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。

●ニコニコ動画で不正ログイン被害…リスト型攻撃か

http://www.itmedia.co.jp/news/articles/1805/11/news093.html
http://blog.nicovideo.jp/niconews/73053.html

このニュースをザックリ言うと･･･

- 5月10日（日本時間）、ドワンゴ社より、同社が運営する「ニコニコ動画(niconico)」において、5月上旬にアカウントへの不正ログインが複数確認されたとして注意喚起が出されています。

- 発表では、ニコニコ動画自体からのアカウント情報流出ではなく、他のサービスから流出したアカウント情報をもとにした「リスト型アカウントハッキング攻撃」の可能性を示唆しています。

- 対象となったアカウントについては、従来のパスワードではログインできないよう設定し、個別にメールで案内しており、「パスワードが他のサービスと同一であった場合には変更する」よう求めています。

AUS便りからの所感等

- 今年2月以降、様々なサービスから流出したとされるアカウント情報がネット上で公開される事態が発生しており（AUS便り 2018/05/07号参照）、攻撃者はそのアカウント情報をもとに不正ログインを行った可能性があります。

- ニコニコ動画では2016年4月に2段階認証を導入しており、パスワードを他のサービスと同じものにしないことはもちろん、2段階認証についても是非とも設定し、アカウントの保護を行うことを推奨致します。

- リスト型攻撃は自社サーバが被害を受けないということは決してなく、組織で使用しているオンプレミスあるいはクラウド上のWeb・メールサーバに対し不正ログインの試行が行われる可能性もあり、不正ログイン試行の兆候を検知し遮断できるよう、サーバの設定やUTM等によるIDS・IPS機能の有効化も検討に値するでしょう。

ITmedia NEWS

niconicoで不正ログイン被害　リスト型攻撃か

2018年05月11日 12時57分 公開　[ITmedia]

印刷　通知　169　14　B! 16

ドワンゴは5月10日、同社のコンテンツサービス「niconico」で5月上旬から、ユーザー本人のものではないと思われるログインを複数検出しているとし、「リスト型アカウントハッキング攻撃の可能性がある」としてユーザーに注意を呼び掛けた。不正ログインが成功したとみられるアカウントについては、従来のパスワードではログインできないよう設定し、個別にメールで案内したという。

リスト型アカウントハッキングは、他社サービスなどから流出したメールアドレス・パスワードを大量に入手し、ログインを試す攻撃。

niconicoのアカウントが第三者にログインされると、ニコニコポイントを利用されたり、登録メールアドレスやパスワードを変更されたり、性別や生年月日などの情報が閲覧されるおそれがあるという。

同社は、niconicoアカウントのパスワードを他サービスと共通にしているユーザーには、パスワードを変更するよう呼び掛けた。ログイン履歴を専用ページで確認し、身に覚えのない履歴が表示された場合は早急にパスワードを変更してほしいとしている。また、二段階認証を設定するようッ推奨している。

ニコニコインフォ

他社流出パスワードを用いた不正ログインについて(2018/05)

2018年05月10日　Tweet　いいね！ 46　G+　B!ブックマーク 70

いつもniconicoをご利用いただきありがとうございます。

2018年5月上旬より、本人によるものではないと思われるniconicoアカウントへのログインを、複数検出しております。
niconico以外のサービスで使われているメールアドレス・パスワードの組み合わせを不正に入手し、同じメールアドレス・パスワードでniconicoにログインできないかを試しているものと思われます。
※「リスト型アカウントハッキング」などと呼ばれる攻撃の手口です。

▼ 不正にログインされてしまった場合、発生しうること

●niconicoサービス内
・所有しているニコニコポイントの利用
・ニコニコポイントの追加購入(オートチャージ設定が有効な場合など)
・登録メールアドレスやパスワードの変更
・動画やコメントなどの投稿
・公開範囲を限定している登録情報の閲覧（性別、生年月日等）など

●niconicoサービス外
・niconicoへのログインが成功したことにより、他のサービスも同様の手口でログインできると攻撃者に推測され、niconico以外のサービスでも不正にログインされてしまう可能性があります。

▼ ご利用の方々に、ご検討、ご対応いただきたいこと

niconicoアカウントのパスワードが他サービスと共通のものである場合、他サービスとは異なるパスワードに変更することをご検討ください。

●森永乳業の通販サイトからクレカ情報23,000件漏えいか

https://netshop.impress.co.jp/node/5404

このニュースをザックリ言うと・・・

- 5月9日（日本時間）、森永乳業より、同社運営の健康食品通販サイトからクレジットカード情報が流出した可能性があると発表されました。

- 対象となるのは、2017年1月10日～2018年4月24日に、当該サイトで決済に使われた最大約23,000件分のカード情報（番号、名義、有効期限およびセキュリティコード）とされています。

- 4月24日にカード会社から不正利用に関する連絡があって発覚したもので、現在第三者機関による調査が続いており、不正アクセスか否か、あるいは経路についてはまだ明らかになっていません。

AUS便りからの所感等

- カード情報の中でも磁気ストライプ情報やセキュリティコードといった「機密認証データ」については、クレジットカードにおけるデータセキュリティの国際基準である「PCIDSS」において、加盟店側での保持が禁止されています。

- 「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」により、EC事業者は2018年3月末までに、カード情報を保持しないシステムとする、あるいはPCIDSSに準拠することが要求されていましたが、仮に流出が事実だとして、その期限までに準拠が間に合わず、かつこのような事態が発生したことは痛恨と言えます。

- UTM等を用い、不正アクセスされない・されても情報が流出しないシステムを構成するだけでなく、流出しては困るセンシティブな情報について可能な限り保持しない仕組みにすることについても、流出によるダメージを抑えるための方策としては重要です。

●内閣府サイトからアダルトサイトにリンク‥原因は特設サイトのドメイン失効

http://www.itmedia.co.jp/news/articles/1805/09/news089.html

このニュースをザックリ言うと・・・

- 5月9日（日本時間）、内閣府のWebサイトからアダルトサイトへのリンクが張られているという情報がSNS等で拡散しました。

- 問題が指摘されたのは、内閣府「戦略的イノベーション創造プログラム(SIP)」の2015年のシンポジウムに関するページで、特設サイトへのリンクを辿ると、アダルトサイトが表示されるという状態になっていました。

- 特設サイトは内閣府のドメイン（cao.go.jp）とは別の外部ドメイン上で運営されていましたが、これが失効し、その後第三者に取得されたことが原因です。（なお、同日昼には当該ページは削除されています。）

AUS便りからの所感等

- 政府系のWebサイトで発生したことから比較的大きく取り上げられ、このようなことがないよう同じドメイン下で運営すべきだった等の指摘がなされていますが、一時的なイベントや映画作品等の特設サイトのために独自にドメインが取得されることも、失効したドメインを第三者に取得されることによるリスクの指摘も、長年繰り返されてきています。

- この他にも、大手シネコンが買収により古いドメインを放棄したことでやはり失効後に第三者に取得されたことにより、シネコン側が古いドメインへのアクセスを行わないよう注意を呼び掛ける事態にもなったことがあります。

- サイトを運営する側についてはこういったリスクをはらんでいる事実を鑑みながら、ドメインの取得・維持および後始末等に十分に注意を払うこと、また閲覧する側も不審なサイトへのアクセスに際しブラウザ・アンチウイルスおよびUTMのアンチフィッシング機能をそれぞれ有効化する等の防御を固めることが重要です。