Mint Secure

Ransomware Emulation Report

LockBit Ransomware Attack

DRAFT

Example Customer
Attn. Maximus Demoman
Demo Street 1
A-4711 Example

Mint Secure GmbH
Pappelallee 78/79
10437 Berlin

Berlin, 29. Juli 2022

Report Version: 1.0

Mint Secure

Inhaltsverzeichnis

DRAFT

DRAFT

1 Document Control

1.1 Team

Kontakt	Details	Rolle
Felix Thümmler		Pentester

1.2 List of Changes

Version	Beschreibung	Datum
1.0	Final Report	21.09.2025
0.1	Draft	20.09.2025

DRAFT

2 High-Level Summary

2.1 Übersicht

Im Rahmen der Ransomware Emulation haben wir einen Angriff durch den Thread Actor LockBit Simuliert, um die Effizienz Ihres Blue Team testen und Potentiale für die Verbesserungen Ihrer Verteidigung zu identifizieren. Das High-Level-Ergebnis der Ransomware Emulation hat gezeigt, dass Sie bereits gut auf den Angriff reagiert haben, es aber zu lange gedauert hat, bis auf den Angriff reagiert wurde.

2.2 Empfehlungen

Um die Sicherheit Ihrer IT-Infrastruktur zu erhöhen empfehlen wir folgende Maßnahmen:

Schnellere Bearbeitung gemeldeter Infektionen Es wurde ein Alert im SIEM vom Blue Team erst nach 2 Tagen bearbeitet. Dies könnte im Zweifel genug Zeit sein, damit Angreifer sich in der Infrastruktur ausbreiten, Daten Exfiltrieren und Schaden anrichten.

Sofortige Isolierung infizierter Systeme Nach dem Eingang des Alarms im SIEM wurde das infizierte Systems nicht direkt isoliert. Stattdessen wurde zunächst die Infektion auf dem Zielsystem verifiziert, bevor das System vom Firmennetz getrennt wurde. Dies könnte eine Kompromitierung des zum Überprüfen des Systems eingesetzten Accounts zur Folge haben.

Wir hoffen, dass diese Empfehlungen dazu beitragen, die Sicherheitslage Ihres Systems zu stärken und potenzielle Risiken zu minimieren. Gerne stehen wir Ihnen für weitere Beratung und Unterstützung zur Verfügung.

DRAFT

2.3 Engagement Timeline

Nachfolgender Tabelle können Sie die im Rahmen der Ransomware Emulation durchgeführten Aktionen auf dem infizierten System sowie die Reaktionen des Blue Teams entnehmen. In der Spalte ATT&CK wird jeweils auf weiterführende Informationen zu der genutzten Angriffsmethode verlinkt. Die MITRE ATT&CK Matrix ist ein weltweit anerkanntes Referenzmodell, das Angriffsstrategien von Cyberkriminellen in standardisierter Form abbildet und damit eine klare, nachvollziehbare Grundlage für Risikoeinschätzung und strategische Sicherheitsentscheidungen bietet.

Datum	ATT&CK	Aktion
20.09.2025 - 15:43	*T1204.002*	Ausführung der Malware (chrome-setup.exe)
20.09.2025 - 15:43	*T1204.002*	Malware lädt bösartige jli.dll nach
20.09.2025 - 15:44	*T1547.001*	Persistenz wird erreicht, durch das hinterlegen der Dateien %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\VGAuthService.lnk und C:\ProgramData\VGAuthService\VGAuthService.dll

Datum	ATT&CK	Aktion
20.09.2025 - 15:45	*T1082*	Host enumeration mit Powershell wird durchgeführt
20.09.2025 - 15:50	*T1082*	Werkzeug Seatbelt.exe für weitere Analyse des infizierten Systems wird nachgeladen
20.09.2025 - 15:50		Windows Defender erkennt Seatbelt.exe und ein Alarm im SIEM System wird generiert
20.09.2025 - 16:03	*T1486*	Verschüsselungskomponente wird abgelegt unter C: \ProgramData\VGAuthService\zzz.exe
20.09.2025 - 16:05	*T1486*	Verschlüsselung von Testdateien erfolgreich
22.09.2025 - 10:03		Admin meldet sich per RDP an dem infizierten System an
22.09.2025 - 10:37		System wird vom Blue Team isoliert und forensisch untersucht
23.09.2025 - 12:13		System wird vom Blue Team neu aufgesetzt

DRAFT

3 Ransomware Emulation - Methoden

Die Ransomware Emulation wurde durchgeführt, um die Reaktion des Blue Teams des Auftraggebers zu bewerten. Die folgenden Methoden wurden angewendet, um potenzielle Verbesserungen in der Reaktion auf einen Angriff zu identifizieren:

1. **Infizierung** Auf einem von dem Kunden bereitgestellten System wurde eine für dieses Scenario von uns bereitgestellte Malware zur ausführung gebracht. Dies simuliert eine erfolgreiche Phishing Kampagne.

2. **Persistenz** Durch das Platzieren von LNK und DLL Dateien wurde eine Persistenz auf dem infizierten System erreicht. Dies ermöglicht, dass Angreifende auch nach einem Neustart noch Zugang zu dem Zielsystem haben.

3. **Initiale Analyse des infizierten Systems** Auf dem Infizierten System wurden Informationen über den infizierten Account sowie seine Berechtigungen in der Active Directory Umgebung gesammelt. Hierzu wurden ausschließlich PowerShell Befehle verwendet, die auf dem System bereits zur Verfügung standen.

4. **Tiefergreifende Analyse des infizierten Systems** Es wurde eine Komponente nachgeladen und zur Ausführung gebracht, die eine detalliertere Analyse des infizierten Systems ermöglicht.

5. **Nachladen von Verschüsselungskomponente** Es wurde eine Komponente nachgeladen und zur Anwendung gebracht, welche Dateien auf dem Zielsystem verschlüsselt.

Die Kombination dieser Methoden ermöglichte eine umfassende Bewertung der Identifizierungseffizienz, der Reaktionszeit sowie die Wirksamkeit der ergriffenen Maßnahmen des Auftraggebers. Die identifizierten Verbesserungspotentiale wurden dokumentiert und bewertet, um konkrete Empfehlungen für die Verbesserung der Sicherheitslage zu liefern.

DRAFT

4 Disclaimer

Die im Bericht ausgesprochenen Empfehlungen und Maßnahmen wurden nach bestem Wissen und Gewissen erstellt, jedoch müssen sie vor der Umsetzung auf ihre betriebliche Umsetzbarkeit geprüft werden. Es wird darauf hingewiesen, dass wir nicht für Störungen oder etwaige negative Auswirkungen haftbar gemacht werden können, die sich aus der Implementierung der vorgeschlagenen Maßnahmen ergeben könnten. Es obliegt der Verantwortung des Unternehmens, angemessene Prüfungen durchzuführen und Entscheidungen zu treffen, die im Einklang mit den betrieblichen Anforderungen stehen.

DRAFT

A Anlagen

Die Anlagen-Sektion dieses Berichts umfasst eine umfassende Darstellung öffentlich verfügbarer Informationen sowie ergänzende Hinweise, die im Rahmen der Ransomware Emulation erfasst wurden.

DRAFT