Distributed via @police
http://www.npa.go.jp/cyberpolice/

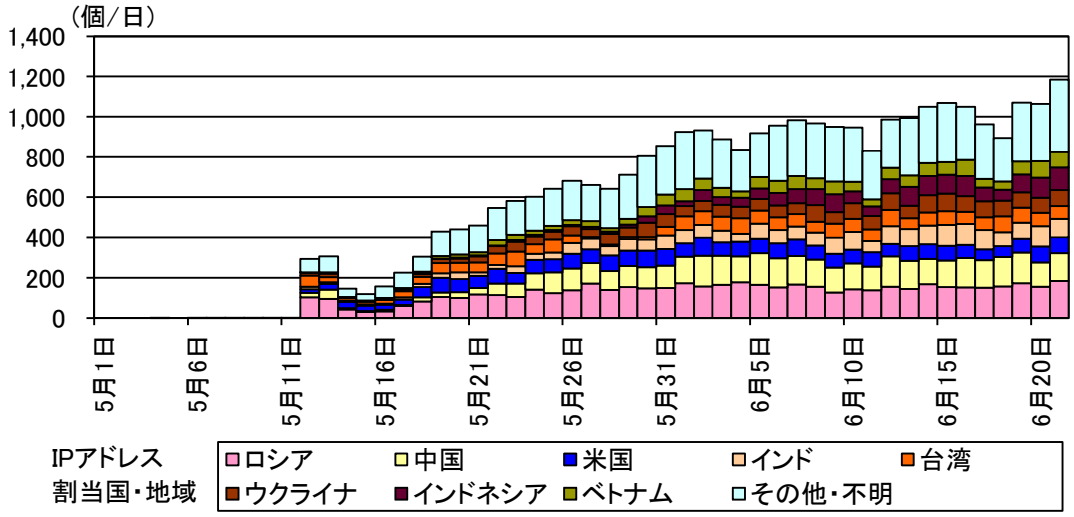
平成 29 年6月 22 日

Topic

ランサムウェア「WannaCry」の亜種に感染した 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」に感染する事案が大規模に発生しました。警察庁では、依然として「WannaCry」又はその亜種に感染した PC からの感染活動とみられる 445/TCP ポート宛てのアクセスを観測しております（図参照）。



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

「WannaCry」は、亜種を含む幾つかのキルスイッチドメイン[i]がセキュリティベンダ等によってシンクホール化[ii]されていることや、脅迫文が画面表示され利用者による感染被害の認知が容易で事後の対処も一定程度講じ得ることから、「WannaCry」のファイル暗号化などの動作や他への感染拡大については、ある程度抑制されていると考えられます。

しかしながら警察庁においては、下記の特徴を持ったランサムウェア「WannaCry」の亜種に感染した PC からの感染活動によるものとみられるアクセスの増加を観測しているところです。

---

[i]「WannaCry」は、特定の外部ドメイン（キルスイッチ）への接続を試み失敗した場合に限り、感染活動やファイル暗号化を行います。

[ii] セキュリティベンダ等は、存在しないキルスイッチドメインを取得し感染 PC がアクセス可能となる状態とし、感染活動やファイル暗号化を行わないよう対策を講じています。

- **特定のキルスイッチドメインへの接続を試みるが、その結果に依らず感染活動を行う**
- **ファイル暗号化を行うプログラム（tasksche.exe）が起動しない（ランサム機能が無効）**

警察庁では、当庁システムの 445/TCP ポートに対するアクセスが「WannaCry」の感染につながるものであることを確認しています。また、6 月初旬以降の感染の多数が「WannaCry」の亜種であることが判明しております。

当該亜種に感染した場合は、PC 内のファイルが暗号化されることはなく、いわゆるランサムウェアの典型的な被害に遭わないことから、その危険性を認識することは困難だと思われます。しかし、当該亜種は、感染後、利用者等に気付かれることなく感染活動を継続し、インターネット上やローカルネットワーク内に感染が拡大することになります。その結果、以下の事象が懸念されます。

- **感染 PC の増加及びこれらの感染活動に伴うトラフィック増大による、ネットワークの輻輳及びこれに伴うシステム障害**
- **感染 PC は脆弱性を有したままの状態であるため、他のマルウエアへの感染等**

2　推奨する対策

今後前述のような状況に陥ることを回避するため、下記の対策を講じるよう改めて注意喚起致します。

- 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。