Dr.WEB®
Anti-virus

トロイの木馬型マルウエア「Fruity」ってなに？

株式会社Doctor Web Pacific

Dr.WEB®
Anti-virus

今回のテーマ

- トロイの木馬とは
- Fruityの攻撃手法

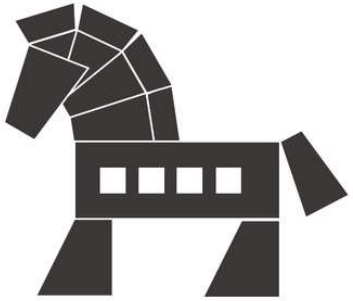
Dr.WEB®
Anti-virus

トロイの木馬型マルウェアとは

トロイの木馬とは

トロイの木馬は、通常のファイルに偽装して潜伏する悪意のあるソフトウェアの総称です。通常のマルウェアと異なり、標的のデバイスに侵入するためのファイルをダウンロードしたり、脆弱性やソーシャルエンジニアリング技術の悪用するなど、様々な間接的な攻撃を行うマルウェアです。

名前の由来は、古代ギリシャのトロイ戦争で使われた戦術に由来しています。



Dr.WEB®
Anti-virus

Fruityの攻撃手法

Fruityの攻撃手法

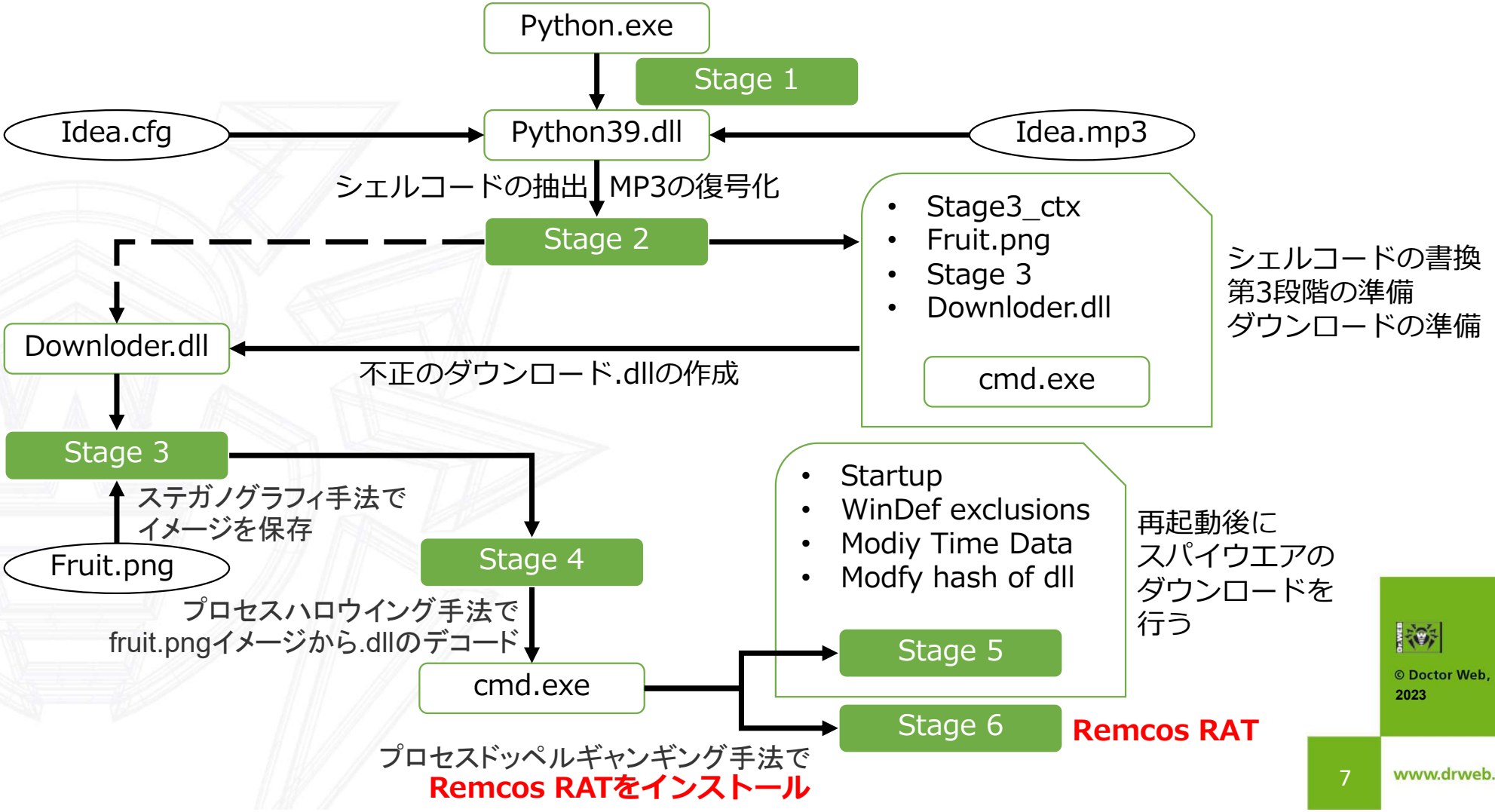
Fruity

Windows PCに対し、多段階プロセスを踏んで
複数のマルウエアを仕込むトロイの木馬型マルウェアです。

Fruityの脅威

段階を踏んでマルウェアが仕込まれることで
アンチウイルスソフトによる検知が困難な状態
に陥ります。

Fruityの多段階攻撃手法



用語集

No.	用語	概要
1	シェルコード	攻撃者がコンピュータを乗っ取るために 送り込む特殊なプログラムコード
2	ステガノグラフィ	データの中に別の情報を埋め込んで 隠ぺいする技術
3	プロセスハロウイング	悪意のあるコードを挿入する コードインジェクション攻撃
4	プロセス ドッペルギャンギング	悪意のあるコードでプロセスを強制停止し、 代替えコードを注入する攻撃
5	Remcos RAT	感染端末から機密情報を詐取する スパイウエアの１つ

Dr.WEB®
Anti-virus

www.drweb.com
www.drweb.co.jp