Deloitte.

発行日:2014年9月8日

デロイト トーマツ サイバーセキュリティ先端研究所
ニュースレター Vol. 2

ソフトウェアのアップデートを装う標的型攻撃

特定組織を対象とした高度な攻撃手法

トーマツ.

ソフトウェアのアップデートを装う標的型攻撃

特定組織を対象とした高度な攻撃手法

「ソフトウェアのアップデート機能を装う標的型攻撃」の脅威 従来の標的型攻撃との差異

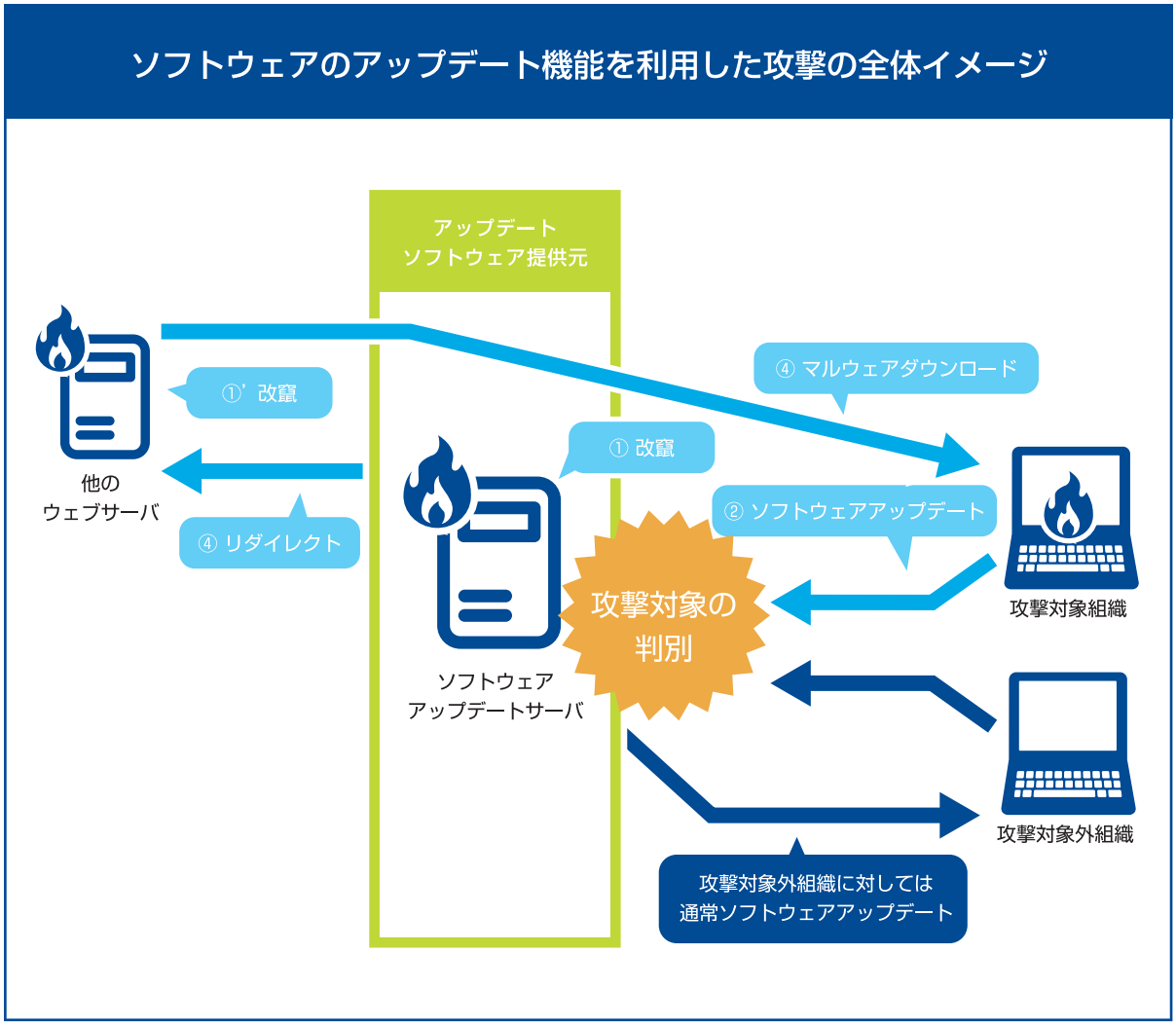
昨年より、特定の組織を攻撃対象とした「ソフトウェアのアップデート機能を装う標的型攻撃」が複数確認されています。攻撃者は、事前に攻撃対象の組織が利用しているオペレーティングシステム（OS）やソフトウェア等の情報を入手し、攻撃インフラを構築することでこれまで以上に巧妙な攻撃を実現しています。

従来のメールによる標的型攻撃は、添付ファイルを実行する等の利用者（被攻撃者）の操作に依存する部分がありましたが、本攻撃はソフトウェアの自動アップデート機能の仕組みを利用するため、利用者が意識的に操作せずとも攻撃が行われる点が特徴といえます。考え方としては「水飲み場攻撃」に類似しており、同様の攻撃手法としてクラウド・ストレージのデータ同期の仕組みを悪用したものもあります。ソフトウェアアップデートの多くがインターネット経由で自動実行されるため、今後脅威や被害が増大することが考えられます。

アップデート機能を悪用した標的型攻撃の仕組み

ソフトウェアのアップデートファイルを提供するサーバの多くはウェブサーバで運用されており、アップデート機能はOSやアプリケーションの起動時にバックグラウンドで動作しています。つまり、攻撃者はアップデートサーバに侵入ができれば、特定の利用者に対して悪性コードを受信させることができてしまうということです。
攻撃者はソフトウェア開発会社が提供する正規のアップデートサーバに侵入（右図①）し、どの組織がアップデートサーバにアクセスしているか調べ、攻撃対象を決定します。その後、攻撃対象の組織からのアクセス（同②）のみを攻撃者が用意した別のサイトへ誘導（同③）することで攻撃を行います。攻撃対象組織の利用者は正規のアップデートサーバにアクセスするため、悪性コードを含む偽アップデートファイルに対してOSやアンチウイルスソフト等がセキュリティ侵害の警告を発した場合でも特に意識せずに実行（同④）してしまいます。

当研究所において確認した攻撃は、いずれも「特定の組織」のみが標的となっており、且つ「一定の期間、時間帯」にのみ悪意あるウェブサーバへ誘導する設定となっていました。攻撃対象を限定することで被害も特定組織に限定され、攻撃の発見と対応が遅れる原因となっており、公開されているセキュリティ情報のみでは十分な対応が困難になったといえます。



複雑化する標的型攻撃の対策に先立って

当研究所で確認した範囲では、偽アップデートプログラムはいずれも不正な署名が行われていました。したがって、利用者がアップデート時に表示されるコード署名用の証明書に関する警告メッセージを注意深く確認することや、利用者が個別にインターネット上にファイルを取得することを防止するため、インストールするアプリケーションやアップデートを一元管理可能なソフトウェア自動配布システム等を利用することが対策として考えられます。
これらの他にも対策は考えられますが、信頼するソフトウェアのサーバが侵害されているため、利用者側からの対策は困難といえます。したがって、偽アップデートによる侵害にいち早く気付くための体制構築と事後対応（ダメージコントロール）について、このような攻撃を想定した準備を事前にしておくことが重要であるといえます。

国内ネットワーク

有限責任監査法人トーマツ

東　京　〒100-0005　東京都千代田区丸の内3-3-1　新東京ビル Tel:03-6213-1112
大　阪　〒541-0042　大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング Tel:06-4560-6021
名古屋　〒450-8530　愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館　Tel:052-565-5517
福　岡　〒810-0001　福岡県福岡市中央区天神1-4-2 エルガーラ　Tel:092-751-1517

デロイト トーマツ サイバーセキュリティ先端研究所　http://www.tohmatsu.com/dtarlcs/
〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル

デロイト トーマツ リスクサービス株式会社
本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル Tel:03-6213-1300