# 核施設を攻撃したスタクスネットに類似したマルウェア「Duqu」について～GData

G Data Software株式会社（本社：東京都千代田区、日本支社長：Jag
山本）は、昨年にイランの核施設を攻撃したことで話題になったスタクスネットに類似したコードを持つマルウェア「デューキュー」(Duqu)が新たに発見されたことに対して、単に、今後の次なる産業設備への攻撃だけを警戒すべきではなく、むしろ、一般ユーザーの個人情報を窃取する強力かつ新たな脅威とみなした警戒も必要であることを指摘します。

2010年6月
、スタクスネット（Stuxnet)の出現は、これまでのマルウェア史を大きく塗り替えるものでした。USBメモリを悪用してWindows
OSで動作するコンピュータに侵入し、そのうえで連動している核施設の制御システムの運転に影響を与え、実際に物理的に、遠心分離機が破損するに至ったと言われています。

次いで、2011年10月14日
、すでに各社より発表されています通り、シマンテック社と深いつながりのある研究所が、このスタクスネットにとても似通ったマルウェアを発見しました。

このマルウェアは、作成されるファイル名に「DQ」という文字が含まれることから、「Duqu」（デューキュー）と名付けられました。

デューキューは、大別すると、リモートアクセス型のトロイの木馬（＝RAT）に分類され、感染したコンピュータからの情報を盗み出すキーロガーのコンポーネントを隠し持っているルートキットであり、スタクスネットのような、産業機器の統御にかかわる仕組みは持っていません。

とはいえ、スタクスネットと類似したコードが使用されているので、共通の人物もしくは組織が作成し、攻撃を行う前準備に情報収集を行うことを目的として作成した可能性がある、と指摘するセキュリティベンダーもあります。

しかし、スタクスネットもリバースエンジニアリングにより情報の一部が知られているため、別の人間（もしくは組織）がデューキューを作成した、と考えることも可能です。

そもそも、攻撃側にとって類似したコードを使うことは、このようにベンダー各社や関係機関が注目してしまっては、デメリットのほうが多いと思われます。

いずれにせよ、このような、産業設備を狙うマルウェアはこれからも増加するおそれは十分にあるので、関係機関ならびにその施設の近隣の人々には注意が必要なのは言うまでもありませんが、それのみならず、巧妙なマルウェアの増加により、私たち個人や中小企業における個人情報や機密情報の窃取にも、今まで以上に留意すべきである、とG Dataは考えます。

デューキューの特徴
・RAT（リモートアクセス機能を持つトロイの木馬）
・XP、Vista、7のWindows OSで動作
・ネットワーク情報を盗み出すのが目的

・OSシステム
・クライアント
・インストール済みのソフトウェア
・SCADA（監視制御システム）環境
・自己消去機能により36日後に消滅
・G Dataは、Rootkit.Duqu.A、Trojan.Generic.6742310として検知

ジーデータソフトウェアとは
G Data Softwareは、1985年に創業し、1987年に世界最初の個人向けウイルス対策ソフトを発売した、ドイツのセキュリティソフトウェア会社です。
EUを中心に、個人向け・法人向け製品を展開しています。日本法人は2007年に設立しました。最大の特徴は、ダブルエンジンによる世界最高位のウイルス検出率です。また、新種や未知ウイルスへの防御、フィッシング対策、迷惑メールへの外国語フィルターなど、インターネットやメール環境を安全・快適にする機能を豊富に搭載しています。その結果G Dataのセキュリティ製品群は、マルウェアやフィッシング詐欺サイトを常に高検出することに定評があり、過去5年間以上にわたって、第三者機関・雑誌における受賞獲得数は他社の追随を許しません。2011年にはアンドロイド端末向けのセキュリティアプリも発売しました。

＊本リリースに記載されている各種名称、会社名、商品名などは各社の商標または登録商標です。

【本リリースに関する問合せ先】
G Data Software株式会社
101-0042 東京都千代田区神田東松下町48 ヤマダビル6F
窓口： 瀧本往人
E-mail: gdata_japan_info@gdatasoftware.com
URL： http://www.gdata.co.jp/

---

Generated by ぷれりりプレスリリース
https://www.prerele.com