VECTRA
SECURITY THAT THINKS®

インダストリーレポート

2020年 Office 365 スポットライトレポート

エグゼクティブサマリー

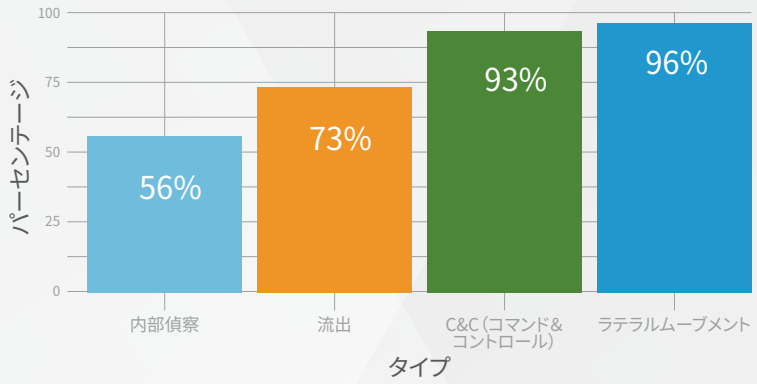
Microsoftの2020年第3四半期の収支報告によれば、同社は2億5,800万以上のOffice 365ユーザーや、7,500万以上のTeamsユーザーを擁する、世界で最も多く採用されているSaaSアプリケーションプロバイダーであり、更なる成長を続けています。結果として、重要な業務データを格納する膨大なリポジトリを保有することになった、これらのアプリケーションは、サイバー攻撃者の格好の標的となっています。

Vectra® AI社が提供する Cognito® Detect for Office 365 は、隠れたサイバー攻撃者の振る舞いを自動的に検知して対応し、インシデント調査を迅速化することで、プロアクティブな脅威ハンティングを可能にします。

Cognito Detect for Office 365 は、2020年に提供を開始後、わずか90日間で400万以上のOffice 365 アカウントに導入され、その保護を行ってきました。Vectra® AI社の2020年 Office 365スポットライトレポートでは、Cognito Detect for Office 365の導入状況の分析や調査結果に加え、サイバー犯罪者が攻撃を仕掛けるために、正当なOffice 365サービスをどのように悪用しているかという点にスポットライトを当てています。主要な調査結果は、以下の通りです。

- 悪意を持った OAuthフェデレーション認証 アプリケーションによって、多要素認証（MFA）コントロールが回避されている。
- Microsoft Power Automate ワークフローサービスが、Office 365 におけるC&C（コマンド&コントロール）やデータ流出攻撃の生成および自動化に向け悪用されている。
- サンプリングしたお客様の96%でラテラルムーブメントが、また93%でC&Cの振る舞いが見られました。

Vectra NDR Office 365 で検出された、不審な振る舞いのカテゴリ別発生頻度



サイバー犯罪者がいかに正当なOffice 365サービスを使って攻撃を仕掛けているのか、また Cognito Detect for Office 365 によって攻撃者の狙いをいかに特定し、阻止できるかの詳細は、スポットライトレポートをご確認ください。

レポート（英語版）を入手

製品、ソリューションなどに関するお問い合わせは、info-japan@vectra.ai までお願いします。

Version: **103020**