2017.5.15

メディカル IT セキュリティフォーラム

ランサムウエア "WannaCrypt" に関する Microsoft 製品の脆弱性対策について

(世界規模のサイバー攻撃に対する対応・対策について(緊急))

前略、既に報道等でご承知かと思いますが、5 月 12 日に世界 99 カ国において大規模なサイバー攻撃が発生し、英国では少なくとも 36 箇所の病院の PC が感染し、”診療業務ができない”等の実害が報告されています。
警察庁の情報では日本国内でも少なくとも 2 箇所の病院が感染したとのことで、今後感染が拡大する可能性があります。

今後の被害拡大を防止するために、現時点での情報と、対策をまとめましたのでご案内申し上げます。

今回の攻撃概要

１．感染するコンピュータウイルス：**ランサムウェア「WannaCrypt(または、WannaCry)」**

２．感染対象**のマシン：**MS17-010 で公開された更新プログラム未適用の Windows 7、Windows Server 2008、またはそれ以前の OS を対象に感染する。設計上、Windows 10 はこの攻撃の影響を受けない。(Microsoft)

３．**ランサムウェア「WannaCry」の挙動・特徴：**

- 166 種類の拡張子を対象に暗号化を行う。
- 暗号化したファイルには「.WNCRY」という文字列をファイル名末尾に追加する。
- 暗号化処理が完了すると、ボリュームシャドーコピー(元ファイルのコピー)の削除を行う。
- デスクトップの背景画像を暗号化したことを示すメッセージを含めたものに変更する。
- 身代金要求の詳細と期限を示すタイマーを表示する。

４．利用される脆弱性：CVE-2017-0145
LAN 上の Windows マシンおよびインターネット上をランダムに走査し感染を試行する。

５．**要求される身代金：**
要求される身代金の金額は 300 米ドル。600 米ドルも当初の攻撃では確認されていた。

(Kaspersky)

3 日以内に支払いがなければ要求金額は倍に、7 日以内に支払いがなければデータファイルは削除されると脅迫。

６．英国の病院での感染事例：NHS(**国民保健サービス)**

７．当該サービスを提供する 248 団体の内、48 団体で端末が使えなくなるなどの被害が発生した。

14 日午前 0 時時点で 6 団体がまだ復旧できていない。*12

内務省の調査によればその後影響を受けた病院の内、97%が通常業務に復旧した。

８．英国内相は攻撃は無作為であり、NHS が直接の標的として狙われたものではないとコメント。

９．感染したマルウェアが Ransomware「Wanna Decryptor」だと確信していると声明。

１０．　NHS より提供されていたシステムが一部地域で停止する事態となった。これにより次のような影響が生じた。

(ア) システムがロックアウトされ、患者のファイルなどを確認することが出来なくなった。手書きによる事務に切り替えた。

(イ) 複数の医療機関で診療が行えなかった。

(ウ) レントゲン撮影を行うことが出来なくなった。

(エ) 予定されていた心臓手術が中止となった。

(オ) 救急搬送された患者を受け入れられず救急車の行先変更が必要となった。

(カ) 急患以外は受診に来ないよう呼びかけが行われた。

英国では合計 62 の病院が影響を受けた。またスコットランド、ウェールズ等の病院には影響は及ばなかった模様。

以上 Piyolog より転載：http://d.hatena.ne.jp/Kango/

対策：

１．不用意にメール本文の URL をクリックしない

２．不用意にメールの添付ファイルを開かない

３．重要なファイルはバックアップを取って、ネットワークから切り離して保存する

４．直ちに Windows Update を行う

・Windows7 以降は正規の Microsoft のサポートページ→

https://www.microsoft.com/ja-jp/safety/pc-security/j_musteps.aspx

・既にサポート終了の OS については、こちらのページから→

Windows Server 2003 SP2 x64, Windows Server 2003 SP2 x86, Windows XP

SP2 x64, Windows XP SP3 x86, Windows XP Embedded SP3 x86, Windows 8 x86, Windows 8 x64

一部に WIdnowsXP 以外には感染しないとのデマが流布しているようですが、Windows10 以外は全て感染する可能性がありますので、ご注意ください。

草々