身代金要求を伴うDDoS攻撃にどのように対処すべきか？

（How to Respond to a DDoS Ransom Note）

By Radware -September 10, 2020

※この資料は、2020年9月10日にRadwareが投稿したブログ
(https://blog.radware.com/security/attack-types-and-vectors/2020/09/how-to-respond-to-a-ddos-ransom-note/)を元に日本ラドウェア株式会社 取締役 カントリーマネージャー安藤 嘉教様が日本語に翻訳、再構成したものです。
同社ご承諾のもと、株式会社テリロジーで掲載させていただいております。

身代金を要求するDDoS攻撃が復活しています。ここ数週間、ハッカー集団は新たな勢いで攻撃を行っており、特に金融、Eコマース、サービスプロバイダーの各業界が深刻な影響を受け始めています。

8月中旬以降、ラドウェアは「Fancy Bear」、「Armada Collective」、「Lazarus Group」を装った脅迫者からの恐喝要求を数件追跡しています。これは世界的なキャンペーンで、APAC、EMEA、北米の金融、旅行、Eコマースの各分野の組織からの脅威が報告されています。

- DDoS 攻撃は、身代金要求の有無にかかわらずどの企業もいつでも攻撃を受ける可能性があり、「DDoS-for-hire 」ツールにより、攻撃者はボタンを数回クリックするだけで簡単に攻撃を開始できるようになっています。DDoS-for-hire tools are making it easier それにも関わらず、DDoS攻撃による身代金要求は攻撃対象となった企業を窮地に追い込みます。特に多額の支払いを要求される場合にはその影響はより深刻です。

とはいえ、DDoS 身代金要求書の被害は、事前に正しい技術で対処しておけばこれを食い止めるこす。

払ってはいけない

DDoS 攻撃者に身代金を支払うことは、様々なレベルでのダメージを受ける可能性があり、実際には支払いにより攻撃者があなたを放っておくことを保証するものではありません。

私たちラドウェアは、身代金の要求を支払うことを避けるようアドバイスしています。なぜなら、これらの悪質な行為者が条件を守る保証はなく、脅威のプレッシャーの下で身代金を支払ってしまうような企業をターゲット組織として「特定」しようとしているからです。また、身代金を支払うことはこの悪意のある活動の資金となり、悪意のある行為者が能力を向上させ、悪しき攻撃キャンペーンを継続する動機付けとなります。

You may also like: Keep It Simple: Choosing the Right DDoS Mitigation Strategy （この事例をお勧めします。：シンプルにすべき。正しいDDoS防御戦略の選択）

身代金要求を伴うDDoS攻撃に対する重要な課題の1つは、実際に誰がこの攻撃の背後にいるのかを見分ける方法がないことです。多くの身代金要求書は、「Fancy Bear」や「Armada Collective」などの有名なグループを名乗っていますが、偽者によって送られたケースも多くあります。このようなDDOS攻撃に伴う身代金要求書は、複数のターゲットに送られることが多く、送信者は、被害者の中の何人かがやみくもに支払ってくれることを期待しているだけで、実際には何もしなくても高額の支払いを受け取れるようにしているのです。

攻撃者にお金を払わないもう一つの理由は、実際には攻撃者があなたを放っておくことを保証しないということです。過去には、被害者がお金を払ったにもかかわらず攻撃を受けたケースがあります。

何よりも重要なのは、このDDoS 攻撃と引き換えの身代金を支払うことで、すぐに身代金を支払ってしまう被害者がいることを攻撃者に伝え、彼らの動機を増進させてしまうことです。繰り返しになりますが、被害者が身代金を支払ったにもかかわらず、攻撃者がより大きな金額を要求して再度被害者に戻ってきたというケースもあります。

You may also like: Why You Should Reconsider DDoS Mitigation from Public Cloud Providers（また、この事例もお勧めします。：パブリック・クラウド・プロバイダーからのDDoS防御を再考すべき理由）

情報を伝える

多くの場合、DDoS 攻撃と引き換えの身代金要求書は、公開されている電子メールアドレスを使用して、ターゲットに「盲目的に」送られます。これらの要求書の受信者は、ネットワークセキュリティやITに関連する利害関係者ではなく、組織内の無作為な人々であることが多いです。実際、多くの身代金要求通知には、この脅威を関係者に渡すよう指示が含まれています。

そのため、組織は従業員に対して DDoS 身代金要求攻撃の危険性と、身代金要求書が従業員に届いた場合の対処法について積極的に教育する必要があります。ネットワークセキュリティの責任チームの選定とメーリングリストや緊急連絡先を設定し、関連する脅威は全てそのチームに伝えるべきであることを説明しておくと便利です。

DDoS身代金要求書に対する明確なオーナーを設定し、関連情報を早期かつ迅速に伝達することで、DDoS 身代金要求書が届いた場合に備えて組織としての準備を整えることができ、攻撃によるリスクを大幅に軽減することができます。

前兆の攻撃をチェック

多くの身代金要求書には、攻撃者の能力と身代金の脅威の実行可能性を示すために、小規模な事前攻撃を行うことが述べられています。

そのため、小規模なDDoS攻撃を示すトラフィックの急増がないか、ネットワークログをチェックすることが重要です。これらのログは通常、組織のネットワークチーム、セキュリティチーム、ISP、またはクラウドセキュリティプロバイダがチェックすることができます。

攻撃を受けた場合に身代金を支払わないことをラドウェアは推奨していますが、一方でこの事前の攻撃の証跡は脅威の実行可能性を示し、ターゲットとなってしまった企業がどのように準備すべきかを示してくれている可能性があります。

You may also like: 5 Myths About DDoS in 2020]（この記事もお勧めです。：2020年のDDoSについての5つの神話）

事前攻撃の証拠があったからといって、それがないからといって、攻撃が続くとは限らないことに注意してください。ラドウェアは、事前攻撃の脅威があったにもかかわらず、事前攻撃がなかったケースや、プレカーサー攻撃の証拠はあったが、より大きな攻撃が行われなかったケースを見てきました。それでも、事前攻撃の兆候を探すことは、脅威の深刻さを知る上で有効な指標になるのです。

セキュリティプロバイダーに警告を出す

リスクの深刻度にかかわらず、セキュリティプロバイダに脅威を警告し、攻撃活動を共同で監視してもらう必要があります。

セキュリティ・プロバイダに警告することで、セキュリティ・プロバイダに準備の時間を与え、トラフィックをより綿密に監視し、必要に応じて追加のセキュリティ・メカニズムを適用させることができます。

まだ専用の DDoS スクラビングソリューションを導入していない場合は、今が導入を検討する良い機会です。dedicated DDoS scrubbing solutions

You may also like: How to Recover from a DDoS Attack（お勧めの記事：DDoS攻撃からの回復方法）

警戒を怠らない

最後に、警戒心を保つことの代替策はありません。DDoS攻撃は身代金要求書を伴っているかどうかに関わらず、いつでもやってくる可能性があります。しかし、DDoS 攻撃と引き換えの身代金要求書はリスクを増大させており、DDoS 攻撃に対する包括的な防御がより一層必要となってきています。comprehensive protection against DDoS attacks

今回のこの脅威を機会に、DDoS 防御のためのベストプラクティスを適用すべきです。

1. アプリケーション、IP、サーバー、データセンター、場所など、公開されているすべての資産のリストを作成すること。
2. 保護すべき資産のリストに優先順位をつけ、どの資産がミッションクリティカルであり、更なる保護を必要とするかを評価すること。assess which assets are mission-critical
3. 攻撃前、攻撃中、攻撃後に何をすべきかを事前に定義した手順で、DDoS 攻撃対応計画を策定し、実行すること。before, during, after an attack
4. 大規模で洗練された攻撃に対応する十分な能力と経験を持つ、大手 DDoS 防御ベンダーによる専用の DDoS 防御を導入すること。dedicated DDoS protections
5. DDoS防御に関するSLAを確認し、セキュリティ・プロバイダーが真に効果のある防御をコミットし、継続的に強化していることを確認してください。Verify DDoS protection SLAs

身代金要求を伴うDDoS 攻撃は笑い事ではなく、真剣に対応する必要があります。しかし、これらの対策をいくつか実行することで、DDoS 攻撃と攻撃が行われた場合の脅威に対する適切な準備と対応に大いに役立つのです。

出典

How to Respond to a DDoS Ransom Note

By Radware -September 10, 2020

https://blog.radware.com/security/attack-types-and-vectors/2020/09/how-to-respond-to-a-ddos-ransom-note/

身代金要求を伴うDDoS攻撃にどのように対処すべきか？（How to Respond to a DDoS Ransom Note）

By Yoshinori Ando Radware - Country Manager,Japan

https://www.linkedin.com/pulse/how-respond-ddos-ransom-yoshinori-ando/?fbclid=IwAR0bJFtI5PZ8UVpDECqfI-SMmR62eh5HyItE9ytT4bhk4D4tGPUL1JFGfBc

お問い合わせ窓口

株式会社テリロジー　Radware営業部　担当 宛

製品に関するお問い合わせは当社のお問い合わせフォームからお寄せください