



今月の脅威: SMB の弱点と、ワームの復活

SMB (Server Message Block) とは

SMB は、コンピュータ間でのファイル共有やネットワーク印刷、各種デバイス間の接続などを可能にするネットワーク プロトコルです。1990 年代初頭から Microsoft 社が採用、実装、投資を続けてきたため、SMB は最も一般的なプロトコルに数えられてきました。Windows 上では簡単な手順でセットアップ・使用でき、さまざまな用途に利用できます。リモート コンピュータ上にあるファイルでも、SMB を介せばローカル ファイルと同様にシームレスにアクセスできます。コンピュータ間で通信するのにサーバすら必要ではありません。直接接続ができるのです。

注目すべき理由

便利な SMB には問題もあります。コンピュータ間通信のプロトコルであるため、必然的にネットワークラバーサル攻撃の標的になるのです。また、ワームをネットワーク内で拡散させ、コンピュータ間でペイロードの感染を広げようとする攻撃も、SME の性質を考えれば当然の成り行きだと言えます。

SMB を標的とした脅威

SMB では 2017 年に、「EternalBlue」と呼ばれる重大な脆弱性が発見されました。影響を受けるコンピュータはマルウェアに感染する危険性があります。その後まもなく WannaCry が登場し、EternalBlue を利用して拡散しました。その翌月には Nyetya も登場したのです。EternalBlue を利用していない脅威 (SamSam、Bad Rabbit、Olympic Destroyer など) も多く登場し、SMB を利用するコンピュータを危険にさらしています。

なぜ問題なのか

SMB は、ローカル ネットワーク内でコンピュータ間ネットワークを構成できる便利なオプションです。ただし、その利便性にはリスクが伴います。ファイル共有目的の接続では認証がほぼ皆無で、接続間の通信は暗号化されていなかったのです。その後に更新されたバージョンではセキュリティが向上しましたが、後方互換性を保つため、危険性が判明した後も旧バージョンは使用され続けました。コンピュータ間における SMB の性質を踏まえると、ハッカーやワームの標的になったのが必然だったと言えます。

その他の参考資料

<https://gblogs.cisco.com/jp/2017/05/wannacry/>

<https://gblogs.cisco.com/jp/2017/06/worldwide-ransomware-variant/>

<https://gblogs.cisco.com/jp/2018/01/talos-samsam-evolution-continues-netting-over/>

<https://gblogs.cisco.com/jp/2017/10/talos-bad-rabbit/>

<https://gblogs.cisco.com/jp/2018/02/talos-olympic-destroyer/>

対策

最も簡単な解決策は SMB の使用を中止することです。SMB を使用し続ける理由はほとんどありません。SMB 接続によりファイルを共有する代わりに、専用のファイル サーバまたはクラウド ベースのサービスを使用してください。ネットワーク プリンタには、SMB 以外のプロトコルを使用するように設定します。現在の環境で SMB を無効にできない場合は、少なくとも SMB1 を無効にしましょう。ネットワークの境界で TCP ポート 445 と 139 をブロックして、SMB 通信が内部ネットワークに限定される状況を確認しましょう。さらに、SMB を介したエンドポイント間通信を不可能にする必要があります。

シスコによる保護

次世代ファイアウォール/次世代侵入防御システム	SMB に対する攻撃で、悪意のある関連トラフィックを検出してブロックします。
エンドポイント向け Advanced Malware Protection (AMP)	継続的な監視と遡及的なレトロスペクティブ セキュリティにより、SMB を狙った脅威を阻止します。
Cisco Stealthwatch®	SMB 共有に対する接続を検知し、そのアクティビティを相互に関連付けて管理者に警告します。
Threat Grid	悪意のあるファイル動作を特定し、シスコのすべてのセキュリティ製品に自動的に通知します。