必要があります。」
「Kremez によると、最近 Ryuk の感染速度が落ちているそうです。"脅威の主体が休暇のような状態になっているのでしょう"と言っています。」
「静的検出を除去するには、プログラムコードの中から、この検出を行う場所を見つけ、それを変更する必要があります（例：ゴミのコードを追加する、コード内の行を入れ替える、関数呼び出しの順番を変える、など）。しかし、プログラムの動作そのものは変わりません。」

- **Trickbot の停止について会話している様子**

「トリック（TrickBot）が死んだ、そうだろ？」
「Mango は閉鎖すると言っている」

- **初期アクセスとして SonicWall VPN を狙っている様子**

「誰がソニックウォールの脆弱性を理解し、動作するスキャナーを作成できるか」
「この件、CVE-2020-5135:重大な SonicWallVPN ポータルスタックベースのバッファオーバーフローの脆弱性」

- **（ロシアの諜報機関 FSB との関連性示唆）2020 年 8 月に毒殺未遂事件に遭ったアレクセイ・ナワリヌイと思われるファイルを標的にしていると推測される趣旨の会話を行う様子**

"兄弟よ、我々は政治に携わるのか？")
"どのような点で？"
"<johnyboy77>重要な情報があるのなら
[21:04:21] <johnyboy77> それとも点数だけ？

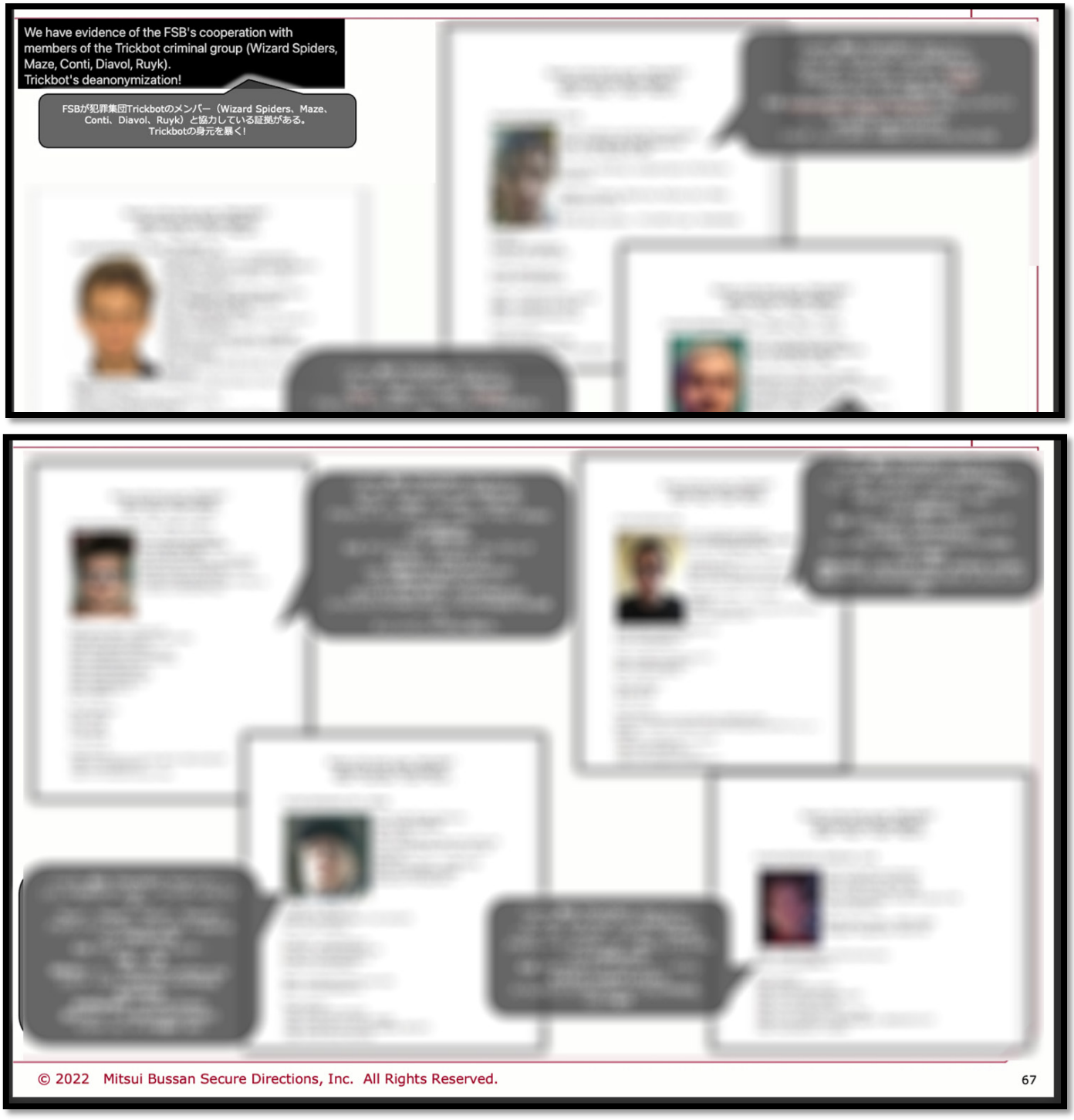
[21:10:55] <Mango> やぁ、兄さん。
[21:11:06] < Mango > 具体的な取得）
[21:11:12] <johnyboy77> こんにちは。
[21:11:13] < Mango > 私たちはお金のために働いている :）
[21:11:20] < Mango > 誰から欲しいかなんて、どうでもいいんです。
[21:11:22] <johnyboy77> 対ロシア工作員（ロシア反対派の人々）の通信記録をリークしてみました。
[21:11:25] <johnyboy77> 情報フィールドで
[21:11:31] <johnyboy77> しかし、復号できない。
[21:11:34] <johnyboy77> 信号の対応
[21:11:52] <johnyboy77> ショートジャーナリスト
[21:11:54] < Mango > 聞かせてください）
[21:11:55] <johnyboy77> ロシアに対して強気なのは誰だ？
[21:12:04] <johnyboy77> ただ、このクソファイルを解読することはできません。
[21:12:13] <johnyboy77> the fuck up happened".
"これは必要なのか？"
"通信の解読の仕方がわからない"
"政治的な騒ぎを起こさずに 金で解決する" か
"E2E だ"
"ごめんなさい、どうしようもないんです。
"したい "とさえ思う。
しかし、私にはどうすることもできない。
"さて、このようなデータに興味はあるかな？"
"愛国者 "なのか "愛国者 "なのか？）
"もちろん私たちは愛国者です")
"解読されたら連絡する"
"先日、オウキオンのことも書きましたが、お忙しいと思い、手を付けませんでした)"
"[21:21:02] <johnyboy77> まもなく bellingcat から男性向けメールあり。
[21:21:06] <johnyboy77> 特に ru と ua を担当するのは誰ですか？
[21:21:06] <johnyboy77> そう言ってください。
[21:21:08] <johnyboy77> そして全てのパスワードがそこにある。
[21:21:17] <johnyboy77> そして、それはまだ有効です。
[21:30:56] < Mango > まあ、少なくとも彼の通信のスクリーンショットを撮っておいてください。
[21:31:05] < Mango > 具体的なブローが必要です。
[21:31:07] <johnyboy77> さて、ファイルをアップロードします。
[21:31:12] <johnyboy77> NAVALNI FSB
[21:31:13] <johnyboy77> こんな感じです。

- **3/4 執筆時点で最新のチャットログが暴露/Conti の内部で混乱が起きている様子がわかる**

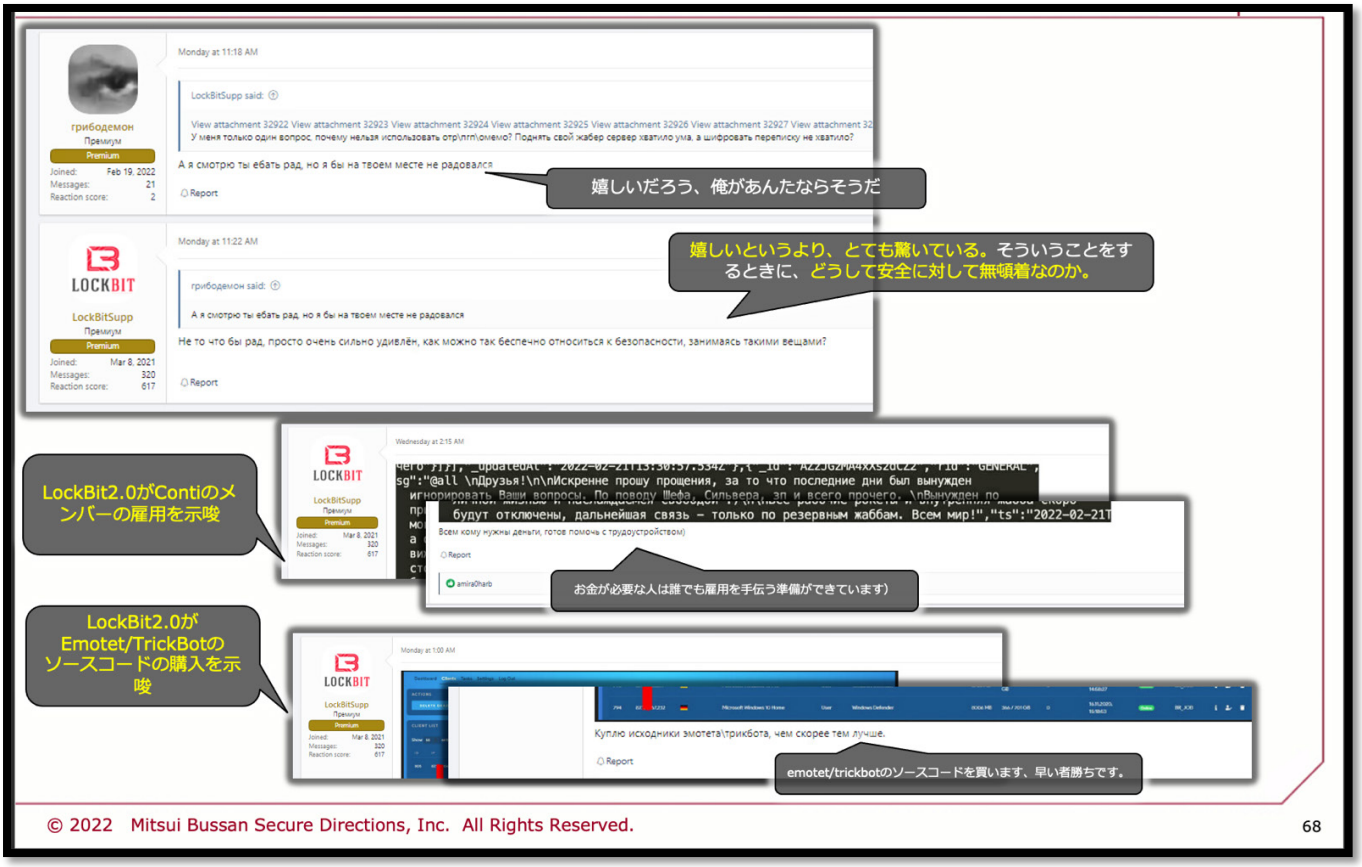
"複製"
"聞け、アジムとスメリアンが今日手紙をよこした。" "彼らは自分たちがバラバラになるのを心配している。
私たちに何か手を出しているのでは？
何を伝えればいいんだろう？"
"了解しました、メールします"
"わかった"
"こんにちは"
"誰がリークしたか、わかったか"？
反乱を起こすか?
"おい、何の話だ？"
"何について？"
"ちょっと
チャットルームのパトリックです。
あなたは誰ですか？
"何の知らせだ？いつになったら反乱を起こすんだ？"
"仕事に行くのか？網が待ってるんだぞ"
"私はここにいる、明日もそこにいる"
「ねえ、給料をもらっていい？最後にイエスと言ったはずなのに..."
"こんにちは、すべての VM ファームをクリアして削除しました、サーバーがダウンしています"
"こんにちは、どうですか？
"環境は全て抹消し、サーバーは停止させた"
"私のヒキガエルのバックアップが必要ですか？"
"私はここにいる、明日もそこにいる"
"待ってる"
"緊急に必要とされている"
"すべて分身に話せ" "報告書と金のことを話せ"
"トランポを経て連絡を"
"このヒキガエルがすべてだ"
"さあ"

■その他、補足情報

本暴露に関連する事象として、その後別のアカウント名からも、攻撃グループ「Trickbot/Conti」のメンバーとされる人物らの個人情報を含む情報が多数暴露され始めている。また本執筆時の最新データによると、攻撃グループのメンバーの一部にサイバーセキュリティ企業の研究開発部門で働く人物と主張する情報も含まれていることを確認している。



また Conti と並び 2 大巨頭ともいえる攻撃グループ「LockBit2.0」が ContiLeaks に反応、今回の件を受けて Emotet や TrickBot のソースコードの購入や Conti メンバーの雇用を示唆するコメントなどをロシアのハッカーフォーラムで残している。



以上

三井物産セキュアディレクション株式会社
https://www.mbsd.jp