Ramsay: A cyber-espionage toolkit tailored for air-gapped networks

Published: 2021-01-08 · Archived: 2026-04-05 14:24:15 UTC

Presented at the VB2020 localhost conference, 30 September - October 2, 2020. ↓ Slides: https://vb2020.vblocalhost.com/upload... → Details: https://vb2020.vblocalhost.com/presen... ✪ PRESENTED BY ✪ • Ignacio Sanmillan (ESET) ✪ ABSTRACT ✪ Air gapping is a network security measure applied on one or more computers to ensure that a given computer network is physically isolated from other networks in a given organization. This measure provides a means to prevent exposure of the subject computer network to the Internet or LAN, usually enforced as a means of securing classified or critical information on military/governmental, financial or industrial control systems networks. Malware targeting air-gapped networks is not rudimentary, as the scarcity of a network connection requires the innovation of alternative methods, leveraging unconventional tactics, techniques and procedures to provide the same capabilities as conventional malware that relies on a network-based communication channel. In March 2020 we discovered a cyber-espionage toolkit we call Ramsay, specifically designed to steal documents and operate within air-gapped networks. In this presentation we will cover the technical aspect of Ramsay, documenting its core capabilities along with the different versions we found. Some of the core capabilities that will be discussed are persistence leveraged via phantom DLL hijacking, covert storage of collected artifacts via API hooking, control mechanisms using a custom file-based protocol, and spreading over the network by infecting files accessible via removable media and network drives leveraging a preprender file-infector. We will also cover artifact and code overlaps found between Ramsay and the DarkHotel APT, and document some OPSEC failures that we observed, which helped us reinforce this connection. ✪ BIO: Ignacio Sanmillan (ESET) ✪ A malware researcher at ESET, Ignacio began his career as a security researcher at Tel Aviv-based cybersecurity firm Intezer, in which he specialized in hunting for new Linux threats and contributed to developing novel code-reuse technologies. He is now part of ESET's Montreal research team investigating current malware trends and APT activity.
