2016年12月

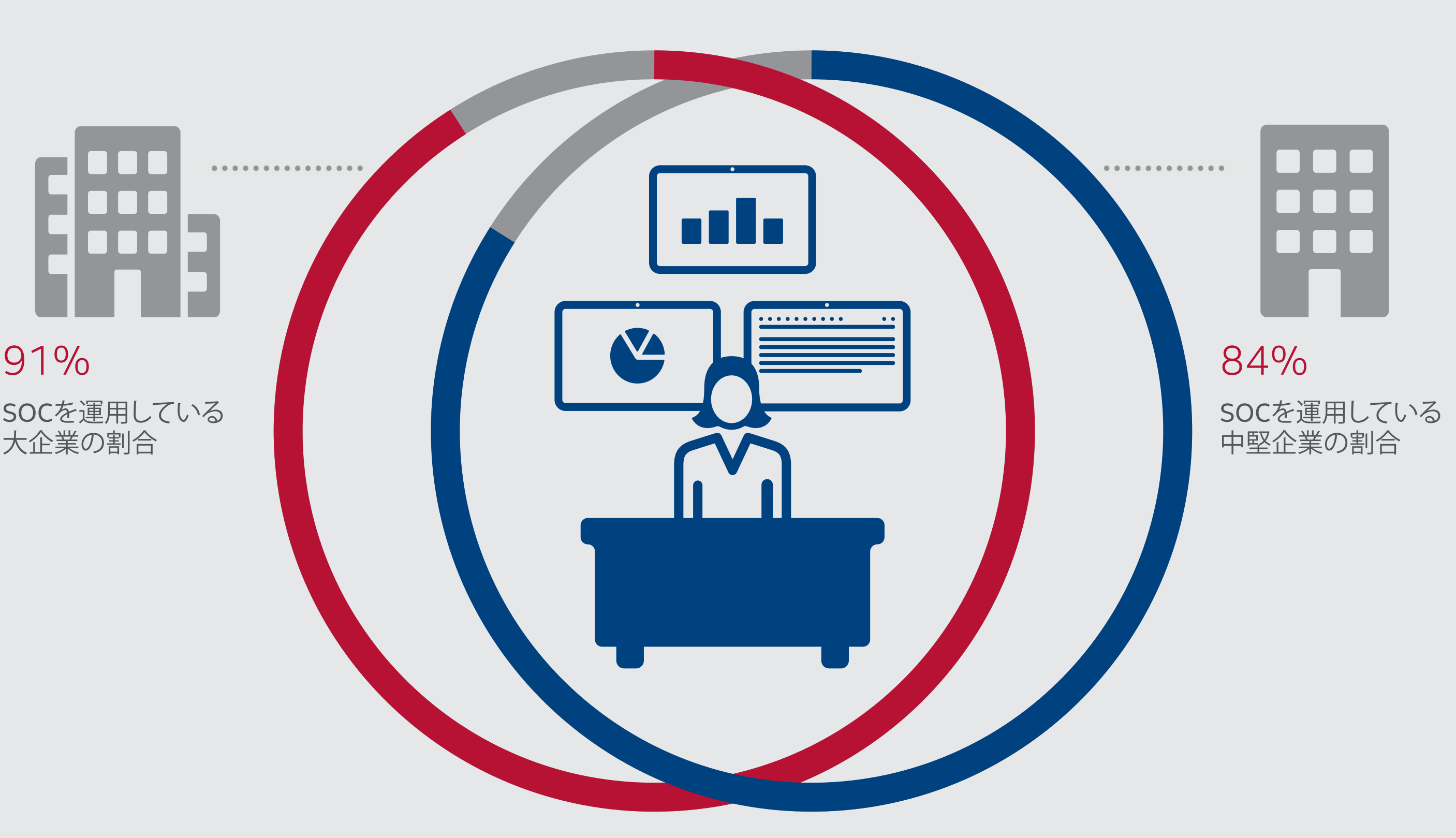
脅威レポート

McAfee Labs

セキュリティ オペレーション センター

セキュリティ オペレーション センター（SOC）の現状と今後

10社中9社がSOCを運用している



91%
SOCを運用している大企業の割合

84%
SOCを運用している中堅企業の割合

74%
プロアクティブで最適化されたセキュリティ運用を目指している組織の割合。ただし、26%はいまだに事後対応型で、セキュリティ管理、脅威検出、インシデント対応を場当たり的に行っている。

64%
マネージド セキュリティ サービス プロバイダーからセキュリティ オペレーションの支援を受けている企業の割合

69%
すでにSIEMソリューションを利用している企業の割合。SIEMを現在利用していない企業の45%は、今後12～18か月以内に導入を予定している。

93%
大半の組織で大量のアラートが発生している。93%の組織が脅威の優先度を判断できていない。

65%
SOCを導入している組織で、体系的な脅威検出を行っている組織の割合

今後、成長・能力向上が期待される領域:

対応
確認した攻撃に対する対応。連携して被害の修復、脅威の根絶、再発防止に取り組む。

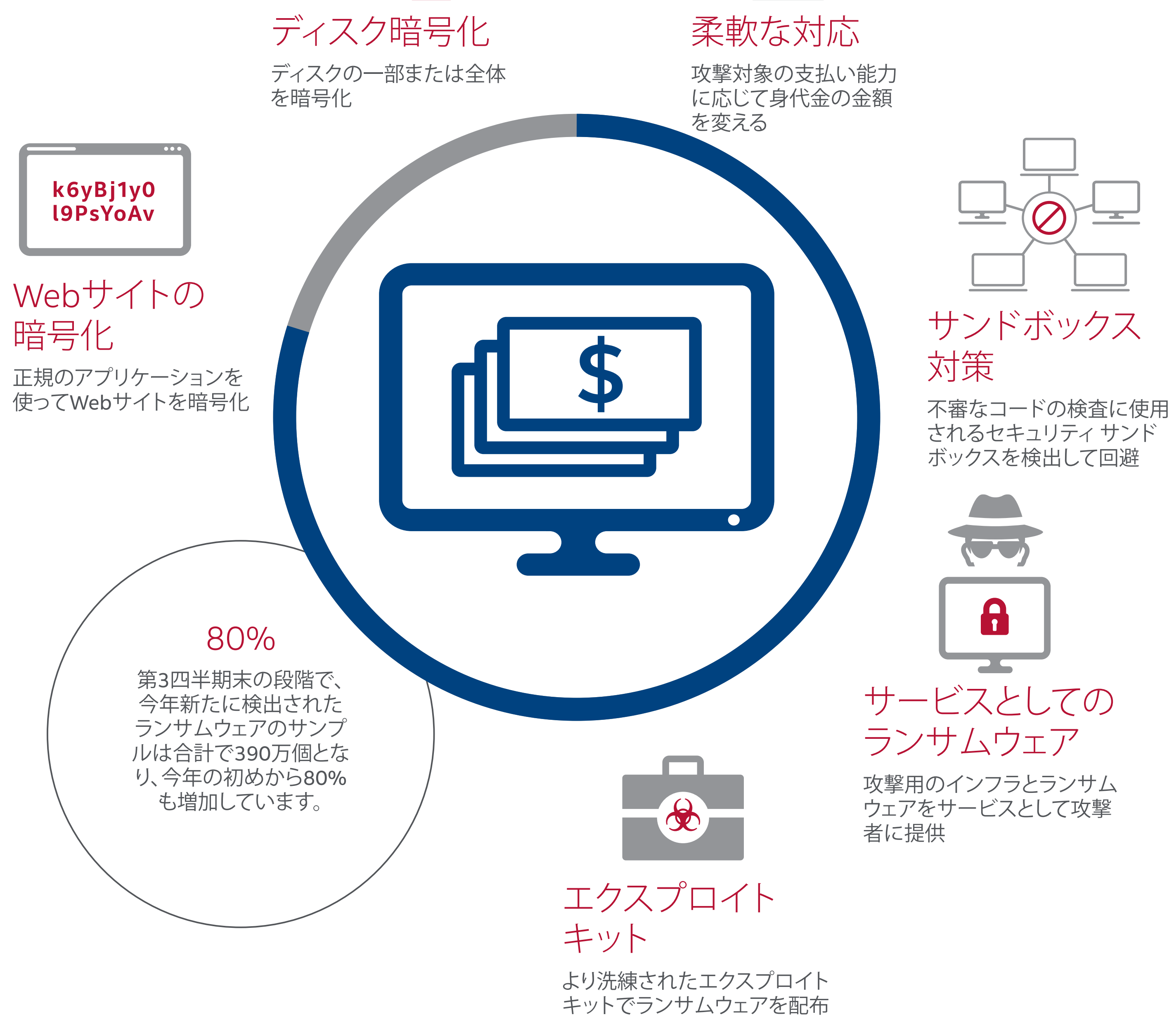
検出
脅威の兆候を表すシグナルを検出。関連するイベントとアラートを識別し、脅威の重大度を判断して優先順位を付ける。

調査
潜在的な攻撃を調査。攻撃の範囲や影響度を事前に調査する。

猛威を振るうランサムウェア

2016年はランサムウェアによる攻撃が急増。非常に高度な技術を駆使するランサムウェアが出現。セキュリティ業界も対策を強化している。

2016年のランサムウェアが使用した高度な手口:



ディスク暗号化
ディスクの一部または全体を暗号化

柔軟な対応
攻撃対象の支払い能力に応じて身代金の金額を変える

Webサイトの暗号化
正規のアプリケーションを使ってWebサイトを暗号化

サンドボックス対策
不審なコードの検査に使用されるセキュリティ サンドボックスを検出して回避

80%
第3四半期末の段階で、今年新たに検出されたランサムウェアのサンプルは合計で390万個となり、今年の初めから80%も増加しています。

サービスとしてのランサムウェア
攻撃用のインフラとランサムウェアをサービスとして攻撃者に提供

エクスプロイト キット
より洗練されたエクスプロイト キットでランサムウェアを配布

セキュリティ業界の対応

コラボレーション

NO MORE RANSOM!

No More Ransom!
7月に設立された組織。被害防止の助言、調査支援、復号ツールの提供を行う。

捜査機関による取締り

WildFire
ランサムウェアの封鎖

Shade
ランサムウェアの封鎖

正規のソフトウェアがトロイの木馬に

トロイの木馬が正規のコードに感染して潜伏。長期にわたり検出を回避し、最大の効果を狙う。

トロイの木馬のメリット

合法的な印象
広く認知されているブランドに隠れ、正当な印象を与える。

隠れ蓑
セキュリティ スキャンやフォレンジック分析で正規のソフトウェアが盾となり、検出を回避する。

持続性
正規のソフトウェアをトロイの木馬にすることで、持続性を維持することができる。

正規のソフトウェアをトロイの木馬にする方法

変更
オープンソースまたは逆コンパイルしたコードを利用

パッチ
仲介者攻撃でダウンロードさせたパッチを実行ファイルに適用

バンドル
バインダーや結合ツールで正常なファイルと不正なファイルをバンドル

実行ファイルの変更
パッチ適用ツールでアプリケーションにシームレスにパッチを適用

有害コードを混入
マスター ソース コード、特に、再配布用のライブラリを狙う

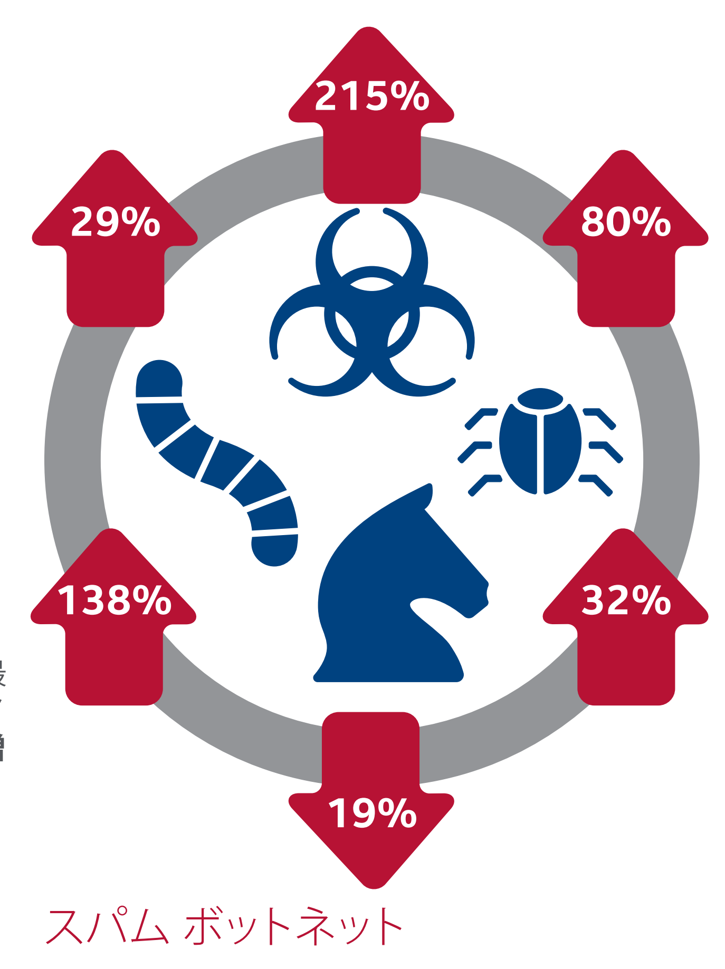
700,000
第3四半期末までに、3つのAndroidマルウェア ファミリだけで、700,000を超えるバイナリがトロイの木馬に変えられています。

30,000
第3四半期までで、2つのバックドア パッチ ツールにより、30,000個のAndroidバイナリがトロイの木馬に変えられました。

統計情報

1分間に出現する新しい脅威は245件で、1秒あたりに換算すると4件を超える。

Mac OSを狙うマルウェア
Windowsの脅威に比べると数は少ないものの、第3四半期に見つかった新しいMac OSマルウェアのサンプルは65%増加。**Mac OSマルウェアの合計数はこの1年で215%増加している。**



マルウェア
第3四半期に見つかった新しいマルウェア サンプルは3,200万件で、第2四半期よりも21%減少。**ただし、総数は昨年よりも29%増加し、サンプル数は6億4,400万件に達している。**

ランサムウェア
第3四半期のランサムウェア サンプルの合計数は18%増加。**2016年の増加率は80%を超える。**

モバイル マルウェア
第3四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200万を超え、過去最高を記録。**モバイル マルウェアの合計数はこの1年で138%増加。**

マクロ ウイルス
新しいマウロ ウイルスは引き続き増加。**マクロ マルウェアの合計は前四半期より32%増加している。**

スパム ボットネット
第3四半期は、Kelihosボットネットから配信されるスパム メールの数が97%減少。逆に、Necursボットネットからのスパムは554%増加。**全体的には、第3四半期にボットネットから送信されたスパム メールの件数は19%減少している。**

McAfee Global Threat Intelligence

McAfee GTIが1日に受信したクエリー: 平均441億件

McAfee GTI

5,700万
第3四半期にMcAfee GTIで阻止した不正なURLは減少。**第2四半期は1日あたり1億件だったが、第3四半期は5,700件に減少している。**

3,200万
第3四半期にMcAfee GTIで阻止した不審なプログラムの数は第2四半期よりも若干増加。2015年の第3四半期と比べると劇的に減少。**2015年第3四半期は1日あたり1億7,500万個だったが、2016年第3四半期は3,200万個に減少している。**

1億5,000万
第3四半期にMcAfee GTIで阻止した不正なファイルは増加。**第2四半期は1日あたり1億400万件だったが、第3四半期は1億5,000件に増加。**ただし、前年同時期よりも減少している。

2,700万
第3四半期にMcAfee GTIで阻止した危険なIPアドレスは若干減少。**第2四半期は1日あたり2,900件だったが、第3四半期は2,700万件。**2015年の第2四半期から第3四半期も減少しているが、これよりも落ち込みが大きい。

McAfee Labs脅威レポート: 2016年12月

レポートの完全版は、www.mcafee.com/December2016ThreatsReport をご覧ください。

intel Security

1941_1016_info_threats-report-dec-2016