LED-it-GO
Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED

Mordechai Guri, Boris Zadov, Eran Atias,Yuval Elovici
Ben-Gurion University of the Negev
Cyber Security Research Center

gurim@post.bgu.ac.il; borisza@gmail.com; elovici@bgu.ac.il

Video: https://www.youtube.com/watch?v=4vIu8ld68fc

Abstract

In this paper we present a method which allows attackers to covertly leak data from isolated, air-gapped computers. Our method utilizes the hard disk drive (HDD) activity LED which exists in most of today's desktop PCs, laptops and servers. We show that a malware can indirectly control the HDD LED, turning it on and off rapidly (up to 5800 blinks per second) – a rate that exceeds the visual perception capabilities of humans. Sensitive information can be encoded and leaked over the LED signals, which can then be received remotely by different kinds of cameras and light sensors. Compared to other LED methods, our method is unique, because it is also *covert* - the HDD activity LED routinely flickers frequently, and therefore the user may not be suspicious to changes in its activity. We discuss attack scenarios and present the necessary technical background regarding the HDD LED and its hardware control. We also present various data modulation methods and describe the implementation of a user-level malware, that doesn't require a kernel component. During the evaluation, we examine the physical characteristics of different colored HDD LEDs (red, blue, and white) and tested different types of receivers: remote cameras, 'extreme' cameras, security cameras, smartphone cameras, drone cameras, and optical sensors. Finally, we discuss hardware and software countermeasures for such a threat. Our experiment shows that sensitive data can be successfully leaked from air-gapped computers via the HDD LED at a maximum bit rate of 4000 bit/s (bits per second), depending on the type of receiver and its distance from the transmitter. Notably, this speed is 10 times faster than the existing optical covert channels for air-gapped computers. These rates allow fast exfiltration of encryption keys, keystroke logging, and text and binary files.

I. INTRODUCTION

In the modern cyber era, attackers have proven that they can breach many organizations thought to be secured. They employ sophisticated social engineering methods and exploit 0-day vulnerabilities in order to infiltrate the target network, while bypassing defense measures such as intrusion detection and prevention systems (IDS/IPS), firewalls, antivirus programs, and the like. For that reason, when highly sensitive information is involved, so-called *air-gap isolation* is used. In air-gap isolation, a network is kept separate, physically and logically, from public networks such as the Internet. Air-gapped networks are commonly used in military defense systems, critical infrastructure, banks and the financial sector, and others industries [1] [2].

But despite the high degree of isolation, even air-gapped network are not immune to breaches. In recent years it has been shown that even air-gapped networks can become compromised. In order to breach such networks, attackers have used complex attack vectors, such as supply chain attacks, malicious insiders, and social engineering. While the most well-known breach cases are Stuxnet [3] and agent.btz [4], other attacks have also been reported [5] [6] [3] [7] [8].