イギリスの医療機関等におけるランサムウェアによるサイバー攻撃への対応

＊WannaCrypt, WannaCry, WannaCryptor, Wcry

2017/5/15

アズビル セキュリティフライデー株式会社
営業部　内田秀和

概要

（Microsoft TechNet 2017/5/14発表より抜粋）

- 概要
  - 2017 年 5 月 12 日 (米国時間) より、マイクロソフトは、イギリスを始めとする複数の国の医療機関やその他の企業に影響を及ぼすランサムウェアによるサイバー攻撃を確認しています。このランサムウェアは Wanna Cryptor マルウェア (WannaCrypt, WannaCry, WannaCryptor, Wcry などと呼ばれる) の亜種であると思われます。日本でも攻撃報告を確認しており、マイクロソフトでは昼夜を徹して本件の影響を受けた全世界のお客様の支援を進めています。
- 対策
  - このマルウェアはメールなどのソーシャル エンジニアリング手法を使い拡散を狙います。また、CVE-2017-0145 を悪用し細工したパケットを SMB サーバーに送ることで拡散します。このランサムウェアは 2017 年 3 月に修正された **SMB v1 の脆弱性 (MS17-010) を利用する**ため、お使いのコンピューターが最新のセキュリティ更新プログラムをインストール済みであることを確認してください。
- **追加の保護策： SMBv1 の無効化**
  - 攻撃手法はさらに進化する可能性もあります。追加の多層防御対策が追加の保護を提供する場合もあります。また、MS17-010 の適用ができない環境においては、SMBv1の無効化が役立つ場合があります。

VISUACT-X 緊急対応

- VISUACT-X（パラメータファイル）のバージョンアップを行います
  - SMBv1（SMB1.0)が有効になっている端末の特定が可能になります
    - SMBv1を使用したアクセスを抽出し、“管理者レベルのアクセスログ”にログ出力できます
    - ログからSMBv1を使用している端末を特定し、SMBv1の無効化を施す運用が可能になります(＊)
  - 既存ユーザ様には修正パッチを提供いたします

＊管理者レベルのログ
ファイル名：vx_yyyymmdd.log
例）2017年5月15日の管理者ログ：vx_20170515.log

DateTime	Client	Server	Protocol	ComputerName	User Account	Operation
22/Dec/2015:19:50:48 +09:00	192.168.100.100:57594	192.168.100.201:445	SMB1/tcp	SATO-PC	Administrator	Logon Failure
22/Dec/2015:19:50:48 +09:00	192.168.100.100:57594	192.168.100.201:445	SMB1/tcp	SATO-PC	Administrator	Logon Failure
22/Dec/2015:19:51:36 +09:00	192.168.100.100:57614	192.168.100.200:445	SMB1/tcp	SATO-PC	bakabon	Resource Connect
22/Dec/2015:19:51:36 +09:00	192.168.100.100:57614	192.168.100.200:445	SMB1/tcp	SATO-PC	bakabon	Create File
22/Dec/2015:19:51:36	192.168.	192.168.			bakabon	Close
22/Dec/2015:19:51:36	192.168.	192.168.			bakabon	Create File
22/Dec/2015:19:51:36	192.168.	192.168.			bakabon	Write
22/Dec/2015:19:51:36	192.168.	192.168.			bakabon	Close
22/Dec/2015:19:51:36 +09:00	192.168.100.100:57614	192.168.100.200:445	SMB2/tcp	SATO-PC	bakabon	Create File
22/Dec/2015:19:51:36 +09:00	192.168.100.100:57614	192.168.100.200:445	SMB2/tcp	SATO-PC	bakabon	Close
22/Dec/2015:19:51:36 +09:00	192.168.100.100:57614	192.168.100.200:445	SMB2/tcp	SATO-PC	bakabon	Create File
22/Dec/2015:19:51:36 +09:00	192.168.100.100:57614	192.168.100.200:445	SMB2/tcp	SATO-PC	bakabon	Write

該当する端末

SMBv1が使用されている

VISUACT-X付属のViewerでSMB1のアクセスだけを抽出することも可能です

azbil

SMBv1 を無効にする方法

参考資料

- **Windows Vista 以降を実行しているお客様の場合**
  - マイクロソフト サポート技術情報 2696547 を参照してください。
- **Windows 8.1 あるいは Windows Server 2012 R2 以降を実行しているお客様向けの代替の方法**
  - クライアント オペレーティング システムで:
    - **[コントロール パネル]** を開き、**[プログラム]** をクリックし、次に **[Windows の機能の有効化または無効化]** をクリックします。
    - Windows の設定画面で **[SMB1.0/CIFS ファイル共有のサポート]** のチェックボックスを “オフ” にし、**[OK]** をクリックしてウィンドウを閉じます。
    - コンピューターを再起動します。
  - サーバー オペレーティング システムで:
    - **[サーバーマネージャー]** を開き、**[管理]** メニューをクリックし、**[役割と機能の削除]** を選択します。
    - 設定画面で **[SMB1.0/CIFS ファイル共有のサポート]** のチェックボックスを “オフ” にし、**[OK]** をクリックしてウィンドウを閉じます。
    - コンピューターを再起動します。

（Microsoft TechNet 2017/5/14発表より抜粋）

azbil