2015 年 7 月 31 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2015 年 5･6 月号）概要

本概要は、米国土安全保障省の運営する ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）発行の“ICS-CERT Monitor May/June 2015”の概訳となります。内容の詳細につきましては、原文をご参照ください。（※特記が無い限り、本文中のリンク先は全て英語となります）
URL：https://ics-cert.us-cert.gov/monitors/ICS-MM201506

1. インシデント対応活動

（1）直近の事例

ある事業者において、APT（Advanced Persistent Threat）攻撃が OA 系ネットワークから生産ネットワークに侵入拡大した可能性が見つかった。事業者の依頼により、ICS-CERT では攻撃活動が生産ネットワークで行われていないか、また、全体としてのセキュリティ対策状況はどうか、評価を実施した。

現地にオンサイト対応チームおよび評価チームを派遣し、攻撃活動の有無の確認を試みたが、以下の事情等により究明は困難であった。

- 生産ネットワークにどのようなシステムや機器が存在し、どのようなネットワーク構成になっているのか、全体像が不明
- わかっているシステムにおいても、管理責任者が不明など、役割や責任が定められていない
- ネットワーク監視機能がない
- データフォレンジック用のログが適切に取得されておらず、解析ができない
- 物理セキュリティ対策が取られておらず、重要機器についても従業員なら誰でも見つからずにアクセス可能

OA 系ネットワークと生産ネットワークが実質的には分離されていないことなども判明し、ICS-CERT では、資産管理のやり直しや、ネットワークアーキテクチャの検証、監視機能の導入など、セキュリティ対策の抜本的な見直しを推奨した。

（2）ICS-CERT によるセキュリティレビュー

2015 年 5 月、6 月は、3 業界で 17 件のオンサイト評価を実施した。うち 6 件は Cyber Security Evaluation Tool（CSET）によるレビュー、4 件は Design Architecture Review（DAR）によるレビュー、7 件は Network Architecture Verification and Validation（NAVV）によるレビューであった。

- CSET レビュー
  政府基準や業界標準に照らして、組織のセキュリティ対策状況を確認することができるツール「CSET」を使用した汎用的な評価サービス
- DAR レビュー
  設計や構成、相互依存性やアプリケーションなど、組織の制御システムネットワークに特化した、より詳細な評価サービス

- NAVV レビュー
  ネットワークを流れるパケットデータの解析による、機器間の通信フローの洗い出しと見直し

各レビューの詳細は、https://ics-cert.us-cert.gov/Assessments を参照。

2. セキュリティトピックス

(1)インターネットに繋がっているなら、感染していると思え！

産業用制御システム(ICS)は、外部ネットワークから完全に切り離すことで安全性は高くなる。重要インフラの ICS を狙った Black Energy キャンペーンでは、被害に遭った事業者全てにインターネットに直接繋がった ICS 機器が存在し、悪用された。ICS-CERT がインターネットに接続された ICS 機器が存在する旨を通知した組織の殆どは、自分たちの ICS 機器がインターネットからアクセス可能だと気付いてもおらず、そうした機器を探せる SHODAN のようなツールが存在することも知らなかった。更には、ICS 機器は正しく設定され、ベンダによってファイアウォールや VPN 等の適切なセキュリティ対策がなされているものと思い込んでいた。事業者は、ICS へのリモートアクセスを可能な限り禁ずると共に、どうしても必要な場合は VPN など安全な接続方法を使用し、アクセスする機器のセキュリティも確保するほか、アクセスの監視等を行い、不正アクセスの防止と攻撃の検知・対応を可能にすることが求められる。

併せて、以下の実施や活用を検討することが望ましい。

- サイバーセキュリティ責任者を任命し、対策の導入促進や実施に責任を持たせる
- ICS-CERT や標準技術研究所(NIST)が提供するベストプラクティスガイドを活用する
- ICS-CERT のインシデント対応支援サービスや、脅威や攻撃に関する情報共有サービス等を利用する

(2)マルウェア検知ツール YARA の活用

YARA は、マルチプラットフォーム(Windows、Linux、Mac)上で動くオープンソースのマルウェア検知ツールで、元のマルウェアを一部変えて作成されたマルウェアのような、共通のコードを持つ一連のマルウェアを検知することが可能。ICS-CERT のアドバイザリで、YARA ルール(YARA 用の検知情報)を提供することもある[1]。こうしたフリーツールを上手く利用することで、様々なソースから提供されるセキュリティ情報を有効に活用することができる。(※原文では、ICS-CERT が提供した Black Energy(v3)用の YARA ルールを用いた、YARA のインストールおよびマルウェア検査の実行事例あり)

YARA
http://plusvic.github.io/yara/

3. ICS-CERT ニュース

(1)FY2015 中間統計

FY2015 前半(2014 年 10 月～2015 年 4 月)は、108 件のインシデント対応支援を行った。最も多かったのは前年に続きエネルギー業界(27%)、次いで水道(19%)、重要製造業(18%)であった。また、最も多く使われた手口はスピアフィッシング(21%)であった。セキュリティ教育等を通じ、少しでも不審なメール内のリンクや添付ファイルを開かないことの重要性を従業員等に理解してもらい、徹底することが重要となる。

[1] Alert (ICS-ALERT-14-281-01) Ongoing Sophisticated Malware Campaign Compromising ICS
https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-281-01

懸念は、インシデントの報告件数のうち、事業者自身からの報告の少なさである（27%）。殆どのインシデントは、連邦政府関連（45%）や研究者（17%）から報告されている。

報告は任意であるが、事業者が攻撃情報やインシデント情報を ICS-CERT と共有することで、ICS-CERT においてその業界や他の重要インフラ業界の事例を含めた相関分析が可能になる。分析の結果得られた攻撃の傾向、使われた手法やマルウェア、攻撃検知のための情報や対策情報といった有用な情報を事業者にフィードバックすることで、被害の拡大防止やセキュリティ対策の向上につなげることが可能になる。情報共有は匿名であり、共有された情報は Protected Critical Infrastructure Information（PCII）プログラムによって保護される。事業者には是非とも積極的な情報共有をお願いしたい。

（2）Industrial Control Systems Joint Working Group

Industrial Control Systems Joint Working Group（ICSJWG） Spring 2015 Meeting は、2015 年 6 月 23 日～24 日に、ワシントン D.C.で開催され、幅広い議題のもと、プレゼンテーション、パネルディスカッション、デモ等が行われた。次回の ICSHWG Fall 2015 Meeting は 10 月 27 日～29 日にジョージア州サバンナで開催。アジェンダや参加登録などの詳細は、決まり次第以下に掲載予定。

ICSJWG
https://ics-cert.us-cert.gov/Industrial-Control-Systems-Joint-Working-Group-ICSJWG

4. 最近公開された脆弱性

※原文の Recent Product Releases を参照ください。

5. オープンソースニュース（ハイライト）

- 制御システムを標的とした Black Energy、目的は情報窃取か（2015/5/28）
  http://www.darkreading.com/endpoint/data-theft-the-goal-of-blackenergy-attacks-on-industrial-control-systems-researchers-say/d/d-id/1320599?%20%20mc=RSS%20%20DR%20%20EDT&utm%20%20source=dlvr.it&utm%20%20medium=twit

6. 協調的な脆弱性の公開に協力頂いたセキュリティ研究者の方々

ICS-CERT では、発見した脆弱性を一般への公開前にベンダに通知し、パッチや対策版の提供を可能にする「協調的な脆弱性の公開（Coordinated Vulnerability Disclosure）」を奨励しており、そのための仕組みを提供している。様々な事情により困難な場合もあるかもしれないが、是非活用頂き、協調的な公開への協力をお願いしたい。

2015 年 5 月、6 月に協調的な公開に協力頂いた研究者の方々については、原文の Coordinated Vulnerability Disclosure を参照のこと。

7. 今後のイベント

※原文の Upcoming Events を参照ください。

以上