2012 年 9 月 5 日

独立行政法人情報処理推進機構(IPA)

ICS-CERT/US-CERT Joint Security Awareness Report
JSRA-12-222-01-情報窃取型マルウェア「Gauss(ガウス)」

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)と US-CERT(United States Computer Emergency Readiness Team)が発行する、"JSAR-12-222-01-Gauss Information-Stealing Malware)"の抄訳となります。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/JSAR-12-222-01.pdf

概要

セキュリティベンダ・カスペルスキー社は、2012 年 8 月 9 日に、同社が発見し"Gauss(ガウス)"と命名した新しい情報窃取型マルウェアについて公表した。

カスペルスキー社のレポートによれば、ガウスは主にレバノン、パレスチナ領、イスラエルで確認されているが、影響については判明していない。また、米国でも限られた件数ながら感染が確認されているが、現状、ガウスが制御システムや米国政府機関を標的としていると断じる証拠は挙がっていない。

ガウスは、スタックスネットと同じ「.LNK」の脆弱性(CVE-2010-2568)を悪用しているほか、モジュールの 1 つに暗号化されたペイロードが含まれている(機能は不明)。

確認されているガウスの機能は以下:

- 様々なブラウザに自身のモジュールのコピーを埋め込み、セッション情報、パスワード、クッキー、閲覧履歴などの情報を取得する
- ネットワーク接続に関する情報を収集する
- プロセスやフォルダに関する情報を収集する
- BIOS や CMOS RAM に関する情報を収集する
- ローカルドライブ、ネットワークドライブ、リムーバブルドライブに関する情報を収集する
- 他のコンピュータの情報を盗むため、リムーバブルメディアを情報窃取型マルウェアに感染させる
- "Palida Narrow"という独自フォントをインストールする(目的は不明)
- ツールキットを読み込み、利用できるようにする
- C&C サーバと通信を行い、収集した情報の送信、および追加モジュールのダウンロードを行う

対策

現時点では具体的な対策方法はない。カスペルスキー社がガウスの分析情報を公開しているので、利用できる情報を使って対策を行うことが望ましい。

また、ICS-CERT と US-CERT では、以下を行うことを奨励する。なお、実際に対策を行う前に、影響分析とリスク評価を行うこと。

- ガウスの感染拡大を防ぐため、USB ドライブなどリムーバブルメディアを使用する時には注意する

- Windows Update を行い、脆弱性「CVE-2010-2568」を修正する
- ガウスを検知できるよう、ウィルス定義ファイルを更新する
- 制御システム機器のネットワークへのアクセスポイントを最低限に絞り込む。制御システム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とリモートデバイスは、ファイアウォールで守る。また、企業のビジネス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

なお、サイバーインシデントに遭った場合の検知と復旧に関して、Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies(推奨対策:多層防御戦略による産業制御システムのサイバーセキュリティ改善)も参照可能。

また、「制御システムセキュリティプログラム(CSSP:Control System Security Program)」では、US-CERT ウェブサイト上で、他にも推奨するセキュリティ対策を纏めたドキュメント等も提供しており、こちらも利用可能。

以上