— AUS（アルテミス・ユーザ・サポート）便り 2017/10/16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。

●企業はDNSを狙うサイバー攻撃に弱い…Infoblox調査

https://japan.zdnet.com/article/35108608/
https://www.atpress.ne.jp/news/139980

このニュースをザックリ言うと・・・

- 10月3日（現地時間）、セキュリティベンダーの米Infoblox社より、企業の大半が「ドメインネームシステム(DNS)」を狙うサイバー攻撃に対し脆弱であるとする調査結果が発表されました。

- この調査は、マルウェア「Mirai」によるDNSサービス「Dyn」への攻撃から約1年が経過したことを機に、同社とディメンショナル・リサーチ社によって1000社以上のセキュリティおよびIT担当者に対し行われたものです。

- 調査結果によれば、平均で10社中3社がDNSへの攻撃で被害に遭ったことがあり、うち40%は1時間以上ものダウン発生により、ビジネスに大きな影響を受けたとしており、また24%の企業が10万ドル以上、54%の企業が5万ドル以上の損失を出しているとのことです。

- DNSに対する全てのタイプの攻撃を防御できている企業は37%に過ぎないとされており、過半数となる63%が本質的に攻撃に対して無防備状態であることが指摘されています。

AUS便りからの所感等

- DNSにアクセスできず、外部のユーザが自組織のドメイン名を引くことができない事態が発生すると、Webサイトへのアクセスやメールの送信をしてもらう機会が損失し、経済的損失につながり得ます。

- Miraiによって引き起こされたようなDDoS攻撃から自ドメインを守るには、単一のDNSサービスではなく、複数のサービスと契約して分散させることが重要です。

- もしそれが困難で、DNSサーバーを社内ネットワークに自前で設置せざるをえないのであれば、DDoSを含めその他の攻撃からの防御のため、UTMの設置は欠かせないでしょう。

ZDNet Japan

企業はDNSを狙うサイバー攻撃に弱い --Infoblox調査

ZDNet Japan Staff 2017年10月12日 06時00分

いいね！ 17　ツイート　G+　B! 0　Pocket 28

印刷　メール▼　ダウンロード▼　クリップ

インターネット利用に欠かせないDomain Name System（DNS）を狙うサイバー攻撃に対して企業の大半が脆弱であるという。ネットワークセキュリティを手掛ける米InfobloxとDimensional Researchが実施した調査結果から分かった。

ウェブサイトのドメインとIPアドレスをひも付けるDNSは、インターネットアクセスに不可欠なインフラの1つとなる。DNSを狙う攻撃手法には、インターネットユーザーを不正サイトに誘導するハイジャックや、サービス妨害（DoS）を狙って「名前解決」と呼ばれる機能への要求を増幅させるリフレクションなど、さまざまなものがあり、被害に遭えばインターネット利用に深刻な影響が出る。

調査は、2016年10月にDynがIoTマルウェア「Mirai」による分散型のDoS（DDoS）攻撃によって、大規模なインターネット接続障害に見舞われた事件から約1年が経過したことを踏まえて実施したという。1000社以上のセキュリティやITの担当者が回答した。

それによると、平均で10社中3社がDNSへの攻撃で被害に遭い、そのうち40%は1時間以上ものダウンタイムよってビジネスに大きな影響を受けたことが分かった。71%の企業はDNSへの攻撃をリアルタイムに監視していたが、このうち86%の企業は攻撃の発生を適切に把握できない状況にあった。20%の企業が外部からの苦情などで、攻撃の事実を把握していたという。

@Press

Infoblox、最新のグローバルサーベイ結果を発表 多くの企業がDNS攻撃に対する準備ができていないという結果に

Infoblox株式会社　2017.10.11 13:00

いいね！ 0　シェア　ツイート　G+　B! 0　その他の共有　印刷する

Infoblox株式会社(本社：東京都港区、カントリーマネージャー：仁枝 かおり、以下 Infoblox)は、2017年10月11日(水)、グローバルサーベイの結果を発表しました。Dyn へのDDoS攻撃から1年、Infobloxとディメ、DNSセキュリティは、サイバーセキュリ判明しました
本リリースは、2017年10月3日、本社サます。

リサーチ調査によると、DNSセキュリティしばしば見過ごされており、多くの企業でておりません。

ほとんどの企業がDNS攻撃に対し"未対応"という事実から判断できる他の調査結果は以下の通りです。

●DNS攻撃は非常に効果的である
10社のうち3社は、すでにDNS攻撃の犠牲になっています。そのうちの93%が直近のDNS攻撃の結果としてダウンタイムに苦しんでいます。 40%が1時間以上ダウンし、ビジネスに大きな影響を与えました。

●DNS攻撃の認識が遅い企業
71%の企業がDNS攻撃のためにリアルタイムのモニタリングをしているにもかかわらず、それらモニタリングソリューションの86%は、DNSの攻撃が発生した際に、速やかに担当チームへの通知ができませんでした。さらに、企業の20%が顧客の苦情によって初めてDNS攻撃に気づきました。つまり、すでにビジネス、評判、顧客満足度に影響を与えていました。

●DNS攻撃に対してほとんどの企業が脆弱である
企業のわずか37%だけがすべてのタイプのDNS攻撃(ハイジャック、悪用、キャッシュポイズニング、プロトコル異常、リフレクション、NXDOMAIN、増幅)を防御することができました。つまり、過半数(63%)は、本質的に攻撃に対して無防備状態といえます。

●アドレス400件流出…神奈川県警の防犯メール

https://www.jiji.com/jc/article?k=2017100600428&g=soc

このニュースをザックリ言うと・・・

- 10月6日（日本時間）、神奈川県警相模原署より、防犯情報のメール送信時に誤って400件のメールアドレスが外部に流出したと発表されました。

- 発表によれば、5日午後に管内の犯罪発生状況に関するメールを希望者に送信する際、受信者のアドレスを他の受信者が閲覧できる状態で入力したことで発生したことが原因で、メールを受け取った利用者からの問合せで発覚したとされています。

- 送信前に別の署員がペアチェックを行う体制にはなっていたものの、他の業務で忙しかったためにチェックを怠ったことも原因とされています。

AUS便りからの所感等

- メーラーにおいて、受信者のアドレスをBcc:ヘッダに列挙する形がとられていたところ、誤ってTo:やCc:に列挙してしまった可能性が高いと考えられます。

- 多数のメールアドレスを毎回コピー＆ペーストで入力するやり方やペアチェックに依存するやり方は、万が一のメールアドレス流出を根本的に防止できるものではありませんので、そういう観点からの対策として、メーリングリスト等の同報メール送信のためのシステムの導入は重要です。

- 一方で、メールサーバやUTMにおけるメールチェックにより、To: Cc:に不自然に大量のメールアドレスが含まれているメールを拒否する等も検討に値するでしょう。

JIJI.COM

アドレス４００件流出＝登録者全員に誤送信－神奈川県警

神奈川県警相模原署は６日、防犯情報などを配信するメールに登録された約４００件のメールアドレスを、誤って登録者全員に送信したと発表した。

同署によると、生活安全課の男性署員が５日午後４時５分ごろ、４日朝から５日朝までの犯罪発生状況を知らせるメールを配信した際、誤って登録者全員のアドレスが見える形で送信した。配信を受けた人から連絡があった。誤配信したのはアドレスだけで、誰のものかは特定できないという。

同署は６日中に、登録者におわびのメールを配信する方針。信沢公昭副署長は「個人情報を流出させてしまい、大変申し訳ない。今後は業務管理を徹底し、再発防止に努める」としている。（2017/10/06-10:20）

【社会記事一覧へ】 【アクセスランキング】

●iOSの偽ダイアログを出してパスワードを盗み取るフィッシングとその判別法

http://gigazine.net/news/20171011-ios-steal-password/

このニュースをザックリ言うと・・・

- 10月10日（現地時間）、iOS向けツール開発者のFelix Krause氏より、iPhone等の画面に偽のパスワード入力ダイアログを表示するフィッシングについて、ブログ記事にて警告が出されています。

- 記事では、iOSが表示する本物のダイアログと、ある手法によって模倣された偽のダイアログの例がそれぞれ画像で示されており、ホーム画面やアプリ起動画面にも割り込んで表示されるケースもあるとしています。

- 一方で、同氏は偽のダイアログを見分ける方法として「ホームボタンを押すこと」を挙げており、本物のダイアログであれば画面に表示されたままになるが、偽のダイアログでは表示が消えてホーム画面に戻るとしています。

AUS便りからの所感等

- 偽のダイアログが表示される原因は、デバイスに感染したマルウェア以上に、一見安全に見えるアプリに仕込まれる不正なコードである可能性が高いでしょう。

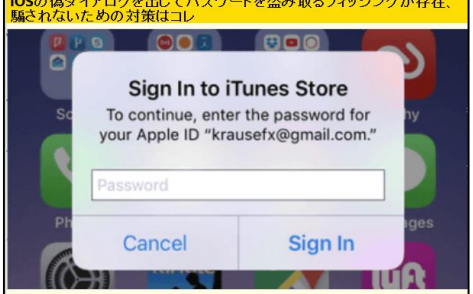
- それまで全く問題が報告されなかったようなアプリが開発元の買収等により、アップデートで不正な行為を行うようになるケースも時々ある模様です。

- ダイアログが表示された場合は上記に挙げた自衛策を必ずとるよう心がけると同時に、インストールしているアプリは必要最小限に抑え、アプリストアやSNS上の評判を随時注視すること、そしてアップデート時に追加で権限が要求される場合は特に注意を払うことが肝要です。

GIGAZINE

2017年10月11日 13時00分00秒

iOSの偽ダイアログを出してパスワードを盗み取るフィッシングが存在、騙されないための対策はコレ



iPhoneなどの画面に時おり現れる「パスワードを入力してください」というダイアログが、実は非常に簡単な手口によって第三者が模倣できることが専門家の調査で明らかになっています。この方法が悪用されるとユーザーのiCloudのパスワードがいとも簡単に盗み取られてしまう危険性が高いのですが、同時に単純な方法で偽のダイアログであることを見抜く方法も明らかにされています。