コピーセンター通信　2022年4月号　中小企業を襲うサイバー攻撃の実態

中小企業を襲うサイバー攻撃の実態

富士フイルムビジネスイノベーションは、独立行政法人情報処理推進機構が実施した「サイバーセキュリティお助け隊」（2019年度）の長野県、群馬県、栃木県、茨城県、埼玉県における事業実施会社として、101社の事業協力企業様に**セキュリティ機器端末（beat）**を設置し、中小企業におけるサイバー攻撃の実態調査を行いました。

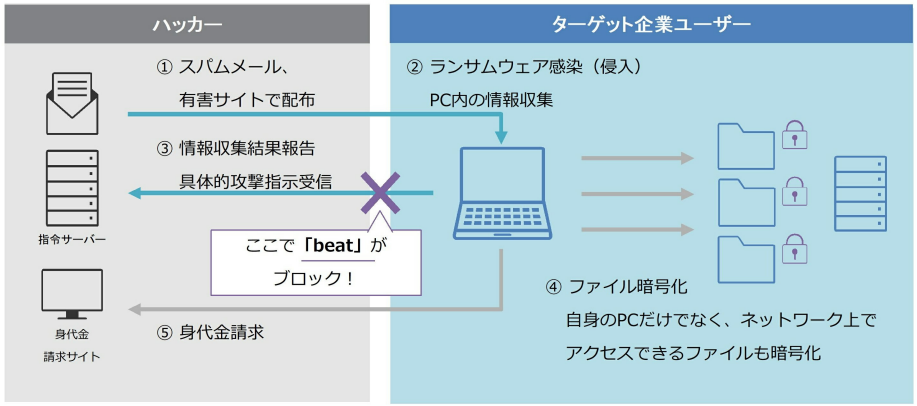
結果、下表のとおりのサイバー攻撃の実態が明らかとなり、「まさかうちの会社が…」と協力会社様も驚く実態が明らかとなりました。

期間：2019年9月～2020年1月

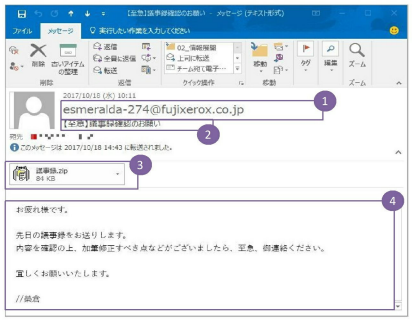
内容	総件数	1社あたり/月
情報漏えいの可能性がある内部から外部への通信※1	7,000,000件	13,861件
危険サイトへのアクセス	3,200,000件	6,337件
スパムメール受信	140,000件	277件
インターネット上の存在確認（ドアノック※2）	94,000件	187件
ウイルス、スパイウエア検知	300件	0.6件

※1 IPS検知
※2 ping/port-scan件数

実際に起きた「ランサムウェア」への感染



どの様にして「ランサムウェア」は企業に入り込むのか。（メール例）



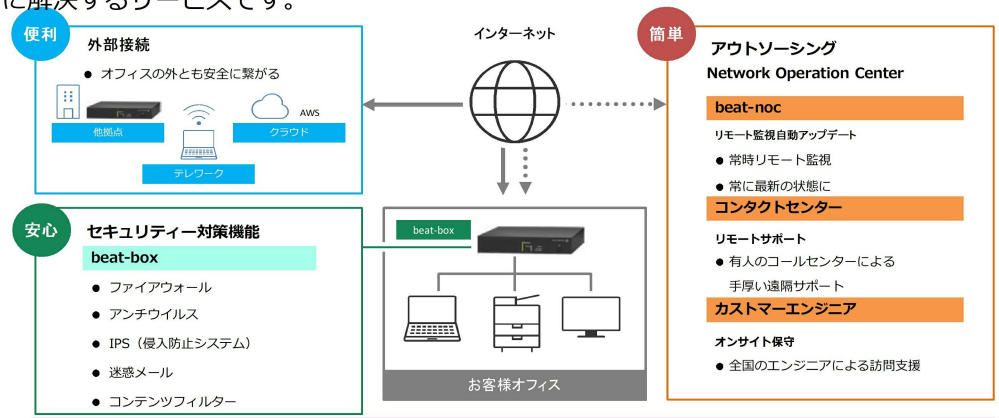
1. 実在する組織を連想させるメールアドレスを偽装。
2. 「ご依頼の件」のようにある程度凡用性のあるタイトルではなく、件名も具体的。
   →「最新組織図です」や「会議資料の事前送付」など。
3. 形式は「zip」や「pdf」「xlsx」が多い。
   添付ファイルをクリックするとランサムウェアに感染！
4. 記載されている内容には当人または当人関係者しか知りえない内容が記載されているケースもある。
   →関係者のPCがランサムウェアに感染しており、そこから得た情報で、感染拡大を試みている。

複数企業でネットワーク化されているが故に、一つの穴を突破口にサプライチェーン全体を攻撃できることをハッカーは知っています。**御社のみならず取引先企業全体を狙っているのです。**

ランサムウェアで攻撃ができなくても、侵入により得た情報で次の突破口を探します。

富士フイルムビジネスイノベーション「beat」をご検討ください

beatは、ネットワーク環境に関するお客様のさまざまなお悩みを 安心 簡単 便利 に解決するサービスです。



今ならお試し利用も可能です。サイバー攻撃の実態診断してみませんか？

- オフィスのネットワークを守るセキュリティーを提供！
- 専任の管理者がいなくても大丈夫。運用は富士フイルムビジネスイノベーションにお任せ！
- テレワークに必要なリモートアクセス環境も簡単に構築可能です！

株式会社いわきコピーセンター　〒970-8026 いわき市平字作町3丁目4－5　TEL:0246-24-2371　FAX:0246-22-2638　http://www.iwakicopy.co.jp