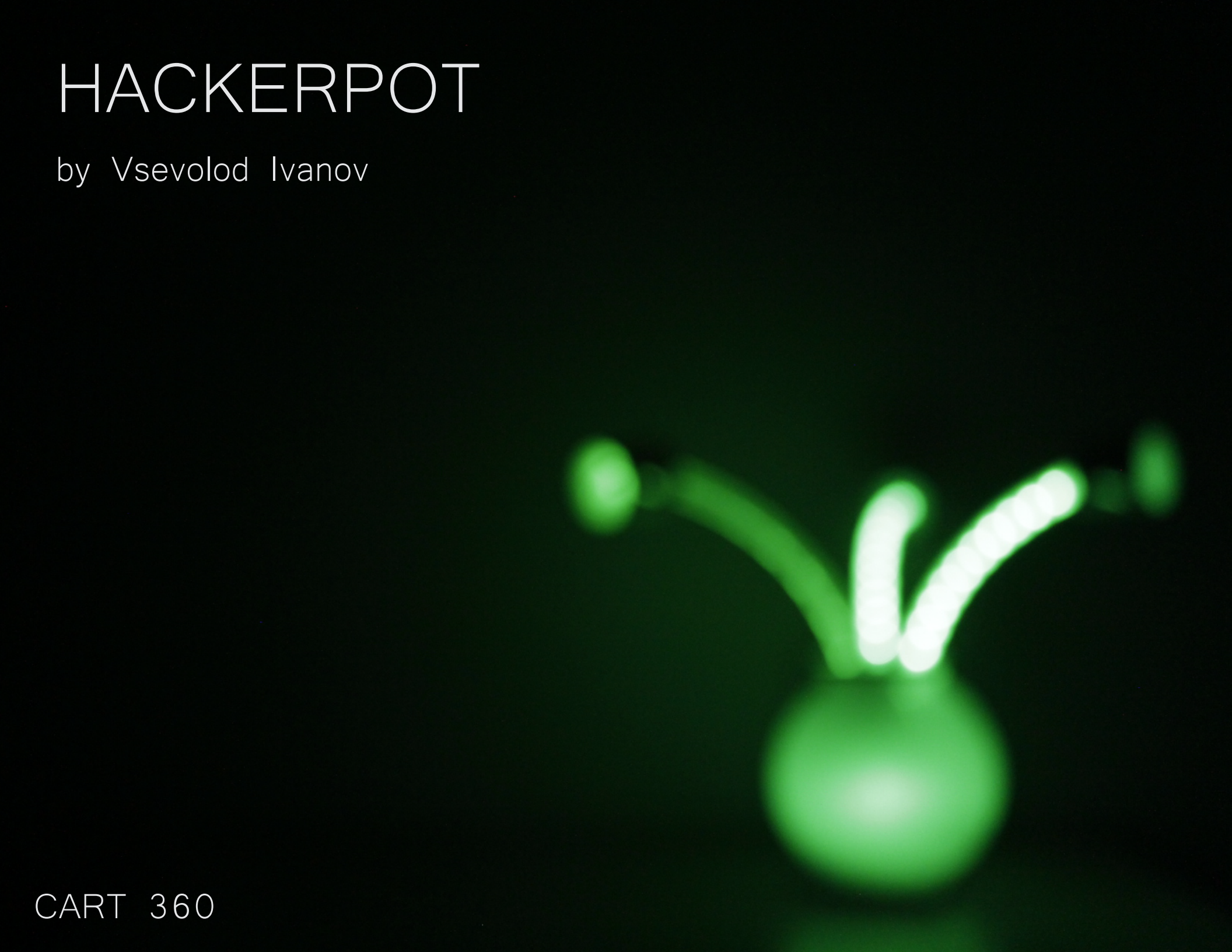
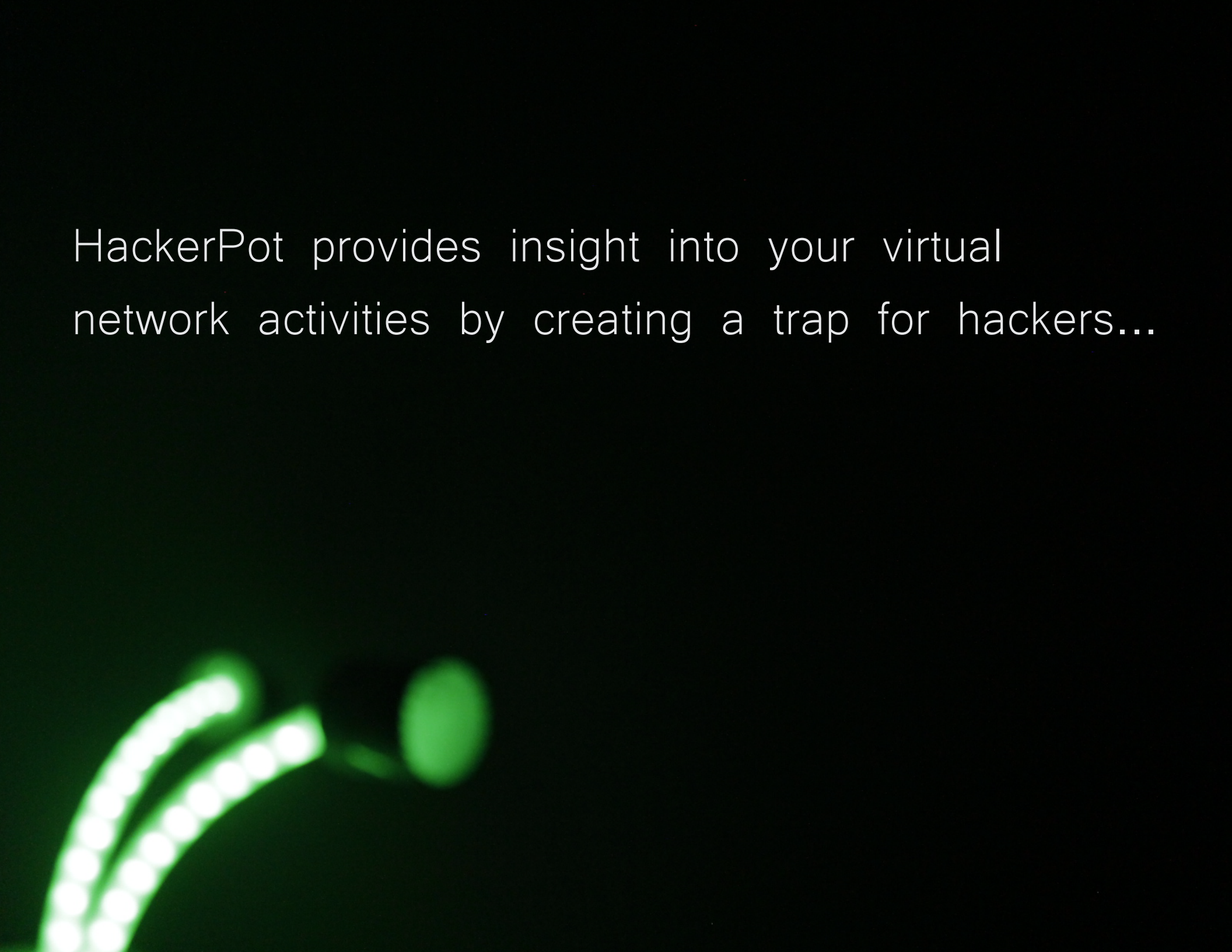
HACKERPOT

by Vsevolod Ivanov

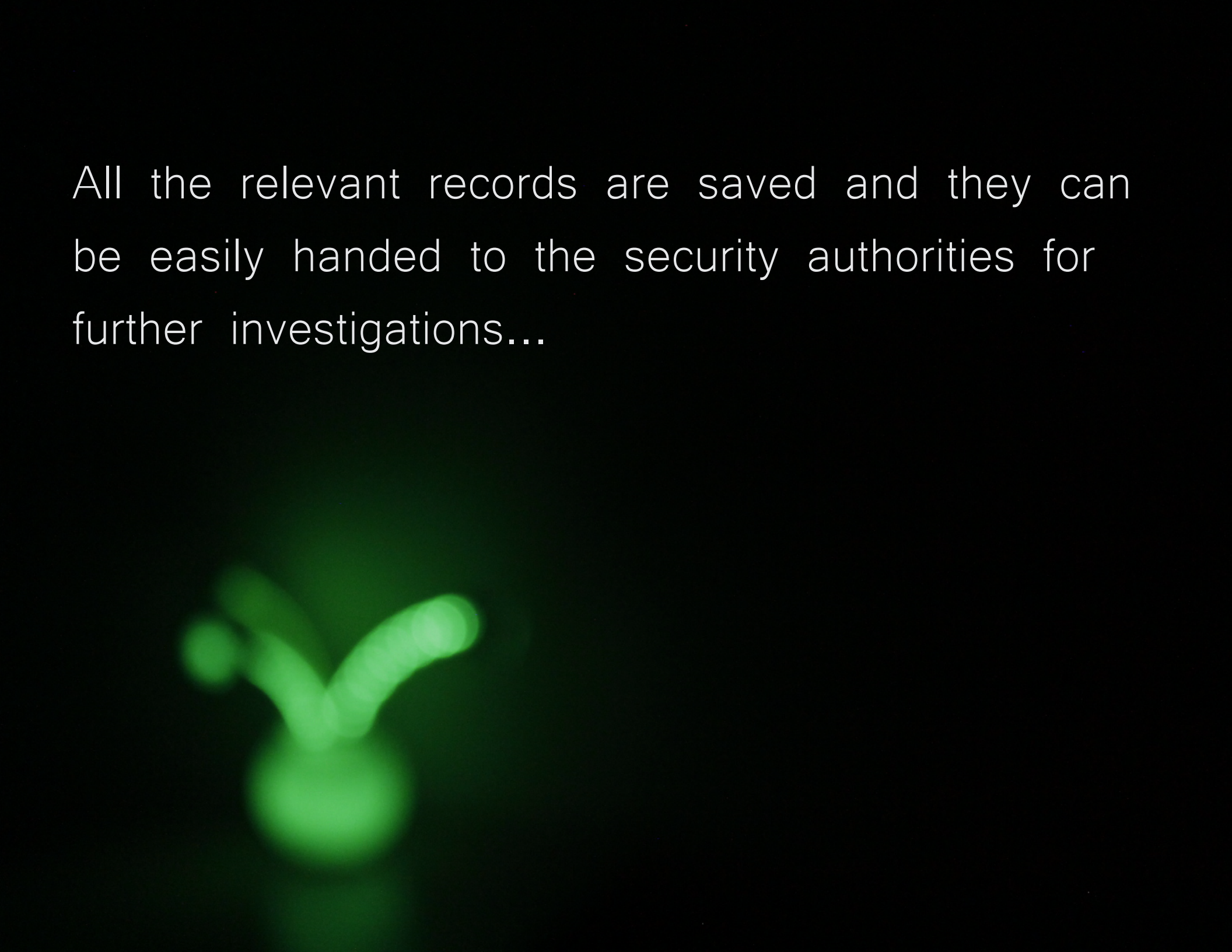


CART 360

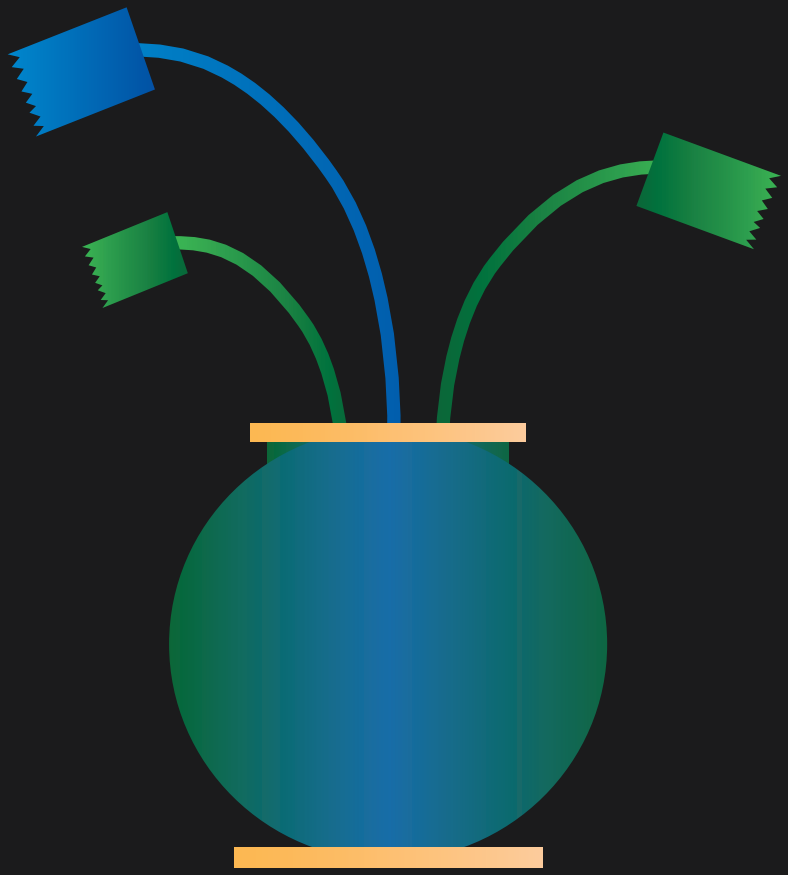
HackerPot provides insight into your virtual network activities by creating a trap for hackers...



All the relevant records are saved and they can be easily handed to the security authorities for further investigations...



HackerPot protects your IoT devices by notifying you of a “hacker catch” divided into three different kinds using distinct colors...

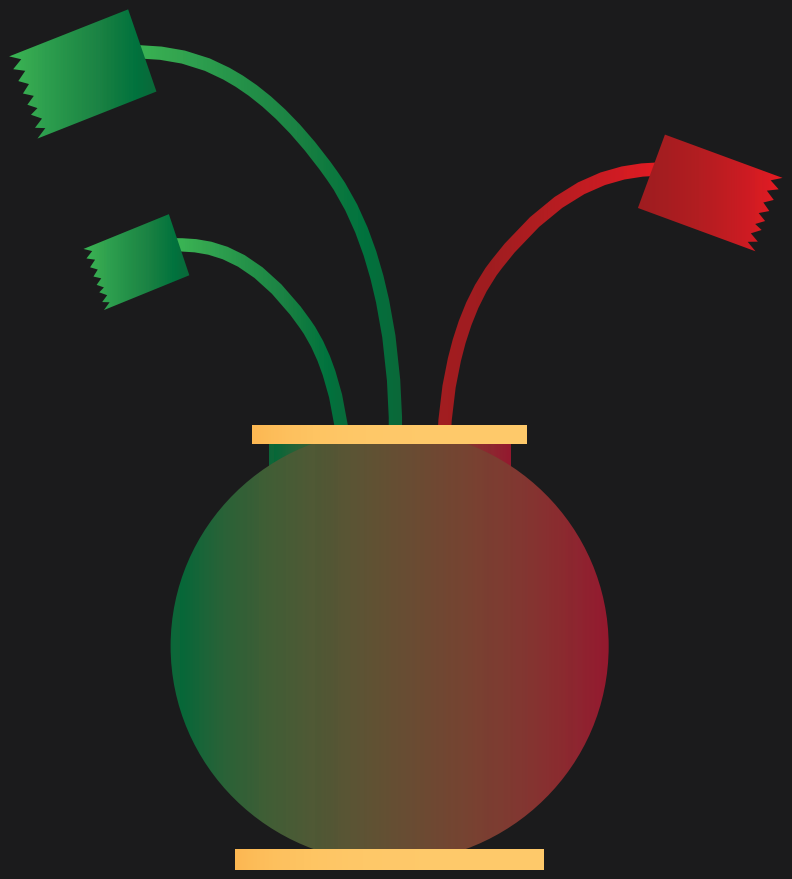


CONNECTION

A connection happens when an attacker is scanning your devices to look for vulnerable applications.

A color transition into blue indicates that the attacker is active and connects to your IoT application traps to analyse them.

Your IoT devices should not be scanned without your conscent. This may indicate a possible undesired presence in your network.

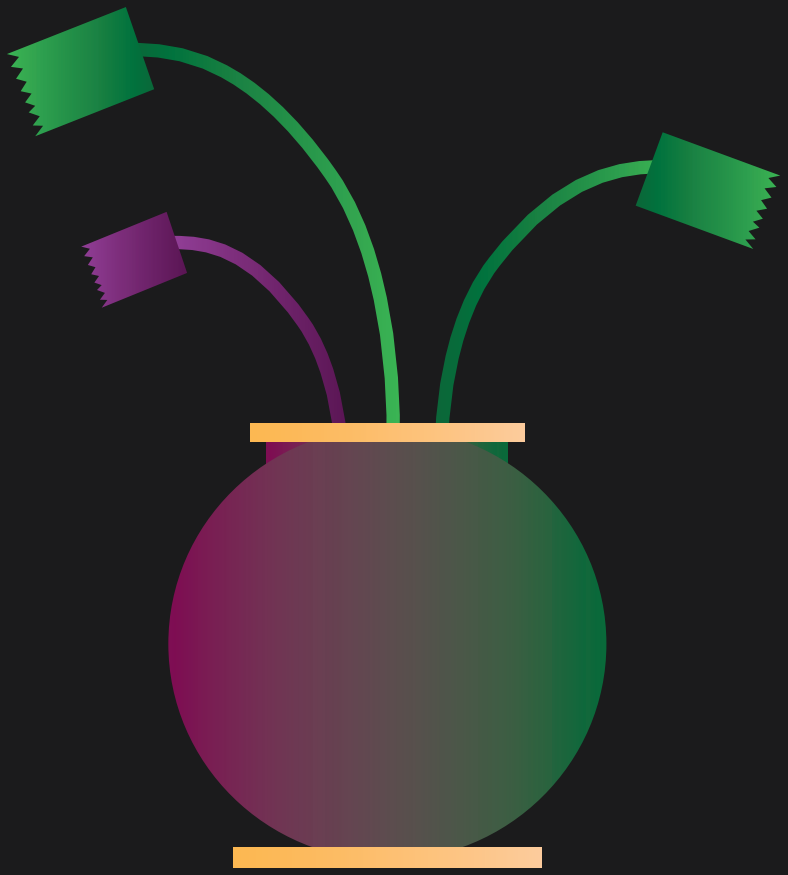


INTRUSION

An intrusion happens when an attacker breaks into one of your HackerPot application traps.

This indicates that the attacker is agressive and determined to get access to your IoT devices.

You IoT devices may be strong enough to resist intrusion but it is recommended to inform your Internet providor or a security analyst.

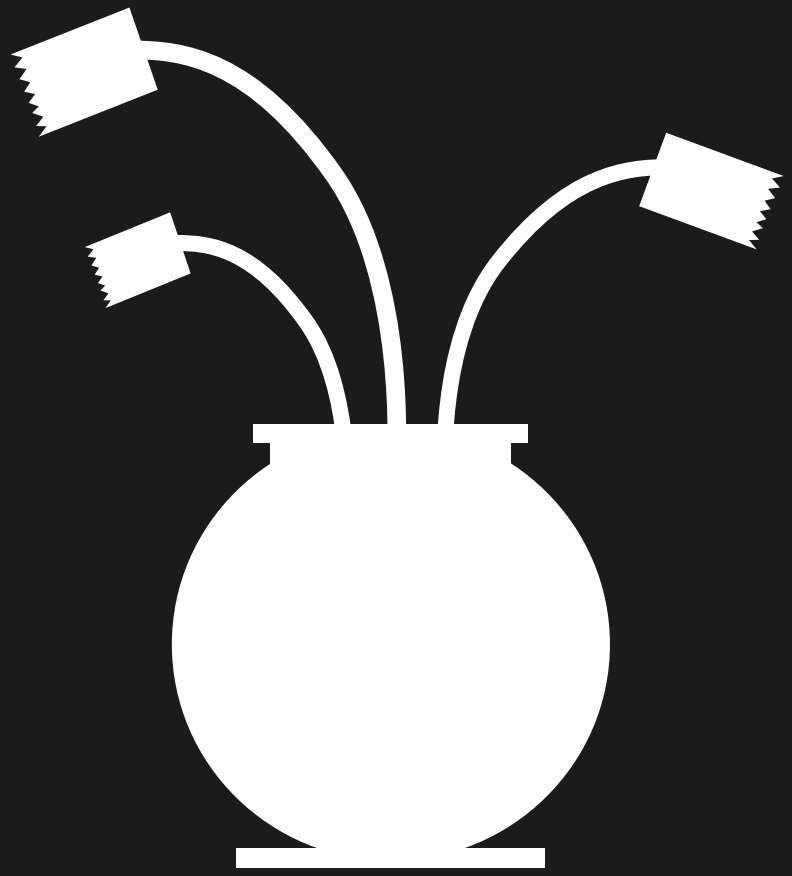


DoS

A Denial of Service happens when an attacker is sending data to make your HackerPot busy.

This indicates that the attacker is active and tries to put your IoT device out of service.

Your IoT devices should not be denied service. This may indicate a possible undesired presence in your network.



HACKERPOT