News Release

報道関係者各位

ニュースリリース

平成30年7月26日

株式会社サイバーセキュリティクラウド

GPONルータを狙うサイバー攻撃の急増を日本国内でも観測
サイバーセキュリティクラウド

株式会社サイバーセキュリティクラウド（本社：東京都渋谷区、代表取締役：大野　暉、以下「サイバーセキュリティクラウド」）は、企業に対してサイバーセキュリティに関する注意喚起をリアルタイムに実施するため、自社独自に集約したサイバー攻撃に関するデータを分析した「サイバー攻撃速報」を発表いたします。

■GPONルータを狙った攻撃状況について

2018年7月20日に、日本国内でもGPON[1]ルータを狙った攻撃がキャンペーン的に増加したことを観測しました。今回観測した攻撃は2 つの脆弱性 「CVE-2018-10561」と「CVE-2018-10562」を悪用するものです。

同様の観測は、eSentire Threat Intelligence [2]でも観測が発表されていることから、世界規模で発生したサイバー攻撃と考えられます。

サイバーセキュリティクラウドでは、GPONを利用するルータの2つの脆弱性(CVE-2018-10561、CVE-2018-10562)が公表された2018年5月時点より、本脆弱性の観測を継続してきましたが、7月20日に攻撃数の一時的な増加がみられた為、注意喚起を目的に観測データを公表いたします。

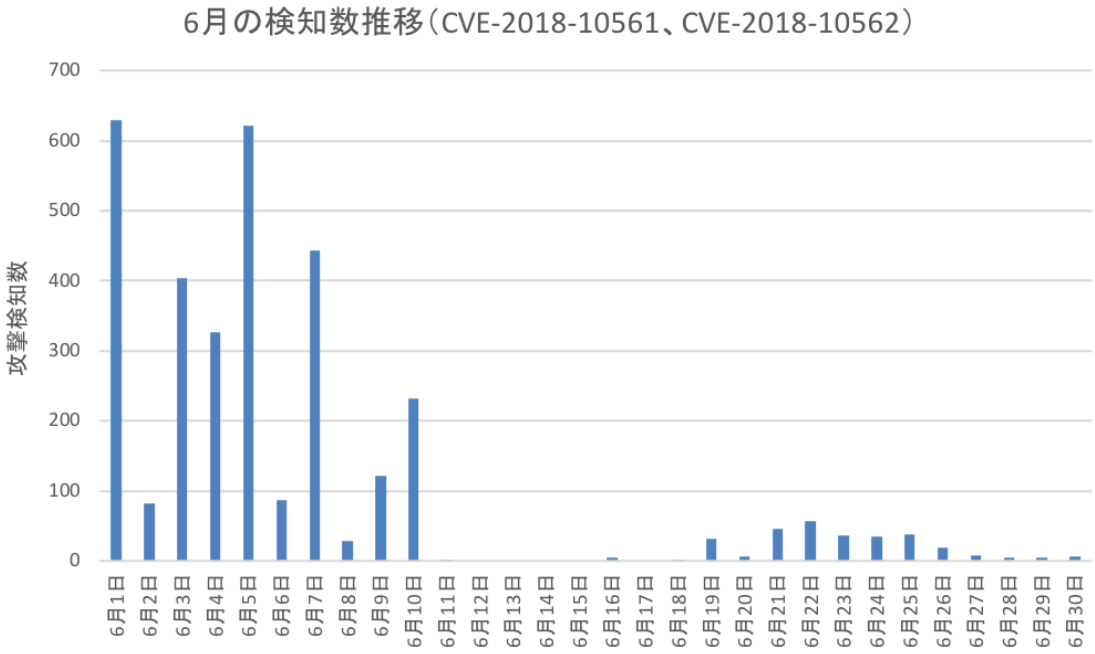

図1. 2018年6月に検知したCVE-2018-10561、CVE-2018-10562を悪用した攻撃の推移

本脆弱性のPoCは5/3に公表されているため、図1のとおり、6月10日までは検知数が多い状況が継続していましたが、それ以降は検知数が”100”を超えることはありませんでした。

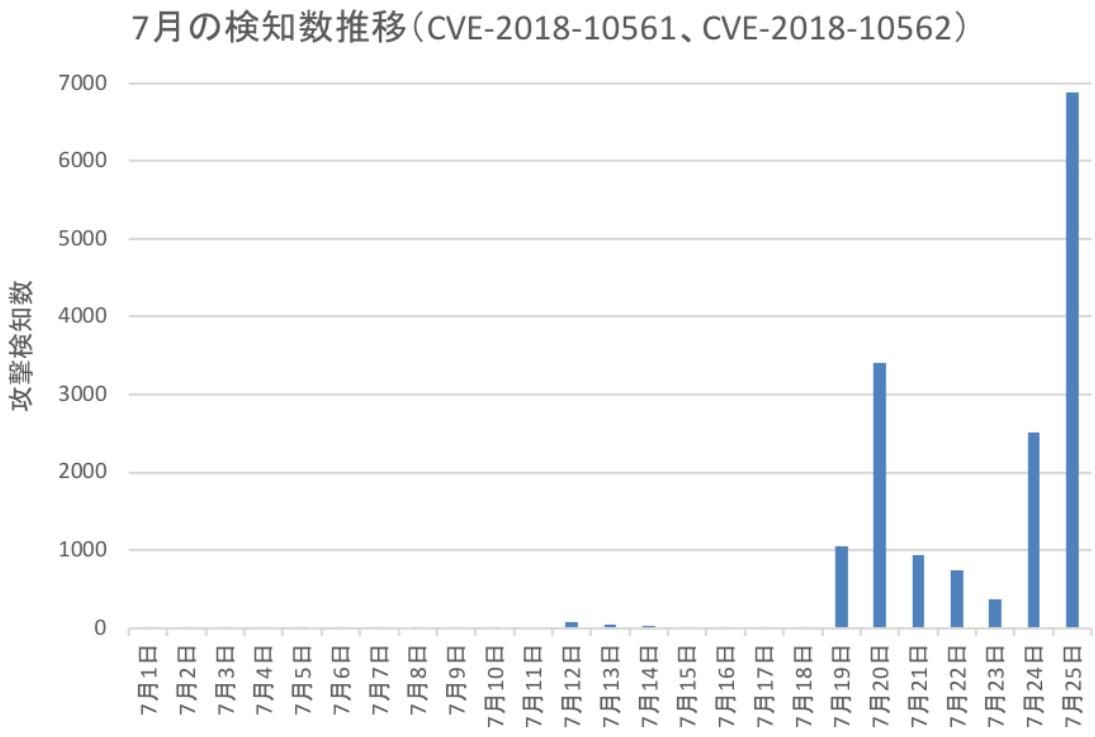

図2. 2018年7月に検知したCVE-2018-10561、CVE-2018-10562を悪用した攻撃の推移

図2のとおり、7月19日に突如として検知数が”1,000”を超え、再び本脆弱性を悪用した攻撃が増加しました。さらに7月25日には検知数”6,793”となり、非常に多くの攻撃を検知しました。

また、攻撃元国（発信源）に着目してみると、エジプトに偏っていることが判明しました。エジプトを発信源とする攻撃の送信元IPアドレスの数は、7月19日～7月25日のわずか7日間で、8,947個に及びました。送信元IPアドレスの数が膨大に及ぶことから、攻撃者はすでに感染している踏み台の機器に命令を出し、今回の攻撃を発生させた可能性も十分考えられます。

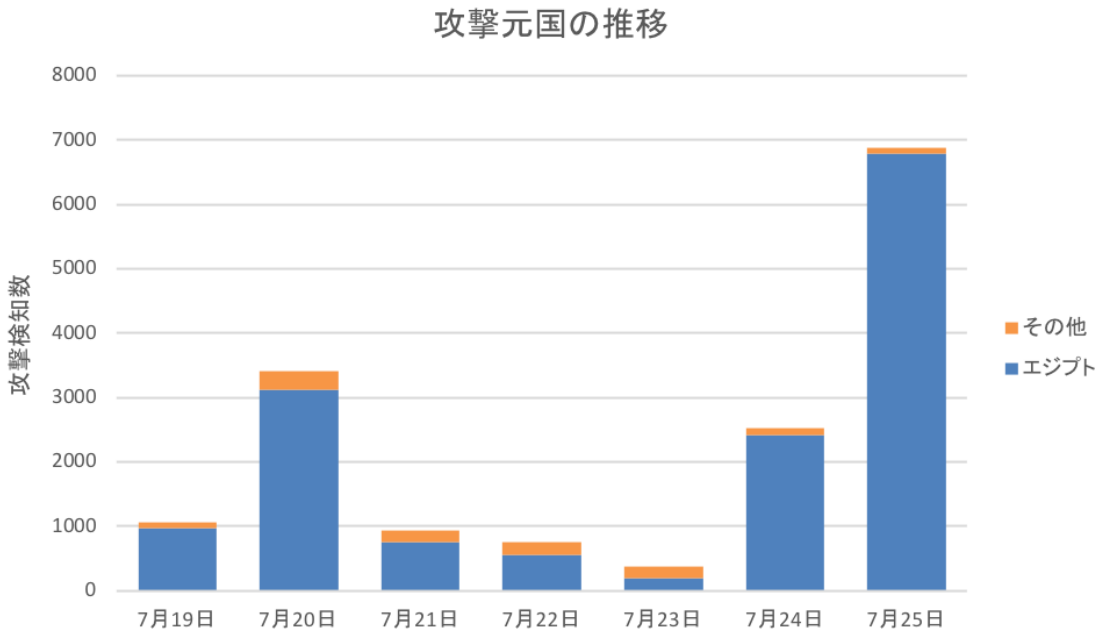

図3. 2018年7月に検知したCVE-2018-10561、CVE-2018-10562を悪用した攻撃の発信源

本攻撃を成功させると、機器への侵入とリモートでコードの実行が可能となります。また、これにより感染したデバイスがボットネット化し、新たなDDoS攻撃の攻撃元となってしまう可能性があります。

■クラウド型WAF「攻撃遮断くん」の対応状況

なお、クラウド型WAF「攻撃遮断くん」におきましては、本攻撃に関して、既存のシグネチャにて検知し遮断しております。

[1] 光通信規格「Gigabit Passive Optical Network」の略

[2]
https://www.esentire.com/blog/esentire-observes-an-increase-in-exploitation-attempts-against-routers/

■「攻撃遮断くん」について

「攻撃遮断くん」は、Web サイトへのサイバー攻撃を可視化・遮断するクラウド型 WAF の Web セキュリティサービスです。
官公庁や金融機関をはじめ、大企業からベンチャー企業まで業種や規模を問わず様々な企業にご利用いただき、
2013 年 12 月のサービス提供開始から約 3 年半で累計導入社数・導入サイト数 国内第1位※2 を記録しています。

※攻撃遮断くんの名称、ロゴは、日本国における株式会社サイバーセキュリティクラウドの登録商標または商標です。

※1 出典：Netlab Botnets never Die, Satori REFUSES to Fade Away：http://blog.netlab.360.com/botnets-never-die-satori-refuses-to-fade-away-en/

Radware Satori IoT Botnet Variant：http://blog.netlab.360.com/botnets-never-die-satori-refuses-to-fade-away-en/

※2 出典：「クラウド型 WAF サービス」に関する市場調査（2017 年 8 月 25 日現在）＜ESP 総研調べ＞（2017 年 8 月調査）

■株式会社サイバーセキュリティクラウドについて

会 社 名 ： 株式会社サイバーセキュリティクラウド
所 在 地 ： 〒150-0031 東京都渋谷区桜丘町 24-4 第 5 富士商事ビル 4 階
代 表 者 ： 代表取締役 大野 暉
設 立 ： 2010 年（平成 22 年）8 月
U R L ： https://www.cscloud.co.jp/
https://www.shadan-kun.com/

「世界中の人々が安心安全に使えるサイバー空間を創造する」この理念を掲げ、サイバーセキュリティクラウドでは、自社で一貫してWebセキュリティサービスの開発・運用・保守・販売を行っています。全ての企業様が安心安全に利用できるサービスを開発し、情報革命の推進に貢献するために私たちは挑戦し続けます。