IT時事ネタキーワード「これが気になる！」(第69回)

最近よく聞く「暴露型ウイルス」

2020.12.14

2020年11月、大手ゲームメーカーが、暴露型ウイルスの被害に遭った。暴露型ウイルスとは、“暴露型”ランサムウエアで身代金を要求するウイルスだ。同社はこの攻撃により、顧客情報など最大約35万件が流出した可能性があると発表。犯行声明から6営業日で株価が16％下落したという。

ランサムウエア(Ransomware)は、身代金ウイルスとも呼ばれ、「Ransom(身代金)」と「Software(ソフトウエア)」を組み合わせた言葉だ。感染によりコンピューターやスマートフォン内のデータが勝手に暗号化されて利用できない状態になり、復旧と引き換えに金銭を要求される。データによっては業務に大きな支障を来したり、信用の失墜や経済的損失を招いたりするのは想像に難くない。

従来のランサムウエアは、ウイルスメールをばらまくなど無差別に感染させるケースが多かったが、2018年頃から標的を定めて感染させる傾向にある。最近は、暗号化を解くための身代金要求に加え、支払わなければ盗んだ情報を公開すると二重に脅迫するのが手口だ。こうした二重脅迫ウイルスを「暴露型」と呼んでいる。ただでさえコロナ禍で大変な中、こんな目に遭ったら、組織を揺るがしかねない。

日本経済新聞社がトレンドマイクロと共同で行った調査によれば、2019年以降、闇サイトで情報を暴露される被害が急増、暴露型ウイルスの攻撃の増加がうかがえる。情報を暴露されたと見られる組織数は、累計で1000社を超える。クラウドストライク社の調査によれば、日本企業の52%がランサムウエアの攻撃を受けており、被害にあった組織の32％が身代金を支払った。平均額は117万ドル(約1億2300万円)だったという。

1000社が被害に遭う暴露型ウイルスの内容と仕組み

ウイルスの仕組みは、コンピューターにウイルスを感染させて組織のネットワークに侵入→ネットワーク構成を把握し、データの在りかを突き止める→データを盗んだり暗号化を行ったりする→脅迫文などで身代金を要求→闇サイトなどでデータを公開、といった手順だ。

第一段階のウイルス感染は、不正なメールを送り付けてマルウエアなどに感染させて端末を乗っ取る、ネットワーク内の脆弱性を利用する、組織がインターネット上に公開しているリモートデスクトップやサーバーの認証を突破して侵入する、などが考えられる。

標的型メールが感染源になりがちだが、その危険性は広く周知され警戒するのがいまや常識となっている。ところが最近はパスワード付きファイルを送る手口が横行している。暗号化ZIPファイルを送付した後に、別メールでパスワードを追送する通称「PPAP」は、業務上のやり取りで推奨される方法だ。つい警戒なく開いてしまい攻撃に利用されるリスクも大きいうえ、マルウエアフィルタで解析できないなど、セキュリティ面で多くの問題がある。平井卓也デジタル改革担当大臣は11月24日、内閣府と内閣官房でのPPAPの廃止を宣言し、各企業がこれに続き、脱PPAPの動きが盛んとなった。

なお、コロナ禍による在宅勤務の増加で、リモートデスクトップやクラウドサーバーの利用も多くなった現在、サービスのIDとパスワードを解析して権利を奪い、侵入するケースも多いと思われる。

ランサムウエアでは被害者がデータを開こうとすると身代金を要求する脅迫文が表示されるが、最近では身代金が払われる前にデータの一部を公開し、日数の経過に伴い徐々に範囲を広げ、身代金を支払わざるを得ない状況に追い込む手口も使われる。

データ保管場所を分離、防衛演習も人気。防ぎ方と被害に遭ったときの対処

第一の予防策はデータのバックアップだ。定期的なバックアップと世代管理で確実性を高めよう。バックアップはローカルや異なるネットワークでの保管が基本。ローカルなら記録媒体はバックアップ時のみ接続し、普段は切り離しておく。データが膨大なら、大規模バックアップに対応した外部サービスを利用する。なお、バックアップから復旧できるのを定期的に確認することも大切だ。

組織の場合は感染を防ぐ教育も重要となる。メールやWebサイトの十分な確認、添付ファイルやリンクを安易に開かない、不審なプログラムを実行しない、OSやソフトウエアを最新にする、ウイルス対策ソフトの導入、端末のロックなど、普段の心得を啓発しておく。まさかに備えた防衛演習も効果的だ。

管理側では、フィルタリングツールの導入、不要なサービスの無効化、サービスや共有サーバーへのアクセス権を最小限にする、リモートやサーバーのパスワードの定期的な見直し、PPAPの廃止などが挙げられる。

さらなる知識と対策は、
・NISC「サイバーセキュリティ2020」
・IPA「【注意喚起】事業継続を脅かす新たなランサムウェア攻撃について」
・IPA「ランサムウェア対策特設ページ」
・JPCERT/CC「ランサムウエア対策特設サイト」
・JC3「ランサムウェア対策について」
などを参考に。

被害に遭ったら、感染した端末をオフラインに→ランサムウエアの種類を特定→ランサムウエアを駆除→データの復旧を試みる、の手順で復旧する。ランサムウエアの被害低減をめざす国際的なプロジェクト「No More Ransom」では、Web上でランサムウエアを特定、ランサムウエア別に複合ツールを入手して対策を行える。

ただし、早く業務を再開させるためにも、業務システムを熟知したITサービスへの相談が有効だろう。自社の業務システムを熟知したITサービス事業者がいなければ、IPAの「情報セキュリティ安心相談窓口」、JPCERT/CCの「インシデント対応依頼」に相談できる。

今後どうするか、どうなっていくか、傾向と対策

身代金を払うべきかの問いに対しては、「払うべきでない」のが結論だ。払った金銭は犯罪組織の活動資金になり、さらなる犯罪を増幅させる。それに、送金してもデータが復旧する保証もない。そもそも機密データを握られているので、継続して脅迫に遭う可能性も否定できない。

データの暗号化による身代金の要求から、データの公開という二重の脅迫に“進化”したように、第一段階の攻撃が、不特定多数から特定の組織を狙った標的型に、さらにPPAPで業務上の習慣を利用するなど、内容も手口も巧妙化しつつある。

サイバー攻撃はやまない。先に紹介したサイトやニュースなどの情報をチェックして常に動向をつかみ、備えよう。予防や対策のための予算や人材、相談先の確保も重要だ。もちろん、組織員1人ひとりが十分な知識と自覚をもってIT機器やデータを扱うよう心掛け、情報交換し合うことも大切だ。