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。

●教員のメールアカウントが不正アクセス、スパムメール6万件送信等の被害

https://scan.netsecurity.ne.jp/article/2020/02/10/43661.html
https://www.nagaokaut.ac.jp/oshirase_ut/200207.html

このニュースをザックリ言うと・・・

- 2月7日(日本時間)、長岡技術科学大学より、同大学教員1名のメールアカウントが不正アクセスの被害を受けたと発表されました。

- 不正アクセスは2019年10月17日～18日に発生していたとされ、同18日に当該教員から「スパムメールが大量送信されている」との報告があったことで発覚、パスワード変更等の対応を行ったとのことです。

- 不正アクセスにより、計66,482件のスパムメール送信に悪用された他、メールボックスに保存されていたメールのべ1,139件が攻撃者に閲覧された可能性もあり、その中には学内外関係者のべ51件の個人情報(氏名・所属・電話番号・メールアドレス等)が含まれていたとされ、現時点で流出等の被害は確認されていないものの、該当者に対し個別に対応を行っているとのことです。

AUS便りからの所感等

- 今回の不正アクセスに至った詳しい経緯は不明ですが、2018年に同様の事件が新潟大学で発生した(AUS便り 2018/10/9号)際は、複数の職員に対するフィッシングでアカウントが奪取されています。

- Office 365やG Suiteのような2段階認証(ないし多要素認証)を提供するメールシステムであれば、アカウントが不正アクセスを受ける可能性をある程度抑制することが可能ですが、そういったメールシステムへの移行は困難を伴うものであり、また2段階認証等をも突破する巧妙な攻撃が行われるケースにも注意する必要はあります。

- あるいは、社内ネットワーク上にメールサーバーを構築している場合であれば、クライアントPCとの隔離および不正な外部へのメール送信の遮断等のため、UTM等のソリューションの採用も検討に値するでしょう。

ScanNetSecurity by iid

教員のメールアカウントに不正アクセス、大量の迷惑メール送信の踏み台に（長岡技術科学大学）

国立大学法人長岡技術科学大学は2月7日、同学教員のメールアカウントに不正アクセスがあり、当該アカウントから大量の迷惑メールが送信されたことが判明したと発表した。

国立大学法人長岡技術科学大学は2月7日、同学教員のメールアカウントに不正アクセスがあり、当該アカウントから大量の迷惑メールが送信されたことが判明したと発表した。

これは2019年10月17日午後9時8分頃に、同学の教員からメールサーバ管理者に当該教員のメールアカウントから迷惑メールが大量送信されているとの報告があり、管理者が当該教員のメールアカウントのパスワード変更等の対応を実施したというもの。不正ログイン時にメールボックスに保存されていた10月2日から10月17日のメールについて、攻撃者に閲覧された可能性がある。

トップページ

リリース（不正アクセスによるスパムメールの送信及び情報漏洩の可能性について（お詫び））

リリース（攻撃者に閲覧された可能性のある情報）

リリース（再発防止に向けた今後の取組み）

●NICTが「NICTER観測レポート2019」を公開…攻撃パケットは前年の1.5倍に

https://internet.watch.impress.co.jp/docs/news/1235048.html
https://www.nict.go.jp/press/2020/02/10-1.html

このニュースをザックリ言うと・・・

- 2月10日(日本時間)、情報通信研究機構(NICT)サイバーセキュリティ研究所より、サーバー攻撃関連通信の観測分析を行うNICTERプロジェクトの2019年における分析結果が「NICTER観測レポート2019」として公開されました。

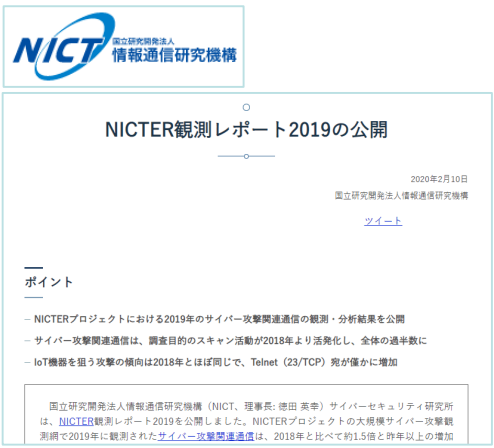
- レポートによれば、同プロジェクトで2019年に観測されたサイバー攻撃関連のパケットは合計3,279億個で、2018年(AUS便り 2019/2/25号参照)の2,121億個から約1.5倍に増加、うち53%近くの1,750億個が海外組織からの調査目的のものとされており、また1IPアドレスあたりの観測パケットは約120万個(前年：約79万個)と初めて100万個を超えています。

- 宛先ポート別のパケットの割合ではTelnetサービスで用いられるTCPポート23番宛が依然最も多く24.2%と前年(21.7%)より微増、その他のポートの結果も含め、Webカメラや家庭向けルーター等IoT機器を狙った通信の傾向は前年とほぼ同じとされています。

AUS便りからの所感

- この他、2019年に特徴的な事例として、SSL-VPN製品の脆弱性公表後に、これを悪用する攻撃が世界的に観測されたこと等が挙げられています。

- NICTではこれと並行して国内の脆弱なIoT機器について調査・注意喚起を行うプロジェクト「NOTICE」も実施しており、クライアントPC等と比べてユーザーの意識が届きにくいとみられるIoT機器の脆弱性に対し、ファームウェア等のアップデートやUTM等による外部からの無用なアクセスの遮断といった対策が行われていくことに期待したいものです。



●MSより月例セキュリティパッチ発表…Windows 7はESUなしでは適用できず

https://japan.zdnet.com/article/35147980/
https://portal.msrc.microsoft.com/ja-jp/security-guidance/releasenotedetail/2020-Feb

このニュースをザックリ言うと・・・

- 2月12日(日本時間)、マイクロソフト(以下、MS)より、2月度の月例セキュリティパッチが公開されました。

- 1月18日に報告されていたInternet Explorer(IE)の未修正の脆弱性(AUS便り 2020/1/27号参照)を含め、OS・Office等においても、PCが乗っ取られる恐れのある重大な脆弱性等が修正されており、適用が強く推奨されます。

- なお無償サポートが終了したWindows 7についてもセキュリティパッチが提供されていますが、一部エディション(Professional等)向けの有償サポート(ESU)加入者のみが適用可能となっています。

AUS便りからの所感

- 前述したIEの未修正の脆弱性は古いスクリプトエンジン(JScript.dll)にのみ存在し、通常使用されるスクリプトエンジンには影響しないとのことでしたが、悪用も確認されており、MSでは最も深刻度の高い「緊急」の脆弱性として扱っています。

- Windows 7については、1月にリリースされたセキュリティパッチの不具合を一部修正しているオプションパッチ(KB4539601)が事前にリリースされていますが、ESUに加入していないデバイスに適用できるのは現在これまでとみられ、今回のセキュリティパッチをインストールしようとしても失敗するとのことです。

- ESUに加入せず(できず)、脆弱性が未修正のまま稼働し続けるPCが今後も一定数残り、マルウェアの格好のターゲットとされると予想されますが、やむを得ない事情があり、周辺をアンチウイルスやUTMで固める、ネットワークから適宜隔離する、といった対策をとっていない限りは、10への移行計画を確実に行うようにしてください。