モノづくりプリザーブ
Preservation for Industries in kyoto
モノプリ・ニュース！ 第20号

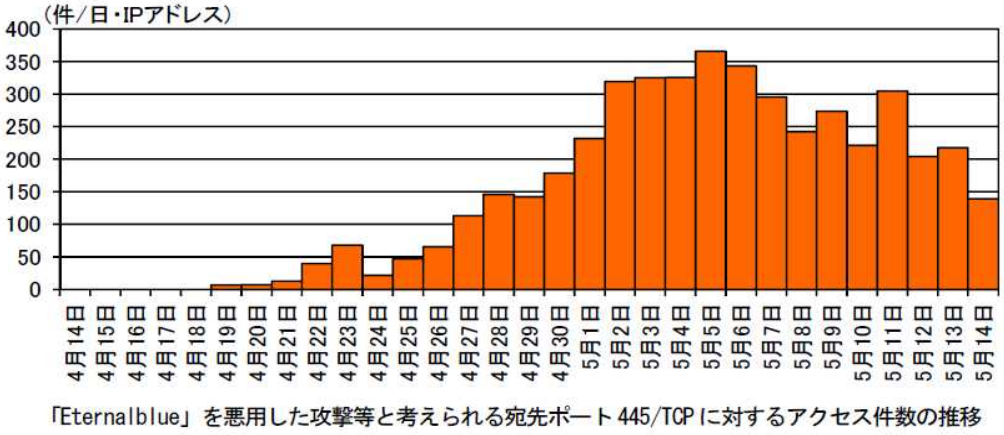
攻撃ツール「Eternalblue」を悪用した攻撃と考えられるアクセスの観測について

○ 主な観測結果

【概要】

４月14 日に「The Shadow Brokers」を名乗る集団が、インターネット上で複数の攻撃ツールを公開しました。同集団が公開したツール及び脆弱性情報には、Microsoft Windows の脆弱性MS17-010 を標的とする攻撃ツール「Eternalblue」及びMicrosoft Windows に感染するバックドア「Doublepulsar」等が含まれおり、これは、現在、世界的な被害を発生させているランサムウエア「WannaCry」等にも関連するものです。

警察庁では、「Eternalblue」を悪用した無差別な攻撃、又は、「Doublepulsar」に感染してバッグドアが作られたコンピュータの探索と考えられるアクセスを４月19 日以降継続して観測しています。



「Eternalblue」を悪用した攻撃等と考えられる宛先ポート 445/TCP に対するアクセス件数の推移

【分析】

「Doublepulsar」等のバックドアや「WannaCry」等のランサムウエアは、攻撃ツール「Eternalblue」と組み合わせることにより、ネットワーク経由で遠隔から感染させることが可能であることが判明しています。

また、同手順を具体的に解説した資料もインターネット上に公開されています。

以上のことから 「Eternalblue」を悪用して、さまざまな不正プログラムに感染させる攻撃活動が行われている可能性があります。

【対策】

Microsoft 社が公開するMS17-010 等のパッチを適用してMicrosoft Windows を最新の状態にするなど適切な対策を早急に実施してください。

※ リアルタイム検知ネットワークシステムについて

○ サイバーフォースセンターでは、インターネットとの接続点に設置したセンサーに対するアクセス情報等を集約・分析することで、ＤｏＳ攻撃の発生や不正プログラムに感染したコンピュータの動向等の把握を可能とする**リアルタイム検知ネットワークシステム**を24時間体制で運用しています。

参考：警察庁広報資料@Police（攻撃ツール「Eternalblue」）を悪用したと考えられるアクセスの観測について」
http://www.npa.go.jp/cyberpolice/important/2017/201705151.html

京都府警察本部モノづくりプリザーブ事務局 075-451-9111(内線 5821)