進化する標的型攻撃

ADVANCED PERSISTENT THREATS

巧妙なマルウェアを
見破れるか?

NEARLY 88%

近年のマルウェア

変異を繰り返し、シグニチャベースの
セキュリティ対策では検知できない*

標的型攻撃(APT)とは?

標的の絞り込み
公的機関、国家・組織、
先進技術を持つ企業
不正侵入

高度な技術
未知のゼロデイ攻撃
マルウェアペイロード、
カーネルルートキット
検知からの回避技術

執拗かつ悪質
諦めない
執拗なフィッシング
感染させるための
綿密な計画

APT の進化

APT はもはや大企業や国家、団体だけ
を標的にしていない。規模に関係なく、
すべての企業にAPTのリスク

January 2010 — オペレーションオーロラ
標的: Google
被害: ソースコードが漏えい

June 2010 — スタックスネット(Stuxnet)
標的: イラン
被害: 原発の運用への影響

March 2011 — RSA/Lockheed
標的: RSA、ロッキードマーチン社
被害: SecureIDに関する情報漏えい

September 2011 — Duqu
標的: イラン、スーダン、シリア、キューバ
被害: デジタル証明書の漏えい

May 2012 — Flame
標的: 中東諸国
被害: 情報収集と漏えい

January 2013 — New York Times
標的: NY Times
被害: 情報・企業パスワードの漏えい

October 2013 — Adobe
標的: Adobe
被害: 顧客情報とデータの漏えい

December 2013 — Target
標的: Target
被害: 顧客クレジットカード情報の漏えい

APT 攻撃の例

複数の攻撃手法の組合せ
常に複雑化、進化

APTに有効な対策と効果のない対策

効果のない対策

ウイルス対策単体
アプリケーション制御
スパム対策
従来のファイアウォール
IPS

有効な対策

多層型防御、
ログ分析と可視化ツール
、シグネチャレス検知技術

(次世代のサンドボックス、
エミュレーション、
リアルタイムレピュテーション
セキュリティ)

WATCHGUARD APT BLOCKER

リアルタイム 脅威の可視化
迅速な防御

WatchGuard APT Blocker - WatchGuard XTM

www.WatchGuard.co.jp/APTBlocker