クリティカルな社会インフラをターゲットにしたロシアのサイバー攻撃と NozomiNetworks の対応とは

by Heather MacKenzie and Moreno Carullo | Mar 16, 2018

米国政府は、米国のエネルギーとその他の重要な社会インフラをターゲットにしたロシアのサイバー攻撃による重大なサイバーセキュリティ警告を今週発表した。
最近、これら社会インフラ業界ではサイバー攻撃による脅威が大幅に増大の傾向にある。これまでのところ、攻撃犯罪者が誰なのか、その動機は何なのかについての推測は出来ている。
米国政府はこうした推測はめったに特定して公表はしませんが、このケースでは、脅威の犯罪組織と彼らの攻撃目的が何であるかについては明確に確認している。
さらに、US-CERT アラートには、攻撃の各ステージ、脆弱性の詳細な IOC(Indicators of Compromise：不正アクセスの痕跡)および検出と防止対応についての長い項目が記載されている。攻撃手口の多くは Dragonfly 2.0 のようなもので、Dragonfly 拡張版プレイブックと呼んでいる。Nozomi Networks のソリューションには、Dragonfly 2.0 の IOC をチェックするための分析ツールキットを同梱されている。
このブログ記事は、今回このアラートの全体像を俯瞰し、このサイバー攻撃対策を講じるための補足ガイダンスを提供し、Nozomi Networks のソリューションがどのように役立つかを紹介している。
（注）Symantec の研究者らが、米国、トルコ、スイスなどの送電施設に大規模なサイバー攻撃をしかけた IoC（攻撃犯罪の痕跡）を見つけ、これを彼らが「Dragonfly 2.0」と名付けた。Dragonfly とは、この攻撃を仕掛けているハッカー集団の呼称。

＊このような米国のエネルギー施設は、ロシアが狙うサイバー攻撃の重要なインフラターゲットの１つ。事故のあったスリーマイル島の原子力発電所は世界的に有名。

早期予兆のマルチステージ挙動を検知

US-CERT アラートでは、ロシアのサイバー攻撃組織がスピアフィッシングの手口（偽の電子メールを使って不特定多数の人から個人情報などを盗み取るフィッシング詐欺）を用いて、標的の産業ネットワークにリモートアクセスで侵入するマルチステージのサイバー侵入活動であると特定している。アクセス権を奪った後、脅威の感染経路を探すためにネットワーク偵察を行い、ネットワークに沿って移動スキャンし、産業制御システム（ICS）の様々な資産情報を収集する。

この挙動パターンは、典型的な APT タイプ（高度な標的型持続的攻撃）である。APT は継続的に行われるため、大きな損害が発生する前に APT の予兆を検知してブロックすることが必要である。産業ネットワークをモニタリングする従来技術を用いて、サイバー攻撃のダメージを受ける前の予兆を監視するのはきわめて難しい。

今回のケースでは、ロシアのサイバー攻撃は、まず足場となる標的、例えば、信頼されている第三者のサプライヤーといった周辺関係者にまず感染させることから始めて、要所要所に展開しながら最終的な標的拠点に攻撃を与える。

攻撃者は、まず足場となる標的に初期感染させ、産業制御システム（ICS）担当に関与している多くの情報を入手する。具体例を以下に列記する:

- 業界メディアのウエブの乗っ取り
- MS ワードの関連ファイルを添付してまず標的の宛先にメールを送信する
- 公開されている写真等、産業システムに関する情報を調べる

スピアフィッシングの手口を使って偽のメールを足場となる標的スタッフに送信して彼らの個人情報を盗み取る。悪意な.docx ファイルを彼らに感染させ、コマンド&コントロールサーバー（C&C）と通信させて個人情報を盗み出す。

上述の Dragonfly 2.0 攻撃では、スピアフィッシングの手口を通じて外部サーバー（C&C）と通信するために **SMB**（サーバーメッセージブロック）ネットワークプロトコルを使用。これは独特の手口である。SMB は通常、LAN 内での通信にのみ使用され、アウトバウンド通信では使用されない。こうした手口が考えられるので、設備資産管理担当者は、アウトバウンドのアクセス禁止をファイアウォールで設定しているかどうかを確認する必要がある。

標的ネットワークにアクセスするために上記で盗み取った個人情報が使用される。そこから、マルウェアはそれぞれ複数の管理者の標的メンバーに感染を広げる。最終ゴールはこれらのアカウントを盗んで証跡をクリーンアップするまでの作業。
次に、リモートサーバからツールをダウンロードして、Microsoft Windows ショートカットファイルの作成とレジストリを操作してユーザーの個人情報を収集して格納する。また、取掛かりの標的インフラを利用して、盗んだ個人情報とリモートアクセスサービスを使用して最終攻撃の標的に接続する。
ICS 環境の偵察フェーズには以下の手口が含まれている:

- バッチスクリプトを用いて産業制御システムネットワークを調べる
- スケジュールされたタスクとスクリーンショットユーティリティを用いてネットワーク上のシステム構成の画面をキャプチャする
- テキストファイルでホスト情報リストを管理する
- 企業ネットワーク上のコンピュータにアクセスし、ICS ベンダ名や参照ドキュメントを含む制御および SCADA システムに関するデータ出力を取得する
- ICS システムのプロファイルと構成情報を収集する

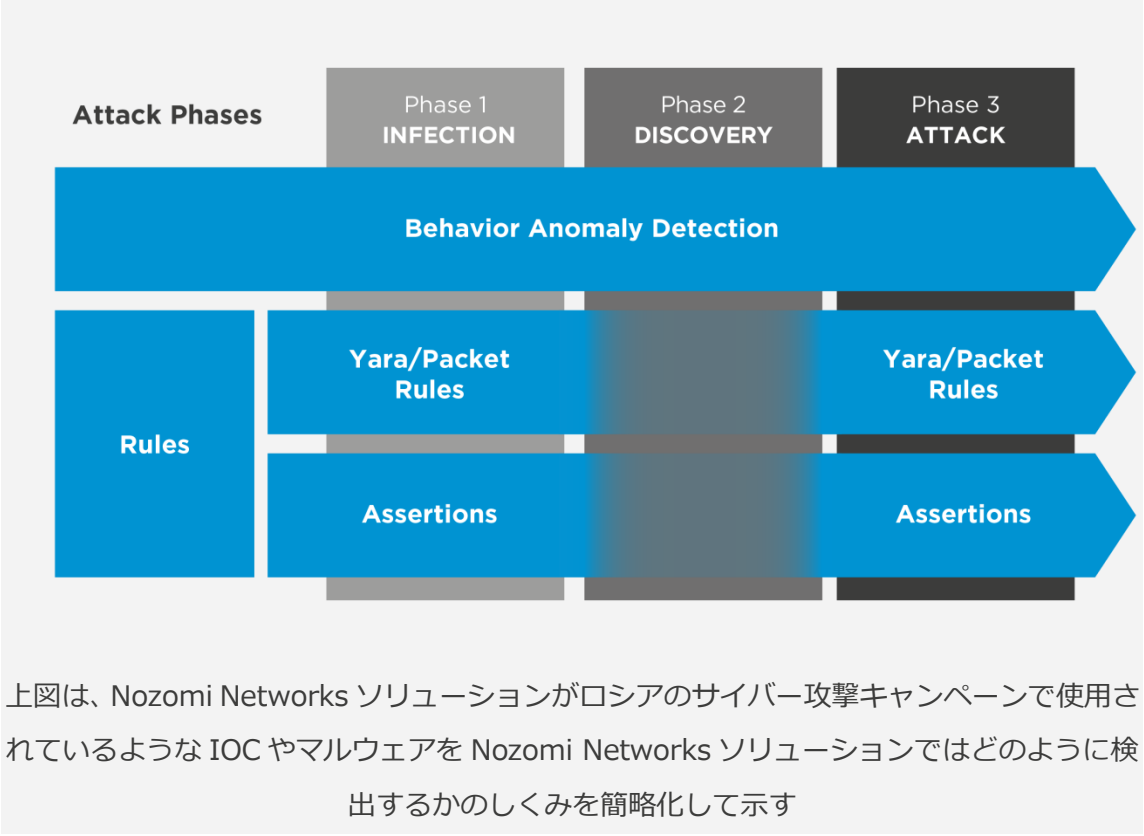
脅威の犯罪組織はまた、ログをクリアしたり、マルウェアアプリケーション、レジストリキー、スクリーンキャプチャを削除するなどの証跡を隠す行動をとる。
ロシアのサイバー攻撃の感染と偵察フェーズに関する詳細については長い間、US-Cert のアドバイザリーによれば、どのような装置が標的とされたのか、そしてどのような攻撃が意図的に行われたのかについて詳しくは不明。
今回の米国政府からの警告の目的は、業界施設が感染しているかどうかの判断の幅広い手がかり提供することである。

ハイブリッド脅威検出は APT を特定し、モニタリング作業を大幅に削減

アラート（TA18-074A）で提供される検出および予防対策のリストは広範囲である。リストに目を通す人は誰でも、ログとファイルのチェックをすべて行うために多くの人的資源と集中力が必要である。
Nozomi Networks のソリューションはこうした課題を解決する。Dragonfly 2.0 を識別する分析ツールキットを同梱し、挙動の有無を継続的に監視し、より効率的な検知インジケータに対応する。

これを達成するために使用される主な技術は、ハイブリッド脅威検出である。これは、脅威とリスクを特定するためのシグネチャと動作ベースの異常検出のハイブリッド。 結果をお互いのコンテキストで相関し、何が起こっているかを迅速に把握し、それによって軽減時間を短縮する。

APT（高度な標的型持続的攻撃）：全体の攻撃フェーズ

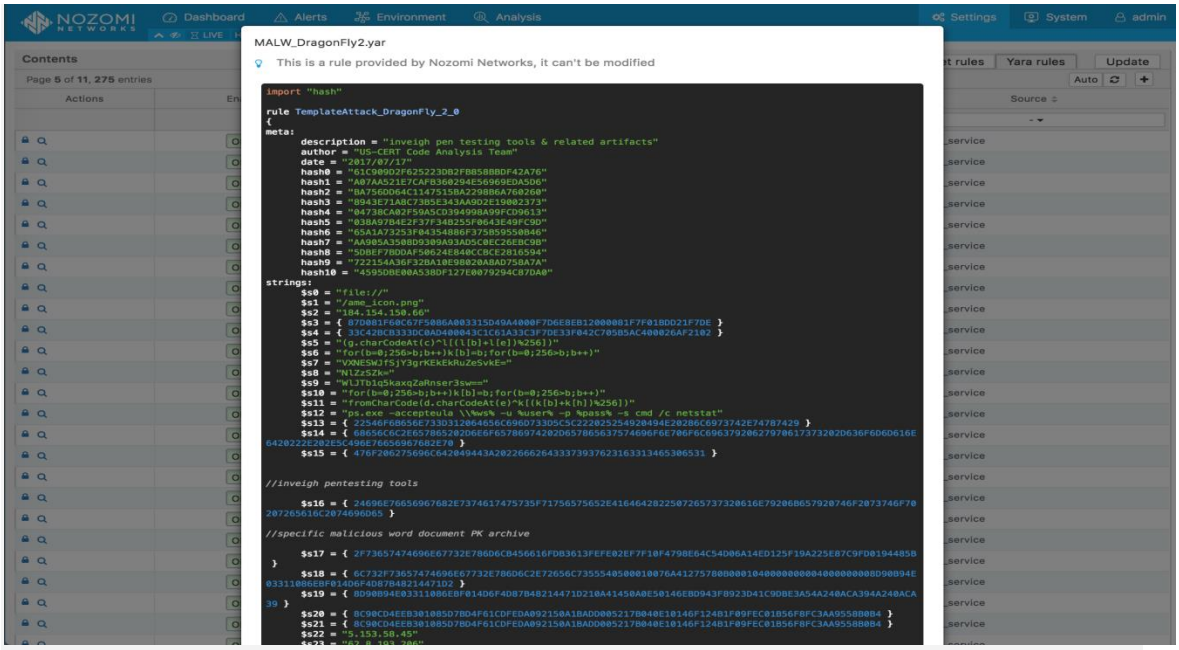


上図は、Nozomi Networks ソリューションがロシアのサイバー攻撃キャンペーンで使用されているような IOC やマルウェアを Nozomi Networks ソリューションではどのように検出するかのしくみを簡略化して示す

YaraRules

YaraRules はマルウェア IOC の存在をチェックする高度なスクリプトのライブラリである。マルウェアに関する複数の IOC をチェックし、手動による脅威検出作業を削減する。グローバルなセキュリティ研究者達のオープンコミュニティによって開発された YaraRules ライブラリは、ナレッジの集合体として技術革新している。

Nozomi Networks SCADAguardian は YaraRules をプラットフォームに組み込み、YaraRules for Dragonfly 2.0 で出荷している。



SCADAguardian ユーザーは、YaraRules を使用して Dragonfly 2.0 の IOC を自動的にチェックすることによりメリットを得ている。

Assertions

アサーションは、デバイス属性、ネットワーク通信、サイバー・リスク、およびプロセス変数のあらゆる側面に関するリアルタイム情報を提供する Nozomi Networks のクエリーツール。クエリーで条件が直ぐに合致するかどうかを確認する間、アサーションを使用して、特定の IOC が存在しないことを定期的にチェックできる。ある時点で見つかった場合に、アラートが生成され、SIEM などの別のセキュリティアプリケーションに送信される。

Nozomi Networks の顧客は効率的に IOC をチェック

” 私は検出した *IOCs* をサイバーセキュリティコミュニティに渡します。だから、瞬時に、問題を特定し、速やかに解決することができます“

Kris Smith, Manager Operations Engineering, Vermont Electric Cooperative

Smith 氏は、Nozomi Networks のクエリーとアサーションを使用して、E-ISAC（電気情報共有分析センター）やその他の情報源を通じて IOC をチェックする方法について説明しています。

Anomaly Detection

異常検出機能は、SCADAguardian のアーキテクチャの基盤であり、通常のネットワークおよびプロセスの動作を学習する機能（機械学習）である。ベースラインが設定され、それらのバリエーションが疑わしいアクティビティの指標となる。ロシアのサイバー攻撃の場合、異常検出は次のような異常動作を検出する:

- SMB プロトコルを使用する外部コマンドおよび制御サーバーなどの不適切な/新しいアウトバウンドの接続
- ネットワーク経由でトラフィックを送信する新しいユーザー
- 異常なトラフィックパターン

ロシアのサイバー攻撃の証跡をシステムで確認しようとする場合は、US-Cert アラートの中で広範なログチェックを行う必要がある。ただし、SCADAguardian を導入すると、異常検出のおかげで多くの作業が自動化される。

ロシアのサイバー攻撃 - 次のステップ

この US-CERT アラートは画期的である。それは、米国のインフラとクリティカルな製造設備がロシアのサイバー攻撃を受けていることをほぼ完璧に掌握したからである。

ある企業組織が標的分野の 1 つになっている場合は、最終的な ICS 攻撃が発生する前にマルウェアをチェックし、撲滅する必要がある。