Emotet でお困りのお客様必見！！ 国内でも感染報告多数あり！

SOPHOS
Cybersecurity evolved.

ランサムウェアの運び屋 “ Emotet ” の封じ込めに成功している

Intercept X Advanced

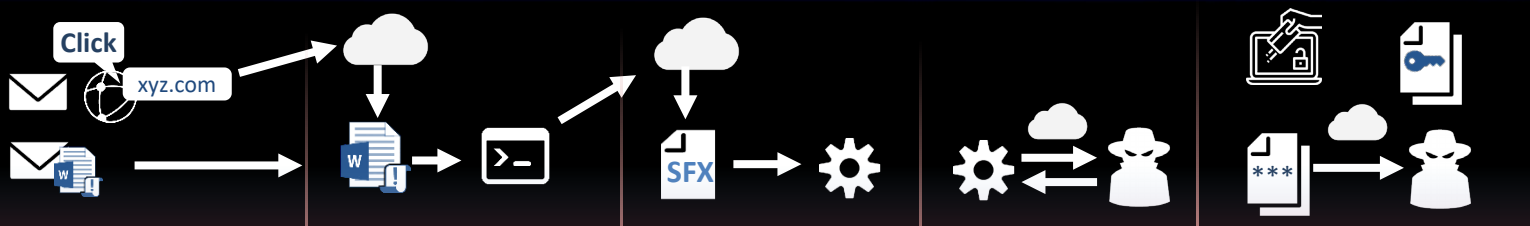
Intercept X

Go To
Intercept X

No 1 の評価を獲得した Intercept X

FORRESTER MRG Effitas SE Labs AV comparatives PC MAGAZINE CRN AV-TEST

Emotet の５つの攻撃チェーン毎に ブロック



配布	エクスプロイト	インストール	C&C 通信	脅威行動の実行
不正なURLや添付ファイル	PowerShell スクリプトの実行と接続	ペイロードやランサムウェアのダウンロードと実行	脅威命令やさらなるマルウェアの実行	情報の送信や暗号化、さらなるバックドアの設置
WEB プロテクション	エクスプロイト防止（コード/メモリ/APC ）	ディープラーニング	MTD(C2通信検知)	アンチランサムウエア
	アプリケーション制御	HIPS		認証情報窃取防止
	ローカル権限抑制			ランタイム HIPS
				根本原因解析 & EDR

瞬く間に増え続ける “亜種” も ディープラーニング で効率的にブロック

NEWS 作成者もお手上げ !?

Intercept Xの鉄壁の守りに
Emotet の作成者も
苛立ちを隠せない様子

ソースコード上で
Sophos を名指しで中傷か！？

```
push    offset aEudc    ; "EUDC"
mov     esi, ecx
mov     [esp+74h+var_10], edi
mov     [esp+74h+var_14], ebx
mov     word ptr [esp+74h+var_24], bx
call    sub_41F527
add     esp, 4
push    eax
push    offset aEudc    ; "EUDC"
lea     ecx, [esp+78h+var_28]
call    sub_40
push    offset aF※kSophos ; "F※k Sophos"
mov     [esp+74h+var_4], ebx
mov     [esp+74h+var_2C], edi
mov     [esp+74h+var_30], ebx
mov     word ptr [esp+74h+lpMem], bx
```

Emotet を防ぐ Intercept X の主な機能

1 高性能な AI 検出

- ✓ ディープラーニング (検体ビッグデータ35年分)
- ✓ 米国防高等研究計画局 (DARPA)のアルゴリズムを独自に進化させ搭載

2 業界最多を誇る エクスプロイト検出

- ✓ 25種類以上のエクスプロイトを検出
- ✓ EternalBlue にもいち早く対応

3 ランサムウェア検出 (復旧機能付き)

- ✓ 暗号化と同時に対象ファイルをバックアップ
- ✓ ランサムウェアと判断された時点で自動的に復元

Intercept X の 機能比較表

	Intercept X Advanced	Intercept X Advanced with EDR	備考
管理コンソール	Sophos Central	Sophos Central	クラウド管理プラットフォーム (サーバーの購入やメンテナンス不要)
従来のマルウェア保護機能	✓	✓	シグネチャーベース, HIPS, web 制御, 周辺デバイス制御, アプリ制御など
次世代型保護機能	✓	✓	AI ディープラーニング(シグネチャーレス)、エクスプロイト防止機能、アンチランサムウェア機能など
EDR 機能		✓	脅威ハンティング、ガイド付き調査機能、SophosLabs 脅威インテリジェンス、Live Discover, Live Responseなど

注意：一部の機能は Windows のみの提供となります。

Check Firewall / UTM / Email 保護製品と Intercept X との併用で保護！

最近では、手口が巧妙化され、日本語メールや取引先を送信元と偽装したり、悪意ある添付ファイルもパスワードで保護され、Firewall / UTM / Email 保護製品による検出を回避します。Intercept X と併用がお勧めです。

事例 お客様事例 をご覧ください！！

トーヨーカネツ株式会社様をはじめ多くのお客様を Intercept X が保護しています。

www.sophos.com/ja-jp/lp/jp-case-studies/

QRコードからアクセス

(販売店)
株式会社エイコー
TEL:0120-506-815
MAIL：eicoh-inside@eicoh.com

無償評価版 (30日間)へのお問い合わせは販売店までご連絡ください

ソフォス株式会社