シスコ 2015 年
中期セキュリティ レポート

コンビネーション攻撃回避 ポイント ソリューション

2015 年の前半、悪意のある攻撃者は目的を達成するために俊敏性、破壊力、適応性、速さを十分に用いた高度な攻撃を仕掛けてきました。Angler、Rombertik、Adware MultiPlug、および Dridex は、これらを組み合わせた攻撃が検出を回避し、防御された場所に侵入し、システムを破壊する方法を示した最もよく知られている 4 つの例です。

Angler

俊敏性が強み

不正アクセスしたランディング ページを **分かりにくくする**

遅延分析のために **ペイロードを暗号化**する

効果を高めるために種類の異なる **「わな」**を投入し続ける

パッチを適用していないソフトウェアを
標的にして弱点を突く

40% のユーザに侵入

75% **以上**
のドメイン シャドウイング アクティビティが Angler に至る

Rombertik

変更されたら破壊される

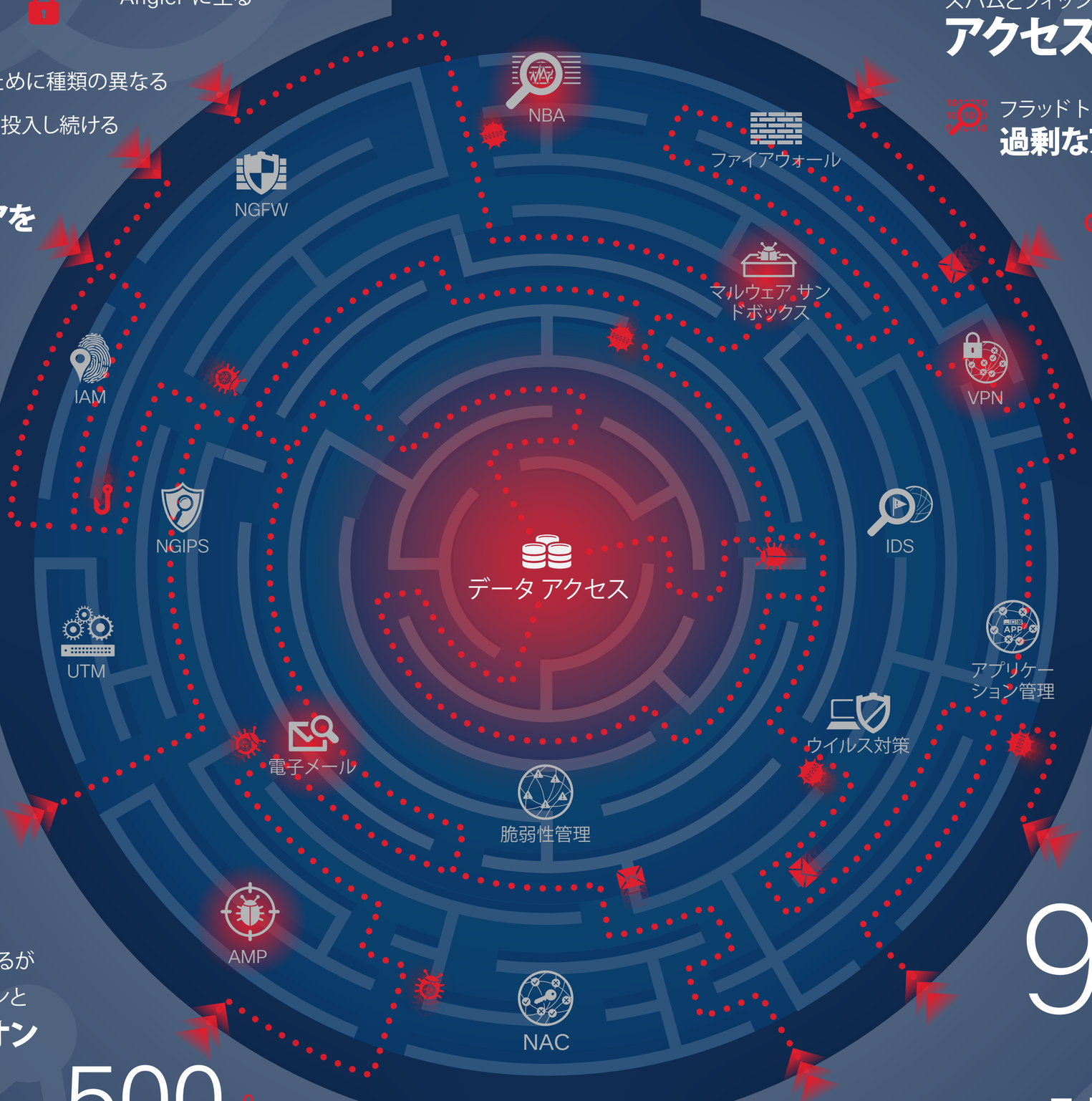
9 億 6000 万回
のメモリへの命令、サンドボックスに対する引き延ばし戦術を実施する

マスター ブートレコードを破壊して
コンピュータを動作不能にする

スパムとフィッシングを使用して **アクセスする**

フラッド トレース ツールに対する **過剰なアクティビティを実行**

サンドボックスを通過して、アンチ デバッギング メカニズムとして Windows API を **335,000 回**コールする



Adware MultiPlug

検出されないように順応し、変異する

一見役に立つように見えるが不必要なアプリケーションと **悪意のあるアドオン**をバンドルする

500
ドメインが使用された（3 ヵ月間）

侵入率を上げるため古い URL 符号化方式から **転換**

4,000
個のアドオン変異が採用された

Dridex

センサーの速度を上げる

9 時間で
従来のウイルス対策ツールが反応する前に侵入行動を完了

Microsoft® Office の **マクロ**を使用して銀行にトロイの木馬をすばやく送信

最大 850 回の ユニークな侵入行動が一定時間内に観測された

ユーザ エージェント、添付ファイル、リファラなど **侵入行動の内容をすばやく変化させ** 侵入行動を再試行する

セキュリティ業界はコンビネーション攻撃に対応するように、統合型の脅威に対する防御に移行する必要があります。詳細については、2015 年の中期セキュリティ レポートをダウンロードしてください。

www.cisco.com/jp/go/msr2015