ボットネット キャンペーンの分析
実態と数字

FORCEPOINT™ SECURITY LABS™

JAKU

国別 JAKU 被害上位 5 位

韓国 — 日本 — 中国 — 台湾 — 米国

平均滞留時間
93 日

最長滞留時間
348 日

被害者の所在地：
世界各地
（日本と韓国、中国に大半が集中）

ペイロードの配信方法：
侵害された BITTORRENT サイト、ライセンス許諾のないソフトウェアの使用、WAREZ ソフトウェアのダウンロード

マルウェア タイプ:
多層追跡およびデータ不正転送マルウェア

コマンド・コントロール サーバーの場所
マレーシアおよびタイ、シンガポール

JAKU 被害者が存在する国の数
134

被害者総数
19,000

使用される回避テクニック:
暗号化、ステガノグラフィー、偽のファイル タイプ、ステルス攻撃、アンチウィルス エンジン検出、その他

現時時点での調査期間:
6 か月

FORCEPOINT
POWERED BY Raytheon

恐れることなくビジネスを前進

JAKUは特定の個人を標的に

JAKU とは、現在 Forcepoint Security Labs の特別調査チームが調査しているボットネット キャンペーンの呼び名です。JAKU の特徴は、何千ものボットネット被害の中でも特定の個人のみを厳選して狙い攻撃するという点です。標的となっているのは、国際的な非政府組織（NGO）やエンジニアリング関連企業の関係者、研究者、科学者、政府関係者です。こうした個人の共通点は北朝鮮（DPRK）または平壌に何らかの関連があることです。

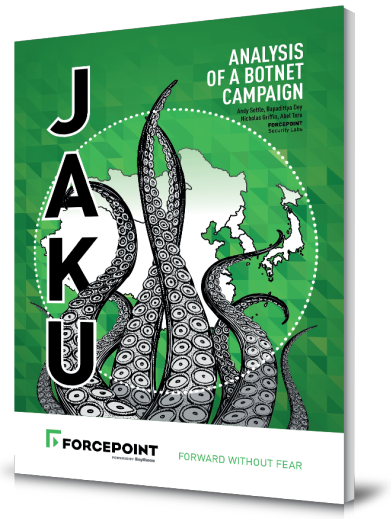
JAKU の被害は主に「危険な」BitTorrent ファイルの共有を通じて起こっています（被害件数は重複を除き控えめに見積もっても 19,000 件）。被害は世界中で報告されていますが、その大多数は韓国と日本です。Forcepoint Security Labs では、ボットネット コマンド & コントロール（C2）サーバがシンガポール、マレーシア、タイを含むアジア太平洋地域にもあるということを突き止めています。

高度なボットネット キャンペーン

JAKU は 3 種の C2 メカニズムを使用しているため、回復力に優れています。画像ファイルに埋め込まれた圧縮暗号コードを使用してマルウェアに二次感染させる一方で、難読化された SQLite データベースを介してボットネット感染者を監視します。また、UDT ネットワーク トランスポート プロトコルなど広く出回っているオープン ソース ソフトウェアや朝鮮語ブログ サイトからコピーしたソフトウェア、公開済みコードの書き換えなどを巧みに再使用しています。

JAKU ボットネット キャンペーンの黒幕は？

Forcepoint Security Labs では、意図の把握と理解に全力で取り組んでいます。そうすれば今後の行動を特定することができます。特定の属性に注目しているわけではありませんが、現在特定されているマルウェアの作成者は朝鮮語を母国語とする人物であるということを示唆するサインが確認されています。



JAKU ボットネット キャンペーンの詳細については、レポート（www.forcepoint.com/jaku からダウンロード）をご覧ください

FORCEPOINT
POWERED BY Raytheon

恐れることなくビジネスを前進