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?



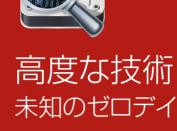
## 近年のマルウェア 変異を繰り返し、シグニチャベースの

セキュリティ対策では検知できない\*

標的型攻撃(APT)とは?



公的機関、国家·組織、 先進技術を持つ企業 不正侵入



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



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 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、

APT の進化

すべての企業にAPTのリスク オペレーションオーロラ January 標的: Google

標的: イラン

2010

被害: ソースコードが漏えい

June 2010

被害: 原発の運用への影響

スタックスネット(Stuxnet)

March

2011

標的: RSA、ロッキードマーチン社

RSA/Lockheed

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

標的: NY Times

January 2013 **New York Times** 

被害: 情報・企業パスワードの漏えい

October

Adobe 標的: Adobe 被害: 顧客情報とデータの漏えい

**Target** 

えい

標的: Target

2013

December

2013

被害: 顧客クレジットカード情報の漏

APT 攻撃の例

複数の攻撃手法の組合せ

常に複雑化、進化

スピアフィッシング +

カーネルルートキット

+ カスタム化 = APT



ゼロデイネットワークコード +

盗難、デジタル認証の詐欺行為 + OSの特権昇格 = APT

> 水のみ場攻撃 + データの暗号化+

知的財産(IP) = APT

効果のない対策

効果のない対策

スパム対策

従来の ル IPS

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)

有効 🏔 な対策 多層型防御、

コンカキュリティ

エミュレーション、

リアルタイムレピュテ·

リアルタイム 脅威の可視化 迅速な防御

WATCHGUARD APT BLOCKER

WatchGuard APT Blocker - WatchGuard XTM

www.WatchGuard.co.jp/APTBlocker © 2014 WatchGuard Technologies. All rights reserved.