高まる DDos 攻撃の脅威

IoT や 5G の普及が DDos 攻撃をパワーアップさせる

DDos 攻撃の踏み台は大量の IoT 機器

企業だけでなく政府機関が狙われている

- ルータ
- ビデオレコーダー
- 監視カメラ
- プリンター
- NAS
- スマートプラグ

etc.

IT セキュリティに関し、現在、企業や組織団体にとっての最大の脅威は DDos 攻撃だと言われています。
DDos 攻撃とは、DoS 攻撃が 1 台のコンピューターから攻撃をしかけてくるのに対し、複数のコンピューターから一斉にサイバー攻撃をしてくるという分散型サービス妨害攻撃のことです。
数年前まで、ランサムウェアがメディアでも大きく取り上げられ企業にも影響しはじめたので、最大の脅威だといわれておりましたが、最近では明らかに DDos 攻撃が大規模化し、それによる企業や組織団体の被害額も増大しています。
DDos 攻撃は、攻撃対象のマシンに成りすまして大量のマシンにパケットを送信して、攻撃対象のマシンに大量の応答を集中させる DoS リフレクション攻撃 という攻撃もありますが、一般的には、攻撃者が大量のマシンを乗っ取り、それを踏み台として一斉に DoS 攻撃をしかける分散型の規模を大きくした DoS 攻撃です。
DDos 攻撃の脅威が増したのには、IoT の普及があります。
この踏み台にされるマシンの多くは、PC やサーバに限らず、監視カメラや、レコーダーなどの家電機器が不正利用され、それらからとてつもなく大量のトラフィックを送信し攻撃対象のマシンをダウンさせます。
攻撃者の乗っ取りの対象となる IoT 機器の代表例としては、ルータ、ビデオレコーダー、監視カメラ、プリンターなどがあげられます。今では、ハードディスクレコーダーも、スマート TV もインターネット接続が当たり前となってきました。特に家庭に設置する Wi-Fi ルータやレコーダーなどは、素人にはよくわからないので、デフォルトのパスワードのまま設置してしまうことが多いです。最近は、家電の取扱説明書もインターネット上でほとんどが閲覧可能なため、デフォルトのパスワード名も、侵入のための攻略法もわかってしまいます。怖いのは、私たちは、どの IoT 機器が乗っ取られているのかさえもわかりません。ひょっとすると、自分たちが所有している機器が犯罪に使用されている可能性さえあります。
マスコミでサイバー戦争という言葉がよく使用されますが、以前は金融サービスや E コマースなどが多く狙われていたのに対し、それを抜いて現在は政府機関の約 6 割が標的とされているという現状があります。
2020 年の東京オリンピックに向けて、セキュリティ強化が叫ばれておりますが、5G 回線などにより DDos 攻撃がさらにパワーアップされる懸念もあり、企業や組織団体はさらなる対策が必要になってきます。