— AUS（アルテミス・ユーザ・サポート）便り 2019/11/11号 —
https://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●DDoS攻撃を示唆し仮想通貨を要求する脅迫メールに注意喚起

https://crypto.watch.impress.co.jp/docs/news/1215815.html
http://www.jpcert.or.jp/newsflash/2019103001.html

このニュースをザックリ言うと・・・

- DDoS攻撃を示唆して仮想通貨を要求する脅迫メールが出回っているとして、10月24日(現地時間)にドイツのセキュリティベンダLINK11より、同30日にはJPCERT/CCより、相次いで注意喚起等が出されています。

- 脅迫メールは、対象組織が管理および利用するWebサイトやIPアドレスに対しDDoS攻撃を行うとの予告と、攻撃を回避するために仮想通貨を期日内に支払うよう要求する内容が含まれているとのことです。

- 単なる脅しに留まらず、実際に最大60GbpsのDDoS攻撃が行われたケースもある模様で、JPCERT/CCでは、「決して攻撃者の要求には応じず、冷静に対応を行うこと」「攻撃が発生した場合の対応体制、攻撃への対策および利用している対策サービスの状況を確認すること」および「外部から接続可能なサーバやインフラについて、使用するポートやサービスを制限すること」等を呼び掛けています。

AUS便りからの所感等

- 攻撃者が行うDDoS攻撃手法としては、DNS(ポート53番)・NTP(ポート123番)・WS Discovery(ポート3702番)・Apple Remote Management Service(ポート3283番)といったUDPサービスを悪用し、膨大な量に増幅したパケットの送受信を行わせる、いわゆる「リフレクション攻撃」が主とみられます。

- プライベートIPアドレスとNATを利用しているため「たまたま」外部からは直接パケットを送信できない社内LANであっても、利用しているサーバー等を踏み台に攻撃を受ける可能性もあるため、社内LANの前面のルーターやUTM等におけるフィルタリングでそういったケースについても対応されていることが望ましいでしょう。

- 当然ながら各サーバーについても、明示的に外部に提供しているサービスポート以外はアクセスを遮断するよう設定を行い、かつその設定が行われているか適宜見直しをかける、あるいは第三者機関による診断を受けることを推奨致します。

仮想通貨（暗号資産）ニュース

DDoS攻撃を示唆し仮想通貨を要求する脅迫メールに注意喚起＝JPCERT/CC

要求には応じず、万が一の攻撃に備え対応体制を確認するよう呼びかけ

高橋ビョン太　2019年10月31日 06:00

(Image: Shutterstock.com)

JPCERTコーディネーションセンター（JPCERT/CC）は10月30日、DDoS攻撃を示唆して仮想通貨を要求する脅迫メールが拡散中であることを警告した。10月中旬以降、複数の組織宛てに脅迫メールが送られていると、ドイツのセキュリティベンダLINK11が注意喚起して以来、日本国内においても同様の脅迫メールが観測されているとJPCERT/CCは報告する。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

DDoS 攻撃を示唆して、仮想通貨を要求する脅迫メールについて

最終更新: 2019-10-30

CyberNewsFlash一覧

2019年10月24日 (現地時間)、ドイツのセキュリティベンダ LINK11 は、DDoS 攻撃を示唆して仮想通貨を要求する脅迫メールが出回っていると注意を呼びかけています。同社によると、10月中旬以降、複数の組織を対象にメールが送付されていることを観測しているとのことです。JPCERT/CC においても国内の組織が同様の脅迫メールを受信していることを確認しています。

LINK11
Warning of Serious DDoS Blackmail Campaigns Attributed to Fancy Bear Group
https://www.link11.com/en/blog/warning-of-serious-ddos-blackmail-campaigns-attributed-to-fancy-bear-group/

同社が確認しているメール本文には、メールの受信組織が管理する Web サイトや使用する IP アドレスなどに DDoS 攻撃を行うとの予告に加え、攻撃を回避するために仮想通貨を期日内に支払うよう要求する内容が含まれています。メール受信者には受信者の危機感を高めるため、実際に最大 60 Gbps の DDoS 攻撃などが行われる場合があり、観測された攻撃として次の特徴が確認されているとのことです。

【観測された DDoS 攻撃の特徴】
1) 攻撃手法として、一般的な DNS、NTP、CLDAP を使用した DDoS リフレクション攻撃に加え、WS Discovery [1] や Apple Remote Management Service [2] などを使用した攻撃が行われている
2) 攻撃を受ける対象として、Web サイトだけではなく、外部から接続可能なサーバ/インフラも標的となる場合がある

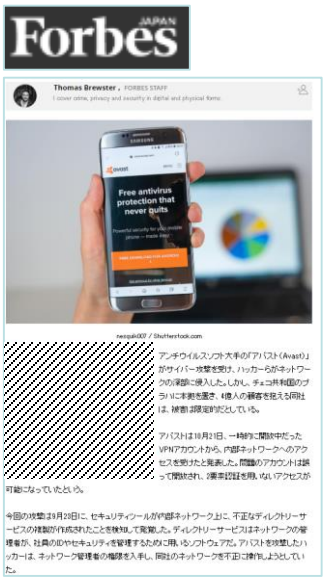
もし、このようなメールを受信した場合は攻撃者の要求には応じず、冷静に対応を行ってください。実際に DDoS 攻撃が行われることを想定し、攻撃が発生した場合の対応体制の確認や、攻撃への対策や利用している対策サービスの状況を確認することをお勧めします。また、外部から接続可能なサーバやインフラについて、悪用や攻撃による被害を最小限にするため、使用するポートやサービスの制限などを検討してください。

●Avast社を狙った不正アクセスが確認される…サプライチェーン攻撃が目的か

https://cybersecurity-jp.com/news/33963
https://forbesjapan.com/articles/detail/30421
https://blog.avast.com/jp/ccleaner-fights-off-cyberespionage-attempt-abiss

このニュースをザックリ言うと･･･

- 10月21日(現地時間)、セキュリティベンダーのAvast社より、同社ネットワークに対するサイバー攻撃を確認したと発表されました。
- 攻撃は9月23日に発覚し、一時的に開放していたVPNアカウントを悪用されて内部ネットワークに侵入されたとみられます。
- 発表では、攻撃者は5月頃から侵入を試みていた模様で、また同社製品にマルウェアを混入させる「サプライチェーン攻撃」を狙った可能性があるものの、深刻な被害がもたらされる恐れは無いとしています。



AUS便りからの所感

- 発表では、サプライチェーン攻撃によって実際に被害が生じた例として、人気ユーティリティである「CCleaner」のアップデートにマルウェアが仕込まれたケース(AUS便り 2017/9/25号参照、なおCCleanerの開発元は事件発生の前後にAvast社に買収されていました)を挙げていますが、今回も主要なターゲットはCCleanerだった可能性があるとしています。
- Avast社自体も無料のアンチウイルスソフト等が人気であり、同様に正規の署名付きでマルウェア入りのアップデートが配布された場合、会社自体にも大きな損害が生じていたことが考えられます。
- 今回のような一時的に開放されていたアカウントのみならず、例えばテスト用アカウントや退職者のアカウントが、第三者や当の退職者等に狙われる可能性も十分に考えられますので、そういったアカウントを放置することなく随時削除やパスワードの変更を含めた管理を徹底すること、他にも今回のような内部ネットワークでのインシデントを検知するシステムの導入等が重要となるでしょう。

●130万件のクレジット・デビットカード情報流出、単一ファイルで過去最大規模

https://news.mynavi.jp/article/20191101-917320/

このニュースをザックリ言うと･･･

- 10月29日(米国時間)、シンガポールのセキュリティ企業Group-IB社より、130万件を超えるクレジットカードおよびデビットカード情報の漏洩を検出したと発表されました。
- カード情報はインターネット上にアップロードされていた単一のデータベースファイルから見つかったものとされ、単一ファイルの漏洩としては過去最大規模、時価総額は1億3,000万ドル以上と推定されているとのことです。
- 同社の分析によれば、カード情報の98%以上はインドの銀行、その他1%はコロンビアの銀行に関連するものとされています。

AUS便りからの所感等

- 攻撃者が奪取した情報がダークウェブ等にアップロードされるパターンでは、通常小さなファイルに分割されてアップロードが行われるとされ、今回のように単一のファイルで大規模なアップロードが発生したとみられるのは過去に例が無いとされています。
- 例えば内部ネットワークに侵入した攻撃者により、このような情報を外部に大量送信されることのないよう、侵入対策のみならず出口対策にも着目し、適切なソリューションを導入すべきでしょう。
- 個人情報が大量に保存されたデータベースがインターネット上で発見されるケースには、クラウド上に設置したデータベースが外部からアクセス可能な状態にされていたパターン(AUS便り 2019/9/17号参照)もあり、アクセス制限を確実に設定する等、それぞれの可能性に対しとるべき対策を適切に洗い出し、実行することが肝要です。