Rubrik Zero Labs

データセキュリティの現状：

直面する多くの課題

目次

データソース

RT **RUBRIKテレメトリー**　WR **WAKEFIELD RESEARCH**　ER **イベント対応データ**

データについて

Rubrik Zero Labsは、データセキュリティのリスクを軽減するための、ベンダーに依存しない実用的な情報提供に取り組んでいます。この目的のために、Rubrikでは2022年1月1日～12月31日までの様々な情報源から見出した調査結果を使用しました。

RUBRiKテレメトリー：

Rubrikでは、Rubrikテレメトリーを使用して、組織の日常から得た実データを詳しく調査しています。ここでは、私たちが偏った先入観を持っていることについてもお伝えします。

5000社以上
顧客

3
地域

22
業界

57
国

保護されているデータの合計量：

28
エクサバイト（EB）の
論理ストレージ

659
バックエンド
ペタバイト（BEPB）

機密データが格納されている場所：

87億個以上
ファイル

38ファイル中1つ
のファイルに
機密データが含まれる

190億以上
ファイル内の
機密データレコード

データのスケールについて：

ある推定によると、歴史上すべての言語で話された言葉は5 EBで、これは2022年にRubrikが保護対象にしたデータの18%にすぎません。[1、2、3、4]

28 EB vs 659 BEPB

一般人の想像を超えている数字です
世界中の人々は大抵、「データ」と聞くと論理ストレージ（フロントエンドストレージとも呼ばれる）を思い浮かべます。一方、データビジネスに従事する私たちが扱うのは、主にバックエンドストレージです。

Rubrikは組織のデータを全体的に捉え、重複排除や圧縮などの様々な技術によって、バックエンドストレージに格納するデータ量を削減しています。そのため、このレポートの残りの部分では、主にバックエンドストレージについて説明します。

事例
このレポートでは、Rubrikテレメトリーの対象となっていた、ある組織に対する攻撃を詳しく見ていきます。プライバシー保護のため、組織の名前は変更しています。

1 https://www.space.com/18383-how-far-away-is-jupiter.html
2 https://www.sizes.com/tools/filing_cabinets.htm
3 https://www.zmescience.com/science/how-big-data-can-get/
4 https://www.backblaze.com/blog/what-is-an-exabyte/

WAKEFiELD RESEARCH :

Rubrikでは、データセキュリティの状況について、より広範な見解でRubrikテレメトリーを強化するために、Wakefield Researchに調査を委託しました。

また、ITチームやセキュリティチームのリーダーに、自分たちの見解における違いについて学習してもらうようにしました。

1600人以上
IT/セキュリティのリーダー

49%
CIO
およびCISO

3つの地域
北米、ヨーロッパ
およびアジア

16%
VP

38%
シニアディレクター
またはディレクター

10か国
米国、
英国、
フランス、ドイツ、
イタリア、オランダ、
日本、オーストラリア、
シンガポール、インド

イベント対応データ :

Rubrikでは、データセキュリティの状況についてより包括的に把握するために、信頼できる以下のサイバーセキュリティ企業に協力を依頼しました。

Mandiant :
Global median dwell times and ransomware investigation ratios（攻撃者の滞留時間の世界平均とランサムウェアの調査率）出典『M-Trends 2023』

Palo Alto Networks Unit 42 :
2022 Ransom demands（2022年のランサムウェアが要求したもの）出典『2023 Unit 42 Ransomware and Extortion Report』

Expel :
Ransomware precursor activity and growth of intrusions in public clouds（ランサムウェアの前兆活動とパブリッククラウドへの侵入増加）出典『Great Expeltations 2022』

Permiso :
Illicit credential use in cloud intrusions and credential privilege levels（クラウドへの侵入における認証情報の不正利用と認証情報の権限レベル）出典『Permiso 2022 - End of Year Observations』

データの海景

組織はデータの海、つまり混沌とした膨大なデータの上にいます。
この海は、表面的には広大で、しかも安定しているように見えます。

けれど、いったん海の深いところまで潜った人は皆、生き物であふれていることがわかります。

視界は悪いですが、洞窟の中や岩の下などほとんどの場所で、
探せば探すほど、多くのデータが見つかります。
水の流れは速く、
同じ光景は二度と見ることができません。

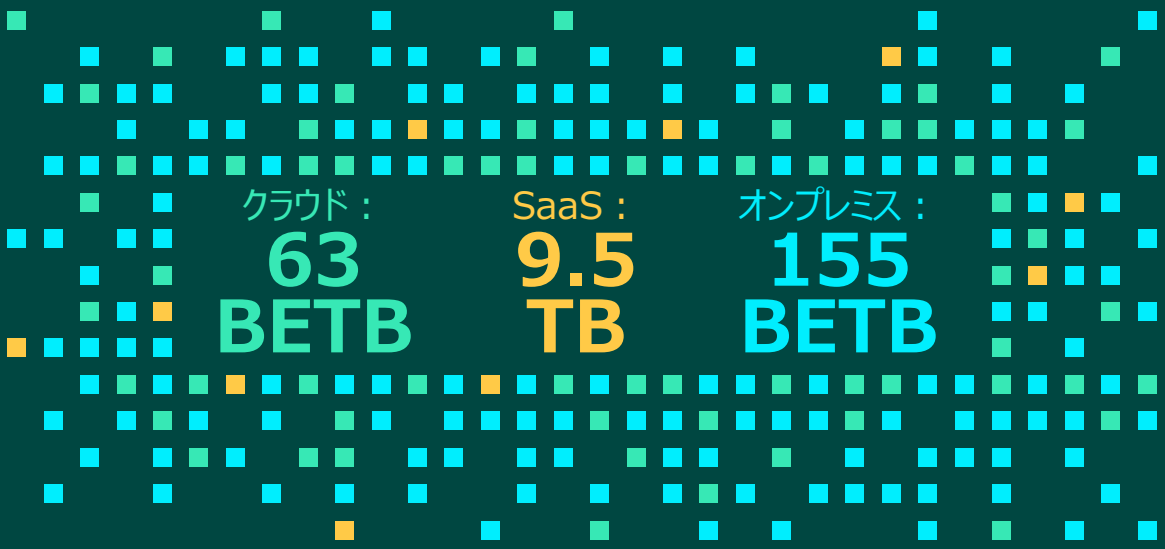
そして
ずっと考えています。

「侵略者が暗闇に潜んで攻撃するのを待っているのでは？」

データは、私たちが考えている以上に速く、多くの場所で増えています®

通常の環境で保護されているデータ：

合計：227 BETB



2022年に保護したデータの平均増加率：

合計：	クラウド：	SaaS：	オンプレミス：
25%	**61%**	**236%**	**19%**

一般的な組織のデータ量は、今後5年間に3倍になり、
増加率が一定の割合である場合、保護するために

545 BETB

が必要になります。

45%

世界全体の組織のうち、オンプレミス、クラウド、SaaSの混合環境でデータを保護している組織の割合。

36%

世界全体の組織のうち、複数のクラウドベンダーを同時に使用している組織の割合。

それぞれのデータセキュリティソリューションには、フォローオン（追加）の課題があります[WR]

データのバックアップシステムと復旧システム、およびそれに関連するプロセスは、危機的状況における最後の防衛線となります。しかし、単にバックアップソリューションを持っているだけでは十分でないことに、組織は気付いています。

99%

の外部組織は、バックアップおよび復旧ソリューションが用意されていると報告しました。

しかし、93%

の組織が、ソリューションを使用しても重大な問題が発生したと回答しています。最も一般的な問題は、スタッフの不足、帯域幅の制限、インフラストラクチャのギャップ、想定していた計画または優先順位の欠如です。

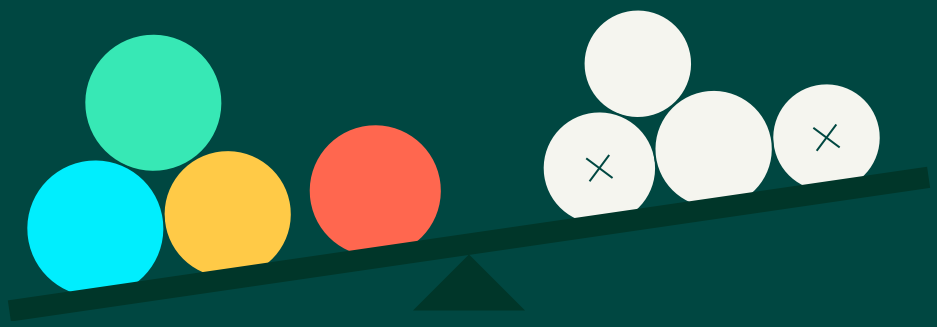
93%

悪意のある攻撃者がサイバー攻撃中にデータのバックアップに影響を与えようとした、と報告した外部組織

73%

少なくともシステムの一部が攻撃された、と報告した組織

誰もがデータセキュリティを**実施**していますが、2022年の実態はバラバラです®



56%

少なくとも1つのゼロトラストの取り組みを導入している組織。

56%

インシデント対応計画を策定または審査した組織。

54%

バックアップおよび復旧のオプションをテストした組織。

52%

データ復旧のオーケストレーションを作成または改善した組織。

事例

2024

2022年、米国を拠点とする、ある教育機関は、データセキュリティの厳しい現実を身をもって体験しました。彼らのストーリーを通じて、その体験は「ごく一般的」であるということを見ていきましょう。

この事例の出来事は実際に起こったものですが、
組織名はお客様のプライバシーを保護するために匿名化されています。

Stone Universityの環境：

2.9 PB

論理ストレージ

64 BETB

を物理的に格納

データは2か所の

異なる環境に格納

155%

2022年のデータ増加率

1～3日目：
侵入

WHAT YOU DON'T KNOW

WILL HURT YOU

攻撃者がLog4jの脆弱性を使用して
Stone Universityのセキュリティを侵害しました。
同校のヘルプデスクチケットのシステムサーバーには
脆弱性が悪用される危険性が残っています。

Log4j

最も普及しているオープンソースソフトウェアの一つである、ApacheのLog4jソフトウェアライブラリにおいて、2021年の終わりに脆弱性が見つかりました。サイバー犯罪者は、この脆弱性（現在はLog4Shellと呼ばれている）を12時間も経たずに悪用し、今日にいたるまで悪用を続けています[5]。

5 The Guardian: Recently uncovered software flaw 'most critical vulnerability of the last decade'

このサーバーにアクセスすることで、
攻撃者は境界インフラストラクチャの
セキュリティ対策を回避することに
成功しました。

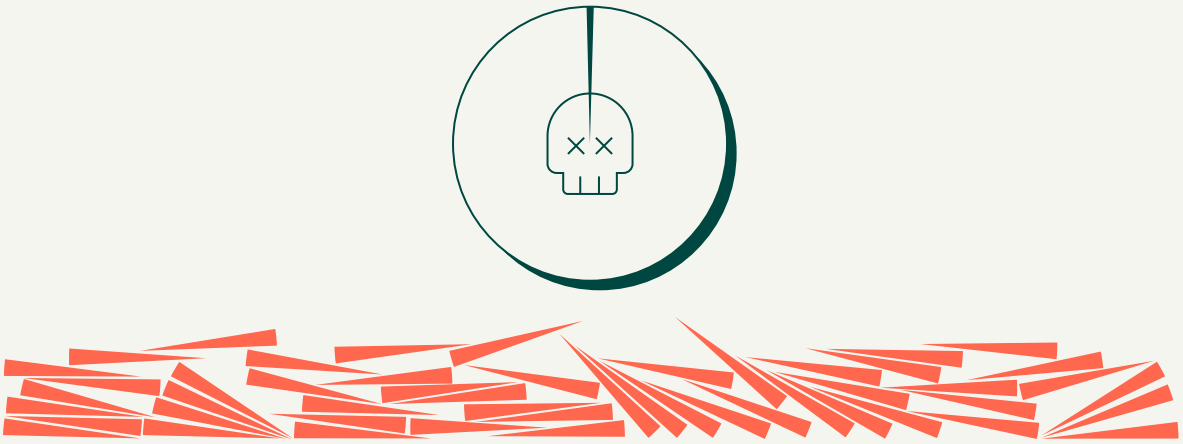
攻撃者は正規のツールを組み合わせて不正な認証情報を作成し、
アクセスを拡大し、環境全体に新たな足場を作り、
Active Directoryのセキュリティを侵害しました。

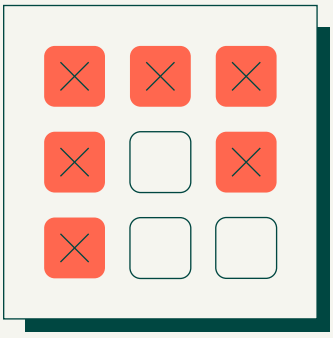
サイバー犯罪者はStone University内を水平展開し、
VMware環境内の5台の個別マシンへのアクセス権を取得し、
その過程で重要な詳細情報を収集しましたが、これらの作業は
Stone Universityに気付かれずに行われました。

Stone Universityの体験は、憂慮すべき事態でありますが、昨年多くの組織が直面したことと照らし合わせると、非常に「よくある」内容です。®

99%

2022年に少なくとも1回の攻撃を受けたと認識しているIT/セキュリティリーダーの割合。平均すると、**リーダーは2022年に52回の攻撃を受けている。**





61%

これらの攻撃のうち、最も標的とされる環境であるSaaSアプリケーションに影響した割合。

データの詳細：

悪意のある活動によって影響を受ける環境の割合（タイプ別）

61% SaaS

62% クラウド

50% オンプレミス

Expelによると、3つの主なパブリッククラウドで悪意のあるインシデントは2021年から2022年までに70%増加しました。

注意：ここで引き合いに出した3つのパブリッククラウドとは、Amazon Web Services（AWS）、Google Cloud Platform（GCP）、Microsoft Azure（Azure）です。[6]

サイバー犯罪者は、この脆弱性を悪用してStone Universityの環境にアクセスすると、すぐに不正な認証情報の使用に切り替えました。Permisoは、同社が検知および対応したクラウド侵入原因の100%が認証情報の漏洩であったと報告しています。[7]

また、これらの認証情報には90%以上の過度の権限が付与されていました。言い換えれば、認証情報では、割り当てられた権限のわずか5～10%しか使用されていませんでした。[8]

「大半の企業には、自社の認証情報がどのように使用されているか、について「見てわかるしくみ」（監視および監査）がまったくと言ってよいほどありません。また、いつセキュリティが侵害されたのかを簡単に特定することもできません。API駆動型のエコシステムが増加するのに伴い、これらの情報は驚異的な速さで漏洩および拡散しており、漏洩するキー、トークン、認証情報の数が劇的に増加しています。」

Permiso、統括責任者兼P0 Labs責任者、Ian Ahl氏

6 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
7 https://permiso.io/blog/s/permiso-2022-end-of-year-observations
8 https://permiso.io/blog/s/permiso-2022-end-of-year-observations

4日目：
ランサムウェアの準備

KNOCK KNOCK

多くの場合、企業は攻撃者から告げられるまでは攻撃を受けていることに気付きません。

Stone Universityの攻撃者は気付かれないまま、
その存在を知らしめるための準備を進めました。

彼らは同校のシステムについて複数のアクセスポイントがあることを
確認していました。その結果…

STONE UNIVERSITYは「たった1枚ドアを閉めた」だけで攻撃者の進行をブロックすることはできないでしょう。

サイバー犯罪者はまた、レガシーデータの
バックアップサーバーへアクセスして、
Stone Universityの対応を観察していました。

注目すべき点は、Stone Universityはすでにバックアップベンダーとテクノロジーを新しいものに替えていましたが、バックアップサーバーはニーズを満たしていないにもかかわらず、そのままにしておいたことです。

最終的に、
サイバー犯罪者は同校全体のデータを8GB流出させました。

The cybercriminals
REMAINED UNDECTED
throughout this process.

ランサムウェアの被害にあう割合は？ ®

40%

調査対象の外部組織の40%が、実際にランサムウェアの被害にあったと報告しています。

11%

Expelは、同社のSOCが経験した悪意のあるイベントのうち、11%がランサムウェアの活動に関連するものであったと報告しています。[9]

18%

Mandiantは、同社の業務の18%がランサムウェアイベントに関するものであると報告しています。[10]

データの詳細：

サイバー攻撃の被害にあう割合は？
2022年に外部組織が直面した攻撃のタイプ：

- 59% データ漏洩
- 54% ビジネスメールの漏洩または不正転送
- 41% 内部犯行者イベント
- 40% ランサムウェア

Stone Universityの攻撃者の行動は、Mandiantの調査による「攻撃者の滞留時間の世界平均」と一致しています。

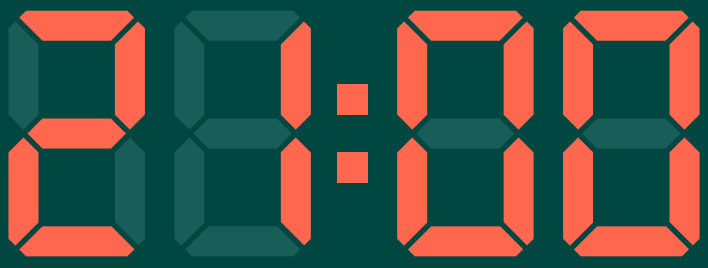
- 滞留時間の世界平均
- 16日 すべての調査
  （産業スパイ、金銭的利益、不明な結果など）
- 9日 ランサムウェアの調査のみ
  （Mandiantの調査全体の18%）
- ランサムウェアが標的を調査するための滞留時間は一般的に短い傾向にあります。これは、ランサムノート（身代金の要求文書）の送信や、環境の暗号化によるものです。[11]

9 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
10 https://www.mandiant.com/m-trends
11 https://www.mandiant.com/m-trends

5日目：
ランサムウェアの拡散

OH SH*T

Stone Universityの攻撃者は、日曜日の夜9時頃に、侵入に対する身代金の要求を開始しました。



彼らはAvosLockerを使用し、侵入時に侵害した最初の5台のVMを含めて、VMware ESXiインフラストラクチャの150台のVMすべてのファイルを暗号化しました。

さらにAvosLockerは、ファイルを暗号化する直前に仮想マシンの管理ツールを遮断し、Stone Universityが効果的に対処できないようにしました。

AvosLocker

AvosLockerは、マルウェアファミリーと脅威グループの両方を記述するために使用されます。これは、「サービスとしてのランサムウェア（RaaS）」モデルに基づいて動作します。この場合、攻撃者の仲間はサービスに登録して、ランサムウェアの拡散を実行し、身代金を回収します。AvosLockerの場合、このサブスクリプションの対象には、身代金交渉の直接対応、窃取した被害者データの公開、特定のランサムウェアツールの実際の使用が含まれます。[12]

12 https://www.cisa.gov/news-events/alerts/2022/03/22/fbi-and-fincen-release-advisory-avoslocker-ransomware

最終的に、攻撃者はランサムノートを送ってきました…

実際に
ランサムウェアが
登場するのは
攻撃の
中盤
であり、
最初や終わりでは
ありません。

多くの人は、ランサムウェア攻撃の最後は「暗号化イベント」だと
考えていますが、そのようなケースはめったにありません。
たとえば、サイバー犯罪者は数日間にわたって検知されずに
Stone Universityのシステムに自由にアクセスできました。
そして、Stone Universityでランサムウェア攻撃が
完全に解決するまで、さらに数日かかります。

データの詳細：

ランサムウェアは、データ拒否（data denial）型の脅威です。

データ拒否には、ランサムウェア、ワイパー、正当なアクセスによるデータ削除、サービス拒否（DoS）などの手段があります。また、サイバー犯罪者は暗号化イベントの前に、様々な目的でデータを日常的に流出させています。

2022年、Rubrikのランサムウェア対応チームは、数十の組織の復旧業務を支援しました。

これらの対応において最も普及しているランサムウェア攻撃者は、以下のとおりでした。

- LOCKBIT2.0
- BLACKCAT/ALPHV
- AVOSLOCKER
- META
- PLAY
- HIVE
- SPARTA
- BLACK BASTA
- SPIDER
- VICE Society

5〜7日目：
初期対応

TAKE BACK CONTROL

攻撃者を撃退できるかどうかは、
対策がどれだけ整っているかによって決まります

Stone Universityはすぐに対処を始めましたが、すでに拡散していた暗号化により、その作業は制限されました。

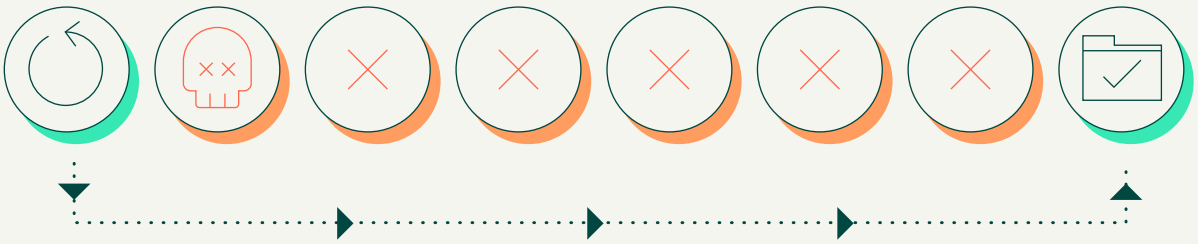
復旧のために、Stone Universityはデータをフォレンジック環境とテスト環境に復元し、調査、および次のアクションの優先付けを行いました。

また、オフラインデータバックアップの分析、侵害が疑われるサーバーの特定を行い、特定されたサーバーをさらに分析するためにフォレンジック環境へライブマウントしました。

その際に、攻撃者の侵害計画と、侵害されたアカウントと時間が記載されているメモを発見しました。さらにフォレンジックを実施することで、後から侵害された7台のサーバー、および最初の侵害ポイントが明らかになりました。

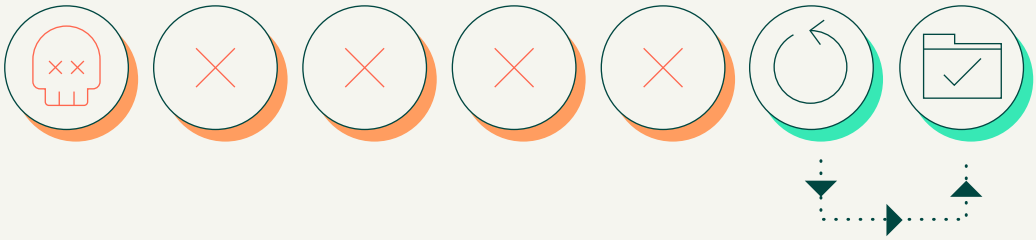
希望をもったStone Universityは、次の2つの段階によって、急いで環境を構築し始めました。

まず、最初の侵入で侵害されたサーバーを対象としました。



Stone Universityのチームは、攻撃者が到達した前日から5台のVM内にあり、侵害された8台のサーバーを復元しました。しかし、結果的に合計6日間分のデータを失いました。

次に、最初に侵害されていないけれども、ランサムウェアによって暗号化されたサーバーを対象としました。



このため、残りの145台のVMは暗号化処理が行われただけで、それほど集中的な対応は必要ありませんでした。ランサムウェアが攻撃した1日前に取得したバックアップから復元したため、145台のVMについて、さらに5日間のデータを損失することは回避できました。

全体的な復旧作業には、新しいESXiホスト、新しいvCenter、Active Directoryの再構築が必要でした。

あらゆる可能性の中で、これはStone Universityが望む最高の結果でした。攻撃者の進捗を楽観していたStone Universityは、身代金を支払わないことに決めました。

暗号化イベントでは、最初の大きな問題を見過ごしてしまいがちです。

暗号化されたものは、どのように診断・分析しますか？
身代金の支払いは有効に機能しますか？ この最初の暗号化の瞬間に備えて、
クリーンなデータのコピーを準備することで、攻撃からの回復で成功するチャンスが生まれます。
Stone Universityは暗号化に備えて対策していましたが、このためにどのような対策をしておけばよいでしょうか？

身代金の支払いは有効に機能しますか？®

46%

身代金を支払った外部組織は、攻撃者から提供された復号化ソリューションを使用しても一部のデータしか取り戻せません。46%の組織は、攻撃者を介して半分以下のデータしか復元できませんでした。

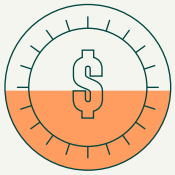
16%

攻撃者の復号化ツールを使用してすべてのデータを復元できた外部組織は、わずか16%でした。

Rubrikテレメトリーで、ランサムウェアの前兆と暗号化の割合を明らかにしました。®

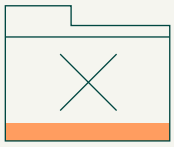
75%

世界全体の組織で、ある程度の異常な活動を観察している割合



48%

世界全体の組織で、自社に対する何らかのランサムウェア試行を観察した割合



15%

世界全体の組織で、自社の環境において、データの復元が必要な暗号化の被害にあった割合

保護されている全データのうち、暗号化イベントが発生したのは**0.004%**未満®

用語説明：

異常な挙動の検知
「異常な挙動の検知」は、ランサムウェアを特定するための2段階プロセスにおける最初のフェーズです。このプロセスにおいてRubrikは、異常な数のファイルが追加・削除・複製されているなど、ファイルシステムのメタデータについての異常な挙動を分析します。大半の異常な活動はランサムウェアではありませんが、その後の調査が必要です。

不審なファイルの検知
ランサムウェアを特定する2段階プロセスの2番目のフェーズは、不審なファイルの検知です。このフェーズでは、AIと機械学習の組み合わせを使用して、異常な挙動の検知フェーズで特定されたファイルについて、データエントロピー、ファイル拡張子、圧縮、既知の悪意のあるランサムウェアアクション、その他ランサムウェアを示す様々な要因を評価します。

スナップショットの分析
スナップショットはオフラインデータバックアップのコピーであり、通常は自動化された反復パターン、またはアドホックのタスクで発生します。完成したスナップショットに対して分析を実行できます。

- Rubrikのすべてのお客様を対象として、ランサムウェアの活動に関して27,266,649個のスナップショットを分析しました。
- 20,692個のスナップショット（全体の0.07%）に異常な活動が含まれていました。
- 1,198個の異常なスナップショット（異常な活動のうちの6%）が、スナップショットの完成を妨げる暗号化イベントの続発につながりました。
- 評価したスナップショットのうち、暗号化の問題があったのは0.004%だけでした。
- 暗号化イベントはすべて、事前に異常のある活動として特定されています。
- 暗号化イベントの100%が多要素認証の欠如と結び付いていました。

2022年のRubrikの顧客全体®

セキュリティが保護されていた全データのうち、さらなる分析が必要であったもの、またはランサムウェア活動の兆候を示したものは0.004%未満でした。

この図は、組織が脅威領域をどのように制御できるかを示しています。

脅威の広範な攻撃対象からあなたの組織を外すことは実質的に不可能ですが、この攻撃領域からリスク領域の大部分を排除できる可能性は高いです。

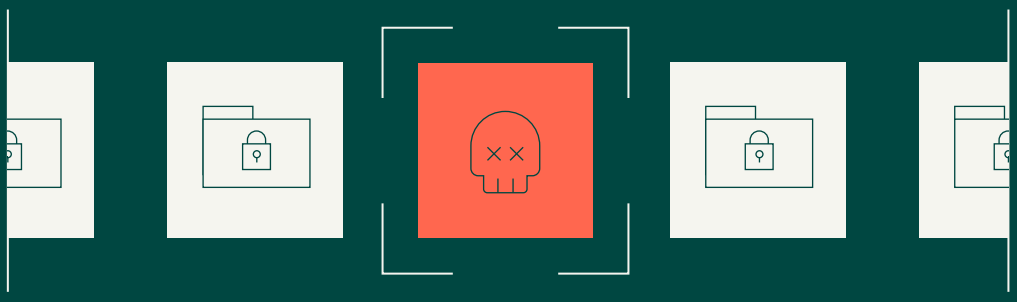
8日目：
2回目の身代金要求

WAIT... WHAT?

暗号化が攻撃者の唯一（またはお気に入り）の
武器ではありません

3日後

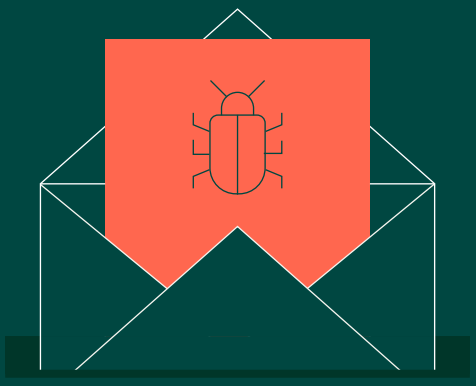
初回の身代金要求の後、攻撃者は2回目の要求を送ってきました。
今回は、4日以内に身代金を払わないと、窃取した8 GBのデータを
AvosLockerが管理する漏洩サイトに流出させると脅迫しました。



また、Stone Universityの環境の新たな部分を侵害して対応措置を妨害しようとしました。

希望をもって対応を始めた後、この予想外の展開によってStone Universityは振り出しに戻され、もう一つの厳しい判断が迫られました。

「身代金を支払う」か、または「データがオンラインに流出するのを見ているか」という判断です。



72%

身代金の要求に対して支払ったことを報告した、Rubrik以外の組織の割合。[WR]

データの詳細：

身代金を支払ったRubrik以外の組織について、支払った身代金の具体的な内容：Ⓦ

40%

暗号化イベントに対する身代金の要求。

37%

データ漏洩の脅迫に対する身代金の要求。

Palo Alto NetworksのUnit 42インシデント対応によって確認された2022年の身代金：Ⓔ

5,000万米ドル以上

身代金要求の最高額

700万米ドル

支払った身代金の最高額[13]

13 https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report

AND BREATHE

データを「見える」かたちにしておくことで、意思決定の機会が生まれます

Stone Universityは、データ脅迫の身代金要求に対処するために、今までの対応策を、次の3つの具体的な取り組みに切り替えました。

1

最初に、後続の侵入行動を特定して防止するために、検知および対応の取組みを行います。これには、複数のサーバーやファイアウォールの交換、その他の強化対策が必要でした。

2

次に、復旧した環境の一部をテストし、それを本番環境に移行することで、継続してデータを復元しました。

NEW
3

最後にStone Universityは、攻撃者が窃取したデータがオンラインに流出した場合の影響を評価し始めました。

しかし...

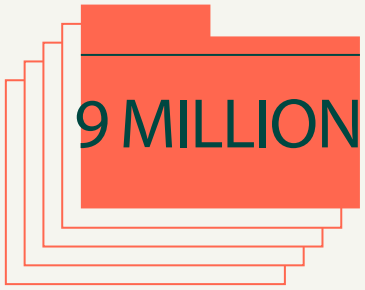
暗号化の問題が解決していなかったため、Stone Universityは、攻撃者が実際に8 GBのデータを盗んだのか、またはどのようなデータが盗まれたのかを判断することができませんでした。

よって...

代わりに、データの影響の確認作業を最新のデータバックアップに切り替えました。

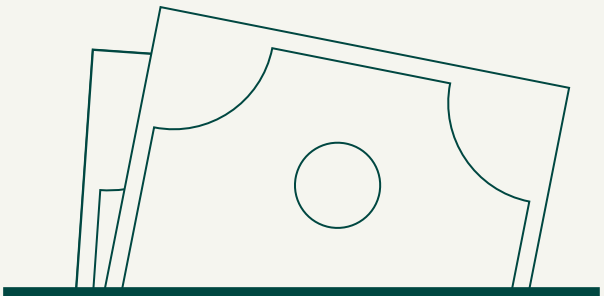
良いニュース

24時間以内に答えが見つかったため、十分な情報を得たうえで意思決定を行う猶予が3日間ありました。



悪いニュース

2013年から現在にいたるまで、攻撃者は900万件以上の機密情報が含まれている8 GBのデータを盗み出すことに成功していました。



STONE UNIVERSITYは2回目の身代金は支払わず、犯罪者に資金は渡さない選択をしました。

機密データが流出することはStone University にとって大きな痛手となりますが、同校は、「**身代金を払っても**機密データが流出しないとは限らない」という現実を理解していました。

代わりに、
3日間かけて、影響を受ける個人と組織に事前に通知しました。

データが漏洩するまでにStone University は主な対応措置をすべて終わらせ、大変だけれども必要な、以下の作業を行いました。

- ✓ 規制機関やコンプライアンス機関に通知を行う
- ✓ 影響を受ける人に連絡する
- ✓ 長期的な改善と、その他必要なデータ漏洩対策に切り替える

二次的な影響

侵入が終わると、Stone Universityのほとんどの機能が正常に戻りました。ただし、ランサムウェアの発生から2週間は、解決するのに数週間～数か月の労力と決断を要する、二次的な影響がありました。

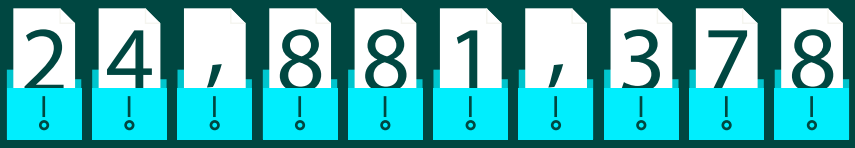
短期間にデータの移行や分散を行うことは、組織にとって真のリスクとなります。[RT]

一般的な組織は、機密データが含まれているファイルを

個保持している

さらに、

その機密データレコードの合計は



件になる

ファイルと機密データレコード：ファイルにはデータのレコードが含まれています。これらのレコードには、機密性が高いものが含まれている場合があります。たとえば、あるスプレッドシートに数百個の機密データレコードが含まれていることがありますが、他のファイルには機密データが含まれていないこともあります。

一般的な組織は、いずれか（またはすべて）の罰金の最高限度額に達するくらいの機密データを保有しています

データの詳細：

グローバルな組織は膨大な量のデータを所有しているだけでなく、それらのデータの中には、突然使用できなくなったり、セキュリティが侵害されたりすると、多大な被害を及ぼすものもあります。

その一例は機密データです。機密データは、PII、HIPAA、GDPR、CPAAなどの様々な業界標準または規制から派生したデータです。[14、15、16、17]

消費者にも組織にもデータの影響を評価するうえで多くの課題がありますが、機密データに対して金銭的な罰則を設けることは一つの選択肢になります。[18、19、20]

いくつかの例を見てみましょう。

GDPR
機密データ漏洩に対するペナルティ：重大な違反あたり最大2,000万ユーロまたはグローバル企業の収益の4%のどちらか多い金額。

一般的な場合は、1レコードあたり2ユーロ未満の罰金で2,000万ユーロになります。

HIPAA
機密データ漏洩に対するペナルティ：違反あたり50～50,000米ドル（最大ペナルティは150万米ドル）。

典型的なファイルの平均数のみを使用すると、最低の50米ドルのペナルティでも合計金額は2,800万米ドルに達し、優に最大の150万米ドルを超えることになります。

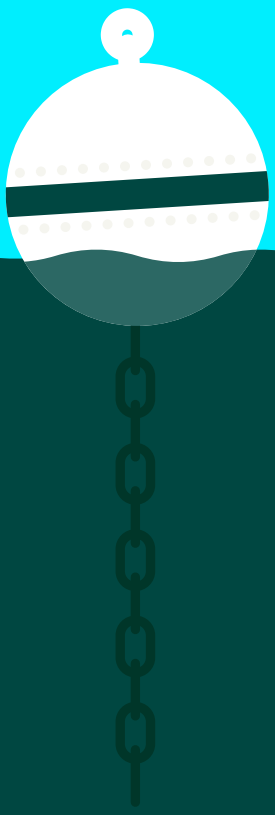
CPRA
機密データ漏洩に対するペナルティ：違反あたり最大2,500米ドル、または意図的な違反ごとに最大7,500米ドル。ペナルティの上限はありません。

一般的な組織のファイル数だけで、罰金は11億米ドルになります。

14 https://gdpr-info.eu/art-4-gdpr/
15 https://www.cdc.gov/phlp/publications/topic/hipaa.html
16 https://www.dol.gov/general/ppii
17 https://oag.ca.gov/privacy/ccpa#:~:text=The%20right%20to%20limit%20the,personal%20information%20collected%20about%20them.
18 https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(5)%20GDPR%2C%20the,fiscal%20year%2C%20whichever%20is%20higher.
19 https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/united-states/topics/penalties-for-non-compliance
20 https://cppa.ca.gov/

IMPACT

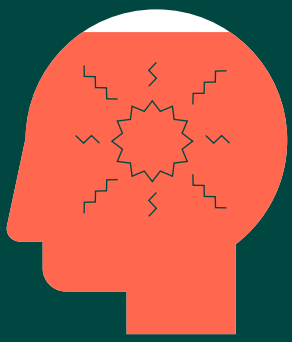
すべての侵入は当然の結末を迎えますが、私たちの関心をこの出来事で終わらせてはいけません。代わりに、海底に深く潜っていた私たちが海面に戻ってきた、と想像してみましょう。



このディープダイブから何を学ぶべきでしょうか？
何を変えればよいのでしょうか？

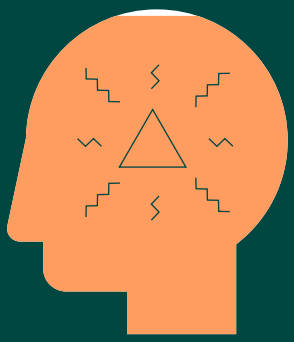
侵入は企業にも人にも影響を与えます®

このような侵入による影響は、フォレンジックやITの措置が終わった後も、
企業や人に影響を及ぼします。これらの影響は長引き、
事業展開に疑問を抱かせるものになります。



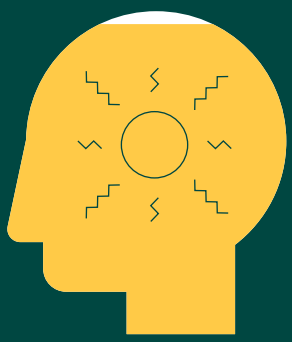
93%

2022年にサイバー攻撃を受け、マイナスの影響を受けた外部組織。



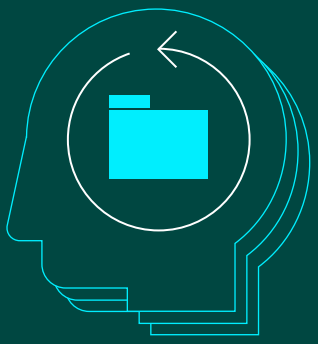
98%

サイバー攻撃により感情的または心理的に重大な影響を受けたと報告したIT/セキュリティチームのリーダー。



96%

自社がサイバー攻撃を受けた場合、事業の継続性に不安を抱いているIT/セキュリティチームのリーダー。



39%

これらのリーダーの1/3以上は、「サイバー攻撃を受けた場合に重要なデータやビジネスアプリケーションを回復させる組織の能力について、取締役や経営幹部はほとんど自信をもっていない」と考えています。

身代金の要求に対して支払う可能性が高い外部組織。

2022年にサイバー攻撃を受けた企業の93%は、以下のようなマイナスの影響を被っています。[WR]

49% 顧客の流出

45% 収益損失

44% 否定的な報道やイメージの悪化

42% リーダーの交代が余儀なくされた

5% 株がマイナスの影響を受けた

このような攻撃なリーダーに負担をかけており、98%のリーダーが昨年のサイバー攻撃で精神的・心理的に大きな影響を受けた、と報告しています。

53% 自分の職務に関する不安の高まり

46% 雇用の確保に対する不安

43% 同僚やチームメンバーの信頼を失う

41% 睡眠不足または睡眠の問題

「侵入前の問題」に「侵入後の問題」が追加される[WR]

侵入は、それ自体で完結しているイベントではありません。課題は侵入の前から存在しており、すでに存在していた障害と、侵入後に予測できる影響がペアになっています。

47%

ITチームやセキュリティチームのリーダーのほぼ半数（47%）が、2023年のサイバーセキュリティの予算に対する投資が十分ではないと考えています。

27%

同じリーダーの27%が、2023年にITとサイバーセキュリティの予算が減ると想定しています。

4%

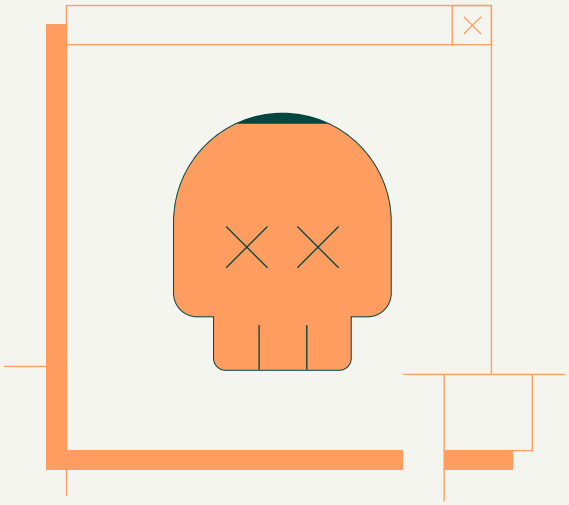
ITチームやセキュリティチームのリーダーは、チームをまとめる必要がありますが、その中で、注目すべきITとセキュリティの連携を制限する要因はないと述べているのは、わずか4%です。

サイバー攻撃から組織を防御するITチームとセキュリティチームの間で、調整不足の原因となっている上位5つの課題は以下のとおりです。®

1. **52%** 別々のツールセット
2. **51%** 可視性の違い
3. **50%** 優先順位の相反
4. **47%** 正式な計画またはプロセスの欠如
5. **45%** 統一されていない指導体制

侵入はポジティブな機会をもたらす®

暗闇の中にも希望の光はあります。あなたの組織は、避けようのない脅威を乗り越え、打ち勝つことができます。
同じ侵入でも、改善と変革のチャンスになります。



99%

2022年にサイバー攻撃を受けた組織のうち、以下の新たな措置を講じた組織の割合

48%

より良い成果を出すためにベンダーまたはサードパーティとの関係を変えた

54%

新しいテクノロジーまたはサービスに対する支出を増やした

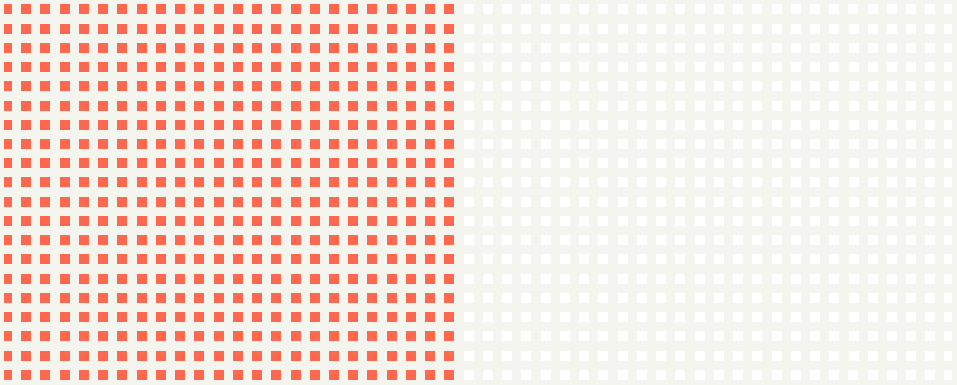
43%

スタッフを追加で雇用した

このような課題はありますが、組織は全面的に改善されています®

ただし、すべての変化がサイバー攻撃によってのみ生じたわけではありません。「系統立てて回復力を高める取組み」だけでなく、「危機的状況から得られる機会」を活用する準備が整っていれば、ポジティブな結果を生み出すことができます。

Rubrikの顧客の**48%**が何らかの形態のランサムウェア活動を受けていますが…



保護されているデータのうち、暗号化イベントが発生したのは**0.004%**未満でした。

Rubrik Zero Labsは、2022年に組織が前向きな改善を行ったことを確認しており、この傾向は2023年も続くと見込んでいます。
この改善の傾向は、すべての業界および領域で確認できます。

16%

これらの変化により、一般的な組織は2022年にセキュリティ態勢を16%強化させました。

97%

Expelは、ランサムウェアの試行の97%が展開前に停止されたと指摘しています。[21]

21 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

EXPELによるデータセキュリティの展望：ER

11% Expelが2022年に確認したインシデントのうち、ランサムウェアの拡散につながっていた可能性がある割合

97% これらのイベントのうちランサムウェアの拡散前に阻止された割合 防御者がランサムウェア攻撃者の侵入サイクル内で検知・対応できれば、悪意のある目標を阻止する大きなチャンスとなります。[22]

Rubrikは、累積的なデータセキュリティスコアを測定してお客様に提供しており、組織の改善には継続的なプラスの傾向が見られます。データセキュリティスコアは、以下のカテゴリに基づいて24時間ごとに計算されます。

1. プラットフォームセキュリティ：データが格納されているインフラストラクチャのセキュリティの効果を測定します。これには、ユーザーの管理、管理上の認証、監査ログなどがあります。
2. データの保護と復旧：バックアップデータがどれくらい適切に保護されているか、最新のバックアップのクリーンコピーが使用可能かどうか、その他関連する要因を分析します。
3. ランサムウェア調査：ランサムウェア脅威の監視のクオリティと頻度や、データを暗号化イベントの後に復元できるかどうかを確認します。
4. 機密データの検知：機密データがどの程度保護されているか、データのアクセス制御、機密データが復元に対して優先されているかを測定します。
5. スコアは以下のように評価されます。
   - 0～50：不満足
   - 51～75：改善が必要
   - 76～90：満足
   - 91以上：優良

2022年、一般的なグローバル組織のスコアは**51.2**から**59.47**へ、**16%上昇**しました。

全体的なスコアの平均：59.47

2022年の改善率：16.2%

「セキュリティは真空の中に存在するものではない、ということを忘れてはいけません。
企業がより少ない労力でより多くの成果を成し遂げようとする場合、クラウドオプションなどのスケーラブルで効率的なテクノロジーを使用することが、急務になることがあります。しかし、特にクラウドに不慣れな企業の場合、急速な導入にはリスクが伴います。絶えず変化する市場に対応するために新しいテクノロジーの導入を続ける中で、セキュリティチームはセキュリティインシデントの増加を予測しているようです。これは通常、目立たずに悪用されやすい誤った設定や、アクセスキーの流出などが原因です。」

Expel、セキュリティオペレーション部門統括責任者、Jonathan Hencinski氏

22 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

より多くのコミュニティがサイバー攻撃を受けるようになると、私たちが背負うものも多くなります。

私たちは、より優れた製品やサービスを作り、ベストプラクティスを推奨すると同時に、体得した知識を共有する義務があります。新しく学んだことはすべて、次へつながる一歩です。

一歩ずつ進んでいくことで状況は改善していきます

この目的を達成するために、Rubrik Zero Labsは、データの利用を許可していただいた4社に感謝するとともに、Wakefield Researchの取組みにも謝意を表します。また、このストーリーの作成にご協力いただいたShaped Byに感謝し、この取組みに直接関わり、貢献してくれたRubrikのメンバー、Amanda O'Callaghan、Ajay Kumar Gaddam、Sham Reddy、Kumar Subramanian、Linda Nguyen、Lynda Hall、Kelsey Shively、Kelley Cooper、およびRubrikのクリエイティブチームと開発チームもここに紹介させていただき、このレポートを締めくくりたいと思います。

Rubrik Zero Labs