＊本資料は、2014 年 4 月 29 日に米国で発表されたプレスリリースを翻訳したものです。

報道関係各位

2014 年 5 月 7 日
アーバーネットワークス株式会社

Arbor Networks がかつてないスパイク状態を報告、NTP を悪用した DDoS 攻撃の増加

- *2014 年第 1 四半期最大の攻撃、325 GB/秒*
- *第 1 四半期に 100 GB/秒 を超える攻撃が 72 回*
- *2014 年第 1 四半期だけで、20 GB/秒超の攻撃が 2013 年全体比の 1.5 倍*

米国マサチューセッツ州バーリントン－エンタープライズやサービス・プロバイダのネットワーク向けに分散型サービス拒否（DDoS）攻撃や高度な脅威の対策ソリューションを提供するリーディング・プロバイダ Arbor Networks, Inc.（以下「Arbor Networks」）は、本日、インターネット脅威監視インフラ ATLAS から取得したグローバル DDoS 攻撃データを公開しました。このデータは、DNS 反射/増幅攻撃の蔓延により、スパイクがかつてないレベルで発生していることを示しています。

NTP は、ネットワークを通じてコンピュータの時刻を正しい現在時刻と同期させる UDP ベースのプロトコルです。DNS、SNMP、NTP、chargen、RADIUS を含む UDP ベースのサービスは、プロトコルがコネクションレスであり、基本的なスプーフィング防止措置が適用されていないネットワークにある感染ホストや「ボット化された」ホストをコントロールする攻撃者にソース IP アドレスがスプーフィングされる可能性があるため、DDoS 攻撃の潜在的ベクトルなのです。なかでも NTP は、およそ 1000 倍という増幅率の高さから標的にされやすくなっています。さらに、攻撃ツールが簡単に入手できるようになったことが、攻撃実行を容易にしています。

ATLAS は、Arbor Networks と匿名のトラフィック・データを共有している 300 社近いサービス・プロバイダ顧客との協力的提携関係に基づくシステムで、グローバルなトラフィックと脅威に関する包括的かつ集約的な見識を提供しています。ATLAS は 80TB/秒のトラフィックを収集し、Google Ideas が構築したグローバルな攻撃トラフィックを可視化するデジタル アタック マップにデータを提供しています。

NTP 攻撃のハイライト

- 2013 年 11 月の世界の NTP 攻撃は平均 1.29GB/秒、2014 年 2 月は 351.64GB/秒に激増
- NTP 攻撃は DDoS イベントの 14% だったが、10GB/秒を超える攻撃がイベントの 56%、100GB/秒超は 84.7%に
- 攻撃の主な対象国は米国、フランス、オーストラリア
- 大規模攻撃の主な対象国は米国とフランス

Arbor Networks のソリューション・アーキテクト、Darren Anstee (ダレン・アンスティー) は、「Arbor は、2000 年以降 DDoS 攻撃を監視し、その対策に取り組んできました。2014 年現在、スパイクの規模そして大規模攻撃の発生頻度は前代未聞の状態です。攻撃規模は拡大し、ISP からエンタープライズまであらゆるインターネットインフラに深刻な脅威を与えています」と述べています。

NTP リソース:
Arbor Networks では、急増する NTP 攻撃に関する広範なデータや研究、分析、ベスト プラクティスを提供しています。

- **ウェビナー**:Too Much Time on My Hands: Network Scale Mitigation of NTP DDoS Attacks (英語)
- **Arbor セキュリティ・エンジニアリングおよびレスポンス・チーム (ASERT)**:Threat Intel Brief (英語)
- **ブログ記事:***NTP Attacks: Welcome to The Hockey Stick Era*、*NTP attacks continue – a quick look at traffic over the past few months* 、*The Danger of the Latest NTP Attacks (英語)*

Arbor Networks について
Arbor Networks は DDoS 攻撃や高度化する脅威から世界の大手企業および大手サービス・プロバイダのネットワークを安全に守ることを支援しています。Arbor Networks は全世界のエンタープライズ、キャリア、モバイルの市場において DDoS 保護ソリューションを提供する世界をリードする主要ソリューションプロバイダです（Infonetics Research 社調べ）。高度化する脅威に対する Arbor Networks のソリューションは、パケットキャプチャと NetFlow 技術を組み合わせることで、ネットワーク全体を可視性し、マルウェアや悪意のあるインサイダーの脅威を迅速に検出し、削除することを可能にします。Arbor Networks はまた、動的なインシデント対応、履歴分析、視認性、フォレンジクスについても市場をリードする分析機能を提供しています。Arbor Networks は、企業のネットワークやセキュリティの担当者がセキュリティのエキスパートになり、企業のセキュリティ強化を実現することを目指しています。Arbor Networks の目標は、お客様がセキュリティ問題を迅速に解決し、事業リスクを低減できるよう、ネットワーク上の脅威の視認性とセキュリティ・インテリジェンスの提供を可能することです。

Arbor Networks の製品およびサービスについて詳しく知りたい方は、Arbor Networks の日本語サイト www.arbornetworks.com/jp/ を参照してください。また、業界唯一の革新的なインターネット監視システム ATLAS®のデータに基づく調査、分析および知見については、ATLAS セキュリティポータル（英文）をご覧ください。