— AUS（アルテミス・ユーザ・サポート）便り 2020/07/20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。

●Twitter有名人アカウント乗っ取り多発…原因はTwitter社従業員への攻撃

https://www.nikkei.com/article/DGXMZO61570300W0A710C2I00000/
https://www.watch.impress.co.jp/docs/news/1266352.html

このニュースをザックリ言うと・・・

- 7月15日(米国時間)、Twitterにおいてビル・ゲイツ氏やTesla社のイーロン・マスク氏等著名人物、あるいはAppleやUber等企業の公式アカウントが相次いで乗っ取られる被害が発生しました。

- 乗っ取られたアカウントからBitcoinの送金を呼びかける不正なツイートが投稿されましたが、同日中にTwitter社により、該当するアカウントのロックや不正投稿の削除等の対応が行われたとのことです。

- 同18日までのTwitter社からの発表によれば、アカウント乗っ取りが発生した原因として、同社の一部従業員に対し、いわゆる「ソーシャルエンジニアリング」による攻撃が行われ、社内サポートチームだけが使用可能なツールが操作されたためとされています。

AUS便りからの所感等

- 発表により、同社の認証を受けた130のアカウントが攻撃を受け、メールアドレスや電話番号を奪取されたこと、うち45のアカウントでパスワードリセットに成功し不正な投稿を行われたこと、また認証を受けていない最大8アカウントについては過去のツイートや他者とやり取りしたDM等のデータがダウンロードされた可能性があること等が明らかになっています。

- Twitterのような大規模な公開サービスではもちろん、そういったサービスを提供していない場合でも、例えば内部の人間になりすました攻撃者等により、顧客とのやりとりの記録等の機密情報や社内ネットワークの権限を奪取される恐れがあることに注意し、システム面での対応と、リテラシー面の教育とを適宜実施して頂ければ幸いです。

日本経済新聞

マスク氏らのTwitter一斉ハッキングか　サービス停止も

ネット・IT　北米

2020/7/16 7:12 (2020/7/16 7:41更新)

保存 共有 印刷 その他

乗っ取り被害にあったとみられるテスラのマスクCEOのツイッター画面

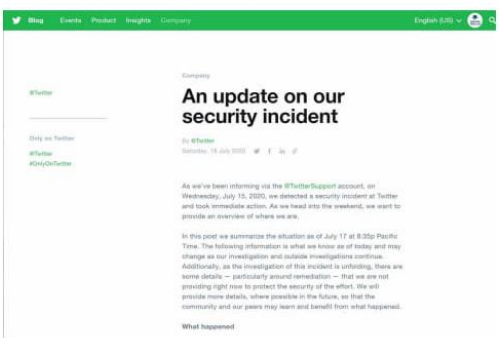
【シリコンバレー=白石武志】米テスラのイーロン・マスク最高経営責任者（CEO）やバイデン前米副大統領ら複数の米著名人のツイッターアカウントが15日、一時的に乗っ取られる被害にあった。いずれも暗号資産（仮想通貨）「ビットコイン」による送金を促す内容が投稿されており、米メディアはハッカーによる詐欺行為だと伝えている。

Impress Watch

Twitterの乗っ取り、アカウント侵入被害は45件。「責任を痛感」

臼田勤哉　2020年7月20日 06:00

ツイート リスト B! 4 Pocket 3 いいね！ 6 シェア



Twitterは18日(米国時間)、15日に発生した有名Twitterアカウントへの侵入問題に対する調査結果を発表した。現在も調査中だが、Twitter社員を狙ったソーシャルエンジニアリングによりTwitterの内部システムに侵入され、130のTwitterアカウントが狙われ、そのうち45のアカウントで攻撃者はパスワードリセットを実行。アカウントにログインし、ツイートを送信した。

● Windows ServerのDNS機能に脆弱性…サーバー乗っ取り、ワーム拡散の可能性も

https://forest.watch.impress.co.jp/docs/news/1265438.html
https://msrc-blog.microsoft.com/2020/07/14/20200715-dnsvulnerability/

このニュースをザックリ言うと・・・

- 7月15日(日本時間)、マイクロソフト(以下、MS)より、月例のセキュリティパッチがリリースされました。

- 今回修正された脆弱性のうち、Windows Serverに搭載されるDNSサーバー機能である「Windows DNS Server」に存在していた脆弱性(CVE-2020-1350)については、サーバーの乗っ取りの他、LAN上のPCないし外部に対するワームの拡散等に悪用される可能性がある等、危険度が高いものとされ、政府機関等からも注意喚起が出されています。

AUS便りからの所感

- 当該脆弱性はセキュリティベンダーのCheckPoint社によって発見され、「SIGRed」と命名されたもので、Windows Server 2003以降に存在していた一方で、MS以外によるDNSサーバーソフト(BIND等)には影響しないとのことです。

- 通常、Active Directory(以下、AD)を利用している企業等ではドメイン構築時にWindows DNS Serverが必須となり、特に脆弱性の影響を受ける可能性が高いとみられるため、MSから提供されるパッチの適用、あるいはパッチが適用できない場合の回避策の実行を速やかに行うよう推奨致します。

- 毎月第2火曜日(米国時間、日本時間ではその翌日)はMSのみならずAdobeやOracle等からも各種ソフトウェアのセキュリティパッチがリリースされており(Oracleは四半期毎のリリース)、日頃よりこの日の対策の実行を念頭に置いたシステム管理を心がけるとともに、パッチの適用等が間に合わない場合に未対策の脆弱性を突かれる可能性を抑止するためのアンチウイルス・UTM等による多重防衛の実施が重要となるでしょう。

●2020年4～6月はスパムメールの量が急増中…IIJ発表

https://eng-blog.iij.ad.jp/archives/6231

このニュースをザックリ言うと・・・

- 7月13日(日本時間)、IIJ社より、2020年4～6月に同社の迷惑メール計測システム環境で受信したスパムメールの分析結果が発表されました。

- 日ごとのスパムメール受信量について、5月上旬に4月時点の10倍(以下4月時点比)に急増した時期があり、以後5月中旬に40倍、5月下旬～6月上旬には60倍前後、6月下旬には70～80倍に達したとのことです。

- 一方、マルウェアが添付されたメールについては、4月時点に比べ5・6月の日ごとの受信量は少なくなったものの、6月上旬に1～2日程突出して大量の受信が確認された日があり、「Look at this photo!」「Photo just for you」等の件名で「IMG135123.jpg.js.zip」といったファイル名のマルウェアが添付されたものがみられたとのことです。

AUS便りからの所感

- スパムメールの流量について、不定期な波があるものの、4月時点から6月末時点で最大80倍に増加するというすさまじい結果となっています。

- スパムメール全体に対するマルウェア添付メールの割合は非常に低いものの、UTMでの防御が間に合わず、PC側のアンチウイルスによってマルウェアが検出されるケースが多発した日もありました。

- どんなスパムメール・マルウェア添付メールが流通しているかの情報を適宜入手し、それらに記載されたリンクをクリックしたり、添付ファイルを開いたりといった「相手をする」ようなことは決してせず、アンチウイルスとUTMによる防御を固めることを怠らないようにすることが肝要です。