2022年のEmotetの活動

キヤノンITソリューションズ株式会社
サイバーセキュリティラボ

ご紹介内容

- Emotetについて
- 2022年におけるEmotetの変化
- Emotetダウンローダー検出統計

Emotetについて

2014年頃にバンキングマルウェアの1つとして確認
2017年頃から様々なマルウェアをダウンロードし感染させる媒介機能を持ち
全世界で多くの被害が発生

Emotetがもたらす主な被害

- 情報漏えい
- ランサムウェアなど
  他のマルウェアへの感染
- 社内端末への感染拡大
- Emotet感染を狙った
  ばらまきメール送信の踏み台

JPCERT/CCによるEmotetに関する注意喚起

出典:JPCERT/CC マルウェアEmotetの感染再拡大に関する注意喚起
https://www.jpcert.or.jp/at/2022/at220006.html

Emotetについて　～３つの特徴～

モジュール型

・情報窃取

・スパムメールの送信

・他のマルウェアをダウンロードする　など様々な機能を持つ

頻繁な更新と機能拡張

・Emotet本体の更新

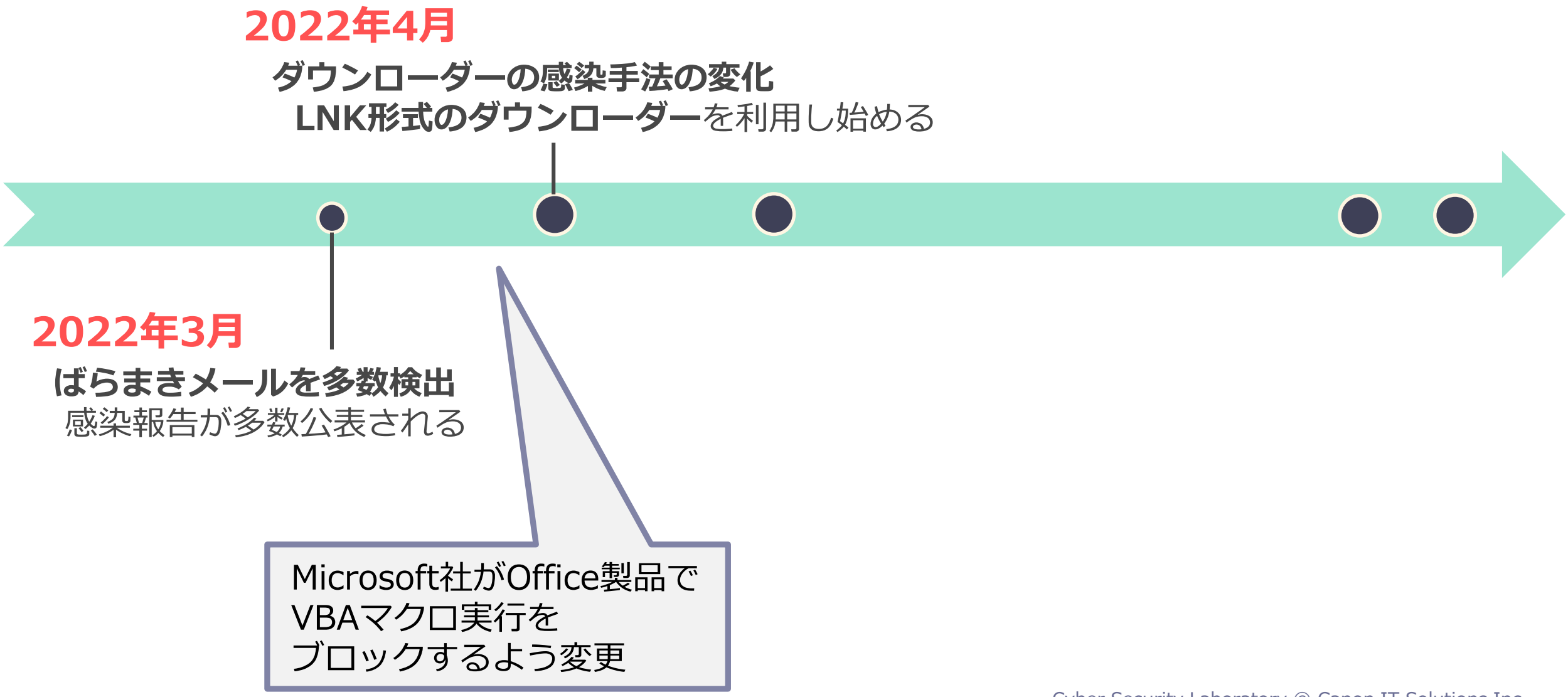
・モジュールの追加

感染拡大機能

・内部：SMBの悪用（脆弱性、パスワードリスト攻撃）

・外部：感染端末から盗んだ情報を流用したばらまきメール

2022年におけるEmotetの変化



ショートカットファイルの悪用（2022年4月25日～）

パターン①

メールに添付された**ショートカットファイル**を開く

パターン②

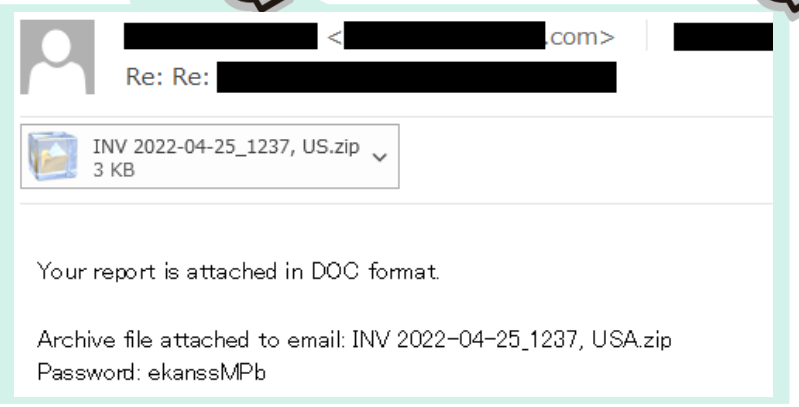
メールに添付された**暗号化Zipファイル**を展開し、
ショートカットファイルを開く

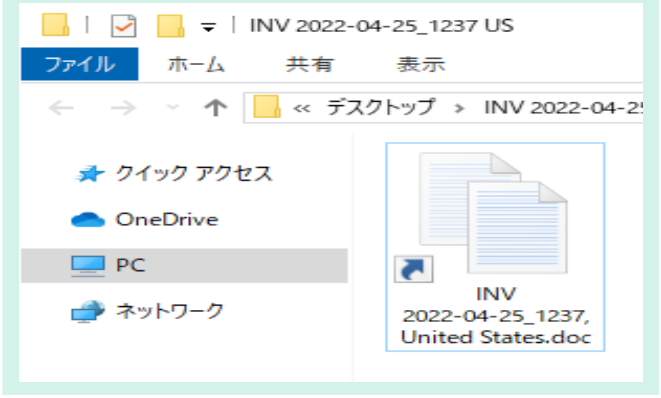
ユーザ操作

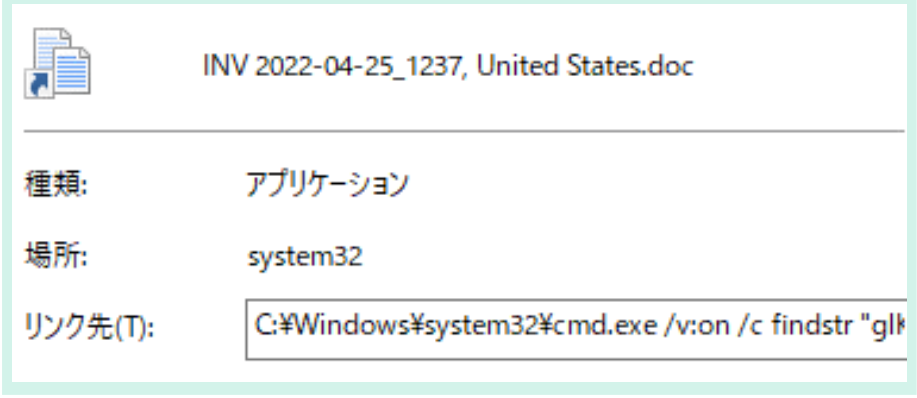
- PowerShell
- cmd & wscript

スクリプトが実行され、
Emotetがダウンロード・実行される

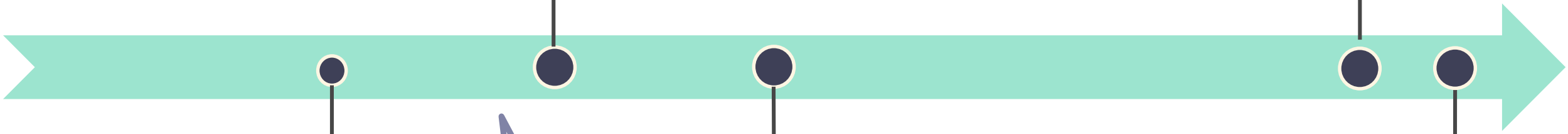
Emotetに感染







2022年におけるEmotetの変化



2022年3月

ばらまきメールを多数検出
感染報告が多数公表される

2022年4月

ダウンローダーの感染手法の変化
LNK形式のダウンローダーを利用し始める

Microsoft社がOffice製品で
VBAマクロ実行を
ブロックするよう変更

2022年6月

情報窃取モジュールの変化
Webブラウザ（Google Chrome）に保存された
クレジットカードの認証情報も窃取対象に

2022年10月

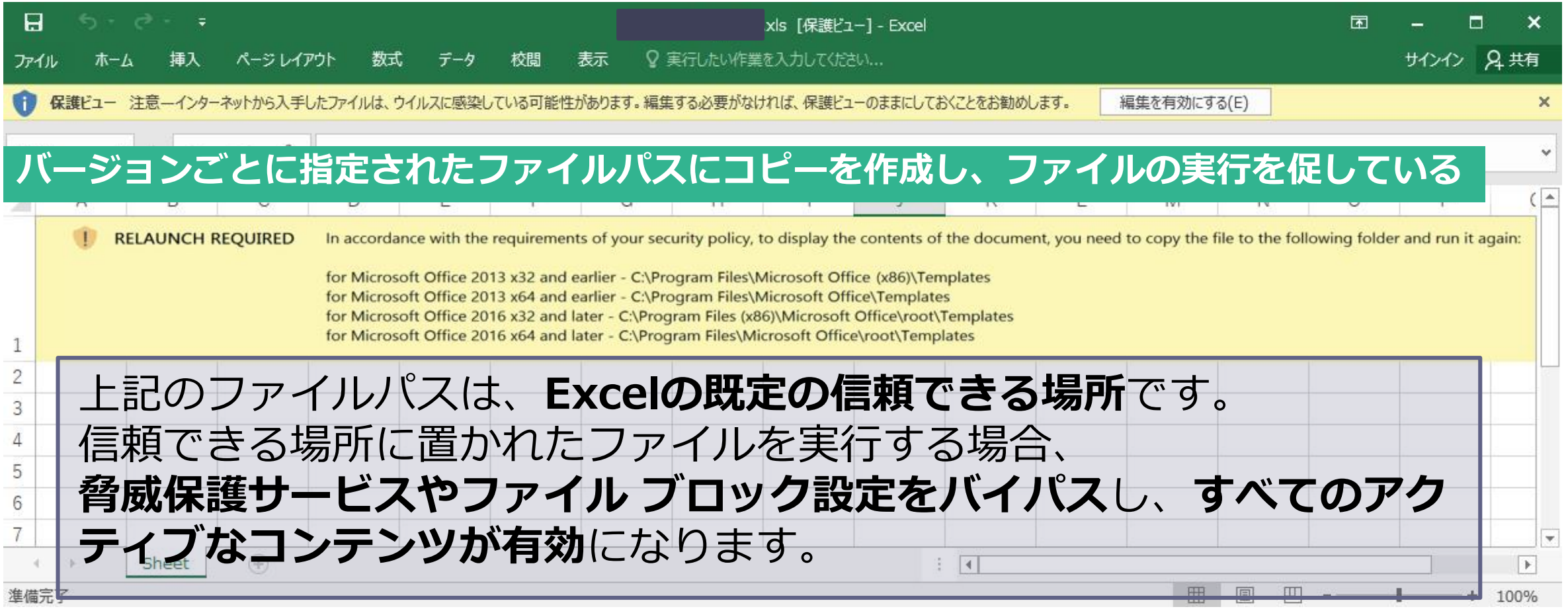
情報窃取モジュールの変化
窃取する**感染端末の設定情報**が変化

2022年11月

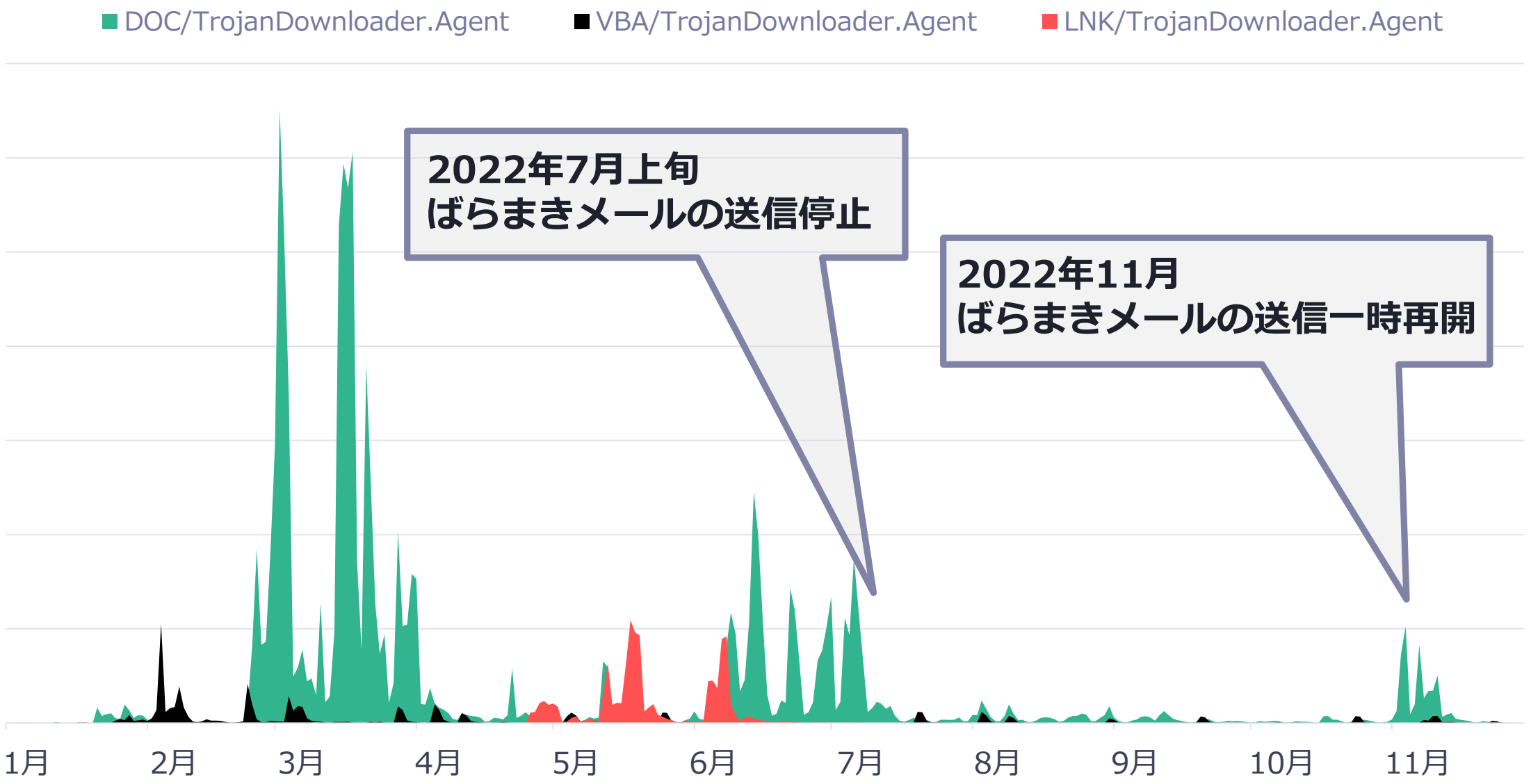
ダウンローダーのExcelファイルの変化
添付ファイルを開いた際の表示画面が変化

2022年11月のメール送信再開後のEmotet

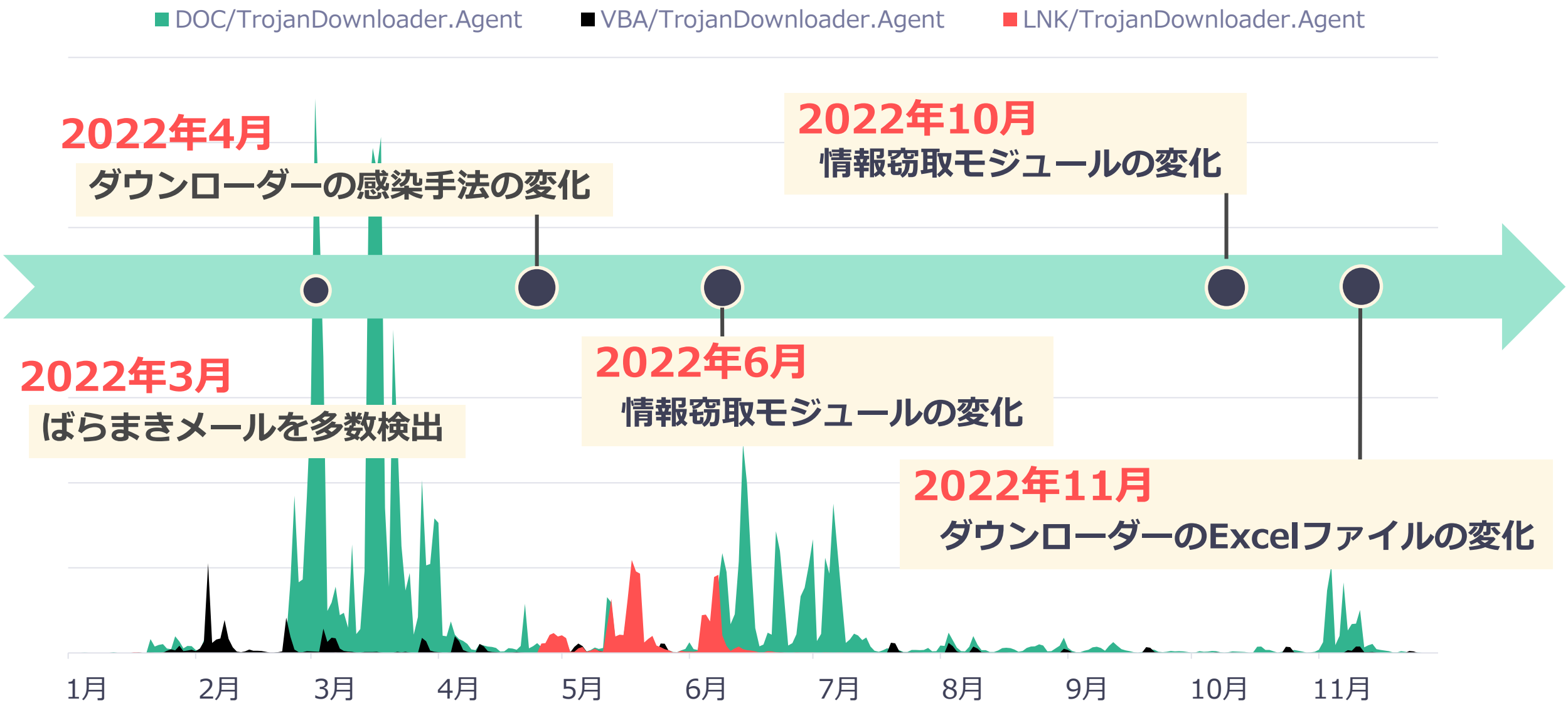
添付ファイルのExcelファイルが変化



Emotetダウンローダー検出統計（2022年1～11月・国内）



Emotetダウンローダー検出統計（2022年1～11月・国内）



まとめ

セキュリティ製品の正しい運用と監視

- ネットワークトラフィックログから不審な通信がないか監視
- 定義ファイルと製品バージョンを最新の状態に保つ
- 複数の層で守る

脆弱性への対応

- 組織内のソフトウェアやOSを把握し、情報収集する
- セキュリティパッチを迅速に適用する

ばらまきメールへの対応

- 添付ファイルやURLを不用意に開かない
- Office製品のマクロが無効化されていることを確認する
- スクリプトファイルの既定アプリケーションをテキストエディタに変更する

セキュリティ教育と情報共有

- ばらまきメールの特徴や手法変化について共有する
- ばらまきメールの送信開始・停止について共有する
- 感染した場合の作業手順を明確にする

サイバーセキュリティ情報局のご紹介

キヤノンマーケティングジャパンと ESETが提供する最新のセキュリティ情報

最新のセキュリティ動向やキーワード解説のほか
サイバーセキュリティラボがまとめた
日本におけるマルウェア動向を
詳細なレポートにて提供

情報収集にご活用ください

サイバーセキュリティ情報局　Search