平成２９年１月１１日

１２月中の不正プログラム関連情報

※　ニュースの内容は、各種報道、インターネット等で公表されている情報に基づくもので、県警が事実を確認したものではありません。

鳥取県警察本部サイバー犯罪対策室

○　身代金代わりに「別の２人を感染させる」ことを要求するランサムウェア

ITmedia ニュースは 12 月 13 日、身代金を支払う代わりに別の２人をマルウェアに感染させれば、人質に取ったファイルの復号鍵を提供すると被害者に交換条件を持ちかけ、犯行に荷担させようとする新手のランサムウェア（身代金要求型マルウェア）が見つかったと報じた。コンピュータ情報サイトの Bleeping Computer が 12 月８日付けで伝えているという。

このランサムウェア「Popcorn Time」はマルウェア対策を手掛けるセキュリティ企業が発見した。感染すると、コンピュータの画面に「Warning Message!!」という警告が表示され、英語で「あなたのコンピュータとあなたのファイルは暗号化された」と通告、ファイルを取り戻したければ身代金を支払えと脅迫する。

人質に取られたファイルを取り戻すには、身代金 1.0 ビットコイン（約 10 万円）を支払うか、他人を同じランサムウェアに感染させるという選択肢を提示。被害者が別の相手に不正なリンクを紹介し、そこから２人以上が Popcorn Time に感染して身代金を支払えば、最初の被害者のファイルは無料で復号できると持ちかけている。

また、Popcorn Time はまだ開発の途上にあり、もし被害者が誤った暗号解除鍵を４回入力すると、ファイルの消去が始まってしまう機能が追加されている可能性もあるという。

○　モバイルバンキングの情報を盗み出すマルウェア「Faketoken」

露セキュリティ企業カスペルスキーラボは 12 月 20 日、Android 端末に感染してモバイルバンキングの情報を盗み出すマルウェア「Faketoken」の被害が世界 27 か国に広がり、2,000 本以上の金融アプリが標的にされていることが分かったと伝えた。ユーザーのファイルを暗号化して人質に取るランサムウェアの機能も追加されているという。

カスペルスキーによると、Faketoken は正規のアプリやゲーム、あるいは FlashPlayer を装う手口でユーザーを騙してダウンロードさせ、執拗に管理者権限を要求する画面を表示して、承認する以外にほとんど選択肢がない状況に追い込む。

管理者権限を取得すると、メッセージや連絡先、通話等へのアクセスを次々にしつこく要求してユーザーに同意させ、最新版の Android からもユーザーのデータを盗み出せる状態にしてしまう。

さらに他のアプリを覆い隠す形でFaketokenの画面を表示する権限も要求。77の言語を使い分け、OSの言語を認識してユーザーを騙すフィッシング詐欺のメッセージを表示し、Gmailアカウントのパスワードを入力させるほか、正規のGooglePlayアプリを不正な画面で覆い隠して銀行カード情報を盗もうとする。

これまでにカスペルスキーが確認しただけでも世界で2,249本の金融アプリがFaketokenの標的にされ、ロシアやドイツ、タイ等27か国で16,000人を超す被害者が出ているという。

Faketokenには新たにユーザーのファイルを暗号化して人質に取るランサムウェアの機能が実装されていることも分かった。ただしモバイル端末ではほとんどのファイルがクラウドにバックアップされているため、ファイルと引き換えに身代金を要求する手口はあまり意味がなさそうだとカスペルスキーは指摘している。