LevelBlue - Open Threat Exchange

By AlienVault

Archived: 2026-04-05 23:12:39 UTC

FileHash-MD5: 3 | **FileHash-SHA1:** 3 | **FileHash-SHA256:** 3 | **YARA:** 1

This Malware Analysis Report (MAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government – commonly known as HARDRAIN. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https[:]//www[.]us-cert.gov /hiddencobra. FBI has high confidence that HIDDEN COBRA actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation. DHS and FBI are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity. This MAR includes malware descriptions related to HIDDEN
