NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2017年9月版 (第22号)＞(選り抜き版)

2017年9月25日
ＮＴＴデータ先端技術株式会社
セキュリティ事業部

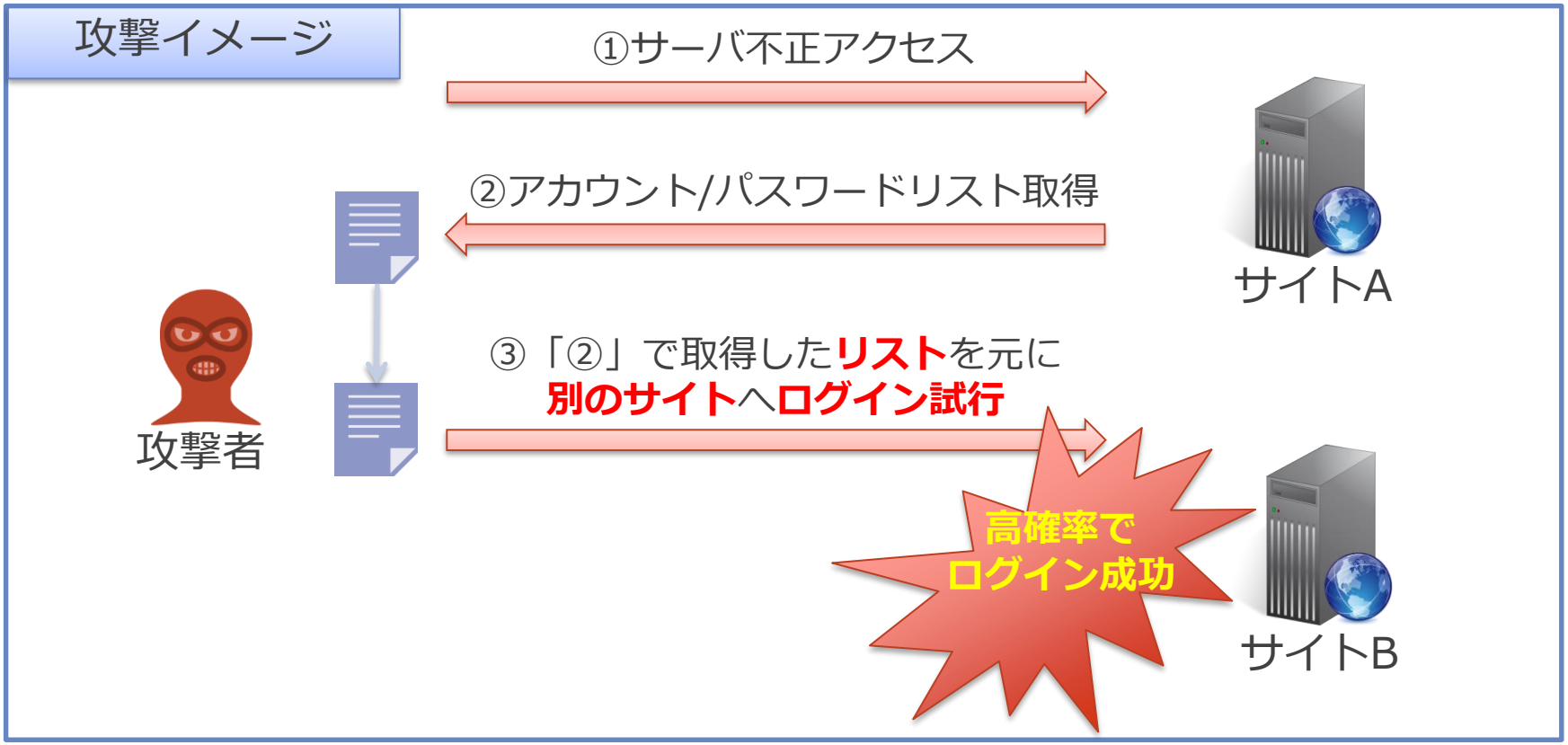
今回のサマリー

ディノス・セシール通販サイトに「なりすまし」による不正アクセス
繰り返されるリスト型アカウントハック！ - ディノス・セシールの場合、「リスト型アカウントハック(リスト型攻撃)」が利用されました。この攻撃手法について改めて解説するとともに、ユーザと企業が取るべき対策を解説します。

繰り返されるリスト型アカウントハック！
～ ディノス・セシールの場合 ～

1. リスト型アカウントハックの概要 (1/2)

リスト型アカウントハックとは、ウェブサイトに対する不正ログイン攻撃手法の一種です。
オンラインサービスの増加に伴い、ユーザには複数のアカウントとパスワードの管理が求められるようになりました。ただし実態は同一のアカウントとパスワードを複数のウェブサイトで使いまわしているユーザが多く、一つのウェブサイトでパスワードの漏えいが起きた場合に悪用されやすく、被害も拡大しやすくなります。



1. リスト型アカウントハックの概要 (2/2)

IPAが毎年発刊する「情報セキュリティ 十大脅威」でも常に上位にランクインする攻撃手法であり、企業/ユーザの認知度も年々高まっています。

	IPA 情報セキュリティ 十大脅威					
	2013年度	2014年度	2015年度	2016年度	2017年度(個人)	2017年度(組織)
1位	クライアントソフトの脆弱性を突いた攻撃	標的型メールを用いた組織へのスパイ・諜報活動	インターネットバンキングやクレジットカード情報の不正利用	インターネットバンキングやクレジットカード情報の不正利用	インターネットバンキングやクレジットカード情報の不正利用	標的型攻撃による情報流出
2位	標的型諜報攻撃の脅威	不正ログイン・不正利用	内部不正による情報漏えい	標的型攻撃による情報流出	ランサムウェアによる被害	ランサムウェアによる被害
3位	スマートデバイスを狙った悪意あるアプリの横行	ウェブサイトの改ざん	標的型攻撃による諜報活動	ランサムウェアを使った詐欺・恐喝	スマートフォンやスマートフォンアプリを狙った攻撃	ウェブサービスからの個人情報の窃取
4位	ウイルスを使った遠隔操作	ウェブサービスからのユーザー情報の漏えい	ウェブサービスへの不正ログイン	ウェブサービスからの個人情報の窃取	ウェブサービスへの不正ログイン	サービス妨害攻撃によるサービスの停止
5位	金銭窃取を目的としたウイルスの横行	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取	ウェブサービスへの不正ログイン	ワンクリック請求等の不当請求	内部不正による情報漏えいとそれに伴う業務停止
6位	予期せぬ業務停止	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ	ウェブサイトの改ざん	ウェブサービスからの個人情報の窃取	ウェブサイトの改ざん
7位	ウェブサイトを狙った攻撃	SNS への軽率な情報公開	ウェブサイトの改ざん	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ	ネット上の誹謗・中傷	ウェブサービスへの不正ログイン
8位	パスワード流出の脅威	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃	内部不正による情報漏漏えいとそれに伴う業務停止	情報モラル欠如に伴う犯罪の低年齢化	IoT 機器の脆弱性の顕在化
9位	内部犯行	ウイルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃	巧妙・悪質化するワンクリック請求	インターネット上のサービスを悪用した攻撃	攻撃のビジネス化(アンダーグラウンドサービス)
10位	フィッシング詐欺	サービス妨害	悪意のあるスマートフォンアプリ	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加	IoT 機器の不適切な管理	インターネットバンキングやクレジットカード情報の不正利用

※「リスト型アカウントハック」の名称は2014年度から使用されています

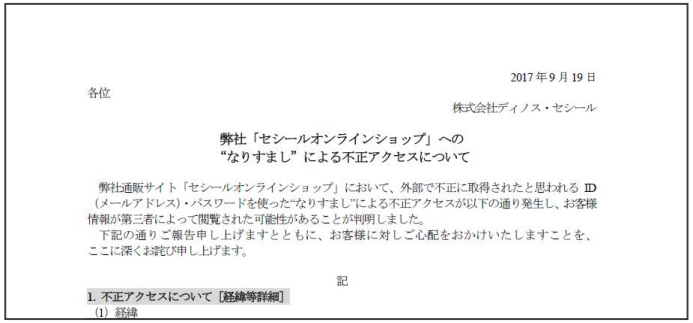
2. リスト型アカウントハックによる被害 (ディノス・セシール 2017) (1/2)

2017年、セシールオンラインショップが複数回のアカウントリスト型ハックの攻撃を受けたとされています。本件においてはディノス・セシール社の調査の結果、「正規ユーザがログインした覚えがないタイミングで、ユーザのアカウントにてログイン操作が行われた」ことが確認できたため、不正アクセスであることが確定しました。

ディノスセシール社管理のオンラインショップへの不正アクセス (2017年)

日時	試行回数	ログイン成功	成功率	被害
2017/7/31 15:01～15:02	11回	1回	9%	顧客情報1名分(氏名・所有ポイント)が第三者に閲覧された可能性あり
2017/8/21	-	2回 (8/22と同一IPアドレスからアクセス)	ー	顧客情報1名分(氏名・所有ポイント)が第三者に閲覧された可能性あり 及び顧客情報改ざん(第三者のクレジットカード情報を登録)
2017/8/22 02:21～02:31	11回	1回	9%	顧客情報1名分(氏名・所有ポイント)が第三者に閲覧された可能性あり

セシールWebサイト



2017年9月19日

各位

株式会社ディノス・セシール

弊社「セシールオンラインショップ」への
“なりすまし”による不正アクセスについて

弊社通販サイト「セシールオンラインショップ」において、外部で不正に取得されたと思われるID（メールアドレス）・パスワードを使った“なりすまし”による不正アクセスが以下の通り発生し、お客様情報が第三者によって閲覧された可能性があることが判明しました。
下記の通りご報告申し上げますとともに、お客様に対しご心配をおかけいたしますことを、ここに深くお詫び申し上げます。

記

1. 不正アクセスについて［経緯等詳細］
（1）経緯

出典：https://www.dinos-cecile.co.jp/whatsnew/pdf/topics_20170919.pdf

2. リスト型アカウントハックによる被害 (ディノス・セシール 2017) (2/2)

ただ先述の調査結果から不正アクセスされたことは明白ですが、なぜ攻撃手法がリスト型アカウントハックであると特定できたのでしょう？

それは「ログイン試行回数に対する”成功率の高さ”」にあるといえます。

セシールオンラインショップにおけるアカウント、パスワードの設定ポリシは以下の表のとおりとなっています。最も脆弱な組み合わせである「メールアドレス(公知)+パスフレーズ(数字のみ4桁)」で試算しても、総当たり攻撃の成功率は0.01%(10000回に1回)です。今回の攻撃ではわずか11回ずつ(約10%の確率)で攻撃に成功しており、偶然にしては高すぎます。この成功率の高さがリスト型アカウントハックの最大の特徴といえます。

セシールオンラインショップ　アカウント/パスワード設定				
設定ポリシ				備考
アカウント (いずれか片方)	お客様番号	数字	9桁	推測可能である可能性あり
	メールアドレス	英語、数字、記号	約10桁以上	メールアドレスは公知である可能性あり
パスワード	パスワードフレーズ	英数字	4～15桁	-

【！ポイント！】
ログイン試行による不正ログインの対策方法に、アカウントを一定期間使用できなくさせる「アカウントロックアウト」がありますが、10%近い成功率であるとロックする前に突破される可能性が高く、対策が機能しない恐れがあります。

3. リスト型アカウントハックによる被害 (ディノス・セシール 2016以前)

　ディノス・セシール社では、過去にもアカウントリスト型ハックによる攻撃を受けています。都度パスワードの変更や監視体制の強化、注意喚起を行っていますが根本的な解決には至っていません。
　なおユーザの利便性を優先してか、設定できるアカウントとパスワードに大きな変更はないようです。

ディノスセシール社管理のオンラインショップへの不正アクセス (2016年以前)				
日時	**試行回数**	**ログイン成功**	**成功率**	**被害**
2013/5/8 09:30	111万回	1.5万回	1.3%	お客様情報(氏名・所有ポイント)が第三者に閲覧された可能性あり
2016/8/31 22:36～22:50	50回	8回	16%	
2016/9/3 13:45～13:52	30回	7回	23%	

4. リスト型アカウントハックによる被害 (ニッセン)

興味深いのは、同業他社であるニッセン社のオンランショップサイトにおいても、同時期に攻撃を受けていることです。

ニッセン社管理のオンラインショップへの不正アクセス					
日時	試行回数	ログイン成功	成功率	被害	(参考)ディノス・セシール
2013/6/18 16:48～22:28	11,031回	126回	1.1%	詳細は非公開	2013/5/8 09:30

ニッセン社のサイトにおけるアカウント、パスワードの設定ポリシは、ディノス・セシール社と同等となっており、同一の設定とすることも可能です。

ニッセン社管理のオンラインショップ　アカウント/パスワード設定				
設定ポリシ				(参考)ディノス・セシール
アカウント (いずれか片方)	お客様番号	数字	10桁	9桁
	メールアドレス	英語、数字、記号	大凡10桁以上	大凡10桁以上
パスワード	パスワードフレーズ	英数字	5～8桁	4～15桁

2社とも提供しているサービスとしては類似のサービスですので、両方のサイトを利用しているユーザが多いと推測できます。そのため、ディノス・セシール社及び、ニッセン社以外の企業が管理する同様のオンラインショップで2013年5月8日以前に漏えいしたアカウント/パスワード情報が悪用されたものと考えられます。

5. その他のリスト型アカウントハックによる被害

ディノス・セシール社やニッセン社以外でも、毎年のように多くの企業がリスト型アカウントハックにより攻撃を受けており情報漏えいなどの被害に繋がっています。
以下表では、ログイン成功率1%以上の事例を掲載しています。

企業名	サイト名	日付	試行回数	ログイン成功	成功率
イーブックイニシアティブジャパン	eBookJapan	2013/4/5	2821回	779回	27%
Panasonic	CLUB Panasonic	2014/4/23	460万回	7万8361回	1.7%
ドワンゴ	ニコニコ動画	2014/6/13	220万回	22万回	10%
Mixi	Mixi	2014/6/17	430万回	26万3596回	6.1%
サイバーエージェント	Ameba	2014/6/24	229万3543回	3万8280回	1.6%
ヤマト運輸	クロネコメンバーズ	2014/9/26	19万回	1万589回	5.5%
So-net	PostPetメールアカウントサービス	2015/1/13	1万8877回	1835回	9.7%
東京ガス	東京ガスオートサービス	2016/3/7	138回	4回	2.9%
サイバーエージェント	Ameba	2016/5/11	223万6076回	5万905回	2.2%
丸井	マルイウェブチャネル	2016/9/4	302回	32回	10%
サイバーエージェント	Ameba	2016/11/28	3754万回	59万回	1.5%

6. 対策方法

先述のとおりリスト型アカウントハックの手法を用いられた場合、正常のログイン試行の範囲内で攻撃が行われるため従来の対策手法であるアカウントロック制御だけでは対策として不十分です。そのため、以下に挙げるような追加対策についても導入を検討する必要があります。

対策	詳細
通信の監視	同一のIPアドレスから短時間に大量にログイン試行をするケースがないか、常に監視することを検討してください。「通常のユーザが、同一の時間帯に異なるアカウントで複数回にわたりログイン試行する」ことは不自然であるといえます。閾値を設け、場合によっては都度ユーザに確認を取るなどの対応が必要となります。
IPロックアウト制御の導入	同一のIPアドレスから短時間に大量にログイン試行があった場合、当該IPアドレスをロックすることを検討してください。アカウントロック制御と組み合わせることでより効果的に攻撃を防ぐことが可能です。 ただしモバイル環境など、攻撃者と正規ユーザが同一のIPアドレスを使用している場合、正規ユーザもロックアウトされる恐れがあるため、導入される場合は十分な検討が必要となります。
多要素認証の導入 (要素:知る)	認証に使用する情報を、従来のアカウントとパスワードのみではなく、本人のみが知りうる情報を加えることを検討してください。その際、他のサイトで情報として登録されうることのない独創的な内容の情報とすることが効果的です。
多要素認証の導入 (要素:持つ)	認証に使用する情報を、従来のアカウントとパスワードのみではなく、本人のみが持ちうる情報を加えることを検討してください。例えばワンタイムトークンや生態認証などが挙げられます。
機械的ログイン試行の阻害	攻撃者がPCを用いて機械的にログイン試行を行うことを阻害する方法を検討してください。例えば認証画面に都度異なる画像を表示し、人間が判断して画像の内容を入力することを求めるCAPTCHAが挙げられます。
ログインアカウントの使い回し	ユーザアカウント(ログインユーザ名)に、メールアドレスや電話番号等公知の情報を利用しない。
リスクベース認証	ユーザが利用しない地域やブラウザ、デバイス等、脅威と定義されたIPアドレス等から、「不正のリスク」を判定し、高リスクと判定された場合には追加認証などを行うような仕組みです。
ユーザへの注意喚起	リスト型アカウントハックに関する説明文と共に、他サイトで登録しているアカウントとパスワードを使用しないようユーザに注意喚起を行うことを検討してください。

7. まとめ

　攻撃者がリスト型アカウントハックの手法を用いるためには、どこかのシステムまたはサイトにおいてアカウントとパスワードのリストを入手する必要があります。
　企業において自衛という意味では前頁で挙げた様な対策が必要となりますが、その他にも攻撃に加担しないために、情報が漏えいすることがないようセキュアなシステム/サイトを構築するための努力が求められます。

　また本攻撃手法における根本的な問題は、ユーザのパスワード運用によるものですので、ログインを伴うシステムを運用されている方は、引き続きユーザに対する注意喚起を行っていくことが重要です。
　不正ログインの成功率が高い場合には、他サービスでも多く使われているアカウント/パスワード情報を用いて攻撃を行うことが考えられます。
　それに対する対策として、速やかに他サービスと異なるアカウント/パスワードへの変更を利用者へ促す等の対策が必要です。

　これらの他に、ダミーアカウントを自システムに登録しておき、漏えいの検知や、漏えいされていることの確認に用いる方法も考えられます。

8. 参考URL

- 弊社「セシールオンラインショップ」への“なりすまし”による不正アクセスについて
  https://www.dinos-cecile.co.jp/whatsnew/pdf/topics_20170919.pdf
- ディノス・セシール 弊社「セシールオンラインショップ」への“なりすまし”による不正アクセスについて
  https://www.dinos-cecile.co.jp/pdf/topics_20170824-2.pdf
- ディノス・セシール 弊社「セシールオンラインショップ」への不正アクセスについて
  http://www.cecile.co.jp/fst/information/20160905.pdf
- ディノス 【重要】弊社運営のオンラインショッピングサイトへの不正ログイン被害について
  https://www.dinos.co.jp/guide/info/pdf/20130513.pdf
  https://www.dinos.co.jp/guide/info/pdf/20130509.pdf
- ニッセン 【重要】ニッセンオンラインショッピングサイトへの不正ログイン状況、及びお客様へのお願いについて
  http://www.nissen-hd.co.jp/ir/pdf/IR_13_06_19_1.pdf
- IPA 10大脅威 2017
  https://www.ipa.go.jp/security/vuln/10threats2017.html
- IPA 10大脅威 2016
  https://www.ipa.go.jp/security/vuln/10threats2016.html
- IPA 10大脅威 2015
  https://www.ipa.go.jp/security/vuln/10threats2015.html
- IPA 10大脅威 2014
  https://www.ipa.go.jp/security/vuln/10threats2014.html
- IPA 10大脅威 2013
  https://www.ipa.go.jp/security/vuln/10threats2013.html
- パスワードリスト攻撃(アカウントリスト攻撃)の公表事例
  http://jamhelper.com/caseoflistattack/
- Piyolog パスワードリスト攻撃の2013年4月～8月の状況についてまとめてみた
  http://d.hatena.ne.jp/Kango/20130818/1376839935

NTT DATA

Trusted Global Innovator