RawPos Malware: Deconstructing an Intruder's Toolkit

Published: 2017-02-16 · Archived: 2026-04-06 00:09:48 UTC

Over the years, Kroll's Cyber investigators have been engaged by our clients in diverse industries to address a wide range of issues, from breach response to traditional digital forensics, and from identification of custom malicious software ("malware") to breach response.

Commonly, network intruders will leverage malware as part of the compromise or network reconnaissance and information gathering phases of their malicious cyber intrusion. Once Kroll's team is engaged, it is common for our investigators to discover fragments of malware remaining in the system's memory ("fileless malware") or written to the disk in scattered locations. What begins as a hunt for circumstantial clues evolves into a deep dig to identify and understand the malware capabilities, so that the knowledge gained from the analysis can be used to answer questions that otherwise would often go unresolved in the course of a traditional forensic and incident response scenario.

In 2016, Kroll's Cyber experts had the opportunity to focus on a collection of malware related to the RawPOS family, and Kroll proceeded to identify numerous tools that the attacker(s) had dropped into the enterprise environment in order to expand their foothold, target specific machines, collect additional information about the compromised environment, and prepare that data for exfiltration.

Through the following Report, Kroll is pleased to share the research conducted on the malware and the intruder's toolkit with the greater information security community.
