日本経済新聞

敵は「本気」だ 標的型サイバー攻撃に狙われる日本

2015/6/17 6:30 | 日本経済新聞 電子版

日本年金機構の情報流出問題は氷山の一角にすぎず、日本を本気で狙ったサイバー攻撃が予想以上に広がっている――。セキュリティー会社のラックは16日、国内で広がる標的型攻撃について調査結果を説明し、国内の企業や組織が深刻な危険にさらされている現状について警告を発した。攻撃者は情報を抜き出すために、これまでとは格段に違う巧妙な手段を駆使しており、すでに侵入を許しながら気づいていないところが数多く存在するという。

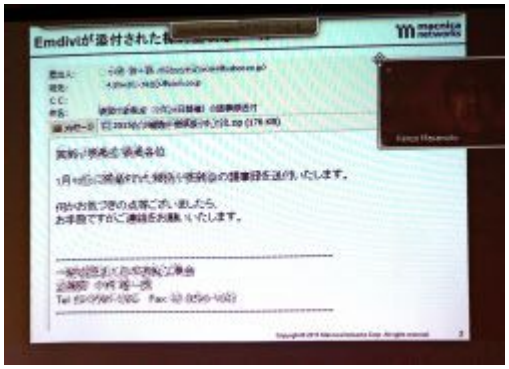
ラックは、日本年金機構への標的型攻撃に使われたウイルス「Emdivi（エンディビ）」を例に、国内が置かれている深刻な状況を指摘する。感染を発見した報告数は4月以降に急激に増えており、6月はまだ半月ながらすでに4月の2倍以上に達している。しかも、6月に感染したウイルスを調べると「（実際に）感染したのは4月より前のケースが多く2カ月たってようやく気づいたことになる」（内田法道サイバー救急センター長）と語り、もし年金機構の問題が報道され注目を集めなければ、水面下でさらに広まっていた可能性もあるだろう。

サイバー攻撃による年金情報流出で、日本年金機構が送付する謝罪文書＝共同

■判別はほぼ不可能

「健康保険組合です。添付ファイルで医療費をご確認ください」――。つい自分の会社から届いたメールかと勘違いしてクリックしてしまいそうだ。ほとんどの標的型攻撃で侵入のきっかけとして送られてくるメールは、とてもすぐに判断できないほどに巧妙化している。

以前ならば、日本語が不自然でいかにも“怪しい”メールが多かった。だが、「最近では、自然な日本語のメールが増えている」（説明会に同席したマクニカネットワークスの政本憲蔵セキュリティ研究センター長）。インターネット上に公開されている文書のテンプレートをコピーして日本語として違和感のない文書を作っているケースもあり、タイトルや文面で見分けることはほぼ不可能になっている。



最近の攻撃では、あたかも議事録を送付したかのように見せかけてメールが送られてくる

内容についても、講演会開催、セミナー参加、保険金配当、懇談会、勉強会など、誰でもどれかは心当たりがありそうなくらい多彩になってきた。攻撃者はメールを送る相手の仕事や取引先についても調べ上げた上で「関連する内容のメールを送る」（政本氏）ように悪質になってきている。

例えば、フェイスブックなどのSNSで勉強会に参加したと書き込んだのを見て、「6月1日の勉強会の資料を添付ファイルで送ります」などと、いかにもその勉強会の資料を送ってきたかのようなメールが届く。ほとんどの人が「あぁ、あのときの資料か」とついつい開いてしまうだろう。送り主を取引先の担当者に偽装した上で、「先日の資料に間違いがあったので再送します」というメールが届くこともある。

ウイルスを仕込んだ添付ファイルは、一見するとPDFやワード、エクセルといった文書に見えるアイコン

で送られている。ところが、このアイコンはなりすましで、文書だと思ってうっかり開いてしまうとプログラムが実行されウイルスに感染してしまう。

最後の頼みの綱は、パソコンに入っているウイルス対策ソフトだが、ほとんどの場合で役に立たない。「各社のウイルス対策ソフトの働きをシミュレーションして、すり抜けられるかを確認した上でウイルスを送ってくる」（内田センター長）のが当たり前だからだ。

「発見したら全力で封じ込めることが重要」と指摘するラック取締役の西本逸郎CTO

いったん組織内に潜入したウイルスは、パソコン内部に潜伏しつつ内部のネットワーク上で増殖していく。そして、それぞれのパソコン内や社内サーバー上の情報を脆弱性を突いて盗み出し外部に送って流出させる。こうした動作については外部の指令サーバーとやり取りするが、その際のデータは暗号化した上で細切れにし、どんなデータを送信しているか分からないようにしているのだ。

このため、「組織内部では分からず、セキュリティー団体など外部からの連絡で発覚するケースが多い」（内田氏）。ラックでは、現時点でも感染していながら、そのことを把握していない企業や組織が国内に多数存在すると指摘する。

■攻撃主は近隣にあり

こうした攻撃を仕掛けてくるのは、個人はなく組織的グループのようだ。マクニカが捕獲した65個のウイルスについて作成時間を調べてみると、日本時間で午前9時から数が増え午前11時がピークになっていることがわかった。その後、14時に極端に少なくなってからまた増え始め、19時以降はまた少なくなる。日本と時差が少ない地域ならば、ほぼビジネスアワーと一致するカーブだ。曜日ごとに見ても、平日に多く土日が少ないといったように「一般的なサラリーマンのように規則正しく働く組織によって作られたと推測される」（政本氏）

ラックの西本逸郎CTO（最高技術責任者）は、韓国で流行している中東呼吸器症候群（MERS＝マーズ）に例えながら「警察やセキュリティー団体から連絡があったら、もはや単なるかぜでは済まない。ウイルスに突破されたということなので、全力で封じ込めることが重要だ。最低限の策しか取れないと傷口を広げる」と警告する。具体的には、従来の対処法にとどめず、社内全体の通信を遮断する「封じ込め」が必要と訴えた。

（電子編集部　松元英樹）