

# Oops!...I think I scanned a malware

*Ben Nassi*

*Dept. of Software and  
Information Systems Eng.,  
Ben-Gurion University  
of the Negev,  
Be'er-Sheva, Israel  
nassib@post.bgu.ac.il*

*Adi Shamir*

*Computer Science  
department,  
Weizmann Institute  
of Science,  
Rehovot, Israel  
adi.shamir@weizmann.ac.il*

*Yuval Elovici*

*Dept. of Software and  
Information Systems Eng.,  
Ben-Gurion University  
of the Negev,  
Be'er-Sheva, Israel  
elovici@bgu.ac.il*

## Abstract

This article presents a proof-of-concept illustrating the feasibility of creating a covert channel between a C&C server and a malware installed in an organization by exploiting an organization's scanner and using it as a means of interaction. We take advantage of the light sensitivity of a flatbed scanner, using a light source to infiltrate data to an organization. We present an implementation of the method for different purposes (even to trigger a ransomware attack) in various experimental setups using: (1) a laser connected to a stand (2) a laser carried by a drone, and (3) a hijacked smart bulb within the targeted organization from a passing car. In our experiments we were able to infiltrate data using different types of light sources (including infrared light), from a distance of up to 900 meters away from the scanner. We discuss potential counter measures to prevent the attack.

## 1. Introduction

The popularity of computer scanners has increased significantly since they were first introduced, and today they are commonly used by organizations and individuals to scan images, handwriting, as well as printed text to a digital image [33]. Considered the successors of traditional fax input devices, scanners are based on the concept of telephotography, however instead of enabling the transmission of simple text, entire images can be transmitted by a scanner. In recent years, different types of scanners [36] have been introduced, including: sheet-fed scanners, integrated scanners, drum scanners and even portable scanners. Probably the most popular type of scanner is the flatbed scanner, sometimes called a reflective scanner, which works by shining white light onto the scanned object and reading the intensity and color of the light that is reflected from it. Even today, nearly three decades since they were initially introduced, the popularity of flatbed scanners continues, and they are sold as an integrated part of a multi-function printer and as a standalone device. Even in the new era of smartphones, scanners continue to exist because they provide higher resolution output than any other device.

In this article we present a novel method to infiltrate data into an organization. Our method uses light transmitted by an attacker to a flatbed scanner, which is then extracted by a malware installed in the organization. Our method exploits an organization's scanner which serves as a gateway to the organization, in order to establish a covert channel between a malware and an attacker. The attacker controlling the light source can be located far away from the targeted scanner. We present different experimental setups using several types of light sources and varying visibility and distance from the targeted scanner: (1) an external laser installed on a stand positioned far away but within clear sight of the scanner, (2) an external laser connected to a micro-controller installed on a drone, remotely controlled by an attacker to approach the scanner when clear sight to the targeted scanner is available at a very close distance and even by (3) an internal smart bulb within the organization that was hijacked by an Android device located in a passing car.

The motivation to establish a covert channel for data infiltration can vary from the aim of triggering a malware to encrypt critical files (ransomware), a day before an important presentation, to harming an organization by deleting important files.

A persistent attacker eventually finds a way to bypass security measures in order to infect a computer in the organization with a malware. Even isolated networks are not protected against malware infection as was shown in the cases of Stuxnet[32] and the Equation Group APT[19]. The main challenge of the attacker is to find ways to control the malware without being detected. Given a malware/bot installed on organizations' internal network, the proliferation of flatbed scanners and their connection to the network of the organization, countless organizations are vulnerable to our attack; the equipment required to establish the covert channel can be purchased for less than \$20 on eBay.

The contribution of this research is our ability to exploit a legitimate flatbed scanner to establish a covert channel between a C&C server and a malware (previously installed in the organization). This proposed covert channel can evade existing security measures that focus on monitoring suspicious cyber-attack activities using commercial tools such intrusion detection and prevention systems (IDS/IPS), firewalls, and data leakage prevention (DLP) systems.

The paper is structured as follows: section 2 provides an overview of the related work, and section 3 contains the necessary background to understand the scanning process and the vulnerability

exploited by the covert channel. Section 4 describes the general schema to establish the covert channel, the parties involved, the challenges, and the protocol. Sections 5, 6 describe the algorithms of the attacker and the malware. Section 7 presents analysis of the factors involved in the attack. Sections 8-9 present different implementations of the attack: (1) when a clear line of sight to the scanner is available, and (2) when a clear line of sight is not available. In section 11 we discuss counter measures, and in section 12 we provide a summary.

## 2. Related Work

In this section we describe the topic of covert channels and air-gapped networks and present related work in this area. The term covert channel was coined by Lampson [35, 20] who defined it as creating a capability to transfer information between parties that are not supposed to be allowed to communicate by measures that were not designed for communication. Covert channels can be used to circumvent system and network policies, by establishing communication that has not been considered in the design of the computing system for the purpose of communicating under the radar.

There are many ways to establish a covert channel between two parties. In some cases a bidirectional channel is established in which two parties can communicate fully. Other methods include a one way channel whereby only one party can transmit data, and the second party can receive it (broadcasting). The unidirectional covert channels can be used for various purposes including: (1) exfiltration of data from an organization (2) infiltration of data to an infected computer inside the organization's network from a C&C server.

One well-known method of establishing a covert channel is by exploiting acoustical emanations. Previous studies [25, 14, 5] presented a method to establish a bidirectional covert channel between two parties using inaudible sound. The main disadvantage of this method is that sound deteriorates with distance, so the parties must remain a reasonable distance from one another.

Another famous method used to establish a covert channel exploits optical emanations. A research over a decade ago, [21] explored information leakage using devices' LED lights. They classified devices (such as modems, storage devices, CD-ROM drives and others) into three classes based on how informative the device's LED projection is (in term of information that can be gathered by watching it). More recent work [29], showed how to establish a unidirectional channel to exfiltrate data from an organization using a smart bulb. Other research used the same principle to exfiltrate data using a monitor's LED indicator [30].

Less well-known means of establishing a covert channel used temperature as an indicator of the bits. Recent research [22] showed how to establish a thermal channel between different cores in multicore platforms to create a bidirectional channel. Other research [13] used the same principle of thermal channels to exfiltrate data from one computer to another assuming they are positioned side by side. In both cases, the covert channel is based on a process that either heats or cools a device and a sensor to measure the change of temperature. This measurement

is then demodulated to bits. This method primary disadvantage is its low transmission rate which is a result of the time needed to heat and cool the device.

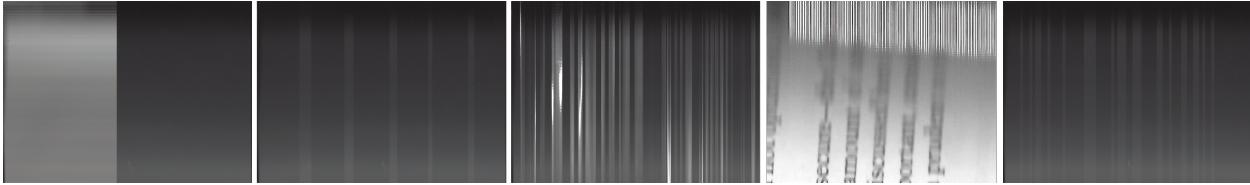
Covert channels have also been investigated in air-gapped networks where they are used for communication with a compromised computer. Air-gapped networks are isolated networks that are not connected to the Internet and don't provide a way to communicate with computers that are outside of the air-gapped network. They are primarily used within closed organizations (e.g. military), in order to prevent confidential data from being transferred outside the network. In this context, covert channels are used in order to bridge the air gap and exfiltrate data from an infected computer connected to the air-gapped network to a device located outside the network, in the outside world. Another research [12] showed how to establish a unidirectional covert channel by transmitting a radio signal from a compromised isolated computer using the display video unit to a mobile phone with a radio receiver. In other work [11] researchers established a unidirectional covert channel by exfiltrating data from an isolated computer to a mobile phone using a software that transmitted electromagnetic signals at cellular frequencies by invoking specific memory-related instructions and utilizing the multi-channel memory architecture to amplify the transmission.

In this article we present a novel and relatively easy to implement scheme to establish a covert channel that uses different light sources (such as laser and infrared beams) to interact with a malware that has been previously deployed in a network. In the rest of the paper we refer to our method in the context of bridging an air-gapped network, although it is not limited to this type of network, and it can be deployed in any other network.

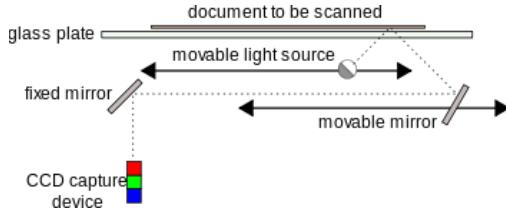
## 3. Sensitivity of Flatbed Scanners

In this section we describe how a flatbed scanner works [38, 23, 33, 36]. A flatbed scanner is made up of a lamp that is passed over a pane (from the bottom) to illuminate the scanner's pane. Using a series of lenses and mirrors, the light is bounced back to a light sensory array (CCD). A lens splits the image into three colors and the associated electrical charge is measured. The brighter the light reflected, the greater the electrical charge. Finally, an ADC device converts the electrical charge to a binary code that represents the document that is located on the pane. The scanning process results in a file in a configured format (such as PDF, PNG, etc.) that is transferred to a computer for storage by a direct physical connection between the scanner and the computer or using a network connection (wired or wireless).

Since the entire scanning process is influenced by the reflected light, interfering with the light that is illuminated on the pane will result in a different electrical charge which will therefore be parsed to a different binary representation of the scanned material. We wanted to examine the effect of external lighting on the scanner (during the scanning process). We conducted an experiment in which we used a flatbed scanner, which was partially open and located on a table. Figure 1a contains the output of a scan that was conducted in a room in which the light was turned on at the beginning of the scan and turned off in the



**Figure 1: Sensitivity of scanners to different light sources (from left to right): (1a) alternating room's light, (1b) alternating flashlight, (1c) alternating infrared laser pen, (1d) alternating laser on a document (1e) alternating screen saver of a monitor**



**Figure 2: Scanning process. Taken from Wikipedia**

middle of the scan. Figure 1b shows an output of a scan that was taken when a flashlight of a mobile phone flickered on the pane. As can be seen, the scanner is sensitive to a change in the room's lighting, even the subtle change caused by the illumination of a mobile phone flashlight results in brighter shades. This light sensitivity causes the scanner to produce different shades in the output (binary representations) when the same experimental setup is used with different lighting conditions. The experiment was repeated with different flatbed scanners, and they were all found to be sensitive to external illumination even when a document was left on the their pane (as can see in figure 1d). In addition, the scanners were sensitive to all of the kinds of lights used (i.e. the color of the light did not impact the results). Another interesting observation is that scanner light sensitivity is not limited to the visible spectrum, but also includes infrared light. Figure 1c contains the output of a scan that was taken while an infrared laser pen was flickered on it. An infrared light, that can't be detected by the human eye causes the same effect on scanner output.

Since the output of the scan is highly influenced by external illumination, it can serve as the infrastructure to deliver messages from an external attacker to an organization that contains a flatbed scanner.

## 4. The Attack

In this section we describe the threat model, the parties involved, the interactions, the assumptions, the challenges, and finally the considerations that led us to select the protocol to transmit data as a light sequence.

### 4.1 Threat Model

Our attack's goal is to use the scanner as a gateway to an organization/home in order to infiltrate data/commands to a malware that has been deployed on a compromised computer/network. We use the scanner as a way to establish a covert channel be-

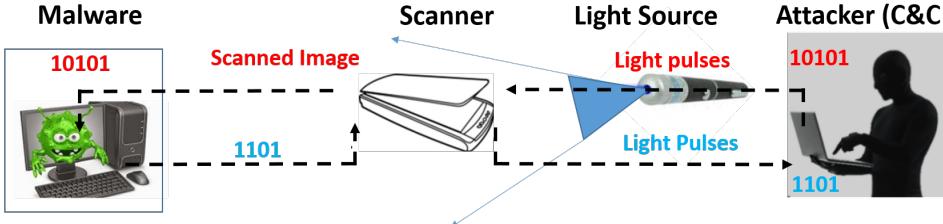
tween an external attacker and a malware installed in an organization. In this attack there are four parties involved:

1. Attacker's computer - This is a C&C server operated by the attacker that controls a light source for the purpose of modulating commands. The attacker's control of the light source may be based on wired or wireless communication.
2. Light Source - The light source can be an external light source that is connected to a micro-controller and belongs to the attacker. The micro-controller modulates a given command (represented in binary code) from the C&C server as a sequence of lights corresponding to the given command (the protocol used will be discussed later). The external light source and the micro-controller can be installed on a stand or even carried by a drone using a wireless connection to the C&C (the attacker's PC). Another option is to use an internal light source, located in the organization which the attacker has managed to control remotely (hijack).
3. Flatbed Scanner - The flatbed scanner is located in the organization and is connected to the organization's network.
4. Compromised Computer within the Organization - Connected to the Organization's Network, This computer has been infected with a malware that can be used to command the scanner to launch a scan and access the output (scanned digital image). The malware extracts the command sent from the C&C and executes it.

The attacker controls a light source that modulates the data as a "light signal" to a partially opened scanner during scanning. The scanning is launched by the malware in order to receive commands at known times (known both by the attacker and the malware). The malware extracts the command from the scan and executes it from the infected computer within the organization. The malware can then use the scanner to send an acknowledgment notification back to the attacker or to exfiltrate data from the organization by modulating the 1/0 bits as lights sent by launching scans.

### 4.2 Assumptions

We assume that the attacker has already successfully managed to infect a computer in an air-gapped network that has direct access to a scanner. Such a malware could be installed via a supply chain attack, by a malicious or unsuspecting insider, via



**Figure 3: Information Flow**

active spear phishing emails, etc. Regarding the location of the scanner, we assume one of the following:

1. A clear line of sight from the outside to the scanner is exists - The scanner is located in a room with external wall. Two scenarios exist: (1) the wall may allow outside light to pass (e.g., curtain wall), or (2) the wall contain a window.
2. A clear line of sight to the scanner is not exists - In this case, a device that produces light and can be hijacked is located in proximity of the scanner.

It is important to note that we do not make any assumptions about the physical distance between the attacker and the organization (the two parties can be located far away from another or nearby). We also do not assume anything regarding the window's state (closed or open).

### 4.3 Challenges and Solutions

1. Physical Obstacles - The presence of obstacles can prevent an attacker from establishing a clear line of sight with the targeted scanner. For example this can occur when the targeted scanner is located on a very high floor that the attacker cannot reach or when the scanner is located in an isolated area of a building, far away from the attacker. Establishing a clear line of sight can be accomplished with the use of a drone equipped with the equipment required to conduct the attack and cellular connection that enables the attacker to send commands remotely; in addition, a powerful laser can be used to transmit the data in cases of long distance between the attacker and the targeted scanner.
2. Synchronization - Since the attacked network can be air-gapped, there may be no way to communicate with a malware in order to schedule scans. This problem can be solved by hardcoding the time of the scan to be fixed (e.g., every day at 23:00) in the code of the malware. Another option is to hardcode the time of first scan in the malware code and include the date of the next scan in the infiltrated data. The attacker can avoid minor time differences between the time that the scan was launched and the time that the attack launched using a camera to identify the beginning of the scan and trigger the attack. The camera may be installed on a drone or in another location within clear sight of the scanner.

3. Identifying a Scan - A problem can occur when an attack was not performed, and the malware must be able to identify these situations and ignore them. This problem can be solved by using a hardcoded prefix in each command as an identifier of the attack.

### 4.4 The Protocol

In order to establish a communication channel using the output of a scan a protocol that exploits a scanner's sensitivity to external illumination must be used. As was shown in section 3, the effect of external illumination on the pane of the scanner results in brighter shades in the output of the scan (compared to the original shade). Given a command/data represented as a sequence of 1 and 0 (the original command is parsed to ASCII and represented in binary) and a light source pointed at the scanner or in proximity to the scanner, we modulate the bits as follows: we turn on the light source to indicate a 1 bit (i.e., illuminating on the pane) We turned off the light source to indicate a 0 bit. We pad the sequence with 1001 at both the beginning and the end of the command/data to be sent. Padding helps address potential problems of distinguishing between an empty packet and data that has not been transmitted). In addition, padding also helps identify the beginning and the end of the signal on from the output of the scanner and it allow the malware to calculate the window size of each bit of the scan (described in section 6).

Figure 4 presents the original image that was scanned from the sequence of 1010...01 without padding using a laser that was controlled by a micro-controller. We found that different experimental setups, such as different distances, result in different shades to indicate a 1/0 bit. Adding padding that contains 1 and 0 bits helps the malware's code to identify the RGB value that associated with each of the bits. It allow the code to extract the values of the shades dynamically rather than making assumptions regarding them (described in section 6).

### 5. Attacker's Algorithm

This section describes the attacker's algorithm. More precisely, we present how the algorithm that is deployed on the micro-controller (and connected to the light source) modulates a given command to attack a scanner according to the protocol discussed in subsection 4.4.



**Figure 4:** Output scans of the signal 1010..01 being transmitted by a laser from different distances (left to right): 3.2, 4.5, 7 meters.

---

**Algorithm 1** Attacker’s Algorithm

---

```

1: procedure ATTACK(command,window)
2:   cmd ← getInBinary(command)
3:   paddedCmd ← applyPadding(cmd)
4:   index ← 0
5:   length ← length(paddedCmd)
6:   while (index < length) do
7:     if (paddedCmd[index] == 1) then project()
8:     else dontProject()
9:     index ← index+1
10:    wait(window)

```

---

Algorithm 1 presents the stages of attack execution. The only parameter that is required to execute the protocol (besides the command itself) is a transmission window. First, the given command is represented as an array of 1/0 in binary (line 2). Then suffix and prefix padding are added to the binary representation as discussed in subsection 4.4 (line 3). Finally, the code is iterated over the array (lines 4-10). The light source is turned on to indicate a 1 bit and turned off the to indicate a 0 bit. The last command of the code is to wait a given period of time before proceeding to iterate. The reason for waiting before proceeding to the next iteration is to ensure that the light source is either opened or closed for the given amount of time that is denoted by the window (rate of a single bit).

The rate of a single bit is primarily influenced by the ability of the scanner to absorb fast switches cleanly (describe in section 7, the ability of the light source to switch between on/off states quickly and the speed of the scanning that adapts the required resolution. The speed of scanning can be measured by the attacker before the attack by performing a scan using the same type of scanner in the attacker’s home/lab, or by reading the scanner’s specifications. Given a scan speed and a sequence of bits (generated from a command), the window parameter can be computed by:

$$window = \frac{\text{Time of scanning}(ms)}{\#bits} \quad (1)$$

## 6. Malware’s Algorithm

This section describes the algorithm of the malware. As discussed in subsection 4.2 the malware is previously installed on one of the organization’s computer. The mal-

ware algorithm should be able to (1) execute a scan at a scheduled time and (2) extract a command from the scanned image. The algorithm’s main challenge is to extract the command in various experimental setups, each of which will result in the same signal being scanned differently. As can be seen in figure 4, the white shades corresponding to the 1 bit deteriorates in each of the images, depending on the distance between the laser and the scanner, and therefore algorithm should be immune to shade’s changes. Algorithm 2 presents the signal extraction without hard-coded colors to identify 1 and 0 bits.

This algorithm should be executed at a scheduled time

---

**Algorithm 2** Malware’s Algorithm

---

```

1: procedure SCANANDEXTRACTCOMMAND()
2:   path ← scan()
3:   image [] [] ← loadToRGB(path)
4:   contrast [] [] ← applyContrast(image)
5:   background ← getDominantColor(contrast)
6:   lineAverage [] ← averageLines(contrast,background)
7:   threshold ← max(lineAverage)/2
8:   stretchedSignal [] ← stretchSignal(lineAverage,threshold)
9:   paddedSignal [] ← extractSignal(stretchedSignal)
10:  signal [] ← removePadding(paddedSignal)
11:  applyCommand(signal)

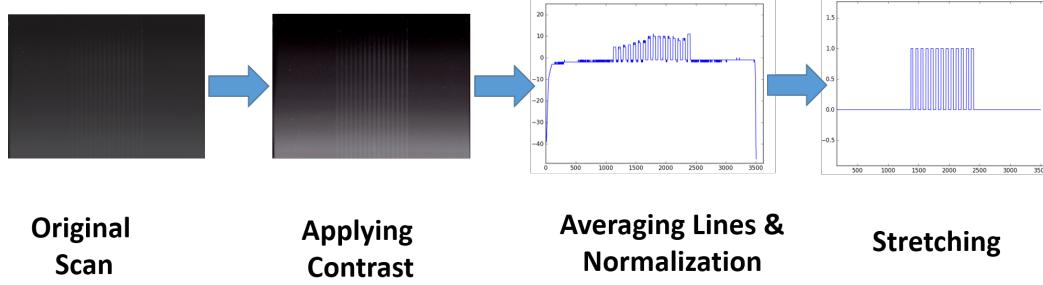
```

---

that is known by the attacker (the attacker can hard-code the first scan date and supply the next date in each attack or hard-code all of dates alternatively). First, the algorithm triggers the scan (line 2) and loads the image to the memory as a two dimensional RGB array(line 3). A contrast function is applied to the image to emphasize the shade of the bits (line 4) and the background color (line 5) in is then extracted (the value with the most appearances in the matrix). A vector of lineAverage is computed (line 6); each index  $i$  in the vector is calculated by averaging the line and normalizing the value according to the background value:

$$\text{lineAverage}[i] = \sum_{col=0}^{\text{columns}} \left( \frac{\text{contrast}[i][col]}{\text{columns}} \right) - \text{background} \quad (2)$$

A stretching is applied to the values of lineAverage (lines 7-8) to produce a new signal, where each value in index  $i$  of the new signal is 1 (if it is larger than the threshold) or 0 (if it is smaller than the threshold). The signal is then extracted by identifying the padding prefix and suffix in the signal that starts and ends the signal, (line 9) and removing the padding from it(line 10). Finally, the



**Figure 5: Signal Extraction**

command is executed (line 11).

The algorithm assumes that the infiltrated packet size is less than half the size of the image. It will ensure that the background will be selected as the 0 bit. The attacker should design the transmission rate of the bits such that it results in a scan that takes less than half of the scanning time (half of the length of the image). Different kind of algorithms can be used to extract the code. We chose this algorithm because it is simple to implement.

Figure 5 presents the signal extracted from the sequence of 101010...101. The positive effect of applying contrast to the image is demonstrated by comparing the image before the contrast to the image after contrast.

## 7. Analysis of the Attack

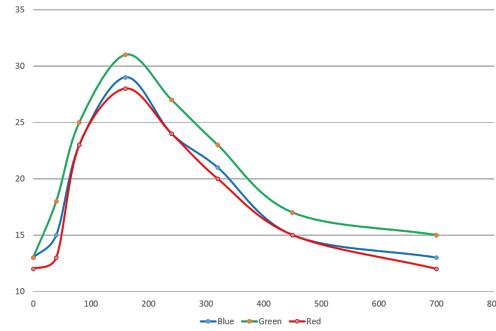
This section presents an analysis of the four main factors in designing the attack: the type of light source to use, the distance between the scanner and the attacker, the rate of transmission, and the time of the attack.

### 7.1 Influence of Light Source

There are two types of light sources that can be used by the attacker to perform the attack: visible and invisible light. As mentioned in section 3, scanners are sensitive to both types (see figure 1). In a case of an organization with a window with an IR filter (e.g., sunlight filters or a curtain wall), a visible light source can be used to attack the scanner. The selection of the specific light is primarily a function of the conditions of the room in which the targeted scanner is located. We prefer to use IR light whenever it is possible since it cannot be detected by the naked eye, making it an ideal covert communication channel.

### 7.2 Influence of Distance

Selecting the distance to attack a scanner using an external source light is highly influenced by the experimental setup (such as line of sight) and the intensity of the used light source. If the attacker has a clear line of sight to the scanner from his location he can use a stand to direct the source light (such as laser) to point to the pane of the scanner and perform the attack. Alternatively, the attacker can install the laser on a drone to minimize the



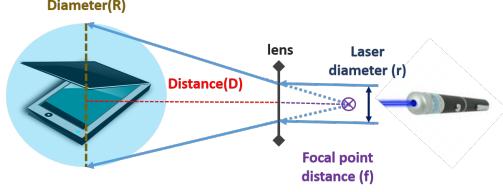
**Figure 6: Difference between 1 and 0 shades of Red, Green, Blue values from different distances. X axes represents the distance in cm between the attacker and scanner. Y axes represents the difference between 1/0 shades.**

distance in order to create a clear line of sight to the pane of the scanner and launch the attack remotely.

There are few issues to be considered. First, there is a trade-off between the stability that is required in order to attack a scanner from a distance of 10 meters away versus 100 meters away; the light source must remain stable in order to reach the scanner and perform the attack. This is extremely crucial when using a drone equipped with a light source to attack a scanner.

Second, since light deteriorates with distance, the attacker need to use a light source that is strong enough to project the light the necessary distance. This need demonstrated in figure4 which shows how the quality of the scanned image is compromised, to the point that it cannot be extracted, when the distance between the attacker and the scanner increases.

Third, another important observation is that the distance of lighting influences also on the diameter of projection on the scanner pane. The projected diameter is decreases when the distance decreases. In our experiments we found that the best way to effect the result of a scan is with a diameter that covers the entire pane of the scanner. Since small distances between a laser and a scanner result in small diameters that is too focused in a specific dot on the pane it results in weak spreadness of the light on the



**Figure 7: Illustration of the focal (f), distance (D), diameter(R). The focal can calculated by equation 6**

pane. Again, the quality of the image is compromised, when the distance between the attacker and the scanner decreases under a threshold.

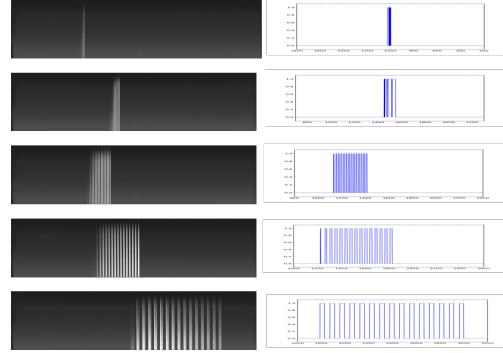
The attacker's goal is to produce a clear scan (i.e maximize the differences between the 1/0 bits) so the malware will extract the signal correctly. The trade-off between the diameter of the projected light and the intensity of the light that is projected is presented on figure 6. The figure presents the differences in the RGB values between the 1/0 shades as a function of the distance of projection. This graph was produced from seven experiments in which we used the same 300mW red laser under the same experimental setups from different distances (0-700cm). We extracted the shades of the 1/0 bits (from each output) and calculated the difference between them. The 1st interval of the graph, (0-40cm), shows a linear (even asymptote) behavior, as in this range the laser did not cover the scanner area. The 2nd interval (40-160cm) shows that increasing the distance increases the intensity of the shades as a result of a diameter optimization. The 3rd interval (160-450cm) shows that increasing the distance damaged the intensity of the laser. The 4th interval (450-700cm) shows linear (even asymptotic) behavior. The optimum distance to attack the scanner using the laser we used is from 160cm as it got the highest difference of RGB values between 1/0 bit. This optimum is achieved when achieving the minimal diameter to cover the pane. We computed the difference of the RGB shades as a function of the distance using Lagrange interpolation (equations 3,4,5).

$$\begin{aligned} Red = & -1.29^{15}x^7 + 2.61^{-12}x^6 - 2.03^{-09}x^5 \\ & + 7.88^{-07}x^4 - 0.0001x^3 + 0.01x^2 - 0.35x + 12 \end{aligned} \quad (3)$$

$$\begin{aligned} Green = & 1.07^{-18}x^7 + 9.08^{-14}x^6 - 1.65^{-10}x^5 \\ & + 1.08^{-07}x^4 - 3.1^{-05}x^3 + 0.003x^2 + 0.03x + 13 \end{aligned} \quad (4)$$

$$\begin{aligned} Blue = & -1.37^{-15}x^7 + 2.7^{-12}x^6 - 2.1^{-9}x^5 \\ & + 8.36^{-7}x^4 - 0.0001x^3 + 0.01x^2 - 0.4x + 13 \end{aligned} \quad (5)$$

One option to focus the projection and maximize the intensity of the light is by using a lens on top of the light source. Figure 7 illustrates the required circle to cover the scanner and the parameters of distance and diameter. The required lens's focal point can be calculated as a function of the distance (D), the laser diameter (r) and the required projection circle (R) to cover the scanner using



**Figure 8: Scans and Extracted signals in different rates (100ms,50ms,25ms,10ms,5ms)**

Transmission Rate	Extracted Signal	Number of Errors
100 ms	101010101010101010101010101	0
50 ms	101010101010101010101010101	0
25 ms	001010101010101010101010101	1
10 ms	111111111111111111111111111111	14
5 ms	100111111111111111111111111111	15

**Table 1: Number of Errors of Extracting the signal 101010101010101010101010101 in different rates of transmission.**

the next formula:

$$focallength = \frac{r * D}{R - r} [\text{meter}] \quad (6)$$

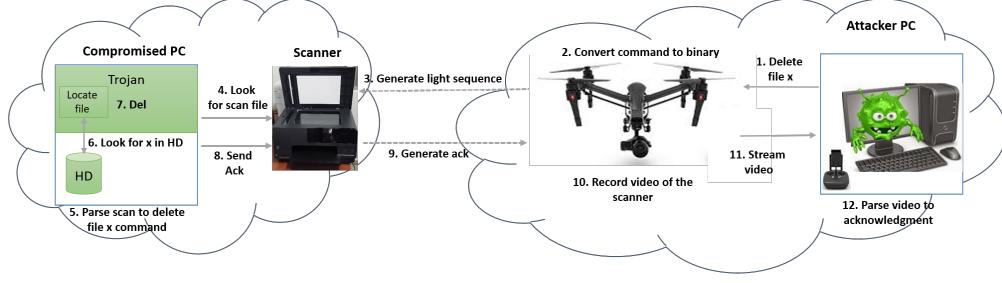
### 7.3 Influence of Transmission Rate

As can be seen in figure 4, from a sequence of two alternating bits we can calculate the window (in terms of corresponding number of lines to a single bit) from the malware's perspective. When using padding, the first two bits are: 10, and the rate of transmission of a single bit can be calculated by identifying the first line of transmission of the 1 bit denoted by *first*, and the first line of transmission of the 0 bit is denoted by *last* to calculate the window as follows:

$$\text{Rate}(\# \text{lines}) = \text{first} - \text{last} \quad (7)$$

By calculating the rate dynamically we can change the rates of transmission in each scan in order to infiltrate more/less data (depending on the action we want the malware to apply) without the need to change the malware. The number of lines (transmission rate) that adapt to infiltrate a single bit are influenced by the speed of the scan and by the rate of transmission. We want to maximize the amount of the data that we are can infiltrate. The limitations from the attacker side on the maximum rate of transmission are influenced by the ability of the attacker's light source to switch its states between the on and off. From the malware side The limitation on the maximum rate of transmission is the ability to identify correctly the bits 1/0 bits to reconstruct the signal.

Figure 8 presents the scanning and the extracted signal of the sequence 1010101010101010101010101 with different transmission rates for a single bit (100ms,50ms,25ms,15ms,10ms,5ms).



**Figure 9: Schema of the attack using external light source.**



**Figure 10: Experimental setup (from left to right): (a) The Inspire 1 equipped with the laser (circled in green) and the Edison SoC, (b) the attacked organization during the attack, a green laser is projecting on a scanner behind a curtain wall in the 3rd floor, (c) the scanner in the office from the inside**

As can be seen from the figure, different transmission rates result in thinner sequence of columns that correspond to a single bit. Table 1 presents the error (number of incorrect bits) of the extracted signal for each of the rates. Using our laser and our scanner, we found that maximum infiltration rate possible to use without any errors is 50 milliseconds. An error correcting code can be integrated to the malware's code to detect and correct the extracted code for rates faster than 50 milliseconds. It is important to note that the speed of scanning can be changed by configuring different resolutions (Dots Per Inch) of the output scan. In the entire set of experiments described in this article we used standard quality of 300 dpi (default quality of the scanner), that lasted around 8 seconds. Higher resolution results in slower scanning and can help the attacker to infiltrate more data.

#### 7.4 Influence of Time

We checked the influence of the hour of the day on the attack. We were able to perform the attack during day and night. Picking the hour to attack is only a consideration of minimizing the amount of people in the organization.

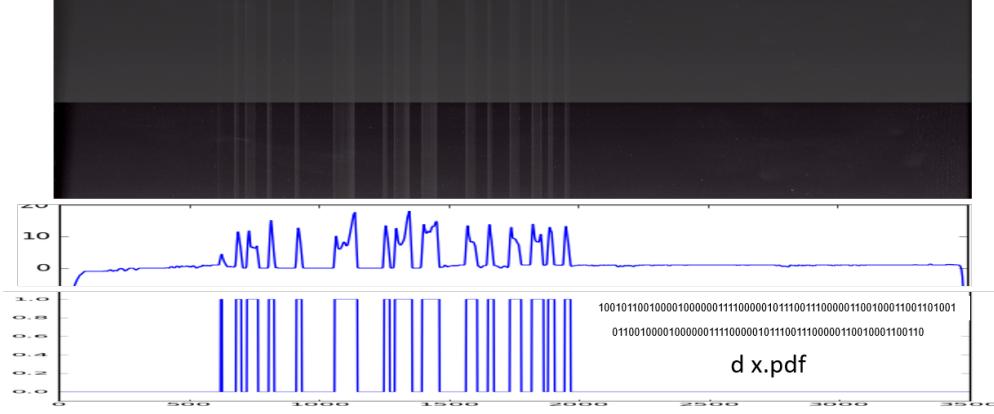
### 8. Infiltration of commands with a clear line of sight to the scanner

The first scenario demonstrates few attacks using an external light source when a clear line of sight to the scanner is available. We implement the first type of attack using an external light source connected to a micro-controller. The micro-controller can be installed on a stand if clear sight to the targeted scanner is available. Another possibility is installing the micro-controller on a drone to improve the sight of the target laser and control the micro-controller remotely using GSM communication from the C&C.

Figure 9 presents the steps of the attack. An attacker's PC generates a sequence of binary signals transferred a micro-controller (phases 1-2). The micro-controller launch the attack by modulating the received signal as light sequence using a connected laser that is directed to a scanner's pane while the scanner is scanning (phase 3). Next, the scan is extracted to a command (phases 4-5), and executed by the APT (phases 6-7). Finally, a message sent from the scanner to the attacker by modulating the bits of the message as scan and emitting visible light pulses from the flatbed (phase 8). The emitted light is captured by a drone equipped with a video recorder (maintaining a line-of-sight with the scanner). Finally, the video is processed by the attacker to extract the message from the malware.

#### 8.1 Experimental Setup

The described attack presents harming an organization, located in the 3rd floor in its building, by deleting an important file. The organization contained HP OfficeJet Pro8610 [16] a multi-function printer with a scanner and a fax connected to the network of the organization located on a table within a room as can be seen in figure (10c). As can be seen in figure 10b, the building constructed from curtain walls that filters the sunlight and IR. So we decided to use a visible green laser that was dismantled from a laser pen (bought from eBay and operates on 600mW). We build an electrical circuit as follows: We took an Intel Edison [17], System on a chip (SoC), and connected it to a battery and the green laser. We installed the code described in section 5 on the Edison. We installed the Edison SoC on top of the Inspire 1 pro (a drone) [8] while the laser was installed on its camera that was positioned on the stabilizer of the drone to maximize the stability during the attack. The drone equipped with the Edison and the laser can be seen in figure 10. The video from the camera of the drone was streamed to an Android application [7] using radio signals. We established a communication channel between the C&C computer and the



**Figure 11:** Extracted Signal delete x.pdf, from top to bottom: (a) The original signal, (b) the signal after contrast, (c) line averaging (c) Stretching unpadding and ASCII representation



**Figure 12:** Left to right: (a) The laser with the stand. (b) The attacked office with the scanner. (c) The IR projector.

Intel Edison SoC using its WiFi interface over a hot-spot that was opened from a mobile phone. The attacker had the ability to (1) launch the attack using the Edison SoC remotely from the C&C and to (2) maneuver the drone using its joystick and watch the streamed video in an Android application.

As for the malware, we implemented the code described in section 6 using a python library Pyinsane [1]. We installed the malware on a computer inside the organization that was connected to its internal network. The malware scanned the network for a scanner (we found the IP of the scanner dynamically) and triggered by the scanner to launch a scan exactly at 23:00.

## 8.2 Results

The attack was recorded and uploaded to a link<sup>1</sup>:1. We flew the drone to stand in front of the scanner in the 3rd floor from a distance of 15 meters and launched the attack after we detected that a scan was launched using the camera of the drone (23:00). We used a transmission rate of 50 milliseconds for each bit and infiltrated the command of "d x.pdf" where d is correlative to delete and x.pdf is the file to delete. Only 7 bytes are required (including the space) to encode this command. We padded the command with 1001 prefix and 1001 suffix (as described in section 4.4. The padding added one more byte results in 8 bytes in total. The infiltration time took 3.2 seconds (64 bits that were transmitted in a rate of 50 milliseconds per bit). This was the entire time that the laser was used. The malware extracted the signal in real-time and sent an acknowledgment message by triggering another scan after the command was executed. Figure 11 presents the output of each of the stages of the signal

extraction process as was described in section 6.<sup>1</sup>

We repeated the experiment with much powerful laser (10W) that we installed on a dedicated stand from 900 meters from the targeted scanner (that was located in another room) as presented in figures 12a and 12b. We successfully infiltrated data to the scanner and received its acknowledgment using a telescopic camera. Finally, we repeated the same experiment with invisible light using an IR projector (the IR projector can be seen in figure 12c) from a distance of 20 meters and successfully infiltrated the command "erase file xxx.doc". As discussed in section 4, we could even increase the distance using a lens and a stronger laser.

## 9. Infiltration of commands with no clear line of sight to the scanner

The second scenario demonstrates an attack using an internal light source (within the organization) when a clear line of sight to the scanner is not available and external light source can not be used. We implement the second type of attack using an internal IoT device that produces light either directly or indirectly. More precisely, the attacker performs a functional attack (as was described in [29]) on an IoT device inside an organization to produce the light sequence of a given command while the malware launches a scan and extracts the command from it.

IoT devices have become increasingly popular in the recent years and are widely sold. They can be controlled from vari-

<sup>1</sup><https://youtu.be/vy8dKaHNB-A>

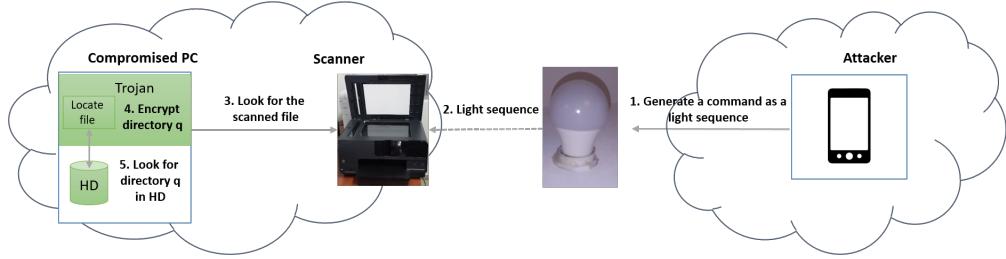


Figure 13: Schema of the attack using hijacked internal light source



Figure 14: Left to right: (a) Passing car (circled in green) attacks a scanner located in an office (circled in red), (b) The attacked office from the inside, the bulb (circled in yellow), the scanner (circled in blue) that is hidden behind a close curtain, (c) The hijacked smart bulb (MagicBlue)

ous types of controllers (e.g., smartphones, PCs, smart remotes) using different protocols such as WiFi, infrared, Zigbee[37], Bluetooth, and Bluetooth Low Energy (BLE) [34]. In practice, many commercial devices do not implement strong authentication mechanisms (some don't even implement any authentication mechanisms at all) exposing them to different kinds of attacks, including replay attacks (hijacking the device). For example, a television news report recently prompted viewers' Amazon Echo devices to order unwanted dollhouses [9]. The same thing happened to Google's assistant as a result of Google Home's Super Bowl ad[4]. Commercial Smart Bulbs were also found vulnerable to attacks on their bridge using external ZigBee signal [28, 24] and many BLE devices (even smart locks) were founded to be vulnerable to different kind of attacks, including hijacking[18, 27, 15].

In this scenario the attacker exploits : (1) the unauthenticated protocols of IoT devices, and (2) the ability to produce a light from a specific IoT device which its light reflections can be received by the scanner. The attacker hijacks an IoT device with that produces lights in order to modulate the command to the scanner. The attacker can either attack an IoT device whose purpose is to illuminate (e.g., a smart bulb) or attack an IoT device in which illumination is a side effect, (e.g., a smart TV).

This attack scenario is preferable to the previously one described in the article, because there is no clear line of sight between the attacker and the scanner. However, in this scenario the attacker did manage to hijack an IoT device, located close enough to the scanner, in such a way that the produced lights from the IoT device effects the scanner's output. In this scenario the attacker attacks the scanner indirectly by attacking the IoT device.

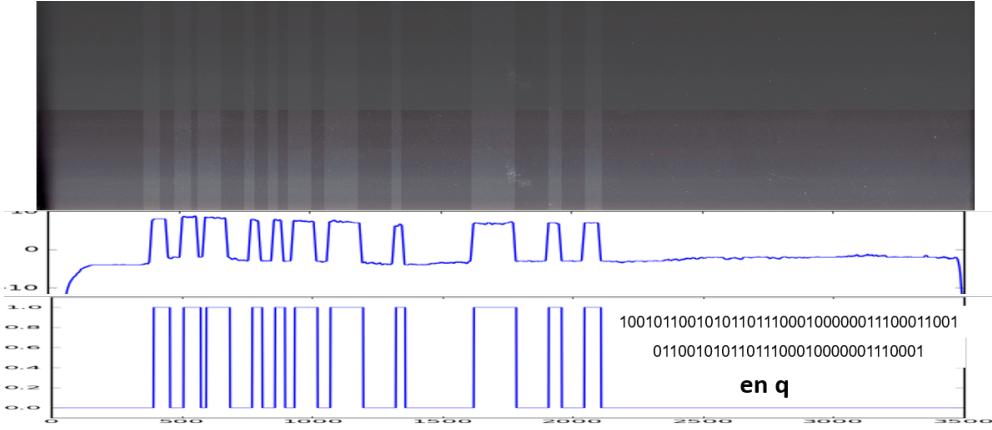
Figure 13 outlines the attack. First, the attacker hijacks an IoT device and use it to modulate the command as a sequence of lights. The scanner, which was scheduled to launch a scan by

the malware, scans the reflections of the lights produced by the IoT device to an image and the malware extracts the signal from the scan and executes the command. In the current scenario the acknowledgment from the malware side is not part of the protocol (there is no clear line of sight to the scanner).

## 9.1 Experimental Setup

In our experiment we decided to attack a commercial smart bulb in order to infiltrate the required command to the organization via the scanner. Smart bulbs have been shown to be vulnerable to hijacking in various researches [31, 10, 6, 28]. The ability to control (hijack) a smart bulb inside an organization enables the attacker to exploit the known "on" and "off" commands to modulate the light sequence of a command.

We attacked the same organization mentioned in the previous scenario. However, this time we attacked a different room which contained a scanner and a Magic Blue UU E27 Bulb[3] (presented in figure 14c). The scanner, as can be seen in figure 14b, is hidden behind a closed window and a clear line of sight does not exist. The MagicBlue smart bulb exposes BLE API for control. The BLE protocol has become quite popular for IoT devices, and it provides the ability to control from short distances (less than 100 meters). This bulb does not contain any type of authentication mechanism (as was found by [31]). We reverse engineered by triggering commands using its official application [26] and sniffing the BLE traffic that was transmitted from the Android device. We used Wireshark [2] to parse the PCAP file that was produced by the Android and found the commands:



**Figure 15:** Extracted Signal encrypt dir q, from top to bottom: (a) The original signal, (b) the signal after contrast, (c) line averaging (c) Stretching unpadding and ASCII representation

BLE Command	Functionality
0xCC2333	ON
0xCC2433	OFF
0x56FFFFFF00F0AA	Max Brightness
0x5600000000F0AA	Min Brightness

It is important to note that many kind of commercial smart bulbs are vulnerable to hijacking as was shown in the past [31, 28, 10, 6, 24]. The contribution of this attack is that it shows that despite the fact that smart bulb does not contain any important information and might cause a minor damage if a external attacker has manage to hijack it (as opposed smart locks for example), the bulb can cause big damage when used as a mediator in attacks.

In our study we performed the attack in different experimental setups and different rates to produce the required light sequence in order to infiltrate the data. We found that even the slightest change of brightness (5%) produced by the bulb can be detected by the scanner (e.g., changing the brightness of a bulb from 100% to 95%). Also, as described in section 7 we found that lights that produced by the bulb during a daylight were detected by the scanner. Also, we found that we are able switch the bulb states in frequencies less than 25 milliseconds, rates that will not be detected by the human eye, but as was shown in section 4.4, we would have to add the malware's code an error correcting code for this purpose.

## 9.2 Results

Finally, we present the attack in the context of triggering a ransomware (with hardcoded key) given a directory, from a passing car (figure 14a) on a scanner located in the 3rd floor (figure 14b) behind a closed curtain with no line of sight using hijacked smart bulb, in the evening. The driver held a Samsung Galaxy S4 while driving in order to perform the attack from, a dedicated application that we wrote and installed on the Galaxy. The application scans for a MagicBlue smart bulb and connects to it. After connection, the application modulates a given command as light sequence using a series of "on" (1 bit) and "off" (0 bit) signals sent from over a BLE channel. The attack was

recorded using a video camera and can be seen on the link<sup>2</sup>. <sup>2</sup> We used the same malware as described in 6, so the selected transmission rate was picked to be 100 milliseconds (that does not require any error correcting code). We infiltrated 40 bits (four bytes of data plus one byte of padding). The entire attack lasted for four seconds. The malware as explained in section 6 is independent of the number of bits as well as the rate of transmission and does not require any error correcting code. The signal "en q" that is correlated to "encrypt directory q" was extracted by the malware in real-time and presented in figure 15.

## 10. Limitations

Our method is effective with a partially open scanner or an open scanner. In our experiments we were unable to infiltrate a signal when the scanner was completely closed since light can not be projected on the pane when the scanner is closed. Since most of the organizations don't require closing scanners after each scan, and it is not out the question that an organization's employees could get paid by an attacker to intentionally leave a scanner open, opportunities exist to use our method.

## 11. Counter Measures

Since manufacturers don't consider scanners a mean to infiltrate data, they offer Ethernet and WiFi connectivity and drivers in order to support remote and direct scanning. As was shown in section ??, limiting the line of sight to scanners by positioning them behind a wall doesn't provide a solution for the threat (shown in section ??).

Various solutions can be used to automatically prevent/detect the threat, rather than relying on the awareness of individuals within an organization to close the scanner after completing a scan including: (1) disconnecting the scanner from the network. Many scanners support scanning directly to a disk on key device using USB interface. Doing so, prevents an attacker

<sup>2</sup><https://youtu.be/jHb9v0qviGA>

from establishing the covert channel in this paper. This might be considered an extreme solution, since it also limits printing and faxing remotely, if the scanner is part of an all-in-one device. (2) Extending the scanner’s remote protocol to support two levels of authentication.

However, we believe that a proxy based solution will prevent the attacker from establishing such a covert channel without the need to apply extreme changes. The scanner will be connected by a wire directly (e.g., using a USB interface) to a computer (proxy) within the organization’s network instead of being connected to the network. The proxy will provide an API. When a scanning request is received, the computer initiates a scan and processes the output in a classifier in order to detect malicious scan. If the scanning was classified as benign, the output is returned to the entity that requested the scan. Otherwise, the scan will be stored on the proxy for analysis of the IT team. The classifier’s logic for detection of suspicious scans can be based on (1) robotic detection or anomaly detection by analyzing the characteristic of the scan (e.g. unusual hour of the day), or (2) raw data analysis (the scan output) using a machine learning model that was trained on malicious/benign scans.

## 12. Summary

In this research we showed how a simple organization’s scanner can be used in order to establish a covert channel between an outside attacker and a malware installed on one of the computers in the organization. We showed that even physical obstacles (e.g., high distance, high floor, and hidden scanner) do not prevent an attacker from establishing the described covert channel. We hope our study will increase the awareness to the threat and will result in secured protocols for scanning that will prevent an attacker from establishing such a covert channel specifically in the era of Internet of Things.

## 13. References

- [1] Pyinsane. <https://github.com/jflesch/pyinsane>.
- [2] Wireshark. <https://www.wireshark.org/>.
- [3] BEST, G. Magic blue. [http://www.gearbest.com/smart-light-bulb/pp\\_230349.html](http://www.gearbest.com/smart-light-bulb/pp_230349.html).
- [4] DAILYMAIL. Google-home-s-super-bowl-ad-sends-viewers-devices-crazy. <http://www.dailymail.co.uk/news/article-4196830/Google-Home-s-Super-Bowl-ad-sends-viewers-devices-crazy.html>.
- [5] DESHOTELS, L. Inaudible sound as a covert channel in mobile devices. In *8th USENIX Workshop on Offensive Technologies (WOOT 14)* (San Diego, CA, Aug. 2014), USENIX Association.
- [6] DICOLA, T. Reverse engineering a bluetooth low energy light bulb. <https://learn.adafruit.com/reverse-engineering-a-bluetooth-low-energy-light-bulb/overview>.
- [7] DJI. Dj go. <https://play.google.com/store/apps/details?id=dji.pilot&hl=en>.
- [8] DJI. Inspire1. <http://www.dji.com/inspire-1-pro-and-raw/>.
- [9] FOXNEWS. Alexa. <http://www.foxnews.com/tech/2017/01/06/tv-news-report-prompts-viewers-amazon-echo-devices-to-order-unwanted-dollhouses.html>.
- [10] GUILLIER, F. Reverse engineering of a ble bulb. <http://www.guillier.org/blog/2015/04/reverse-engineering-of-a-ble-bulb/>.
- [11] GURI, M., KACHLON, A., HASSON, O., KEDMA, G., MIRSKY, Y., AND ELOVICI, Y. Gsmem: Data exfiltration from air-gapped computers over gsm frequencies. In *24th USENIX Security Symposium (USENIX Security 15)* (Washington, D.C., Aug. 2015), USENIX Association, pp. 849–864.
- [12] GURI, M., KEDMA, G., KACHLON, A., AND ELOVICI, Y. Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on* (2014), IEEE, pp. 58–67.
- [13] GURI, M., MONITZ, M., MIRSKI, Y., AND ELOVICI, Y. Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations. In *2015 IEEE 28th Computer Security Foundations Symposium* (July 2015), pp. 276–289.
- [14] HANSPACH, M., AND GOETZ, M. On covert acoustical mesh networks in air. *JCM* 8, 11 (2013), 758–767.
- [15] HO, G., LEUNG, D., MISHRA, P., HOSSEINI, A., SONG, D., AND WAGNER, D. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security* (New York, NY, USA, 2016), ASIA CCS ’16, ACM, pp. 461–472.
- [16] HP. Hp. <http://support.hp.com/us-en/product/hp-officejet-pro-8610-e-all-in-one-printer-series/5367603>.
- [17] INTEL. Edison. <https://software.intel.com/en-us/iot/hardware/edison>.
- [18] JASEK. Gattacking bluetooth smart devices. <https://www.blackhat.com/docs/us-16/materials/us-16-Jasek-GATTacking-Bluetooth-Smart-Devices-Introducing-a-New-BLE-Proxy-Tool-wp.pdf>.
- [19] LABS, K. Equation group. [http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation\\_group\\_questions\\_and\\_answers.pdf](http://25zbkz3k00wn2tp5092n6di7b5k.wpengine.netdna-cdn.com/files/2015/02/Equation_group_questions_and_answers.pdf).
- [20] LAMPSON, B. A note on the confinement problem. ACM.
- [21] LOUGHRY, J., AND UMPRESS, D. A. Information leakage from optical emanations. *ACM Trans. Inf. Syst. Secur.* 5, 3 (Aug. 2002), 262–289.
- [22] MASTI, R. J., RAI, D., RANGANATHAN, A., MÜLLER, C., THIELE, L., AND CAPKUN, S. Thermal covert channels on multi-core platforms. In *24th USENIX Security Symposium (USENIX Security 15)* (Washington, D.C., Aug. 2015), USENIX Association, pp. 865–880.
- [23] MERCER, E. How does a flatbed scanner work? aqa computing comp2. [HowDoesaFlatbedScannerWork?](#)
- [24] MORGNER, P., MATTEJAT, S., AND BENENSON, Z. All your bulbs are belong to us: Investigating the current state of security in connected lighting systems. *CoRR abs/1608.03732* (2016).
- [25] O’MALLEY, S. J., AND CHOO, K.-K. R. Bridging the air gap: Inaudible data exfiltration by insiders. In *20th Americas Conference on Information Systems (AMCIS 2014)* (2014), pp. 7–10.
- [26] PLAY, G. Magicblue application. <https://play.google.com/store/apps/details?id=com.Zengge.BluetoothLighthDark&hl=en>.
- [27] RAMSEY, A. R. . B. Picking bluetooth low energy locks from a quarter mile away. <https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEFCON-24-Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks-UPDATED.pdf>.
- [28] RONEN, E., O’FLYNN, C., SHAMIR, A., AND WEINGARTEN, A. Iot goes nuclear: Creating a zigbee chain reaction. *IACR Cryptology ePrint Archive 2016* (2016), 1047.

- [29] RONEN, E., AND SHAMIR, A. Extended functionality attacks on iot devices: The case of smart lights. In *2016 IEEE European Symposium on Security and Privacy (EuroS P)* (March 2016), pp. 3–12.
- [30] SEPETNITSKY, V., GURI, M., AND ELOVICI, Y. Exfiltration of information from air-gapped machines using monitor's led indicator. In *Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference* (Washington, DC, USA, 2014), JISIC '14, IEEE Computer Society, pp. 264–267.
- [31] SHAKED, U. Reverse engineering a bluetooth lightbulb.  
<https://medium.com/@urish/reverse-engineering-a-bluetooth-lightbulb-56580fcb7546#.6u6m1cydr>.
- [32] SYMANTEC. Stuxnet. [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/stuxnet\\_0\\_5\\_the\\_missing\\_link.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf).
- [33] TECHWALLA. History of computer scanner.  
<https://www.techwalla.com/articles/the-history-of-computer-scanners>.
- [34] WIKIPEDIA. Ble. [https://en.wikipedia.org/wiki/Bluetooth\\_low\\_energy](https://en.wikipedia.org/wiki/Bluetooth_low_energy).
- [35] WIKIPEDIA. Covert channel.  
[https://en.wikipedia.org/wiki/Covert\\_channel](https://en.wikipedia.org/wiki/Covert_channel).
- [36] WIKIPEDIA. Image scanner.  
[https://en.wikipedia.org/wiki/Image\\_scanner](https://en.wikipedia.org/wiki/Image_scanner).
- [37] WIKIPEDIA. Zigbee.  
<https://en.wikipedia.org/wiki/ZigBee>.
- [38] YOUTUBE. How does a flatbed scanner work? aqa computing comp2.  
<https://www.youtube.com/watch?v=shnYIjG20i4>.