2012 年 11 月 12 日
独立行政法人情報処理推進機構（IPA）

ICS-CERT マンスリー・モニター（2012 年 9 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 Monthly Monitor September 2012”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。（※本文中のリンク先は、全て英文となります）
URL：http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Sep2012.pdf

1. Shamoon

（1）Shamoon について

Shamoon ウィルスは、システム破壊モジュールを持つ情報窃取型マルウェアである。シマンテックが 2012 年 8 月 16 日に最初に発見し、同社およびカスペルスキー・ラボ、Seculert がレポートを公開している。Shamoon は、感染すると、ネットワーク上の他の機器へと感染を拡げる。その後、情報の収集を終えると、マスター・ブート・レコード（MBR）、パーティションテーブル、ファイルなどをランダムデータで上書きし、使用不能にする。調査の結果、Shamoon は特に制御システムを標的として作られたものではないと見られるが、破壊力を持つこともあり、制御システムの所有者および運用者は、一般の業務ネットワークが Shamoon に感染した場合に感染が制御システムネットワークに拡がらないよう、制御システムネットワークのセキュリティを固めておくべきである。

シマンテックによれば、Shamoon は 3 つの基本的な機能要素から構成されている。

1. Dropper：核となるモジュール。最初にコンピュータを感染させ、他のモジュールをインストールする
2. Wiper：破壊機能を担うモジュール
3. Reporter：攻撃者への情報送信を担うモジュール

カスペルスキー・ラボによれば、Shamoon は特定の時刻になると破壊モジュールが機動する時限装置が組み込まれており、その後のレポートでは、Saudi Aramco の業務ネットワークの大部分を使用不能にしたのは Shamoon であった可能性が非常に高いとしている。
感染経路は未だ確定されていないが、リムーバブルメディアの使用および内部脅威のリスクを浮き彫りにしたと言える。
業務ネットワークに限られていたとは言え、Saudi Aramco の損害は大きく、同様の破壊攻撃は制御システムでも起きていたかもしれない。

（2） 対策

- 重要なファイルは、ネットワーク上で共有し、バックアップを可能にする
- 全ての重要システムについて、日次バックアップを実施する
- 重要ファイルを、リムーバブルメディアなどのオフライン媒体に定期的にバックアップする
- ネットワークリソースが使用できなくなった場合のため、緊急通信手段を確保しておく
- 重要なネットワーク（制御システム運用ネットワークを含む）は全て、業務ネットワークから分離する

- 重要システムを特定し、有事にサービスを迅速に復旧するために、予備品を確保しておく必要性の有無を検討する
- ウイルス対策ソフトは常に最新の状態に更新しておく。亜種は検知できないという報告もあるが、それでも、ウイルス定義ファイルの更新は必須となる
- 重要ネットワークおよびシステムへの物理的、電子的なアクセス制御を見直す。制御システム環境におけるリムーバブルメディアの使用を制限することは特に大事
- 実行ファイルがネットワーク上やリムーバブルドライブ上で自動的に実行されないよう、自動実行（AutoRun）機能を無効化する。また、不要時にはリムーバブルドライブは取り外しておく。書き込み権限が必要でなく、読み取り権限のみの設定が出来るのであれば、読み取りのみにする
- パッチは常に最新のものが適用されているようにする。ファイアウォールを通して公共サービス（HTTP、FTP、電子メール、DNS サービスなど）を提供するコンピュータについては特に注意する
- 制御システム機器のネットワークへの接続を最低限に絞り込む [1]。制御システム機器は、直接インターネットに接続しない
- 制御システムネットワークをファイアウォールで守る。また、業務ネットワークから隔離する
- リモートからのアクセスが必要な場合、VPN などセキュアな手段を用いる。但し、VPN のセキュリティの強度は、接続機器のセキュリティの高さ（弱さ）に準じることを理解したうえで検討する

他に、ICS-CERTのJSAR-12-241-01B-Shamoon/DistTrack Malware [2]、およびICS-TIP-12-146-01A Cyber Intrusion Mitigation Strategiesを参照。また、US-CERTウェブサイト上で提供しているImproving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategiesも参照のこと。

2. 今月のトピックス

（1） ICS-CERT、CVE 採番機関（CNA）に

2012 年 6 月 1 日、ICS-CERT は、CVE 採番機関として正式に MITRE に任命され、ICS-CERT に届け出があった脆弱性に直接 CVE 番号を付番できるようになった。

（2） スマートグリッドの進化によって、電力の不正使用の検知、リスクの低減が可能に

電力供給システムにおける負荷の監視は、機器やシステムの過負荷、ひいては停電を避けるためにも非常に重要である。今夏のインドにおける大規模停電の事例では、電力の不正使用と過負荷が引き起こす問題が浮き彫りとなった。スマートグリッドの促進により、電力の不正使用の防止や正確な需要の把握が可能になりつつあるが、一方で、スマートメータを不正に使用する方法も同じように進化している。Black Hat などのカンファレンスでは、米国で展開中のスマートメータの脆弱性等も発表されている。

（3） 8月の訓練プログラム

歴史的に、産業制御システム（ICS）はインターネットからは隔離されていた。この産業制御システムの領域と情報技術（IT）の領域が融和することにより、これまでは制御システムのデータを取得するには多数の情報源からのデータの照合が必要であったのが、一瞬のうちに取得できるようになったほか、離れた場所から監視することなどができるようになった。接続性の向上は、こうした利点をもたらした一方で、制御システムの領域に深刻な脆弱性をもたらすことにもなった。

---

1 IPA にて抄訳を公開しています。http://www.ipa.go.jp/security/controlsystem/pdf/InternetAccesibility.pdf

2 IPA にて抄訳を公開しています。http://www.ipa.go.jp/security/controlsystem/pdf/JSAR-12-241-01B.pdf

ICS-CERT では、制御システムの所有者、運用者、ベンダに対し、制御システムの脆弱性に関する意識向上と対策についての訓練プログラムを提供しており、懸念事項について相談したり、関係者と知り合ったり、知識を高める場としても活用されている。
この 8 月の訓練には軍の様々な施設から 61 人が参加した。また、アトランタで開催された Government Forum on Incident Response Security Teams（GFIRST）では、「制御システムサイバーセキュリティ＜入門編＞」「制御システムのサイバーセキュリティ＜中級編＞」といったプレゼンテーションを行った。

3. 8月のインシデントレスポンス活動

ICS-CERT では、8 月にエネルギー業界、水道業界、IT 業界で計 5 件のオンサイト・インシデント対応を行った。各案件において、「NIST SP800-82：産業制御システムセキュリティ」、「NIST SP800-53：連邦政府情報システムにおける推奨セキュリティ管理策」、包括的なアーキテクチャおよび個々の取組みの評価を行った。全体的な評価結果として、外部ネットワークとの相互接続における多層防御戦略の導入の必要性や、よりセキュアなシステムへの移行の検討などを話し合った。

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. 今月のオープンソースニュース（ハイライト）

- カタール第 2 位の大手天然ガス開発会社 RasGos、サイバー攻撃により業務システムがダウン（2012/8/30）
- インド政府、中国製ネットワークインフラ機器の購入制限を検討（2012/8/30）
- Java のゼロデイ脆弱性、攻撃コードも公開され、より悪用が活発に（2012/8/28）
- 世界最大の石油会社 Saudi Aramco に対するサイバー攻撃、30,000 台を感染させたという犯行声明の内容について、Aramco 幹部が肯定と取れる発言（2012/8/27）
- ハッカー集団ラルズセックの元リーダー・Sabu、当局に協力した見返りに 6 ヶ月の判決延期を得る（2012/8/22）
- 米政府、シーメンス製品の脆弱性に関する報告を調査（2012/8/22）
- 米国家情報長官、連邦政府機関と情報機関の間でテロ関連情報の共有がなかなか進まない状況を報告（2012/8/17）
- Stuxnet、Flame に連なるとされるマルウェア Gauss、標的はレバノンの銀行の顧客か（2012/8/9）
- 米国防総省、現状防衛面でのみ許されたサイバー軍事力の行使に関して、攻撃面への権限拡張を狙う（2012/8/9）
- カスペルスキー社、独自のセキュアな制御システム向け OS の開発を目指す（2012/8/7）
- イラン、インターネットを介したサイバー攻撃から守るため、来月にも中央や州の主要省庁をインターネットから切り離す予定（2012/8/5）
- 米エネルギー省と国土安全保障省、電力業界における、セキュリティと予算に合った合理的な対策の導入を支援するための導入モデル（DOE Electricity Subsector Cybersecurity Capability Maturity Model）を紹介（2012/8/2）
- Industrial Control Systems Joint Working Group（ICSJWG）、制御システム業界における脆弱性情報公開方法の標準化を図るフレームワーク、“Industrial Control Systems Common Vulnerability Disclosure Framework”を公開（2012/8/2）

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(CVM)に協力頂いたセキュリティ研究者の方々(2012 年 8 月)

※原文の NOTABLE COORDINATED DISCLOSURE RESEARCHERS IN AUGUST 2012 をご参照ください。

以上