According to Karen Scarfone and Scarfone Cybersecurity (2019), Adobe Flash Player has a vulnerability that could allow for arbitrary code execution. If successfully exploited, this vulnerability could allow the threat actor to execute arbitrary code in the context and privileges of the affected application. For example, the vulnerability is in an email reader; the attacker may execute the commands as the user of the email reader.

Though remote code execution(RCE) has diverse forms, on a basic level, RCE refers to the process of exploiting a vulnerability in the network to execute arbitrary code on a targeted computer or application by the threat actor. In an RCE attack, the threat actor executes malware on the targeted system by exploiting RCE vulnerability. The malware could enable the threat actor to perform malicious transactions such as elevation of privileges, compromising the confidentiality of data by gaining access and stealing the data, and carrying out a total distributed denial of service(DDoS) (N-able Technologies, 2019).

Kovacs Eduard (2018) states that North Korean hackers exploited the vulnerability in Adobe Flash Player in attacks targeted at South Korea. The attack starts with a spam email containing a link to a document stored on safe-storage[.]biz. Once downloaded and opened, the document informs users that an online preview is not available and instructs them to enable editing mode to view the content. If users comply, the Flash vulnerability is exploited, and the Windows command prompt is executed. The associated cmd.exe file is then injected with malicious shellcode that connects to the attacker's domain. A DLL file is then downloaded by the shellcode and executed using the Microsoft Register Server (regsvr32) utility. The legitimate tool is abused in an effort to bypass whitelisting products (Kovacs Eduard, 2018).

References:

Karen Scarfone and Scarfone Cybersecurity (2019) *(No Title)*. Available at: https://searchsecurity.techtarget.com/feature/Introduction-to-email-security-gateways-in-the-enterprise [Accessed: 14 March 2021].

Kovacs Eduard (2018) *North Korea's Flash Player Flaw Now Exploited by Cybercriminals | SecurityWeek.Com*. Available at: https://www.securityweek.com/north-koreas-flash-player-flaw-now-exploited-cybercriminals [Accessed: 19 May 2021].

N-able Technologies, I. (2019) *Remote Code Execution Overview*. Available at: https://www.n-able.com/blog/remote-code-execution [Accessed: 18 May 2021].