脆弱性対応研究会

2020/04/11-18 のランサムウェア ニュース
簡易レポート

発行：2020/04/19
脆弱性対応研究会

ランサムウェアニュース　概要

- インターポールが、ランサムウェアを使用して重要な医療危難を標的とするサイバー攻撃の試みが増加している、との報告（※1）
- 今年初めにランサムウェア攻撃を受けた Travelex は、システムをオンラインに戻すために 285bitcoin（230 万ドル）の身代金を支払った（※2）
- 02 月に発生した PENNCREST 学区へのサイバー攻撃は、データロック解除に 1 万ドル（保険会社が攻撃の調査費用含めて 7 万 5 千ドル支払った)を支払った（※3）
- COVID-19 のパンデミックにより、学校がランサムウェ攻撃の標的になる可能性がある（※4）
- 3 月にフロリダ州ジュピターに対してランサムウェア攻撃があったが、バックアップがあったことにより身代金支払いをせずに済んだ（※5）
- ポルトガルの電力会社 EDP がサイバー攻撃の標的となり、10TB の機密情報が盗まれ、1,580bitcoin（12 億円程度）の要求をされている（※6）
- CyberCube の報告書によると、攻撃対象は消費者から企業に代わり、今後はソーシャルエンジニアリングは人工知能（AI）を利用した大規模になるものと予想している（※7）
- 医療機関への攻撃は、500 人未満の施設への攻撃がターゲットとされている（※8）
- BleepingComputer のレポートによると、Sodinokibi ランサムウェアは、BTC の代わりに Monero を利用し始めた（※9）
- [物理 ransam]国際商工会議所（ICC）の国際海事局（IMB）によると、2020 年第一四半期で 37 隻の船に海賊が乗込み、誘拐事件も発生している（※X）

状況や対策

- 予防と緩和が鍵となる（※2）（※8）
    - ランサムウェアは電子メールを介して拡散するので、リンクをクリックしたり添付ファイルを開くのは、信頼されたソースのみから行う
    - すべてのハードウェアとソフトウェアを定期的に細心に保つことを推奨している
    - こまめに重要なファイルをバックアップしたり、メインとなるシステムとは別に保管する
    - すべてのシステムに最新のアンチウイルスソフトを入れ、常に起動していることを確認する
    - すべてのシステムで、協力でユニークなパスワードを使用し、定期的に更新する
    - 組織は、協力で実践的なインシデント対応計画が必要
    - リモート作業が増加しているため、ファイアウォール外にあるデバイスの脆弱性にも注意が必要
- バックアップはオフサイトへ置くことが有用（※2）（※5）（※8）
    - ネットワーク全体の暗号化、バックアップファイルの削除をされた
    - バックアップからの復旧で、身代金支払いをせずに済んだ
    - データのバックアップだけでは不十分で、オフラインバックアップやオフサイトへの保存が有効
- サイバー保険に加入する（※3）
    - データ復旧にかかる法外な費用を避けることができる
- ネットワーク活動の検出は重要（※3）
    - 数年間使用されていなかったホストが RD 接続を介して攻撃された
        - 以前、2018/12 に Nozelesn ランサムウェア攻撃を経験している
- 教育機関が狙われる（※4）
    - 01/01 から 04/08 の間に、少なくとも 17 の学区と大学がランサムウェア攻撃を受けた
    - これは去年の同時期（8）に比べ、2 倍以上の攻撃となる
    - COVID-19 により学術機関が遠隔学習プラットロームを利用することを攻撃者は知っているため、身代金を支払うための圧力をかけられる可能性が高くなる

リソース

- ※1
  - https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware
- ※2
  - https://newsdio.com/travelex-forked-billionaire-rescue-to-restore-its-systems/89046/
  - https://trendingnewsbuzz.com/2020/04/12/travelex-travelex-paid-2-3m-ransom-in-bitcoin-to-get-its-systems-back-from-hackers/
- ※3
  - https://insurancenewsnet.com/oarticle/penncrest-officials-cyber-attack-in-february-has-been-resolved#.Xpq7qcgzZPY
- ※5
  - https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/sodinokibi-attacks-florida-towns-digital-services/
  - https://www.infosecurity-magazine.com/news/revil-rocks-jupiter/
- ※6
  - https://www.explica.co/the-attackers-ask-for-a-ransom-of-10-million-according-to-a-portuguese-outlet/
  - https://www.bleepingcomputer.com/news/security/ragnarlocker-ransomware-hits-edp-energy-giant-asks-for-10m/
  - https://oilprice.com/Latest-Energy-News/World-News/Portugals-Energy-Giant-EDP-Hit-By-Ransomware-Attack.html
  - https://ourbitcoinnews.com/hackers-demand-ransom-of-r-55-million-in-bitcoins-from-an-energy-company-that-operates-in-brazil/
- ※7
  - https://www.insurancejournal.com/blogs/ijam/2020/04/17/565406.htm
- ※8
  - https://healthitsecurity.com/news/hackers-favor-small-hospitals-health-centers-as-ransomware-targets
  - https://www.fiercehealthcare.com/practices/hackers-target-small-hospitals-practices-for-ransomware-attacks
- ※9
  - https://coingeek.com/hacking-group-behind-sodinokibi-embraces-monero/
- ※X

- https://iccwbo.org/media-wall/news-speeches/piracy-and-armed-robbery-a-threat-to-ships-crews-warns-imb/

以上