Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:27:29 UTC

Description(VirusTotal) The GandCrab ransomware, which is no longer active, was actively distributed for a little over a year. GandCrab variants caused a great deal of damage worldwide, including in South Korea.

The GandCrab ransomware shares an interesting history with AhnLab. Like many other examples of ransomware, GandCrab searches for any running or pre-installed anti-malware program and when it finds one it interferes with its normal execution and shuts it down. However, when it came to AhnLab, GandCrab went the extra mile, specifically targeting the company and its anti-malware program V3 Lite by mentioning it in its code. It even revealed a vulnerability in the security program and made attempts to delete it entirely.

To effectively respond to and protect against GandCrab attacks, the AhnLab Security Analysis Team analysed GandCrab and all its different versions by thoroughly investigating the distributed code, encryption method, restoration method, and the evasive method it used to avoid behaviour-based detection. Each time a new attack feature targeting AhnLab and V3 was identified, the company’s product developers promptly addressed it to ensure maximum security.

The interesting conflict between AhnLab and the GandCrab ransomware was widely discussed in the IT security industry. However, the details that were revealed at the time were only the tip of the iceberg, with more details being kept private for reasons of confidentiality.
