AsiaNet 98446 （2666）

AV-ComparativesがLSASSセキュリティーを徹底調査－全ての製品が万全とは言えない

【インスブルック（オーストリア）2022年10月24日PR Newswire＝共同通信JB】WindowsのLocal Security Authority Subsystem Service（LSASS）は、サイバー犯罪者が組織のネットワークに標的型攻撃を仕掛ける際の標的の1つである。このブログポストで、われわれは標的型攻撃に対するこのプロセスの重要性について説明する。

攻撃者の観点から見ると、WindowsマシンでのLSASSプロセスは、多くの場合、ドメインユーザーから有用な認証情報（クレデンシャル）を取得し、それらを使用して標的のネットワーク内を横断するための手掛かりとなっている。攻撃者やレッドチームがLSASS（<https://redcanary.com/threat-detection-report/techniques/lsass-memory/> ）プロセスから認証情報を抽出するために使用できるカスタム設計のマルウエアを含め、幾つかの異なる方法がある。

▽LSASS認証情報ダンピングに対する保護

インストールされているセキュリティー製品と適用されるポリシーに応じて、攻撃者がLSASSのアドレスメモリーをダンプして、Windowsユーザーの認証情報を取得するのが容易になったり、困難になったりする（<https://s3cur3th1ssh1t.github.io/Reflective-Dump-Tools/> ）。

一部のセキュリティー製品は特定の強化対策を内蔵し、LSASSプロセスを保護し、認証情報のダンピングを防止する。しかし、一部の組織の環境では、一部のレガシーアプリや適切にプログラムされていないアプリで問題が発生する可能性があるため、こうしたより制限的なポリシーを常に使用できるとは限らない。従って、IT管理者は製品の強化設定をテストして、望ましくない副作用がないかどうかを確認することが推奨される。

さらに、ブルーチームは、インストールされているセキュリティー製品が特定のコードを使用してLSASSプロセスを攻撃に対して強化したとしても、断固とした攻撃者がLSASSプロセスをダンプする方法を見つけると想定する必要がある。つまり、LSASSプロセスからユーザーの認証情報を抽出できる可能性がある。特定のLSASS強化対策に加えて、セキュリティー製品は、例えば対策モジュールを使って、認証情報のダンプを防ぐことができる。これは、使用されたマルウエアや、マルウエアによって生成されたその他のファイルを検出したり、動作検出を使用して悪意のあるアクションをブロックしたりする可能性がある。時には、セキュリティー製品が攻撃をブロックしないことがあるが、少なくともアラートを生成し、悪意のあるアクションを調査する必要があることをシステム管理者に警告する。

一部のビジネスセキュリティー製品では、デフォルトでLSASS強化対策を有効にしている。Avast Ultimate Business Security、Bitdefender GravityZone Business Security Enterprise、Kaspersky Endpoint Detection and Response Expertがその例である。マイクロソフトは、LSASSプロセスを保護するために特に使用される2つの機能、つまりPPL（<https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection> ）（Protected Process Light）とASR（<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/attack-surface-reduction-rules-reference?view=o365-worldwide#block-credential-stealing-from-the-windows-local-security-authority-subsystem> ）（attack surface reduction）ルールを提供している。PPLはWindows 11では既定で有効になっているが、現在Windows 10では有効になっていない。これはWindows 10と11のProfessional、Enterprise、Educationエディションには搭載されている。 ASRルールは、組織のネットワークでMicrosoft Defenderと組み合わせて使用でき、現在いずれかのOSで事前設定する必要がある（<https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-will-soon-block-windows-password-theft/> ）。

▽セキュリティー製品における認証情報のダンピング防止テスト

LSASS認証情報ダンピングを防止することの重要性を考え、AV-Comparativesは2022年5月に幾つかのビジネスセキュリティー製品を試し、強化対策がLSASSへの攻撃からどの程度保護されているかを調査した。

以下に、それぞれのLSASS強化手段を有効にして、テストで使用された15の攻撃に対して効果的な保護を示した製品（アバスト、Bitdefender、カスペルスキー、マイクロソフト製）の数例を挙げる。

上の表には、次の製品（LSASS保護設定が有効になっている場合）の結果が含まれている。アバスト アルティメット ビジネス セキュリティ、Bitdefender GravityZone Business Security Enterprise、Kaspersky Endpoint Detection and Response Expert、Microsoft Defender for Endpoint

マイクロソフトは当社に対し、LSASS保護機能（PPLおよびASR）を有効にせずに実行したMicrosoft Defender for Endpointの追加テストの結果を公開するように要請した。これは、上記の攻撃が他のマイクロソフトのセキュリティー機能によって検出されるかどうかを判断するために行われた。各テストケースについて、AV-Comparativesは、セキュリティー製品による検出またはアクティブなアラートの場合に、攻撃がLSASSに関するMITRE ATT&CK戦術と手法に正しく起因するものであるかどうかを確認した。セキュリティー製品によって攻撃が防止された場合、AV-Comparativesは、脅威に関するどの情報が管理コンソールに提供されているかを確認した。このテストの方法論とその他の詳細は、PDF（<https://www.av-comparatives.org/wp-content/uploads/2022/09/avc_sp_lsass_ms_2022.pdf> ）を参照。追加情報については、マイクロソフトのブログ投稿（<https://www.microsoft.com/security/blog/2022/10/05/detecting-and-preventing-lsa> ）を参照。

E-mail: media@av-comparatives.org

Phone: +43 720115542

Contact: Peter Stelzhammer

Photo -

<https://mma.prnewswire.com/media/1927734/AV_Comparatives_LSASS_Table_Infographic.jpg>

Logo - <https://mma.prnewswire.com/media/1867361/AVC_Logo.jpg>

ソース：AV-Comparatives