製薬・医療業界を狙ったランサムウェアに関する動向

本資料は、新型コロナウイルスによるパンデミック発生以降に報道された主な製薬業界へのサイバーインシデント等の脅威動向を示します。

PwCコンサルティング合同会社
2020年9月

pwc

世界的なパンデミックの危機の中、製薬業界や医療業界はサイバー攻撃の標的になっています。特に、ランサムウェアと呼ばれるサイバー攻撃（ファイルを暗号化し、解除と引き換えに身代金を要求）が増加しています。

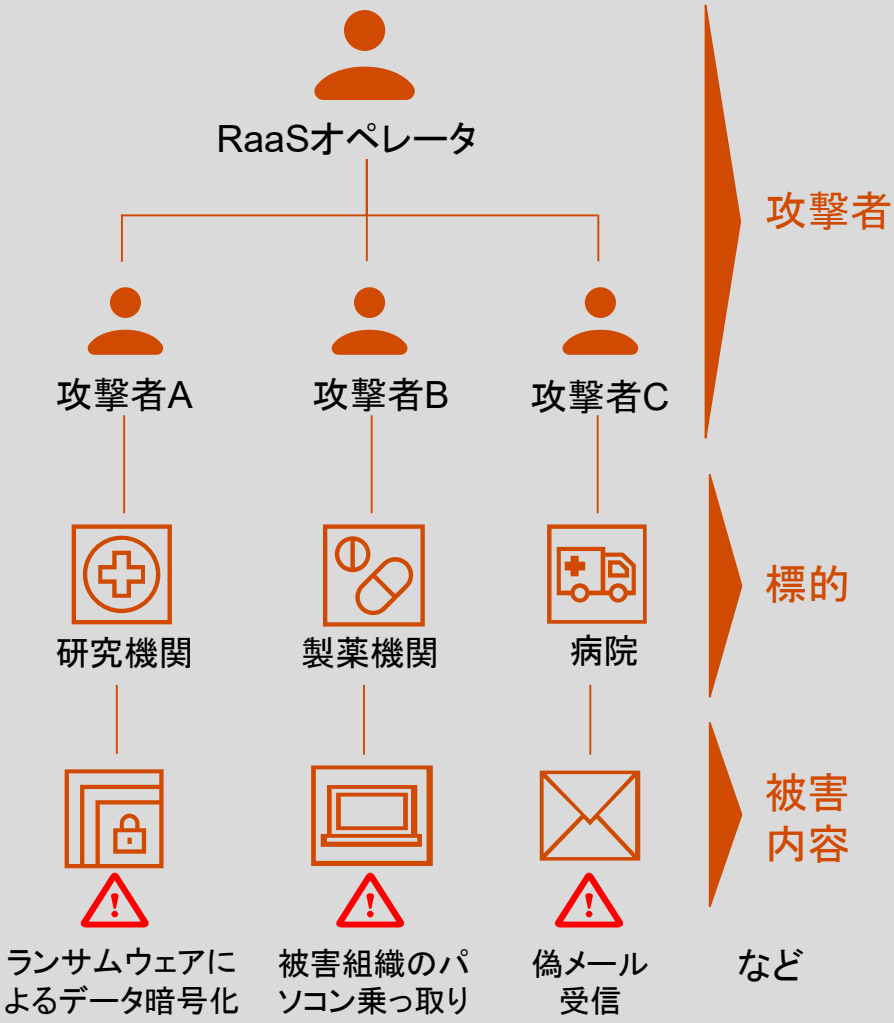
製薬業界や医療業界を狙った高度に組織されたランサムウェア攻撃

2020年7月、米国連邦捜査局（FBI）は、米国や海外の製薬・医療機関を標的にしたランサムウェアが大幅に増加していることを警告するフラッシュアラートを発表しました。サイバー攻撃者は、パンデミックに乗じて製薬・医療業界を狙い、金銭を要求していたことが確認されています。また、攻撃者は他の組織と連携し、ランサムウェア・アズ・ア・サービス（RaaS）と呼ばれる高度に組織化された攻撃を行っているという報告もあります。

製薬業界や医療業界を狙った高度に組織化されたランサムウェア攻撃
「ランサムウェア・アズ・ア・サービス（RaaS）」

ランサムウェア・アズ・ア・サービス（RaaS）の特徴:

- RaaSは、COVID-19のパンデミック以降、急拡大している
- 有料のランサムウェア等が闇市場で売買されており、これを使ってデータ暗号化等のサイバー攻撃が行われる
- RaaSオペレーターは、サイバー攻撃者にソフトウェアを提供。サイバー攻撃者は、少ないリソースで攻撃を実現できる



出所: https://www.documentcloud.org/documents/7009488-FBI-FLASH-7-28-2020-BC.html
https://healthitsecurity.com/news/fbi-alerts-to-rise-in-targeted-netwalker-ransomware-attacks
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/
https://blog.trendmicro.com/outsourcing-crime-how-ransomware-as-a-service-works/

製薬・医療業界におけるランサムウェアによるインシデント

国	被害組織	発生時期	サイバー攻撃の概要
米国	ボイス・テクノロジーズ（人工呼吸器メーカー）	2020年8月	サイバー犯罪者が同社から盗んだデータの一部をブログで公開し、**身代金が支払われない場合は更に情報公開すると脅した**。
米国	アンファスター製薬	2020年7月	ランサムウェア攻撃の結果、**約2GBのデータが流出**。漏洩したデータには、監査報告書、会計書類、化学製品の研究、企業の機密契約書などが含まれている。
米国	カリフォルニア大学サンフランシスコ校（UCSF）	2020年6月	UCSF大学医学部の複数のサーバがランサムウェアに感染。大学側は、暗号化を解除するために攻撃者が要求した**身代金114万ドル（約1.2億円）を支払った**。（UCSFは他の研究者と協力して、COVID-19に関連した抗体検査や臨床試験を行っている）
米国	イリノイ州シャンペーン・アーバナ公衆衛生局	2020年3月	公衆衛生局のウェブサイトがランサムウェアに感染。しかし、半年前にメール情報、健康情報、患者の電子カルテ情報等はクラウド環境に移行していたため、**ランサムウェアの影響は受けなかった**。

出所：各種報道よりPwCが作成

エグゼクティブ向け推奨事項

1. **セキュリティ対策を強化するため、経営層を巻き込んだ組織横断的なセキュリティガバナンス強化に取り組むべき**
2. **重要データのバックアップを取得する。バックアップデータは、オフライン環境など安全な環境を利用し、データの変更や削除ができないようにする必要がある**

Pharmaceutical Segment Targeted by Ransomware

PwC Consulting LLC
September 2020

pwc

Pharmaceutical companies continue to be hit by Ransomware attacks. During the pandemic, a global trend avid ransomware attacks is observed.

Pharmaceutical Segment Targeted by Ransomware

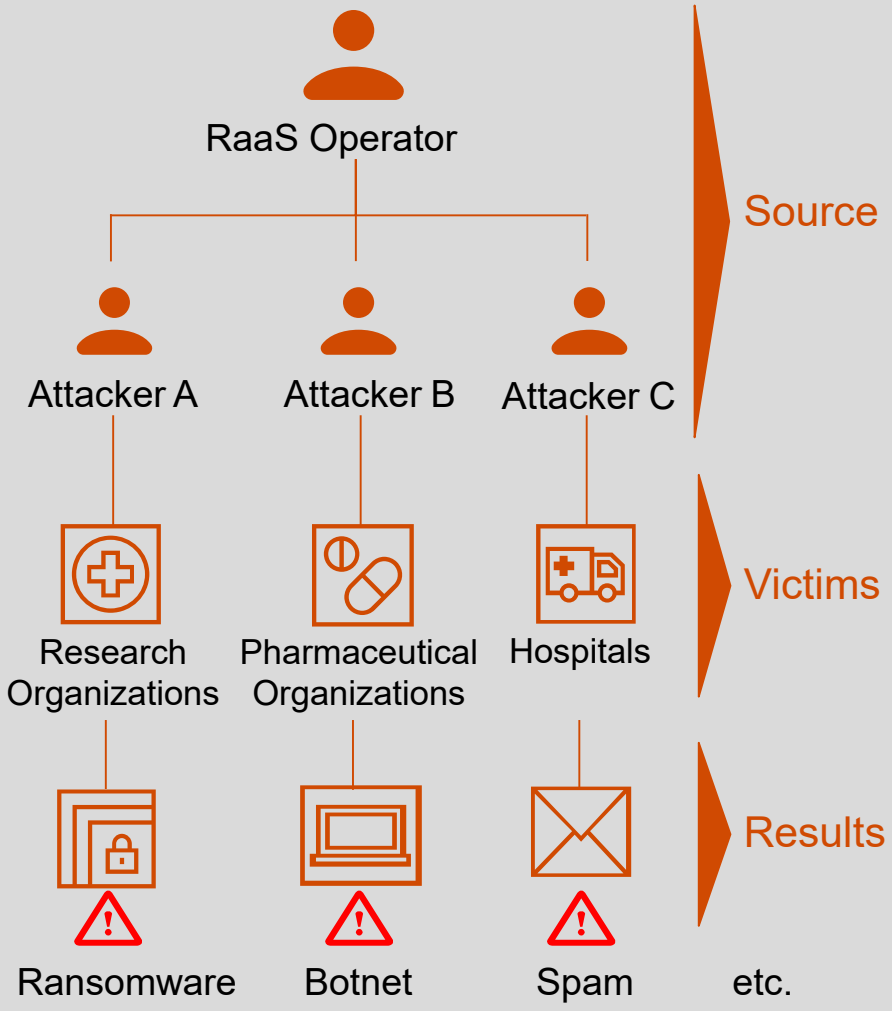
In July, the Federal Bureau of Investigation released a flash alert warning a significant increase in targeted Netwalker ransomware attacks on US and foreign health agencies among others. It is observed that NetWalker ransomware actors have targeted the healthcare sector throughout the COVID-19 crisis. Netwalker hackers were partnering with other cybercriminals to gain access to enterprise networks through Ransomware-as-a-Service (RaaS) model.

Highly organized ransomware attacks targeting the pharmaceutical and medical industries

Ransomware-as-a-Service (RaaS)

RaaS Overview:

- RaaS is an offering of pay-for-use malware created for extortion over stolen or encrypted data, known as ransomware.
- Author of the ransomware makes the software available to customers called RaaS Operators.
- The operators can use the software to hold people's data hostage with relatively little technical skill.



Source: https://www.documentcloud.org/documents/7009488-FBI-FLASH-7-28-2020-BC.html
https://healthitsecurity.com/news/fbi-alerts-to-rise-in-targeted-netwalker-ransomware-attacks
https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/
https://blog.trendmicro.com/outsourcing-crime-how-ransomware-as-a-service-works/

Ransomware incidents in the pharmaceutical industries

Country	Target	Date	Overview
US 	Boyce Technologies (Ventilator manufacturer)	Aug 2020	Cybercriminals **published samples of commercial data** they stole from the company and threatened to release more if the ransom is not paid.
US 	Amphastar Pharmaceuticals	Jul 2020	Around **2GB of data was leaked** in DoppelPaymer ransomware attack. The compromised data includes audit reports, accounting documents, chemical product research, confidential corporate agreements and more.
US 	University of California San Francisco (UCSF)	Jun 2020	NetWalker threat actors infected several servers of the university's School of Medicine with ransomware. **UCSF paid the hackers' ransom demand of $1.14M**. UCSF is working with other researchers on antibody testing and clinical trials related to COVID-19
US 	Champaign-Urbana Public Health Illinois	Mar 2020	Hackers infected the website with NetWalker ransomware. However, the provider had already moved email accounts, health records and electronic patient health information to the cloud, hence they **have not been impacted**

Source: Multiple News Article

Recommendations for Executives

1. Work to **strengthen security governance** across the organization, **involving senior management** to strengthen security measures.
2. Get a **backup of critical data**. The backup data should be in a secure environment, such as an offline environment, so that data cannot be changed or deleted.

Thank You

www.pwc.com/jp