アクロニスのサイバー脅威レポート2022年上半期・日本語版を公開 ランサムウェアが最大の脅威となり 2023年までの被害予想額が300億ドル超に

スイス、シャフハウゼン 2022年10月21日
サイバープロテクションのグローバルリーダーであるアクロニスは本日、アクロニスのサイバープロテクションオペレーションセンターが取りまとめたサイバー脅威レポート中間アップデート版「Acronisサイバープロテクションオペレーションセンターレポート（上半期）」の日本語版をリリースしました。

このレポートは、各企業の専門家が注目するサイバー脅威の傾向を詳細にまとめたものです。政府機関、エンタープライズから中規模企業にとってランサムウェアが引き続き最大の脅威になっている背景、ITとインフラストラクチャの過剰な複雑さが攻撃の増加につながっている理由について詳しく取り上げています。2022年上半期に報告された侵害のうち、フィッシングキャンペーンやランサムウェアキャンペーンに用いられるログイン情報の盗難が全体の約半数を占めており、より包括的なサイバーセキュリティアプローチが求められていることが調査結果から明らかになりました。

ログイン情報をはじめとする機密情報を抜き出すために、サイバー犯罪者たちは主な感染経路としてフィッシングと悪意のあるEメールを使用しています。悪意のあるリンクやファイルが含まれるEメールは全体の約1%にあたります。それらの4分の1以上（26.5%）が（Microsoft 365でブロックされず）ユーザーの受信トレイに到達した後、アクロニスのEメールセキュリティによって削除されました。

データを抜き出し、組織に身代金を要求するためにサイバー犯罪者がマルウェアをどのように使用し、パッチが適用されていないソフトウェアの脆弱性を標的にしているかも今回の調査で明らかになりました。サイバーセキュリティの脅威の状況が複雑さを増すなか、従来の侵入経路とは異なる経路を使用した攻撃が増加しています。最近では、暗号通貨と分散型金融プラットフォームが主な標的となっています。こうしたさまざまなルートを使った侵害が成功した結果、数十億ドルの被害が生まれ、テラバイト単位のデータが失われました。

ITが過剰なまでに複雑になっていることが、こうした攻撃を可能にしています。ベンダーとプログラムの数を増やせばセキュリティが強化されると多くのテクノロジーリーダーが考えているため、多くの組織でこの問題が起きています。複雑さが増すことで攻撃対象範囲が拡大し、攻撃者に付け入られる隙も増えているため、壊滅的な被害を引き起こしかねない脆弱性を組織は常に抱えています。

アクロニスのサイバープロテクション研究所担当バイスプレジデントであるキャンディッド・ヴュースト（Candid
W est）は次のように述べています。「今日のサイバー脅威は常に進化しており、従来のセキュリティ対策をかいくぐっています。マルウェア対策からEメールセキュリティ、脆弱性評価機能まで、あらゆるものを統合した包括的なサイバーセキュリティアプローチをあらゆる規模の組織が求めています。サイバー犯罪は高度に洗練されてきており、単層型のアプローチとポイントソリューションでは攻撃に対抗できません」

重要なデータポイントが示す複雑な脅威の状況
クラウドを利用する企業が増えたことで、クラウドベースネットワークに侵入するさまざまな手段を攻撃者たちは手に入れました。Linuxオペレーティングシステムとマネージドサービスプロバイダー（MSP）、MSPのSMB顧客のネットワークを標的にするサイバー犯罪者が増えています。脅威の状況は変化しており、企業はそれに遅れをとらないようにする必要があります。

ランサムウェアは予想をはるかに超えるペースで悪質さが増しています。
　ContiやLapsus$などのランサムウェア集団は深刻な被害をもたらしています。
　Contiはコスタリカ政府に身代金として1,000万ドルを要求し、盗み出した672
GBのデータの多くを公開しました。
　Lapsus$は1
TBのデータを盗み出し、70,000人を超えるNVIDIAユーザーのログイン情報を漏えいさせました。さらに、T-Mobileからは30 GB相当のソースコードを盗み出しました。

懸念を募らせた米国国務省は、Contiの主犯と共犯に関する情報に対して最大1,500万ドルの懸賞金をかけています。

フィッシング、悪意のあるEメールやWebサイト、マルウェアは増え続けています。

2022年の上半期には、悪意のあるEメールを使ったキャンペーンが600件もインターネット上で展開されました。
　悪意のあるEメールの58%がフィッシング攻撃でした。
　28%がマルウェアを含むEメールでした。

ビジネスの世界では分散が進んでおり、2022年第2四半期には、平均で8.3%のエンドポイントが悪意のあるURLへのアクセスを試みていました。

暗号通貨と分散型金融（DeFi）プラットフォームを標的としたサイバー犯罪が増え続けています。スマートコントラクトの欠陥を悪用したり、マルウェアやフィッシング攻撃によって秘密の合言葉やパスワードを盗み出したりすることで、ハッカーたちは暗号通貨ウォレットや暗号通貨取引所に侵入して情報を引き出しています。
　2012年以降、600億ドルを超える分散型金融通貨がサイバー攻撃によって失われています。
　そのうち、440億ドルは過去12か月間で消失しました。

Kaseyaに対する攻撃のように、公開されたサービスのパッチ未適用の脆弱性も感染経路としてよく使われています。こうした現状を踏まえ、MicrosoftやGoogle、Adobeといった企業ではソフトウェアのパッチに力を入れ、公にされている脆弱性に関する透明性を高めています。こうしたパッチのおかげで、毎月79件の新たなエクスプロイトが食い止められていると見られています。パッチが適用されていない脆弱性はいずれも利用されやすいことからも、過剰な複雑さは企業にとって助けになるよりもむしろ害になっていることがよくわかります。

侵害がもたらす金銭的被害とSLAに関連する被害
多くのサイバー犯罪者は身代金を要求するか、標的から直接金銭を盗み出します。しかし、各社が被害を受けているのは自社の利益だけではありません。多くの攻撃でダウンタイムなどのサービスレベルの侵害が発生しており、企業の評判やカスタマーエクスペリエンスに影響を及ぼしています。

2021年だけで、ビジネスメール侵害（BEC）により合計24億ドルの損失が発生したとFBIでは見ています。
　2021年に発生したダウンタイムのうち、3分の１以上（36%）がサイバー攻撃に起因しています。

現在のサイバーセキュリティ脅威の状況を踏まえると、マルウェア対策、EDR、DLP（データ損失防止）、Eメールセキュリティ、脆弱性診断、パッチ管理、RMM（リモート監視および管理）およびバックアップ機能をすべて1つに統合した多層型ソリューションが必要になってきます。こうしたさまざまなコンポーネントを統合することで、サイバー攻撃の回避、攻撃が成功した場合の被害の軽減、攻撃の過程で改変された、または盗まれた可能性があるデータの保持を実現できる可能性が高まります。

「Acronisサイバープロテクションオペレーションセンターレポート（上半期）」日本語版の全文はこちらからダウンロードいただけます。
https://www.acronis.com/ja-jp/lp/cyberthreats-report-2022-mid-year/#registration

アクロニスについて:
アクロニスはデータ保護とサイバーセキュリティを１つのソリューションに統合し、現代のデジタル社会の安全、アクセス性、プライバシー、真正性、セキュリティ（SAPAS）問題の解として統合と自動化されたサイバープロテクションを提供します。アクロニスは、サービスプロバイダーやITプロフェッショナルすべてのシステム、データ、アプリケーション保護のニーズに、革新的な次世代のアンチウイルス、バックアップ、ディザスタリカバリ、人工知能（AI）によるエンドポイント保護管理とサイバープロテクションを柔軟な導入オプションで提供します。アクロニスは、最新のマシンインテリジェンスによる高度なマルウェア対策とブロックチェーンベースのデータ認証テクノロジーで、クラウド、ハイブリッドからオンプレミスまですべての環境を予算に応じて保護します。
2003年シンガポールで設立、2008年にスイスで法人登録のアクロニスは、世界中19か国、34拠点で従業員2,000人を超える規模の企業に成長しました。Acronis Cyber Protectブランドのソリューションは、150か国以上の国に26言語で提供され、2万社を超えるサービスプロバイダーで利用されており75万社を超える企業を保護しています。

Generated by ぷれりりプレスリリース
https://www.prerele.com