2014 年 10 月 31 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT モニター（2014 年 5 月～8 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 – August 2014”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/sites/default/files/Monitors/ICS-CERT_Monitor_May-Aug2014.pdf

1. インシデントレスポンス活動

（1）上下水道処理施設において汚水槽が溢れる事件が発生

下水道処理施設の運用者から ICS-CERT に対し、メンテナンス要員が少なくとも 4 度、許可なく制御システムにアクセスした見られること、および汚水槽が溢れる事件が発生した旨の報告が為された。オンサイトチームがメンテナンス要員による不正アクセスがあったのか、また、事件と関わりがあるのか調査を行ったが、以下の理由から結論には至ることはできなかった。

- 各ホストで、ログインを記録していない
- 基本的に、ネットワーク全体で 1 つのユーザ名を共用している
- ある行為の有無や真偽を確認できるようなネットワーク監視の仕組みが存在しない
- ホストにインストールされているリモートアクセスツールに関するログが取得されていない、または役に立つログが取られていない
- 報告された不審なアクセスに関する OS の記録が、保存期間超過のため失われている

ログの取得や、ユーザ単位の認証、業務に最低限必要な権限のみに絞ったアクセス制御といった対策の必要性が教訓として示された事例であった。

（2）大手重要製造業者における数ヶ月に及ぶハッキング

大手重要製造業者のシステムが、複数の攻撃犯によって数ヶ月にわたりハッキングされていたことが判明。オンサイトチームが攻撃の存在や痕跡を示す情報（indicators）を用いてネットワークを調べたところ、大量のホストに侵入されていたほか、攻撃犯は複数のドメインアカウント情報を窃取し、特権権限でネットワーク内を自由に動き回っていたという。同社は企業の買収によりネットワークが拡張し、インターネットとの接続点が 100 を超える状態となっていた。

（3）産業制御用システム（ICS）を狙ったマルウェアの発覚

6 月に重要インフラ事業者を狙ったと思われるマルウェアキャンペーンが確認された。使われたマルウェアは Havex または Backdoor.Oldrea と呼ばれるリモートアクセスツール（RAT）で、攻撃経路として、フィッシングメール、マルウェアサイトへのリダイレクトのほか、判明しているだけで 4 社の ICS ソフトウェアベンダが、各社がサイト上で提供しているソフトウェアアップデートインストーラにマルウェアが仕込まれた、いわゆる水飲み場型攻撃が行われた。何か特定の目的を持ったマルウェアである可能性が懸念されていたが、現状、ICS に特化した機能は見つかっていない。

2. ICS-CERT ニュース

(1)フォレンジックに必要な情報の取得と保存の重要性

攻撃や侵入が疑われた場合、フォレンジックに必要な情報を保護し、保存することは、侵入範囲の特定や復旧計画の策定に重要な役割を果たす。先ずは以下のようなことに留意し、必要な情報が必要な時に使えるようにすることが求められる。

- ネットワークログ(トラフィック情報、DNS ログ、ファイアウォールログ、ネットワーク IDS ログ等)を、改ざん防止対策が取られており、バックアップを取得しているシステムに集約して保存する
- フォレンジック時に幅広い情報を提供できるよう、ローカルシステムにおいてもログを取得する
- フォレンジックに有用なデータの保存には十分な容量を確保し、保存期間を長めに設定する

また、攻撃を検知した時には、以下のことに注意する。

- 電源を落とさない(ハードドライブの変更や揮発性メモリの情報が失われる)
- すぐにはネットワークから切り離さない(攻撃者に気付かれ、マルウェアや攻撃の痕跡が消されてしまう)
- ウィルス対策ソフトを実行しない(ファイルのアクセス日などが変更されてしまう)
- レジストリやファイルのクリーンアップツールを実行しない(様々なファイルが変更されてしまう)
- ツールの実行や新たなツールのインストールを行わない(様々なファイルが変更されてしまう)。但し、イメージ化ソフトの実行は例外とする

(2)ICS-CERT によるセキュリティレビュー

ICS-CERT ではオンサイト評価において、Cyber Security Evaluation Tool(CSET)によるレビュー、Design Architecture Review(DAR)、Network Architecture Verification and Validation(NAVV)によるレビューを提供している。

CSET は、組織のセキュリティ対策状況を、国際標準や業界標準、ガイドラインに照らしてレビューできるようにしたフリーツールで、ICS-CERT のサイトからダウンロード可能[1]となっている。自己診断に使えるほか、オンサイトチームがレビューを支援するサービスも行っている。

DAR は、ネットワークアーキテクチャについて階層的防御(defense-in-depth)が取られているかを、境界線防御(perimeter defense)、ゾーニング、セグメンテーション、ICS ネットワーク内および ICS ネットワークと他ネットワーク間の通信フロー等のレビューを行い、相互依存性や脆弱な点がないか確認し、対策を提言する。

NAVV は、ICS ネットワーク内で発生するトラフィックのレビューを行うツールで、機器間の通信を分析し、ネットワークに接続されている全機器の通信の相関関係を洗い出すことで、ネットワークトポロジーの正確さ、通信が本来の設計通りに行われているか、不審な機器や通信が存在しないか等の確認を可能としている。

様々な事業者のレビューで見つかる問題点には、共通するものが多くある(下表)。

[1] https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

レビューにおいて共通して見られる問題点

	カテゴリー	共通して見られる問題点
ゾーニング	境界線防御と境界での対策	デュアルホーム：ICS ネットワークが企業ネットワークと繋がっている（境界線防御が回避されている）
		フラットなネットワーク：ICS ネットワークと企業ネットワークがフラットで、セグメンテーション・境界線防御が為されていない
	ICS 内部のゾーニング	コントロールセンター間にファイアウォールによる対策が取られていない
		ICS ネットワークと企業ネットワークで DMZ が設けられていない
		外部から企業ネットワークに VPN 接続できるため、ICS ネットワークへもアクセス可能となっている（ネットワークセグメンテーションがないため）
		信頼できないネットワークセグメントから、ICS ネットワークにリモートデスクトップで接続している
		ゾーン（ICS ネットワークと企業ネットワーク）間で 1 つの Historian データーベースを共有している
	ゾーンごとの境界での対策	ゾーン間にファイアウォールによる適切な対策が取られていない
		ファイアウォールのルールが弱い（ICS ネットワークへの/からのアクセスが広く許可されている）
		ICS ネットワークから外部に出るデータのフィルタリングやモニタリングがされていない
		ファイアウォールのルールやセキュリティ機器の設定の監査や検証が為されていない
リモートアクセス		モデムバンクが自動応答（auto-answer）に設定されている
		リモートアクセスが二要素認証でない
		セキュリティ機器やスクリーニング機器を回避するアウトバウンドのインターネット接続がある
認証		ユーザーアカウントを共有している
		自動ログインを使用している（無人または安全でない場所にある ICS）
		簡単なシングルサインオンパスワードを使用している
		L2 ネットワーク機器のポートセキュリティに制限があり、MAC フィルタリングもされていない
装置・電子媒体対策		同じワークステーション／ノート型 PC を、企業ネットワーク、ICS ネットワーク両方で使っている
		媒体の使用を制限していない
		ディスクを暗号化していない
監視		侵入検知システム（IDS）がない
		IDS の設置場所が適切でない（暗号化通信や帯域外の通信を使った攻撃を検知できない可能性）
		ICS ネットワークにおけるデータおよびトラフィックフローのベースラインを把握していない
		外部に出る通信の監視やフィルタリングを行っていない
		ICS ネットワーク内で発生するイベントのログが取られていない

事業者は米国の重要インフラをサイバー攻撃から守るため、セキュリティ対策を ICS の運用に必須なものと認識し、必要な投資および対策を行うことが急務となる。

（3）ウェブベースの ICS トレーニングを提供

ICS-CERT では、ウェブベースの ICS トレーニングコースとなる「Cybersecurity for Industrial Control Systems（201W）」を提供している。同コースは、講義形態で提供されている「初級コース（101）」「中級コース（201）」の e ラーニング版となっており、従来に比べて以下のメリットがある。

- 自身のスケジュール、ペースに合わせて受講が可能
- 元のコースの受講内容の冗長を見直し、より効率的に学習できるよう改訂

- 受講地への移動の手間やコストが不要

アカウントの作成・受講は、https://ics-cert-training.inl.gov/ から可能。

3. 最近公開された脆弱性

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

4. オープンソースニュース(ハイライト)

- 研究者ら、信号機のハッキングが非常に容易なことを示す(2014/8/20)
- 原子力規制機関が外国によりハッキングされた可能性(2014/8/18)
- エネルギー業界、増加するサイバー攻撃に警戒を強める(2014/7/15)
- 70%の重要インフラ事業者が昨年度サイバー攻撃により侵入を受けたと回答(2014/7/11)
- ICS を標的にしていたとされる Havex マルウェアの狙い、依然として不明(2014/7/7)
- ICS-CERT、ICS を標的とするマルウェアの発見を受け、重要インフラ事業者に警戒を呼び掛け(2014/7/2)
- OpenSSL、コードおよびコード管理の改善に向けたロードマップを発表(2014/7/1)
- 石油・ガス会社、ソフトウェアアップデートに仕込まれたマルウェアによりハッキングされる(2014/6/30)
- ロシアのハッカーら、石油・ガス会社を狙いサイバー攻撃(2014/6/30)
- 現在進行中のマルウェアキャンペーン、攻撃者らによる米エネルギー産業の妨害を可能に(2014/6/30)
- 石油・ガス業界が新たな ISAC を立ち上げ(2014/6/27)
- Stuxnet が発見された日を前に、新たな SCADA への攻撃が発見される(2014/6/26)
- モンタナ州の保健局がハッキングされる(2014/6/25)
- 連邦エネルギー規制委員会(FERC)、北米電力信頼度協議会(NERC)の 3 基準を承認(2014/6/19)
- ファイア・アイとマンディアント、ICS 市場に進出(2014/6/18)
- 軍が考える制御システムの可視化(2014/6/11)
- NIST SP800-82 産業用制御システム(ICS)セキュリティ(ドラフト)(第 2 版)(2014/5/14)
- 米エネルギー省(DOE)、電力網のサイバーセキュリティに関するガイドを公開(2014/4/28)
- 政府と業界、航空管制システムに対するサイバー攻撃対策に連携して取組み(2014/4/25)
- 重要インフラにおける Heartbleed の影響とは(2014/4/23)
- 米国土安全保障省(DHS)、油田のサイバーセキュリティ対策を促す(2014/4/23)
- 米政府・電力業界幹部、議会において物理攻撃・サイバー攻撃に対する米国電力網の脆弱さについて懸念を訴える(2014/4/16)
- 保険業界による調査、サイバー脅威が重要インフラにシフトしていることを示す(2014/4/9)
- 保険大手ウィリス、エネルギー業界に対して大惨事につながるサイバー攻撃が行われるのは時間の問題と予測(2014/4/8)

5. 今後のイベント

※原文の UPCOMING EVENTS をご参照ください。

6. 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。

7. 脆弱性対策に協力頂いたセキュリティ研究者の方々

RESEARCHERS CURRENTLY WORKING WITH ICS-CERT

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

Adam Crain	Dmitry Serebryannikov	Lucas Apa
Alain Homewood	Eireann Leverett	Martin Jartelius
Alexander Tlyapov	Eric Forner`	Matthew Luallen
Alexey Osipov	Eric Wustrow	Neel Mehta
Andrea Micalizzi	Gleb Gritsai	Ng Yi Teng
Arnaud Ebalard	Ho Ping Hou	Ralf Spenneberg
Aivar Liimets	Ilya Karpov	Reid Wightman
Billy Rios	Jared Bird	Ryan Lee
Bob Radvanovsky	J. Alex Halderman	Sergey Gordeychick
Carlos Mario Penagos Hollmann	Joel Langill	Seyed Dawood Sajjadi Torshizi
Carsten Eiram	Joel Sevilleja Febrer	Shawn Merdinger
Cecil Unuver	John Leitch	Stephen Dunlap
Cesar Cerrudo	Juan Vasquez	Terry McCorkle
Chris Sistrunk	Kirill Nesterov	Timur Yunusov
Dmitry Nagibin	Ling Toh Koh	Wei Gao

以上