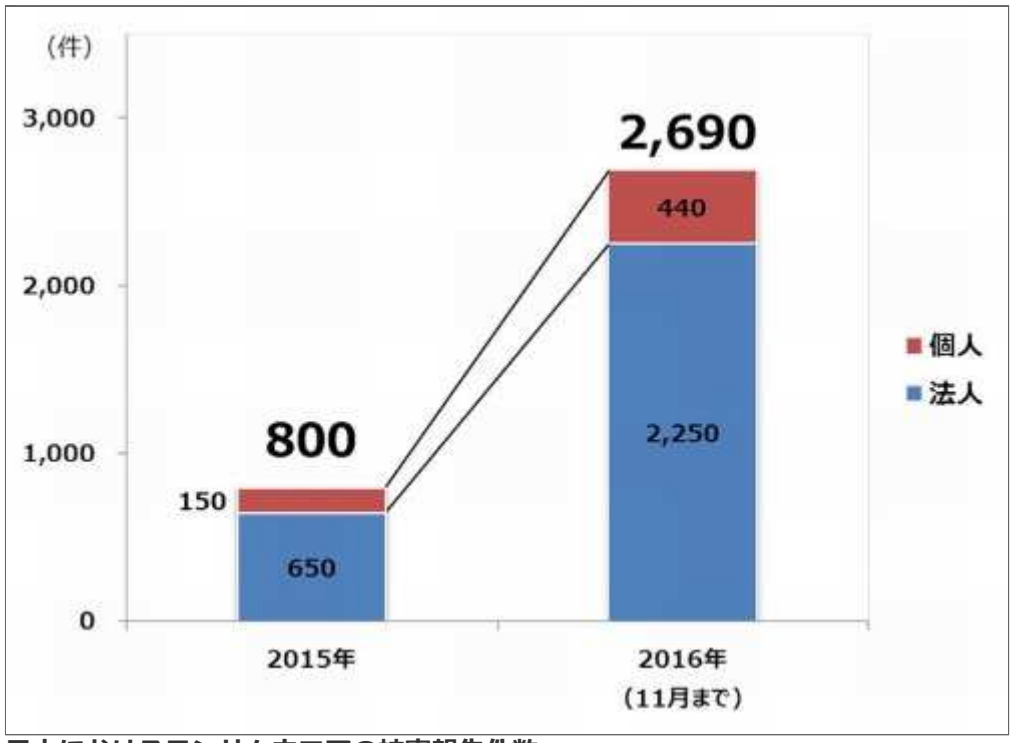
日経コンピュータ

ランサムウエアに感染したIT社長、怒ってセキュリティソフトを作る

2017/01/23

井上 英明＝日経コンピュータ

PCやサーバーなどのデータを暗号化し、復号のための金銭を要求する「ランサム（身代金）ウエア」。2016年に日本への攻撃が本格化した結果、法人被害が急増。トレンドマイクロの調査では2016年1～11月に2250件の被害が報告された。2015年の年間被害件数（650件）の約3.5倍という増加ぶりだ。



日本におけるランサムウエアの被害報告件数

（出所：トレンドマイクロ、2015年1～2016年11月、トレンドマイクロサポートセンター調べ）

[画像のクリックで拡大表示]

2017年もランサムウエアの年

ロシアのカスペルスキーの調査では2016年、ランサムウエアの攻撃が最も多い国は日本だった。既にランサムウエアは「ビジネス」化しており、ランサムウエアの配布や感染、脅迫をクラウドの「RaaS（ランサムウエア・アズ・ア・サービス）」として提供し、利用者（攻撃者）は巻き上げた身代金に応じてサービス提供者からバックマージンをもらえる仕組みすらある。言うまでもなく、未知のランサムウエアも急増している。

セキュリティ各社の2017年脅威予測を見渡しても、ランサムウエアの猛威は衰えそうにない。唯一、米インテル・セキュリティ（マカフィー）だけが「2017年の後半はランサムウエアの勢いが低下する」とした。欧州警察機構（ユーロポール）や20カ国以上の捜査機関、複数のセキュリティベンダーが参加して、復号ツールを提供する「No More Ransom」の取り組みや、取り締まりの継続、新しい対策技術の開発などが奏功してくるという見立てだ。

ただ2017年に入っても、「他の2人を紹介して感染させれば感染者自身を助けるとそそのかすランサムウエア」や「2個だけ解除させて、あとは個数に応じて身代金を要求し、再感染しないためのツールまで販売するランサムウエア」、「クラウド上のデータベースや全文検索エンジンを人質に取るランサムウエア」などが相次ぎ報じられている。

ランサムウエアはデータを暗号化する前にまず盗むように進化していると見られる。解除費用をゆすれなくともインターネット上で暴露するぞと脅したり、そのまま盗んだデータをアンダーグラウンドで売ったりできるからだ。警戒レベルを下げるのはまだずっと先になりそうだ。

うっかりで感染、3カ月間かけて自力で復旧

脅威が本格する直前の2015年11月、あるIT企業社長のPCがランサムウエアに感染した。今年で創業20年を迎えるアイエフエス（東京・中央）の佐藤昭弘代表取締役がその人だ。社員20人程度だが、バーコードシステムを開発したり、様々な社会インフラのシステムを構築したりしている。

その日、佐藤社長はうっかりした。海外から送られてきたと思われる、契約関係を問う英文メールの添付ファイルを開けてしまったのだ。同社の取引先は国内企業だけだが、「普段は英文メールは基本的に開けないのに、その前にニューヨークに何度か行っていたこともあり、その仲間関係からと思った」。

佐藤社長は本文をざっと読んだ。「アダルト系スパムメールやフィッシングメールという感じもなかった。ただ思い返せば、本当に深く考えずに開いてしまった」。

添付ファイルはExcelのアイコンだったが、ダブルクリックしてもExcelが立ち上がらない。一方で「ディスクI/Oランプがピコピコし

ていた」。瞬間、「しまった！マルウエア（悪意のあるソフトウエア）だ」。とっさにノートPCの電源を落とした。

　佐藤社長は開発プロジェクトの“火消し”やセキュリティコンサルティングを引き受けることが多いという。「うっかりとはいえ、人のことを言えた場合じゃない…」と感染を振り返る。

アイエフエスの佐藤昭弘代表取締役
[画像のクリックで拡大表示]

　しばらくしてノートPCを立ち上げる。「何も起きていない。電源オフで何とかなったか」。そのまま3時間ほど仕事をして、ファイルサーバーにある経理ファイルにアクセスしようとしたところ、ファイルが開かない。

　ファイルサーバーには社内のあらゆるデータが入っている。調べると6個のファイルが暗号化されていた。佐藤社長が感染に気付いてノートPCの電源を切るまでのわずかな間に、ランサムウエアは確実に“仕事”をこなしたのだ。

　「ランサムウエアはノートPCのレジストリーを調べているようだ」と佐藤社長は独自の解析結果を話す。「ノートPCで扱った新しいファイルのうち、ファイルサーバーにあるものだけを暗号化していった。とてもいやらしい」。

　ファイルサーバーのファイルは社員で共有して使うものが多い。それを暗号化してしまえば業務に支障が出ると攻撃者は分かってい

る。だからこそ法人被害者の6割が解除のための身代金を支払うのだ（関連記事：世界はランサムウエアに屈するのか）。

「感染した自分に頭にきた」で一念発起

佐藤社長は「頭にきた」という。「攻撃者はどうでもいい。技術者でありセキュリティを人に説くこともある自分が、うかつにも開いてしまったことに腹が立った」。ファイルサーバーのバックアップを取ったのは4カ月前で、暗号化された経理ファイルは税務署に提出する類いのもので、復旧しなければいけなかった。

身代金は支払わなかった。「復旧が保証されていないのだから支払う道理もない」と即断したからだ。佐藤社長は業務の合間を縫って、銀行や取引先に事情を説明。必要な情報を集めて、バックアップファイルから地道に復旧していった。費やした時間は3カ月間。「会社経営の機密情報なので人に頼めない。『バカなことをしている』とずっと思っていた」。

同時に、改めて攻撃者有利のサイバー攻撃の実態を感じ、自身の被害から、同様の被害に遭う人が続出するだろうと思いを巡らせた。「メールを開かなければ仕事ができないのに、メールと添付ファイルを開いた瞬間に“負け”てしまう。どんなに気を付けていても、うっかりや操作ミスは必ずある」。

2016年4月、佐藤社長はセキュリティソフトの開発に取り掛かった。目指したのは「添付ファイルを開いても本文中の不審なURLをクリックしても感染しない」仕組みだ。佐藤社長は過去、マルウエア解析ツールや定義ファイル作成ソフト、ハニーポット構築などにも携わった経験があるという。

数カ月をかけて完成させたのが「Preview Mail」というソフト。クラウドサービスとして提供する。その名の通り、添付ファイルの中身やURLのリンク先Webサイトを“プレビュー”するもので、実態はクラウド上の仮想デスクトップ環境で添付ファイルを開いたり、Webサイトを閲覧したりする。攻撃コードが仕込まれていても、仮想環境内に閉じるため、手元のPCは感染しない。いわゆる無害化ソフトの一種だ。

信頼できるのはAIよりも業務経験

仮想環境上で添付ファイルの中身を確認し、「本当に業務で必要だったら元のファイルをダウンロードする。人工知能（AI）の活用

が進みつつあるが、人間の判断にはまだまだかなわない」と佐藤社長は話す。ちゃんと中身を見て、判断できるところが新しい。

「とにかく多くの人に使ってほしい。しかも今困っているのは中堅中小企業だ。そのためには低価格でなければ」。そう考え、佐藤氏はオープンソースソフトウエア（OSS）でサービスを構築。仮想デスクトップを提供するコンテナにはDocker、OSにはUbuntu、オフィス文書ソフトにはApache OpenOfficeとLibreOffice（パスワード付文書の展開に使う）、WebブラウザーにはGoogle Chromeを採用した。ソフトはGO言語で開発したという。

価格は1ユーザー当たり月額300円（100～1000ユーザーの場合）とした。既に臨床試験受託大手EPSグループのITサービス会社であるイートライアルが採用を決めているという。

「企業では痛い目を見ないとサイバー攻撃対策は進まない」というのが記者が見てきた傾向。今回は技術者も痛い目に遭うとここまで奮起するものかと感じた次第だ。