情報漏洩
診断レポート

example.com

本レポートは、2025年2月20日時点の情報に基づき作成されています。

お問い合わせ先：wa-asm-support@ntt.com
NTTコミュニケーションズ株式会社

目次

- 1. 診断対象 3
- 2. 診断結果 - 概要 5
- 3. 診断結果 - 詳細 7

1. 診断対象

トップドメイン「example.com」を基点として、以下に示すドメイン名を検出しました。 本レポートでは、これらのドメイン名に対して、情報漏洩に関する診断を実施し、その結果を記載しております。

No	ドメイン名
1	example.com
2	o.example.com
3	h.example.com
4	0.example.com
5	r.example.com
6	7.example.com
7	a.example.com
8	3.example.com
9	5.example.com
10	9.example.com
11	s.example.com
12	m.example.com
13	4.example.com
14	w.example.com
15	6.example.com
16	x.example.com
17	8.example.com
18	1.example.com
19	c.example.com
20	p.example.com
21	i.example.com
22	v.example.com
23	d.example.com
24	43.example.com
25	m5.example.com
26	34.example.com
27	55.example.com
28	m4.example.com
29	97.example.com
30	ss.example.com
31	wk.example.com
32	87.example.com
33	kr.example.com
34	hk.example.com
35	90.example.com
36	98.example.com
37	mt.example.com
38	m9.example.com
39	33.example.com
40	qg.example.com
41	m3.example.com
42	ua.example.com
43	a7.example.com
44	fc.example.com
45	70.example.com
46	32.example.com
47	dl.example.com

No	ドメイン名
48	it.example.com
49	rs.example.com
50	15.example.com
51	76.example.com
52	h3.example.com
53	lo.example.com
54	en.example.com
55	h1.example.com
56	a6.example.com
57	23.example.com
58	82.example.com
59	m8.example.com
60	hv.example.com
61	86.example.com
62	61.example.com
63	88.example.com
64	ro.example.com
65	ja.example.com
66	63.example.com
67	al.example.com
68	71.example.com
69	36.example.com
70	cm.example.com
71	92.example.com
72	m6.example.com
73	31.example.com
74	ni.example.com
75	17.example.com
76	09.example.com
77	mb.example.com
78	tl.example.com
79	f2.example.com
80	59.example.com
81	h2.example.com
82	ao.example.com
83	la.example.com
84	48.example.com
85	54.example.com
86	57.example.com
87	f1.example.com
88	me.example.com
89	64.example.com
90	96.example.com
91	04.example.com
92	cc.example.com
93	a9.example.com
94	i9.example.com
95	s4.example.com
96	12.example.com
97	11.example.com
98	bd.example.com
99	dc.example.com
100	pg.example.com

2. 診断結果 - 概要

今回の診断結果は下記となります。

緊急	高	中	低	情報
4件	33件	8件	2件	1件

リスクレベル	説明
緊急	攻撃の対象となった場合、被害が甚大、もしくは攻撃が容易に実行可能な状態
高	攻撃の対象となった場合、影響が大きい、またはある程度の知識や技術、推測ができれば攻撃が可能な状態
中	攻撃の対象となった場合、影響が限定的または間接的で、攻撃の実行難易度が比較的高い状態
低	攻撃の対象となった場合、影響が軽微であり、攻撃の実行には複数の条件が必要など、実現が困難な状態
情報	セキュリティ上の潜在的なリスクや改善の余地があるポイントを示す情報

早急に対策が必要な「緊急」の脅威は下記の通りです。

緊急	1. ダークウェブにて情報漏洩を検出 - AntiPublic				
解決方法	他サービス含め、同じパスワードを使い回しているサービスがあればそのパスワードを変更する				
対象のIT資産	メールアドレス	パスワード	電話番号	ユーザ名	氏名
1.1	laz_kral_@example.com	05*****4			
1.2	missrose@example.com	on*********e			
1.3	nicolenorman_009_@example.com	ni****0			
1.4	luisbernal@example.com	ni****0			
1.5	lalsouth@example.com	te********7			
1.6	mEHevaXoAiyfq@example.com	mE**********q			
1.7	qiaomumumu@example.com	12******9			

緊急	2. ダークウェブにて情報漏洩を検出 - 2844Breaches				
解決方法	他サービス含め、同じパスワードを使い回しているサービスがあればそのパスワードを変更する				
対象のIT資産	メールアドレス	パスワード	電話番号	ユーザ名	氏名
1.1	aatal864@example.com	33***5			
1.2	ai@example.com	ai*****k			
1.3	kba62788@example.com	kb*****8			
1.4	tester@example.com	te***r			
1.5	netsparker@example.com	t2*****j			
1.6	antonio_loqueando@example.com	sa**********l			

緊急	3. ダークウェブにて情報漏洩を検出 - 123RF				
解決方法	他サービス含め、同じパスワードを使い回しているサービスがあればそのパスワードを変更する				
対象のIT資産	メールアドレス	パスワード	電話番号	ユーザ名	氏名
1.1	Jose87siu@example.com	1A*********a			
1.2	asdf@example.com	as*****q			
1.3	Blablatrucmachin@example.com	sp*******4			
1.4	a_l_e_x@example.com	ue*****h			
1.5	usernamefromsl@example.com	us*****e			

緊急	4. フィッシングドメインの可能性				
解決方法	フィッシングサイトのホスティングプロバイダに連絡し、違反を報告します。通常、プロバイダは速やかに対応し、サイトを閉鎖します。また、ドメインを登録している機関にフィッシングの報告を行い、ドメインの停止を依頼します。				
対象のIT資産	ドメイン名	類似ドメイン名	国	サーバ	類似率
1.1	example.com	example.org	United States		100%

1.2	example.com	example.net	United States		100%
1.3	example.com	example.edu	United States		100%

3. 診断結果 - 詳細

以下は、危険度が「緊急」「高」「中」「低」「情報」に分類された脅威の一覧です。将来的に重大なリスクに発展する脅威が存在するため、対策を講じることを推奨します。

No	カテゴリ	内容	危険度	件数
1	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AntiPublic	緊急	1
2	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 2844Breaches	緊急	1
3	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 123RF	緊急	1
4	フィッシングドメイン	フィッシングドメインの可能性	緊急	1
5	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Tumblr	高	1
6	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - PokemonCreed	高	1
7	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Peatix	高	1
8	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - LinkedIn	高	1
9	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Lifebear	高	1
10	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Dailymotion	高	1
11	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Appen	高	1
12	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Animoto	高	1
13	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AnimeGame	高	1
14	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AnimalJam	高	1
15	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AndroidLista	高	1
16	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AndroidForums	高	1
17	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Altenen	高	1
18	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AlpineReplay	高	1
19	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Ajarn	高	1
20	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Aipai	高	1
21	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AdultFriendFinder2016	高	1
22	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Adobe	高	1
23	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Adecco	高	1
24	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AcneOrg	高	1
25	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AbuseWithUs	高	1
26	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - ABFRL	高	1
27	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Abandonia2022	高	1
28	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Abandonia	高	1
29	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 8tracks	高	1
30	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 8fit	高	1
31	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 7k7k	高	1
32	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 500px	高	1
33	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 17Media	高	1
34	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 17173	高	1
35	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - 000webhost	高	1
36	ブラックマーケット	ブラックマーケットに情報の漏洩の可能性あり	高	1
37	フィッシングドメイン	フィッシングドメインの可能性	高	1
38	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Twitter200M	中	1
39	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Facebook	中	1
40	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Duolingo	中	1
41	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Apollo	中	1
42	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - ApexSMS	中	1
43	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AIType	中	1
44	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - AdultFriendFinder	中	1
45	フィッシングドメイン	フィッシングドメインの可能性	中	1
46	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - Zurich	低	1

No	カテゴリ	内容	危険度	件数
47	情報漏洩発生サービス	ダークウェブにて情報漏洩を検出 - ActMobile	低	1
48	フィッシングドメイン	フィッシングドメインの可能性	情報	1

No1. 情報漏洩発生サービス

ダークウェブにて情報漏洩を検出 - AntiPublic

Breached service is Detected - AntiPublic

緊急

1件

説明

メールアドレスや平文のパスワード等が漏洩しています。

情報漏洩日

2016年12月

漏洩背景

2016年12月、「Anti Public」と呼ばれる「コンボリスト」に、メールアドレスとパスワードのペアの膨大なリストが登場した。このリストには4億5800万件のユニークな電子メールアドレスが含まれており、その多くはさまざまなオンラインシステムからハッキングされた複数の異なるパスワードが設定されていた。このリストは広く流布し、「クレデンシャル・スタッフィング」に使用された。つまり、攻撃者は、アカウント所有者がパスワードを再利用した他のオンライン・システムを特定するために、このリストを使用したのである。この事件の詳細な背景については、パスワードの再利用、クレデンシャル・スタッフィング、そしてHave I Been Pwnedのもう10億件の記録をお読みください。

(参考：Have I Been Pwned)

解決方法

他サービス含め、同じパスワードを使い回しているサービスがあればそのパスワードを変更する

参考資料

・https://www.ipa.go.jp/security/guide/ps6vr70000007pkg-att/rouei_taiou.pdf

検出内容

対象のIT資産	メールアドレス	パスワード	電話番号	ユーザ名	氏名
1.1	laz_kral_@example.com	05*****4			
1.2	missrose@example.com	on*********e			
1.3	nicolenorman_009_@example.com	ni****0			
1.4	luisbernal@example.com	ni****0			
1.5	lalsouth@example.com	te********7			
1.6	mEHevaXoAiyfq@example.com	mE**********q			
1.7	qiaomumumu@example.com	12******9			

No36. ブラックマーケット

ブラックマーケットに情報の漏洩の可能性あり

Possible leak of information to Black Market.

高

1件

説明

お客様のドメインが含まれた販売データを検出しました。

解決方法

必要に応じて販売データを購入し、漏洩している情報の確認が必要です。

参考資料

・https://www.trendmicro.com/ja_jp/research/20/g/blackmarket-losing-confidence.html

検出内容

対象のIT資産	ドメイン名	販売データ	料金	販売日
1.1	example.com	archive.zip ・Chrome ・Debug.txt ・Default ・Profile 1 ・All Passwords.txt ・Brute.txt ・Cookies ・Cookies_Chrome_dev_Default.txt ・Cookies_Brave_Default.txt ・Cookies_Mozilla Firefox_ricrcxjq.default-release.txt ・Cookies_Chrome_dev_Profile 1.txt ・Cookies_Edge_dev_Default.txt ・GoogleAccounts ・Restore_Chrome_Profile 1.txt ・Wallets ・Bitwarden_Chrome_Default ・Edge ・Debug.txt ・Default ・Brave ・Default ・Mozilla Firefox ・ricrcxjq.default-release ・Software.txt ・Applications ・Steam ・Discord ・Processes.txt ・Clipboard.txt ・System.txt ・Screen.png	$ 10	2024年11月24日
1.2	example.com	passwords.txt	$ 5	2024年5月10日
1.3	example.com	passwords.txt	$ 4	2024年2月17日

No45. フィッシングドメイン

フィッシングドメインの可能性

Possible phishing domain

中

1件

説明

ドメイン名が類似しており、サイトの類似度も高いです。

解決方法

必要に応じて、フィッシングサイトのホスティングプロバイダに連絡し、違反を報告します。通常、プロバイダは速やかに対応し、サイトを閉鎖します。また、ドメインを登録している機関にフィッシングの報告を行い、ドメインの停止を依頼します。

参考資料

・https://www.antiphishing.jp/report/guideline/

検出内容

対象のIT資産	ドメイン名	類似ドメイン名	国	サーバ	類似率
1.1	example.com	exämple.com	Germany	Apache	72%
1.2	example.com	example.tr	Germany	nginx/1.18.0 (Ubuntu)	55%
1.3	example.com	examplé.com	United States		60%

No46. 情報漏洩発生サービス

ダークウェブにて情報漏洩を検出 - Zurich

Breached service is Detected - Zurich

低

1件

説明

メールアドレスが漏洩しています。

情報漏洩日

2023年1月

漏洩背景

2023年1月、チューリッヒ保険の日本法人がデータ漏洩に見舞われ、260万件の顧客記録と75万6000件以上の固有の電子メールアドレスが流出した。データはその後、人気のあるハッキング・フォーラムに投稿され、氏名、性別、生年月日、保険車両の詳細も含まれていた。このデータは、"IntelBroker "に帰属することを要求した情報源からHIBPに提供された。

(参考：Have I Been Pwned)

解決方法

不審なログインや未承認の変更がないか定期的に確認します。また、不審なメールやリンクを開かないようにし、個人情報を入力しないようにします。

参考資料

・https://www.ipa.go.jp/security/guide/ps6vr70000007pkg-att/rouei_taiou.pdf

検出内容

対象のIT資産	メールアドレス	パスワード	電話番号	ユーザ名	氏名
1.1	Hiroshi@example.com				
1.2	harutorikusomeone@example.com				
1.3	minami@example.com				
1.4	user@example.com				
1.5	ryo3932@example.com				
1.6	someone@example.com				
1.7	marines-2014@example.com				
1.8	kktnbaby@example.com				

No48. フィッシングドメイン

フィッシングドメインの可能性

Possible phishing domain

情報

1件

説明

名前が似ているドメイン名が存在しますが、サイトの類似度はなく、危険性は低いです。

参考資料

・https://www.antiphishing.jp/report/guideline/

検出内容

対象のIT資産	ドメイン名	類似ドメイン名	国	サーバ	類似率
1.1	example.com	eximple.com	United States		0%
1.2	example.com	exampla.com	United States	openresty/1.13.6.1	0%
1.3	example.com	uxample.com	United States		0%
1.4	example.com	supportexample.com			
1.5	example.com	example.ch	Switzerland	Apache	0%
1.6	example.com	examplc.com	United States	nginx	0%
1.7	example.com	example9.com	United States		0%
1.8	example.com	examplet.com	United States		0%
1.9	example.com	examplen.com	Hong Kong	nginx	0%
1.10	example.com	examplek.com		cloudflare	
1.11	example.com	example4.com	Germany	Apache/2.4.57 (Rocky Linux) OpenSSL/3.0.7	0%
1.12	example.com	examplel.com	Germany	Python/3.11 aiohttp/3.8.6	0%
1.13	example.com	example1.com	United States	Apache	0%
1.14	example.com	exampleq.com	United States	nginx/1.10.3 (Ubuntu)	0%
1.15	example.com	examplep.com	Canada		
1.16	example.com	example5.com	United States		
1.17	example.com	safeexample.com			
1.18	example.com	examplec.com	United States		
1.19	example.com	exampleb.com	United States		
1.20	example.com	examples.com	United States		0%
1.21	example.com	examplee.com	United States	nginx	0%
1.22	example.com	exampleg.com	Hong Kong	Apache	0%
1.23	example.com	exampled.com	Germany	Parking/1.0	0%
1.24	example.com	example0.com			
1.25	example.com	exqmple.com			
1.26	example.com	exemple.com	Australia	Apache	0%
1.27	example.com	axample.com	Australia	Apache	0%
1.28	example.com	ezample.com	United States		
1.29	example.com	webexample.com		cloudflare	0%
1.30	example.com	examplecdn.com		cloudflare	0%
1.31	example.com	example-web.com		cloudflare	
1.32	example.com	examplepay.com		cloudflare	0%
1.33	example.com	secure-example.com		cloudflare	0%
1.34	example.com	exampledownload.com	United States		0%
1.35	example.com	my-example.com	United States		0%
1.36	example.com	example-business.com	United States	sffe	0%
1.37	example.com	businessexample.com	United States		0%