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。

●狙いはG7サミット？DNSキャッシュサーバーを悪用した企業・官庁へのDDoS攻撃多発

https://nordot.app/1024954370013462528
https://jprs.jp/glossary/index.php?ID=0137

このニュースをザックリ言うと･･･

- 4月29日(日本時間)、共同通信より、企業・中央省庁および地方自治体のWebサイトに対するDDoS攻撃が今年3月以降頻発していると報じられています。

- DDoS攻撃は「DNS水責め攻撃」と呼ばれる手法をとり、サイトが短時間の間繋がりにくくなる事象が多く発生している模様です。

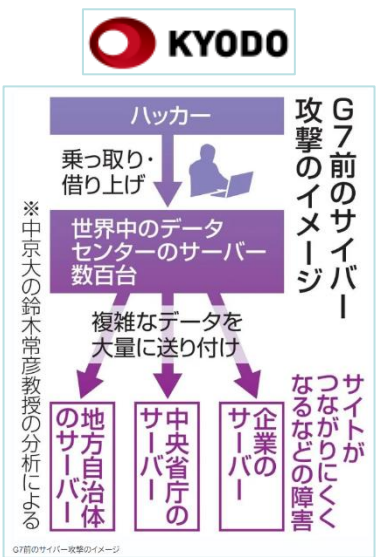
- 内閣サイバーセキュリティセンター(NISC)は「G7広島サミット議長国として狙われている可能性があり、関係機関に警戒するよう注意喚起した」としています。

AUS便りからの所感等

- DNS水責め攻撃は2014年頃から確認されており、本来は自組織やISPの契約ユーザーからのリクエスト処理のみを許可するDNSキャッシュサーバーにおいて、任意のアクセス元IPアドレスからの問合せを受け付ける設定になっている、いわゆる「オープンリゾルバー」状態のキャッシュサーバーを多数悪用し、ターゲットとなる組織等のドメイン名情報を返すDNSサーバー(権威サーバー・コンテンツサーバー)に大量のリクエストが送り付けられるよう仕向ける攻撃です。

- キャッシュサーバー側でも「qwerty12345.target.example」「asdfgh67890.target.example」等、先頭にランダムな文字列を含めたFQDNでのリクエストを大量に受けるため、キャッシュした結果を返すことができず、都度権威サーバーにリクエストを送信させられることになります。

- DNSのオープンリゾルバー問題はメールサーバーのオープンリレー問題とともに攻撃者に踏み台にされる等の恐れがある古典的な問題であり、今回のような攻撃にも悪用されないよう、組織内で使用しているDNSキャッシュサーバーの設定を厳密に確認する(モバイル回線等第三者ネットワークを利用してリクエストを受けないか診断する等も有用です)ことが肝要ですが、他にも詐称されたアクセス元IPアドレスからのリクエストが本来来ないようなネットワークから飛んでくる可能性や、家庭用ブロードバンドルーター等にもDNSキャッシュサーバー機能が備わっており、設定次第では外部からリクエストを受け付けるオープンリゾルバー状態となる可能性にも注意を払うべきでしょう。



G7前にサイバー攻撃が頻発　特殊な手法、企業や官庁に

2023/04/29

今年3月以降、企業や中央省庁、地方自治体のウェブサイトを狙った特殊なサイバー攻撃が頻発していることが29日、関係者への取材で分かった。大量のデータを送り付けシステム障害を起こすDDoS攻撃の一種だが、サイトの重要サーバーを狙った特殊な手法を使っていた。ほとんどは短時間で復旧した。

内閣サイバーセキュリティセンターは「G7広島サミット議長国として狙われている可能性があり、関係機関に警戒するよう注意喚起した」と話す。中京大の鈴木常彦教授は「本格的な攻撃の前の下調べの可能性がある」と分析している。

●公文書管理システムでファイル103,389件誤消去、75%は復旧できず

https://www.niikei.jp/698953/
https://www.itmedia.co.jp/news/articles/2304/24/news085.html
https://www.pref.niigata.lg.jp/sec/bunsho/0577006.html
https://www.pref.niigata.lg.jp/sec/bunsho/0580656.html

このニュースをザックリ言うと・・・

- 4月21日(日本時間)、新潟県より、県の公文書管理システムに登録した文書の添付ファイルが消失する事故が4月9日に発生したと発表されました。
- 対象となるファイルは3月24日～同31日に登録した文書の添付ファイルの一部103,389件で、いずれも庁内の起案や決裁等の意思決定手続きに関するものとされています。
- 5月9日には続報が同県より発表され、25,439件のファイルは復旧したものの、残る77,950件(全体の75.4%)は復旧できず、控えを保存していたものは再登録するとしています。
- ファイルの消失はシステム上の問題によるもので、外部からの攻撃はなく、流出もなかったとのことです。

AUS便りからの所感

- 3月24日、システム内において、保存する添付ファイルの拡張子を大文字から小文字に変更する機能が追加された際、不要な添付ファイルを削除する既存のプログラムが、拡張子が小文字の添付ファイルを誤って不要なファイルと判断し、削除したことが原因としています。
- 追加機能は必要な社内手続き(運用テスト、社内審査等)を経ずに適用され、かつ開発・運用担当者間で適用の事実が共有されていなかったこと、バックアップが3日間の保存で、4月9日の削除発生後、判明したのが同13日だったため、復旧に用いることができなかった等の問題が明らかになっています。
- サイバー攻撃以外の運用上の問題ながら、完全性・可用性に拘ったものといえ、システムに関わっている全ての機能について担当者が把握し、機能間の齟齬でデータ消失等のトラブル、さらには外部からの侵入や情報流出を許す状態が発生しないようとりまとめる体制は不可欠でしょう。

● 4月度フィッシング報告件数は92,932件、急増止まらず

- https://www.antiphishing.jp/report/monthly/202304.html

このニュースをザックリ言うと・・・

- 5月9日(日本時間)、フィッシング対策協議会より、4月に寄せられたフィッシング報告状況が発表されました。
- 4月度の報告件数は92,932件で、3月度(https://www.antiphishing.jp/report/monthly/202303.html)の77,056件から15,876件増加しています。
- フィッシングサイトのURL件数は21,230件で3月度(14,343件)から6,887件増加、一方フィッシングに悪用されたブランド数は92件で3月度(110件)から18件減少となっています。
- Amazonを騙るフィッシングは全体の約30.6%と割合は再び増加(3月度22.1%)、以下ファミペイ・えきねっと・Uber Eats・ETC利用照会サービスを騙るものと合わせて全体の約64.2%を占めたとのことです。
- 同協議会の調査用メールアドレスへ配信されたフィッシングメールの約88.3%が中国の通信事業者からの配信とされ、またDNS逆引き設定がされていないIPアドレスからの送信は約96.5%を占めているとしています。

AUS便りからの所感

- 2022年10月～2023年1月の減少期からの急激な回復により、8万件台以上を維持していた2022年3月～同9月の水準にまで戻っており、恐らくはこの勢いがそのまま続くものとみられます。
- ファミペイを騙るフィッシングは同協議会から4月21日に注意喚起が出ており、手元でも大量の受信が確認されています。
- 5月は現時点でApple・大和ネクスト銀行・横浜銀行のフィッシングについても同協議会から注意喚起が出ており、ユーザーPCのアンチウイルスやUTMによるアンチフィッシング機能、自組織のメールサーバーにおけるSPF・DMARC等によるスパムメールチェック、また取引相手等の保護のため自社ドメインについてもSPF・DMARCレコードの設定と適切な運用を行うことが肝要です。

フィッシング対策協議会
Council of Anti-Phishing Japan