2013 年 7 月 18 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2013 年 4 月/5 月/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 April/May/June 2013”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、全て英文となります）
URL：http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monitor_April-June2013.pdf

1. インシデントレスポンス活動

（1）インターネットに接続された制御システムへのブルートフォース攻撃

2013 年 2 月 22 日、ICS-CERT はあるガス事業者からガスコンプレッサーステーションのプロセス制御システムへのアクセスを試みる攻撃が増加しているとの報告を受けた。ICS-CERT では、US-CERT のセキュアポータルで IP アドレスなど攻撃の特徴となる情報を含めて注意喚起を行い、他の重要インフラ事業者、とりわけ天然ガス業界に対して類似の活動が行われていないか監視するよう呼びかけた。この結果、他の事業者も同様の攻撃を受けていることが判明した。

今回の攻撃はいずれの試みも失敗に終わっているが、これらの攻撃は、重要インフラ事業者が常に警戒を怠らないでいる必要性があることを浮き彫りにした。

ICS-CERTは、重要インフラ事業者に対し、ICS-CERTが公開している注意喚起やアドバイザリ、推奨される対策を参照するよう推奨している。最新情報は ICS-CERT Web site RSS feeds を購読するか、またはTwitterをフォローすることで確認が可能。

（2）最近の活動

直近では、ICS-CERT はエネルギー業界や重要インフラ機器製造業界の事業者に対して、サイバー攻撃による侵入の試みへの対応支援を行った。これらのインシデントには、共通の手法および簡単に入手可能なツールが使用されていた。

ICS-CERT では、US-CERT のセキュアポータルの制御システムセンターを通して、これらのインシデントの詳細を提供している。

- 攻撃手段
- 攻撃者によるツール、戦術、手順（tools, tactics and procedures（TTPs））
- インシデントへの対応を通して学んだ教訓
- 侵入検知および既存のサイバーセキュリティ対策改善のための推奨および軽減施策

ICS-CERT では、サイバーインシデントが報告されることによって新たな攻撃活動を把握でき、対策の改善に繋がるため、インシデントの報告を奨励している。

2013 年上半期（2012 年 10 月～2013 年 3 月）、ICS-CERT は 200 件以上の全重要インフラ分野にわたるインシデントに対応した。最も報告が多かったエネルギー業界が 53%を占め、重要インフラ機器製造業界はこれに続いて 17%であった。また、主な攻撃手法としては、水飲み場型攻撃、SQL インジェクション、スピアフィッシングなどが使われていた。

ICS-CERT が対応するインシデントの多くは、被害を受けた事業者から提供されたマルウェアやログファイル等の分析をリモート対応で行っているが、要望があればオンサイトチームを現場へ派遣している。オンサイト支援の依頼や詳細については ics-cert@hq.dhs.gov まで。

なお、オンサイト対応では、制御システムへの侵入があったかどうかも調査を行ったが、制御ネットワークのログやフォレンジックデータがなく、断定できないことが多かった。

2. 寄稿記事

(1)SCADA 機器への攻撃(トレンドマイクロ社 Kyle Wilhoit 氏)

SCADA システムが実際に攻撃されているのかについては、多くの議論がなされている。トレンドマイクロでは、これらの機器が実際に攻撃されているのか、もし攻撃されているのならばどのくらい攻撃されているのか、調査を行った。結果、恐ろしいことがわかった。それは SCADA 機器への攻撃が行われていたという事実ではなく、インターネットに接続している機器は、どれもいずれ攻撃されるだろうということである。

調査は、水道システムを模した、高対話型(high-interaction)と低対話型(low-interaction)の 2 種類のハニーポットを構築して行った。驚くほど多数の攻撃が検知され、攻撃者が Modbus を理解した上で攻撃していることも確認できた。攻撃のうち 17 件は、壊滅的な結果を招くようなものであった。

これらの攻撃を軽減するためには、SCADA/PLC 機器をインターネットから外し、ファイアウォールを使用してネットワークを分け、堅固なセキュリティ対策を実施する必要がある。

詳細は以下を参照:

http://blog.trendmicro.com/trendlabs-security-intelligence/whos-really-attacking-your-ics-devices/

(2)機器を処分する際はサニタイズ(データを消去)し、情報漏えいを回避せよ

PLC 等の機器は数千ドルするため、調査では中古の機器を購入するが、どの機器も情報の宝庫であり、中古機器の一片から多くの企業情報を得ることができる。数時間のリバースエンジニアリングで、前所有企業の会社名、制御システムのネットワークレイアウト、生産履歴などが入手できるほか、技術者の氏名や連絡先までもが保存されていることもある。悪意のある人物にとっては、これらのデータはソーシャルエンジニアリングやインサイダー取引、企業ネットワークへの直接攻撃などに役立つ。

こうした事態は、機器を処分する前にサニタイズを行い、保存されている機密情報を消去することで予防できる。業者がサニタイズする手段を提供していなければ、業者に送り返してサニタイズして貰うという手もある。制御システムを守るためにできることは多くあるが、機器の適切な処分はその中でも最も低コストで実現できるセキュリティ対策の 1 つである。

3. トピックス

(1)ベライゾン:データ漏えい報告書の概要と分析

ベライゾンでは、2013 年版のデータ漏えいに関する報告を公開した。報告書には、世界中にある 19 の組織から収集した 2012 年度のインシデントデータの分析結果を纏めている。

報告書は過去 9 年間の 2,500 件のインシデントで漏えいした、少なくとも 11 億に及ぶデータに基づいている。2012 年単独でも 47,000 件のインシデンが報告されており、621 件のインシデントで少なくとも 4 千 400 万のデータの漏えいが確認されるなど、データ漏えいが増加している。

報告書は、主に以下の問題について分析している。

- 攻撃者と、使われた攻撃手段の特徴
- 確認された脅威の種類およびスタイル
- 侵入された情報資産
- 侵入されたデータ
- 攻撃対象および攻撃の難易度
- タイムライン
- 発見手段
- 結論および勧告

ベライゾンと Consortium for Cybersecurity Action（CCA)は、有効な対策の検討に関して協力している。成果となる報告書では、万能な解決策は存在しないとしつつ、より一般的でフレキシブルな多層防御を実現するセキュリティ対策を推進している。

以下に検討の成果を示す。

- 脅威が高度化しているといっても、特別に革新的な手法が使われているわけではない。
- 脅威は組織によって異なる。
- トップ 10 中の 7 つの脅威は、「マルウェア関連」に分類される。
- インシデントへの対応処能力は、問題および影響の特定、阻止、軽減において非常に重要である。
- ビジネス機能および可用性を守るため、データ復旧能力は必須である。
- 良く考えられた（設計された）セキュリティ対策とは、各攻撃を 1 対 1 で防止する対策ではく、複数の攻撃に対して効果を発揮するような対策である。
- 予防措置にのみ注力しない。検知も同等に重要であるのに加え、是正施策がより重要である。
- 特定の脆弱性を見つけることに注力したり、特定の攻撃のみをブロックしようとするのでは、初めから負け戦となることが見えている。
- マイクロソフトが提供する脆弱性緩和ツール「Enhanced Mitigation Experience Toolkit（EMET）」は、個別の種類の攻撃でなく、あらゆる種類の攻撃のブロックを試み、セキュリティ対策を対処療法的な事後対策（reactive security）から事前対策（proactive security）にシフトさせ、攻撃者にとっての攻撃のハードル（コスト）を上げることができる。
- 標的型攻撃はコンピュータだけでなく、ユーザを「攻略」するため、頻繁にフィッシング、水飲み場型攻撃等のソーシャルエンジニアリング戦術を使用している。

報告書では、サイバーインシデントの防御、検知、対応には、階層的で継続的なアプローチが必要であると示唆している。1 人の人員や 1 つのグループが組織のサイバーセキュリティに関する責任を負うのではなく、むしろ、サイバーセキュリティは経営陣を含む、全ての従業員の責任であるという文化を組織として育てることが望ましい。

（2）CSET の発展

Cyber Security Evaluation Tool（CSET)はバージョンが 4.1 から 5.0 となり、直観的でわかりやすい言葉を使用した質問へと改善されたほか、基準ごとに同じような質問に繰り返し答える必要をなくし、評価時間を短縮している。将来リリース予定のバージョンでは、ユーザのフィードバックを生かし、評価プロセスの更なるスピードアップや、ユーザが選択した基準とセキュリティレベルでセキュリティプランを生成できるようにするほか、

業界基準への対応や既存の基準のアップデートへの対応等を予定。

より詳しい情報や CSET のダウンロード、またはオンサイト評価に関する問い合わせは、http://ics-cert.us-cert.gov/Assessments を参照するか、または cset@hq.dhs.gov へ。

(3)重要インフラ業界スポットライト: エネルギー分野

今号より本項目を新設し、米国の 16 の重要インフラ業界をそれぞれ紹介していく。

エネルギー業界は、大きく電力、石油、天然ガスの 3 つのセグメントに分けられる。同業界は、他の業界を支える、重要な原動力を供給している。エネルギーなしでは先進国はすぐに機能しなくなってしまう。

米国の 85%以上のエネルギーインフラは民間企業が所有しているが、米連邦政府もエネルギーインフラおよび他の重要インフラを多く所有している。

(4)ICS-CERT ニュース

ICS-CERT が、SC Magazine の「セキュリティ・オブ・ザ・イヤー」に選出される。ICS-CERT ディレクターの Marty Edwards 氏は、「ICS-CERT の非常に素晴らしい働きをとても誇りに思う。受賞は ICS-CERT と、国土安全保障省(DHS)によるサイバーセキュリティのコーディネイションおよび官民情報共有の分野における重要な発展が認められたことを意味する」と述べる。

4. 最近公開された脆弱性

※原文の RECENT PRODUCT RELEASES をご参照ください。

5. オープンソースニュース(ハイライト)

- IOActive、TURCK の制御システム機器におけるバックドアを発見(2013/05/23)
- NIST Special Publication 800-82:制御システムセキュリティの改訂第1版を公開(2013/05/21)
- 制御システム分野における情報共有の発展(2013/05/16)
- 「サイバー犯罪最前線」ラルズセックのハッカー4 人に 32 か月の禁固刑(2013/05/16)
- ハッカーグループ・アノニマス、石油およびガス業界への攻撃を計画(2013/05/16)
- Honeynet Project、一般利用可能な ICS Honeypot を構築(2013/05/15)
- スタックスネット、イランの核開発ポテンシャルを「増大」(2013/05/15)
- SCADA、新しいアルゴリズムでより安全に(2013/05/14)
- 標的型攻撃:新たな現実(2013/05/09)
- 研究者ら、グーグル・オーストラリア本社ビルの制御システムをハッキング(2013/05/06)
- 新しいイスラム過激派雑誌、無人偵察機のハッキング支援を呼びかける(2013/05/06)
- 私の仕事:Marty Edwards, ICS-CERT(2013/05/01)
- サイバー攻撃によるダム崩壊の序曲?(2013/05/01)
- Mozilla、英スパイウェアベンダが同社ブランドを騙ったと非難(2013/05/01)
- ボーイング、制御システムと企業ネットワークを新たなアプローチで接続(2013/04/28)
- システムの不具合により、メリーランド州モントゴメリー郡刑務所で舎房の鍵が開錠される(2013/04/27)
- シリアルポートスキャンによって、インターネットに繋がる 10 万以上のハッキング可能な機器が存在することが判明。信号機システムやビル管理システムの燃料ポンプの制御システム等も含む(2013/04/23)
- Watts Bar 原子力発電所に侵入者。逃走した犯人を連邦政府が徹底捜索中(2013/04/22)

- カナダ、アルカイダに刺激されたテロリストによる列車テロを阻止（2013/04/22）
- 「オーロラ作戦」、目的は人権活動家のアカウントではなく、スパイに対する米国の監視網を調査するための対敵諜報活動（2013/04/22）
- ソーホーのネットワークシステムが狙われる（2013/04/18）
- ICS-CERT、重要インフラ機器製造業者の制御システムのハッキングについて注意喚起（2013/04/09）
- Shodan：インターネット上の最も危険な検索エンジン（2013/04/08）
- カーネギーメロン大学、ジョンズ・ホプキンス大学、手術ロボットのバグを見つけるためのバグ検知ツールを開発。切ってはならないものが切られる前に一見の価値あり（2013/04/08）
- POS システムや ATM を標的とする新しいマルウェアが米主要銀行を攻撃（2013/03/27）
- 韓国の銀行およびメディアのコンピュータネットワークがクラッシュ。北朝鮮が関与か（2013/03/20）
- セキュリティ脆弱性により、政府と契約する企業の機密情報が漏えい（2013/03/19）
- タリン・マニュアル、既存の国際法をオンライン攻撃にも適用できると解釈（2013/03/19）
- 米情報機関、政府にサイバー攻撃の深刻性を警告（2013/03/13）

6. 今後のイベント

※原文の UPCOMING EVENTS をご参照ください。

7. 協調的な脆弱性の公開（CVD）に協力頂いたセキュリティ研究者の方々

※ICS-CERT では、脆弱性を ICS-CERT に報告し、ベンダとの調整に協力くださったセキュリティ研究者の方々に感謝の意を表し、当該研究者の方々の功績として、氏名と対象の脆弱性の一覧を掲載しています。実際の氏名・脆弱性については、原文の COORDINATED VULNERABILITY DISCLOSURE を参照ください。

8. 脆弱性対策に協力頂いたセキュリティ研究者の方々（2013 年）

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT IN 2013

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

J. Alex Halderman	Christopher Sistrunk	Mashahiro Nakada
Aaron Patterson	Dale Peterson	Michael Toecker
Aaron Portnoy	Derek Betker	Nadia Heninger
Adam Crain	Dillion Beresford	Neil Smith
Alexey Osipov	Eric Wustrow	Nicholas Miles
Andrew Brooks	Gleb Gritsa	Postive Technologies Security
Anton Popov	Hisashi Kojima	Reid Wightman
Artem Chaykin	Ilya Karpov	Roman Ilin
Arthur Gervais	Joel Langill	Rubén Santamarta
Billy Rios	Jon Christmas	Ryan Green
Bob Radvanovsky	Juan Vasquez	Sergey Bobrov
Brendan Harris	Jürgen Bilberger	Sergey Gordeychick
Carlos Mario Penagos Hollmann	Justin W. Clarke	Shawn Merdinger
Carsten Eiram	Kuang-Chun Hung (ICST)	Terry McCorkle
Cesar Cerrudo	Lucas Apa	Timur Yunusov
Christopher Scheuring	Luigi Auriemma	Zakir Durumeric

以上