

North Korean Malicious Cyber Activity | CISA

Published: 2020-05-12 · Archived: 2026-04-05 19:48:01 UTC

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Defense (DoD) have identified three malware variants—[COPPERHEDGE](#), [TAINTEDESCRIBE](#), and [PEBBLEDASH](#)—used by the North Korean government. In addition, U.S. Cyber Command has released the three malware samples to the malware aggregation tool and repository, VirusTotal. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA.

CISA encourages users and administrators to review the Malware Analysis Reports for each malware variant listed above, U.S. Cyber Command's [VirusTotal page](#)[↗], and CISA's [North Korean Malicious Cyber Activity page](#) for more information.

Source: <https://www.us-cert.gov/ncas/current-activity/2020/05/12/north-korean-malicious-cyber-activity>