セキュリティ・アドバイザリ

安全でないプロトコルの使用は組織のサイバーセキュリティを危険にさらす

エグゼクティブ・サマリ

近年、既知の脆弱性を持つ、安全でないプロトコルは深刻なサイバー・リスクをビジネスにもたらすという苦い教訓を世界中の組織が学んできました。しかし、WannaCry や NotPetya のような損失の大きいイベントが発生しても、組織の多くは、それを知りつつ、またはそうとは知らずに、安全でない非推奨プロトコルを自社の環境で実行することを許しています。このレポートでは、現在でも広く使用されている安全でないプロトコルをいくつか考察し、それに伴うリスクを評価して、環境内に潜む脆弱性を見つけて排除する方策について、セキュリティと IT の運用チームに指針を与えます。

目次

はじめに

2017 年 5 月 12 日、ランサムウェア WannaCry の亜種は山火事のように急速に広がり、世界中の公共/民間部門の組織が所有する 23 万台を超えるコンピュータを感染させ、暗号化しました。その損害額は、数十億ドルまではいかないにせよ、数億ドルに及んでいます。それから 2 か月も経たないうちに、NotPetya による別のランサムウェア攻撃が発生し、再びグローバル組織が直撃を受けました。このときは海運業が一時的に活動不能になり、損害は Maersk の 1 社だけで 3 億ドルにのぼりました。

NotPetya と WannaCry の共通点は、両者が与える損害の規模や範囲に留まりません。マイクロソフトのサーバ・メッセージ・ブロックのバージョン 1（SMBv1）プロトコルが抱える脆弱性を悪用する点も同じです。この脆弱性を突くのが EternalBlue と呼ばれるエクスプロイトです。これらの攻撃による苦痛がとりわけ堪え難いのは、避けることができたかもしれない攻撃だからです。

EternalBlue が米国の国家安全保障局（NSA）によって開発されたエクスプロイトであることは周知の事実です。NSA は、EternalBlue の存在をマイクロソフトに公開するまで、このエクスプロイトをほぼ 5 年にわたって使用しました。2017 年 3 月、マイクロソフトは速やかにパッチを発行し、その 2 か月後に WannaCry による攻撃が起きました。高度な脅威アクターが探し求めているのは先進テクノロジではありません。それとは逆に、企業内における最大の弱点を探します。基本的に安全でない、旧式のプロトコルは特に関心の的となります。

マイクロソフトによるパッチ発行と対応するアラートによってさえも、広範囲にわたるパッチの適用が実現していなかった場合、Shadow Brokers と呼ばれるグループによる 2017 年 4 月 14 日の脆弱性の公開により、この脆弱性の重大度は明確に伝わっていたはずです。それにもかかわらず、公開の 1 か月後、この脆弱性は、WannaCry の犯行者によって効果を最大限に高めるために悪用されました。わずか 6 週間後に再び起こったことで、この悪用はさらに堪え難いものになりました。

それにもかかわらず、こうした破壊的な攻撃から 4 年経った現在でも、SMBv1 はエンタープライズ環境で驚くほど広く使用されていることが ExtraHop の調査で明らかになりました。エンタープライズ環境のほぼ 90%は、このプロトコルを今なお実行しているデバイスを 1 つ以上使用していました。さらに、安全でないプロトコルは SMBv1 に限定されません。LLMNR（Link-Local Multicast Name Resolution）や NTLM（NT LAN Manager）など、安全でない他のプロトコルもまだ使用されています。元来、HTTP は安全性が低いわけではありませんが、機密データの送信に使用すると深刻な問題が生じます。エンタープライズ環境では、この HTTP も今なお広く使用されています。

このレポートでは、安全でないプロトコルが企業内で広く使用されている実態とそれぞれのプロトコルに伴うリスクについて洞察し、こうした弱点をエンタープライズ環境から排除するための推奨事項を提供します。

プロトコルの仕組み

プロトコルはネットワークの共通語です。接続しているデバイスは、オペレーティング・システム、ハードウェア、プロセスの違いを越えて、プロトコルを介して相互に通信することができます。異なるネットワーク・デバイス間でのデータの送信方法を定めた、一連のルールを確立することでプロトコルは機能します。プロトコルには、データを保護する方法（暗号化）からドメインを解決する方法まで、すべてのルールが含まれます。ネットワーク通信のプロトコルは更新や改良が可能であり、新規に作成することもできますが、今日、広く使用されているプロトコルの多くは数十年前から存在しています。

IT チームと悪意のあるアクターの双方が、各種のプロトコルをさまざまな方法で使用しています。たとえば、ドメイン・ネーム・システム（DNS）プロトコルは、人間が判読可能なドメイン名に IP アドレスをマッピングすることで、ユーザによるインターネット上の移動を容易にします。しかし、コマンド・アンド・コントロール（C2）やデータ流出などの悪意のある目的のために、このプロトコルは攻撃者によってしばしば悪用されています。

ExtraHop のネットワーク・プロトコル・ライブラリにアクセスして、プロトコルとそれに関連する脅威アクティビティの詳細情報をご覧ください。

このレポートでは、SMBv1、LLMNR、NTLM、HTTP の 4 つのプロトコルを重点的に取り上げて、企業の IT 環境内で広く使用されている実態と、それぞれのプロトコルに伴うリスクについて説明します。

SMBv1
2021 年、
エンタープライズ
環境の 67%は
SMBv1 を使用

導入
1983 年
非推奨
2013 年
損害
10 億ドル以上

Server Message Block (SMB) v1

サーバ・メッセージ・ブロック（SMB）は 1980 年代に開発されたプロトコルであり、ファイルやプリンタ・サービスの共有、ネットワーク・デバイス間の通信に主に使用されています。1980 年代から 1990 年代にかけて、マイクロソフトは Common Internet File System（CIFS）という名称で SMBv1 のイメージー新を図り、その機能を拡張して大きなファイルの送信を実現し、ポート 445 経由の直接接続を確立しました。

その結果、SMBv1（CIFS）はバグが多く、頻繁なやりとりを必要とする、使いづらいことで有名なプロトコルとなり、セキュリティ上の大きな欠陥を抱えていました。2006 年に SMBv2 を導入すると、マイクロソフトは CIFS という名称を完全に放棄しました。6 年後の 2012 年、マイクロソフトは SMBv3 を導入し、2013 年には SMBv1 を公式に非推奨としました。

非推奨にもかかわらず、マイクロソフトは自社の Windows Server への SMBv1 のインストールを 2016 年まで継続しました。その頃までには、マイクロソフトは、SMBv1 の使用をやめるように自社のユーザ･コミュニティに積極的に働きかけていました。しかし、このプロトコルを使用しているマシンは数百万台に及んでおり、警告の多くは見過ごされました。そうした警告には、Windows Server のエンジニアリング・グループ内から出されたものもありました。EternalBlue とその関連エクスプロイト（Eternal(x)と総称）が 2017 年に明らかになっても、世界中の IT 環境で SMBv1 が引き続き広く使用されていたのは、こうした理由によるものです。Eternal(x)は、SMBv1 のバッファ・オーバーフローの脆弱性を悪用します。

EternalBlueの仕組み

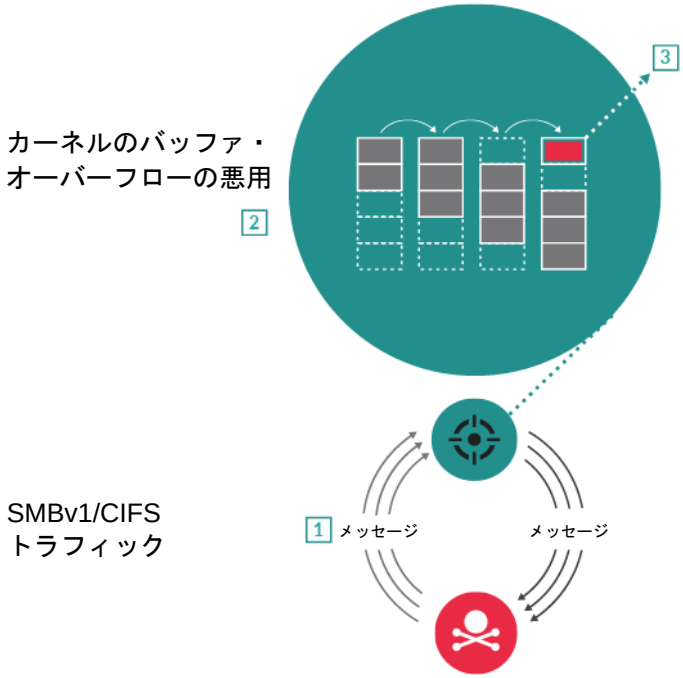

図1 サーバ・メッセージ・ブロック 1.0（SMBv1）は、ファイル共有/トランザクション・プロトコルの 1 バージョンであり、EternalBlue エクスプロイトの標的となる、メモリ計算の脆弱性を抱えています。最初に、攻撃者は複数の要求またはメッセージを SMBv1 経由でファイル・サーバに送信します（1）。SMBv1 の各メッセージは、ファイル・サーバのメモリを操作して、最終的にバッファ・オーバーフローを引き起こすように特別に作られています（2）。これにより、攻撃者はランサムウェアなどの悪意のあるペイロードをサーバのカーネルに配信することができます（3）。WannaCry ランサムウェアなど、いくつかの周知のセキュリティ攻撃は、この EternalBlue エクスプロイトと関係があります。

> “SMBv1 の設計上の基盤となった世界はもはや存在していません。それは、悪意のあるアクターがいない世界、膨大な量の重要データがない世界、ほぼ普遍的なコンピュータの使用がない世界です。
> 率直に言って、現代の視点から見ると、その素朴さは信じがたいほどです。
>
> - Ned Pyle 氏。マイクロソフトで 15 年の勤務経験を持つ、Windows Server エンジニアリング・グループのプリンシパル・プログラム・マネージャ

SMBv1 の使用状況

2021 年の 1～3 月に ExtraHop が実施した調査によると、エンタープライズ環境の 88%は、SMBv1 を実行しているデバイスを 1 つ以上使用しています。驚くべき数字と思うかもしれませんが、ここでの朗報は、デバイスが 1 つだけの場合は意図的である可能性が高いことです。レッド・チームは、侵入テストを実行するツールとして SMBv1 を引き続き使用しており、1 つのインスタンスのみを保有している環境はこれで説明がつくものと思われます。

問題は、SMBv1 を実行しているデバイスを 10 個以上使用しているエンタープライズ環境が 67%もあることです。こちらは、意図的である可能性は低いでしょう。10 個のデバイスは比較的少ないと思われるかもしれませんが、Eternal(x)エクスプロイトによって有効化されるリモート・コード実行により、SMBv1 を実行しているデバイスは容易なピボット・ポイントと化します。ここから、大規模な攻撃を仕掛けることができるのです。この 10 個のデバイスは、環境内にある資産のほんの一部かもしれません。しかし、防御は失敗ゼロのミッションです。破壊的な攻撃を仕掛けるために、環境内のすべてのデバイスに SMBv1 がインストールされている必要はありません。1 つのデバイスにあればよいのです。

次の数字を知るとさらに恐ろしくなります。ExtraHop のデータによると、エンタープライズ環境の 37%は、50 個以上のデバイスで SMBv1 を実行しています。さらに、エンタープライズ環境の 31%は、世界を揺るがした WannaCry と NotPetya の攻撃から 4 年経過しても、100 個以上のデバイスでこのプロトコルを引き続き使用しています。

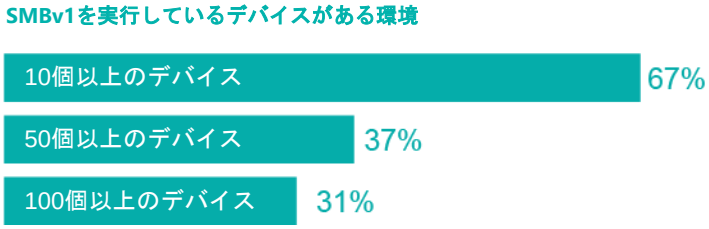

図 2 この図は、SMBv1 を実行しているデバイスが環境全体で広く使用されていることを示しています。

現場の状況：SMBv1

いちかばちかの賭け

EternalBlue による脆弱性が表面化してから 2 年近く経った 2019 年の初め、ExtraHop は、米国の連邦政府機関のある部局と協働していました。その機関は、SMBv1 を実行しているマシンを引き続き使用していることは知っていました。一方、どのマシンか、また何台あるのかについては知りませんでした。

> 破壊的な攻撃を仕掛けるために、環境内のすべてのデバイスに SMBv1 がインストールされている必要はありません。1 つのデバイスにあればよいのです。

この機関が抱える課題は 2 つの要素から成り立っていました。第一に、SMBv1 を引き続き実行していたのは、このプロトコルを使用しているレガシ・システムの数が非常に多かったからです。このプロトコルの排除は、ロジスティクス上の大仕事でした。というのも、システムの多くは、SMBv1 の後続バージョンを使用できない Windows XP で実行されていたからです。しかし、最近になって、この機関は、SMBv1 プロトコルのサポートを打ち切ることになると NAS ベンダから告げられました。

第二に、SMBv1 の脆弱性（とその悪用がもたらす損害）が明らかになった後もそれをずっと使い続けていたものの、この機関は、このプロトコルに付随するリスクを十分に知っていました。

この機関のセキュリティ・チームは、Reveal(x)の SMB/CIFS ダッシュボードを使用して、SMBv1 を実行しているすべてのデバイスを特定しました。セキュリティ・チームは、このプロトコルを使用しているデバイスが依然として多数にのぼることにすぐに気づきました。VDI の導入全体もそれに含まれていました。このプロトコルは、動きの速いランサムウェア攻撃をはじめとする、大きなリスクを連邦政府機関の部局にもたらしていました。

SMBv1 からの移行には努力を要しましたが、この措置により、この機関の環境は最終的により安全なものとなりました。残念なことに、SMB プロトコルの新しいバージョンをサポートしていないレガシ・システムが引き続き使用されており、多くの組織が Eternal(x)に悪用されるリスクにさらされている大きな理由となっています。

WannaCry の 4 年後のランサムウェアとの遭遇

2021 年 3 月、台湾のコンピュータ大手企業 Acer が、ランサムウェアによる深刻なセキュリティ侵害を受けていたことが報道されました。5,000 万ドルの身代金要求は過去最高額でした。また、攻撃に関わったサイバー犯罪グループの REvil は、切り札を用意していました。このランサムウェア攻撃では、Acer のファイルの大半を暗号化しただけでなく、大量のデータ流出も実行していたのです。Acer がバックアップを取っていた場合でも、盗んだデータを漏らすと脅迫すれば身代金を取れると考えたのです。

サイバー犯罪者がその支配力を最大限に発揮しようとするなかで、流出させて暗号化するという手口は、ランサムウェア攻撃でよく使われるようになっています。Acer への攻撃が報道されるわずか数か月前に、ExtraHop のお客様がこれとよく似た攻撃を体験していました。

2020 年末、北米に拠点を置く ExtraHop の大口顧客が、ランサムウェア活動の検知に関するアラートを Reveal(x) 360 から受け取りました。これらのデバイスについては、SMB のデータ・ステージングと疑わしいファイル読み取りの検知を知らせるアラートも表示されていました。関連する検知を調べることで、お客様のセキュリティ・チームは、最大限の損害を与えられるように、攻撃者がデータの暗号化に先立ってデータ流出のプロセスも進めていると判断しました。

セキュリティ・チームは、影響を受ける資産とアカウントを速やかに特定して隔離することができました。その結果、攻撃者は、標的にしたファイルのごく一部しか暗号化できませんでした。

この場合、お客様は難を逃れることができましたが、この体験は教訓となります。新しいランサムウェアのプレイブックとしてだけでなく、SMBv1 に付随する継続的なリスクについても教訓を含んでいます。このプロトコルを実行しているデバイスは、攻撃者、とりわけ情報よりもお金に関心を寄せているランサムウェアの犯罪グループにとって常に格好の標的となります。

ランサムウェアの動向の詳細については、こちらを参照してください。

> 攻撃者は、パッチが適用されていない他のサーバにネットワーク経由で急速にマルウェアを拡散できます。

SMBv1 のリスク

SMBv1 が簡単に悪用され、WannaCry や NotPetya などの攻撃に利用されているのは、攻撃者は、SMBv1 が有効になっているサーバへのアクセスに成功すると、パッチが適用されていない他のサーバにネットワーク経由で急速にマルウェアを拡散できるからです。SMBv1 に基づく攻撃では、攻撃者は複数の要求またはメッセージを SMBv1 経由でファイル・サーバに送信します。SMBv1 の各メッセージは、ファイル・サーバのメモリを操作して、最終的にバッファ・オーバーフローを引き起こすように特別に作られています。これにより、攻撃者はランサムウェアなどの悪意のあるペイロードをサーバのカーネルに配信することができます。

特に危険なのは、システム・レベルのサービスに対するバッファ・オーバーフロー攻撃です。攻撃者は、より自由に後続アクティビティを選べるからです。その例として、悪意のあるペイロードの注入、メモリからのユーザ資格情報の取得、メモリ内にのみ存在する非表示の永続化メカニズムのセットアップなどが挙げられます。

LLMNR
2021 年、
エンタープライズ
環境の 70%は
LLMNR を使用

導入
2007 年
非推奨
なし
損害
不明

LLMNR（Link-Local Multicast Name Resolution）

LLMNR（Link-Local Multicast Name Resolution）は、DNS サーバを使用せずに名前解決を可能にするプロトコルです。基本的には、LLMNR はポート UDP 5355 経由でマルチキャスト・ネットワーク・アドレス（224.0.0.0～239.255.255.255）に送信されるネットワーク・パケットに基づいて、ホスト名から IP アドレスへの解決を提供するレイヤ 2 プロトコルです。マルチキャスト・パケットはすべてのネットワーク・インターフェイスに対してクエリを実行し、そのクエリで確実にホスト名と見なすことができるものを探します。

LLMNR は、IETF 標準プロトコルに採用されたことがないという点で、このレポートに記載されている他のプロトコルとは異なります（ただし、RFC 4795 では定義されています）。

当初、LLMNR は、小規模なプライベート・ネットワークなど、DNS サーバが実用的でない環境で名前解決を可能にする回避策として作成されました。LLMNR は、DNS の煩雑な要件なしに名前解決を実現する方法として生み出されました。このプロトコルは、ファイル・サーバなどのネットワーク・デバイスを識別するために、Microsoft Windows をはじめとするオペレーティング・システムによって使用されてきました（現在も使用されています）。

LLMNR の使用状況

リスクの大きい、完全なプロトコルとは言えないプロトコルにしては、今でも驚くほど広く使用されています。ExtraHop Reveal(x)が提供する匿名化されたネットワーク・テレメトリによると、エンタープライズ環境の 70%は、10 個以上のクライアントで LLMNR を引き続き実行しています。残念なことに、デバイス数が増えても、脆弱なクライアントを使用している環境の数はそれほど減っていません。エンタープライズ環境の 55%は 50 個以上の LLMNR クライアントを使用しており、46%は 100 個以上の LLMNR クライアントを使用しています。

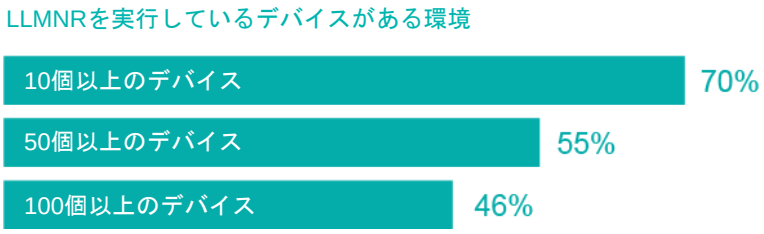

図 3 この図は、LLMNR を実行しているデバイスが環境全体で広く使用されていることを示しています。

LLMNR のリスク

LLMNR により、DNS のないメカニズムによるホスト名解決がローカル環境内で実現しますが、悪意のあるアクターも攻撃の手段を得ることになります。攻撃者はこのプロトコルを使用して、被害者をだましてユーザ資格情報を開示させることができます。これは、LLMNR を利用してユーザの資格情報ハッシュにアクセスすることで行われます。資格情報ハッシュが破られると、実際の資格情報が明らかになります。これが特に該当するのは、LANMAN のような古い MS パスワード技法が無効になっていない場合です。

攻撃者はどのような手順を踏むのでしょうか。最初のステップは、いかなるクエリに対しても関連のあるホスト名であると応答するようにネットワーク上のノードを設定することです。要求元のクライアント側では、これによって競合状態が生まれ、クライアントは最初に応答したデバイスを無条件に受け入れるだけでなく、それを信頼するようになります。というのも、LLMNR のプロトコル仕様には、すべてのクライアント応答は信頼できると明記されているからです。

資格情報ハッシュが役割を果たすのはこのときです。セキュリティ侵害を受けたデバイスから「私です！」という決定的な応答を受信したクライアントは、応答の一環として、現在のユーザの資格情報のハッシュされたコピーを自動的に送信します。これにより、資格情報のハッシュされたコピーを受け取った攻撃者は、その資格情報を復号することも、Pass-the-Hash 攻撃で利用して、より広範なネットワーク内で特権昇格を開始することもできます。

SolarWinds SUNBURST の攻撃者が DNS をどのように使用したのか詳細を確認 ›

DNS には課題も伴いますが、ホスト名を正確に識別できる、はるかに安全な方法です。そうは言うものの、不正目的で使用されることがないように、DNS 自体を慎重に監視すべきです。

LLMNR のブロードキャスト

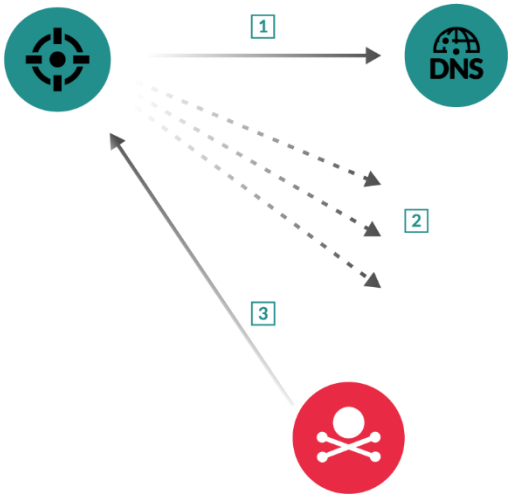

図 4 ホスト名の DNS 要求を解決できない場合や、DNS サーバを利用できない場合（1）、LLMNR が有効になっているクライアントは、すべてのローカル・デバイスに UDP 5355 経由でクエリをブロードキャストします（2）。攻撃者がリッスンしている場合は、これに応答して要求されたホストを偽装することができます（3）。ホストが認証済みリソースの場合、クライアント応答にユーザの資格情報が含まれます。

NTLMv1
2021 年、
エンタープライズ
環境の 34%は
NTLMv1 を使用

導入
1993 年
非推奨
2010 年
損害
不明

NTLM（New Technology LAN Manager）v1

NTLM（New Technology LAN Manager）は、LANMAN（Microsoft LAN Manager）の後継プロトコルとして 1993 年に導入された、マイクロソフトの専用プロトコルです。NTLM は、認証、整合性、機密性を一括してユーザに提供することを目的とする、マイクロソフトのセキュリティ・プロトコル群に属しています。

NTLM はいわゆるチャレンジ/レスポンス・プロトコルであり、パスワード・ハッシュを使用したサーバのクライアント認証で使用されます。初代の NTLMv1 では、かなりシンプルな（セキュリティ侵害が容易な）認証方法が使用されていました。マイクロソフトは、NTLM がユーザを認証するプロセスを次のように説明しています。

> ***NTLM の資格情報は、対話型ログオン・プロセスで得たデータに基づいており、ドメイン名、ユーザ名、ユーザ・パスワードの一方向ハッシュで構成されています。NTLM は、暗号化されたチャレンジ/レスポンス・プロトコルを使用してユーザを認証します。その際、ユーザのパスワードがネットワーク経由で送信されることはありません。代わりに、認証を要求するシステムは、セキュリティで保護された NTLM 資格情報へのアクセス権がユーザにあることを証明する計算を実行する必要があります。***

最終的に、NTLMv1 は NTLMv2 に置き換えられましたが、悪意のあるアクターがパスワードを傍受するのを実際に防ぐという点では、この次世代プロトコルもそれほど効果を上げていません。タイム・スタンプとユーザ名がハッシュに追加されるなど、NTLMv2 ではいくつかの機能が加えられました。この機能追加はオフラインでのリレー攻撃の軽減には役立ちますが、別の脆弱性を取り込むことになり、全体的なプロトコルのセキュリティはほとんど改善されませんでした。

この暗号方式が抱える問題は、信じられないほど簡単に解読されることです。2012 年には、NTLM の 8 バイト・ハッシュによる、可能なすべての順列が 6 時間足らずで解読できることが実証されました。2019 年、オープン・ソースのパスワード復元ツールである HashCat は、どんな 8 バイト・ハッシュでも 2 時間半以内に解読できることを実証しました。*The Register* は、映画「アベンジャーズ/エンドゲーム」を観るよりも短い時間だと、そのトレードマークである皮肉を込めて言及しました。

NTLMv1 の使用状況

はるかに安全な Kerberos 認証プロトコルを選択して、NTLM の使用は中止するようにマイクロソフトが勧告したにもかかわらず、エンタープライズ環境では NTLM が今でも広く使用されています。ExtraHop は NTLMv2 の遍在性については調査しませんでしたが、2 つのバージョンのうち、安全性で劣る NTLMv1 はまだ広く使用されています。

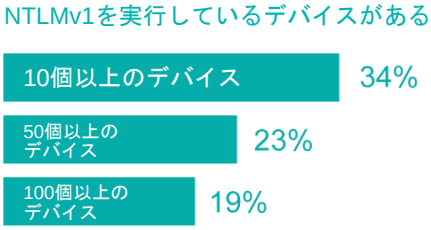

図 5 この図は、NTLMv1 を実行しているデバイスが環境全体で広く使用されていることを示しています。

Reveal(x)が提供するネットワーク・テレメトリによると、エンタープライズ環境の 34%は、10 個以上のクライアントで NTLMv1 を実行しています。これと同じ数のデバイスで SMBv1 や LLMNR を実行している組織よりは数は減りますが、10 年間、非推奨とされてきたプロトコルにしては相当な数と言えます。組織の 23%は 50 個以上のクライアントで NTLMv1 を使用しており、19%は、100 個以上のクライアントでこのプロトコルを認証に使用しています。

> 熟練した攻撃者は、パスワードに等しい NTLM ハッシュを容易に傍受することも、NTLMv1 のパスワードをオフラインで解読することもできます。

NTLM のリスク

NTLM を認証に使用すると、組織は多くのリスクにさらされます。熟練した攻撃者は、パスワードに等しい NTLM ハッシュを容易に傍受することも、NTLMv1 のパスワードをオフラインで解読することもできます。NTLMv1 認証の悪用に成功すると、攻撃者は、マシン・イン・ザ・ミドル（MITM）攻撃を仕掛けたり、ドメインを完全に掌握したりできます。

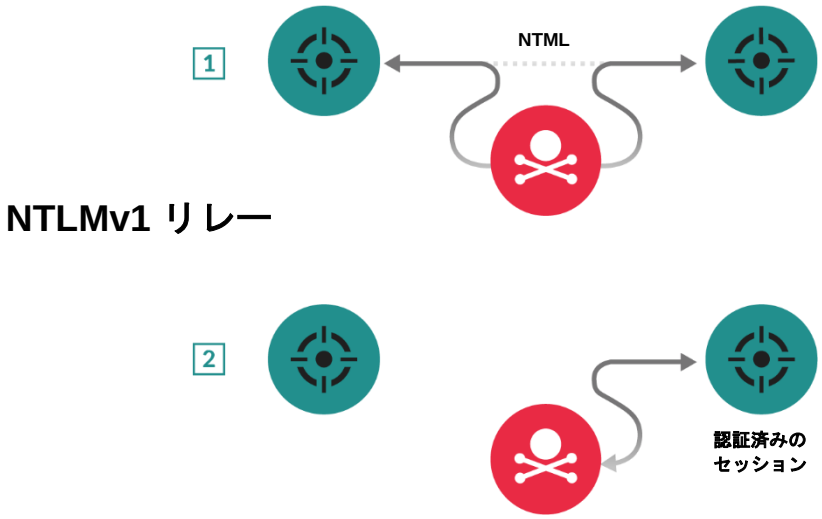

図 6 NTLM リレー攻撃の実行中、攻撃者は間に割り込むマシンの役割を果たし（マシン・イン・ザ・ミドル：MITM）、NTLM メッセージを受信して転送します[1]。次に、攻撃者はサーバとの認証済みセッションを作成します[2]。この技法では、NTLM ハッシュさえあれば、攻撃者はネットワークを横方向に移動することも、サーバに保管されている機密情報にアクセスすることもできます。

MITM 攻撃では、悪意のあるアクターはクライアントとサーバの間に割り込んで、この 2 つのデバイス間で送信されるデータをすべて傍受することができます。通信が暗号化されていない場合や、NTLM のように暗号が弱い場合、MITM 攻撃は、資格情報のセキュリティ侵害、PII の廃棄、企業秘密の盗難、偽データや操作されたデータの注入などの結果を招くおそれがあります。その証拠に、最近パッチが適用された、NTLM の現行バージョンの欠陥は、攻撃者が NTLM プロトコル内のセキュリティ機能を強制的にダウングレードすることを許しています。攻撃者は盗んだ資格情報を利用して、ドメイン管理者アカウントを識別するまでマシン間を移動することができます。この管理者アカウントを使用すると、AD サーバへの直接アクセスやドメインの完全奪取が可能になります。

HTTP
2021 年、エンタープライズ環境の 81%は HTTP を使用

導入
1991 年
非推奨
なし
損害
10 億ドル以上

HTTP（ハイパーテキスト転送プロトコル）経由のプレーンテキストの資格情報

HTTP（ハイパーテキスト転送プロトコル）は、ほぼ間違いなく最も知られているアプリケーション・プロトコルです。ネットワークの知識があるかどうかにかかわらず、これまでにアクセスしてきたあらゆる Web アドレスの冒頭で目にしているはずです。この分散/協調型のハイパーメディア情報システムを使用することで、ユーザはワールド・ワイド・ウェブ上でデータをやりとりすることができます。その姉妹プロトコルである HTML とともに、現在、私たちが知っているインターネットの基盤をなすのが HTTP です。

HTTP の導入から 4 年後の 1995 年、そのセキュリティ強化版である HTTPS が登場しました。HTTPS の登場は、インターネット上で支払い情報を処理できるようにしたいという企業の要望に応えるものでした。支払いカードの情報をむき出しにすることなく、HTTP でこれを実現することは不可能でした。HTTP とは異なり、HTTPS では TLS を使用してクライアント/サーバ間の通信を暗号化するため、送信中のデータを他人が傍受して読むのを防ぐことができます。さらにデータの整合性が維持され、データの破壊/破損防止にも役立ちます。

HTTP は、公式に非推奨となったことはありません。それでも、2017 年、Google は安全でない HTTP の使用を段階的に減らしていくために大きな一歩を踏み出しました。2017 年 1 月、Google Chrome は、HTTPS 以外のすべての Web サイトに「保護されていない」ことを知らせる表示を出すようになりました。それ以来、ログイン資格情報、クレジット・カード情報、PII などの情報を保存している Web サイトは、Chrome で効率的に機能するために HTTPS を使用しなければならなくなりました。Google はまた、HTTPS のサイトを検索で優先しています。

HTTP は本質的に問題を抱えているわけではありませんが、機密データの送信に使用すると、間違いなく大きなリスクを生むことになります。プレーンテキストの資格情報を HTTP 経由で送信すると、その資格情報は無防備な状態に置かれます。人がたくさんいる部屋でパスワードを叫ぶのに匹敵することをインターネット上でしているようなもので、資格情報の傍受や窃取が簡単に行えてしまいます。

HTTP 経由のプレーンテキストの使用状況

ExtraHop Reveal(x) 360 が提供する検知データによると、100 のエンタープライズ環境中 81 は、安全でない HTTP の資格情報を引き続き使用しています。

81%
暗号化されていない HTTPの資格情報を使用

図 7 この図は、安全でない HTTP がエンタープライズ環境全体で広く使用されていることを示しています。

現場の状況：HTTP 経由のプレーンテキストの資格情報

ExtraHop の専門家が大都市圏の法執行機関と協働していた 2021 年 3 月、Reveal(x)が「HTTP 経由で送信された資格情報」を検知しました。この検知によれば、資格情報の送信元デバイスは法執行機関のノート PC でした。ホスト名はこの機関のノート PC の命名方式と一致し、IP アドレスは同機関のドメイン領域内でした。さらに、ノート PC に関連付けられているユーザは、同機関の法執行官でした。

その後、セキュリティ・チームはピボッティングを行って HTTP 資格情報の宛先を調べました。それは、インターネット・アドレスでした。関連する記録を調べたセキュリティ・チームは、そのアドレスが広く知られた法執行機関の研究フォーラムであり、一般の人間も利用できることを確認しました。そのドメインは HTTPS ではなく、HTTP でした。

さらに憂慮すべきことは、その法執行官は、ログインを必要とする、身元が証明されたメンバ（通常は警察官などの捜査官）のサイトにアクセスしていたという事実です。ドメインが HTTPS ではなく HTTP であったため、ユーザ名とパスワードはいずれも暗号化されずに送信されました。そのため、悪意のあるアクターが資格情報を見つけて Web から直接盗むことも簡単にできました。

さらに調査を進めると、問題のサイトは適切な SSL 証明書を所有しており、SSL は有効化されていたことがわかりました。このサイトが暗号化を義務付けるように設定されていなかっただけですが、確認済みサイトのユーザである、何千人もの法執行官や捜査官のログイン資格情報を公開してしまう可能性がありました。

HTTP 経由のプレーンテキストの資格情報が抱えるリスク

上記の例で示したように、プレーンテキストの資格情報を HTTP 経由で送信すると、ユーザとその所属組織に多くのリスクをもたらします。資格情報に加えて、HTTP の Web サイトでは、クレジット・カード情報や PII などの顧客の機密データが容易に公開されるおそれがあります。

> “HTTP の Web サイトでは、クレジット・カード情報や PII などの顧客の機密データが容易に公開されるおそれがあります。

もちろん、HTTPS でも絶対に確実とは言えません。2014 年に最初に発見された、OpenSSL の深刻な脆弱性である Heartbleed は、HTTPS が悪用された典型的な例です。通常の場合、インターネット経由で送信されるログインやクレジット・カード番号などの情報は、SSL/TLS 暗号化によって保護されます。Heartbleed の脆弱性は、OpenSSL によって保護されているシステムのメモリを知らぬ間に公開し、トラフィックの暗号化に使用する秘密鍵を侵害して、ユーザ名やパスワードなどの機密情報に攻撃者がアクセスできるようにします。

HTTP/HTTPS は、Web サイトや Web アプリケーションからのユーザ入力の送信に使用されることが多いため、これらのプロトコルが悪用されて、パブリック・インターネットからプライベート環境への悪意のあるコンテンツの送信に使われることがあります。たとえば、SQL インジェクションの戦術をとる攻撃者は、HTTP プロトコルの HTTP ヘッダや、ユーザが操作可能な他のフィールドに SQL ステートメントを隠して送信します。HTTPS が使用する暗号化により、SQL インジェクション攻撃の検知が実際には難しくなるおそれがあります。

Heartbleed のような脆弱性はありますが、機密情報の送信に関しては、HTTPS は HTTP よりもはるかに安全と言えます。

TLS 1.0/1.1 についての注記

最近、IETF は、TLS プロトコルのバージョン 1.0/1.1 を公式に非推奨とすることを発表しました。今後数か月間にわたって、ExtraHop は、これらのプロトコル・バージョンの継続使用をエンタープライズ環境全体で注意深く監視し、その使用が段階的に減少しているのか判断し、その状況の把握に努めます。

安全でないプロトコルを実行しているかどうかを判断する方法

非推奨または安全でないプロトコルやプロトコル・バージョンを環境内で実行するまでの道筋はさまざまですが、その状況に気づいてそれを排除する方法は限られています。

安全でないプロトコルの導入については、「デフォルトの横行」がしばしば原因とされます。ネットワーク経由で通信するデバイスやソフトウェアは、時間とともに古くなるおそれのあるデフォルト設定で構成されています。エンタープライズ環境に新しいデバイスやソリューションを導入しても、デフォルト設定をそのまま維持すれば、もはや安全とは見なされないプロトコルを実行することになりかねません。

同様に、クラウドのシステムとワークロードでは、構成テンプレートを使用してプロトコルの使用法を決めますが、時間とともに新しいプロトコルが開発されて古いバージョンが非推奨になると、その構成テンプレートは時代遅れになり、更新が必要になることもあります。新しいワークロードを古いテンプレートで作成すれば、安全でないプロトコルを環境に取り込む可能性もあります。クラウド・ワークロードは一時的で短命な性質を持つことが多いため、安全でないプロトコル使用法の実例を見つけて、システムから排除する方法を習得するのは容易なことではありません。

> 環境内のソフトウェアとハードウェアのインベントリを保持することは、セキュリティ・ハイジーンにとって必須のことです。

それでは、どのように実行すればよいのでしょうか。

特定の時点における手動監査

環境内のソフトウェアとハードウェアのインベントリを保持することは、セキュリティ・ハイジーンにとって必須のことです。この管理策は、CIS のセキュリティ・コントロール・トップ 20 の 1 番目と 2 番目で推奨されています。セキュリティに欠かせない方法であるにもかかわらず、このインベントリの保持は多くの組織にとって課題となっています。このインベントリを収集する方法として、スキャン・ツールの組み合わせを使用した手動監査が挙げられます。使用するスキャン・ツールは、オープン・ソースの無料ツールである Nmap からコストのかかる市販製品まで多岐にわたります。

ネットワークをスキャンして使用中のデバイスやプロトコルを探すことで、特定の時点における有益なスナップショットは得られますが、安全でないプロトコルの新たな発生を防ぐことはできません。さらに、安全でないプロトコルがアクティブに使用されている実例が、特定の時点のスキャンによってすべて見つかるとは限りません。特に、高度にセグメント化された大規模なネットワークの場合、スキャン・ツールは、探しているものを発見できないことがあります。あるセキュリティ・アナリストがかつて述べたように、「ネットワークは暗く、恐怖に満ちている」のです。

それでは、安全でないプロトコルを企業規模のネットワークで見つけるにはどうすればよいのでしょうか。

ネットワークの継続的な監視

ネットワーク・トラフィックの受動的な監視と分析を継続することで、ネットワークで使用されている個々のプロトコルをあらゆる時点で検出できます。これにより、以下に示す 2 つの大きな課題に対処できます。

1. 手動監査では、特定の時点におけるスナップショットしか得られません。通常は年 4 回程度しか実施されない監査の合間に、さまざまな形で安全でないプロトコルが環境に再導入されていることが文書で十分に裏付けられています。

2. 手動監査は多大な時間と労力を必要とし、実際の脅威への対処など、重要性がより高い他のセキュリティ機能の時間を奪っています。

従業員のリモートワークと分散化が増加し、オンプレミスとクラウド・コンポーネントのハイブリッド環境が増加するなか、安全でないプロトコルが環境に取り込まれる方法の数も増加しています。そのため、正確なインベントリを保持することがますます困難になっています。プロトコルの識別と脅威の検知と対応のためにネットワーク・トラフィックを継続的に監視することは、もはや「あるといいもの」ではなく、「なくてはならないもの」となっています。

データ・ソーシングについての注記

ExtraHop のプラットフォームは、プライバシーとセキュリティに最初から配慮して設計されています。当社の製品は、1 日あたり 4 ペタバイトを超えるネットワーク・トラフィックを受動的に監視、分析し、すべてのデバイス間およびアプリケーション間の通信を把握します。次に、匿名化されたメタデータを抽出してクラウドに送信します。クラウドではスケーリングとコンピューティングのリソースを活用し、75 を超えるプロトコルに高度な機械学習を適用して、正確な脅威検知を行います。

一方、ExtraHop Reveal(x)は、クラウドからデータ・センタ、IoT デバイスに至るまで、お客様の環境内にあるすべての通信、デバイス、ワークロードを確認できますが、ExtraHop のセキュリティ研究者が同じことをできるわけではありません。ExtraHop のプラットフォームには、お客様の保護を目的とするセキュリティ/プライバシー・コントロールのレイヤが組み込まれています。当社がお客様のデータに触れるレポートをあまり発行していないことを不思議に思ったことがあるかもしれません。それは、データの持ち主であるお客様以外の人間によるデータ・アクセスを極めて困難にしているからです。私たちはそれがあるべき姿だと固く信じています。

このレポートの統計は大規模なサンプルから集めたものであり、わずかな許容誤差が含まれている場合があります。

ExtraHop のプラットフォームから引き出せるものは、優れた可視性と洞察をお客様へ確実に提供することを目的とした情報です。デバイスのデータを例に挙げましょう。ExtraHop は、匿名化（非特定化）された集計データを使用してデバイス・モデルの目録を作成します。これにより、Reveal(x)センサによって新しいモデルが確認されると、お客様のすべてのシステムはそれを即座に学習します。プライバシーやセキュリティを損なうことなく皆がデータを活用でき、誰もが満足できる仕組みです。

ExtraHop
info@extrahop.com
www.extrahop.com