2016年9月

脅威レポート

McAfee Labs

情報の窃盗

情報漏えいの現状

53%
外部の組織によって発見された侵害

62%
顧客情報や従業員情報が盗まれた侵害

約40%
物理的な媒体の盗難による情報漏えい

68%
報告義務のある情報漏えいが発生した侵害

25%以上
顧客情報や従業員情報に対するアクセスを監視していない企業

わずか37%
エンドポイントでユーザー アクティビティ、物理的なメディアを含むモニタリングを実行している企業

医療機関の危機

病院を狙うランサムウェア

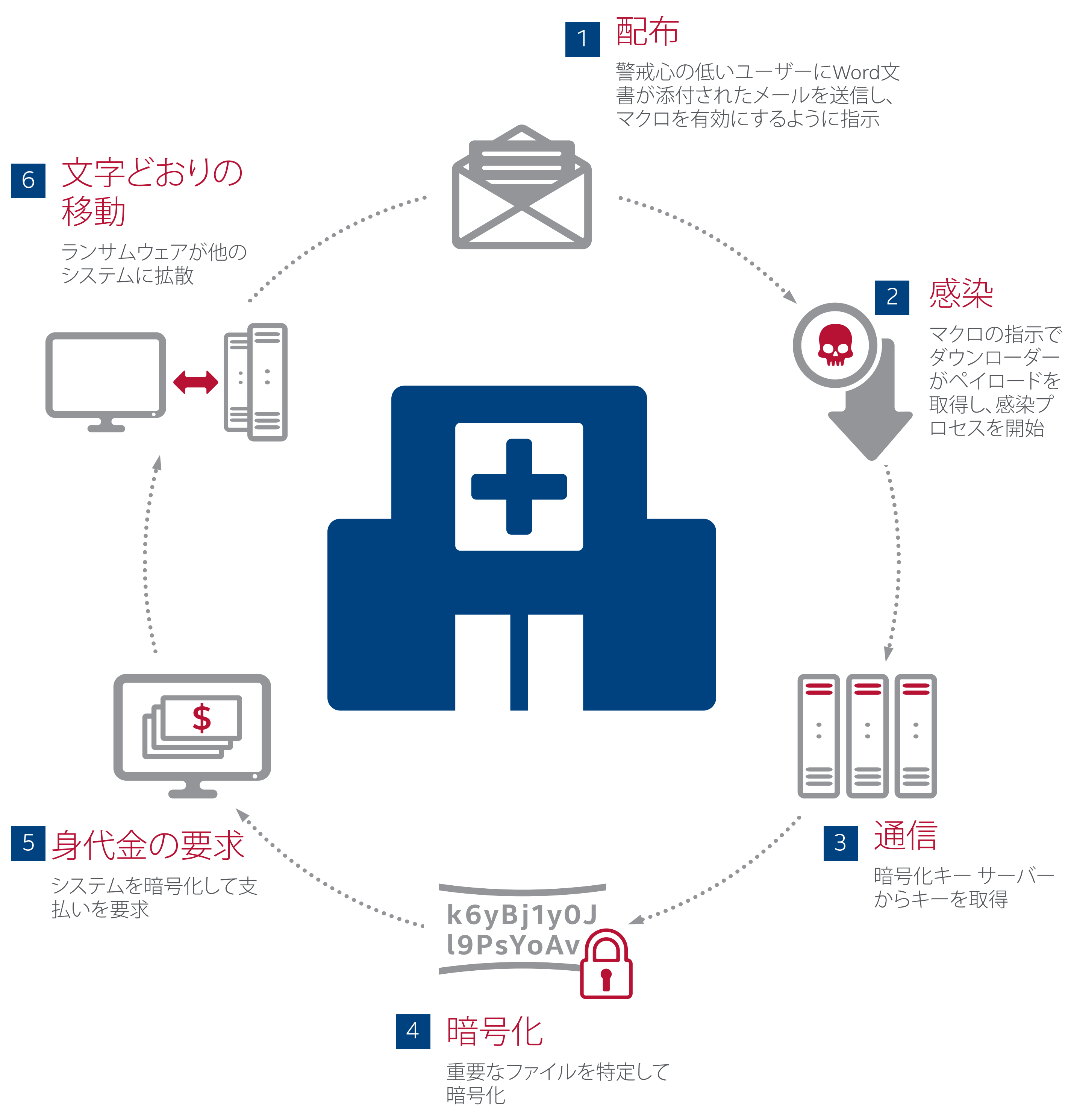
ランサムウェアの作成者が医療機関を狙う理由

レガシー システム
脆弱性のあるレガシー システムを使用

医療機器
脆弱な医療機器またはセキュリティを導入していない医療機器を使用

患者管理
最適な患者管理を行うには情報への迅速なアクセスが不可欠

医療機関を狙うランサムウェアの攻撃



1 配布
警戒心の低いユーザーにWord文書が添付されたメールを送信し、マクロを有効にするように指示

2 感染
マクロの指示でダウンローダーがペイロードを取得し、感染プロセスを開始

3 通信
暗号化キー サーバーからキーを取得

4 暗号化
重要なファイルを特定して暗号化

5 身代金の要求
システムを暗号化して支払いを要求

6 文字どおりの移動
ランサムウェアが他のシステムに拡散

19の病院
第1四半期と第2四半期で少なくとも19の病院がランサムウェアに感染

$17,000
第1四半期、カリフォルニアの病院がランサムウェアに感染し、システムが5営業日も停止。ファイルとシステムを復旧するため$17,000を支払う。

$100,000
Intel Securityが確認したところ、第1四半期、病院への標的型攻撃に関与したグループが$100,000の身代金を受け取る

分析

機械学習による攻撃の阻止

複数のコンピューターを使用して継続的な分析を自動的に実行

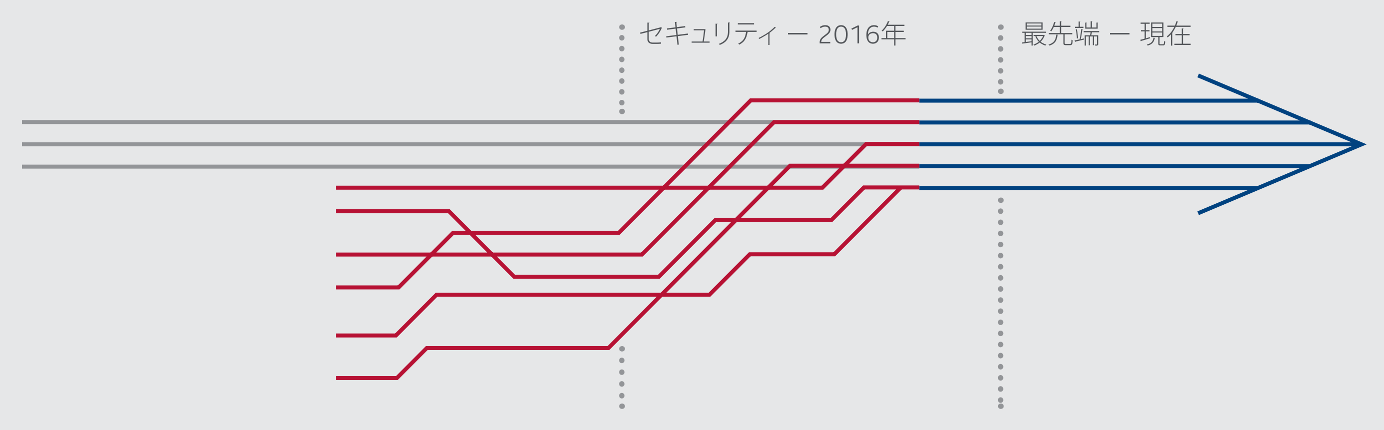
処方的分析
予測される事態に対して何をすべきかを指示

記述的分析
何が起きたのかを記述

予測分析
何が起きるのかを予測

診断的分析
発生した理由を分析

分析の進化



1.0
Analytics 1.0
- 内部の構造化されたデータセット
- 記述と診断
- 受け身的だが有益

2.0
Analytics 2.0
- ビッグデータ複雑で構造化されていない膨大なデータ
- 内部と外部の情報源からデータを収集

3.0
Analytics 3.0
- ビッグデータの利用、ディープラーニング、コグニティブ コンピューティング
- 迅速でプロアクティブな検出

情報ソース: International Institute for Analytics.

統計情報

1分間に出現する新しい脅威は316件で、1秒あたりに換算すると5件を超える

マルウェア 32%
第2四半期に見つかった新しいマルウェアのサンプル数は4,100万で、過去2番目の記録。**McAfee Labsのデータベースに登録されたマルウェアのサンプル数はこの1年で32%増加し、6億を超える**

ランサムウェア 128%
第2四半期に見つかった新しいランサムウェアのサンプル数は約130万で、過去最高。**ランサムウェアの合計数はこの1年で128%増加**

モバイル マルウェア 151%
第2四半期に見つかった新しいモバイル マルウェアのサンプル数は約200万で、過去最高。**モバイル マルウェアの合計数はこの1年で151%増加**

マクロ ウイルス 106%
第2四半期に見つかった新しいマクロ マルウェアは前四半期よりも200%以上も増加。この増加にはダウンローダー型トロイの木馬が関与。**マクロ マルウェアの合計はこの1年で106%増加**

McAfee Global Threat Intelligence

McAfee GTIが1日に受信したクエリーは平均で486億件

McAfee GTI

1億
McAfee GTIで阻止した不正なURLは昨年より若干増加。**第2四半期は1日平均1億件**

3,000万
McAfee GTIで阻止した不審なプログラムは**昨年より83%減少。第2四半期は1日平均3,000万個**

1億400万
McAfee GTIで阻止した不正なファイルは**昨年より77%減少。第2四半期は1日平均1億400万個**

2,900万
McAfee GTIで組織した危険なIPアドレスは過去2年間で最高に。**1日あたり2,900万件で、前四半期よりも128%増加**

McAfee Labs脅威レポート: 2016年9月

レポートの完全版は、www.mcafee.com/September2016ThreatsReportをご覧ください。

intel Security

912_0816_info_sept-2016-quarterly-threats