TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2020年 第21号

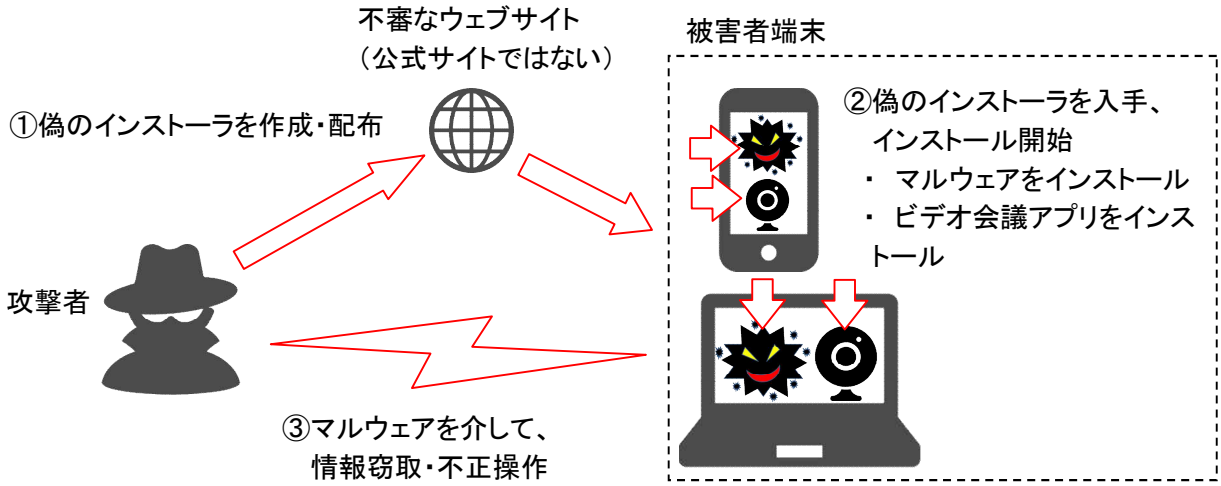
偽のZoomインストーラに注意！

新型コロナウイルス対策として急速に利用が拡大しているビデオ会議アプリ「Zoom」に、マルウェアが付属された偽のインストーラが２つ発見されました。

偽のインストーラは不審なウェブサイトで配布されていて、インストールを開始するとマルウェアをインストールして設定を変更、その後に正規または改変された Zoom 本体をインストールします。Zoom 自体はインストールされるのでマルウェアに気付きにくいのが特徴です。

マルウェアに感染すると、ユーザー認証情報を窃取される、リモートで不正操作される、ボットネットとして更なる攻撃の踏み台にされるなどの脅威があります。

急速に利用が拡大するビデオ会議アプリは攻撃者の格好の標的になっています。



【被害に遭わないための対策】

1. アプリは公式サイトや正規のマーケットプレイスから入手する。
2. ＯＳやソフトウェア、セキュリティ対策ソフトを最新に保つ。
3. 会議にはパスワードを使用し、ホスト管理を設定する。
4. 製品のアップデート機能からアプリを更新する。

【参考】トレンドマイクロ　セキュリティブログ
『偽の Zoom インストーラに隠されたバックドアとボットネット「DevilShadow」』
https://blog.trendmicro.co.jp/archives/25286