オープンソースのRATを改良したマルウエアRedLeaves(2017-04-03) - JPCERT/CC Eyes

By 朝長 秀誠 (Shusei Tomonaga)

Published: 2017-04-02 · Archived: 2026-04-05 15:39:40 UTC

- RedLeaves

オープンソースのRATを改良したマルウエアRedLeaves

JPCERT/CCでは2016年10月頃から、RedLeavesと呼ばれるマルウエアに感染したことによる情報漏えいなどの被害事例を複数確認しています。RedLeavesは2016年以降、新たに確認されるようになったマルウエアで、標的型攻撃メールで送信されています。
今回は、RedLeavesの詳細や分析の結果判明したRedLeavesとPlugXとの関連性、RedLeavesが作成されるベースとなったツールについて紹介します。

RedLeavesが動作するまでの流れ
RedLeavesが動作するまでの流れを、図1に示しています。

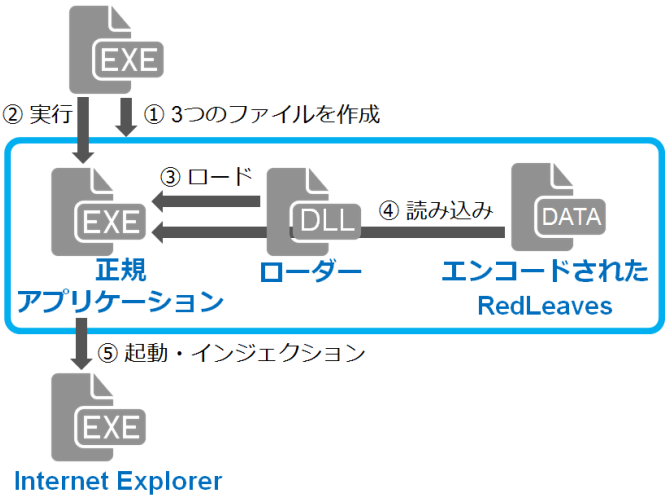


図 1：RedLeavesが動作するまでの流れ

JPCERT/CCで確認している検体は、実行されると以下の3つのファイルを%TEMP%フォルダに作成し、正規アプリケーションを実行します。

- 正規アプリケーション（EXEファイル）：同じフォルダに存在するDLLファイルを読み込む署名された実行ファイル
- ローダー（DLLファイル）：正規ファイルにより読み込まれる不正なDLLファイル
- エンコードされたRedLeaves（DATAファイル）：ローダーに読み込まれるエンコードされたデータ

実行された正規アプリケーションは、DLL Hijacking（DLLプリローディング）によって同じフォルダ内に存在するローダーをロードします。DLL Hijackingについて詳しくは[1]を参照してください。
正規アプリケーションにロードされたローダーは、エンコードされたRedLeavesを読み込み、デコードし、実行します。実行されたRedLeavesは設定内容に応じてプロセス（Internet Explorer）を起動し、自身をインジェクションします。その後、RedLeavesはインジェクションされたプロセスの中で動作するようになります。以降では、インジェクションされたRedLeavesの詳細な挙動を解説します。

RedLeavesの挙動の詳細

RedLeavesは、特定のサイトとHTTPまたは独自プロトコルで通信を行い、受信した命令を実行するマルウエアです。図2はインジェクションされたRedLeavesのPEヘッダ部分です。”MZ”や”PE”などの文字列が”0xFF 0xFF”で削除されています。

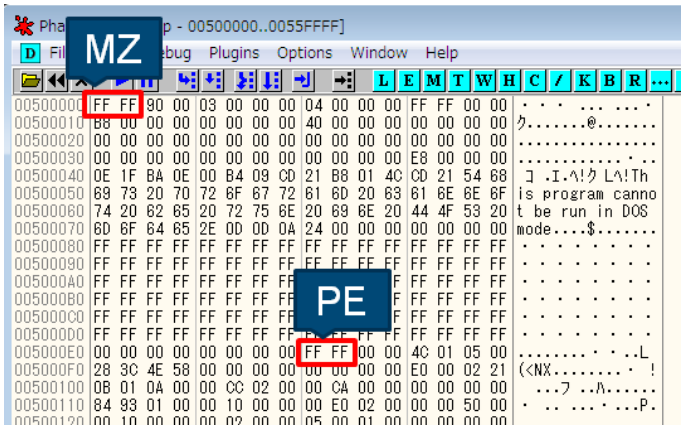


図 2： インジェクションされたRedLeaves

インジェクションされたRedLeavesは、HTTP POSTリクエストまたは独自プロトコルでC&Cサーバに接続します。通信先や通信方式については、設定情報に含まれています。設定情報の詳細に関しては、Appendix Aをご覧ください。
以下は、HTTP POSTリクエストの例です。送信するデータのフォーマットについては、Appendix B表B-1、表B-2をご覧ください。

POST /YJCk8Di/index.php
Connection: Keep-Alive
Accept: */*
Content-Length: 140
Host: 67.205.132.17:443

[データ]

データはRC4で暗号化（キーは設定情報に含まれている）されており、以下のような内容が含まれています。

```
__msgid=23.__serial=0.clientid=A58D72524B51AA4DBBB70431BD3DBBE9
```

C&Cサーバから受信するデータには、コマンドなどが含まれており、受信したコマンドに応じて、以下の機能を実行します。（受信するデータについてはAppendix B表B-3をご覧ください）

- ファイル関連の操作
- 任意のシェルコマンド実行
- 通信方式の設定
- ドライブ情報の送信
- システム情報の送信
- ファイルアップロード・ダウンロード
- スクリーンキャプチャ
- プロキシ機能の実行

RedLeavesのベースとなったコード

以上のような機能を持つRedLeavesですが、分析した結果Github上で公開されているTrochilus[2]と呼ばれるRAT（Remote Administration Tool）のソースコードと類似する部分が多数あることを確認しました。図3は、送受信するデータを処理するコードの一部です。Appendix B表B-3で記載した内容と同じデータを処理していることが分かります。

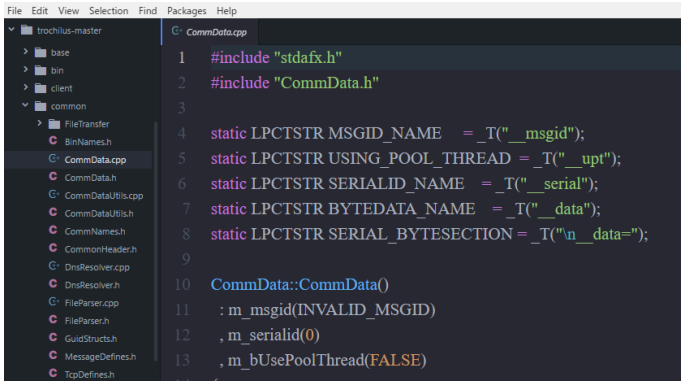


図 3： Trochilusのソースコードの一部

RedLeavesは、一から作成されたわけではなくTrochilusのソースコードを改良して作成されたと考えられます。

PlugXとの関連性

JPCERT/CCで確認しているRedLeavesと、過去に特定の攻撃グループが使用していたPlugXを比較すると、一部の処理に類似のコード使われていることが分かりました。以下は、本体が3つのファイル（正規アプリケーション、ローダー、エンコードされたRedLeavesまたはPlugX）を作成する際の処理です。

図 4： ファイル作成処理の比較

さらに、ローダーがエンコードされたデータ（エンコードされたRedLeavesまたはPlugX）をデコードする処理も類似しています。

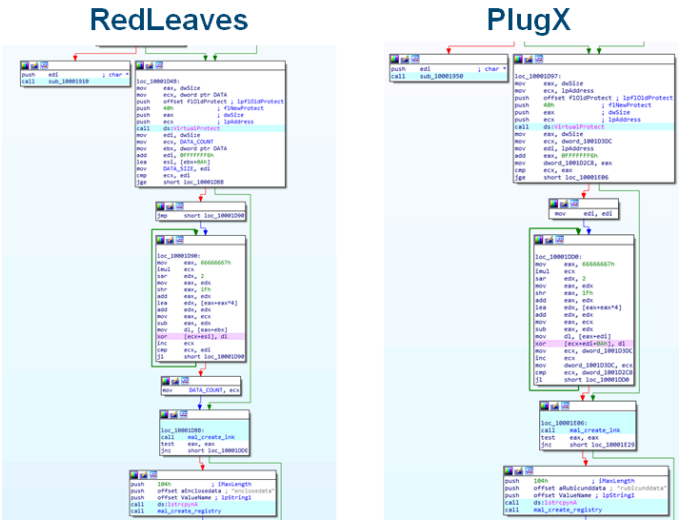


図 5： ファイルデコード処理の比較

また、上記の類似のコードを持つRedLeavesとPlugXの検体の中には同じ通信先を使用するものが存在することを確認しています。このことから、RedLeavesを使用している攻撃グループは、RedLeavesを使用する以前はPlugXを使って攻撃を行っていたと考えられます。

おわりに

RedLeavesは、2016年から確認されるようになった新しいマルウエアです。現在も標的型攻撃メールとして送信されており、今後もRedLeavesを悪用した攻撃は続く可能性があるため、注意が必要です。
今回解説した検体のハッシュ値に関しては、Appendix Cに記載しています。また、これまでJPCERT/CCで確認しているRedLeavesの通信先の一部はAppendix Dに記載していますので、このような通信先にアクセスしている端末がないかご確認ください。

分析センター 朝長 秀誠

参考情報

[1] JPCERT/CC分析センターだより: 巧妙化するDLL hijacking ～ CVE2011-1991を悪用する攻撃 ～(2013-01-31)
https://blogs.jpcert.or.jp/ja/2013/01/vol1.html

[2] Trochilus: A fast&free windows remote administration Tool
https://github.com/5loyd/trochilus

Appendix A 設定情報

表 A: 設定情報の一覧

オフセット	説明	備考
0x000	通信先1	
0x040	通信先2	
0x080	通信先3	
0x0C0	ポート番号	
0x1D0	通信モード	1=TCP, 2=HTTP, 3=HTTPS, 4=TCP and HTTP
0x1E4	ID	
0x500	Mutex	
0x726	インジェクションプロセス	
0x82A	RC4キー	通信の暗号化に使用

RC4キーの例

- Lucky123
- problems
- 20161213
- john1234
- minasawa

Appendix B 送受信データの内容

表 B-1: HTTP POSTリクエストで送信されるデータフォーマット

オフセット	長さ	内容
0x00	4	RC4暗号化されたデータ長 （RC4キーの先頭の4バイトでXOR）
0x04	4	Server id （RC4キーの先頭の4バイトでXOR）
0x08	4	固定値
0x0C	-	RC4暗号化されたデータ

表 B-2: 独自プロトコルで送信されるデータフォーマット

オフセット	長さ	内容
0x00	4	ランダムな数値
0x04	4	固定値
0x08	4	長さ
0x0C	4	RC4暗号化されたデータ長 （RC4キーの先頭の4バイトでXOR）
0x10	4	Server id （RC4キーの先頭の4バイトでXOR）
0x14	4	固定値
0x18	-	RC4暗号化されたデータ

表 B-3: 受信データに含まれる内容

文字列	種類	内容
__msgid	数値	コマンド
__serial	数値	
__upt	true など	コマンドをスレッド実行するか
__data	データ	コマンドパラメータなど

Appendix C 検体のSHA-256ハッシュ値

RedLeaves

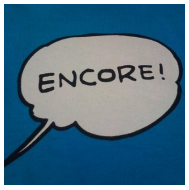
・5262cb9791df50fafcb2fbd5f93226050b51efe400c2924eecba97b7ce437481

PlugX

・fcccc611730474775ff1cfd4c60481deef586f01191348b07d7a143d174a07b0

Appendix D 通信先一覧

・mailowl.jkub.com
・windowsupdates.itemdb.com
・microsoftstores.itemdb.com
・67.205.132.17
・144.168.45.116



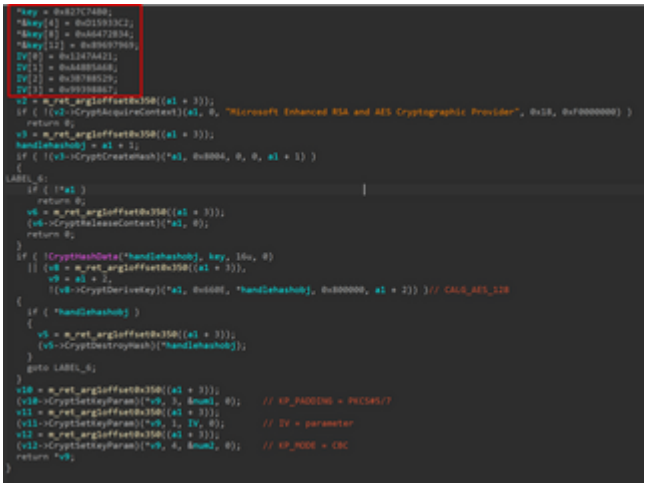
朝長 秀誠 (Shusei Tomonaga)

外資系ITベンダーでのセキュリティ監視・分析業務を経て、2012年12月から現職。現在は、マルウェア分析・フォレンジック調査に従事。主に、標的型攻撃に関するインシデント分析を行っている。CODE BLUE、BsidesLV、BlackHat USA Arsenal、Botconf、PacSec、FIRSTなどで講演。JSACオーガナイザー。

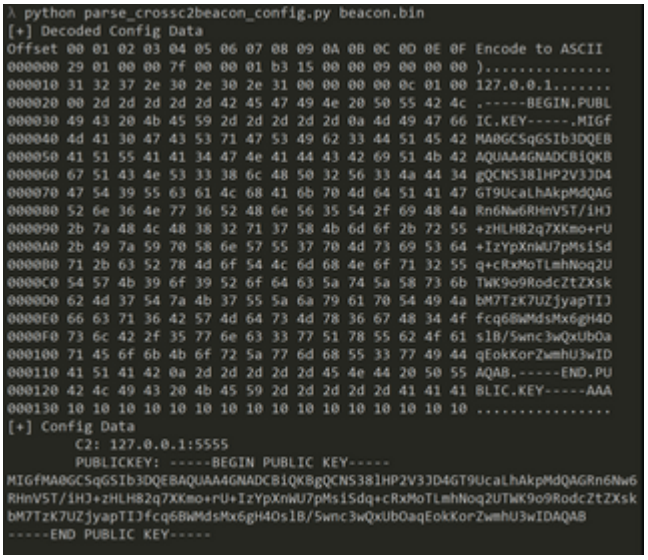
関連記事

- 

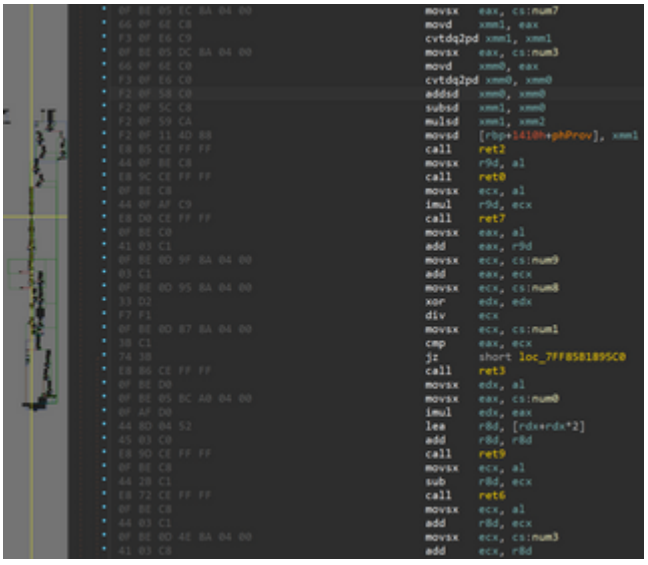
  JSAC2026 開催レポート ～DAY 2～

- 

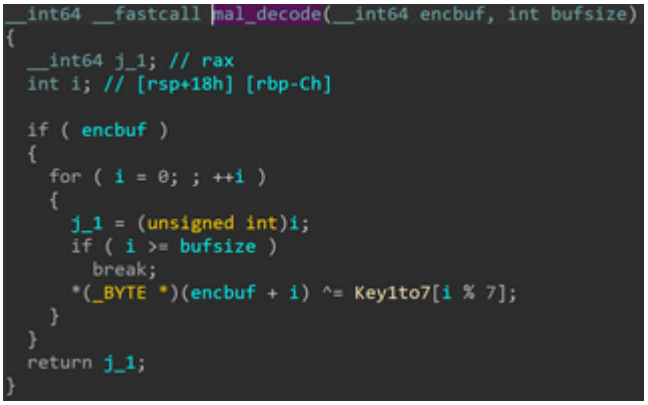
- [攻撃グループAPT-C-60による攻撃のアップデート]



- [Cobalt Strike Beaconの機能をクロスプラットフォームへと拡張するツール「CrossC2」を使った攻撃]



- [Ivanti Connect Secureの脆弱性を起点とした侵害で確認されたマルウェア]



Ivanti Connect Secureに設置されたマルウェアDslogdRAT
