2017 年 11 月 29 日
株式会社セキュアソフト

注意喚起：ファイルレス・マルウェア攻撃の脅威について

1. 概要

マルウェア感染による被害が世界的に多数報告されております。その種類も数多く新種のマルウェアが攻撃者達によって日々開発されており、セキュリティ対策を実施する企業とのいたちごっことなっております。その中でもファイルを持たない「ファイルレス・マルウェア攻撃」と呼ばれる新たなサイバー攻撃が今年に入って急増しており脅威となっております。

攻撃被害としては今年の初めに、世界数十か国以上の規模で銀行の ATM を不正に操作され多額の金額を搾取されたとの報告もされております。同種の攻撃への被害拡大を防ぐ為、攻撃の特徴と、弊社セキュリティソリューションによる対策をご紹介致します。

2. ファイルレス・マルウェア攻撃とは

⑴ 攻撃の特徴

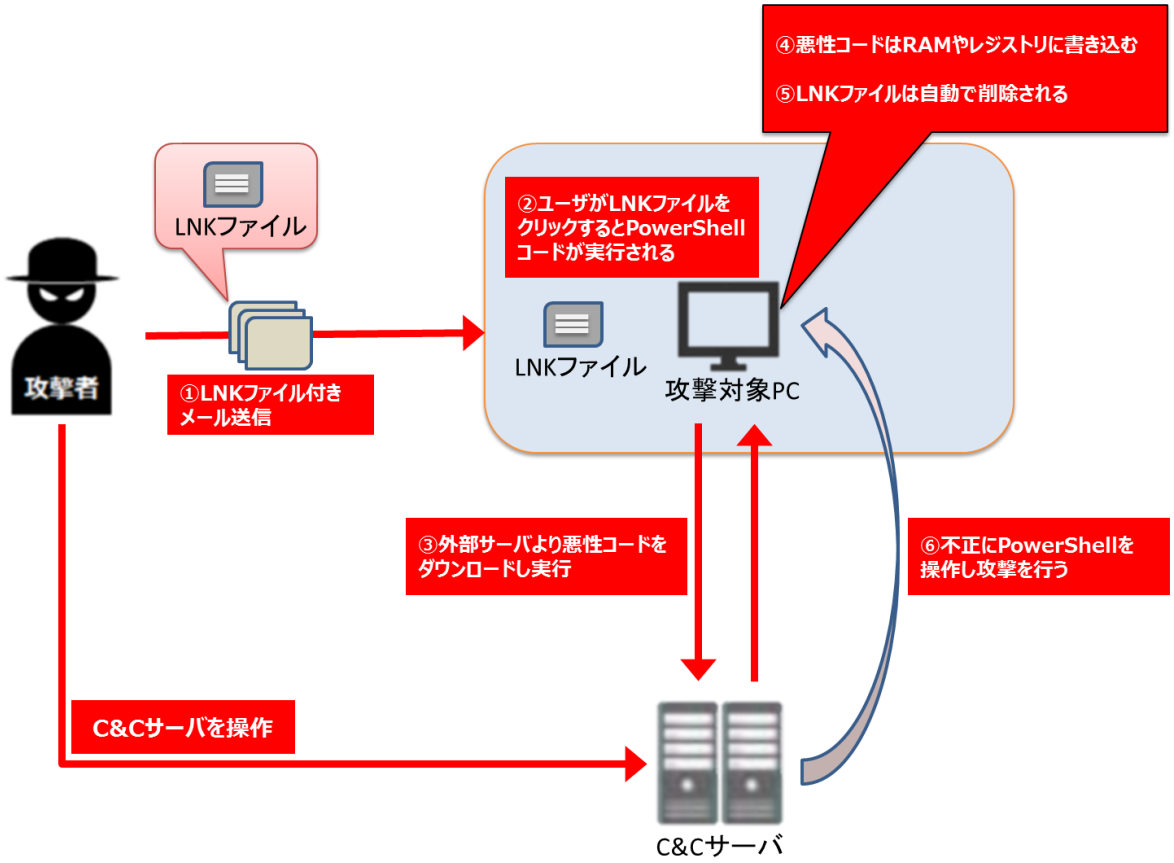
攻撃対象へ送付するファイルは、EXE や DLL 等の直接実行可能な形式ではなく、LNK ファイル等を用いて Windows 標準プログラムを利用する為、ウィルス対策ソフトの検知が困難な特徴があります。また、メモリや OS のレジストリにコードを直接埋め込み動作する為、ファイルそのものをパソコンのディスク内に残しません。

※LNK は Windows ショートカットファイルの拡張子です。
拡張子の偽造等が容易な為、様々な攻撃手法に用いられています。

⑵ 攻撃シナリオの一例

① 攻撃者は EXE 形式のファイルでは無く、LNK ファイルを偽メールに添付し拡散します
② LNK ファイルは見かけ上は通常のショートカットとして表示されますが、ショートカット先が巧妙に隠ぺいされており ユーザが LNK ファイルをクリックすると、PowerShell コードが実行されます
③ PowerShell コードが実行されると外部サーバから悪性コードをダウンロードし実行します
④ 悪性コードはディスク内にファイルは残さず、PC 内のメモリや Windows レジストリに書き込みます
⑤ LNK ファイルは自動で削除されます
⑥ 悪性コードが実行されると PowerShell を制御できるようになる為、遠隔の C&C サーバから不正に PowerShell を操作することにより、様々なウィルスのダウンロードや、PC 内の情報を収集することが可能となります

※攻撃シナリオについては PowerShell 使用例を掲載しております。



【図　1】ファイルレス・マルウェア侵入イメージ

(3) 一般的な対策

① EXE 形式で無くとも不用意にファイルを開かない
② PowerShell 自体の無効化（攻撃手法に PowerShell が用いられた場合に有効）
③ FW や IPS 等により C&C サーバとの通信をブロックする出口対策
④ OS やアプリケーションのアップデートを実施し、脆弱性のあるシステムを無くすことでマルウェア感染時の脅威を阻止する
⑤ 共有ファイルやフォルダのセキュリティ設定、ユーザアクセス権限を厳重に行う

3. mamoret BE による対策

一般的な対策とは別にコンテナ技術を利用した対策として mamoret BE を使用することをお勧めいたします。

⑴ mamoret BE 概要説明

一般業務を行うローカル環境とインターネットアクセス環境を PC 上で分離し、マルウェアから PC を守る製品です。
万が一、マルウェアがインターネットアクセス環境に侵入してもローカル環境内のデータを保護することができます。

【図 2】mamoret BE 概念図

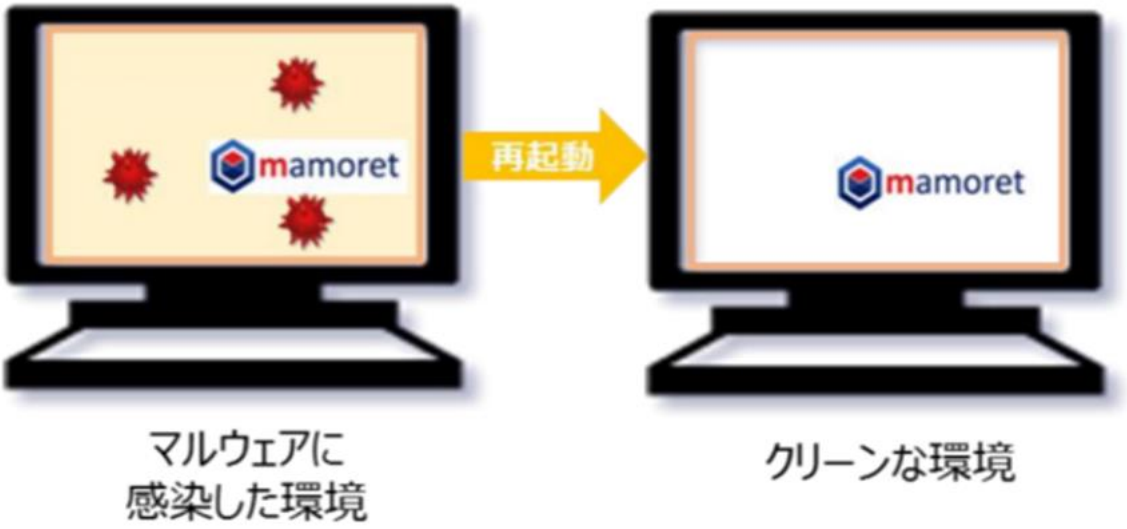
⑵ 対策概要

① サーバモードのネットワーク制御機能を利用することにより、上記【攻撃の典型的なシナリオ】2 -⑵-⑥へ記載している不正な外部通信はブロックされる為、PowerShell を制御してローカル環境への不正なダウンロードや、情報収集の被害を防ぐことができます。
※サーバモードとはクラウド上で管理サーバを利用することによりネットワーク制御、ポリシーの一元管理を行える機能

② 万が一、インターネットアクセス環境にマルウェアが侵入しても mamoret BE の環境分離機能にてローカル環境へのマルウェア攻撃・情報収集被害を防ぐことができます。

【図 3】ネットワーク制御機能のイメージ

③ mamoret BE にはインターネット接続環境の自動初期化機能があり、万が一マルウェアに感染しても mamoret BE を再起動すると次回起動時には、クリーンなインターネット接続環境が利用可能となります。



【図 4】インターネット接続専用環境の初期化イメージ

⑶ mamoret BE を使用した運用例

メールはインターネットアクセス環境内で Web メールを使用して閲覧

メールをインターネットアクセス環境内で Web メールを使用することでマルウェアが添付されたメールを開いてもローカル環境内のデータを保護できます。安全が確認できたファイルについては、ファイル持込・持出機能によりローカル環境へ持ち込みます。

上記の運用を行うことにより、万が一、マルウェアがインターネットアクセス環境に侵入してもローカル環境内のデータを保護することができます。

mamoret BE についての詳しい情報は、下記 URL をご参照ください。
【製品 URL】https://www.securesoft.co.jp/products/mamoret-be

«お問合せ先»
株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp