2020年11月26日

ランサムウエアによるサイバー攻撃について【注意喚起】

2020年11月26日、内閣サイバーセキュリティセンターは、重要インフラ事業者等に向けてランサムウエアによるサイバー攻撃について注意喚起を行いました。

また、本件は、昨今、ランサムウエアによるサイバー攻撃が国内外の様々な組織で確認されていることを踏まえ、あらかじめ、予防策、感染した場合の緩和策、対応策などを検討しておくための注意喚起ですが、広く一般にも活用していただけるよう公開するものです。

資料　ランサムウエアによるサイバー攻撃について(注意喚起)

本件に関する連絡先
内閣サイバーセキュリティセンター
電話番号03-5253-2111（代表）
重要インフラ第２グループ

2020 年 11 月 26 日

内閣サイバーセキュリティセンター
重要インフラグループ

ランサムウエアによるサイバー攻撃について(注意喚起)

ランサムウエアによるサイバー攻撃が国内外の様々な組織で確認されており、注意が必要です。

1. 概要

ランサムウエアによるサイバー攻撃の高度化・巧妙化、攻撃活動が活発になっており、本年度に入ってから、我が国及び関連する海外の組織でランサムウエアの感染による業務支障が多く報道されています。とりわけ、本年は新型コロナウイルス感染症拡大防止対策により、リモートアクセス環境やインターネットからアクセス可能な機器等の外部ネットワークの利用が拡大しており、こうした接続点から組織内のネットワークに侵入する事例が多く確認されています[1]。また、ネットワークで接続される海外グループ会社を含め、セキュリティ対策の弱い拠点から侵入される事例が確認されています[2]。

今のところ、我が国の重要インフラ事業者等において問題となっていませんが、ランサムウエアの感染は、経済、社会に大きな支障を与えることを踏まえ、あらかじめ、予防策、感染した場合の緩和策、対応策などを検討しておくことが重要です。

2. 最近のランサムウエアの特徴

(1) 2 段階の脅迫

従来のランサムウエアによるサイバー攻撃は、PC 等のデータを暗号化し、利用不能とさせ、復元のための身代金を要求するものでした。他方、2019 年以降、「Maze」、「Sodinokibi(別名:REvil)」、「Clop」、「Snake(別名:EKANS)」、「Ragnar Locker」、「Ako」等のランサムウエアにおいて、従来の手法に加え、あらかじめ窃取したデータを公開すると脅迫し、身代金を要求する手法がみられるようになってきました[3]。

(2) 人手によるランサムウエア攻撃 (human-operated ransomware attacks)

標的型攻撃等で利用される手法を用いて、標的の組織のネットワークに侵入し、機密情報や重要情報が格納されたサーバーを特定し、ランサムウエアに感染させる攻撃が報告されています[4]。本攻撃は、機械的に実行されるものとは異なり、攻撃者が組織

---

[1] *NHK「リモート接続ねらうサイバー攻撃が急増 テレワーク増加で(2020/11/12)」、https://www3.nhk.or.jp/news/html/20201112/k10012708711000.html (2020/11/26 閲覧)*

[2] *経済産業省「昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について(2020/6/12)」、https://www.meti.go.jp/press/2020/06/20200612004/20200612004-1.pdf (2020/11/26 閲覧)*

[3] *NEC「二重脅迫ランサムウェア攻撃の増加について(2020/7/31)」、https://jpn.nec.com/cybersecurity/blog/200731/index.html (2020/11/26 閲覧)*

[4] *IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について(2020/8/20)」、https://www.ipa.go.jp/security/announce/2020-ransom.html (2020/11/26 閲覧)*

内を十分探索した後に攻撃が実行されるため、被害規模が大きくなるものです。最近の標的型攻撃の侵入経路には、新型コロナウイルス感染症拡大防止対策として急遽構築したテレワーク環境の設定ミスによるもの[5]、SNS(ソーシャル・ネットワーキング・サービス)を利用したもの[6]、MSP(マネージドサービスプロバイダー)[7]を経由して組織に侵入するもの[8]があることも考慮に入れる必要があります。

3. 対応策

米国サイバーセキュリティ・インフラセキュリティ庁(CISA)は、米国の医療機関や医療提供者に対するサイバー犯罪の脅威が増大しているとして、2020 年 10 月 28 日にランサムウエアを利用したサイバー攻撃に対するアドバイザリを公開しています[9]。

我が国においても、ランサムウエアの感染により、組織が保有する機微情報や個人情報等が攻撃者に窃取され、外部に公開される事案やサーバー等に格納した情報が暗号化される事案が発生しています。

こうしたことを踏まえ、海外での発生状況を教訓として、我が国においても適切な対応が必要です。

ランサムウエアを利用した攻撃への対応策の例を以下に示しますが、これは一例にすぎず、組織によって、保護すべき内容、ネットワーク構成が異なることなどを踏まえ、各重要インフラ事業者等の CISO、CSIRT、SOC、サイバーセキュリティ関係者は、自らの組織の実態を踏まえ、適切な対応をとることが必要です。

(1) ランサムウエアの感染を防止するための対応策(予防)

ランサムウエアの感染を防止する観点から、組織のネットワークと外部との接続点の堅牢性について確認のうえ、対策が必要です。

- インターネットからアクセス可能な機器について、インターネット公開の必要性を確認する。インターネットからアクセスする必要がある機器については、セキュリティパッチを迅速に適用する、不要なポートやプロトコルを外部に開放しない等の対策を講じているか確認する。

- リモートアクセス環境を構成する製品に対する迅速なアップデートや適切な設定が行われているか確認する。特に、Virtual Private Network (VPN) 機器の脆弱性等を利用し、組織に侵入する事例が多く確認されていることから、VPN 機器に対するセキ

---

[5] *NHK「狙われるリモート社会(2020/11/12)」、https://www3.nhk.or.jp/news/html/20201112/k10012707531000.html (2020/11/26 閲覧)*

[6] *ESET「Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies (2020/6/17) 」、https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/ (2020/11/26 閲覧)*

[7] *顧客の利用する IT 環境の運用、監視、保守等を請け負う事業者*

[8] *ウォッチガード・テクノロジー・ジャパン「MSP インフラストラクチャを標的とし、ランサムウェアをインストールする攻撃につい(2019/7/8)」、https://www.watchguard.co.jp/security-news/msps-beware-attackers-targeting-msp-infrastructure-to-install-ransomware.html (2020/11/26 閲覧)*

[9] *CISA「Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector(2020/10/28)」、https://us-cert.cisa.gov/ncas/alerts/aa20-302a (2020/11/26 閲覧)*

ュリティ対策の重要性を強く認識し、迅速なセキュリティパッチの適用、VPN 機器やクラウドサービスに対する多要素認証の導入の検討等について、十分留意する。

・ 自組織で使用している PC やサーバー等の OS、アプリケーション等が常に最新化されているか確認する。特に、ドメインコントローラーの深刻な脆弱性（CVE-2020-1472）[通称：Zerologon]を悪用し、組織内で侵害範囲を拡大する事例が多く確認されていることから、本脆弱性への対応については、特に留意する。

・ 必要な機器にウイルス対策ソフトが導入され、パターンファイルが最新化されているか確認する。また、定期的にスキャンが実行される設定になっているか確認する。

(2) ランサムウエアによるデータの暗号化に備えた対応策(予防)

従来のランサムウエア対策の常套手段であったバックアップは、引き続き有効です。しかし、2 重脅迫ランサムウエアに感染した場合は、組織の機微データ、個人情報が流出する懸念があることから、「機微データの厳格管理」については、改めて検討する必要があります。

・ 重要なデータに対する定期的なバックアップの設定を確認する。バックアップの検討に当たっては、ランサムウエア感染時でもバックアップが保護されるように留意する。例えば、バックアップをオフラインで保管する、クラウド上や外部のストレージ上に重要なデータをコピーし、コピーしたデータは保護対象のネットワークからアクセスできないようにする等の対策を講じる。

・ バックアップで取得したデータをもとに、実際に復旧できることを確認する。

・ 公開された場合、業務に支障が生じるような機微データや個人情報等に対して、特別なアクセス制御や暗号化を実施する。

・ システムの再構築を含む復旧計画が適切に策定できているか確認する。

(3) 不正アクセスを迅速に検知するための対応策(検知)

不正アクセスを迅速に検知するための対応策が必要です。迅速な検知を実現するためには、オペレーターとマシンによる自動化を検討する必要があります。

・ サーバー、ネットワーク機器、PC 等のログの監視を強化する。

・ 振る舞い検知、EDR(Endpoint Detection and Response)、CDM(Continuous Diagnostics and Mitigation)等を活用する。

(4) 迅速にインシデント対応を行うための対応策(対応・復旧)

ランサムウエアによる攻撃の被害を受けた場合でも、冷静で適切な対応ができるように、組織一丸となった対処態勢を構築する必要があります。

・ データの暗号化及び公開を想定した対処態勢、対処方法、業務継続計画等を含むランサムウエアへの対応計画が適切に策定できているか確認する。

・ 自組織に携わる職員がランサムウエア感染の兆候を把握した場合、職員が迅速にシステム管理者に連絡できるか確認する。

参考 URL
- 【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について（IPA）
  https://www.ipa.go.jp/security/announce/2020-ransom.html
- CISA and MS-ISAC Release Ransomware Guide（CISA）
  https://us-cert.cisa.gov/ncas/current-activity/2020/09/30/cisa-and-ms-isac-release-ransomware-guide
- FBI FLASH MU-000140-MW（WaterISAC）
  https://www.waterisac.org/system/files/articles/FLASH-MU-000140-MW.pdf