平成 29 年5月 19 日

Topic

ランサムウェア「WannaCry」に感染した PC からの感染活動とみられる 445/TCP ポート宛てアクセスの観測について

1 概要

平成 29 年5月 12 日以降、世界約 150 か国において政府機関、病院、銀行、企業、個人等のコンピュータが、ランサムウェア「WannaCry」に感染させられる事案が大規模に発生しています。警察庁では「WannaCry」の検体の解析を進めていますが、現在解析中の「WannaCry」の検体については、以下の動きを示しました。

○ 「WannaCry」に感染したPC（以下「感染PC」という。）に保存されている文書ファイル、映像ファイル等のデータの暗号化

○ 感染PCが接続されているネットワーク上で、他のPCへの感染活動
- ローカルネットワーク（LAN）の場合、同一LAN上の全てのPCが対象
- グローバルネットワーク（インターネット）の場合、ランダムなPCが対象
- 感染活動の際、宛先ポート 445/TCP に対して、特徴的なデータを含む不審な通信パケットを発信

これらの解析結果に基づき、インターネット定点観測システムにより、上述の特徴的なデータを含む通信パケットの動向について分析したところ、5月 12 日以降、現在に至るまで、感染PCが感染活動を継続している可能性が高いことが分かりました。（下図）

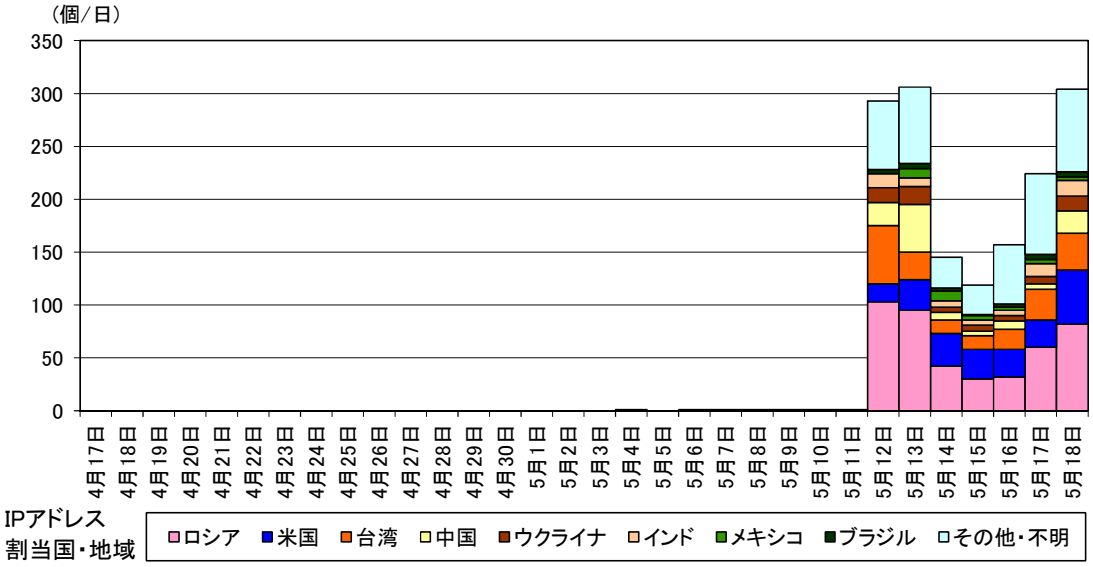


図 「WannaCry」に感染した PC からの感染活動とみられる不審な通信パケット（445/TCP ポート宛）の発信元 IP アドレス数の推移

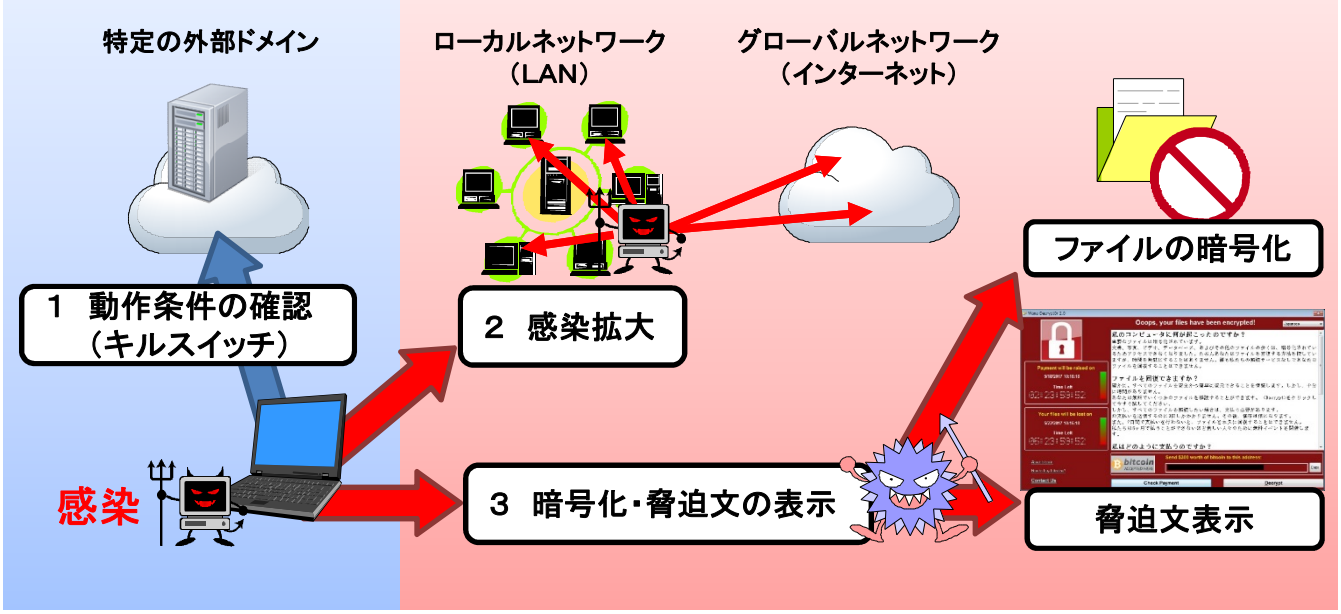
2 推奨する対策

- Microsoft 社が公開する MS17-010 等のパッチを適用して、利用している Microsoft Windows を最新の状態にしてください。
- MS17-010 が未適用の Microsoft Windows が稼動している PC 又はサーバ等を直接インターネットに接続していた場合には、既に感染している可能性があります。不審なプロセス、ファイル及び通信等が存在しないか確認してください。
- Microsoft Windows が稼動している PC をインターネットに接続する際は、直接接続するのではなく、ルータ等を使用して NAT を介して接続してください。自宅等ではルータを使用してインターネットに接続していても、モバイル回線を利用する場合には直接インターネットに接続される場合もあるので注意してください。
- Microsoft Windows が稼動しているサーバをインターネット上に公開している場合には、運用状況に応じて、可能であれば 445/TCP ポートに対するアクセスを遮断してください。

（参考）

ランサムウェア「WannaCry」の動作概要について

警察庁では、ランサムウェア「WannaCry」の検体の解析を進めています。
平成29年5月19日現在で判明している「WannaCry」の動作の概要については、下記のとおりです。



【感染後の動作の流れ】

1　動作条件の確認（キルスイッチ）

特定の外部ドメインへの接続が成功した場合は、ランサム動作を行いません。
※ただし、動作条件の確認（キルスイッチ）を行わない亜種も報道されています。
（URL:　http://japan.cnet.com/article/35101198/ ）

2　感染拡大

Windowsのぜい弱性を悪用するパケット（445/TCP）を送信し、他の端末へ感染拡大を試みます。
［送信先］
・ローカルネットワーク（LAN）　：　同一ネットワーク上のIPアドレス宛に送信
・グローバルネットワーク（インターネット）　：　ランダムなIPアドレス宛に送信

3　暗号化・脅迫文の表示

①　動作の準備［複数のファイルを作成（順不同）］
・暗号化を実行するプログラム
・秘匿通信用プログラム（Torモジュール）
・暗号化実施に必要な暗号鍵等
・脅迫文を記述した画像・テキストファイル
・支払先（Bitコインアドレス）を表示するプログラム

②　ファイルの暗号化
・特定の拡張子を持つファイルを暗号化します。
・暗号化されたファイルの拡張子は「.WNCRY」になります。
・Windowsの標準バックアップ機能で保存しているデータ（シャドーコピー）を削除します。

③　脅迫文の表示
・デスクトップの背景画像が脅迫文を記述した画像に差し替わります。
・支払先（Bitコインアドレス）が画面に表示されます。