公開レポート

NTT DATA
Global IT Innovator

【緊急レポート】
ランサムウエア「BadRabbit」の大規模感染について v1.1

株式会社NTTデータ　セキュリティ技術部　情報セキュリティ推進室
NTTDATA-CERT

2017年11月2日

目次

2017年10月24日、ロシア、ウクライナ等の複数国でランサムウエア大規模感染が報告された。

1. 被害状況（10/25時点）（*1-1～*1-3）

ロシア：インタファクス通信など報道機関2社で不具合が発生。
ウクライナ：首都キエフの地下鉄や、オデッサ国際空港で不具合が発生。数便に遅れ。
その他、ブルガリア、トルコ、日本、ドイツ、米国等で被害を受けた可能性。

2. 攻撃情報（*1-3、*2-1～*2-5）

ランサムウエア：BadRabbit（一部Petya亜種のコードを流用）
攻撃手法：ネットワーク経由で感染を広げる。端末上のファイルを使用不能にし、復旧と引き換えに300ドル相当のビットコインの支払いを要求する。(Petya亜種と類似)
最初の攻撃は協定世界時で24日8時頃に検知され、ファイルの配布元サイトが停止する同日15時まで続いた。
初期感染には、有名サイトを侵害しFlash Playerのアップデートを装ったマルウエアをダウンロードさせる。感染拡大には、予め保有するパスワードリストとのマッチング、パスワード抽出ツールMimikatzの使用や脆弱性を悪用した方法が報告されている。
（感染経路等の詳細は「4.本攻撃の全体像と攻撃手法」を参照）

3. 推奨される対策（*2-2、*2-3、*3-1）

- 既知の悪性ドメイン、悪性IPアドレスをフィルタリングする。
- ブラウザの設定でポップアップをブロックする。
- 定期的にバックアップを取得する。
- ウイルス対策ソフトの定義ファイルを更新する。
- Windowsセキュリティパッチの最新化(MS17-010は必須)
  - ✓ 困難な場合はSMBv1を無効化
- 読み取り専用ファイル「C:¥windows¥infpub.dat」を作成する。万が一感染しても、ファイルが暗号化されることを防ぐ。(BadRabbitのキルスイッチになる)
- 以下の名前のプロセスを「タスクスケジュール」に登録させないよう制約する。
  - ✓ viserion_
  - ✓ rhaegal
  - ✓ drogon

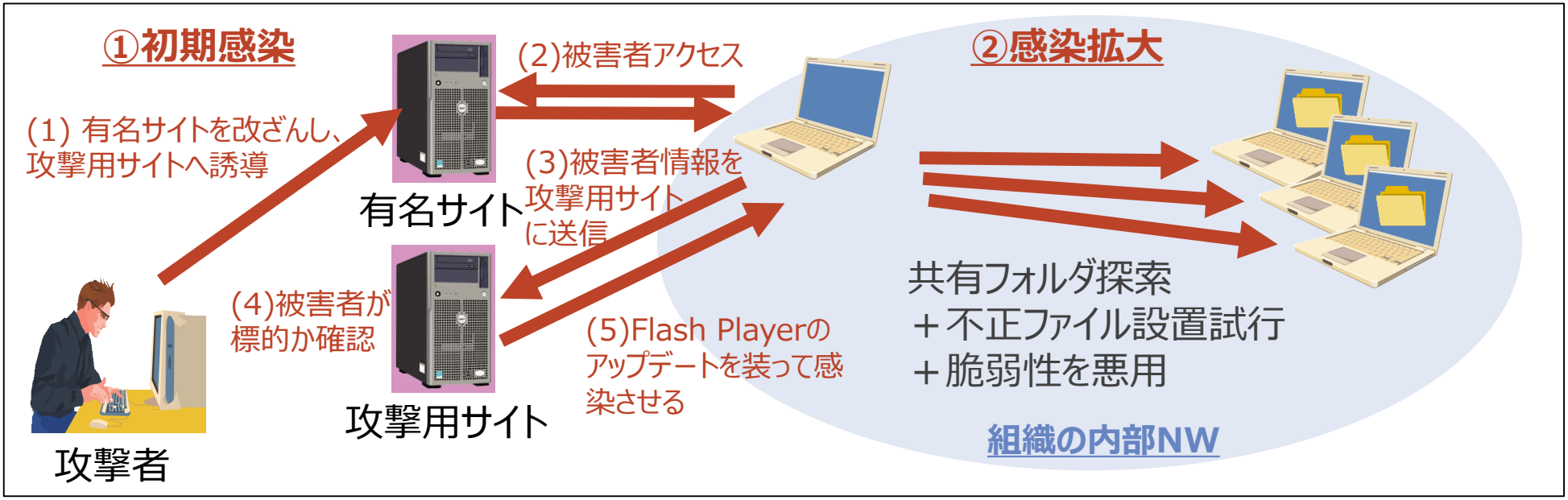
また、万が一感染が確認された場合は、初期対応として下記を迅速に行う。

- 感染が確認されたコンピュータをネットワークから外す。

なお、11/1時点で復号ツールの存在は確認できず。

4. 本攻撃の全体像と攻撃手法

感染経路については、セキュリティベンダ等から調査報告が公開されている。複数組織の調査報告から読み取れる内容をまとめ、下図に示す（*2-1~*2-3、*2-5）。



①初期感染は、水飲み場攻撃※を契機とし、Flash Playerのアップデートを装ってインストールボタンを押下させる。

②感染拡大は、内部ネットワークに対して以下の3つを試みる。

(a) 共有フォルダのスキャン

(b) 予め保有するパスワードリストと、「Mimikatz」を使って取得した認証情報を用いて認証を試行。
書き込みアクセスを行える共有フォルダを発見した場合、当該フォルダへ不正ファイルを設置し、
WMI(Windows Management Instrumentation)等の正規の管理ツールを用いてファイルを実行する。

(c) MS17-010未適用の端末に対し、SMBv1実装の脆弱性を悪用するツールを実行する。

※攻撃対象ユーザが普段アクセスするWebサイトを改ざんし、改ざんサイトへアクセスしたユーザをマルウエア等に感染させる攻撃

5. WannaCry、Petya亜種との比較

~~BadRabbitは、WannaCry、Petya亜種と異なり、感染に脆弱性を使用しない。~~WannaCry、Petya亜種と共通する点として、BadRabbitは感染拡大にSMBv1実装上の脆弱性を利用する（*2-1、*2-2、*2-5）。
異なる点としては、初期感染経路が水飲み場攻撃であり、また、感染拡大では、自身でもパスワードリストを持ち、拡散を試みる点が挙げられる。

	WannaCry	Petya亜種	BadRabbit（*2-1、*2-2、*2-5）
初期感染経路	インターネットからWindowsのSMBv1実装の脆弱性を突いて	会計ソフトMeDocの更新機能を侵害？ 水飲み場攻撃？メール経由？	水飲み場攻撃で、Flash Playerのアップデートを装って
感染拡大方法	対象：ローカルネットワーク内の端末に加えてグローバルの無作為なIPへ ・SMBv1実装の脆弱性	対象：ローカルネットワークのみ ・Mimikatzを改造したツールで取得した認証情報を用いて、PsExecとWMICを利用して拡散 ・SMBv1実装の脆弱性	対象：ローカルネットワークのみ ・自身が持つユーザ名とパスワードのリストとMimikatzで取得した認証情報を用いて、WMI等を利用して拡散 ・SMBv1実装の脆弱性
要求内容	300ドル相当のビットコインの支払い要求	300ドル相当のビットコインの支払い要求	300ドル相当のビットコインの支払い要求
被害地域	150か国以上	主としてウクライナ、その他ロシアや英国等65か国	主としてロシアやウクライナ、その他ブルガリア、トルコ、日本、ドイツ、米国等
被害額	約10万ドル(5/22時点)	約1万ドル(7/3時点)	不明。支払先のビットコインウォレットは個別に指定される（*5-1）。
キルスイッチ	特定URLへのアクセスに成功すると処理を終了	特定のファイルが存在すると処理を終了	特定のファイルが存在すると処理を終了（*2-3、*5-2）

6. 調査を経ての不明点

■ 初期感染経路

- ESETの報告では、ある特定の企業に対しては、攻撃者が当該企業ネットワーク内に足掛かりを持っており、囮として水飲み場攻撃を実行すると同時に、水飲み場攻撃以外の手段で、当該企業ネットワーク内に感染拡大させた可能性があると指摘している（*2-1）。

■ 攻撃の目的

- WannaCryやPetya亜種の大規模感染で、金銭目的では成功しているとは言えない状況にも関わらず、再度ランサムウエア大規模感染を仕掛けた目的は何か？
- 侵害されたサイト（*2-1）は、ほとんどニュースサイトだが、日本では建材メーカーのアイカ工業のサイトが被害を受けている（*6-1）。どのようなユーザーをBadRabbitの標的にしていたのか不明である。

7. 日本での報道状況※(11/1 12:00時点)

※ あくまでNTTDATA-CERTで確認できた範囲での主な状況

- 10/25　新聞社：ロイター通信が報じた内容を元に報道(日経、産経、毎日等)
  テレビ局：ロイター通信が報じた内容を元に報道(TBS)
  インターネットメディア：海外セキュリティベンダの報告を元に報道。また、JPCERT/CCの注意喚起について報道
- 10/26　新聞社：アイカ工業のWebページ改ざんについて報道
- 10/27　テレビ局：海外セキュリティベンダへの取材内容を報道(NHK)

参考情報

(*1-1) 日本経済新聞「ウクライナ、地下鉄や空港にサイバー攻撃」https://www.nikkei.com/article/DGXMZO22668070251020 17FF2000/
(*1-2) REUTERS「ロシアなどに新たなサイバー攻撃、日本でも被害」https://jp.reuters.com/article/russia-cyber-attack-idJPKBN1CU032
(*1-3) 産経ニュース「ロシアや欧州、日本で大規模なサイバー攻撃が発生」http://www.sankei.com/world/news/171025/wor1710250021-n1.html
(*2-1) welivesecurity “Bad Rabbit: Not-Petya is back with improved ransomware” https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back/
(*2-2) TrendLabs Security Intelligence Blog “Bad Rabbit Ransomware Spreads via Network, Hits Ukraine and Russia” http://blog.trendmicro.com/trendlabs-security-intelligence/bad-rabbit-ransomware-spreads-via-network-hits-ukraine-russia/
(*2-3) GROUP iB “BadRabbit There is a connection between Bad Rabbit and Not Petya” https://www.group-ib.com/blog/badrabbit
(*2-4) Security NEXT「国内でも「Bad Rabbit」を観測 - 2月には誘導スクリプトが稼働か」http://www.security-next.com/086930
(*2-5) Talos “Threat Spotlight: Follow the Bad Rabbit” http://blog.talosintelligence.com/2017/10/bad-rabbit.html
(*3-1) IPA「感染が拡大中のランサムウェア「Bad Rabbit」の対策について」https://www.ipa.go.jp/security/ciadr/vul/20171026-ransomware.html
(*5-1) Malwarebytes LABS “BadRabbit: a closer look at the new version of Petya/NotPetya” https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/
(*5-2) MBSD Blog「ランサムウェア「Bad Rabbit」の内部構造を紐解く」https://www.mbsd.jp/blog/20171027.html
(*6-1) 日本経済新聞「アイカ工業がサイト停止　不正改ざんの疑い」https://www.nikkei.com/article/DGXMZO22725040261020 17CN0000/

変更履歴

• 2017/10/27	v1.0	新規作成
• 2017/11/1	v1.1	「２．攻撃情報」を更新 「３．推奨される対策」を更新 「４．本攻撃の全体像と攻撃手法」を更新 「５．WannaCry、Petya亜種との比較」を更新 「７．日本での報道状況」を更新

NTT DATA

Global IT Innovator