Sicherheitsstrategien in Zeiten von Access-as-a-Service und Supply Chain Compromise

Dr. Carsten Willems
CEO
VMRay

Robby Zeitfuchs
Malware und Threat Intelligence Analyst CERT-BPOL
Bundespolizei

Platzierung von Schadsoftware

Platzierung von Schadsoftware

Platzierung von Schadsoftware

Platzierung von Schadsoftware

Platzierung von Schadsoftware

Definitionen

Access-as-a-Service

„Geschäftsmodell”, bei dem Unternehmen Cyberfähigkeiten bereitstellen, um Dritten **Zugang für offensive Cyberoperationen** zu ermöglichen.

Supply Chain Compromise

Manipulation eines Produkts oder Dienstes innerhalb der Lieferkette, um **Zugang zu Endnutzersystemen** zu erhalten.

Zusammenhang zwischen Access-as Service und Supply Chain Compromise

Durch die Kombination können Angreifer eine größere Reichweite und Wirkung erzielen, effizienter agieren und die **Cyberfähigkeiten von Dritten nutzen**.

- Spezialisierung und Arbeitsteilung
- Flexibilität und Ressourcenoptimierung

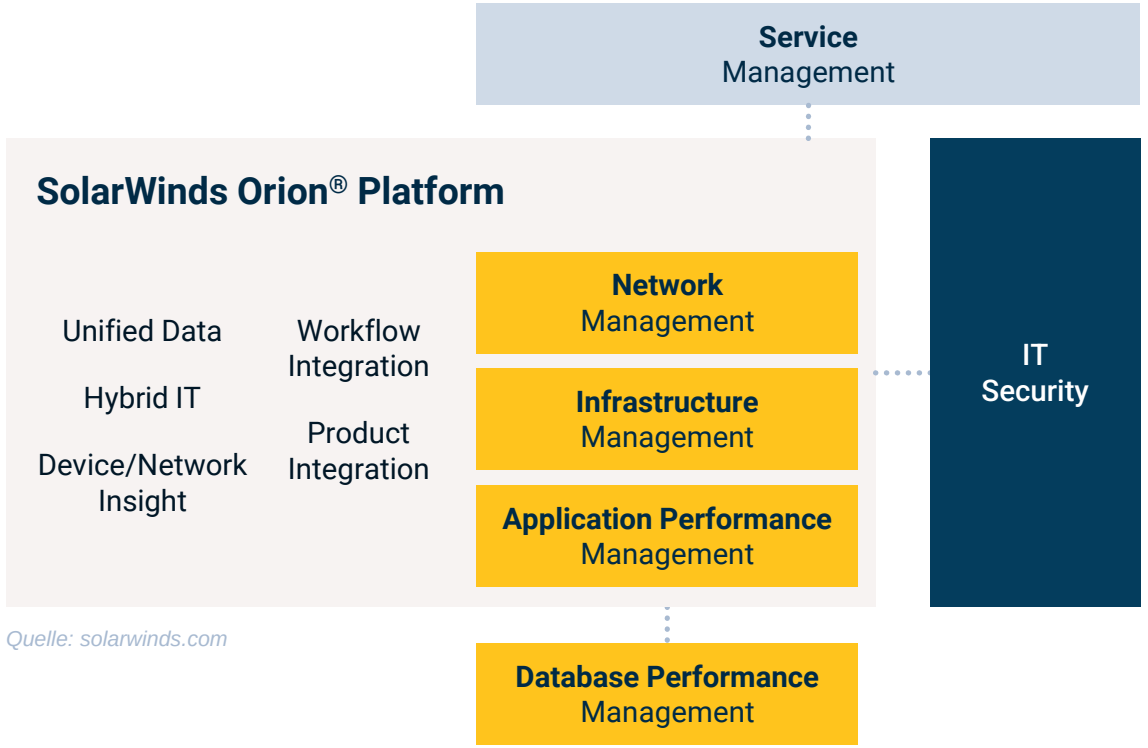
Fallstudie: SolarWinds Orion

Überblick

- 33.000 Kunden der SolarWinds Orion Plattform
- ~18.000 Kunden installierten das **kompromittierte Update** (März – Juni 2020)

Betroffene Organisationen und Behörden

- Mehr als ein Dutzend US-Behörden
- Software- und IT-Sicherheitsunternehmen
- Finanzdienstleister



Quelle: solarwinds.com

SUNBURST Backdoor: Funktionsweise

Integrität und Signatur

- SUNBURST Backdoor ist **digital signiert**
- Quellcode der Backdoor **integriert sich nahtlos** in die Solarwinds Orion Software

Verzögerter Start

- Schadsoftware wird erst **nach etwa zwei Wochen** aktiv
- Führt **detaillierte Analyse** der infizierten Systeme durch

Kommunikation zum Command-and-Control Server (C2)

- Wird über **dynamisch generierte Subdomain** und einen **DNS-Kanal** initiiert
- Wenn System als **interessant** eingestuft wurde: **HTTP-Kanal** zu beliebigem C2-Server wird aufgebaut
- Wenn System als **uninteressant** eingestuft wurde: Schadsoftware kann über DNS-Kanal deaktiviert werden

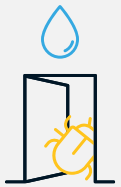
Einblick in die Angriffsmechanismen

VMRAY

Initialer Zugang durch SUNBURST

- Verteilung der SUNBURST Backdoor durch das **kompromittierte SolarWinds Software-Update**

Installation weiterer Schadsoftware



- Die SUNBURST-Backdoor installierte auf infizierten Systemen die **sekundäre Malware TEARDROP**
- Im späteren Verlauf wurde TEARDROP durch **RAINDROP** ersetzt

Cobalt Strike Integration

- TEARDROP und RAINDROP dienten als speziell entwickelte **Loader für die weitverbreitete Schadsoftware Cobalt Strike**

Versteckte Verbindungen

Eine **ausgeklügelte Übergabemethode** erschwerte selbst bei Entdeckung von TEARDROP / RAINDROP die Rückverfolgung zur ursprünglichen SUNBURST-Infektion

Auffälligkeit: Qualitativer Bruch im Angriffsverlauf

Analysen zeigen einen **deutlichen qualitativen Bruch**
zwischen den beiden Malware-Komponenten SUNBURST und TEARDROP

SUNBURST
Hochgradig ausgeklügelte Malware, äußerst unauffällig

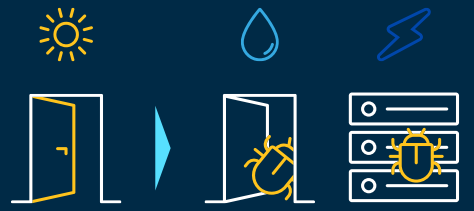
TEARDROP
Relativ einfache Malware, die eine Zuordnung ermöglicht

Cobalt Strike
Standard Malware

Bewertung:

Möglichkeit einer **Access-as-a-Service Operation**

Trennung der **hochentwickelten Initialphase** und der nachfolgenden **Ausnutzungsphase**



Spezialisierter Akteur oder Contractor mit hoher Expertise war für den initialen Einbruch (SUNBURST) verantwortlich

Nutzung des initialen Zugangs und gezielte Nachfolgetätigkeit auf interessanten Zielsystemen mithilfe von TEARDROP

Erkenntnisse zur Optimierung der Reaktionsstrategien

Basierend auf den verfügbaren Informationen über den Vorfall lassen sich mehrere Schlüsselpunkte identifizieren, die während der Untersuchung und Bewältigung des Angriffs **Optimierungspotenzial** aufweisen:

Unzureichende Erkennung der Orion-Kompromittierung

- **US-Justizministerium:**
  Die **Kompromittierung des Orion-Systems** wurde bei der Reaktion auf den Sicherheitsvorfall **nicht erkannt**.
- **IT-Sicherheitsunternehmen Volexity:**
  Erkannte die Orion-Kompromittierung **ebenfalls nicht**.

Erfolgreiche Erkennung einer Kompromittierung

- **IT-Sicherheitsunternehmen FireEye:**
  Konnte eine Kompromittierung des eigenen Netzwerks **erfolgreich identifizieren**.

Vorbeugende Maßnahmen und Abwehrstrategien

Die wichtigsten **Komponenten zum Schutz** vor Supply Chain und Access-as-a-Service Angriffen:

Förderung der **Zusammenarbeit** und des **Informationsaustauschs** zwischen Organisationen

Schneller Austausch von **Bedrohungs-Informationen**

Zero Trust Architektur

Fortgeschrittene **Detektions- und Reaktionstechnologien**

Forensik und **Ursachenanalyse**

Business Continuity und **Disaster Recovery**

Trusted Builds / **Reproducible Builds**

VMRAY

BUNDESPOLIZEI

Vielen Dank!

Q & A