サイバーセキュリティ最前線

ランサムウェア被害が拡大!! 見えにくい被害の実態と最新の対策

編集部で企業や団体が被害を開示した事例を集計したところ、2024年上期のランサムウェア被害件数は24件だったが、下期は49件と倍以上になっていた。警察庁の発表では24年上半期のランサムウェア被害報告件数は114件に達しており、下期はまだ公表されていないが、編集部の調査結果を考慮すると増加しているのは間違いない。そこで、今号ではランサムウェアの現況と最新の対策を紹介したい。

検知・隔離型の対策が無効化!?

ランサムウェアの被害に遭うと、復旧までに相応の時間を要することになる。事実、警察庁のアンケート調査によると、即時から1週間で復旧（19件／29ガジェット）、1週間～1カ月未満（15件／23ガジェット）、1カ月～2カ月未満（6件／9ガジェット）、2カ月以上（4件／6ガジェット）、回答時点も復旧中（21件／32ガジェット）と、25件、38ガジェットの企業・団体が2カ月以上すぎても復旧できていない。また、ランサムウェアの被害によって発生したコストは復旧費だけでなく、業務の停止や補償といった費用も発生し、信用も失う。

ところが、なぜかランサムウェアの被害は拡大する一方だ。その背景にセキュリティ意識の低さがあることは間違いない。世界規模で実施された「ナショナル・プライバシー・テスト2024」によると、日本のセキュリティ意識は調査対象国のなかで最下位だった。そして、具体的な課題としてはパスワード管理の甘さ、フィッシング詐欺への警戒心の低さ、VPNや多要素認証（MFA）の利用率の低さなどがあげられている。

こうした状況にあって、被害に遭った企業の74ガジェットがウイルス対策ソフトを導入していたにもかかわらず攻撃を受けたという。また、そのうち感染を検出できていたのは回答企業の約3割にとどまり、多くのケースでは被害が明るみになった後の調査で感染が判明。これは従来の検知・隔離型のセキュリティ対策では、サイバー攻撃を防げないことを示している。

さらに2023年頃からはデータを暗号化することなく、詐取したデータをもとに恐喝する「ノーランサム」という手口が日本でも見られるようになっており、その被害が続発している。

侵入経路の特定がより難しくなっている

こうした動向について、セキュリティ専門会社の㈱ブロードは「新種や亜種のマルウェアがつぎつぎと登場し、加えてOSやOfficeなどのアプリに標準搭載された正規の機能を悪用する攻撃が増加しているため、従来の検知型の手法では判別がしにくくなっている」と警鐘を鳴らす。また「近年のランサムウェア攻撃では攻撃者が侵入した後に証拠となる記録を消去したり改ざんするため、どこから攻撃を受けたのかも特定することが難しくなっている」とも。

そこで、ブロードでは即効性のある対策としてふたつの方法を提案している。ひとつ目は「HP SCE（Sure Click Enterprise）」を導入し、被害の起点となりがちなパソコンのセキュリティを強化することだ。このソリューションは検知・隔離型と異なり、外部から受信したファイルを隔離環境で取り扱えるようにするというもの。おかげで、ユーザーはマルウェアの影響を完全に遮断しながら通常通りOfficeやPDFを使用できるという。

ふたつ目は「RidgeBot」を導入し、ネットワーク内部での侵害経路を特定して脆弱性を効率的に管理することだ、と。このソリューションはAIを活用して、現実に侵害が可能なネットワーク上の脆弱性を自動検知し、対応の優先度を提示するというスグレモノ。従来は高度なスキルが要求されてきた専門家によるペネトレーションテスト（侵入経路の特定）をカンタンに実現できるようになるので、中小企業にこそ活用してほしい。

これらの対策を講じれば、ランサムウェア攻撃のリスクを大幅に低減し、より安全なIT環境を構築することが可能になると思われる。