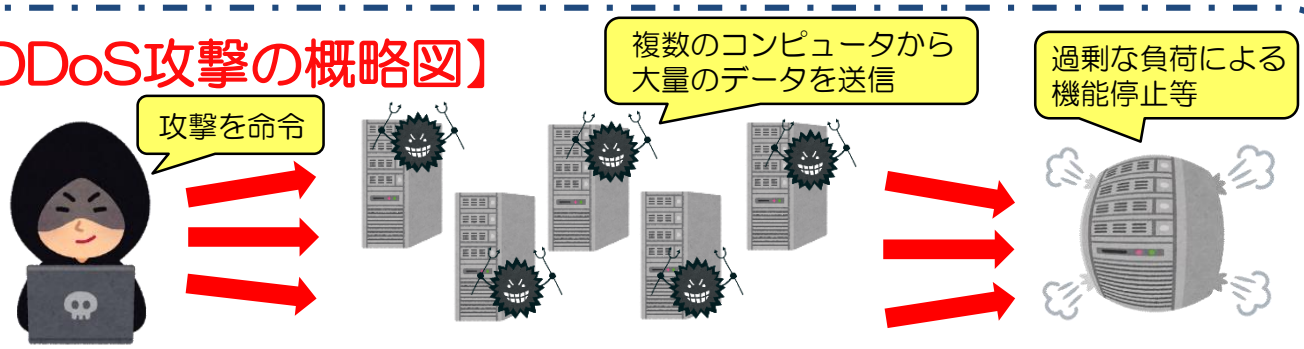
Ksisnetだより
発行:Ksisnet事務局
令和2年10月1日
Vol.85

DDoS攻撃を示唆した脅迫行為について

攻撃者が標的の組織宛にメールを送り、指定する期間内に仮想通貨を支払わなければ、DDoS攻撃を実行すると脅迫する手口が確認されています。

外部から接続可能なサーバやインフラについて、悪用や攻撃による被害を最小限にするため、使用するポートやサービスの制限などを検討してください。

【DDoS攻撃の概略図】



【脅迫行為の流れ】

（1）攻撃者が標的の組織を選定する

主に金融業、旅行業、小売業などを標的とした攻撃が確認されています。

組織のwebサイトだけでなく、外部から接続可能なサーバやインフラも対象とされます。

（2）攻撃者が標的の組織にメールを送付する

「指定する期間内にBTC（ビットコイン）アドレスに送金しなければ、DDoS攻撃を実施する」等と記載されたメールが送付されます。

（3）攻撃者が標的の組織のシステムにDDoS攻撃を行う

攻撃者はメールを送付した後、攻撃能力を示すために一定時間DDoS攻撃を行う場合があります。なお、支払い期限を過ぎてもDDoS攻撃が行われない場合もあります。

（4）攻撃者が仮想通貨を受け取る

攻撃者は、指定したBTCアドレスに仮想通貨の支払いがあるかを確認しているとみられますが、仮想通貨を支払ったとしても攻撃が必ず収束する保証はありません。

対策および対応

- 攻撃の影響を受ける可能性のあるシステムの特定およびリスクの評価
- 攻撃を検知および防御するための対策状況の確認
- 攻撃を検知および認識した場合の対応手順や方針の確認
- 攻撃で事業への影響が生じた場合の連絡体制や連絡方法の確認

参考　JPCERT/CC・ＩＰＡ