2017年4月

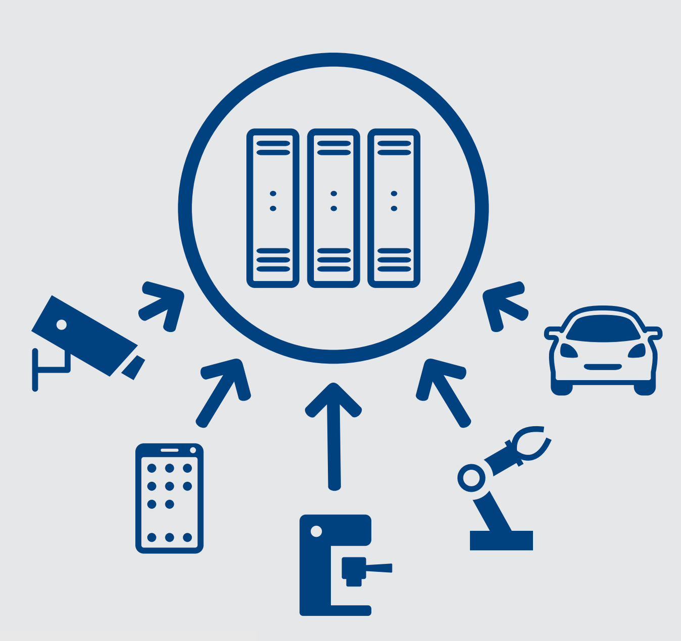
脅威レポート

McAfee Labs

Mirai ー IoTボットネット

Miraiボットネットは、セキュリティ対策が不十分なIoTデバイスを攻撃し、過去最大規模の分散型サービス拒否攻撃を実行しました。

攻撃のプロセス



1 IoTデバイスをスキャン
MiraiがIPアドレスをスキャンし、開いているTelnetまたはSSHポートからIoTデバイスに侵入する。

2 総当たり攻撃
Miraiが、一般的なデフォルトのユーザー名とパスワードの辞書を使用してIoTデバイスに総当たり攻撃を実行し、脆弱なデバイスを識別する。

3 認証情報を送信
総当たり攻撃に成功すると、感染先のIoTデバイスのIPアドレスと認証情報を指令サーバーに送信する。

4 Miraiボットをダウンロード
ローディング サーバーがMiraiボットのバイナリをIoTデバイスにダウンロードする。

5 攻撃命令を待機
IoTデバイスに感染したマルウェアがDDoS攻撃命令を待機する。

6 DDoS攻撃を開始
MiraiがOSIモデルの第3、4、7層でDDoS攻撃を実行する。

250万
約250万台のIoTデバイスがMiraiに感染

1分あたり5個
1分あたり5個のIPアドレスがMiraiボットネットに追加される

1.2 Tbit/sのトラフィック
Miraiボットネットの標的の一つでピーク時に1.2 Tbit/sのトラフィックが発生。過去最大規模のDDoSトラフィックを記録

1日あたり$50～$7,500
MiraiによるDDoS攻撃サービスが1日あたり$50～$7,500で提供される

Miraiの進化

1 2016年8月ごろ
最初のリリース
Mirai ELFバイナリが出現

2 2016年9月20日
Krebs on SecurityのWebサイトに対するDDoS攻撃
MiraiがTelnetポートでDVRとCCTVに感染

3 2016年10月1日
ソースコードの公開
Anna-SenpaiがMiraiのソースコードを公開

4 2016年10月4日
サービスとして提供されるMiraiボットネット
地下フォーラムでDDoSサービスが提供される

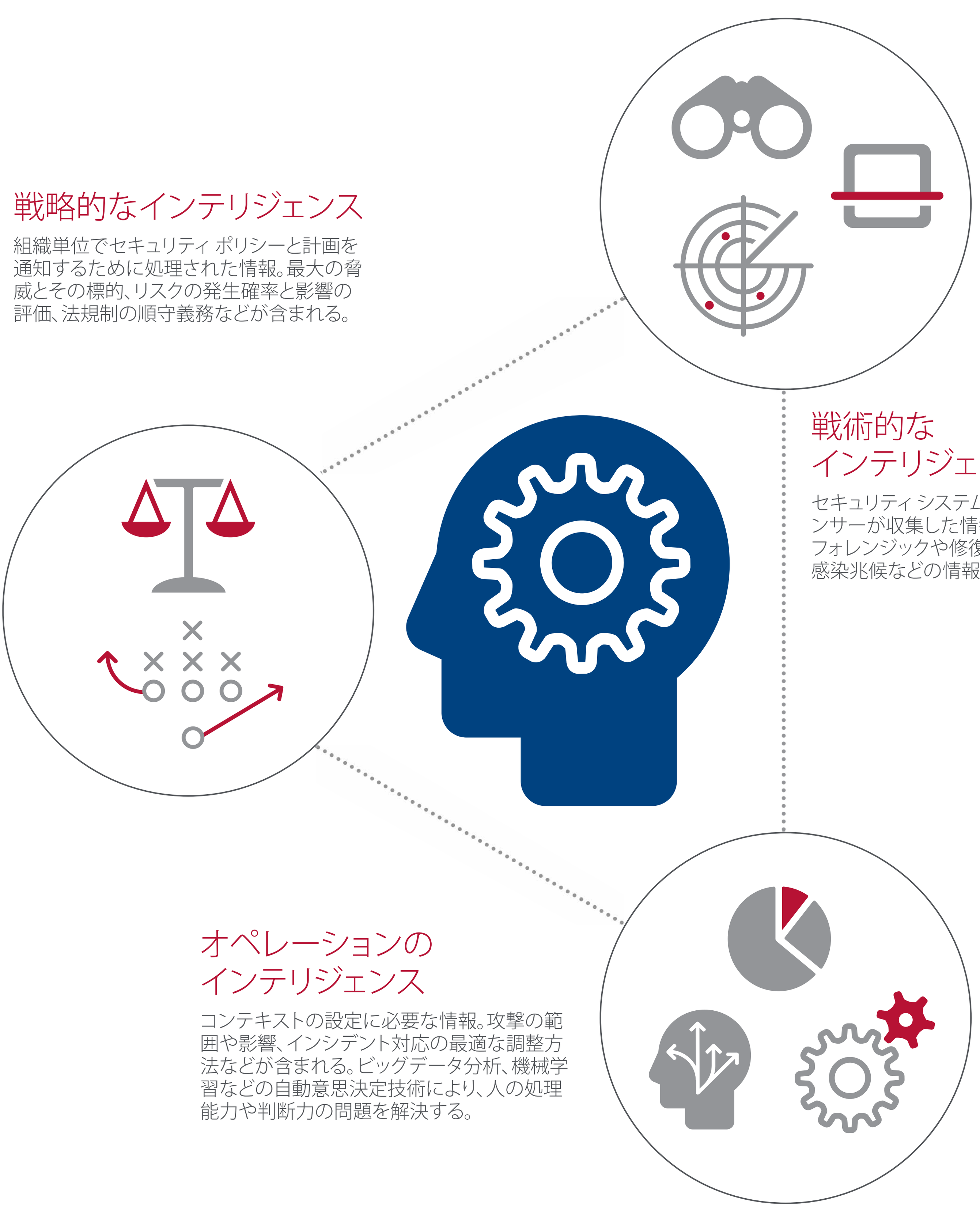
5 2016年11月28日
ドイツテレコムのサービスを停止
Miraiの新しい亜種が出現
ポート7547を攻撃

8月 | 9月 | 10月 | 11月

脅威インテリジェンスの共有

情報がないと被害を受ける可能性があります。

脅威インテリジェンスとは?



戦略的なインテリジェンス
組織単位でセキュリティ ポリシーと計画を通知するために処理された情報。最大の脅威とその標的、リスクの発生確率と影響の評価、法規制の順守義務などが含まれる。

戦術的なインテリジェンス
セキュリティ システム、スキャナー、センサーが収集した情報。多くの場合、フォレンジックや修復作業に有益な感染兆候などの情報が含まれる。

オペレーションのインテリジェンス
コンテキストの設定に必要な情報。攻撃の範囲や影響、インシデント対応の最適な調整方法などが含まれる。ビッグデータ分析、機械学習などの自動意思決定技術により、人の処理能力や判断力の問題を解決する。

脅威インテリジェンス共有における重大な課題

量
セキュリティ センター、ビッグデータ分析、機械学習ツールにより大量の情報が生成されるため、適切な情報の識別に時間がかかる。トリアージ、プロセス、対応に影響を及ぼす。

検証
脅威インテリジェンス ツールが偽情報の影響を受けないように、脅威インテリジェンスの情報源を検証し、正規の情報源から受信したデータかどうかを確認する。

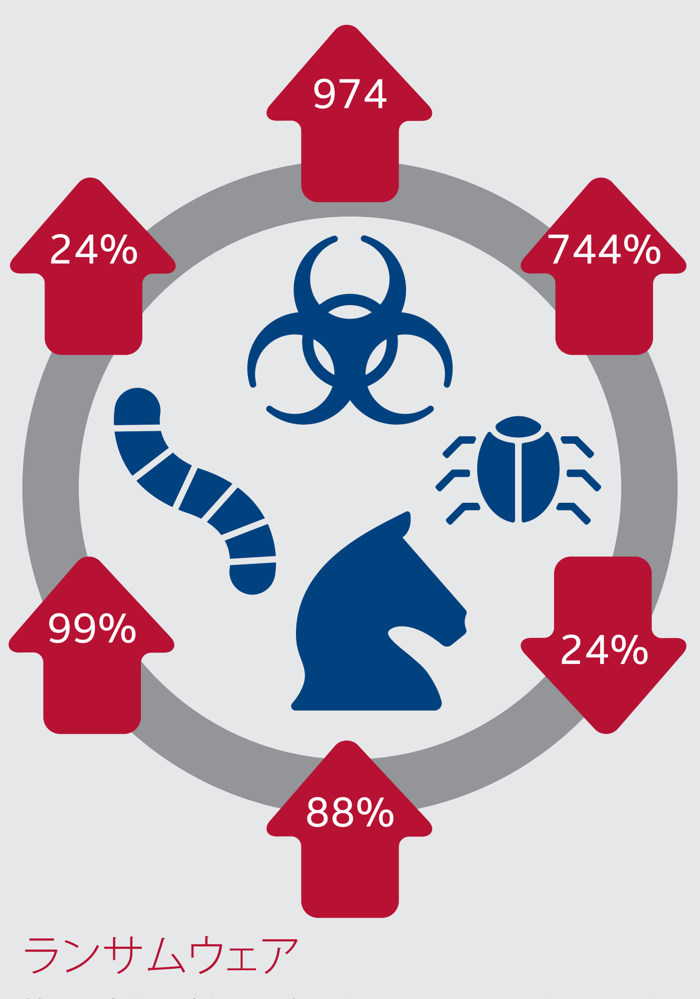
相関分析
効果的な対策を行うには、データをリアルタイムで検証し、異なるオペレーティング システム、デバイス、ネットワーク間で相関分析を行い、イベントの優先度を判断して対応範囲を決めることが重要になる。

品質
正規の情報源が、感染兆候からイベントの詳細まで、あらゆる情報を送信する。受信者に関係のない情報が含まれている場合もある。脅威インテリジェンスを効果的に行うには、フィルター、タグ、重複削除などを自動的に行う必要がある。

速度
攻撃の検出から脅威インテリジェンスの受信までの遅延を抑えるには、オープンで標準化されたリアルタイム通信が重要になる。

統計情報

1分間に出現する新しい脅威は176件で、1秒あたりに換算すると約3件になります。



インシデント
第4四半期に197件のインシデントを確認。2016年の合計は974件。

マルウェア
第4四半期に見つかった新しいマルウェア サンプルは2,300万件で、第3四半期よりも17%減少。**合計数で見ると、2016年は24%増加し、6億3,800万件。**

Mac OSを狙うマルウェア
Windowsの脅威に比べると数は少ないが、第4四半期に見つかった新しいMac OSマルウェアは245%増加。アドウェアのバンドルが原因。**合計で見ると2016年は744%増加。**

モバイル マルウェア
第4四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17%減少。**合計数で見ると、2016年は99%増加。**

スパム ボットネット
第4四半期に上位10個のボットネットから送信されたスパム メールは24%減少し、1億8,100通。2016年は上位10個のボットネットで9億3,400億通のスパムメールが生成される。

ランサムウェア
第4四半期に新たに確認されたランサムウェアのサンプルは71%減少。Locky、CryptoWallなどのランサムウェアが減少。**合計数で見ると、2016年は88%増加。**

McAfee Global Threat Intelligence

McAfee GTIが1日に受信したクエリーは平均で496億件です。

6,600万
第4四半期にMcAfee GTIで阻止した不正なURLは増加。一日あたりの件数では、第3四半期の5,700万件に対し、**第4四半期は6,600万件に増加。**

3,700万
第4四半期にMcAfee GTIで阻止した不審なプログラム(PUP)は増加。1日あたりの件数は第3四半期の3,200件に対し、**第4四半期は3,700万件に増加。**

7,100万
第4四半期にMcAfee GTIで阻止した不正なファイルは減少。一日あたりの件数では、第3四半期の1億5,000万件に対し、**第4四半期は7,100万件に減少。**

3,500万
第4四半期にMcAfee GTIで阻止した危険なIPアドレスは増加。1日あたりの件数は第3四半期の2,700件に対し、**第4四半期は3,500万件に増加。**

McAfee Labs脅威レポート: 2017年4月

レポートの完全版は、www.mcafee.com/April2017ThreatsReportをご覧ください。

intel Security