AV-Comparatives testet LSASS Credential-Dumping Security auf Herz und Nieren – es gibt Schatten

Der Local Security Authority Subsystem Service (LSASS) ist eines der Ziele von Cyberkriminellen, wenn sie gezielte Angriffe auf das Netzwerk starten.

AV-Comparatives Tests der LSASS Protection Features für Enterprise Security-Produkte

INNSBRUCK, TIROL, ÖSTERREICH, October 23, 2022 /EINPresswire.com/ -- Aus der Sicht eines Angreifers ist der LSASS-Prozess auf einem Windows-Rechner oft der Schlüssel, um an nützliche Anmeldeinformationen von Domänenbenutzern zu gelangen und diese zu nutzen und durchquert damit systematisch Anwendungen und Geräte im Netzwerk (Lateral Movement). Es gibt verschiedene Methoden, einschließlich speziell entwickelter Malware, die von Angreifern und Red Teams verwendet werden können, um Anmeldeinformationen aus dem LSASS Prozess zu extrahieren.

Schutz vor LSASS Credential Dumping
Je nach installiertem Security-Produkt und angewendeter Richtlinie kann es für einen Angreifer einfacher oder schwieriger sein, über das Dumping des Adressenspeichers von LSASS an die Anmeldedaten der Nutzer zu gelangen.

Einige Security-Produkte enthalten spezielle Härtungsmaßnahmen zum Schutz des LSASS-Prozesses und zur Verhinderung von Credential Dumping. Allerdings ist es in manchen Unternehmensumgebungen nicht immer möglich, diese restriktiveren Richtlinien zu verwenden, da sie Probleme mit einigen älteren oder schlecht programmierten Anwendungen verursachen können. Daher ist es für IT-Administratoren ratsam, die Härtungseinstellungen eines Produkts zu testen, um festzustellen, ob sie unerwünschte Nebeneffekte haben.

Darüber hinaus sollten Blue Teams immer davon ausgehen, dass entschlossene Angreifer einen Weg finden werden, den LSASS-Prozess auszuschalten, selbst wenn die installierten

Sicherheitsprodukte einen speziellen Code verwenden, um den LSASS-Prozess gegen Angriffe zu härten. Das heißt, dass sie immer noch in der Lage sein könnten, Benutzerdaten aus dem LSASS-Prozess zu extrahieren. Zusätzlich zu den spezifischen LSASS-Härtungsmaßnahmen können Security-Produkte das Credential Dumping z.B. mit Hilfe des Antivirus-Moduls verhindern; dieses kann die verwendete Malware oder andere von der Malware erstellte Dateien erkennen oder Verhaltenserkennung einsetzen, um die bösartigen Aktionen zu blockieren. In einigen Fällen blockiert die Antivirus-Software den Angriff zwar nicht, gibt aber zumindest eine Warnung aus und weist den Systemadministrator darauf hin, dass die böswilligen Aktionen untersucht werden sollten.

Test Case	LSASS Attack Method	Avast	Bitdefender	Kaspersky	Microsoft
01	Mimikatz with Process Herpaderping	✓	✓	✓	✓
02	Native APIs DLL	✓	✓	✓	✓
03	Silent Process Exit	✓	✓	✓	✓
04	Alternative API Snapshot Function	✓	✓	✓	✓
05	MalSecLogon	✓	✓	✓	✓
06	Dump LSASS	✓	✓	✓	✓
07	Duplicate Dump	✓	✓	✓	✓
08	PowerShell Mimikatz	✓	✓	✓	✓
09	Invoke Mimikatz (PoshC2)	✓	✓	✓	✓
10	SafetyDump	✓	✓	✓	✓
11	RunPE Snapshot (PoshC2)	✓	✓	✓	✓
12	Unhook (Metasploit Framework)	✓	✓	✓	✓
13	Reflective DLL (Metasploit Framework)	✓	✓	✓	✓
14	Invoke Mimikatz (PowerShell Empire)	✓	✓	✓	✓
15	Invoke-PPL Dump (PowerShell Empire)	✓	✓	✓	✓
	Protection Rate	**100%**	**100%**	**100%**	**100%**

Key: ✓ = attack prevented, user credentials could not be read

AV-Comparatives Tests der LSASS Protection Features für Enterprise Security-Produkte - MITRE ATT&CK-Taktiken und -Techniken

Logo AV-Comparatives

Bei einiger Antivirus-Software für Unternehmen sind die LSASS-Härtungsmaßnahmen standardmäßig aktiviert. Beispiele hierfür sind Avast Ultimate Business Security, Bitdefender GravityZone Business Security Enterprise und Kaspersky Endpoint Detection and Response Expert. Microsoft bietet außerdem zwei Funktionen, die speziell zum Schutz des LSASS-Verfahrens dienen, nämlich PPL (Protected Process Light) und ASR (Attack Surface Reduction) Regeln. PPL ist ab Windows 11 standardmäßig aktiviert (aktuell nicht in Windows 10) und es ist in den Varianten Professional, Enterprise und Education von Windows 10/11 enthalten. Die ASR-Regeln können in Unternehmensnetzwerken in Verbindung mit Microsoft Defender verwendet werden und müssen aktuell auf beiden Betriebssystemen proaktiv konfiguriert werden.

Test des Schutzes vor Credential-Dumping in Security-Produkten

Angesichts der Wichtigkeit, LSASS Credential Dumping zu verhindern, testete AV-Comparatives im Mai 2022 einige Security-Produkte für Unternehmen, um festzustellen, wie gut ihre Härtungsmaßnahmen vor Angriffen auf LSASS schützen.

Nachfolgend finden Sie einige Beispiele für Produkte (von Avast, Bitdefender, Kaspersky und Microsoft), die einen wirksamen Schutz gegen die 15 in unserem Test verwendeten Angriffe bieten, wenn die jeweiligen LSASS-Härtungsmaßnahmen aktiviert sind.

> Angesichts der Wichtigkeit, LSASS Credential Dumping zu verhindern, hat AV-Comparatives untersucht, wie gut Härtungsmaßnahmen in Security-Produkten vor Angriffen auf LSASS schützen."
>
> *Peter Stelzhammer, co-founder, AV-Comparatives*

Die obige Tabelle enthält Ergebnisse für die folgenden Produkte (mit aktivierten LSASS-Schutzeinstellungen): Avast Ultimate Business Security, Bitdefender GravityZone Business Security Enterprise, Kaspersky Endpoint Detection and Response Expert und Microsoft Defender for Endpoint.

Microsoft bat uns, die Ergebnisse eines zusätzlichen Tests von Microsoft Defender for Endpoint zu veröffentlichen, den AV-Comparatives ohne aktivierte LSASS-Schutzfunktionen (PPL und ASR) durchgeführt haben. Damit wollt AV-C herausfinden, ob die oben genannten Angriffe auch von anderen Microsoft-Sicherheitsfunktionen erkannt werden würden. Für jeden Testfall hat das Labor überprüft, ob der Angriff korrekt den MITRE ATT&CK-Taktiken und -Techniken in Bezug auf LSASS zugeordnet werden konnte, wenn das Sicherheitsprodukt einen Angriff erkannte oder aktiv warnte. In den Fällen, in denen der Angriff durch das Sicherheitsprodukt verhindert wurde, wurde überprüft, welche Informationen über die Bedrohung in der Verwaltungskonsole bereitgestellt wurden. Die Methodik und weitere Details zu diesem Test finden Sie in diesem PDF.

Für weitere Informationen lesen Sie bitte auch diesen Blogeintrag von Microsoft.

Peter Stelzhammer
AV-Comparatives
+43 720 115542
media@av-comparatives.org
Visit us on social media:
Facebook
Twitter
LinkedIn