添付資料

2021 年 4 月 30 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関する注意喚起

ランサムウエアによるサイバー攻撃に対する対応策を講じ、重要インフラ事業者等の十全なサイバーセキュリティ確保に務めてください。

1. 概要

ランサムウエアによるサイバー攻撃が活発になっており、日本企業や海外子会社で実際に攻撃者にデータが公開される事例が増えており、クライアント端末だけでなくサーバーも被害を受けています。

ランサムウエア感染によるデータの暗号化、業務情報や個人情報の窃取等の被害は、経済・社会に大きな影響を与えることを踏まえ、予防策、感染した場合の緩和策、対応策等を検討してください。

対策は、予防、検知、対応、復旧の観点から行う必要があります。以下、具体的な対応策の例を示すので、参考にしてください。

① 【予防】ランサムウエアの感染を防止するための対応策
② 【予防】データの暗号化による被害を軽減するための対応策
③ 【検知】不正アクセスを迅速に検知するための対応策
④ 【対応・復旧】迅速にインシデント対応を行うための対応策

2. 具体的対応策

(1) 【予防】ランサムウエアの感染を防止するための対応策

最近のランサムウエアの侵入経路は以下のようなものがあり、これらを踏まえた予防策が必要です。

① インターネット等の外部ネットワークからアクセス可能な機器の脆弱性によるもの
② 特定の通信プロトコル(RDP や SMB)や既知の脆弱性を悪用した攻撃によるもの[1]
③ 新型コロナウイルス感染症対策として急遽構築したテレワーク環境の不備によるもの
④ 海外拠点等セキュリティ対策の弱い拠点からの侵入によるもの
⑤ 別のマルウエアの感染が契機となるもの

[1] *US-CERT(Twitter)「US-CERT(@USCERT_gov)の投稿(2021/4/29)」、https://twitter.com/USCERT_gov/status/1387435697037094919 (2021/4/30 閲覧)*

チェックポイント

- インターネット等外部ネットワークからアクセス可能な機器については、外部ネットワーク公開の必要性を十分検討したうえで、セキュリティパッチを迅速に適用する、外部からの管理機能、不要なポート(137(TCP/UDP)、138(UDP)、139(TCP)、445(TCP/UDP)、3389(TCP/UDP)など)やプロトコルを外部に開放しない等の対応策等、IT 資産管理を改めて確認する。特に、通信プロトコル「SMB」や「RDP」については、これまでも必要最小限のポートの開放や SMBv1 の無効化等を呼びかけているところ、ファイアウォールを含む各機器の設定を改めて確認する。
- ソフトウエアや機器等の脆弱性については、ランサムウエアを用いる攻撃者グループによる悪用が報告されているものを含む以下の脆弱性に十分留意する。
  - Fortinet 製 Virtual Private Network(VPN)装置の脆弱性(CVE-2018-13379)[2]
  - Ivanti 製 VPN 装置「Pulse Connect Secure」の脆弱性(CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510)[3]
  - Citrix 製「Citrix Application Delivery Controller」「Citrix Gateway」「Citrix SD-WAN WANOP」の脆弱性(CVE-2019-19781)[4]
  - Microsoft Exchange Server の脆弱性(CVE-2021-26855 等)[5]
  - SonicWall Secure Mobile Access (SMA) 100 シリーズの脆弱性(CVE-2021-20016)[6]
  - QNAP Systems 製 NAS(Network Attached Storage)製品「QNAP」に関する脆弱性(CVE-2021-28799、CVE-2020-36195、CVE-2020-2509 等)[7]
  - Windows のドメインコントローラーの脆弱性(CVE-2020-1472 等)[8]
- テレワーク等に関連し、職場から持ち出した PC について、休暇中に長期間、十分な管理下になかった PC を職場で再び利用する際は、パッチの適用やウイルススキャンの実施など必要に応じて実施する。
- 最近では、マルウエア「Emotet」に代わり、マルウエア「IcedID」に感染させる不正なメール等も確認されていることから、ウイルス対策ソフトの導入及び最新化、定期スキャンの実施、メール環境に対するセキュリティ対策等、通常のマルウエア対策も実施する。

---

[2] *NISC「Fortinet 製 VPN の脆弱性(CVE-2018-13379)に関する重要インフラ事業者等についての注意喚起の発出について(2020/12/3)」、https://www.nisc.go.jp/active/infra/pdf/fortinet20201203.pdf (2021/4/30 閲覧)*

[3] *Ivanti「Pulse Connect Secure Security Update(2021/4/20)」、https://blog.pulsesecure.net/pulse-connect-secure-security-update/ (2021/4/30 閲覧)*

[4] *Citrix「CVE-2019-19781 - Vulnerability in Citrix Application Delivery Controller, Citrix Gateway, and Citrix SD-WAN WANOP appliance(2020/10/23)」、https://support.citrix.com/article/CTX267027 (2021/4/30 閲覧)*

[5] *Microsoft「On-Premises Exchange Server Vulnerabilities Resource Center(2021/3/25)」、https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/ (2021/4/30 閲覧)*

[6] *SonicWall「CONFIRMED ZERO-DAY VULNERABILITY IN THE SONICWALL SMA100 BUILD VERSION 10.X(2021/4/30)」、https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001 (2021/4/30 閲覧)*

[7] *QNAP Systems「Response to Qlocker Ransomware Attacks: Take Actions to Secure QNAP NAS(2021/4/22)、https://www.qnap.com/en/security-news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas (2021/4/30 閲覧)*

[8] *Microsoft「CVE-2020-1472 Netlogon の特権の昇格の脆弱性(2021/2/9)」、https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2020-1472 (2021/4/30 閲覧)*

(2)【予防】データの暗号化による被害を軽減するための対応策

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。これに加え、2 重脅迫ランサムウエアに感染した場合は、組織の機微データや個人情報流出の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。

チェックポイント

- 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、ファイルのコピーを 3 個取得したうえで、ファイルは異なる 2 種類の媒体に保存、コピーのうち、1 個はクラウドサービスや保護対象のネットワークからアクセスできない場所等に保管するといった対策等を検討する。
- バックアップデータから実際に復旧できることを確認する。
- 公開された場合、実際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ことを確認する。

(3)【検知】不正アクセスを迅速に検知するための対応策

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。

チェックポイント

- 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)【対応・復旧】迅速にインシデント対応を行うための対応策

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。

チェックポイント

- データの暗号化、公開、インターネット公開サーバーに対する DoS 攻撃等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。
- 一部の職員が長期休暇中やテレワーク等であっても、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ことを確認する。
- ランサムウエアの感染による被害を受けた場合に、組織内外(業務委託先、関係省庁を含む)に迅速に連絡できるよう、連絡体制を確認する。

参考 URL

- ランサムウエアによるサイバー攻撃について【注意喚起】(NISC)
  https://www.nisc.go.jp/active/infra/pdf/ransomware20201126.pdf
- 【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
- 大型連休等に伴うセキュリティ上の留意点について(NISC)
  https://www.nisc.go.jp/active/infra/pdf/renkyu20210426.pdf
- 最近のサイバー攻撃の状況を踏まえた経営者への注意喚起(経済産業省)
  https://www.meti.go.jp/press/2020/12/20201218008/20201218008-2.pdf
- 「EMOTET」後のメール脅威状況：「IcedID」および「BazarCall」が 3 月に急増（トレンドマイクロ）
  https://blog.trendmicro.co.jp/archives/27732
- So Unchill - UNC2198 ICEDID のランサムウェア・オペレーションへの融解(FireEye)
  https://www.fireeye.com/blog/jp-threat-research/2021/02/melting-unc2198-icedid-to-ransomware-operations.html
- 2021 年も増加傾向のランサムウェア、被害に関する共通点とは(LAC)
  https://www.lac.co.jp/lacwatch/report/20210405_002585.html
- UNC2447 SOMBRAT and FIVEHANDS Ransomware: A Sophisticated Financial Threat(FireEye)
  https://www.fireeye.com/blog/threat-research/2021/04/unc2447-sombrat-and-fivehands-ransomware-sophisticated-financial-threat.html