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。

●Windowsの重大な脆弱性、依然約100万台のPCに…WannaCry級の攻撃発生のおそれ

https://japan.zdnet.com/article/35137653/
https://japan.zdnet.com/article/35137871/

このニュースをザックリ言うと・・・

- 5月28日（現地時間）、セキュリティ研究者グループ Errata Securityより、Windows 7（およびWindows Server 2008 R2）以前のリモートデスクトップサービスに存在する重大な脆弱性（CVE-2019-0708）について、パッチを適用していない約100万台のPCが依然インターネット上に接続されているという調査結果が発表されています。

- 「BlueKeep」とも呼ばれるこの脆弱性を突いた大規模な攻撃は発表の時点ではまだ確認されていないものの、向こう1・2ヶ月の間に攻撃方法が発見され、かつてのWannaCry並みの攻撃が発生する可能性が指摘されています。

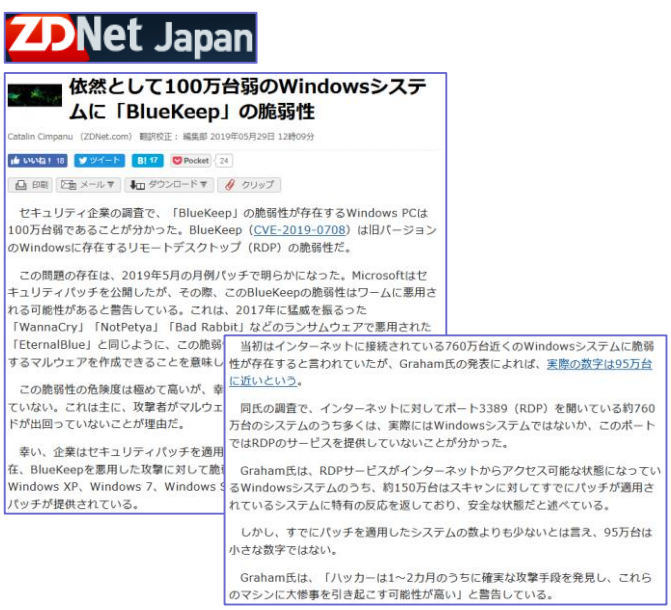
- 同30日にはマイクロソフトからも、パッチの適用を行うよう同社ブログで注意喚起が出されています。

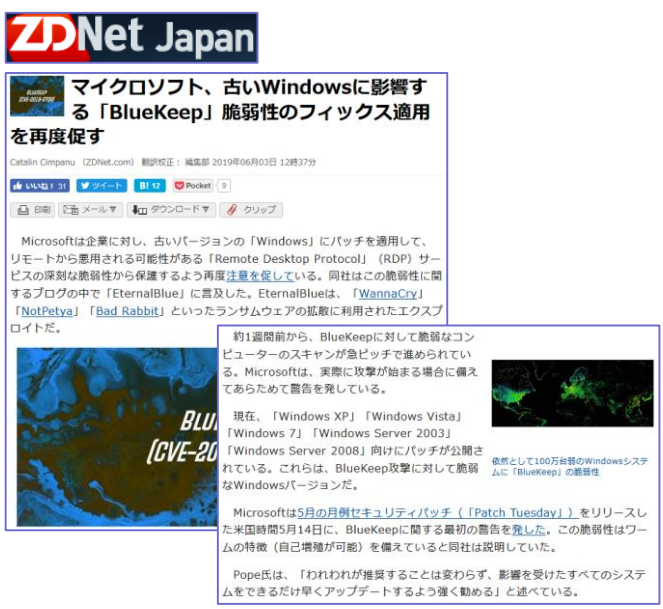
AUS便りからの所感等

- BlueKeepに対するパッチは5月15日（日本時間）に月例のセキュリティパッチとしてリリース済みであり（AUS便り 2019/05/20号参照）、少なくともWindows 7についてはWindows Updateを確実に実行している限り対策済みと思われます。

- 前述の約100万台のPCにおけるOSの分布は不明ですが、サポート切れながら特例でパッチが出たWindows XP（およびWindows Server 2003）が依然多く運用され、かつパッチの適用が（適用方法が7とは異なること等から）進んでいない可能性も考えられます。

- パッチを確実に適用しているか、またアンチウイルスが機能しているか以外にも、そもそもリモートデスクトップが不要なのに有効になっていないか等にも注意を払い、場合によってはUTM等でリモートデスクトップポート（TCPポート3389番）等不必要なポートへのアクセス、および万が一のマルウェア感染時に備え外部への不審な通信を遮断する設定も検討すべきでしょう。





●サイト閉鎖したコンビニのドメイン名、失効でオークションに

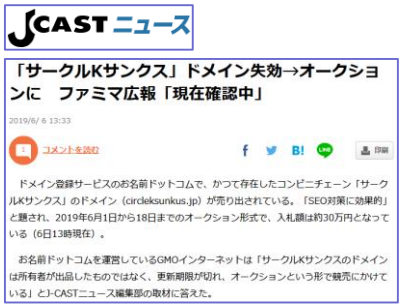
https://www.j-cast.com/2019/06/06359394.html

このニュースをザックリ言うと・・・

- 6月6日（日本時間）、複数のネットメディアより、コンビニエンスストア「サークルK」「サンクス」の公式サイトで使用されていたドメイン名がドメイン名業者のオークションに出品されていることが相次いで報じられました。

- 2018年11月末にサークルK・サンクスがファミリーマートへの転換を完了したことに伴い、公式サイトも終了していましたが、その後今年4月30日にドメイン名の更新期限が切れ、6月1日にドメイン管理業者が取得し、オークションに出品した模様です。

- オークションは6月18日までとなっており、7日の時点で入札価格は50万円を超えています。


J-CASTニュース

「サークルKサンクス」ドメイン失効→オークションに　ファミマ広報「現在確認中」

2019/6/ 6 13:33

コメントを読む

ドメイン登録サービスのお名前ドットコムで、かつて存在したコンビニチェーン「サークルKサンクス」のドメイン（circleksunkus.jp）が売り出されている。「SEO対策に効果的」と題され、2019年6月1日から18日までのオークション形式で、入札額は約30万円となっている（6日13時現在）。

お名前ドットコムを運営しているGMOインターネットは「サークルKサンクスのドメインは所有者が出品したものではなく、更新期限が切れ、オークションという形で競売にかけている」とJ-CASTニュース編集部の取材に答えた。

AUS便りからの所感等

- 一時的なイベント等のために取得した独自ドメイン名が失効 → 第三者に取得されるケース はAUS便りでも度々取り上げています（AUS便り 2019/03/18号等）が、人気があったWebサイトのドメイン名を第三者のWebサイト業者がオークションで大金を払ってでも購入しようとするのは、閉鎖した後もそのドメイン名宛に少なからずアクセスが来ることを見越し、自分たちが運営するWebサイトへのアクセス流入を期待しているためです。

- ファミリーマート側は「ファミマブランドに統合しているため、このドメインを今後使用する予定はない」旨コメントしていますが、長年使用していたサークルK・サンクスブランドのためのドメイン名を終了から1年以内で放棄する（更新しない）判断をしたことへの指摘が多く挙がっています。

- 独自ドメイン名の取得においては、今後のサイト閉鎖についても「サイト上での告知や関係各所への通知を十分に行う」「閉鎖後も数年以上はドメインを維持する」等を可能な限り最初から考慮・計画すべきでしょう。

●佐世保共済病院で院内PCがウイルス感染、患者受け入れ一時困難に

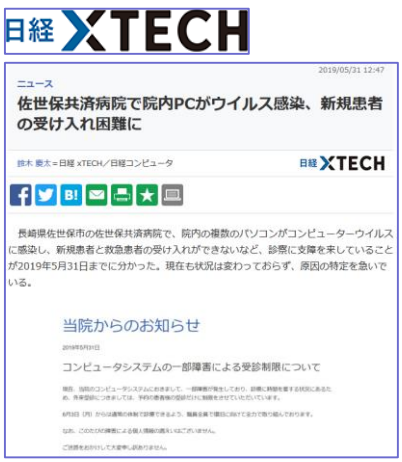
https://tech.nikkeibp.co.jp/atcl/nxt/news/18/05146/

このニュースをザックリ言うと・・・

- 5月31日（日本時間）、長崎県の佐世保共済病院より、同病院内でシステム障害が発生し、新規患者と救急患者の受け入れが困難な状態にあると発表されました。

- 発表によれば、同28日に、放射線検査の機器を接続したPCおよび電子カルテを扱うPCにおいてマルウェアへの感染が確認され、被害の拡大を防ぐため、PCや検査機器をつなぐ全てのネットワークを遮断したとのことです。

- 診察内容を電子カルテに反映できず、診療に時間がかかる事態となったため、一時は1日平均90人程度の外来新規患者の受け入れができない等の影響が発生し、その後院内PCにおいてマルウェア駆除と安全確認を行い、6月3日までに患者受け入れを再開しています。


日経XTECH

2019/05/31 12:47

ニュース

佐世保共済病院で院内PCがウイルス感染、新規患者の受け入れ困難に

鈴木 貴大＝日経 xTECH／日経コンピュータ

日経XTECH

長崎県佐世保市の佐世保共済病院で、院内の複数のパソコンがコンピューターウイルスに感染し、新規患者と救急患者の受け入れができないなど、診療に支障を来していることが2019年5月31日までに分かった。現在も状況は変わっておらず、原因の特定を急いでいる。

当院からのお知らせ

2019年5月31日

コンピュータシステムの一部障害による受診制限について

AUS便りからの所感等

- 病院内でのマルウェア感染の事例としては、昨年10月に奈良県の病院で電子カルテがランサムウェアに感染し、データが暗号化される事件が発生しています（AUS便り 2018/10/29号参照）。

- 今回のケースでは、PCがインターネットに接続されていないため外部からの攻撃である可能性はないとしており、また個人情報の漏洩も特に発生していない模様ですが、患者の受け入れを原則中止せざるを得なくなったとのことです。

- マルウェアの種類や感染の経路は現時点で明らかになっていませんが、今後それらに対する発表があった際には、同様の環境・経路で発生し得るマルウェア感染に対し如何に素早く復旧し、被害を最小限に抑えるかの参考となることを期待したいものです。