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。

●約6,500万件のアカウントによる「リスト型攻撃」のプログラム発見、メールの不正アクセスでサービス絞り込み

https://www3.nhk.or.jp/news/html/20200116/k10012247401000.html
https://www.sankei.com/affairs/news/200117/afr2001170004-n1.html
https://www.jc3.or.jp/topics/listattack.html

このニュースをザックリ言うと･･･

- 1月16日(日本時間)、茨城県警より、2019年5月に押収したサーバーから、Webサイトのアカウント情報約6,500万件が発見されたと発表されました。

- また、日本サイバー犯罪対策センター(JC3)が県警と連携して当該サーバーを調査したところ、このアカウント情報を利用した「リスト型攻撃」を効率的に実行するプログラムが発見されたとしています。

- JC3では同日、ここで発見されたとみられる中国語およびロシア語の攻撃プログラムの画像を提示した上で、リスト型攻撃への対策として「複数のオンラインサービスの間で同じパスワードを使いまわさない」よう注意喚起しています。

AUS便りからの所感等

- JC3による攻撃プログラムの解説によれば、奪取したアカウント情報(ID・パスワード)でまず電子メールサービスに不正ログインを行い、メールの内容を検索してそのユーザーが利用しているWebサイトを把握した上で、そのサイトへの不正ログインを行うとしており、攻撃対象のサービスの絞り込みによる不正ログインの効率化を行っていることが大きな特徴とされています。

- 先週のAUS便り(2020/1/20号)でリスト型攻撃の事件を取り上げた際、メールサービスが狙われる可能性も挙げていましたが、このようにターゲットの絞り込みに利用される可能性もあるため、Webサービスと同様、あるいはそれ以上にアカウントの保護に注意を払うべきです。

- リスト型攻撃への対策の一つに「他のサービスと共有していない、推測されにくいパスワードを設定する」ことが挙げられますが、JC3ではそのためにパスワードやその他アカウント情報をテキストファイルで保存することは流出のリスクがあるとし、信頼のおけるパスワード管理ソフトを利用する等、適切な保管を心がけることも呼び掛けています。

NHK NEWS WEB

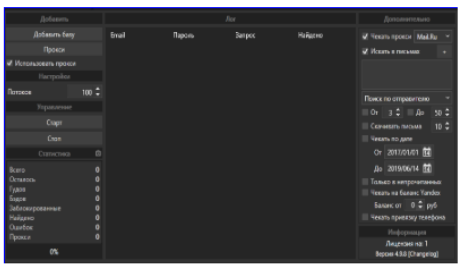
「リスト型攻撃」 新たなプログラム判明 効率的に不正接続か

2020年1月16日 16時51分

インターネット上で不正な接続を試みる「リスト型攻撃」に関する新たなプログラムが、茨城県で警察に押収されたサーバーから見つかったことが、捜査関係者への取材で分かりました。攻撃対象のサービスを絞り込み、効率的に不正接続を試みているとみられています。

JC3 日本サイバー犯罪対策センター
JC3 : Japan Cybercrime Control Center

図：中国語圏のツール



図：ロシア語圏のツール

●IEに未修正の脆弱性…回避策実行かIEの使用中止を

https://forest.watch.impress.co.jp/docs/news/1230028.html
https://www.jpcert.or.jp/at/2020/at200004.html

このニュースをザックリ言うと・・・

- 1月18日(日本時間)、マイクロソフト(以下、MS)より、Internet Explorer(IE)に未修正の脆弱性「CVE-2020-0674」が存在することが発表されました(翌19日にはJPCERT/CCからも注意喚起が出されています)。

- 脆弱性はIEの古いスクリプトエンジン(JScript.dll)に存在し、不正なスクリプトの実行により、PCを乗っ取られる可能性があるとされていますが、同15日に発表された月例のセキュリティパッチでは対策されていなかったものです。

- 2月12日に予定されている次回のパッチリリースまでは、MSが提示する回避策を実行するか、IE以外のブラウザー(Chrome・Edge・Firefox等)の利用が推奨されます。

AUS便りからの所感

- JScript.dllは互換性のために残されているコンポーネントとされ、現在IEにて既定で使用されるJScript9.dllあるいはEdgeで使用されるChakra.dllは脆弱性の影響を受けないとされています(またWindows Server上のIEは既定で制限モードで実行されるため影響が緩和されるとのことです)。

- 回避策の実行には各PC上で管理者権限でのコマンド実行が必要となり、またJPCERT/CCでも稀にJScript.dllを使用するWebサイトや文書ファイルの閲覧に影響が出る可能性を考慮するよう呼び掛けていますが、そもそもIE自体が互換性の為に残されている古いブラウザーであることを鑑み、IEから別ブラウザーへの移行のみならず、IEでしか利用できない社内向けWebサービス等が残っているならば改修を行うことも、重要なセキュリティ対策の一環となり得ます。

- なお別のブラウザーについても、同10日にはFirefox 72.0.1(https://forest.watch.impress.co.jp/docs/news/1228221.html)、同16日にはGoogle Chrome 79.0.3945.130(https://forest.watch.impress.co.jp/docs/news/1229906.html)と、脆弱性を修正したバージョンが相次いでリリースされていますので、Web閲覧が様々な攻撃の玄関口であることに注意を払い、各ソフトウェアの可能な限りのアップデートと、アンチウイルス・UTM等を含めた多重防御とを随時意識するのが良いでしょう。

●弘前市職員約2,700人分の個人情報流出、被疑者不明も内部犯行として告発

https://mainichi.jp/articles/20200109/k00/00m/040/021000c
https://www.itmedia.co.jp/news/articles/1912/13/news134.html
http://www.city.hirosaki.aomori.jp/oshirase/jouhou/2020-0108-1214-438.html

このニュースをザックリ言うと・・・

- 1月8日(日本時間)、青森県弘前市より、2019年12月12日に同市職員の個人情報が地元新聞のメールアドレス宛に匿名で送信された件について刑事告発したと発表されました。

- 流出した個人情報は、市職員と非常勤職員ほぼ全員にあたる計2,747人分の氏名・住所・月給額・および最終学歴等約70項目のデータとされています。

- これ以前の11月18日以降、市に対して流出を示唆するメールが数回送られ、一部に職員の個人情報が記載されていたことから市が調査を進めていましたが、実際の流出を受け、12月16日に市のホームページで発表されていました。

- データは市のNASで2017年度に作成・保存されていたものとみられ、被疑者は特定されていないもののNASにアクセス可能だった人事課の職員ないし元職員が流出に関与したものと結論付け、地方公務員法(守秘義務)違反容疑で刑事告発に至ったとのことです。

AUS便りからの所感

- 内部犯行による個人情報等の流出事案としては、2014年のベネッセや2017年のスタッフサービス、2018年に日経新聞社社員がPCを分解しHDDを抜き取って持ち出したケース等が挙げられます。

- 一方で、今回その形跡はなかったようですが、特定の人間がアクセス可能な領域への不正アクセスとしては、その人間のPCをマルウェアに感染させ、そこを踏み台にする手口も良く知られています。

- 内部の不正行為に対しても、標的型攻撃等でマルウェアに侵入されたケースに対しても有効な防御策として「出口対策」に関する何らかのソリューション導入を検討すること、かつ電子データから紙ベースに至るまであらゆる機密情報の処理について、関係者に対する十分な教育を行うことが、改めて重要となるでしょう。