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。

●ロシアのハッカー集団がプリンターから企業に侵入、MSが警告

https://www.technologyreview.jp/nl/russian-hackers-are-infiltrating-companies-via-the-office-printer/

https://japan.cnet.com/article/35140975/

このニュースをザックリ言うと･･･

- 8月5日(現地時間)、マイクロソフト(以下MS)のセキュリティ調査研究部門より、ロシアの諜報機関と関連しているとみられるハッカー集団「APT28」(「Strontium」「Fancy Bear」とも)がプリンターやWebカメラ等のいわゆるIoT機器を経由して企業のネットワークへの侵入を行っているとする調査結果が発表されました。

- MSではAPT28を1年間監視し続けており、標的となった、ないし侵入された組織に対し計1,400件の通報を送ったとしており、うち20%が世界中の非政府組織やシンクタンク、政治関連団体等で、残り80%は政府機関や企業となっています。

- また、侵入に成功した原因として、複数の事例でIoT機器のパスワードが工場出荷のままだったこと、別の事例において最新のセキュリティ更新プログラムを適用していなかったことを挙げています。

AUS便りからの所感等

- APT28は2007年頃から活動しているとされ、2016年にも米民主党全国委員会への侵入、2017年にはランサムウェア「Notpetya」によるウクライナ等への攻撃を行ったことで知られています。

- インターネット上からアクセス可能な状態になっているIoT機器を探し出すサーチエンジンとしては「SHODAN」「Censys」等が知られており、主に攻撃者がターゲットを探し出すために利用されていますが、一方で管理する側にとっても、外部からの不正アクセスの可能性がないか確認するための手段として有用です。

- 日本では今年に入り、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」が実施されましたが、MSの発表により、その有効性が実証されたとする意見もあります(https://finders.me/articles.php?id=1227)。

- 不特定多数から不正利用されないよう、必ずパスワードを変更し、またUTM等を用いた外部からのアクセス遮断を行うとともに、場合によってはそれでも外部からアクセスを受ける可能性がないか、第三者によるネットワーク診断を受けることも検討すべきでしょう。

MIT Technology Review
Published by KADOKAWA / ASCII

ロシアのハッカー集団がプリンターから企業に侵入、MSが警告

ロシアの諜報機関とつながりのあるハッカー集団が、インターネットに接続された携帯電話やプリンターといったIoT機器を使って企業のネットワークに侵入している。マイクロソフトが8月5日にブログで発表した。

このハッカー集団は、「ストロンチウム（Strontium）」または「ファンシー・ベアー（Fancy Bear）」「APT28」といった名称で呼ばれる集団。ロシア軍の情報機関であるロシア連邦軍参謀本部情報総局（GRU）と通じているとされる。

このハッカー集団は少なくとも2007年には活動を開始しており、数々の悪名高いハッキング行為への関与が確認されている。2016年には米民主党全国委員会（Democratic National Committee）に侵入。2017年にはあらゆる重要データを破壊する「ナットペトヤ（Notpetya）」を使ってウクライナを攻撃し、2018年は年間を通じて欧州や北米地域の政治団体へ攻撃を仕掛けたとされる。

●システム管理ツール「Webmin」脆弱性を標的としたアクセス

…警察庁が観測

https://internet.watch.impress.co.jp/docs/news/1203427.html

http://www.npa.go.jp/cyberpolice/important/2019/201908231.html

このニュースをザックリ言うと・・・

- 8月23日(日本時間)、警察庁より、ウェブベースのシステム管理ツール「Webmin」の脆弱性を標的としたアクセスを観測したと発表されました。

- Webminバージョン1.882～1.921に存在する、サーバー上で任意のコマンドが実行可能になる脆弱性を狙ったものとされ、修正バージョンである1.930以降へのアップデートが推奨されます。

- Webminが通常使用するTCPポート10000番の他、HTTPと同じ80番、あるいは20842番へのアクセスも少なからず観測されているとのことです。

AUS便りからの所感等

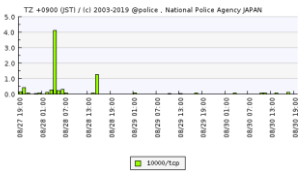
- Webminは主にLinuxサーバーにおいて、ユーザーアカウントの追加や各種ネットワーク設定あるいはWebサーバー・DBサーバーの設定等、多種多様な管理をブラウザーから行えるツールです。

- Webminは上記のような各種設定を行うためにOSの管理者権限で動作するようになっており、不特定多数がこれに外部からアクセス可能な状態になっていることは非常に危険です。

- サーバー上の各種ソフトウェアを常時最新に保つという根本的対策はもちろんですが、管理用ポートに不特定多数が外部からアクセスできないよう、サーバーOS自体やその前方に設置するUTM等のファイアウォール設定を行うことが重要です(特定IPアドレスからのみアクセス許可する設定が良く用いられますが、VPN等を経由した場合のみアクセス可能にする等、より安全な設定も考えられます)。

警察庁 National Police Agency @police

Webminの脆弱性（CVE-2019-15107）を標的としたアクセスの観測状況（グラフ）



●三井住友カード、スマホアプリで16,756件の不正ログイン

https://this.kiji.is/537520310005875809

https://japan.cnet.com/article/35141692/

https://www.smbc-card.com/company/news/news0001468.pdf

このニュースをザックリ言うと・・・

- 8月23日(日本時間)、三井住友カードより、会員向けスマートフォンアプリ「三井住友カードVpassアプリ」において、第三者による不正ログインが発覚したと発表されました。

- 約500万件の不正ログイン試行が行われ、16,756件のIDに対する不正ログインが確認されており、氏名・カード名称・カード利用金額・利用明細・利用可能額が閲覧された可能性があるとのことですが、悪用被害は確認されなかったとのことです。

- 同社では同19日に攻撃を検知しており、不正ログインを受けたユーザーのパスワード無効化を行うとともに、個別にID・パスワードの変更を行うよう連絡したとのことです。

AUS便りからの所感等

- 不正ログイン試行の際、同サービスに存在しないID・パスワードが試行された形跡があることから、外部サービスから流出したID・パスワードを悪用したいわゆる「リスト型攻撃」であるとされています。

- 同社ではクレジットカード番号の一部をマスクしており、流出はないともしていますが、実際にはカード番号16桁のうち下3桁だけがマスクされており、上位13桁は見える状態になっていたとの情報があり、場合によっては現実的な回数の総当たり等により、カード番号全てが取得されてしまう可能性が指摘されています。

- 現時点で悪用被害は確認されていないとしていますが、上記のような指摘もあり、日をおいての二次被害発生の可能性も皆無とは言えず、被害を受けたカードの悪用をいかに確実に水際で食い止められるかが注目されるところです。

KYODO

1万6000件不正ログインか

三井住友カードのアプリ

2019/8/23 15:33 (JST) | 8/23 19:27 (JST) updated

©一般社団法人共同通信社

三井住友カードは23日、会員向けのスマートフォンアプリ「Vpassアプリ」が外部から不正アクセスを受け、1万6756件の顧客IDで不正なログインがあった可能性があると発表した。クレジットカードの番号漏えいや悪用の被害はないが、氏名や利用明細などが閲覧された恐れがあるという。

同社によると、8月19日に実施した通常の検査で発覚した。不正ログインがあったIDのパスワードは無効にし、顧客にも個別に連絡した。