報道関係各位

2020 年 8 月 20 日
アルプス システム インテグレーション株式会社
国立大学法人 横浜国立大学

ALSI、横浜国立大学の独自ハニーポットシステムによって新たに発見可能となった脅威対策データの提供を 8 月 20 日から受け、サイバー攻撃対策の確実性を向上

～セキュリティインシデントの発生を未然に防ぐ～

アルプス システム インテグレーション株式会社（本社：東京都大田区、代表取締役社長：永倉 仁哉、以下 ALSI〔アルシー〕）と、国立大学法人 横浜国立大学（神奈川県横浜市、学長：長谷部 勇一）は、サイバー攻撃対策の確実性向上のために、横浜国立大学 独自のハニーポットシステムにより検知された情報セキュリティ脅威対策データを ALSI が提供する Web フィルタリング製品のデータベースで利用できるように協力し、データの受け渡しを 2020 年8月20日より開始することを発表いたします。

■概要

提供開始日	2020 年 8 月 20 日より提供開始。 ALSI の Web フィルタリング製品へは順次提供
ターゲット	企業、教育機関、官公庁、自治体、金融機関など
詳細情報 URL	https://www.alsi.co.jp/security/

■独自のハニーポットシステムによる脅威対策データの検知

インターネット上の不正行為によって発生する情報漏洩やシステムへの攻撃によるダメージ発生などの対策として、不正行為の検知や攻撃観測などを行うために、ハニーポット環境を用意して検知し脅威対策データとしています。しかし、攻撃パターンの複雑化や生存期間の短いマルウェアの出現などで、従来のハニーポットシステムでは、検知できない脅威が増えています。

横浜国立大学大学院環境情報研究院／先端科学高等研究院の吉岡准教授は、実環境での攻撃を観測する目的の IoT 機器を利用したハニーポットと、多くの攻撃を観測する目的の仮想環境を利用したハニーポットを新たに開発、これらの組み合わせにより従来のシステムでは観測が困難であった不正リクエストの観測、検知を可能にし、より広範囲で即時性の高い脅威対策データの提供が可能となりました。

■新たに発見可能となった脅威対策データのフィルタリングシステムへの提供

ALSI では、吉岡准教授の協力を得て、先進的なハニーポットシステムにて観測、検知された脅威対策データの供給を受け、ALSI 提供のフィルタリングシステムへ提供することで、フィルタリングユーザーのマルウェア感染を防ぐほか、すでに感染している PC からの通信もブロックすることで、情報漏洩の被害を未然に防ぎます。今回提供を受けるデータは、従来の方式に比べて、月間で 2,300 件以上が新規に発見されており、より確実な対応が実施されることで、フィルタリングユーザーは、これまで以上にインターネット上の脅威から守られることになります。

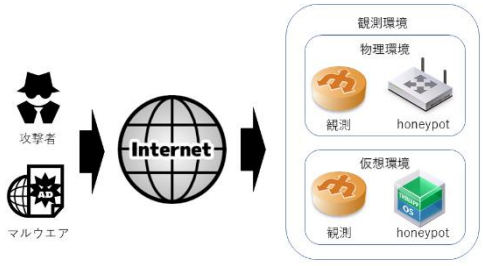
■先進的なハニーポットシステムの概要

（1）物理環境による実環境での攻撃検知

複数の IoT 機器を利用し、大量の IP アドレスを使用した観測活動を実現しています。これにより多様な実環境を持つことで、いままでは検知できなかった攻撃を検知できるようになりました。

（2）仮想環境によるより多くの攻撃検知

仮想環境による大量のポート番号での待ち受けを行い、かつ、通信に対する適切な応答を返す事により、一般的なポート以外のポート(High ポート)などへの攻撃の観測に成功しています。



本システムは、国立研究開発法人情報通信研究機構（NICT）委託研究の「Web 媒介型攻撃対策技術の実用化に向けた研究開発」による吉岡克成准教授の研究成果です。Telnet や HTTP などのプロトコルを利用し攻撃対象への侵入を試み、マルウェアのダウンロードを行い感染する活動や、その攻撃を隠蔽するために生存期間が短いダウンロードサイトを利用した感染活動など、過去に検出困難であった活動が本研究で観測されるようになりました。また危険性が非常に高いリモートからコマンドを実行させる攻撃も観測されており、このような攻撃により利用者の PC が Bot などのマルウェアに感染し、Bot ネットワークが構成され攻撃に加担させられるリスクが高まっています。

これらの攻撃への対策としては、本システムのようなハニーポットで観測された新しい情報を Web フィルタリングのようなセキュリティ対策製品へ迅速に情報適用する事が重要となります。

【吉岡克成　准教授】

横浜国立大学　大学院環境情報研究院／先端科学高等研究院　准教授。サイバーセキュリティ、特に IoT におけるサイバー攻撃の観測や対策に取り組む。総務省　サイバーセキュリティタスクフォース等、政府有識者委員を多数務める。2009 年に科学技術分野の文部科学大臣表彰科学技術賞、2016 年に産学官連携功労者表彰総務大臣賞、2017 年に情報セキュリティ文化賞を受賞。

【製品に関するお問い合わせ・取材受付先】
アルプス システム インテグレーション株式会社　管理部　経営企画課　広報担当　黒澤　宏子
TEL：03-5499-8043 / FAX：03-3726-7050 / E-mail：　hiroko.kurosawa@alsi.co.jp
〒145-0067 東京都大田区雪谷大塚町 1-7　　URL：　https://www.alsi.co.jp/

【研究内容に関するお問い合わせ・取材受付先】
横浜国立大学　大学院環境情報研究院/先端科学高等研究院　准教授　吉岡克成
TEL：045-339-3690/ E-mail：　yoshioka-katsunari-cx@ynu.ac.jp