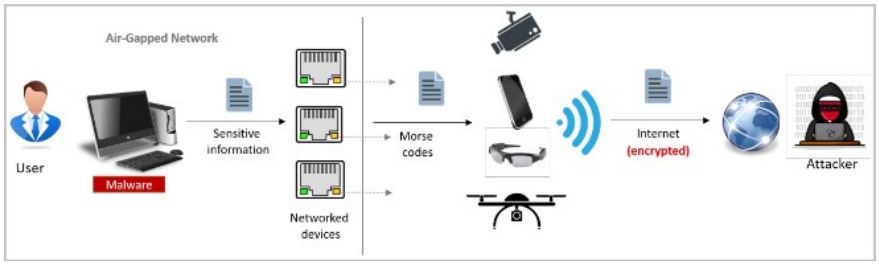
Computers isolated from the internet can still be hacked via the network card LED

Israeli researcher Mordechai Guri has discovered a new method for filtering data from air-gapped computers.

Israeli researcher Mordechai Guri has discovered a new method to steal data from air-gapped computers. The method, called ETHERLED, turns the blinking LED lights on network cards into Morse code that can be decoded by hackers .

To capture the signals, a hacker needs a camera with a direct line of sight to the LEDs on the network card of an air-gapped computer. These can be translated into binary data to steal information.



Air-gapped computers are computer systems that are typically installed in highly sensitive environments (e.g. critical infrastructure, weapons control units, etc.). For security reasons, these computers are isolated from the public internet.

However, they still have network cards to connect to the internal network. Mordechai Guri discovered that if hackers can install special malware that replaces the video card driver with software that modifies the LED color and flashing frequency, they can send encrypted data to the outside.

The ETHERLED method can be used on other peripherals and hardware that use LEDs as status indicators such as routers, NAS, printers, scanners, etc.

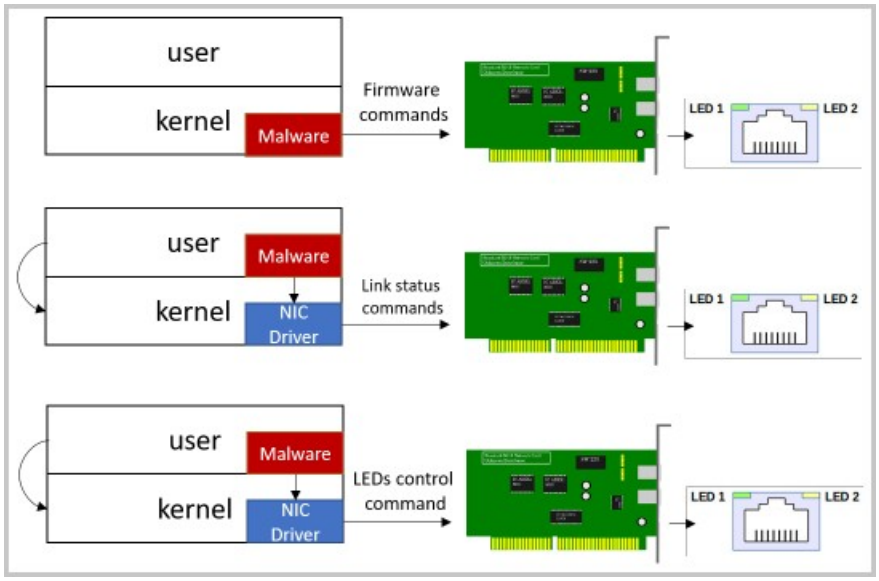
Compared to previously disclosed data exfiltration methods that monitor keyboard and modem LEDs, ETHERLED is a more covert and less likely to raise suspicions.

Details about ETHERLED

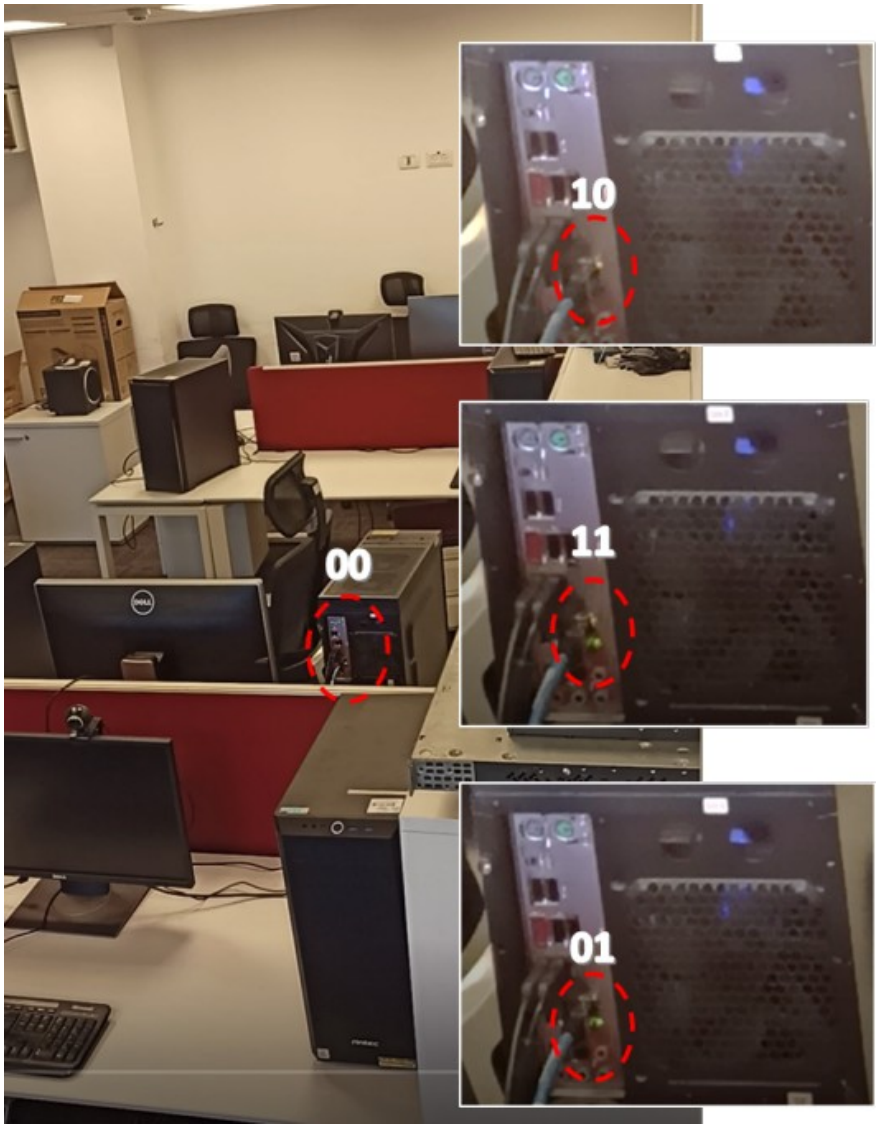
The attack begins by installing malware on the target computer that contains modified firmware for the network card. This allows the hacker to control the frequency, duration, and color of the LED flashes.

```
lan951x_rd_reg(handle, LED_GPIO_CFG, &val);
for (int i=0; i < 3; i++) {
        if (led_arr[i] == MODE_ON) {
                val &= ~(gp_mask[i] & (GP_ALLCTL|GP_ALLDAT));
                val |= (gp_mask[i] & GP_ALLDIR);
        }
        if (led_arr[i] == MODE_OFF) {
                val &= ~(gp_mask[i] & GP_ALLCTL);
                val |= (gp_mask[i] & (GP_ALLDIR|GP_ALLDAT));
        }
        if (led_arr[i] == MODE_STATUS) {
                val &= ~(gp_mask[i] & (GP_ALLDIR|GP_ALLDAT));
                val |= (gp_mask[i] & GP_ALLCTL);
        }
}
lan951x_wr_reg(handle, LED_GPIO_CFG, val);
```

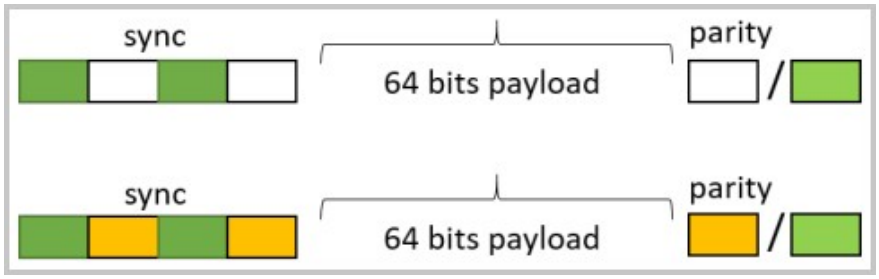
Additionally, malware can directly attack the drive containing the network interface controller (NIC) to change the connection state or adjust the LEDs needed to generate the signal.



The researcher discovered that the malicious driver can exploit hardware functionality to control network connection speed and enable or disable the Ethernet interface, resulting in flickering and color-changing lights.



Guri's tests showed that each data frame begins with a 1010 sequence, to mark the start of the packet, followed by a 64-bit payload.



For filtering data through single status LEDs, Morse code dots and dashes lasting from 100ms to 300ms are generated, separated by indicator off intervals ranging from 100ms to 700ms.

Morse code bitrate can be increased up to 10 times (10m dots, 30m dashes and 10-70ms spacing) using driver/firmware attack method.

To capture signals from a distance, hackers can use anything from smartphone cameras (up to 30 meters), drones (up to 50 meters), hacked webcams (10 meters), hacked surveillance cameras (30 meters), and telescopes or cameras with telephoto or super zoom lenses (over 100 meters).

TABLE VIII
TIME IT TAKES TO LEAK VARIOUS TYPES OF INFORMATION

Information	Size	Single color	Two colors
Passwords	100 bits	1.5 min	0.7 min
Bitcoin private key	256 bits	4.2 min	2.1 min
PIN codes	64 bits	1 min	0.5 min
RSA encryption keys	4096 bits	~30 min	~60 min
Keylogging	5 bit/key	N/A	2 sec / key

TABLE IX
TIME IT TAKES TO LEAK VARIOUS TYPES OF INFORMATION (DRIVER/FIRMWARE)

Information	Size	Single color	Two colors
Passwords	100 bits	2 sec	1 sec
Bitcoin private key	256 bits	5 sec	2.5 sec
PIN codes	64 bits	1.2 sec	0.5 sec
RSA encryption keys	4096 bits	1.4 min	42 sec
Text files	1KB	~2.7 min	~ 1.4 min

The time it takes to leak secrets like passwords via ETHERLED ranges from 1 second to 1.5 minutes, depending on the attack method used. For complex data like Bitcoin wallet keys, it takes 2.5 seconds to 4.2 minutes, and 42 seconds to 1 hour with a 4096-bit RSA key.