Pressemeldung von SentinelOne vom 22.12.2020:

SentinelOne-Kunden sind vor SolarWinds SUNBURST-Attacke geschützt

SentinelOne-Geräte sind ohne Software-Updates oder Konfigurationsänderungen vor der SUNBURST-Malware geschützt

München – 22. Dezember 2020 – SentinelOne <https://www.sentinelone.com/>, das Unternehmen mit der führenden autonomen Cybersicherheitsplattform, bestätigt heute, dass alle seine Kunden eigenständig vor SUNBURST, der Malware-Variante im Zentrum der SolarWinds-Angriffskampagne, geschützt sind, ohne dass Updates für die SentinelOne XDR-Plattform erforderlich sind. Der SolarWinds SUNBURST-Angriff, der speziell auf die Branchen Finanzen, Behörden, Gesundheitswesen, Bildung und Infrastruktur abzielt, hat seit Beginn der Kampagne im März den gesamten Globus erfasst.

SentinelLabs <https://labs.sentinelone.com/>, die Forschungsabteilung von SentinelOne, erklärt <https://labs.sentinelone.com/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/>, dass Geräte, die SentinelOne-Agenten einsetzen, bereits in einem frühen Stadium von der SUNBURST-Attacke ausgeschlossen waren, noch vor jeglicher Kommunikation mit einem bösartigen C2. Die technische Analyse bestätigt, dass SUNBURST in keiner Umgebung in der Lage war, SentinelOne zu deaktivieren oder zu umgehen.

„Wir überwachen und testen kontinuierlich die neuesten SUNBURST-Varianten, um sicherzustellen, dass unsere Kunden geschützt bleiben", sagt Raj Rajamani, Chief Product Officer bei SentinelOne. „Im Gegensatz zu herkömmlichen Antiviren- und anderen Next-Gen-Produkten schützen die autonome KI und der robuste Manipulationsschutz von SentinelOne unsere Kunden am Ort des Angriffs – ohne reaktive Produktupdates zu benötigen. Unsere Kunden haben die Gewissheit, dass sie mit SentinelOne abgesichert sind."

Seit der Nachricht von der Sicherheitsverletzung bei FireEye, die zur Entdeckung von SUNBURST führte, hat SentinelOne die Kampagne genau verfolgt und Kunden und der Community regelmäßig detaillierte Analysen und technische Anleitungen zur Verfügung gestellt:

● Analyse der aktuellen Indicators of Compromise (IOCs) und der Bedrohungsartefakte

● In-Product-Hunting-Packs, die es Kunden ermöglichen, das Deep Visibility-Hunting-Modul von SentinelOne für retrospektives Threat Hunting mit einem Klick zu nutzen

● Surge-Lizenzberechtigung zur Unterstützung von Kunden und Partnern, die Lösungen und Hilfe benötigen

● Webinar-Briefings, die Führungskräften im Bereich Cybersicherheit dabei helfen, die aktuellen Angriffskampagnen an den Unternehmensvorstand zu kommunizieren

SentinelOne hat es sich zur Aufgabe gemacht, alle Unternehmen bei der Navigation durch die heutige unsichere Situation in der Cybersicherheit zu unterstützen. Um SUNBURST zu beheben, ein Bedrohungsbriefing zu erhalten oder eine Bewertung der eigenen Cybersicherheitslage durchzuführen, kontaktieren Sie bitte SentinelOne <https://www.sentinelone.com/contact/>.

Weitere Informationen finden Sie unter folgenden Links:
● https://www.sentinelone.com/blog/fireeye-breached-taking-action-and-staying-protected/
FireEye/SolarWinds: Taking Action and Staying Protected

● https://labs.sentinelone.com/solarwinds-sunburst-backdoor-inside-the-stealthy-apt-campaign/
SentinelLabs: SolarWinds SUNBURST Backdoor: Inside the APT Campaign

Über SentinelOne
SentinelOne bietet autonomen Endpunktschutz durch einen einzigen Agenten, der Angriffe über

alle wichtigen Vektoren hinweg erfolgreich verhindert, erkennt und darauf reagiert. Die Singularity-Plattform wurde für eine extrem einfache Bedienung entwickelt und spart Kunden Zeit, indem sie KI zur automatischen Beseitigung von Bedrohungen in Echtzeit sowohl für standortbasierte als auch für Cloud-Umgebungen einsetzt. Sie ist die einzige Lösung, die direkt vom Endpunkt aus eine vollständige Transparenz über Netzwerke hinweg bietet. Wenn Sie mehr erfahren möchten, besuchen Sie www.sentinelone.com/de oder folgen Sie uns bei @SentinelOneDE, auf LinkedIn oder Facebook.

Kontakt
Kafka Kommunikation GmbH & Co.
Lukas Reck
Dr. Bastian Hallbauer-Beutler
Kafka Kommunikation
089 74 74 70 580
sentinelone@kafka-kommunikation.de