セキュリティ情報発信サイト

IIJ
Internet Initiative Japan

wizSafe

wizSafe Security Signal

安心・安全への道標

wizSafe Security Signal（ウィズセーフセキュリティシグナル）は、
企業や組織のセキュリティ対策の支援を目的に、
今脅威となっている事象に対する即応性の高い情報を発信するサイトです。

掲載コンテンツ例

観測レポート

- DDoS攻撃の観測情報
- IIJマネージドセキュリティサービスの観測情報
- Web/メールのマルウェア脅威の観測情報
- ボットによる攻撃、探査の観測情報
- セキュリティインシデントカレンダー

注意喚起

- 緊急度が高い脅威や攻撃、脆弱性の情報（概要、影響範囲、対策など）

https://wizsafe.iij.ad.jp/

wizsafe security signal　検索

記事例

2019年09月30日掲載
wizSafe Security Signal 2019年8月 観測レポート」より一部抜粋

執筆者:IIJ SOCチーム　URL:https://wizsafe.iij.ad.jp/2019/09/746/

2019年8月観測レポートサマリー

DDoS攻撃の検出では、先月と比較して件数は少々増加しましたが、攻撃時に発生した最大パケット数、最大通信量は大幅に減少しました。最大規模を記録した攻撃ではDNSやLDAPを用いたUDP Amplification攻撃、最長時間を記録した攻撃ではHigh Portに対するUDP Flood攻撃が発生していました。

IPS/IDSにおいて検出したインターネットからの攻撃については、Mirai亜種によるルータに対する攻撃が先月よりも増加し、全体の7割以上を占めました。また、当月公表された、Pulse Secureの脆弱性（CVE-2019-11510）を狙った攻撃などが観測されています。

Webサイト閲覧時における検出では、バンキングマルウェアが最も多く観測されています。メールではユーザの行動情報を収集するスパイウェアが月内で最も多く検出され、特定の日に集中して受信したことを観測しています。

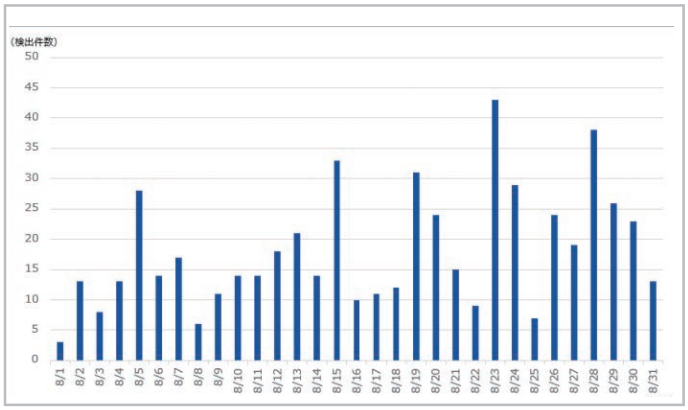
当月は17日にWebminのリモートから任意のコマンドを実行可能な脆弱性(CVE-2019-15107)が修正されたバージョンがリリースされ、本脆弱性の詳細が公表されました。公表後に本脆弱性をスキャンする活発な活動が観測されています。また、当月はWS-Discoveryが利用するポートに対するスキャン活動が中旬頃から多く観測されています。WS-DiscoveryはLAN内に存在するネットワークに接続されたデバイスを探索する際に使用されることから、そのようなデバイスを狙ったスキャン活動であるものと推測されます。

DDoS攻撃の観測情報

IIJマネージドセキュリティサービスやバックボーンなどでIIJが対処したDDoS攻撃のうち、IIJ DDoSプロテクションサービスで検出した当月中の攻撃を取りまとめました。ただし、規模の大小や期間などから、攻撃先が特定可能な事案についてはこの集計から除いています。

■ 攻撃の検出件数と継続時間

今回の対象期間で検出したDDoS攻撃の総攻撃検出件数は561件であり、1日あたりの平均件数は18.10件でした。期間中に観測された最も規模の大きな攻撃では、最大91万ppsのパケットによって8.77Gbpsの通信が発生しました。この攻撃は主にLDAPとDNSを用いたUDP Amplificationでした。また、当月最も長く継続した攻撃は1時間35分にわたるもので、最大で146.60Mbpsの通信量が発生しました。この攻撃はHigh Portに対するUDP Floodでした。



DDoS攻撃の 検出件数(2019年8月)

インシデントカレンダー（抜粋）

8月に発生したインシデントを掲載しています。

カテゴリ凡例					
セキュリティ事件	脅威情報	脆弱性情報	セキュリティ技術	観測情報	その他

日付	カテゴリ	概要
8月2日（金）	脆弱性情報	海外のセキュリティ研究者は、WPA3の脆弱性（CVE-2019-13377）及び、FreeRADIUSの脆弱性（CVE-2019-13456）を公表した。CVE-2019-13377については、Dragonfly HandshakeにBrainpoolの楕円曲線暗号を使用していた場合、サイドチャネル攻撃に脆弱であり、漏えいした情報からブルートフォース攻撃にてパスワードを特定される可能性があるとのこと。また、CVE-2019-13456については、FreeRADIUSのEAP-pwd実装に脆弱性があり、こちらも情報が漏えいする可能性があるとのこと。同研究者は、今年の4月にもDragonfly Handshakeの脆弱性を公表しており、今回の公表においてはサイドチャネル攻撃による情報漏えいの影響を受けずにWPA3とDragonflyを実装するのは大変困難であるとコメントしている。 "Analysing WPA3's Dragonfly Handshake – NEW RESULTS" https://wpa3.mathyvanhoef.com/#new
8月5日（月）	セキュリティ事件	輸入品販売会社が運営する通販サイトにおいて、外部からの不正アクセスを受け、最大40,233件のクレジットカード情報が流出した可能性があることを公表した。流出したクレジットカード情報の中には、カード会員名、カード番号、セキュリティコード及び有効期限が含まれるとのこと。同社によると、Webアプリケーションの脆弱性を利用したクレジット決済アプリケーションの改ざんが行われ、顧客のクレジットカード情報が窃取された可能性があるとしている。 「「omochabakoWEBSTORE」への不正アクセス発生についてのご報告とお詫び」 https://www.omochabako-webstore.jp/contents/information/post-1909
8月6日（火）	脆弱性情報	キヤノン社は、同社製品のデジタルカメラにおけるPTP通信機能及びファームウェアアップデート機能に存在する複数の脆弱性を公表した。公表された脆弱性には、SendObjectInfoの処理におけるバッファオーバーフローの脆弱性（CVE-2019-5994）や、ユーザの操作無しに悪意のあるファームウェア更新ファイルによるアップデートが可能となる脆弱性（CVE-2019-5995）などが含まれるとのこと。今回キヤノン社によって公表された複数の脆弱性を発見したCheck Point社は、同脆弱性を悪用するためには同脆弱性が存在するデジタルカメラと攻撃者が同じLAN内に居る必要があると述べている。キヤノン社によると、2019年8月6日時点では、一部の製品について同脆弱性を修正したファームウェアアップデートの準備が完了しているが、その他の製品についてはファームウェアアップデートの準備が完了次第、順次案内を行うとのこと。 「キヤノン製デジタルカメラにおけるPTP（画像転送プロトコル）通信機能およびファームウェアアップデート機能の脆弱性について」

その他の記事はこちらから　》》　https://wizsafe.iij.ad.jp/

Internet Initiative Japan

お問い合わせ（IIJインフォメーションセンター）
株式会社インターネットイニシアティブ
TEL:03-5205-4466 (9:30～17:30 土・日・祝日除く)
E-Mail : info@iij.ad.jp
URL : www.iij.ad.jp

IIJ-CAT002-0003