サイバー攻撃　最近の動向と対策

**ますます手口が巧妙化するサイバー犯罪が企業にとって大きな脅威に。
防ぐには、全従業員の意識向上・社風の醸成がカギになる。**


クロール・インターナショナル・インク
マネージング・ディレクター
日本支社代表　片山浩樹


同　シニア・ヴァイス・プレジデント
日本支社サイバーセキュリティー責任者
アレックス・シム


同　シニア・ヴァイス・プレジデント
Cyber Threat Intelligence（CTI）チーム
ローリー・ラコノ

サイバー攻撃は、件数が劇的に増加しているだけでなく、その手口もより巧妙化しており、規模や業界を問わず、世界中の企業にとって大きな脅威となっている。

当社の調査「State of Incident Response 2021」によると、回答者の93％が過去12カ月間にデータ漏洩につながるサイバーインシデントの被害に遭っていた。また、回答者の半数近く（49％）がサイバーの脅威を検知・対応するためのスタッフ、リソース、体制が不十分である、と指摘している。

昨今では、ランサムウェア[*注1]などのサイバー攻撃に加え、サプライチェーンを標的とした攻撃や、内部者が犯行へ加担する事例が増加している。

本稿では、フィッシング詐欺を起点とするサイバー攻撃の最近動向について紹介したい。

サプライチェーンが標的に

サプライチェーン攻撃は、サイバー犯罪者が1度の侵害で複数の組織へのアクセスを可能にする新たな手法として注目を集めている。サプライチェーン上の安全性の低いポイントを狙っており、多くの場合、第三者やサービスプロバイダの脆弱性を利用して、1度の攻撃で複数の顧客にマルウェア[*注2]を伝播させる。

2020年末、著名なネットワーク管理ソフトウェア会社に対するサプライチェーン攻撃により、端末1万8000台以上に被害が広がったことが話題になった。

この攻撃は数カ月前、攻撃者がソフトウェア会社のネットワークに侵入し、ソフトウェアシステムに悪意のあるコードをインストールした時点から始まっている。その後、ソフトウェア会社は認識のないまま、悪意のあるコードを含むソフトウェアパッチ[*注3]を顧客へ送信。受信先でパッチがインストールされると同時に、システムにバックドアがつくられ、これを元にスパイ行為が行われ、さらに悪質なマルウェアをインストールさせることを可能にした事案だった。

また、最近では、マネージドサービスプロバイダであるKaseyaに対するランサムウェアの攻撃によって約1500社の企業が影響を受けた。

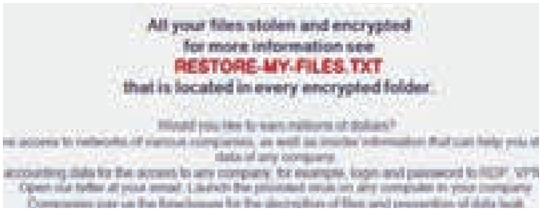
攻撃者はKaseyaの仮想システム管理者（VSA）に対するゼロデイ脆弱性（CVE-2021-30116）[*注4]を利用して大規模にシステムを暗号化。攻撃者は悪意のあるファイルを正規のWindows Defenderに読み込ませることにより、Kaseya VSAを使用している企業全体にランサムウェアを拡散させた。

内部者が犯罪を手助け

サプライチェーン攻撃では、システムにマルウェアを侵入させる外部アプリケーションに焦点が当てられることが多いが、当社ではサイバー攻撃者が企業の従業員を標的にして、ネットワーク内でのサイバー攻撃を手助けさせる事例を確認している。

2021年7月、ランサムウェアLockBit 2.0の運営者は、ランサムウェアの起動に協力した者に対して数百万ドルを支払うとの“内部協力者募集”の広告を出した。LockBit 2.0がWindows環境を暗号化すると、感染した端末にはデバイスが暗号化されていることを知らせる特別なLockBit 2.0の壁紙が表示される。この種の通知は、ランサムウェアに感染した際に見られる標準的なものである。その壁紙には、「RDP、VPN、企業メールなどへのログインIDとパスワードを探している」とあり、専用のチャットリンクを通じて運営者と連絡が取れる方法も示されている（**図**）。

図　LockBit 2.0の“内部協力者募集”広告



（出所）https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/

内部者の脅威はすでに一般的な問題となっており、サイバー攻撃全体の4分の1近くが内部者による犯行という試算もある。

最新情報を従業員と共有

サイバー防御を強化する上で重要な対策の1つとして、多要素認証（MFA）がある。MFAはユーザー名とパスワードに加え、認証アプリやテキストメッセージを介して送信されるワンタイムコードを要求することで、セキュリティを強化する。MFAはその有効性から必須のセキュリティ対策とされている。

サイバーインシデントの影響を受けている企業の大半は、ユーザーや管理者がログインするアカウント全てに対して、MFAを要求していないことが当社の調査で判明している。

また、セキュリティ部門やIT部門だけでなく、全従業員の意識向上・社風の醸成が重要な要素であることも明らかになっている。従業員は不審な電子メールが送られてくる可能性があることは知っていても、魅力ある話に誘惑されるリスクについては、承知していないことも考えられる。

内部者による脅威への技術的な対策としては、例えば、

- リムーバブルメディア（USBスティック、外付けドライブなど）の使用制限
- 営業時間外のリモートアクセスやエクスポートに対する警告・早期認知
- 従業員がアクセスできるドライブやドメインの最小限化

サイバー攻撃を完全に排除することは不可能である。しかし、サイバー脅威や攻撃手法に関する最新情報を常に把握し従業員と共有することが、こうした攻撃から企業と従業員を守る上で、大きな役割を果たすに違いない。

〈＊注〉

1　ランサムウェア：ランサムとは身代金のこと。感染した端末やファイルを使用不可にし、その解除と引き換えに身代金を要求する。

2　マルウェア：マルウェアは悪意のあるソフトウェアの総称。

3　ソフトウェアパッチ：ソフトウェアの修正プログラム。

4　ゼロデイ脆弱性：プログラムの脆弱性を修正するプログラムが提供されていない状態。

クロール・インターナショナル・インク
公式サイト