Legal Wire

pillsbury

Japan Practice

Vol. 157 / December 2023

国際ランサムウェア対策イニシアチブ、政府の身代金支払い停止を誓約、ただし例外も

–米国では、当該誓約は連邦政府による支払いのみを制限し、州政府や地方政府、民間企業による支払いは制限されず

ブライアン・E・フィンチ、エイミー・P・ゴーシュ、アマリス・トロッツォ

- 10 月 30 日から 11 月 1 日にかけて、ワシントン D.C.で国際ランサムウェア対策イニシアチブ（CRI）第 3 回年次総会が行われ、ランサムウェア攻撃に対する集団的な強靭性を構築することを再確認しました。

- CRI のメンバーは、ランサムウェア攻撃者の意欲を削ぎ、ランサムウェア攻撃によってもたらされる金銭的インセンティブを弱めるために、政府機関はランサムウェア恐喝の金銭支払に応じるべきではない、という共同声明（誓約）を発表しました。

- 米国では、上記誓約は連邦政府による支払いのみを制限するものであり、州政府や地方政府、民間団体による支払いは制限されません。また誓約には、政府が必要と判断した場合に身代金の支払いを認める緊急時の例外が規定されています。

年次総会

国際ランサムウェア対策イニシアチブ（CRI）は、48 か国、欧州連合（EU）、国際刑事警察機構（INTERPOL）で構成される国際的な枠組みです。米国は、本年次総会の開催国であるだけでなく、CRI の事務局も務める、CRI の主要メンバーです。CRI の目的は、"ランサムウェアの実行可能性を弱め、責任者を追跡する協力をし、ランサムウェアのエコシステムを支える不正資金に対抗し、ランサムウェア攻撃への対策を行うため民間セクターと協力し、ランサムウェアの脅威のすべての要素に対処するために国際的に協力する "ことです。ランサムウェアの脅威に対する集団的な安全保障を強化するため、CRI はメンバー間の協力関係と情報共有に重点を置いています。

CRI は、ランサムウェアの脅威と活動の増加に対抗するために設立されました。ランサムウェア攻撃は、攻撃者が組織のデータを暗号化して開けなくした上で、データを元に戻す代わりに身代金の支払いを要求する点で、他のサイバー攻撃とは異なります。別のシナリオとして、ランサムウェア攻撃者は、保持するデータを暗号化するだけでなく、身代金を支払わなければ機密データを一般に公開すると脅すこともあります。

米国では、2022 年 5 月から 2023 年 6 月までの間、ランサムウェアの被害者が 15 億ドルの身代金を支払っています。米国の組織は最大の標的であり、米国国家安全保障担当副補佐官のアン・ニューバーガー氏によると、世界のサイバー攻撃の 46%が米国人に集中しています。

誓約

11 月 1 日、CRI の全メンバーは、ランサムウェア攻撃に関連して政府が身代金を支払うべきでない、とする宣誓を表明しました。しかし、この誓約は、身代金の支払いを全面的に禁止するものではなく、政府が具体的な事案に応じて、身代金の支払いを認めるかどうかや、緊急事態の例外をどのように適用するかについて判断する余地を認めるものです。緊急事態には、特別な組織に対するランサムウェア攻撃、例えば患者の健康が差し迫った危険にさらされている病院に対する攻撃等が含まれます。CRI は、この共同声明の目標を達成するため、不正ウォレットのデータ共有に関する米国財務省の協力を通じ、ランサムウェア活動に使用される電子ウォレットのブラックリストを作成する予定です。

また、この誓約は政府機関に限定されています。米国では、連邦政府機関の活動のみにこの誓約は適用され、州および地方政府は除外されています。企業は、独自の費用対効果の分析に基づいて、身代金支払いに関する決定を下すことができます。しかし、支払いを禁止する明確な文言こそないものの、48 か国が支持した誓約は、悪意のある行為者に対し、政府から要求を引き出せることを期待すべきではない、という明確なメッセージを送っています。

CRI の取り組み

上記誓約に加えて、CRI は、メンバー間の協力関係を強化するためのいくつかの行動を起こしています。第 3 回年次総会で発表されたように、2 つの新しい情報共有プラットフォームが近い将来立ち上げられる予定です。1 つ目は、リトアニアが作成したマルウェア情報共有プラットフォームです。もう 1 つは、イスラエルとアラブ首長国連邦が共同プロジェクトとして作成した、データベース、仮想調整プラットフォームおよび連絡先リストを備えた情報共有プラットフォーム「Crystal Ball」です。これらのプラットフォームにより、CRI メンバーは、ランサムウェア攻撃、攻撃の容疑者、進行中の捜査の進展などに関する詳細を共有できます。それにより、被害者が恐喝される前に攻撃を阻止するための集団的な取り組みが促進されます。CRI は、情報の流れを促進するために、メンバーが毎週平均 1 件程度の情報をプラットフォーム上で共有することを期待しています。

第 3 回年次総会のその他の成果としては、人工知能を活用してブロックチェーンのデータを分析し、ランサムウェアのプログラミングに対抗するプロジェクトの立ち上げが挙げられます。また、いくつかのメンバーは「政府やライフライン機能がランサムウェア攻撃を受けた場合、インシデント対応において他の CRI メンバーを支援する」ことも表明しました。さらに、CRI の新メンバーには、サイバー能力を高めるためのメンターシップや戦術トレーニングプログラムの機会が提供されることとなりました。

今後 1 年間、CRI は新規メンバーの受け入れやトレーニングを行い、ランサムウェア攻撃の財務モデルについて理解を深め、各国のランサムウェア対策能力を構築するための情報を共有していく予定です。

CRI の活動は、米国内の他のランサムウェアに焦点を当てた活動を前進・補完する役目も果たします。例えば、合同ランサムウェア対策委員会（Joint Ransomware Task Force）です。同委員会は、ベストプラクティスの発展、調査の実施、ガイダンスの提供、情報の共有を通じて、ランサムウェア攻撃に対処するための連邦政府の各種ツールを調整する省庁間組織で、サイバーセキュリティ・インフラストラクチャ・セキュリティ局と連邦捜査局が共同議長を務めています。同委員会は、ランサムウェア対策のガイダンス（#StopRansomware Guide）を通じて、ランサムウェアの脅威から施設、職員、顧客を守るための「ワンストップ・リソース」を作成し、更新しています。同委員会が米国の各組織に提供するガイダンスを今後も更新し続けること、そして CRI から学んだ教訓を取り入れていくことが、今後期待されます。

本稿の原文（英文）につきましては、International Counter Ransomware Initiative Pledges to Halt Government Ransom Payments, but with Exception をご参照ください。

本稿の内容に関する連絡先

Brian E. Finch
brian.finch@pillsburylaw.com

Aimee P. Ghosh
aimee.ghosh@pillsburylaw.com

Amaris Trozzo
amaris.trozzo@pillsburylaw.com

ジェフ・シュレップファー（日本語版監修）
jeff.schrepfer@pillsburylaw.com

加藤 卓也（日本語版作成協力）

東京オフィス連絡先

サイモン・バレット
simon.barrett@pillsburylaw.com

松下 オリビア（日本語対応可）
olivia.matsushita@pillsburylaw.com

ニューヨークオフィス連絡先

秋山 真也
shinya.akiyama@pillsburylaw.com

Legal Wire 配信に関するお問い合わせ

田中里美
satomi.tanaka@pillsburylaw.com