世界各地で被害が広がる「WannaCry」について

トレンドマイクロ株式会社

話題になっている「WannaCry」とは？

- Server Message Block（SMB）脆弱性と4月に確認されたランサムウェアを組み合わせた攻撃
  - ハッカー集団「Shadow Brokers」が米国国家安全保障局（NSA）から窃取したツールに含まれるSMBv1の脆弱性「CVE-2017-0144」を利用
  - 今年4月に DropboxのURLを悪用した拡散が確認されたランサムウェア
- ネットワーク経由で侵入、拡散するワーム活動を持つ
  - ダウンロードしたファイルを「Microsoft Security Center (2.0)」というサービスとして実行。脆弱なSMBサーバを探索し攻撃。
- 感染端末ならびにネットワーク共有上のファイルを暗号化し、身代金300米ドルを要求
- トレンドマイクロでは、「Ransom_WCRY」、「Ransom_WANNA」として検出

WannaCryの攻撃の流れ

WannaCryが表示する脅迫文

ランサムウェア「WannaCry」の特徴

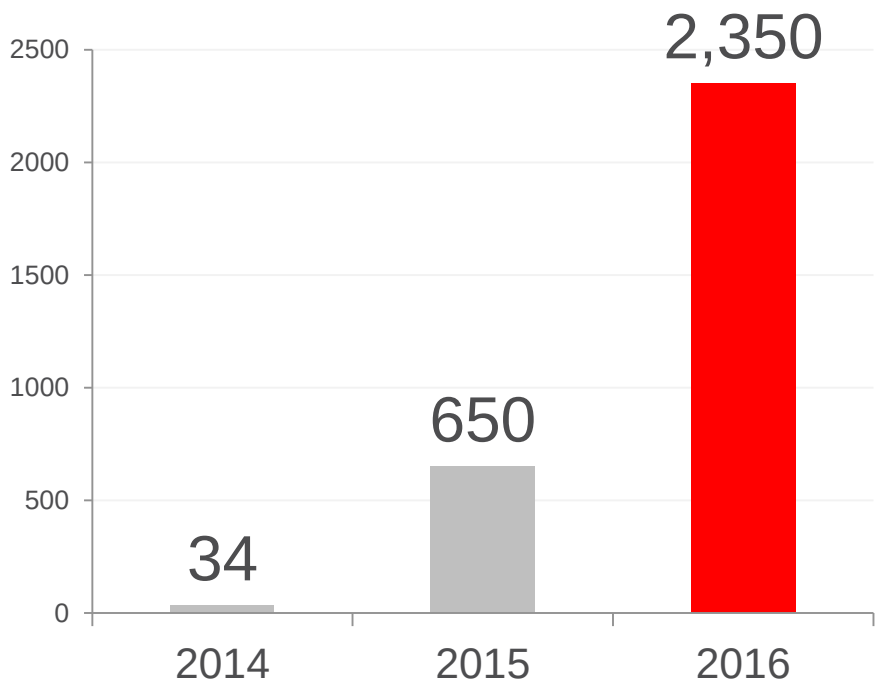
- **最新の脆弱性情報を悪用**：2017年3月に公開された、米国NSAから窃取されたとされる脆弱性
- **ワーム機能を搭載**：ダウンロードしたファイルを「Microsoft Security Center (2.0)」サービスとして実行し脆弱なシステムを探索
- **法人組織が標的に**：法人組織で使われるSMBの脆弱性を利用
- **レガシーシステムを標的に**：Windows XP、Windows Server 2003 といったサポート終了しているシステムにも影響
- **過去の攻撃を悪用**：4月確認のDropbox URLを悪用した攻撃を使用
- **多言語対応した脅迫文**：日本語を含めも 27 の言語に対応
- **業種特有環境での被害**：病院、工場、鉄道、など様々な業種で被害
- **さまざまなファイルを暗号化**：Officeファイル、データベース関連など166種類のファイルが標的に

世界各地で広がる「WannaCry」被害

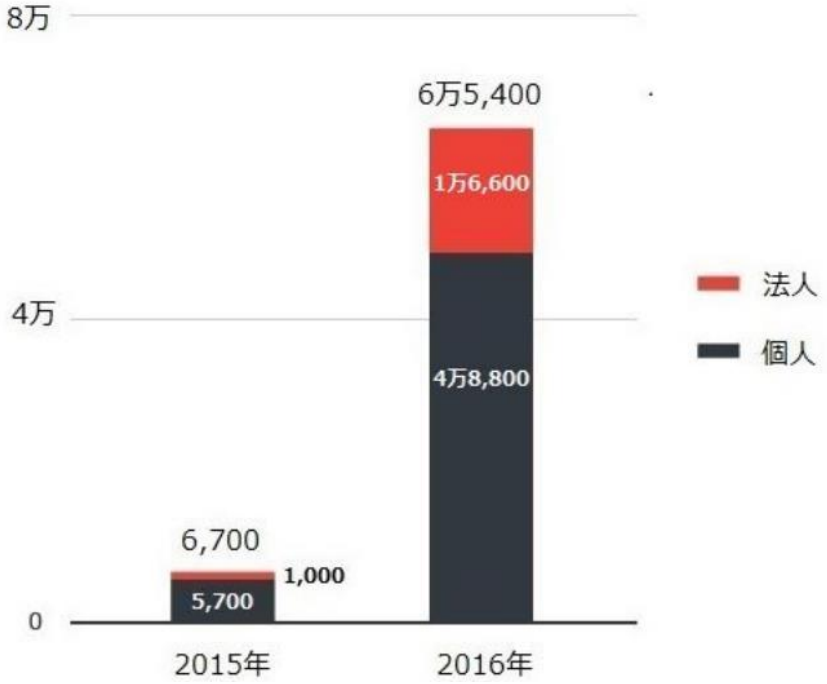
- 2017年5月13日早朝（日本時間）世界各地でランサムウェア「WannaCry」による感染被害報道
  - イギリス：NHS（医療機関、複数拠点で急患対応や手術不能に）、日産自動車（工場で被害）
  - ロシア：銀行、内務省（1000台）、保険・社会開発省、国営鉄道、携帯通信会社
  - スペイン：テレフォニカ（テレコム）、イベルドロラ（電力）、Gas Natural（ガス）
  - ドイツ：鉄道（電光掲示板などに脅迫文表示）
  - フランス：ルノー（複数の工場が操業停止）
  - ポルトガル：ポルトガルテレコム（テレコム）
  - アメリカ：FedEx
- Trend Micro Smart Protection Networkのデータでは、英国、台湾、チリ、、日本、米国、インドなどでWannaCryの検出を確認

ランサムウェア被害は国内で深刻に

トレンドマイクロ法人サポートセンターへの被害報告件数*



ランサムウェアの国内検出台数推移*



*2017年トレンドマイクロ調べ

トレンドマイクロ製品でのWannaCry対策

- 脆弱性への対応：速やかな更新プログラム適用、あるいは「Trend Micro Deep Security™」、「TippingPoint」、「Cloud Edge™」などのIPS機能で緩和策を
- ネットワーク内部の対策：「Deep Discovery™ Inspector」のようなネットワーク内部を可視化するソリューションで兆候の早期発見を
- スパムメールの排除：「InterScan Messaging Secuirty Virtual Appliance」や「Deep Discovery Inspector」などのスパムメールへの対策を強化
- エンドポイントの強化：
  - 「ウイルスバスター™ コーポレートエディション XG」の機械学習型検索で最新の脅威にも対応
  - 「ウイルスバスター™ コーポレートエディション」、「ウイルスバスター™ ビジネスセキュリティサービス」、「ウイルスバスター クラウド」などの挙動監視機能で不審なシステム変更を防御
  - ホワイトリスト型セキュリティ「Trend Micro Safe Lock™」で許可されていないアプリケーションの実行を防止

その他法人組織が取るべき対策

- 重要データの分類：WannaCry は感染端末上だけでなくネットワーク共有上のファイルも暗号化するため、重要度の高いデータへの対策を優先
- バックアップ：重要度の高いデータは、定期的にバックアップをとり、複数のコピーをそれぞれ別々の場所に保管
- ネットワークのセグメント化：繋ぐ必要のない環境間の接続をしないといった適切なネットワーク設計で拡散被害を抑制
- SMBを無効に：不要な場合にはSMB を無効に、あるいはSMBv1の利用をやめる

詳しい情報は

- トレンドマイクロセキュリティブログ
  - 週明け国内でも要注意 – 暗号化型ランサムウェア「WannaCry／Wcry」（http://blog.trendmicro.co.jp/archives/14884）
  - 大規模な暗号化型ランサムウェア「WannaCry／Wcry」の攻撃、世界各国で影響（http://blog.trendmicro.co.jp/archives/14873）

ありがとうございました

TREND MICRO