

## Clickfixによるマルウェア感染

### Clickfixとは？

webサイトを閲覧していると、**偽のCAPTCHA画面**が表示され、案内に従ってコマンドを入力すると不正なプロセスが実行されてしまうものです。

「CAPTCHA画面」という言葉を聞いたことがなくても、インターネットで**“こんな画面”**を見たことがあるんじゃないでしょうか？



こんなやつ



☐ 私はロボットではありません

CAPTCHA

### Clickfixによるマルウェア感染の流れ

- ①. サイト利用者に**偽のCAPTCHA画面**が表示される
- ②. 画面に表示された**“コマンド”**を実行させる
- ③. 利用者が気づかぬうちに**不正な指令が実行**される
- ④. 利用者の端末から情報が抜き出されてしまう。

知らない間に実行  
させられてしまう  
恐怖



偽のCAPTCHA画面が出た時に**バックグラウンドで不正な指令のコマンドがコピー**されており、**偽のエラーメッセージ**が表示される。



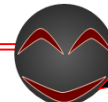
エラーが発生しました。  
次の手順を試してください。

1. **Windowsキー+Rキー**
2. **ctrlキー+Vキー**
3. **enterキー**

windowsのコマンドを直接実行する「ファイル名を指定して実行」のショートカットキー

コピーしているテキストを貼り付けるショートカットキー  
【windows+R】で出た「ファイル名を指定して実行」に不正な指令のコマンドを貼り付ける

貼り付けたコマンドを実行する



マルウェアの動いている画面は  
見せまっせーんwwwwww  
静かに盗ませてもらいまーすwwww



利用者が自ら実行するので、セキュリティソフトがインストールされていても対象外となり、検知されない。

もし、マルウェアに感染してしまうと、端末内に入っている情報や、Webブラウザが記憶している金融機関に関するID、パスワードなどを悪用され、不正送金や不正な証券取引等をされてしまうこともあります。

### 対 策

**突然のコマンド入力要求は無視して消す！**

よく見るwebサイトだからと言って、簡単にクリックしてしまうと取り返しのつかないことになってしまうかもしれません。  
webサイトを見ているときにコマンド実行を促されても従わず、消しましょう！

