Anna Mae Boubacar

May 2nd, 2025

Professor Arif

Cyber Security Fundamentals (CS 462)

CDK Global Attack

CDK Global, a software company based in Austin, Texas was founded in 2014 and is currently led by President & CEO Brian P. MacDonald. CDK Global offers a dealer management platform with integrative tools for financing, selling, advertising, and marketing. well-known automotive companies such as Honda, BMW, Nissan, and Subaru. With this company being one of the leading providers for many automotive brands, it is vital that all systems remain functional and always maintain High Availability. Unfortunately, on June 18,2024, CDK Global fell victim to a ransomware attack that *"cost dealerships $1 billion collectively" (Kerner, 2024).* As a Honda customer myself, I remember this day vividly. I had taken my vehicle in for service around this same time the cyberattack occurred. A sales representative informed me that they would need to call me once the systems were up and running. That call of course never came.

The attack against CDK caused an impact that lasted from June 18,2024 to July 4, 2024. This is approximately 2 weeks (336 hours) of system downtime. During the first initial attack it was reported that a ransomware attack was initiated by a group that emerged in 2023 out of Eastern Europe/Russia, this group is known as **BlackSuit** *(Kerner, 2024)***.** The group demanded that CDK pay $10 million in ransom to decrypt and gain access to all legal files that were stolen by **BlackSuit.** As a result, CDK decided to shut down its servers on June 19, 2024 (Day 2). This was not the end for CDK; that same day another cyberattack was initiated against the company.

Blacksuit was very successful in their attack CDK agreed to pay a $25 million ransom on June 22,2024. This is $15 million more than what was demanded four days prior when the first attack occurred. It is not known or reported as to how **BlackSuit** succeeded in this attack against CDK, however they are known to utilize several tools from previous attacks. The group attracts their victims by sending ‘phishing emails that contain malicious attachments and links’ *(Barry, 2024).* The tools used are PowerShell, a task automation program that can be used to identify victims’ IP addresses. PSExec a program with the ability to interact with console applications. Cobalt Strike an attack simulator, and Mimikatz a password infiltrator. Once the tools are launched successfully, **Blacksuit** begins the ‘data exfiltration and deployment of the payload to the victim’s device’ *(Barry, 2024).*

Works Cited

CDK Global. *CDK Global*. https://www.cdkglobal.com/. Accessed 2 May 2025

Lyngaas, Sean. *CDK Global Paid $25 Million Ransom to Resolve BlackSuit Cyberattack*. CyberScoop, 26 June 2024, https://cyberscoop.com/cdk-ransom-blacksuit-25-million/

Kerner, Sean Michael. "The CDK Global Outage: Explaining How It Happened." *TechTarget*, 17 July 2024, https://www.techtarget.com/whatis/feature/The-CDK-Global-outage-Explaining-how-it-happened.

The DFIR Report. "BlackSuit Ransomware." *The DFIR Report*, 26 Aug. 2024,

Barry, Christine. "BlackSuit Ransomware: 8 Years, 6 Names, 1 Cybercrime Syndicate."* Barracuda Networks Blog*, 29 Oct. 2024,