

サイバー犯罪の半数を占める「EMOTET被害」

中小企業にも強力なエンドポイントセキュリティが必須だ!!

警察庁によると、2021年のサイバー犯罪摘発件数は約1万2000件に達したという。だが、福岡県警ひとつとっても、今年上半年のサイバー犯罪に関する相談件数は前年同期比で約40%増になっており、今年は昨年の数字をはるかに上回る勢いだ。そこで、今号では本誌編集部が調査結果をもとに、昨今のサイバー犯罪の動向と対策を紹介したい。

被害の半数以上がEMOTET関連

本誌編集部が今年に入ってからサイバー攻撃による被害の公表事例を調査してみたところ、114件をリストアップすることができた。もともと、これは氷山の一角にすぎないが、内訳はEMOTET(エモテット)が一般的なセキュリティ対策では検知しにくいマルウェアの一種(関連が64件と半数を占め、ランサムウェア(身代金ウイルス)関連が16件で、学校や病院(各6件)といった公共系、厚生労働省や東京都、相模原市、仙台市といった行政系(委託業者)に対するサイバー攻撃が多かった。一方、有名企業が被害に遭うケースは割合としては少なく、セキュリティ対策に取り組んでいるはずのIT・通信系企業が被害を受けているケースも多いといったことがわかった。

く、EMOTET関連の被害だ。長年にわたってセキュリティシステムを手掛けている(株)ブロード(東京都千代田区)によると「今年3月から4月をピークにパソコンに保存されたメールの履歴やアドレスなどの悪用で被害が広がっていることがわかる」という。実際、それらを精査してみると①実在する従業員の名前やアドレスが悪用された例、②感染したPCからメールの送受信が行われた例、③組織のメールサーバーからメールが送信された例といった具合に、被害内容や深刻さに段階があることがわかったという。これらを防ぐには段階的な対応も当然として、体系的なセキュリティ対策が必要だとブロードは指摘する。

といっても、EMOTETにかぎらず、マルウェアなどの攻撃を確実に防ぐことは難しい。とくに人材不足に悩む中小企業にとつては、セキュリティツールの選定や導入、そして日常的な運用、さらには「権限管理やパスワード管理、ユーザーへの啓発活動などを実践するのも難しいはず」と前出のブロードは指摘する。

しかも、徹底した対策を講じたとしてもわずかなミスが被害につながることもある。たとえば、今年7月には(株)NTTデータ関西がサイバー攻撃に遭った。電子申請サービスのヘルプデスク業務に使用しているパソコンがEMOTETに感染した影響で、サービス利用者のメール情報(合計2312件)が流出した可能性があるという。また、3月にはソフトウェア製品を販売する(株)アシストも同様のEMOTETの被害に遭った。この案件では4段階のセキュリティ対策が講じられていたことが明らかにしているが、そのセキュリティが破られたのだ。

万全なエンドポイント対策を

こういったさまざまな攻撃が侵入する入口で、万全な対策がとれるツールとして注目されているのがHPのエンドポイントセキュリティ製品「HP Sure Click Enterprise (HP SCE)」だ。日本の総代理店として活動するブロード(前出)によると「このシステムはメールやインターネットなど外部から受領するファイルの一切をマイクロVM(仮想パソコン)で開いて閲覧、操作し、リスクがあるすべてのファイルをあらかじめ安全に隔離できるため、組織内に専門的な知識やスキルがなくても、外部からの脅威を確実にブロックできる」という。

ちなみに、HP SCEは比較的大規模な組織での複雑な要件に対応できるような仕様になっているが、顧客のニーズに合った技術を採用した「HP Wolf Pro Security (HP WPS)」も使い勝手がいかにもいい。メールやOfficeソフトの利用、ブラウザでのインターネット閲覧など一般的な範囲でパソコンを利用するのであれば、このシンプルなHP WPSで対応でき、格段にエンドポイントセキュリティのレベルが上がるはずだ、とブロードは太鼓判を押す。



もう無駄な時間と費用は「0」にしましょう

HP Sure Click Enterprise

おかげさまでBromiumはHP Sure Click Enterpriseに進化しました

エンドポイントのサイバー対策に関する費用や専門家は、もう必要ありません。100%* 防御し、レポートします。是非ブロードにお問い合わせください。

*2013年以降、Bromiumは推計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。(Bromium社調べ)

詳細は【BROAD Security Square】で… <https://bs-square.jp/columbus>

株式会社ブロード 〒100-0014 東京都千代田区永田町1-11-30 サウスビル永田町7F
TEL: 03-6205-7463 (代表)