

## Detailed Analysis Of Sykipot (Smartcard Proxy Variant)

By Created by:Rong Hwa Chong

Archived: 2026-04-05 13:34:50 UTC

On January 2012, AlienVault reported a Sykipot variant with smartcard access capability that has drawn high attention in the security industry. The internals of this malware sample, such as flow of the malware, backdoor capabilities, tricks and techniques, and encryption algorithm are described in this paper. Additionally, its backdoor capabilities are compared with the analysis work of another Sykipot variant published by Symantec. This comparison displays the vast improvements that Sykipot has made. And most importantly, this paper facilitates the security analysts or researchers to response and remediate Sykipot infections, analyze the impact of Sykipot infection, decrypt Sykipot encrypted messages, or even design a fake bot to communicate with the attackers for future research works.

---

Source: <https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-sykipot-smartcard-proxy-variant-33919>