NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2017年12月版 (第23号) ＞(選り抜き版)

2017年12月25日
ＮＴＴデータ先端技術株式会社
セキュリティ事業部

今回のサマリー

ランサムウェア「Bad Rabbit」について
2017年10月24日に、Bad Rabbit と呼ばれるランサムウェアによる感染被害が確認されました。このマルウェアの特徴を踏まえた上で、ユーザーや企業が取るべき対策を解説します。

ランサムウェア「Bad Rabbit」について

1. 「Bad Rabbit」の特徴 (1/6)

2017年10月24日に、Bad Rabbitと呼ばれるランサムウェアによる感染被害がロシアやウクライナなどの地域を中心に観測されました。

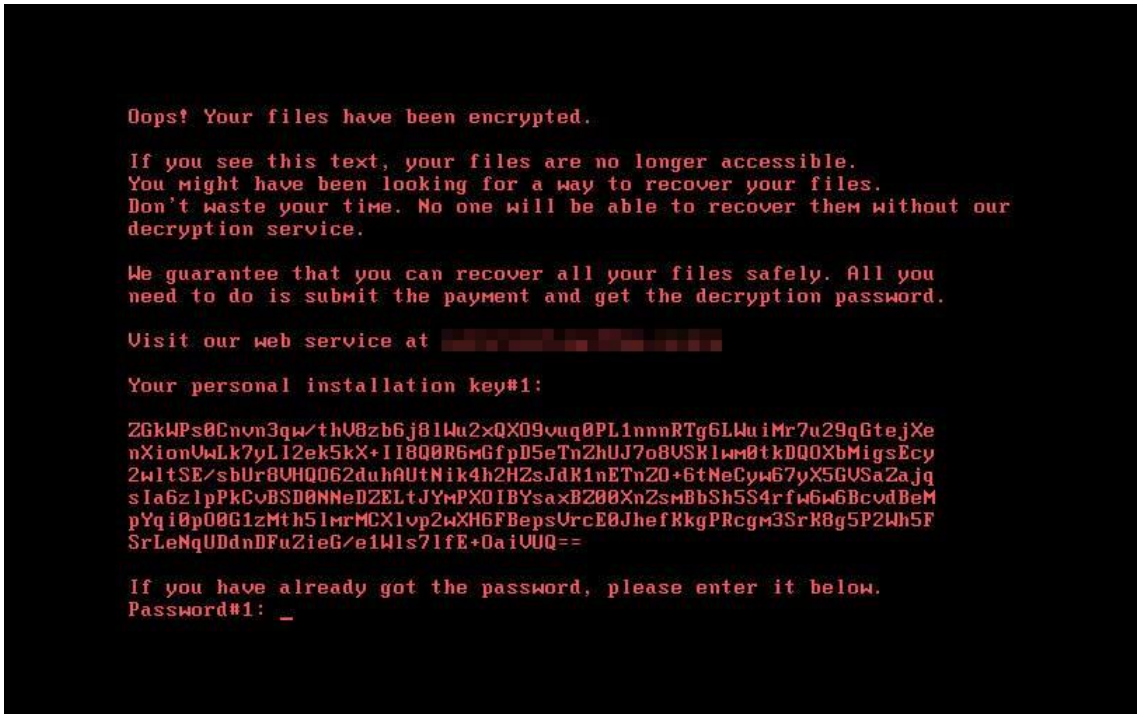
Bad Rabbitによる感染被害の例

組織名	国名	概要
インタファクス通信	ロシア	ウェブサイトによる一部のサービスが停止した。
オデッサ国際空港	ウクライナ	職員が旅客データを手入力する事態に陥った。これにより、同空港を利用するフライト数便に遅れが生じた。
アイカ工業	日本	同社のウェブサイトの閲覧者をBad Rabbitの配布サイトへ誘導するスクリプトが埋め込まれ、「踏み台」として悪用された。これに対する調査と対策のため、同社サイトは約1ヶ月間停止を強いられた。

1. 「Bad Rabbit」の特徴 (2/6)

Bad Rabbitに感染すると、従来のランサムウェアに感染した場合と同様に、ハードディスクの内容が暗号化され身代金要求画面が表示されます。

Bad Rabbit感染時に表示される身代金要求画面



参照元: http://blog.trendmicro.co.jp/archives/16226

1. 「Bad Rabbit」の特徴 (3/6)

Bad Rabbitの特徴として以下が挙げられます。

- 標的となる端末の利用者にAdobe Flash Playerの偽インストーラを実行させることで、標的となる端末が脆弱ではなくても初期感染する可能性がある。
- 認証情報を抽出する「Mimikatz」やディスクを暗号化する「DiskCryptor (Decrypt.sys)」といった正規の目的で作られているオープンソースのユーティリティツールを利用することで、ウイルス対策製品によるランサムウェアの挙動検知を困難にしている。
- 感染拡大時にマルウェアにハードコードされているユーザ名とパスワードのリスト(次ページ)を使う。

1. 「Bad Rabbit」の特徴 (4/6)

マルウェアにハードコードされているユーザ名のリスト

Admin	Administrator	alex	asus	backup	boss	buh	ftp
ftpadmin	ftpuser	Guest	manager	nas	nasadmin	nasuser	netguest
operator	other user	rdp	rdpadmin	rdpuser	root	superuser	support
Test	User	User1	user-1	work			

マルウェアにハードコードされているパスワードのリスト

111111	123	123321	1234	12345	123456	1234567	12345678
123456789	1234567890	321	55555	777	77777	Admin	Admin123
admin123Test123	Administrator	administrator	Administrator123	administrator123	adminTest	god	Guest
guest	Guest123	guest123	love	password	qwe	qwe123	qwe321
qwer	qwert	qwerty	qwerty123	root	secret	sex	test
test123	uiop	User	user	User132	user123	zxc	zxc123
zxc321	zxcv						

1. 「Bad Rabbit」の特徴 (5/6)

Bad Rabbitと従来のランサムウェアとの比較

	WannaCry	Petya亜種	Bad Rabbit
観測時期	2017年5月	2017年6月	2017年10月
初期感染方法	• MS17-010で修正されたSMBv1(※1)の脆弱性を利用	• 会計ソフトMeDocの更新機能の脆弱性を利用 • メールによる感染	• ユーザがAdobe Flash Playerの偽インストーラを実行
感染拡大範囲	• MS17-010で修正されたSMBv1(※1)の脆弱性を利用	• MimikatzやLSADumpの改変版で抜き出した認証情報でPsExec(※2)とWMIC(※3)を利用 • MS17-010で修正されたSMBv1(※1)との脆弱性を利用	• マルウェアにハードコードされたユーザ名とパスワードのリストとMimikatzで抜き出した認証情報でWMIC(※3)を利用 • MS17-010で修正されたSMBv1(※1)の脆弱性を利用
感染拡大範囲	インターネット	ローカルネットワーク	ローカルネットワーク
キルスイッチ(※4)が作動する条件	www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]comへのアクセスに成功すると停止	C:¥Windows¥perfcが存在すると停止	C:¥Windows¥cscc.datが存在すると停止
複号鍵の有無	有	無	有

1. 「Bad Rabbit」の特徴 (6/6)

用語の説明

1. **SMB (Server Message)**
   SMBはLAN上の複数のWindowsコンピュータの間でファイルやプリンタの共有などを行うためのプロトコルおよび通信サービスです。

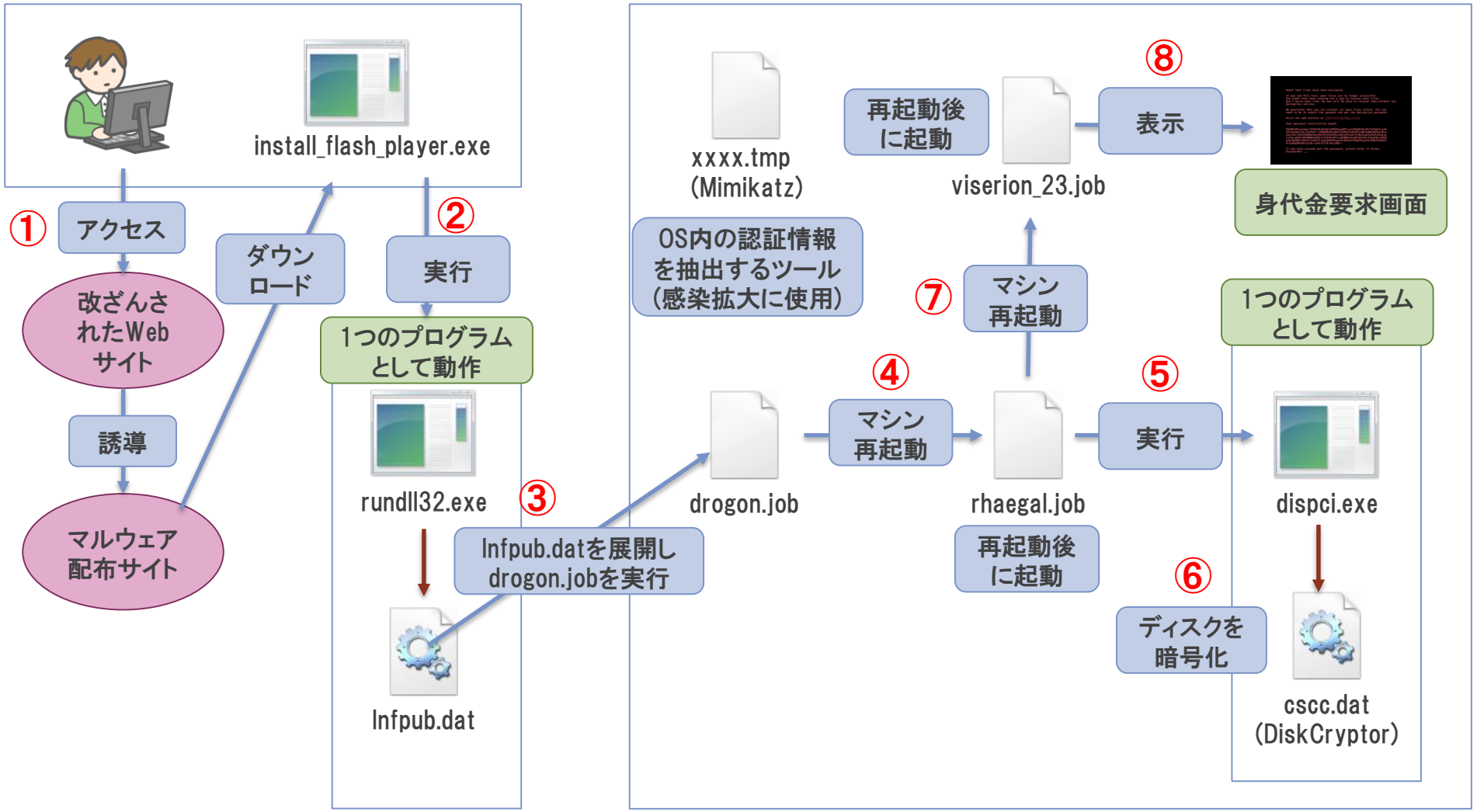
2. **PsExec**
   PsExecはWindowsでプロセスをリモートから実行するためのユーティリティです。PsExecはシステムの管理に役立つコマンドライン・ツールを集めたPsToolsとしてMicrosoft社より配布されています。

3. **WMI (Windows Management Instrumentation)**
   WMIC (WMI Command-line)
   WMIはWindowsの機能の一つで、OSやコンピュータに関する様々な情報を取得したり設定することができるインターフェースです。 WMICはコマンドラインからWMIを利用するためのユーティリティです。

4. **キルスイッチ (killswitch)**
   キルスイッチは緊急停止装置を意味します。キルスイッチの実装を持つランサムウェアは暗号化処理を行う前に特定の条件を満たしているかどうかをチェックし、条件を満たしている場合は暗号化や感染拡大を行わず活動を停止します。

2. 「Bad Rabbit」の動作フロー (1/2)

Bad Rabbitの動作フローを以下に示します。



2. 「Bad Rabbit」の動作フロー (2/2)

① ユーザが改ざんされたWebサイトにアクセスすると、マルウェア配布サイトに誘導され、Adobe Flash Playerのインストーラに見せかけたマルウェア install_flash_player.exeをダウンロードさせられる。
② ユーザがinstall_flash_player.exeを実行すると、マルウェアの本体である infpub.datが生成され実行される。
③ マルウェアはinfpub.datを展開し、ジョブdrogon.jobを実行する。
④ drogon.jobはマシンを再起動させる。
⑤ マシンが再起動するとジョブrhaegal.jobが実行され、 rhaegal.jobの中で dispci.exeが実行される。
⑥ dispci.exeは正規の暗号化ツールであるDiskCryptor (cscc.dat)を利用してディスクの内容を暗号化する。
⑦ rhaegal.jobはversion_23.jobを生成し、その後マシンを再起動させる。
⑧ マシンが再起動するとジョブversion_23.jobが実行され、身代金要求画面が表示される。

また、マルウェアは自身にハードコードされたユーザ名とパスワードのリストやMimikatzを利用して抜き出した認証情報でWNIを利用したり、MS17-010で修正されたSMBv1の脆弱性を利用したりすることで感染拡大を試みます。

3. 「Bad Rabbit」対策

これまでで紹介してきた特徴より、Bad Rabbitに対しては以下のような対策が有効です。

- **正規ではないサイトからダウンロードしたインストーラ等のプログラムを実行しない**
  Bad Rabbitはマルウェア配布サイトからダウンロードされたAdobe Flash Playerの偽インストーラinstall_flash_player.exeを実行することによって感染します。したがって、不審なインストーラ等のプログラムを実行しないことで、初期感染を防ぐことができます。
- **「Admin」、「Guest」、「12345678」のような単純なパスワードを設定しない**
  Bad Rabbitは感染拡大において、マルウェアにハードコードされたユーザ名とパスワードのリストを利用します。したがって、単純ではないパスワードを設定することで、感染拡大を防ぐすることができます。
- **ウィルス定義ソフトを導入し定義を最新に保つ**
  ウィルス定義ソフトを導入し定義を最新に保つことで、たとえ端末内にマルウェアが侵入したとしても、感染前に除去することができます。
- **OSやアプリケーションを最新の状態に保つ**
  OSやアプリケーションを最新の状態に保つことで、OSやアプリケーションの既知の脆弱性を突いた攻撃によるマルウェア感染および感染拡大を防ぐことができます。
- **定期的にバックアップを取得する**
  定期的にバックアップを取得しておくことで、たとえランサムウェアに感染しディスクの内容が暗号化されてしまったとしても、感染する前の状態に戻すことができます。

4. 「Bad Rabbit」のまとめ

Bad Rabbitはランサムウェアの一種であり、感染すると従来のランサムウェアに感染した場合と同様にハードディスクの内容が暗号化され身代金要求画面が表示されます。

Bad Rabbitは従来のランサムウェアとは異なる特徴もいくつか持っていますが、以下に示すような一般的なマルウェアにも適用されうる対策を常日頃より実施しておくことで、感染のリスクを大幅に低減することができます。

- 正規ではないサイトからダウンロードしたインストーラ等のプログラムを実行しない
- 「Admin」、「Guest」、「12345678」のような単純なパスワードを設定しない
- ウィルス定義ソフトを導入し定義を最新に保つ
- OSやアプリケーションを最新の状態に保つ
- 定期的にバックアップを取得する

5. 「Bad Rabbit」参考URL

- 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
- 新しい暗号化型ランサムウェア「Bad Rabbit」、ネットワーク経由で拡散、ウクライナとロシアなどで確認される
  http://blog.trendmicro.co.jp/archives/16226
- 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
- Webから感染する新種のランサムウェア「Bad Rabbit」とは。特徴と対策方法について
  https://www.shadan-kun.com/blog/securitynews/293.html
- Bad Rabbit（バッドラビット）とは？世界的に広がるランサムウェアを解説！
  https://cybersecurity-jp.com/security-measures/18860
- ランサムウェア「Bad Rabbit」は企業を脅すサイバー攻撃の可能性
  https://japan.zdnet.com/article/35109488/
- Don't Miss Another Blog 脅威のスポットライト：Bad Rabbitランサムウェア
  https://www.cylance.com/ja_jp/blog/jp-threat-spotlight-bad-rabbit-ransomware.html
- Bad Rabbit：新たな大規模ランサムウェア攻撃の兆し
  https://blog.kaspersky.co.jp/bad-rabbit-ransomware/18518/
- ExPetr/Petya/NotPetya：ランサムウェアではなくワイパー
  https://blog.kaspersky.co.jp/expetrpetyanotpetya-is-a-wiper-not-ransomware/16707/
- 【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
  http://www.nttdata.com/jp/ja/news/information/2017/pdf/20171102_v1.1_BadRabbitReport.pdf
- New Bad Rabbit Ransomware Attack
  https://www.sentinelone.com/blog/new-bad-rabbit-ransomware-attack/

NTT DATA

Trusted Global Innovator