平成２９年２月８日

１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

○　ランサムウェア被害、報告件数が過去最悪

トレンドマイクロは１月 10 日、データの復旧と引き換えに身代金を要求する「ランサムウェア」の被害が昨年大きく拡大し、日本国内でのランサムウェアの検出台数が１月から 11 月までの間で既に６万２千件を超えたと同社ブログで報じた。2015 年の年間検出台数は 6,700 件であり、9.3 倍まで急増しているという。

また、ランサムウェアによる被害の報告件数は 2,690 件で、2015 年の 3.4 倍に拡大しており、過去最大の被害となった。特に、法人利用者からの被害報告が全体の８割以上を占めており、ランサムウェアが行うネットワーク上のファイルを含めたデータ暗号化の活動が法人の業務継続に深刻な被害を与えていることが窺われる。

ランサムウェアの急増の背景として、トレンドマイクロは世界的なマルウェアスパムによる大量拡散の流入を挙げ、対策を呼び掛けている。

○　Mac を狙うマルウェア、何年も前から密かに流通か

Itmedia ニュースは１月 20 日、アップル社が販売しているコンピュータの「Mac」に感染して情報を盗み出すマルウェアが、生物医学の研究所を標的に、何年も前から検出されないまま出回っているのを発見したとして、ウイルス対策製品を手掛ける米企業のマルウェアバイツがブログでその内容を公表したと報じた。

それによると、このマルウェアは、ある IT 管理者が特定の Mac の不審なネットワークトラフィックに気付いたことから発見されたという。詳しく調べたところ、一見極めてシンプルに見える２件のファイルを使って外部の制御サーバと通信していることが判明。このスクリプトには、Mac の「screencapture」コマンドと Linux の「xwd」コマンドを使って画面をキャプチャするコードが含まれていた。

さらに興味深いことに、画面をキャプチャして Web カメラにアクセスする目的で、OSX 以前の時代の古い①システムコールや、1998 年以来更新されていない②オープンソースライブラリの libjpeg が使われていることも分かったという。

このマルウェアを Linux マシンでも試したところ問題なく実行できたといい、Linux 専用の亜種も存在している可能性があるとマルウェアバイツは推測する。ただし、実例は見つかっていない。

マルウェアに感染していたMacのうち１台は、2015年１月の日付でLaunch Agentファイルが作成されていたことも分かった。また、2014年10月にリリースされたOSX10.10（Yosemite）に合わせて変更したことを示すコメントもあり、少なくともYosemiteがリリースされた当時から、このマルウェアが存在していたことが窺えるという。これまでこのマルウェアが発見されなかったのは、標的を生物医学研究所に絞り込んでいたためではないか、とマルウェアバイツは述べている。

---

① オペレーションシステム（ＯＳ）の機能を呼び出すために使用される機構のこと
② 無償で公開され、利用や改良が誰に対しても許可されているソフトウェア