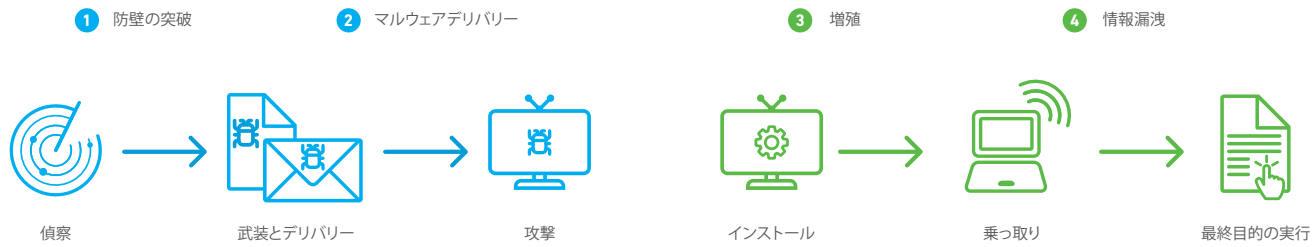
clearswift
RUAG Cyber Security

クリアスウィフトとサイバーキルチェーン

サイバーキルチェーンは、ロッキードマーチン社によって開発されたサイバー攻撃行動の特定や防止に役立てるためのフレームワークです。サイバーキルチェーンは、攻撃者が目標を攻撃する際に必要な行動の流れ（チェーン）をモデル化しています。攻撃の流れを断ち切り、攻撃を阻止します。



不正アクセス

偵察

インターネットで公開されている情報や特定のテクノロジーを調べて事前調査、特定、選定が行われます。攻撃対象となりうる脆弱な標的を見つけ出すことが目的です。

武装

攻撃者は、突破口を利用して攻撃コードを作成します。実行ファイル、Adobe PDFやMicrosoft Officeドキュメントといったクライアントのアプリケーションデータファイルがデリバリーされる武器として使われます。

デリバリー

攻撃者は、電子メール、ウェブ、USBメモリー、QRコードやそれ以外の手段で攻撃コードを攻撃対象にデリバリーします。実際のファイルのこともあれば、クリックさせるように誘うリンクのこともあります。

攻撃

攻撃コードがデリバリーされると、知らぬ間にこっそりとインストールされるか、またはソーシャルエンジニアリングの手法や被害者との交流関係を使ってファイルを開かせたり、リンクをクリックさせようとします。攻撃には被害者のネットワーク内の脆弱なアプリケーションやシステムが標的として狙われます。

不正アクセス

インストール

攻撃が成功すると、攻撃コードが被害者のシステムにバックドアをインストールし、攻撃者が常時アクセスできるようになります。攻撃によっては、情報の盗み出し（あるいは暗号化）が実際に行われるまでに数日から数ヶ月も潜伏していることもあり、インストールされたことに気づかれません。

乗っ取り

攻撃者は乗っ取り用のバックドアを作成します。被害者のサーバーと攻撃者との通信が可能になり、標的のネットワークやサーバーへの「キーボード操作」が継続的にできるようになります。

最終目的の実行

攻撃対象のネットワーク内部において、攻撃者が自己の最終目的を達成するためのアクションを実行します。データの盗み出しやデータ破壊、身代金目的の暗号化や他のターゲットシステムやユーザーへの感染などが行われます。

クリアスウィフトでサイバーキルチェーンを断ち切る

どの段階であれ、サイバーキルチェーンを断ち切ることで攻撃を阻止できます。このためには多層防御を備えておかなくてはなりません。それはデリバリーのフェーズから始まる組織がほとんどです。クリアスウィフトのSECURE Gateway製品なら、以下のことが実現します。

Clearswift SECURE Email Gateway (SEG) / Clearswift SECURE Exchange Gateway (SXG) / Clearswift ARgon for Email

- 先進の脅威防御機能、アクティブコンテンツのサニタイズ、2つのアンチマルウェアエンジンにより、デリバリーフェーズをブロックします。
- ディープコンテンツ分析検査機能により、最終目的の実行フェーズにおいて電子メールトラフィックからの情報漏洩を阻止します。

Clearswift SECURE Web Gateway (SWG) / Clearswift SECURE ICAP Gateway (SIG)

- 先進の脅威防御機能、アクティブコンテンツのサニタイズ、2つのアンチマルウェアエンジンにより、デリバリーフェーズをブロックします。
- ディープコンテンツ分析検査機能を使用し、最終目的の実行フェーズにおいてHTTP/HTTPSトラフィックからの情報漏洩を阻止します。

クリアスウィフト株式会社

clearswift
RUAG Cyber Security

〒163-1030
東京都新宿区西新宿3-7-1　新宿パークタワーN30階
tel. 03-5326-3470（代表）
fax: 03-5326-3001
Email: sales.jp@clearswift.co.jp
Web: http://www.clearswift.co.jp/