2017 年 10 月 25 日
株式会社セキュアソフト

注意喚起：ランサム DDoS 攻撃に対する事前対策について

1. 概要

インターネット上のウェブサイトには一般的な検索エンジンでは到達できない、Deep web や Dark web と呼ばれるウェブページが存在します。このような深層インターネットの闇市場ではサイバー攻撃の代行サービス(CaaS: Cybercrime-as-a-Service)やツールが取引されており、サイバー攻撃が頻発する要因の一つになっています。サイバー攻撃のうち、金銭要求を伴うものをサイバー脅迫といい、最近では「Wanna Cryptor」に代表されるランサム（身代金）ウェアが有名です。ランサムウェアのほかにも DDoS 攻撃の停止と引き換えに金銭を要求するランサム DDoS 攻撃（RDoS: Ransom DDoS）が存在します。

2017 年 9 月、日本国内において、DDoS 攻撃の停止と引き換えに金銭を要求するメールが多数配信されていることが確認されました。このメールとの因果関係は不明ですが、同じタイミングで DDoS 攻撃が発生したことも確認されております。

今やウェブサイトは企業戦略において重要な「チャネル」「ツール」「メディア」として位置づけられており、そのサービス停止は企業活動に大きな影響を与えます。DDoS 攻撃への対応体制を点検するとともに、自身のサーバやルータが踏み台として使用されないようにご注意ください。

2. ランサム DDoS 攻撃とは

ランサム DDoS 攻撃とは DDoS 攻撃の停止と引き換えに金銭を要求するサイバー攻撃の一つです。まずは小規模な DDoS 攻撃を仕掛け、攻撃能力を誇示した上で脅迫メールを送信するシナリオが一般的です。ただし、過去に DDoS 攻撃を行った犯行グループを名乗り、脅迫メールを送信するだけで金銭を窃取した事例もあり、このシナリオの限りではありません。

⑴ ランサム DDoS 攻撃の典型的なシナリオ

① 標的のウェブサイトに対して短期間の DDoS 攻撃をおこなう。
② 脅迫メールを送信する。
③ 要求に従わない場合、大規模な攻撃をおこなう。

⑵ ランサム DDoS 攻撃による被害例

ランサム DDoS 攻撃による被害は身代金支払いによる直接的被害だけではありません。サービス停止が企業活動に大きく影響する場合は例えば株価の下落を招く場合もあります。また DDoS 攻撃を受けた企業がホスティング事業者から解約された事例もあります。身代金を支払っても攻撃が停止される保証はなく、更なる攻撃と身代金要求につながる可能性もあります。

⑶ 脅迫メールの本文例

下記のメールでは攻撃停止の見返りにビットコインの送金を要求しています。

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [redacted] will be DDoS-ed starting [redacted]. if you don't pay 10 Bitcoins @ [redacted]

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([redacted]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by [redacted], attack will start, price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long
time.

This is not a joke.

Our attacks are extremely powerful - our Mirai botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 10 BTC @ [redacted]

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

「Armada Collective」からの脅迫メールのイメージ（出所：JPCERT コーディネーションセンター）

3. SecureSoft Sniper ONE による DDoS 対策

DDoS 対策のポイントは、攻撃通信を検知・防御しつつ正規ユーザに対するサービスの品質を維持するところにあります。これを実現する SecureSoft Sniper ONE を使用した DDoS 対策をご紹介します。

⑴ SecureSoft Sniper ONE とは

SecureSoft Sniper ONE は、従来それぞれ専用機として提供していたセキュリティ機器の機能をオプション化し、1 台で高度な検知・防御機能を実現する製品です。

必要なオプションを選択することで、スモールスタートが可能になり、コスト削減につながります。また、導入後の機能追加も可能なため、ビジネスの変化・拡大に合わせた対策が可能です。

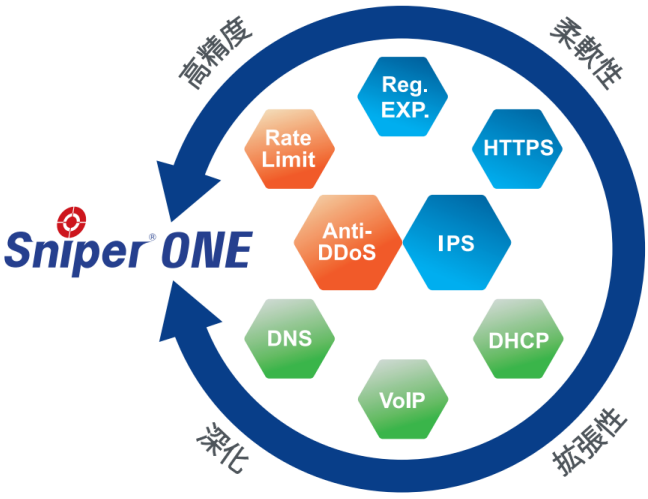

図 1 Sniper ONE のコンセプト

⑵ DDoS 対策概要

SecureSoft Sniper ONE に Anti-DDoS オプション、もしくは Rate Limit オプションを追加することで、DDoS 攻撃から大切な情報資産を防御します。

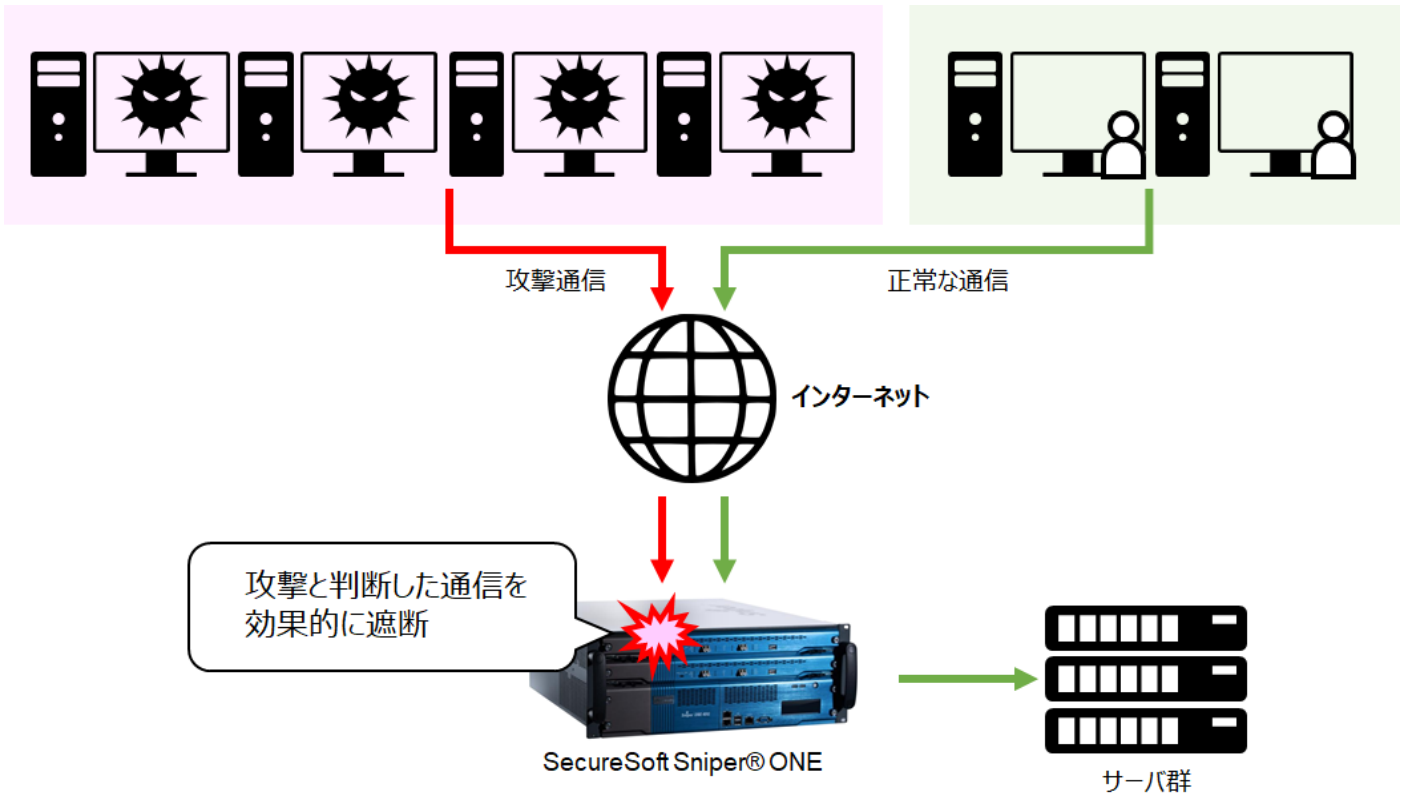

図 2 Sniper ONE による DDoS 攻撃防御イメージ（Anti-DDoS オプション使用時）

⑶ Sniper ONE Anti-DDoS オプションとは

Sniper ONE Anti-DDoS オプションは DDoS 攻撃対策に特化した 8 つの解析エンジンにより、正規ユーザ向けのサービスを維持しながら、DDoS 攻撃を効果的に防御します。Anti-DDoS オプションは DDoS 対策の専用製品である SecureSoft Sniper DDX ベースに更に進化させモジュール化しました。独自機能 Triple 'S'（Smart Session Shaping) Engine によるセッションのコントロールや DDoS 攻撃の通信を分析しシグネチャ化する SEE（Signature Extraction Engine）など、DDoS 攻撃を効果的に抑制し、お客様にサービスの安定稼働をお約束します。

Protocol Anomaly Filtering Engine プロトコル規約違反をフィルタリング	**Dynamic Filtering Engine** IPとPortの組み合わせに対する動的フィルタリング	**Static Defense Engine** 特定IPとPortの組み合わせをフィルタリング	**Triple S Engine** セッションの監査を通じた検知・遮断
Signature Matching Engine シグネチャベースの防御	**Statistics Analysis Engine** 特定のプロトコルやサービスの異常な急増を検知・遮断	**Signature Extraction Engine** 異常に急増する通信を分析し、検出シグネチャを自動生成	**A.L.S.I Engine** Layer7ベースの検出・遮断エンジン

図 3 Sniper ONE Anti-DDoS オプションの解析エンジン

Anti-DDoS オプションによる DDoS 攻撃対策は以下のニュースリリースでも解説しております。

参考情報（セキュアソフト ニュースリリース『Sniper ONE による DoS/DDoS 攻撃対策例のご案内』）
https://www.securesoft.co.jp/news_mt/2015/08/sniper-onedosddos/

⑷ Sniper ONE Rate Limit オプションとは

Sniper ONE によるより効果的な DDoS 攻撃対策としては、 Anti-DDoS オプションに加えて Rate Limit オプションを追加する方法がございます。本オプションは帯域制御によるサーバの保護に有効なオプションです。大量のトラフィックを効果的に制限するため、DDoS 攻撃だけではなく、ユーザの増加やヘビーユーザの利用によってネットワークリソースが枯渇することを防ぐこともできます。

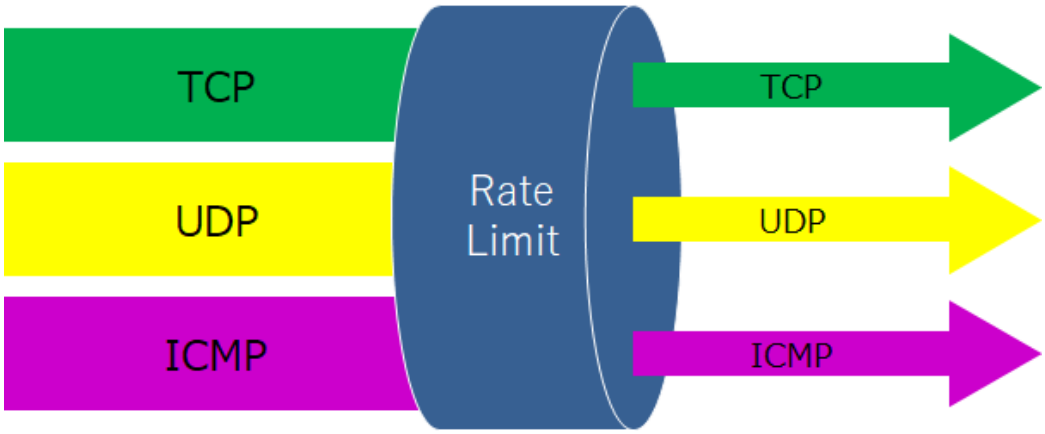

図 4 Sniper ONE Rate Limit Engine

Rate Limit オプションによる DDoS 攻撃対策は以下のニュースリリースでも解説しております。

参考情報（セキュアソフト ニュースリリース『SecureSoft Sniper ONE の特徴 ：Rate Limit 機能』）
https://www.securesoft.co.jp/news_mt/2015/12/securesoft-sniper-one-rate-limit/

«お問合せ先»
株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp