

9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

○ Linux サーバを狙う新手のランサムウェア「FAIRWARE」

ITmedia ニュースは8月31日、Linux サーバに感染してウェブサイト用のフォルダを削除し、被害者に身代金を要求する新手のランサムウェア「FAIRWARE」が確認されたと報じた。コンピュータ情報サイトのBleeping Computerが同月29日付の記事で伝えているという。

それによると、被害者が自分たちのウェブサイトがダウンしていることに気付いて Linux サーバにログインしたところ、ウェブサイトのフォルダが削除されていて、「READ_ME.txt」というファイルが残っていたという。

READ_ME.txt に記載されたリンク先のサイトには、「お前のサーバは FAIRWARE というランサムウェアに感染した。ファイルを取り戻し、漏洩を防ぎたいければ、2週間以内に2ビットコイン（約12万円）を送金しなければならない」等という英語での脅迫文が掲載されていたという。

この内容について、Bleeping Computer は「攻撃者が本当に被害者のファイルを保存しているかどうかは不明で、たとえ身代金を支払ったとしてもファイルを取り戻せるかどうか分からない」としている。



○ Android を狙うランサムウェア、過去最大の19万3,000個を検出

トレンドマイクロは9月15日、8月に同社が検出した Android ユーザーを狙うランサムウェアの規模が過去最大になったと発表した。PCの被害が目立っているが、モバイル端末も危険な状態として警鐘を鳴らしている。

8月に検出された Android 向けランサムウェアは約19万3,000個で、前月の約10万5,000個から2倍近く増えた。このうち約13.5%が日本で検出され、数に相当する脅威が日本に流入しているという。また、同社が確認した検体数はのべ13万個に達し、1年間で4倍に増えたとしている。

Android 向けランサムウェアは、Google が運営する正規のアプリストア「Google Play」や携帯電話事業者が運営するアプリ提供サービス以外の場所で配布されるケースが多いといい、トレンドマイクロは「OSのセキュリティ設定から『提供元不明のアプリのインストールを許可する』の設定を無効にして、信頼できる場所からのみインストールしてほしい」としている。