農林水産研究情報総合センターニュース

第148号
2019年11月25 日

MAFFINにおける不審ファイルダウンロードの検出に関する報告

情報総合センターでは、MAFFINに接続する端末がインターネットから入手するファイルに対して、ネットワーク上でセキュリティ検査を行い、不審なファイルを検出した場合は、当該利用者所属法人のセキュリティ担当者に情報提供しています。本年、これまでに対応した案件についてまとめましたのでご紹介します。

必要なソフトを探した検索結果から不審なサイトに誘導されて、不要なソフトを同梱したファイルをダウンロードしてしまう事例が多くみられます。ダウンロードする際は、下記のチェックポイントを参考に、取得しようとするファイルが安全であるかを十分確認するとともに、万が一の場合に、PCのOS再インストールが必要になっても困らないよう、データバックアップ等の準備をするようにしてください。

「不審ファイルのダウンロード」を頻繁に検出

2019年1月1日～11月20日までの間に不審ファイルのダウンロードに関する情報提供を52件行いました。月ごとの件数は図１のとおりです。随時注意喚起していますが、なかなか減らない状況です。

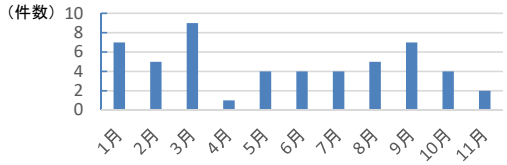

図1　月ごとの情報提供件数「不審なファイルのダウンロード」

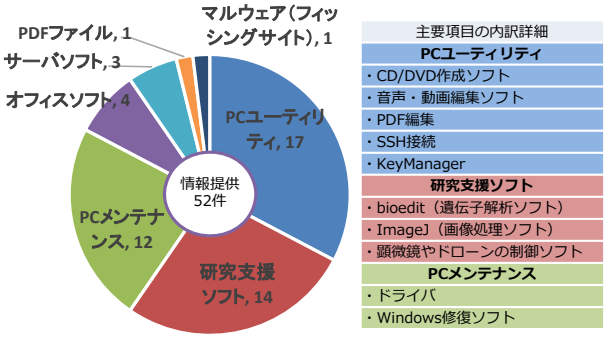

図2　ダウンロードしたソフト、ファイルの種類

ダウンロードの目的はソフトの導入が多く、ソフトの種類は様々

検出した際に入手しようとしていたファイルの種類は、PCのユーティリティソフトや研究支援ソフトが多く（図２）、中には情報総合センターの多要素認証の利用に必要なSoliton KeyManager（クライアント証明書管理ソフト）の事例も確認されました。

PCメンテナンスとした検出の内容は、PCに欠陥があるように誤認させて有償版のソフトを購入させようとする迷惑ソフトが多数で、経緯は、ドライバ等を探索して誘導されてしまった事例の他、サイトの広告等から意図せずにダウンロードされた事例もありました。

Microsoftの修正プログラム提供サイトを模倣した不審なサイトを確認

Windows update時のエラーコードを検索した結果から不審なサイトに誘導されたと報告のあった案件では、誘導先のサイトが図３のように非常に巧妙に模倣されたサイトでした。ドメイン名も「error」「fix」「kit」「help」等の組み合わせで、URLを見てもMicrosoft関連と誤認しやすく細工されていました。

不正サイトと気づくことは難しいですが、まずはこのようなサイトが存在することを認識し、警戒してください。

図3　Microsoftの修正プログラム提供サイトを模倣した不審なサイト

関係者から提供された情報にも細心の注意を

以下のようなケースが、MAFFIN内で確認されていますのでご注意ください。

○取引先がサイバー攻撃を受け、乗っ取られたアカウントから業務連絡を装った不審メールが届いた。

○業者が作成したマニュアルに記載されたソフト入手先のURLが不適切で、ダウンロードしたファイルからマルウェアが検出された。

インターネットからソフトを入手する際のチェックポイント

☑ 適切な入手先か確認する。
（そのサイトは、誰が、何の目的でソフトを配布しているか想像してください）
- ソフトを多数配布しているサイトは要注意
- Whoisでドメインの所有者名や国名を確認する
- ファイル名やサイトのドメイン名を検索して悪い評判がないか確認する
- 書籍や信頼できる紹介サイトに記載されたURLか確認する
- 海外のサイトは、たとえ開発元であっても、不要ソフトの混入を警戒する

☑ ダウンロードしたファイルを実行する前にVirusTotal (https://www.virustotal.com/)でファイルスキャンする
※VirusTotalにアップロードすると第三者が入手可能になるため、機密情報漏洩や利用規約違反になる場合には利用できません。

☑ 一人で判断せず、管理者やセキュリティ担当者等に相談する。

☑ 所内規程を遵守してインターネットを利用する。

ニュースはWebで発信しています。

AFFRIT Portal » 農林水産研究情報総合センターニュース
http://itcweb.cc.affrc.go.jp/affrit/inside/publications/affrit-news/start

トピックス:

マイクロソフト社製品のサポート終了について

(サポート終了日別の対象ソフトウェア)

2020年1月14日
Windows 7
Windows Server 2008
Windows Server 2008R2

2020年10月13日
Office 2010

サポートが終了したOSのMAFFIN接続は禁止されています。