IT時事ネタキーワード「これが気になる！」（第80回）

ランサムウエア最近の潮流。手口の変化

2021.08.04

セキュリティに関するニュースを定期的に見ていると、不正アクセスで顧客情報が流出したとか、ランサムウエア攻撃で身代金を要求されたとか、業務が何日間停止したとか、流出したデータがリークサイトに公開されたとか、企業関連のニュースが絶えない。

仕事や生活にITが欠かせない今の我々にはぞっとする話だ。Webページやサービスが使えない、物流やインフラが止まるほか、個人情報の漏えい、アカウント乗っ取り、クレジットカードの不正使用で大きな被害を受けることも。

そうした中で最近よく聞くのがランサムウエアだ。おさらいすると、端末内およびネットワーク接続された共有フォルダなどに保管されたファイルを暗号化、または画面ロックなどで操作不能にするウイルスの総称。データの復旧と引き換えに身代金を要求する脅迫メッセージを表示することから、「ransom」（身代金）と「software」（ソフトウエア）を組み合わせてそう呼ばれる。

従来のランサムウエア攻撃は明確な標的を定めず、ウイルスに感染させるファイルを添付したメールをばらまいたり、悪意あるWebサイトへ誘導したりして、不特定多数へ広く攻撃を行い、支払いに応じる被害者から身代金を得る戦略だった。

変わってきたランサムウエアの傾向。ターゲットを定める「標的型」

時間や手段を問わず目的達成に向け、特定の組織に特化して継続的に行う攻撃を「標的型サイバー攻撃」と呼ぶ。ランサムウエア攻撃も、不特定多数への攻撃から標的型にシフトしつつある。

実は、ランサムウエア攻撃の件数は世界的には減少傾向にある。2021年1～3月のランサムウエアの検出数が、2020年9～12月と比較して27.0ポイント減少している（ESETサイバーセキュリティ脅威レポートより）。最近の攻撃は、ターゲットの企業・組織に身代金を支払わざるを得ない状況を巧妙に作り上げ、より確実にかつ高額な身代金を得ようとしている。1件1件が大型化、件数は減少という事態を招いたと思われる。

標的を定めたランサムウエア攻撃の傾向には「人手による攻撃」（human-operated ransomware attacks）と「二重の脅迫」（double extortion）という2つの特徴がある。人手による攻撃は、手間や人数をかけてより確実に状況を作り高額な金銭を要求する。効率化のため、ネットワークへの侵入を行う者、ランサムウエアを提供する者、身代金を要求する者、という具合に分業や組織化も進む。

人手によるランサムウエア攻撃でよく使われるのが「標的型メール」だ。特定企業の社員をターゲットに偽メールを送り、添付ファイルを開かせてマルウエアに感染させて侵入のきっかけを作る。言語を駆使し時流の話題を取り入れるほか、情報収集のためにアドレス帳やメールデータをあらかじめ盗み出すケースもあるという。なおコロナ下では、テレワークや社内ネットワークで使うVPN装置の脆弱性を悪用して侵入する事例も増加。こうした複雑かつ巧妙な作業は、人手なくしては行えない。

一方、二重の脅迫とはランサムウエアで暗号化されたデータ復旧のための身代金要求に加え、さらなる身代金を払わない

と窃取したデータを公開すると二重に脅迫する攻撃方法だ。2019年末ごろから確認され、最近の攻撃の定番となってきている。実際に窃取したデータが公開される事例も頻繁に発生。従来、ランサムウエア攻撃対策として、データのバックアップが推奨されてきたが、攻撃者はデータの窃取と公開という、新たな脅迫手段を取り入れたといわれる。

標的型ランサムウエアの被害事例と手口は… 続きを読む