適切なパスワードの利用で悪意なボットに立ち向かうために

パスワード調査レポート

Rapid7 調査担当ディレクター、Tod Beardsley
Rapid7 主任AIリサーチャー、Erick Galinkin
Rapid7 主任セキュリティリサーチャー、Curt Barnard

RAPID7

目次

概要

本レポートでは、リモートアクセスで最も一般的なプロトコルであるSSHとRDPの悪用のために、自動的な攻撃によって最も狙われやすい認証情報の種類について解説します。これらのプロトコルはクラウド上の仮想マシンの管理に広く使用されているため、クラウド化やリモートワークが進む現状を攻撃者が悪用し、狙う手口を把握しておくことが重要です。ユーザー名として最も一般的なものは、「root」、「administrator」、「mysql」など、オペレーティングシステムやアプリケーションにあらかじめ設定されているデフォルトのユーザー名ですが、パスワードに関しては、悪いパスワード例としてよく知られる「123456」、「password」、「admin」などのほか、パスワードが設定されていないケースすら見受けられます。

パスワードリストにはさまざまなものがありますが、ここでは侵入者や攻撃者がよく使用する有名なリストである、rockyou2021.txtを使用しています。驚くことに、Rapid7のハニーポットでモニタリングされた任意の約50万件のパスワードのほぼすべて（99.997%）が、この「rockyou」セットに含まれていました。この事実から、オンライン認証情報を狙う攻撃者は、ランダムなパスワードを試してい成功しているのではなく、推測可能なパスワードのリストを利用していと結論付けられます。

企業の IT 管理者は、以下の方法でこれらの攻撃を防ぐことができます：

- SSHサーバーとRDPサーバーのデフォルトのパスワード（IoTやクラウドソリューションで出荷時に設定されるパスワードを含む）を展開前に変更する。
- デフォルト認証情報のデータベースであるオープンソースのDefaultinatorを利用し、SSH/RDPエンドポイントにデフォルトのパスワードが使われていないか監査する。
- パスワード管理ソリューションを使用し、ランダムに生成された強力なパスワードを使用する企業文化を浸透させる。
- Rapid7が無料で提供している攻撃可能領域管理（ASM）ソリューション Dopplerを使用し、定期的にスキャンしてSSH/RDPエンドポイントを発見する。

はじめに

リモートワークやクラウド化が進むに従い、インターネット経由で企業の情報システムにアクセスする人の数が急増しています。その多くは、リモートデスクトッププロトコル（RDP）とセキュアシェル（SSH）を利用しています。その結果、かつて企業が境界を保護し、従業員に企業ネットワークでのみの作業を強制できた「箱庭」的アプローチは次第に廃れ、従業員が、信頼できないネットワーク経由で接続するアセットの数は急増しました。セキュリティにおいては非常に一般的なことですが、利便性と複雑さとの両方が加わったことで、これらのシステムに対する保護の難易度が急激に上がりました。

2016年、Rapid7はRDPを調査対象とした『Attacker's Dictionary（攻撃者辞書）』を発表しました。この調査で、119か国から221,203件の接続試行があったことが明らかになったことから、ランダムなブルートフォース攻撃ではなく、より成功確率が高いと想定される辞書攻撃が行われていることが判明しました。

本レポートでは、前回のレポートの内容を補足する形で、RDPに加え、Rapid7のSSHハニーポットへの接続についても調査を行っています。2021年9月10日から2022年9月9日までの間に、Rapid7のProject Heisenberg RDPとSSHハニーポットから収集された1年分のユーザー名とパスワードのデータを検討対象としたものです。この調査の間、Rapid7は、ハニーポットへの接続試行を何千万回も観察しました。結果として、RDP/SSHハニーポット全体で一意のIPソースアドレス215,894件と一意のパスワード512,002件（SSHハニーポット：一意のソースIP213,972件と一意のパスワード497,848件、RDPハニーポット：一意のソースIP2,030件と一意のパスワード22,690件）をキャプチャすることができました。

本レポートでは、主に次の2つの疑問に答えていきます：

1. 2016年以降の RDP における変化とは
2. 攻撃者が使用する最も完成された、かつ有名なディクショナリ（「rockyou」セット）とRapid7ハニーポットのパスワードコーパスとの比較

「Rockyou」セット

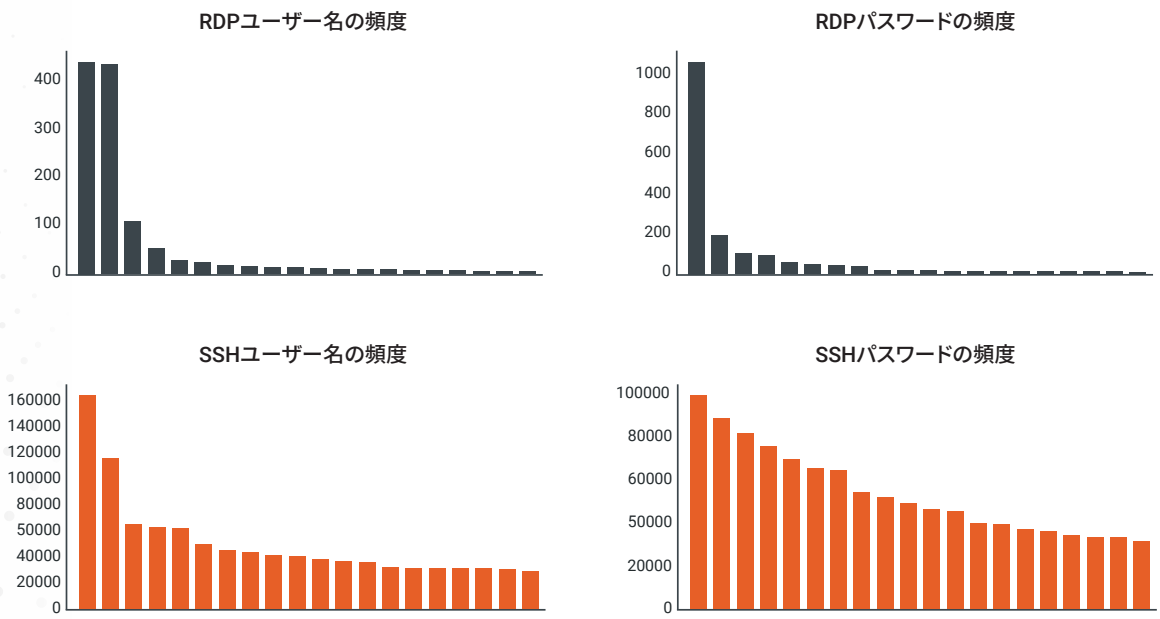
RockYouは、ソーシャルメディアサイト用のウィジェットやプラグインを開発する会社でした。2009年にこのRockYouがハッキングされ、攻撃者はさまざまなユーザーアカウントのパスワードが暗号化されない状態で保存されていることを発見しました。その結果、Linuxの侵入テストに特化したディストリビューション、Kali Linuxに含まれる「rockyou.txt」の14,341,564件に及ぶパスワードが流出したのです。その流出以降、さらに多くのパスワードリストが作成され、その集大成として、漏洩した情報や辞書に長年蓄積された約84億件のパスワードを集めた約92GBのテキストファイル「rockyou2021.txt」（本文中では「rockyou」セットと呼称）が登場しました。この更新バージョンの「rockyou」セットはKali Linuxにデフォルトで含まれていないものの、多くのユーザーがパスワードジェネレーターやパスワードマネージャーの利用し、代わりにパスワードを自分で作成して使いまわし続ける中、あらゆる類の認証情報を盗み出そうとする攻撃者の的とされています。Rapid7では、この「rockyou」セットを攻撃者が手軽に生成して試せるパスワードのソースとして捉え、パスワードリストの利用にとどまらない何らかの進化が見られるかどうかを検討します。

調査結果

SSHとRDPユーザー名の分布全体で、明らかに管理者アカウントに関するものが多く使われています。大文字と小文字を無視すると、RDPで最も一般的なユーザー名上位3位は「administrator」、「user」、「admin」、SSHで最も一般的なユーザー名上位3位は「root」、「admin」、「nproc」となります。パスワードについてはSSHとRDPで違いがありますが、「admin」、「password」、「123456」、空の文字列（パスワード設定なし）などの定番が多く登場します。興味深いことに、1位、または1位～2位が圧倒的に多く、それ以降は数が急減と、リストの分布の形は似ています。これは単純に、攻撃者の多数がユーザー名とパスワードをランダムに数回試してから次へと進むためです。多くの場合、単一のIPで単一のユーザー名とパスワードが試行されています。単一のユーザー名とパスワード（「root:root」や「admin:admin」など）を試すこうしたIPアドレスには何度も観察されたものもあり、これはおそらくボットネットの一部として、自動化された方法で実行されているものと思われます。

注目すべき点は、どちらのプロトコルもパスワード分布がほぼ指数分布となることです。つまり、登場頻度の多いパスワードが登場する頻度はあまり一般的でないパスワードのそれに比べて指数関数的に多いことになります。この分布は、各プロトコルでのユーザー名上位2位が試行された他のユーザー名と比較して大きな外れ値である点を除けば、ユーザー名に関してはやや似た傾向があります。

ユーザー名とパスワードの分布（Y軸が異なる点に注意）



外れ値とデフォルト

いずれのプロトコルにも、頻度の点で大きな外れ値といえるユーザー名が2つあります。RDPについては、「Administrator」と「administrator」がこれに該当します。RDPのユーザー名は大文字と小文字を区別しないことを考慮すれば、これらは実際には同じ1つのユーザー名ということとなり、頻度の点ではさらに外れ値となります。これは、RDPが通常Windowsシステムで実行され、デフォルトのローカル管理者アカウント（インストール中に最初に作成されるアカウント）の名前が「administrator」であることが要因と思われます。

対してSSHの場合は「root」と「admin」の2つが目立ちます。これは、Linuxディストリビューションの大半に「root」という名前のユーザーが含まれていること、また「admin」が特にルーターやIoTデバイスの場合に一般的なデフォルトユーザーであることが理由で、攻撃者にとっては論理的な選択といえます。

マルウェア、特にMiraiなどのIoTデバイスを標的とするマルウェアは一般的に、デバイスのデフォルトの認証情報で認証を試みることによって拡散します。最近の亜種は、一般公開されている脆弱性のエクスプロイットの組み込みに大きく依存する傾向がありますが、観察された認証情報を既知のデフォルトのリストにマッピングすることで、こうしたマルウェアキャンペーンの標的となっている新しいデバイスセットを特定することは依然として可能です。Rapid7がデフォルトの認証情報を通じて検索を行うオープンソースツールDefaultinatorを開発した理由もそこにあります。

「rockyou」セットには一般的なデフォルトパスワードが多数含まれていますが、だからといってこの認証情報ファイルを使用する悪意のあるアクターが個別のデバイスを特別に狙っているというわけではありません。ただ、この一般的なデータソースにデフォルトの認証情報が相当数含まれる以上、管理対象のデバイスからそうした認証情報を削除するよう注意するのが賢明といえるでしょう。

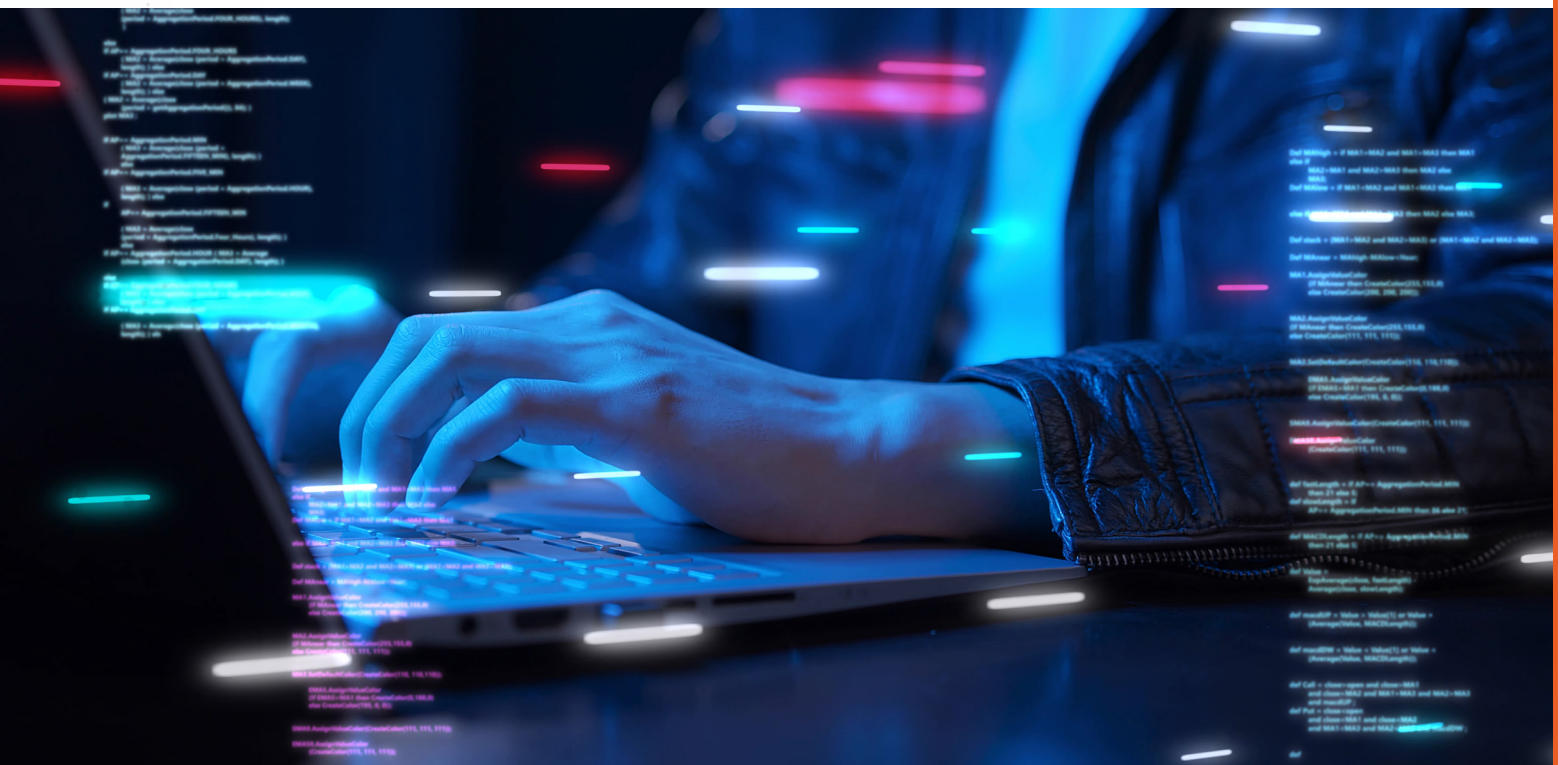
セキュアシェル（SSH）

Rapid7のSSHハニーポットで観察された497,848件のパスワードのうち、群を抜いて多かったパスワードが「123456」と「password」であり、他の一般的なデフォルトパスワードに比べても、攻撃者がシステムに容易に接続するリスクを高めるものといえます。「rockyou」セットの説明で述べたように、こうしたパスワードは簡単に推測可能であり、攻撃者はスキルレベルの巧拙に関係なく、これらのパスワードを使用してシステムに簡単にアクセスすることができます。

観察されたパスワードリストから「rockyou」セットを削除すると、497,848件のパスワードのうち残るのはわずか14件となります。これら14件にはすべてハニーポットのIPアドレスが含まれており、一度のみ観察されました。[1]

確かに「rockyou」セットには膨大な数のパスワードが含まれていますが、考えうるパスワード候補全体に比べればごく一部に過ぎません。例えば、印刷可能なASCII文字95文字すべてを使って7文字きっかりのパスワードを作成すると、合計で約70兆（95^7）件にもなり、「rockyou」セットに含まれる約80億件よりも4桁も

[1] こうしたIPアドレスを含むパスワード14件が存在することはかなり不可解です。Rapid7のハニーポットは動的IPアドレスに存在するため、誰かが動的IPアドレスを含めるように静的パスワードを意図的に設定するのは奇妙に思えます。これが攻撃者が探していた特定のデバイスの機能によるものなのか、この「<パスワード><IPアドレス>」のパターンがこのスキャナー側のプログラミングエラーによるものかは不明ですが、後者の方が可能性が高いように思われます。



多くなります。6文字、8文字、10文字のパスワードをまったく考慮せずにこの規模になるわけですから、自動攻撃システムが本当にランダムなパスワードをスプレー攻撃するならば、その規模は膨大なものになるはずです。

以下は、SSHに対して試行されたユーザー名とパスワードの上位20位です。ユーザー名の1位は「root」、2位が「admin」、最後の20位が「minecraft」、対してパスワードは「123456」が1位、「P@ssw0rd」が20位という結果になっています。

SSHユーザー名上位20位

1. root
2. ubuntu
3. guest
4. hadoop
5. admin
6. postgres
7. support
8. ftp
9. nproc
10. oracle
11. mysql
12. nagios
13. user
14. ftpuser
15. testuser
16. deploy
17. test
18. git
19. user1
20. minecraft

SSHパスワード上位20位

1. 123456
2. nproc
3. test
4. qwerty
5. password
6. 123
7. 12345678
8. 1qaz2wsx
9. 1234
10. root
11. 123456789
12. 123123
13. admin
14. 「」(空の文字列)
15. admin123
16. abc123
17. 12345
18. 1
19. admin1
20. P@ssw0rd

497,848

リモートデスクトッププロトコル(RDP)

RDPは長らく、脅威アクターの格好の標的とされており、過去数年間の侵害の多くは脆弱なRDP認証に起因するものです。侵入テスターによれば、RDPでのパスワードスプレー、ブルートフォース、認証情報の使い回しが標的への初期アクセスを取得する方法としてよく使用されます。さらに、過去6年間でRDP関連の脆弱性(CVE-2019-0708(BlueKeep)が最も有名)が多数出現し、RDPのデフォルトポート3389が開いているシステムを攻撃者が探す理由がますます増えました。

上位20位の中で特に目を引くパスワードが「AuToLoG2019.09.25」です。この文字列を検索しても確からしい結果は表示されませんが、文字列「AuToLoG」が含まれるマルウェアのサンプルが多数表示されます。これらのサンプルは、ほとんどのウイルス対策ベンダーで汎用トロイの木馬に分類されていますが、RDP認証情報がハードコードされているようです。ちなみにこのパスワードは、「rockyou」セットに存在しない唯一のパスワードです。

RDPユーザー名上位20位

1. Administrator	6. tor	11. C	16. rdp
2. root	7. Student	12. adminGG1	17. 1
3. Admin	8. Administrador	13. admin	18. administrador
4. guest	9. user	14. test	19. 「」(空の文字列)
5. administrator	10. user0	15. Guest	20. azureuser

RDPパスワード上位20位

1. 「」(空の文字列)	6. Administrator	11. Aa123456	16. 1q2w3e
2. 123	7. root	12. %username%	17. 1
3. password	8. qwe123	13. AuToLoG2019.09.25	18. %null%
4. 123qwe	9. 123456	14. !	19. administrador
5. admin	10. administrator	15. admin@123	20. !@#123

2016年からの変化

2016年の『Attacker's Dictionary』におけるRDPの上位2位のユーザー名は「administrator」と「Administrator」でした。2022年のランキングでは異なりますが、RDPとWindowsの関連性、加えてWindowsで「administrator」アカウントが一般に使用されていることから、少なくとも攻撃者がユーザー名に大文字と小文字の区別がないことに気付くまで、これらが上位にとどまる可能性は高いでしょう。3位以下は大きな差をつけて「user」、「admin」、「tor」が続きます。2016年と2022年の違いとして注目すべき点に、ユーザー名20位に「azureuser」が登場している点が挙げられます。Microsoft Azureのリリースは2010年でしたが、2016年にはクラウド導入が今日ほど一般的ではなく、またAzure自体もそれほど成熟していませんでした。ここから、攻撃者がオペレーティングシステムとIoTのデフォルトだけでなく、クラウドプロバイダーのデフォルトにも目を向け始めていることが伺えます。

推奨事項

本レポートでは、システムへのアクセスのために脆弱なパスワードを推測するテクニックが、多くの点で、非常に長期にわたり変わっていないことを示してきました。そのため、以下での推奨事項にはお馴染みのものが多くなります。ただ、こうしたテクニックが未だに機能し、犠牲者が出続けていることを考えると、今一度繰り返す価値はあるものと考えられます。

デフォルトのユーザー名使用を回避

標的型攻撃ほどの効果はないものの、日和見攻撃の圧倒的多数では、「root」、「admin」、「administrator」など、少数の推測可能なユーザー名が使用されていました。こうした弱点を修正するには、長年にわたり推奨されてきたことではありますが、可能な限りローカル管理者とゲストアカウントを無効にするのが有効です。これは、変更を忘れやすいIoTデバイス（エンドユーザー側での変更が可能な場合に限る）や、利用期間が短いと思われる（ものの、意外に長く、攻撃対象になりうる）クラウド展開で特に注意すべき点です。

パスワードの使い回しを回避

ユーザーがパスワードを覚えておくべきアカウントの数は数十件に上るため、パスワードは再利用されがちです。アプリケーションに必要な数だけランダムなパスワードを生成し、最新の暗号理論で安全に保護された暗号化保管庫に格納できるBitwarden、1Password、LastPassなどの最新のパスワードマネジャーを使えば、こうした問題は比較的簡単に緩和できます。複数のユーザー間で認証情報が共有されている場合（避けるべき状況ですが実際にはありがちです）、保管庫を他のユーザーと安全に共有することもできます。パスワードマネージャーを使用すると、完全にランダムな（「rockyou」セットにない）パスワードを生成し、ウェブサイトごとに異なるパスワードを設定でき、1つのアカウントが侵害された場合にも、他のアカウントは安全に保てます。

RDPと SSHの保護

RDPとSSHはいずれも、ブルートフォース認証試行の標的となりやすいため、これらのサービスを設定する際にはベストプラクティスに従うことが非常に重要です。こうしたベストプラクティスには、外部への露出を制限し、認証スペースの複雑さを強化する方法が多数含まれています。

こうしたサービスでのブルートフォース攻撃から企業を保護するには、企業VPNを使用し、すべてのリモート接続をVPN認証ホスト経由でのみ機能するように制限することを検討しましょう。また、サービスのデフォルトのポートを変更することもできます。ポートの変更は「隠蔽によるセキュリティ」の試みに当たりますが、ブルートフォース攻撃の大部分を防ぐことができます。

RDPの場合には、RDPを公開しているインスタンスが信頼できるIPアドレスからのみアクセス可能となるよう、ファイアウォールとネットワークセキュリティグループ経由でアクセスを制限するのが最善の方法です。RDPをインターネットに直接公開するのではなく、クラウドデプロイメントにジャンプホストや要塞ホストを使用するのも名案です。

SSHをセキュリティ保護する際に可能な最も重要なセキュリティ対策は、パスワードベースの認証を無効にし、証明書ベースの認証を優先することです。また、sshd_configファイルを変更し、SSHを有効にしているユーザーを制限することも強くお勧めします。こうした推奨事項に従うだけでも、オンラインのブルートフォース攻撃からかなりの水準で保護を確保できますが、他にも対応方法はいくつかあります。一般に、すべてのrootアカウントでSSHを無効にすることをお勧めします。また、最大ログイン試行回数を変更したり、認証試行回数が多すぎるソースを自動的にブロックするfail2banなどのプラグインを使用することもできます。

外部監視

社内とクラウドのインフラストラクチャを日和見主義的なオンラインブルートフォース攻撃に対して保護する対策が完了したら、ポート22/TCPと3389/TCP（それぞれSSHとRDP）につき、外部からの攻撃面を確認することをお勧めします。現時点での露出を確認する作業が完了しても、最新のネットワークには時折新しいサービスが登場するため、外部スキャンを通じてパブリックIP空間を定期的に監視することで、組織内で発生している（善意のものが大半ですが）「シャドーIT」運用を発見し、注意を向けられ、全社的なセキュリティ体制のギャップをすばやく封止する機会につなげることができます。

セキュリティ強化を支援

Rapid7について

Rapid7は、デジタルトランスフォーメーションの加速に直面する組織のセキュリティプログラム強化の支援を通じ、あらゆる人にとってより安全なデジタルの未来を創造しています。Rapid7のソリューションポートフォリオは、セキュリティ担当者がリスクを管理し、アプリからクラウド、従来のインフラストラクチャ、ダークウェブに至るまで、脅威のランドスケープ全体にわたって脅威を排除するための支援を提供します。Rapid7は、オープンソースコミュニティと最先端の研究を促進し、得られる洞察を製品の最適化に活用し、最新の攻撃方法に対応する力を世界のセキュリティコミュニティに届けます。世界中の10,000社以上の顧客組織に信頼され、業界をリードするソリューションとサービスで、企業が攻撃者の一歩先を行き、競争に先んじ、常に将来に備えるためのお手伝いをします。

RAPID7

製品

クラウドセキュリティ
XDR & SIEM
脅威インテリジェンス
脆弱性リスク管理
アプリケーションセキュリティ
オーケストレーションと自動化
マネージドサービス

ラピッドセブン・ジャパン株式会社
電話：03-6838-9720

詳細と無償評価版については、https://www.rapid7.com/ja/trial/insight/ を参照してください。