2017 年 5 月 16 日
株式会社セキュアソフト

注意喚起：ランサムウェア「Wanna Cryptor」が世界中で猛威

1．概要

5 月 12 日にイギリスの国民保健サービス（NHS: National Health Service)など世界的な規模でランサムウェア*1 による被害が報告されています。特にイギリスでは今回の攻撃により NHS の一部のサービスが停止に追い込まれ、複数の医療機関で診療ができなくなり、大きな被害が伝えられました。この重大インシデントを始めとして医療機関に限らず世界中で攻撃が観測され、被害が拡大しています。

今回のランサムウェア「Wanna Cryptor」（別名：WannaCrypt、WannaCry、WannaCryptor、Wcry）は、アメリカ国家安全保障局（NSA: National Security Agency）から流出したとされる「MS17-010」の脆弱性（CVE-2017-0144）を悪用するエクスプロイト*2 を利用していることが特徴です。結果として、PC やサーバ上のファイルを暗号化して開けなくしたうえで、約 300 ドルのビットコインの支払いを要求する脅迫文が表示されます。

各メディアによると、イギリス以外にもロシア、ウクライナ等各国での被害が多く報道されています。すでに日本国内での被害も確認されており、早急な対策が必要となります。

*1 ランサムウェア：
身代金（ランサム）要求型のマルウェアです。感染した PC のデータを暗号化する等して解除に身代金を要求します。

*2 エクスプロイト(exploit)：
コンピュータのソフトウェア、ハードウェア脆弱性を利用したスクリプトやプログラムを指します。

2．脆弱性情報詳細

（1）対象となる OS

- Windows 10 Version 1511 for 32-bit Systems
- Windows 10 Version 1511 for x64-based Systems
- Windows 10 Version 1607 for 32-bit Systems
- Windows 10 Version 1607 for x64-based Systems
- Windows 10 for 32-bit Systems
- Windows 10 for x64-based Systems
- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows 8.1 for 32-bit Systems
- Windows 8.1 for x64-based Systems

・Windows RT 8.1
・Windows Server 2008 R2 for Itanium-based Systems Service Pack 1
・Windows Server 2008 R2 for x64-based Systems Service Pack 1
・Windows Server 2008 for 32-bit Systems Service Pack 2
・Windows Server 2008 for Itanium-based Systems Service Pack 2
・Windows Server 2008 for x64-based Systems Service Pack 2
・Windows Server 2012
・Windows Server 2012 R2
・Windows Server 2016 for x64-based Systems
・Windows Vista Service Pack 2
・Windows Vista x64 Edition Service Pack 2

(2) 対象の脆弱性情報

SMBv1 遠隔コード実行の脆弱性として Microsoft から 2017 年 3 月 14 日にセキュリティパッチが配信されています。

「MS17-010」(CVE-2017-0144)
https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx

※下記のサポート外の OS についてもパッチが配信されています。
□Security Update for Windows XP SP2 for x64-based Systems (KB4012598)
https://www.microsoft.com/en-us/download/details.aspx?id=55250
□Security Update for Windows XP SP3 (KB4012598)
https://www.microsoft.com/en-us/download/details.aspx?id=55245
□Security Update for Windows Server 2003 (KB4012598)
https://www.microsoft.com/en-us/download/details.aspx?id=55248
□Security Update for Windows Server 2003 for x64-based Systems (KB4012598)
https://www.microsoft.com/en-us/download/details.aspx?id=55244
□Security Update for Windows XP SP3 for XPe (KB4012598)
https://www.microsoft.com/en-us/download/details.aspx?id=55247
□Security Update for Windows 8 (KB4012598)
https://www.microsoft.com/en-us/download/details.aspx?id=55246
□Security Update for Windows 8 for x64-based Systems (KB4012598)
https://www.microsoft.com/en-us/download/details.aspx?id=55249

3. 攻撃の状況とパッチアップデートが不可能な場合の対策

（１）攻撃状況

今回のランサムウェア感染ルートは大きく３つが観測されています。

①．メールを介したランサムウェア感染

②．SMBv1 脆弱性を悪用したランサムウェア感染

③．不正サイトを利用したランサムウェア感染

（２）Windows の最新アップデートが不可能な場合の対策（SMBv1 プロトコルの無効化）

システムがどうしてもアップデートできない場合、サービス影響度を検討した上で、以下のような対策があります。

①ネットワークファイアウォール及び Windows ファイアウォールで SMBv1 関連ポートをブロック(TCP/139、445)

②SMBv1 の無効化

■Windows 8.1 または Windows Server 2012 R2 以上の場合

・クライアント OS：

コントロールパネル ＞ プログラムと機能 ＞ Windows の機能の有効化または無効化

＞ SMB1.0/CIFS ファイル共有のサポート のチェック解除 ＞ System 再起動

・サーバ OS：

サーバ管理者 ＞ 管理 ＞ 役割及び機能 ＞ SMB1.0/CIFS ファイル共有のサポートのチェック解除

＞ 確認 ＞ System 再起動

■上記以外の場合

・ネットワーク環境 ＞ プロパティを選択

・「Microsoft ネットワーク用クライアント」と「Microsoft ネットワーク用ファイルとプリンター共有」項目をチェック解除

4. SecureSoft i-コンテナ / SecureSoft mamoret 活用によるランサムウェアの対策

SecureSoft i-コンテナは PC 上にインターネット接続専用環境と通常環境の分離を実現するソリューションです。

SecureSoft mamoret はセキュアブラウジングに特化したソリューションです。

i-コンテナ/ mamoret を活用して以下の構成を取ることで、ランサムウェアの被害を回避することが可能です。

【構成条件と攻撃からの対処ロジック】

１． **インターネットアクセス環境側でメール受信を Web ブラウザメール利用とする。**

悪質なランサムウェアが添付されたメールのファイルを開いたり、不正サイトからランサムウェアをダウンロードしてしまった場合においても、i-コンテナ/ mamoret により分離された環境だけが攻撃対象となり、被害が発生しません。

さらに、i-コンテナ/ mamoret の仮想ドライブ初期化機能により、ランサムウェア自体も削除されるため、安全が確保されます。

２．　**大事な業務データは通常業務環境側での利用・保管・管理とする。**

i-コンテナ/ mamoret の機能により、通常業務環境側のデータ領域と、i-コンテナ/ mamoret によるインターネット利用のデータ領域は分離されるため、万が一、ランサムウェアが i-コンテナ/ mamoret 内に侵入しても大事な通常業務環境のデータを暗号化することができません。

【図】i-コンテナ環境に侵入したランサムウェアの分離イメージ（mamoret も同様）

SecureSoft コンテナ シリーズについての詳しい内容は、下記 URL をご参照ください。
https://www.securesoft.co.jp/products/#container

5. SecureSoft Sniper シリーズによる SMBv1 脆弱性対策

ネットワークセキュリティ対策製品「SecureSoft Sniper シリーズ」では今回の脆弱性に対しては下記シグネチャでの

不正通信の検知、遮断が可能です。

[3477] MS Windows SMB SrvOs2FeaToNt RCE

さらに、本日付で以下のシグネチャを緊急リリースいたします。

[3484] MS Windows SMB Doublepulsar Kernel Dll Injection

SecureSoft Sniper シリーズについての詳しい内容は、下記 URL をご参照ください。
https://www.securesoft.co.jp/products/#sniper

セキュアソフトでは SecureSoft Sniper シリーズ、SecureSoft コンテナシリーズを利用して様々な脅威から
お客様の安心・安全に寄与してまいります。

≪お問合せ先≫
株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp