

平成 22 年 4 月 28 日

Topic

「ガンブラー攻撃」に使用される URL の変化について

「ガンブラー攻撃」に使用される URL として、ロシアのドメイン名である「.ru」以外のものが見られるようになりました。今後、「.ru」に対する通信のみを遮断する方法では、「ガンブラー攻撃」への有効な対策にならない可能性があります。

1 概要

「ガンブラー攻撃」では、改ざんされたウェブサイトを開覧すると、利用者が気付かないうちに不正プログラム配布サーバへ誘導されます。不正プログラム配布サーバでは、利用者のコンピュータに存在する脆弱性を悪用され、不正プログラムに感染するおそれがあります。¹

「ガンブラー攻撃」による改ざんの特徴の一つは、不正プログラム配布サーバへの誘導先 URL を記述したスクリプトを埋め込むことです。警察庁サイバーフォースセンターで確認した誘導先 URL は、平成 22 年 3 月頃までは、すべてロシアのドメイン名である「.ru」でした。しかし、平成 22 年 4 月に入り、ロシア以外のドメイン名である「.info」、「.com」なども見られるようになりました。²

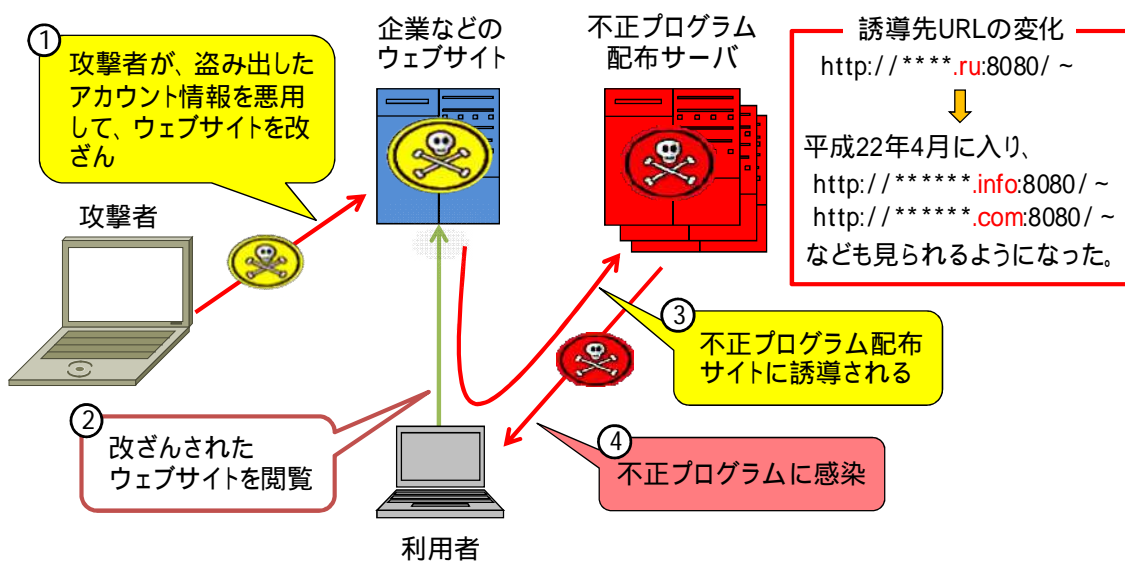


図 1-1 「ガンブラー攻撃」による不正プログラム感染の例

¹ 「情報技術解析平成 21 年報」pp.8-13 「4 「ガンブラー」によるウェブサイトの改ざん」

http://www.cyberpolice.go.jp/detect/pdf/H21_nempo.pdf

² この背景としては、平成 21 年 10 月以降、ロシアのドメイン名「.ru」の取得に身元保証書の提出が義務化されるなど、登録手続きが順次変更され、特に平成 22 年 4 月からは厳格な運用がなされていることが考えられます。

【参考】ru ドメイン名の登録規則」

RU」 <http://www.cctld.ru/ru/docs/RU-2.php>

また、誘導先 URL のサーバの IP アドレスは、「.ru」のもの、「.ru」以外のものとで、共通しているものが見られました。

2 対策

(1) 利用者の対策

「ガンブラー攻撃」の不正プログラム配布サーバへの誘導先 URL に、ロシアのドメイン名（「.ru」）以外のドメイン名である「.info」、「.com」なども見られるようになったため、今後、ロシアのドメイン名である「.ru」に対する通信のみを遮断して、不正プログラム配布サーバへの誘導を止める方法では、「ガンブラー攻撃」への有効な対策にならない可能性があります。

利用者は、不正プログラムに感染しないために、次の対策が重要です。

- セキュリティパッチの適用
- ウイルス対策ソフトの適切な運用

(2) ウェブサイト管理者の対策

ウェブサイト管理者は、管理するウェブサイトが改ざんされ、不正プログラムの配布に利用されないよう、次のセキュリティ対策を怠らないことが必要です。

- ウェブコンテンツの確認
- ウェブサーバのアクセス制御
- ウェブサーバのログ監査
- 管理用パソコンの用途をウェブサイト管理に限定し、ウェブサイトの閲覧には別のパソコンを使用