Tracing the Lineage of DarkSeoul

By Created by:David Martin

Archived: 2026-04-05 13:42:14 UTC

This paper presents a case study of the April 2013 'DarkSeoul' cyber-attack, which crippled tens of thousands of computers in South Korea's banking and media sectors through the use of destructive malware. While the attack was initially believed to be the work of hacktivists, malware researchers discovered it was actually the outgrowth of a multi-year cyber-espionage campaign waged by the North Korean government. By analyzing the code commonalities and tracing the malware used in a number ofseemingly unrelated incidents, researchers were able to trace the evolution of the intruders' techniques and reach the conclusion that the attacks represented a targeted attack by North Korea. At the same time, the South Korean government reached the sameconclusion through its investigation and publically attributed the attacks to North Korea. In particular, this study will focus on the malware lineage analysis techniques used by researchers and identify critical security controls that were subverted in order to successfully launch the attack. This study will also address critical security controls that could have helped prevent this attack, or significantly mitigated its damage.
