SecurityScorecard

詳細レポート

XXXXX社の
スコアカード

生成日： **2021年6月2日**
生成者：xxxxx

このレポートについて
このレポートは、2:00:38 UTC 2021年6月2日時点におけるこのスコアカードのコピーです。ペネトレーション・テストの結果や最終評価ではないことに注意してください。

SecurityScorecardで全体像を把握する
SecurityScorecardには、セキュリティ・チームが組織を保護するために使用できる、継続的な自己監視、履歴レポート、CSVデータ・エクスポートなどの機能が用意されています。組織のスコアカードに完全に無料でアクセスするには、今すぐ******でアカウントを作成してください。

*****で、SecurityScorecardの詳細について今すぐご覧ください。

SecurityScorecardとは

SecurityScorecardは、全般的なセキュリティに加え、10個の主要リスク要因に焦点を当てて、A～Fのシンプルな格付けシステムを使用して企業を評価するセキュリティ評価サービスです。C、D、またはFに格付けされた企業では、AまたはBに格付けされた企業と比較して、セキュリティ侵害が起こる可能性が　倍高くなっています[1]。アプリケーションのセキュリティやパッチ適用の頻度といった特定のリスク要因は、侵害を引き起こす可能性をさらに示唆しています。これらの要因においてFと評価された企業では、データ漏洩や攻撃成功の可能性が、Aの企業よりも10倍高くなる可能性があります。

SecurityScorecardの格付けシステムの詳細については、*****をご覧ください。

1
“SecurityScorecardによる最新の調査によってデータ漏洩を事前に検出することが可能に” (*****)

次のステップ：Aを目指す

1. アカウントを作成する
このファイルには詳しい情報が豊富に含まれていますが、あくまでも特定の時点の情報にすぎません。アカウントを作成すると、組織のスコアカードに加え、継続的な自己監視、履歴レポート、CSVデータ・エクスポートなどの機能に無料でアクセスできるようになります。

2. デジタル・フットプリントを検証する
アカウントを作成したら、組織に帰属する可能性のあるものとしてSecurityScorecardで特定された資産のうち、スコアカードの評価に影響を与えるもの、つまりデジタル・フットプリントを確認します。必要に応じて、IPの削除または追加をリクエストします。

3. 見つかった問題点を確認する
スコアカードの内容をチームで調査します。セキュリティ対策の見落としを特定できたら、それは組織全体のセキュリティ強化につながります。

4. 問題点を修正して、スコアを向上させる
修正プログラムを導入したか、組織に帰属しない資産を見つけたか、あるいは代替コントロールに関する情報を共有したいかどうかにかかわらず、特定された問題点を修正し、解決策の承認申請を行うことによって、弊社にお知らせいただくことができます。解決策はサポート・チームによって処理され、未解決の項目がある場合は、サポート・チームが3営業日以内に解決します。プラットフォーム内で問題を修正するか、Eメール（support@securityscorecard.io）でお問い合わせください。

弊社がお手伝いいたします。

SecurityScorecardプラットフォームは、透明性とコラボレーションに基づいています。弊社のカスタマー信頼性サポート・チームは、修正および解決サービスを無料で提供し、お客様およびその顧客組織と協力して問題解決に取り組みます。このプロセスの過程でサポートが必要になった場合は、Eメール（support@securityscorecard.io）でお問い合わせください。

スコアカードの概要

C

xxxxx社

75 セキュリティ・スコア

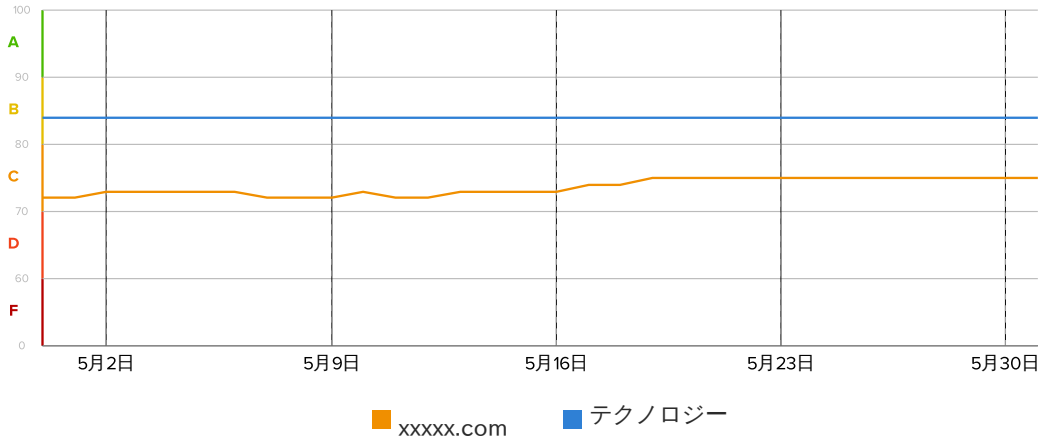
ドメイン : xxxxx.com
業種 : テクノロジー

要因

B	82	アプリケーション・セキュリティ	8 件の問題	A 100	IPレピュテーション	2 件の問題
A	100	キュービット・スコア	1 件の問題	A 90	漏洩された情報	2 件の問題
A	100	DNSの正常性	0 件の問題	F 57	ネットワーク・セキュリティ	20 件の問題
D	67	エンドポイント・セキュリティ	2 件の問題	D 62	パッチ適用頻度	8 件の問題
A	100	ハッカーチャッター	0 件の問題	A 90	ソーシャル・エンジニアリング	2 件の問題

30日間スコア履歴

次のグラフは、この会社の相対的なセキュリティ・ランキングの経時的な推移を示しています。スコア・パフォーマンスのピークは、全般的なセキュリティの向上、未解決問題の修正、企業インフラストラクチャを保護する取り組みの向上を表しています。一方、低下は、システムおよびアプリケーションの誤設定、マルウェア活動の長期化を表しています。



アクション項目

要因	重大度	スコアへの影響	検出された問題点
アプリケーション・セキュリティ	!!	-0.4	HTTPSリダイレクト・パターンが安全ではありません. サイトのドメイン・リダイレクト設定がHTTPSヘッダーとHTTP Strict Transport Security（HSTS）ヘッダーのセキュリティ機能を制限しているため、なりすましサイトや悪意のあるサイトにユーザーがリダイレクトされる脆弱性があります。
	!!	-0.5	HSTSのベスト・プラクティスがWebサイトで実装されていません. WebサイトがHTTPSで保護されている場合でも、明示的に指定されない限り、ほとんどのブラウザーはHTTP版のWebサイトへの接続を最初に試みるため、Webサイトの訪問者はその時点で中間者攻撃に対して脆弱になります。攻撃者は、訪問者が本来のHTTPS版Webサイトにアクセスするのを妨げ、代わりに悪意のあるWebサイトに訪問者を誘導します。（拡張版）HSTSヘッダーを使用すると、ユーザーは最初にWebサイトにアクセスした後、HTTPSで保護されたWebサイトにすぐに接続するため、この中間者攻撃の危険にさらされずに済みます。
	!!	-0.6	コンテンツ・セキュリティ・ポリシー（CSP）がありません. CSPディレクティブは、Webページのレンダリング時にどこからリソースをロードすべきかをWebブラウザーに指示します。これにより、誤ったリソースや悪意のあるリソースがWebページに挿入される（その後、ユーザーのブラウザーによって実行される）のを防ぐことができます。
	!	-0.1	WebサイトでX-Frame-Optionsのベスト・プラクティスが実装されていません. X-Frame-Optionsを明示的に設定しないと、信頼できない別のWebサイトのページ上のフレームにサイトが埋め込まれる可能性があります。この手口は、ソーシャル・エンジニアリング攻撃をより正当に見せるために使用されたり、クリックジャック攻撃に使用されたりします。
	!	-0.1	WebサイトでX-Content-Type-Optionsのベスト・プラクティスが実装されていません. ブラウザーはコンテンツを独自に分析し、MIMEタイプ・ヘッダーの指定とは異なる方法でコンテンツを処理することがありますが、このことは、セキュリティの問題や悪意のあるコードの実行につながる可能性を秘めています。たとえば、攻撃者は、画像の拡張子を使用して悪意のあるコードを隠しておき、イントロスペクションを行うブラウザーにそのコードをJavaScriptとして実行させる可能性があります。
エンドポイント・セキュリティ	!!!	-5.4	古いオペレーティング・システムが確認されました. 古いオペレーティング・システム上のWebブラウザーがWebサーバーに接続されています。
	!!!	-5.7	古いWebブラウザーが確認されました. 古いWebブラウザーがWebサーバーに接続されています。
漏洩された情報	!	<-0.1	認証情報が危険にさらされています. 従業員のEメールに関連付けられた認証情報が発見されました。
ネットワーク・セキュリティ	!!!	-1.6	SSL/TLSサービスが脆弱なプロトコルをサポートしています。. 脆弱なプロトコルをサポートしているTLSサービスが確認されました。
	!!!	-0.6	Elasticsearchサービスが確認されました. データベース管理システムのElasticsearchが一般に公開されていることが確認されました。
	!!!	-0.8	SSHソフトウェアが脆弱なプロトコルをサポートしています. バージョン2よりも下位のSSHプロトコルをサポートするSSHソフトウェアがサーバーで実行されていることが確認されました。
	!!	-0.4	SMBサービスが確認されました. ファイルおよびプリンター共有サービスのSMBが一般に公開されていることが確認されました。
	!!	-1.1	弱い暗号化スイートをサポートしているTLSサービスが確認されました。. 弱い暗号化スイートをサポートしているTLSサービスが確認されました。
	!!	-0.2	MySQLサービスが確認されました. データベース管理システムのMySQLが一般に公開されていることが確認されました。
	!!	-0.4	RDPサービスが確認されました. リモート・アクセス・サービスのRDPが一般に公開されていることが確認されました。

要因	重大度	スコアへの影響	検出された問題点
	!!	-0.5	SSHが脆弱なMACをサポートしています. 脆弱なメッセージ認証符号（MAC）アルゴリズムが検出されました。
	!!	-0.8	証明書の期限が切れています. 期限の切れた証明書を使用すると、TLSクライアントがサーバーに接続できなくなります。
	!!	-0.7	弱いアルゴリズムで署名された証明書が確認されました。. 弱いアルゴリズムで署名された証明書が確認されました。
	!!	-0.2	Microsoft SQL Serverサービスが確認されました. データベース管理システムのMicrosoft SQL Serverが一般に公開されていることが確認されました。
	!!	-0.5	SSHが脆弱な暗号をサポートしています. 脆弱な暗号が検出されました。
	!!	-0.7	証明書が自己署名されています. 自己署名された証明書によって、TLSクライアントとの通信が確立できません。
	!	-0.2	Telnetサービスが確認されました. リモート・アクセス・サービスのTelnetが一般に公開されていることが確認されました。
	!	-0.3	失効制御が機能していない証明書が確認されました。. CRL/OCSPのいずれも実装されていない証明書が確認されました。
	!	-0.3	証明書の有効期間がベスト・プラクティスよりも長く設定されています. CA/Browser Forum(CAブラウザーフォーラム) の要件で指示されている期間よりも長い有効期間が設定されている証明書が確認されました。
	!	-0.2	FTPサービスが確認されました. ファイル共有サービスのFTPが一般に公開されていることが確認されました。
パッチ適用頻度	!!!	-0.7	Patching Cadenceの重大度「高」のCVE. CVEの公開後45日以上経過した重大度「高」の脆弱性が確認されました。
	!!!	-0.6	前回確認された重大度「高」の脆弱性. 前回のスキャンで確認された重大度「高」の脆弱性がまだ一般に公開されている可能性があります。
	!!	-0.4	Patching Cadenceの重大度「中」のCVE . CVEの公開後90日以上経過した重大度「中」の脆弱性が確認されました。
	!!	-0.3	前回確認された重大度「中」の脆弱性. 前回のスキャンで確認された重大度「中」の脆弱性がまだ一般に公開されている可能性があります。
	!!	-0.3	EOS製品. EOS製品（製造元によるサポートが終了した製品）が一般に公開されていることが確認されました。
	!!	-0.2	EOL製品. EOL製品（開発または販売が終了した製品）が一般に公開されていることが確認されました。
	!	-0.1	前回確認された重大度「低」の脆弱性. 前回のスキャンで確認された重大度「低」の脆弱性がまだ一般に公開されている可能性があります。
	!	-0.1	Patching Cadenceの重大度「低」のCVE. CVEの公開後120日以上経過した重大度「低」の脆弱性が確認されました。
ソーシャル・エンジニアリング	!	<-0.1	漏洩した個人情報. 従業員の電子メールに関連する情報の漏洩が確認されました。

B 82 アプリケーション・セキュリティ

Web Application Vulnerabilityモジュールでは、ホワイトハットCVEデータベースやブラックハット・エクスプロイト・データベース、主要な検索エンジンによってインデックス付けされた機密性の高い検出結果などの方法で特定された、悪用される可能性のある既知の問題に基づく脅威インテリジェンスが使用されます。このモジュールは、複数の公開データセットやサードパーティ・フィードに加え、社内開発されたインデックス作成/集計エンジンからもデータを取り込みます。今後Webアプリケーションのセキュリティ侵害が起こる可能性はスコアに基づいて判断され、既存の改ざんコードの有無が調べられます。脆弱なアプリケーション、古いバージョン、アクティブな改ざんの存在は、全般的な格付けを計算するために使用されます。

重大度「高」

Application Securityの重大度「高」の問題はありません

重大度「中」

HTTPSリダイレクト・パターンが安全ではありません	1
HSTSのベスト・プラクティスがWebサイトで実装されていません	3
コンテンツ・セキュリティ・ポリシー（CSP）がありません	3

重大度「低」

WebサイトでX-Frame-Optionsのベスト・プラクティスが実装されていません	2
WebサイトでX-Content-Type-Optionsのベスト・プラクティスが実装されていません	2

プラス要素

Webアプリケーション・ファイアウォール（WAF）が検出されました	2

情報提供目的

サブリソース整合性の実装が安全ではありません	3
WebサイトでX-XSS-Protectionのベスト・プラクティスが実装されていません	3

WebサイトでX-Frame-Optionsのベスト・プラクティスが実装されていません

-0.1 スコアの影響

X-Frame-Optionsを明示的に設定しないと、信頼できない別のWebサイトのページ上のフレームにサイトが埋め込まれる可能性があります。この手口は、ソーシャル・エンジニアリング攻撃をより正当に見せるために使用されたり、クリックジャック攻撃に使用されたりします。

説明
X-Frame-Options HTTP応答ヘッダーを使用すると、ページを「<frame>」、「<iframe>」、または「<object>」の形式で表示することをブラウザーに許可するかどうかを指定できます。サイトはこれを使用して、そのサイトのコンテンツが他のWebサイトに埋め込まれないようにすることで、クリックジャック攻撃を回避できます。

推奨事項
「DENY」または「ALLOW-FROM」ディレクティブを使用して、このWebサイトからの応答に次のヘッダーのいずれかを追加します。X-Frame-Options: DENY' X-Frame-Options: ALLOW-FROM https://example.com/'

2件の検出結果

ドメイン	初期URL	最終URL	リクエスト・チェーン	分析	前回確認日
xxxxx.com	https://xxxxx.com/	https://〇〇〇.□□□.com/?tenant=aaaaaaaaaaaa	https://△△△.xxxxx.com/ https://〇〇〇.□□□.com/?tenant=aaaaaaaaaaaa	Header missing	2021/5/31 22:58:37
証拠：					
xxxxx.com	https://xxxxx.com/	https://xxxxx.com/	n/a	Header missing	2021/5/24 16:23:08
証拠：					

HTTPSリダイレクト・パターンが安全ではありません

-0.4 スコアの影響

サイトのドメイン・リダイレクト設定がHTTPSヘッダーとHTTP Strict Transport Security（HSTS）ヘッダーのセキュリティ機能を制限しているため、なりすましサイトや悪意のあるサイトにユーザーがリダイレクトされる脆弱性があります。

A 100 キュービット・スコア

このプロプライエタリ・モジュールは、企業が抱えている可能性のあるセキュリティ上のさまざまな問題を測定します。たとえば、フラグが付けられたIPアドレスの公開脅威インテリジェンス・データベースがチェックされます。これらの構成ミスは、悪用される可能性が高く、データやインフラストラクチャのプライバシーの重大な侵害を招く可能性があります。

重大度「高」	重大度「中」	重大度「低」	プラス要素
Cubit Scoreの重大度「高」の問題はありません	Cubit Scoreの重大度「中」の問題はありません	Cubit Scoreの重大度「低」の問題はありません	Cubit Scoreのプラスの側面はありません

情報提供目的	
タイポスクワット・ドメインの可能性が検出されました	67

タイポスクワット・ドメインの可能性が検出されました

タイポスクワットの可能性を示しているドメインが検出されました。

説明
この問題は情報提供目的で指摘されるだけで、スコアの一部としては計算されません。URLハイジャッキング、スティング・サイト、URL偽装とも呼ばれるタイポスクワッティングは、サイバースクワッティングの一種であり、正当なドメインと似ているが、よくあるスペルミスや別のTLD（トップレベル・ドメイン）を含んだドメインが悪意のあるアクターによって登録されます。この攻撃が成功するには、ユーザーがURLの入力を誤り、本来の宛先ではなく攻撃者によって制御されるサイトまで到達することが条件となります。これに関連したホモグラフ攻撃と呼ばれる手法では、攻撃者は、見た目の区別が紛らわしい類似したASCII文字や場合によってはUnicode文字を使用して（たとえば、「l」を「I」または「1」で置き換えるなどして）、既存のドメインに視覚的に酷似したドメインを登録します。これらの攻撃は、Eメールの受信者にリンクをクリックさせて攻撃者が制御するWebサイトに誘導する目的で、フィッシング・キャンペーンの一部としても利用されます。ベスト・プラクティスとして、ブランド・レピュテーション・サービスやドメイン保護サービスを利用している組織によっては、悪意のあるアクターによるタイポスクワッティング・ドメインの作成を阻止するために、類似したドメインを意図的に登録する場合があります。

推奨事項
タイポスクワット・ドメインが組織に危険を及ぼしていないことを確認します。必要に応じて、フィッシングに使用される可能性のある悪質なドメインのドメイン削除を実行します。

67件の検出結果

IPアドレス	ドメイン	前回確認日
△.△.△.△	www.11△1.com	2020/9/26 7:17:12
□.□.□.□	wwww.2□22.com	2020/9/26 7:17:12
○.○.○.○	www.333○.com	2020/9/26 7:17:12
X .X .X .X	www.X444.com	2020/9/26 7:17:11
△.□.○.X	www.5△55.com	2020/9/26 7:17:11
□.○ .X.△	www.66□6.com	2020/9/26 7:17:11
○ .X.△.□	www.777○.com	2020/9/26 7:17:11
X .△.□.○	www.8X88.com	2020/9/26 7:17:11
△.△.□.□	www.△999.com	2020/9/26 7:17:10
○.○ .X .X	www.10□1010.com	2020/9/26 7:17:10
□.□.○.○	www.11○1111.com	2020/9/26 7:17:10
X .X .△.△	www.1212X12.com	2020/9/26 7:17:10

A 100 DNSの正常性

このモジュールは、企業のDNS設定の正常性と構成を測定し、悪意のあるイベントが発生していないことをその企業のネットワークのパッシブDNS履歴で確認します。また、なりすましを防げるようEメール・サーバーが適切に保護されていること、DNSサーバーが正しく構成されていることを確認するのにも役立ちます。

重大度「高」

DNS Healthの重大度「高」の問題はありません

重大度「中」

DNS Healthの重大度「中」の問題はありません

重大度「低」

DNS Healthの重大度「低」の問題はありません

プラス要素

DNS Healthのプラスの側面はありません

情報提供目的

DNS Healthの情報提供目的のシグナルはありません

問題は見つかりませんでした

D 67 エンドポイント・セキュリティ

Endpoint Securityモジュールは、オペレーティング・システム、Webブラウザー、関連するアクティブなプラグインに関するメタデータから抽出された識別ポイントを追跡します。企業は収集された情報に基づいてこれらのデータポイントの古いバージョンを識別することによって、クライアント側のエクスプロイト攻撃を防ぎます。

重大度「高」

古いオペレーティング・システムが確認されました	8
古いWebブラウザーが確認されました	17

重大度「中」

Endpoint Securityの重大度「中」の問題はありません

重大度「低」

Endpoint Securityの重大度「低」の問題はありません

プラス要素

Endpoint Securityのプラスの側面はありません

情報提供目的

Endpoint Securityの情報提供目的のシグナルはありません

古いオペレーティング・システムが確認されました

古いオペレーティング・システム上のWebブラウザーがWebサーバーに接続されています。

-5.4 スコアの影響

説明

WebブラウザーがWebサーバーに接続すると、プラットフォームとバージョンに関する情報がサーバーに通知されます。この情報は、サーバーが適切なコンテンツを提供するのに役立てられるだけでなく、インターネット上のさまざまな場所のホストで使用されているプラットフォームとブラウザーのバージョンを特定する目的でも記録および集計されます。これらのデータセットに基づき、次の表で説明する古いオペレーティング・システムが使用されていることが判明しました。次の表に示すものも含め、単一の外部IPアドレスが任意の数の内部ホストに対応する場合があることに注意してください。たとえば、単一の外部IPを持つ企業ファイアウォールやNATゲートウェイは、その企業のデスクトップ・ネットワーク全体のソースとして表示されます。

推奨事項

影響を受けるデバイスのオペレーティング・システムを更新します。ソフトウェア・ベンダーから入手でき、お使いの環境で許可されている場合は、自動更新機能を有効にします。組織内で使用されているすべてのソフトウェアとハードウェアの定期更新スケジュールを維持し、最新のパッチがリリース後すぐにすべて適用されるようにします。

8件の検出結果

製造元	製品	バージョン	ステータス	ソースIP	ポート	証拠	前回確認日
Microsoft	Windows 7	7	end of service	△.△.△.△	33680, 38120, 7409, 5323, 7988, 4045, 46803, 11024, 12824, 29445	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.163 Safari/537.36	2021/5/30 3:32:09
Microsoft	Windows 7	7	end of service	□.□.□.□	56172, 57425	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0	2021/5/27 7:35:24
Microsoft	Windows 7	7	end of service	○.○.○.○		Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36	2021/5/26 4:51:41

A 100 ハッカーチャッター

SecurityScorecardのHacker Chatterモジュールは、アンダーグラウンドのハッカーチャッターの複数のストリームを分析するための自動収集/集計システムです。フォーラム、IRC、ソーシャル・ネットワークなどのハッカー・コミュニティ・ディスカッションの公開リポジトリは、会社名やWebサイトの言及を見つけるために継続的に監視、収集、および集計されます。Hacker Chatterスコアは、収集センサー内に表示されるインジケーターの値に基づいてランク付けされる情報提供レベルの指標です。

重大度「高」

Hacker Chatterの重大度「高」の問題はありません

重大度「中」

Hacker Chatterの重大度「中」の問題はありません

重大度「低」

Hacker Chatterの重大度「低」の問題はありません

プラス要素

Hacker Chatterのプラスの側面はありません

情報提供目的

Hacker Chatterの情報提供目的のシグナルはありません

問題は見つかりませんでした

A 100 IPレピュテーション

IP Reputation and Malware Exposureモジュールは、SecurityScorecardのシンクホール・インフラストラクチャとOSINTマルウェア・フィードのブレンド、およびサードパーティの脅威インテリジェンス・データ共有パートナーシップを利用します。SecurityScorecardのシンクホール・システムは、攻撃者によって乗っ取られた世界中のCommand and Control（C2）インフラストラクチャから数百万のマルウェア・シグナルを取り込みます。着信データは処理され、企業に関連付けられます。Malware Exposure Key Threat Indicatorモジュールを計算する決定要因として、マルウェア感染の量と期間が使用されます。

重大度「高」
IP Reputationの重大度「高」の問題はありません

重大度「中」
IP Reputationの重大度「中」の問題はありません

重大度「低」
IP Reputationの重大度「低」の問題はありません

プラス要素
IP Reputationのプラスの側面はありません

情報提供目的

マルウェア感染履歴	2
アドウェアのインストール履歴	2

マルウェア感染履歴

マルウェア感染を示唆するデータのやり取りが過去365日間で確認されました。

説明
デバイスがマルウェアに感染すると、そのデバイスは、インターネット上のコマンド・アンド・コントロール(C&C) サーバと通信を開始することが確認されます。この通信により、マルウェアは、感染したデバイスを登録し、マルウェアの作成者からの命令を受け取ることができるようになります。この命令により、そのストレージ内のデータが削除や暗号化されたり、分散サービス拒否(DDoS) 攻撃に参加させられたり、さまざまな悪意のある攻撃を実行させられたりする可能性があります。
このイシューは、マルウェア感染のイシューと重複しており、マルウェア感染の直近一年の状況を把握できます。

推奨事項
リストされたIPアドレスに関連付けられているデバイスを調査して、マルウェア感染の証拠があるかどうかを調べます。

2件の検出結果

マルウェア・ファミリー	検出方法	ソースIP	検出結果	前回確認された感染
stealrat	unknown	△.△.△.△	1	2021/2/24 6:54:30
dorkbot	sinkhole	□.□.□.□	1	2021/2/6 0:40:03

アドウェアのインストール履歴

アドウェアのインストールを示す通信が、過去365日間にわたって確認されました。

説明
デバイスにアドウェアがインストールされると、インターネット上のサービスと通信を開始することが確認されます。このサービスによって、アドウェアはインストールされているデバイスを登録し、ユーザーの画面には広告が表示されます。
このイシューは、アドウェアインストールのイシューと重複しており、アドウェアインストールの直近一年の状況を把握することができます。

推奨事項
リストされているIPアドレスに関連付けられているデバイスを調べ、アドウェアのインストールの証拠がないかどうかを確認します。

A 90 漏洩された情報

このInformation Leakモジュールは、チャッター・モニタリングとディープWebモニタリングの各機能を利用して、ハッカーの間で流通している危殆化した認証情報を特定します。一般向けに発表された大量データの漏洩から、小規模な漏洩やハッカー間の小規模な交換まであります。

重大度「高」

Information Leakの重大度「高」の問題はありません

重大度「中」

Information Leakの重大度「中」の問題はありません

重大度「低」

認証情報が危険にさらされています	1

プラス要素

Information Leakのプラスの側面はありません

情報提供目的

危険にさらされている認証情報 （過去の履歴）	1

危険にさらされている認証情報 （過去の履歴）

従業員のEメールに関連付けられた認証情報が発見されました。

説明

個人識別情報と関連付けられた電子メールとパスワードの認証情報が、ハッカーのアンダーグラウンド、または、セキュリティコミュニティ内で出回っていることが確認されました。
同一のパスワードを繰り返し利用していると、セキュリティ上のリスクが高まります。例えば、その状況で認証情報が漏えいし、悪用されると、社内システムや人事管理システム/CRM/またはその企業が使用する他のSaaSプロバイダーなどといった外部に委託しているシステムの侵害につながります。確認された認証情報は、大量の漏洩データの一部として、また、パブリックおよびプライベートのHacker Chatterソースから抽出されました。
漏洩した従業員に関連する個人識別情報は、それらをターゲットに絞った高度なソーシャルエンジニアリング攻撃を実施するためにも利用されます。
尚、プライバシー上の理由から、影響を受けたユーザー情報はそれぞれのスコアカードの管理者権限を持つユーザにのみが確認できます。

推奨事項

従業員が企業またはサードパーティのログインに、影響を受けた認証情報を使用していないことを確認します。セキュリティ侵害の兆候があった後ですべてのパスワードが変更されていることを確認します。企業パスワードの場合は、不審なIPアドレスからのログイン試行の繰り返し失敗やパスワード・リセット試行の繰り返しがないかどうかをログで確認します。

1件の検出結果

ドメイン	漏洩名	漏洩年	説明	影響を受けたユーザー	前回確認日
xxxxx.com	Promo	2020	Promo.com, an Israeli-based marketing video creation site, has disclosed a data breach after a database containing 22 million user records was leaked for free on a hacker forum. Promo is a web site that allows you to create promotional videos or ads that can then be shared on social networks such as Facebook, Instagram, Twitter, and LinkedIn		2020/8/13 12:00:00

F 57 ネットワーク・セキュリティ

Network Securityモジュールは、企業ネットワーク内に高リスクまたは安全でないオープン・ポートがあることの証拠を公開データセットで調べます。安全でないポートは、攻撃者がログイン・プロセスを回避したり、より高いシステム・アクセス権を取得したりする目的で不正利用されることがよくあります。オープン・ポートは構成が正しくないと、ハッカーのワークステーションと社内ネットワークの間のエントリ・ポイントの役割を果たしてしまう可能性があります。

重大度「高」

SSL/TLSサービスが脆弱なプロトコルをサポートしています。	39
Elasticsearchサービスが確認されました	1
SSHソフトウェアが脆弱なプロトコルをサポートしています	4

重大度「中」

SMBサービスが確認されました	12
弱い暗号化スイートをサポートしているTLSサービスが確認されました。	160
MySQLサービスが確認されました	1
RDPサービスが確認されました	15
SSHが脆弱なMACをサポートしています	51
証明書の期限が切れています	30
弱いアルゴリズムで署名された証明書が確認されました。	23
Microsoft SQL Serverサービスが確認されました	1
SSHが脆弱な暗号をサポートしています	36
証明書が自己署名されています	31

重大度「低」

Telnetサービスが確認されました	13
失効制御が機能していない証明書が確認されました。	54
証明書の有効期間がベスト・プラクティスよりも長く設定されています	48
FTPサービスが確認されました	32

プラス要素

Network Securityのプラスの側面はありません

情報提供目的

POP3サービスが確認されました	6
Remote Access Service Observed	1
IMAPサービスが確認されました	2

SSL/TLSサービスが脆弱なプロトコルをサポートしています。

-1.6 スコアの影響

脆弱なプロトコルをサポートしているTLSサービスが確認されました。

説明

Secure Socket Layer（SSL）の後継であるTransport Layer Security（TLS）は、TLSサーバー（Webサイトなど）とTLSクライアント（Webブラウザーなど）間の通信を暗号化するネットワークプロトコルです。その通信は暗号化スイートによって保護されます。
ネットワークプロトコルには、定義づけされた残存期間はありませんが、それらの脆弱性は、研究機関や国家によって常に評価されています。どのプロトコルが信頼できないかについてのコンセンサスは時間の経過と共に状況が変わり、脆弱なプロトコルが利用されている場合、その証明書は変更または偽造される可能性があります。

推奨事項

”EVIDENCE"列にリストされている暗号化スイートを無効化する。

39件の検出結果

ターゲット	ポート	検出結果	前回確認日
△.△.△.△	443	13	2021/5/20 13:04:48
△△△.xxxxx.com	443	5	2021/5/20 10:08:48
□.□.□.□	443	30	2021/5/20 10:02:24
○○○.xxxxx.com	443	30	2021/5/20 10:02:21
X.X.X.X	443	33	2021/5/20 6:05:44
□□□.xxxxx.com	443	6	2021/5/20 4:46:49
○○○.xxxxx.com	443	11	2021/5/19 9:49:24
XXX.□□□.xxxxx.com	443	6	2021/5/19 9:49:24
○.○.○.○	443	6	2021/5/18 17:35:17

D 62 パッチ適用頻度

Patching Cadenceモジュールは、企業が脆弱性にどのくらい迅速に対処しているかを分析して、パッチ適用の実施状況を測定します。企業が問題を修正してパッチを適用するのにかかる時間の他社との比較を調べます。

重大度「高」		重大度「中」		重大度「低」		プラス要素
Patching Cadenceの重大度「高」のCVE	344	Patching Cadenceの重大度「中」のCVE	1,122	前回確認された重大度「低」の脆弱性	115	Patching Cadenceのプラスの側面はありません
前回確認された重大度「高」の脆弱性	247	前回確認された重大度「中」の脆弱性	794	Patching Cadenceの重大度「低」のCVE	115	
		EOS製品	3			情報提供目的
		EOL製品	2			Patching Cadenceの情報提供目的のシグナルはありません

前回確認された重大度「低」の脆弱性

-0.1 スコアの影響

前回のスキャンで確認された重大度「低」の脆弱性がまだ一般に公開されている可能性があります。

説明
Common Vulnerabilities and Exposures（CVE）は、ソフトウェアおよびハードウェアの既知の脆弱性のリストです。各CVEには、脆弱性のIDと説明、およびその脆弱性の影響を受ける製品名とバージョンが含まれています。ソフトウェアとハードウェアは、多くの場合、ホストが接続したときに製品名とバージョンを自己報告します。SecurityScorecardはCVEリストを検索し、この会社のネットワーク上で見つかった製品の名前とバージョンを相互参照することにより、脆弱性の存在を推測できます。

推奨事項
影響を受けるソフトウェアとハードウェアを更新するか、パッチを適用します。ソフトウェア・ベンダーから入手でき、お使いの環境で許可されている場合は、自動更新機能を有効にします。CVEリストと脆弱性リポジトリを監視して、インフラストラクチャに影響を与える可能性のあるエクスプロイト・コードを探します。新しいエクスプロイトと脆弱性がリリースされたときにアラートを受け取ることができるよう、BugTraqメーリング・リストに登録します。組織内で使用されているすべてのソフトウェアとハードウェアの定期更新スケジュールを維持し、最新のパッチがリリース後すぐにすべて適用されるようにします。

115件の検出結果

脆弱性	IPアドレス	ポート	CVE公開日	前回確認日
CVE-2009-4022	△.△.△.△	53	2009/11/25 0:00:00	2021/5/27 14:03:05
脆弱性の説明：Unspecified vulnerability in ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P4, 9.5 before 9.5.2-P1, 9.6 before 9.6.1-P2, and 9.7 beta before 9.7.0b3, with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains an Additional section with crafted data, which is not properly handled when the response is processed "at the same time as requesting DNSSEC records (DO)," aka Bug 20438.				
CVE-2014-0591	△.△.△.△	53	2014/1/14 0:00:00	2021/5/27 14:03:05
脆弱性の説明：The query_findclosestnsec3 function in query.c in named in ISC BIND 9.6, 9.7, and 9.8 before 9.8.6-P2 and 9.9 before 9.9.4-P2, and 9.6-ESV before 9.6-ESV-R10-P2, allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via a crafted DNS query to an authoritative nameserver that uses the NSEC3 signing feature.				
CVE-2014-0591	□.□.□.□	53	2014/1/14 0:00:00	2021/5/27 13:40:02
脆弱性の説明：The query_findclosestnsec3 function in query.c in named in ISC BIND 9.6, 9.7, and 9.8 before 9.8.6-P2 and 9.9 before 9.9.4-P2, and 9.6-ESV before 9.6-ESV-R10-P2, allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via a crafted DNS query to an authoritative nameserver that uses the NSEC3 signing feature.				
CVE-2018-5745	□.□.□.□	53	2019/10/9 0:00:00	2021/5/27 13:40:02
脆弱性の説明："managed-keys" is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which operators configure for use in DNSSEC validation. Due to an error in the managed-keys feature it is possible for a BIND server which uses managed-keys to exit due to an assertion failure if, during key rollover, a trust anchor's keys are replaced with keys which use an unsupported algorithm. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5745.				
CVE-2012-2687	○.○.○.○	443	2012/8/22 0:00:00	2021/5/21 21:07:47
脆弱性の説明：Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.				
CVE-2011-4415	X.X.X.X	443	2011/11/8 0:00:00	2021/5/21 20:44:30

A 90 ソーシャル・エンジニアリング

SecurityScorecardのSocial Engineeringモジュールは、組織が標的型ソーシャル・エンジニアリング攻撃にさらされる可能性を判断するために使用されます。Social Engineeringモジュールは、ソーシャル・ネットワークや公開データ漏洩事例からのデータを取り込み、独自の分析方法を組み合わせます。Social Engineeringスコアは、SecurityScorecard収集センサーに表示されるインジケーターの値に基づいて計算される情報提供レベルの指標です。

重大度「高」

Social Engineeringの重大度「高」の問題はありません

重大度「中」

Social Engineeringの重大度「中」の問題はありません

重大度「低」

漏洩した個人情報	1

プラス要素

Social Engineeringのプラスの側面はありません

情報提供目的

露出された個人情報（過去の履歴）	1

露出された個人情報（過去の履歴）

従業員の電子メールに関連する情報の漏洩が確認されました。

説明

ソーシャルエンジニアリングは、漏洩した個人情報と組み合わせて使用されると、より巧妙な攻撃が可能になります。例えば、アカウントのパスワードをリセットするため、アカウントを復元する際のセキュリティに関する質問に利用されます。さらに、ハッカーが従業員になりすまして、より高いレベルのアクセス権を取得することも容易になります。
SecurityScorecard には、漏洩に関連する情報のカテゴリのみが表示されます。
尚、プライバシー上の理由から、影響を受けたユーザー情報はそれぞれのスコアカードの管理者権限を持つユーザにのみが確認できます。

推奨事項

いったん公開されたインターネットから情報を削除することは困難で、ソーシャルエンジニアリングに対する推奨措置としては、それを軽減する施策になります。
次のことを確認することで攻撃にあうリスクを低減できます。
- 従業員が定期的なサイバーセキュリティ意識トレーニングを受けていること
- 機密情報を処理するための手順が確立されていること
- 抜き打ちのセキュリティテストが定期的で実行されていること

1件の検出結果

ドメイン	漏洩名	漏洩年	説明	影響を受けたユーザー	前回確認日
xxxxx.com	Promo	2020	Promo.com, an Israeli-based marketing video creation site, has disclosed a data breach after a database containing 22 million user records was leaked for free on a hacker forum. Promo is a web site that allows you to create promotional videos or ads that can then be shared on social networks such as Facebook, Instagram, Twitter, and LinkedIn		2020/8/13 0:00:00

漏洩した個人情報

<-0.1 スコアの影響

従業員の電子メールに関連する情報の漏洩が確認されました。

説明

推奨事項

コンテンツ（格付け、データ、レポート、ソフトウェア、その他のアプリケーション、その出力を含む）またはその一部（以下「コンテンツ」と総称）は、SecurityScorecard, Inc.（以下「SSC」）から書面による許可を事前に得ることなく、いかなる手段によっても変更、リバース・エンジニアリング、複製、または配布したり、データベースまたは検索システムに格納したりしてはなりません。コンテンツを違法または不正な目的に使用してはなりません。

SSCおよびすべてのサードパーティ、およびその取締役、役員、株主、従業員、顧客、および代理店（以下「SSC当事者」と総称）は、コンテンツの正確性、完全性、適時性、または可用性を保証しません。 SSC当事者は、誤謬または不作為（過失の有無を問わない）に対してその原因にかかわらず責任を負わず、コンテンツを使用することによって得られた結果に対しても責任を負いません。コンテンツは「現状有姿」で提供されます。 SSC当事者は、明示的か黙示的かを問わず、いかなる保証も行いません。これには以下が含まれますが、これらに限定されません。（1）商品性と特定目的適合性の保証（2）正確性、結果、適時性、および完全性の保証（3）バグ、ソフトウェア・エラー、欠陥がないことの保証（4）コンテンツの機能が中断されないことの保証（5）コンテンツが任意のソフトウェアまたはハードウェア構成で動作することの保証。いかなる場合においても、SSC当事者は、コンテンツの使用に関連した直接的、間接的、偶発的、懲罰的、補償的、特別または派生的な損害、費用、支出、弁護士費用、または損失（収益または利益の逸失、機会費用、過失による損失が含まれるが、これらに限定されない）について、そのような損害の可能性について知らされていた場合も含め、いかなる当事者に対しても責任を負わないものとします。

コンテンツの使用者は、あらゆる損失または損害を軽減すべく、いかなる合理的な努力も払う必要があります。ここに記載されているいかなる内容も、損失または損害を軽減するユーザーの義務を解除または排除するものとみなされることはありません。

コンテンツへのアクセスまたは使用に関連したいかなる理由についても、SSC当事者の累積責任が（A）賠償責任が発生する事象の直前の12か月間に提供されたサービスに対してユーザーがSSCに支払った総額、または（B）100米ドルのうち大きい方を超えることは法律で許可される範囲内でありません。

格付けやコンテンツ内の記述を含むセキュリティ関連の分析は、企業の将来の相対的なセキュリティ・リスクについての意見の表明日時点における陳述であって、任意の事業体との取引の安全性についての現在または過去の事実を陳述するものでも、任意の事業体とビジネスを行う決定について提案するものでも、任意の事業体のセキュリティ対策について第三者として評価したことに関するデータや結論、試行の正確性を支持するものでもありません。ビジネス上の意思決定を行う際のユーザーとその管理者、従業員、アドバイザー、クライアントのスキル、判断力、経験に代わるものとして、SSCの意見、分析、格付けに依拠すべきではありません。SSCは、様式または形式を問わず、公開後のコンテンツを更新する一切の義務を負いません。SSCは信頼できるソースから情報を取得していますが、受け取った情報についての監査を実施しておらず、デュー・デリジェンスまたは独立した検証を行う義務も負いません。ユーザーは次のことに明示的に同意するものとします。（a）コンテンツを介して提供されるセキュリティ評価およびセキュリティに関するその他の意見が、あらゆる脆弱性またはセキュリティの問題を反映、特定または検出し、それ以外のリスクに対処するわけではないこと。（b）提供されるセキュリティ評価およびその他の意見では、ユーザーの特定の目的、状況、またはニーズが考慮されていないこと。（c）各評価またはその他の意見は、ユーザーによって、またはユーザーに代わって行われる決定の1つの要素としてのみ検討されること。（d）ユーザーは、任意の事業体とビジネスを行うリスクについて、十分な注意を払って独自の調査と評価を行うこと。ユーザーがコンテンツで何かを特定した場合は、support@securityscorecard.ioにEメールを送信して、その情報を共有してください。