2022 年 12 月 26 日
サイバーリーズン合同会社

サイバーリーズンによる最新調査で、休日や週末における企業を狙ったランサムウェア攻撃の被害が明らかに

※本資料は米国時間 2022 年 11 月 16 日に
Cybereason Inc.（米国本社）が発表したリリース文の抄訳です。

米国、マサチューセッツ州、ボストン（2022 年 11 月 16 日） -XDR 分野におけるリーディングカンパニーであるサイバーリーズンは、休日や週末にランサムウェア攻撃を受けたことのある組織を対象とした**グローバル調査の結果**を発表しました。この調査では、休日や週末に発生するランサムウェア攻撃がもたらすリスクの増大と、それに対処する企業や組織の準備態勢との間に、継続的なギャップがあることが明らかとなりました。前の年と比べて、休日や週末に発生したランサムウェア攻撃は、その評価と対応により多くの時間がかかるようになっています。

評価と対応により多くの時間がかかっている原因は、44%の企業が、休日や週末に平日比で最大 70%もセキュリティ要員を削減していることにあります。驚くべきことに、20%の企業が、平日と比較して 90%もセキュリティ要員を削減しています。逆に、休日や週末に 80%以上の人員を配置している企業は、わずか 7%に過ぎません。

『【グローバル調査結果】2022 年版 組織が抱えるサイバーリスク～休日の間もランサムウェア攻撃の手は緩まない～』と題した 1,203 人のサイバーセキュリティ担当者を対象とした調査によれば、休日や週末のランサムウェア攻撃は、平日のランサムウェア攻撃よりも大きな収益損失をもたらすことが明らかになりました。回答者の 3 分の 1 は、休日や週末におけるランサムウェア攻撃により、より大きな損失を被ったと答えており、この数字は 2021 年の調査における 13%から増加しました。教育業界と運輸業界では、より大きな収益損失を報告した回答者の割合がそれぞれ 42%および 38%にまで急増しました。

サイバーリーズンの共同創業者兼 CEO である Lior Div は次のように述べています。「ランサムウェアアクターは、休日や週末に攻撃を行う傾向にあります。なぜなら彼らは、そのような時間帯は企業の人的リソースが強固でないことを知っているからです。そのため、セキュリティチームが対応に追われている間に、検知を回避し、より多くの損害を与え、より多くのデータを窃取できるのです。サイバーリーズンでは、今回の調査の結果、リスク評価が遅れるほど、そして企業が最初の攻撃と戦うためのチームを招集するのに時間がかかるほど、修復と回復により多くの時間がかかることがわかりました」。

休日や週末のランサムウェア攻撃について、企業が懸念しているのは金銭的な損失だけではありません。実際、ランサムウェア攻撃は、企業を守るセキュリティ担当者の生活を混乱させており、回答者の 88%が「ランサムウェア攻撃が理由で休日や週末のお祝いを欠席した」と答えています。この数字は金融サービス業界でより高く、90%以上の回答者が「家族との時間を失った」と答えています。

Lior Div は次のように述べています。「サイバーセキュリティ担当者がせっかく得たダウンタイムを中断させ、彼らの私生活に干渉することは、彼らのウェルビーイングに大きな打撃を与え、燃え尽き症候群を引き起こします。さらに、サイバーセキュリティ担当者の中には、それが原因で、この分野から完全に離れる人さえ存在します。サイバー犯罪者たちは、休日や週末に攻撃を行うことで全体的な成功を収めているため、彼らは自らの犯罪帝国をさらに強化する方法の 1 つとして、休日や週末に企業を狙った攻撃をよりアグレッシブに実施しているのです」。

ランサムウェアは防御可能であり、多くの企業がこの惨劇を阻止するための Endpoint Detection and Response（EDR）テクノロジーを提供しています。従業員のセキュリティ意識向上プログラムを実施し、OS やその他のソフトウェアを定期的に更新し、パッチを適用することは、正しい方向への第1歩となります。さらに、ネットワークへの侵入や他のデバイスへのランサムウェアの拡散を阻止するために、明確な隔離方法を確立する必要があります。また、可能であれば、重要なアカウントをロックダウンすることも検討する必要があります。なぜなら、攻撃者は多くの場合、管理者ドメインレベルまで権限を昇格させた後、ランサムウェアを導入するからです。

このレポートの全文は下記のリンクから入手できます。
【グローバル調査結果】
2022 年版 組織が抱えるサイバーリスク～休日の間もランサムウェア攻撃の手は緩まない～
https://www.cybereason.co.jp/product-documents/survey-report/9637/

＜調査方法について＞

本調査は、2022 年 9 月から 10 月に Censuswide 社が実施したものであり、米国、英国、フランス、ドイツ、イタリア、南アフリカ、アラブ首長国連邦、シンガポールの各国におけるサイバーセキュリティ担当者が回答者として参加しました。また本調査で対象となった主な業種としては、テクノロジー、製造、金融サービス、小売、ヘルスケア、自動車、法務、政府機関などです。

＜Cybereason について＞

「Cybereason」は、サイバー攻撃から企業や団体のシステムを安全かつ確実に保護するサイバー攻撃対策プラットフォームで、企業・団体内の膨大なデータをあらゆる角度から深く分析する機械

学習エンジンとグラフ処理システムを構築し、提供します。次世代アンチウイルス（NGAV）や、ランサムウェア対策、悪意のある PowerShell への対策、EDR 機能などを搭載するフルスタックの振る舞い検知型ソリューションである「Cybereason」は、これまでにない脅威を可視化し、複雑化する高度なサイバー攻撃を阻止する力をお客さまへ提供します。