報道関係者各位
（参考資料）

2011 年 10 月 24 日
株式会社インターネットイニシアティブ

IIJ、「マルウェア対策研究人材育成ワークショップ MWS Cup 2011」にて総合優勝

株式会社インターネットイニシアティブ（IIJ、本社：東京都千代田区、代表取締役社長：鈴木 幸一 コード番号：3774 東証第一部）は、2011年10月19～21日に新潟コンベンションセンターで開催された「マルウェア対策研究人材育成ワークショップ（MWS）2011」（※1）のマルウェア解析コンテスト「MWS Cup 2011」にて総合優勝し、10月20日に表彰を受けました。

MWS は、サイバークリーンセンター（※2）等で収集された悪意あるプログラム「マルウェア」の観測データを共通の「研究用データセット」として活用し、対策に関する研究を行うワークショップです。本ワークショップは、情報処理学会の「コンピュータセキュリティシンポジウム（CSS）」と共催で毎年開催され、本年で4回目を迎えます。共通のデータセットを用いた研究成果の共有や切磋琢磨する環境の提供を通して、マルウェアに関する専門知識を備えた研究者や実務者を育成していくことを目的としています。

MWS Cup は、本ワークショップの一環として、研究用データセットを活用したマルウェア対策研究の成果を生かし、一定時間内で課題に取り組み、解析結果を競うコンテストです。技術的な解析の正確性（技術点）と、解析方法の発表（芸術点）により判定を行い、合計点が最も高いチームが総合優勝となります。
今回の「MWS Cup 2011」では、以下の 3 つの課題に取り組みました。

1. **drive-by-download攻撃解析**
   昨年大流行したGumblar等のWeb感染型マルウェアの感染活動に関する解析を実施します。クライアント型ハニーポットの通信データをもとに、攻撃コードの有無、攻撃コードが置かれているWebサイトへ誘導（転送）するWebサイトのURL、攻撃コードが置かれているWebサイトのURL、マルウェアを配布するURLを解析し解答する課題です。
2. ボット感染解析
   標的型攻撃等により、組織内のPCにマルウェアが感染してしまった状況を想定して解析を行います。マルウェアに感染した仮想マシンと感染前後の通信データをもとに、侵入に利用された脆弱性、バックドアポート番号、マルウェアをダウンロードし実行した方法、マルウェアの起動プロセス名、ファイルパスを解析し解答する課題です。
3. **Android**マルウェア解析
   本年話題となっているスマートフォンに感染するマルウェアに関する解析技術を競います。5 個のAndroidアプリをもとに、正常、情報漏えい型、root権限奪取型など特徴を解析し解答する課題です。

今年は、大学や研究者など６チームが参加し競い合った結果、IIJ のセキュリティに関する専門チームであるセキュリティ情報統括室の技術者たちが、総合優勝を勝ち取りました。

（※1）MWS の詳細は、http://www.iwsec.org/mws/2011/about.html をご参照ください。
（※2）ボットネット対策の官民連携プロジェクトサイバークリーンセンターの詳細は、https:/www.ccc.go.jp/ をご参照ください。

＜IIJ セキュリティ情報統括室長　齋藤衛のコメント＞

「今回の優勝を喜ばしく思います。特に、実際に新しい分野であるスマートフォンのマルウェアに関する解析で十分な成果を上げた点は、参加したスタッフの日頃の精進を示すものだと考えています。90 分で結果を出さなければならない MWSCup のような競技は、限られた時間で対策に役立つ情報を抽出しなければならない、実際の対策現場の状況に近い条件で能力を発揮するための訓練として非常に役立ちます。」

最近では、スマートフォンの不正アプリケーションとして流布するマルウェアが増加し、被害が拡大するなど、日々新しい攻撃が発生しています。IIJ では、マルウェア解析技術をさらに高め、さまざまなセキュリティインシデントに対応していくことで、今後ともインターネットの安定運用に尽力してまいります。

報道関係お問い合わせ先
株式会社インターネットイニシアティブ　広報部　川上、富永
TEL：03-5259-6310　FAX：03-5259-6311
E-mail：press@iij.ad.jp　URL：http://www.iij.ad.jp/