FireEye
SECURITY REIMAGINED

セキュリティ脅威
狙われるエネルギー業界

エネルギー業界の組織を狙うセキュリティ脅威は以下のとおりです。

- APT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）[1]の実行グループは、その活動の資金源となっている政府による、国家および経済の安全保障の確保に役立つ情報を窃取しようと試みます。狙われるのは、主に天然資源の探査やエネルギー関連の取引に関する情報と予想されます。エネルギー業界の競合相手との間で衝突が発生した場合には、破壊的な攻撃を仕掛ける可能性もあります。

- ハクティビストは、トラブルに巻き込まれたエネルギー企業を賛否いずれの立場からも攻撃する場合があります。標的の企業に対してDDoS（分散サービス妨害）攻撃、Webサイトの改ざん、または個人情報の搾取、流出を仕掛けて、企業評価の毀損や問題のクローズアップを狙います。

[1] APT 攻撃の実行者は、国家からの指示による情報窃取またはネットワーク攻撃や、失敗してもあきらめない執拗さ、多種多様なツールと技法を駆使するなどの特徴を備えています。

攻撃対象の詳細

FireEyeは、少なくとも9つの高度な攻撃の実行グループによる組織ネットワークの侵害を確認しました。標的となったのは以下のエネルギー業界のサブセクターです。

セキュリティ侵害を受けたサブセクター

代替エネルギー開発	石油・ガスの探査および生産
採炭	油田・ガス田設備製造
原子力開発	石油精製
天然ガスの流通およびマーケティング	

化学業界の企業から窃取されたデータ

経営幹部のやり取り	専有技術
契約交渉情報	市場分析
ビジネス・プロセス情報	

事例：石油精製会社を標的とするAPT攻撃

FireEyeは、さまざまな産業および商業用途で使用される、化学品の研究開発を行う企業で発生したセキュリティ侵害について調査しました。化学業界の企業にとって、農林業で使用される化学物質の品質改善を図り、作物の健康や微生物など自然由来の病気に対する耐性を高めることは重要な課題です。調査の結果、中国を拠点とする攻撃グループがこの企業のネットワークに不正アクセスし、6つのシステムに不正なソフトウェア9種をインストールした事実が明らかになりました。攻撃グループは、同国で広く利用されている製品の主要な設計図を含む、機密情報を窃取しました。摂取した情報を利用すれば、その製品標準書に則って、専用の製造施設を設計、建設、設置、および保守できる、とクライアントは話します。

今後の脅威動向とその影響

国家および経済の安全保障の重要性などを考慮すれば、エネルギー業界が今後も攻撃者の標的とされる可能性は極めて高いと考えられます。FireEyeでは、次のような要因が業界を狙う攻撃の引き金となると予測しています。

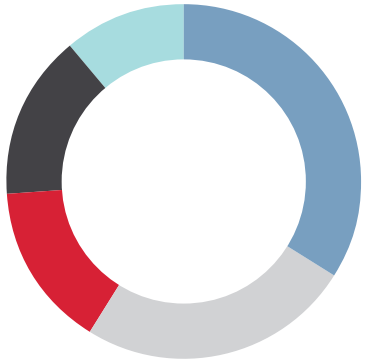
- 化石燃料の開発や代替エネルギーの生産における継続的な技術革新は、サイバー・スパイ活動増加の誘因となると考えられます。APT攻撃の実行グループは、国有企業にとって有益な知的財産や専有データを入手しようと試みます。
- 世界的なエネルギーの需要増加と天然資源の減少も、サイバー・スパイ活動の増加につながると見られます。国家が、エネルギー安全保障において対立関係にある相手に対する優位性確保につながる情報を求めるためです。
- 外国のエネルギー源への依存を減らそうとする政府の方針も、業界への攻撃を引き起こす要因となります。関与する攻撃者は、その活動の資金源となっている政府による国内のエネルギー企業の成長促進や新エネルギー源の開発に有益な情報を入手しようと試みます。
- 国家間の対立も攻撃増加の一因となります。国家の支援を受けた攻撃者は、対立関係にある相手のエネルギー供給を中断させて圧力をかけようと試みる可能性があります。
- さらに、環境問題をはじめとするエネルギー生産関連の問題が挙げられます。このような問題への注意を喚起し、責任があると思われる組織の評価を毀損しようと試みるハクティビストによる攻撃の増加が見込まれます。

FireEye Threat Intelligenceについて

FireEye Threat Intelligenceでは、FireEyeが独自に収集したセキュリティ脅威情報と解析情報を提供します。セキュリティ担当者がこのサービスを利用すれば、高度なサイバー攻撃を素早く検知、防御して、インシデント・レスポンスを実施するために必要となるコンテキスト情報を入手できます。FireEyeは、10年以上にわたるマルウェアや高度なサイバー攻撃に関する情報の収集と解析、数十もの業界やサブセクターにおける攻撃者の行動パターンへの対応、高度なサイバー攻撃者が使用する戦術について、独自に蓄積した比類のない知識の提供を続けています。

標的型マルウェア・ファミリー上位5種

- **9%** Page（別名ELISE）
- **28%** DarkComet
- **16%** Gh0stRAT
- **18%** XtremeRAT
- **29%** LV（別名NJRAT）



クライムウェアの亜種上位5種

- **34%** H-WORM
- **25%** ZEUS
- **15%** PALEVO
- **15%** RAMDO
- **11%** GAMARUE

主要なマルウェア

FireEyeが実施したエネルギー業界の組織ネットワークの侵害調査において、最も頻繁に検知された標的型マルウェア・ファミリーは以下のとおりです。

Page

(別名ELISE) 事前設定されたC&C（指令）サーバからエンコードされたDLLを入手しようとするダウンローダです。DLLがダウンロードされると、メモリに読み込みます。

DarkComet

一般に入手可能なRATです。レジストリの表示と改ざん、リバース・シェルの作成、キー入力内容の記録、認証情報の窃取、録音、ネットワークのスキャン、新しいC&Cサーバまたは新しい機能によるマルウェアのアップデート、ファイルのダウンロード・改ざん・アップロードなど、60以上のサーバ側の機能を備えています。

Gh0stRAT

一般に入手可能なソースコードに由来するリモート・アクセス・ツール（RAT）です。表示中の画像や再生中の音声のキャプチャ、Webカメラの有効化、プロセスのリストアップと停止、コマンド・シェルのオープン、イベント・ログの消去、ファイルの作成・操作・削除・実行・転送を行います。

XtremeRAT

一般に入手可能なRATです。ファイルのアップロードとダウンロード、Windowsレジストリの操作、プロセスとサービスの操作、音声や動画などのデータのキャプチャを行います。

LV

(別名NJRAT) 一般に入手可能なRATです。キー入力内容の記録、認証情報の収集、リバース・シェルへのアクセス、ファイルのアップロードとダウンロード、ファイルやレジストリの改ざんを行います。また、攻撃者が新しい亜種を作成できる「ビルダー」機能も備えています。

主要なクライムウェアの検知

FireEyeの脆弱性データと動的に共有される脅威情報より明らかになった、エネルギー業界で最も一般的に検知されるクライムウェアの亜種は以下のとおりです。

H-WORM

標的型攻撃に限らず、スパム・メールや不正なリンクを介して拡散する幅広いキャンペーンで使用されているRATです。

ZEUS

(別名Zbot) 銀行の認証情報の窃取を主目的としたトロイの木馬の一種です。リモートからのシェル・コマンドの実行など、多種多様な機能を備えています。

PALEVO

リムーバブル・ドライブ、ネットワーク共有、P2P、およびインスタント・メッセンジャー経由で拡散する情報窃取を目的としたワームです。感染したマシンは、UDP　53番ポートを介してC&Cサーバーと通信します。

RAMDO

感染システムのオペレーティング・システムやハードウェアに関する情報をC&Cサーバに送信するトロイの木馬です。アンチウイルス・ソフトウェアの正常な動作を阻む、またはクリック詐欺の実行を試みます。

GAMARUE

(別名Andromedaボット) キーロガー、フォーム・グラバー、またはその他の不正なソフトウェア用のドロッパーとして、さまざまな用途で使用されるトロイの木馬です。デバッグやVMへの対策機能をいくつか搭載しています。

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 | TEL: 03-4577-4401 | japan@fireeye.com | www.FireEye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

FireEye