Quicksand™ - IoT Honeypot

Real-Time Security Intelligence for Embedded Systems

DATASHEET

Get Smarter Intelligence – Be Safer

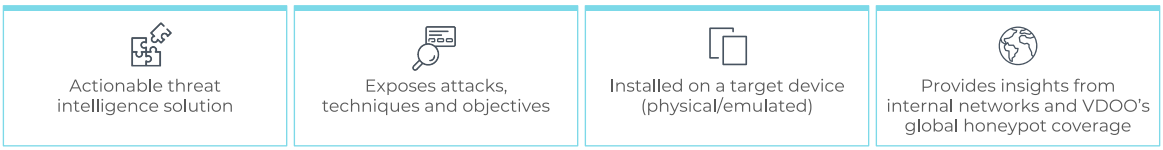
The rising number of IoT cyber-attacks, the complexity of the attacks, as well as the variety of malware samples and malware types crafted specifically for IoT devices reflect the attackers' awareness of the huge opportunity IoT technology holds. Threats are evolving rapidly, and the entire IoT ecosystem is struggling to evolve its security at the same pace; therefore, it is very important to keep up to date with the latest trends and new emerging threats to protect the devices and the network they are connected to. Device manufacturers who want to offer their customers secure devices, as well as enterprises that use IoT devices, are advised to implement a honeypot solution as an additional security layer that allows real-time intelligence on targeted attack attempts, exposure of the attacker's techniques, and understanding of what the attack targets are. In addition, the honeypot enables discovery of new vulnerabilities and detection of opportunistic attacks (using techniques such as easy username and password combinations) and widespread campaigns.

Honeypot Tailored for Your Specific Device

In order to gain all relevant intelligence insights, and only those, a honeypot automatically tailored for each device type is necessary. The honeypot is tailored for each device based on analysis of its firmware binary by VDOO's analysis platform. This approach makes our honeypot the ultimate solution for IoT devices since, thanks to auto-tailoring, the honeypot mocks the device precisely and acts like a real device deployed in the field. Honeypots deployed across the network provide real-time alerts upon attack attempts, revealing the attacker's malicious intentions before any real damage is done or user devices are infected.

Proactive Security – You Target the Attacker

VDOO implements and maintains honeypot devices globally, monitoring the OS and the network activity to build the most advanced IoT threat mapping based on real-world intelligence. VDOO honeypot has two versions—"Bot" and "Zero". The "Bot" honeypots are deployed in the wild as relatively vulnerable devices with minimal to no security measures, to lure an attacker that can easily exploit it. The "Bot" version allows insights on attack attempts by common malware samples and distributed attacks. On the other hand, the "Zero" honeypots are deployed as securely as possible, to reveal zero-days exploited by the most sophisticated and targeted attack attempts—since only the really sophisticated attacker who uses high-complexity methods will be able to exploit the "Zero" honeypot and get caught immediately. VDOO premium offering combines both "Bot" and "Zero" versions to achieve complementary capabilities.



"Bot"
- A vulnerable device, with light security configuration
- Used to identify commodity, distributed attacks
- Scanning, default password attempts, known vulnerabilities exploitation, etc.

"Zero"
- A highly secure device configured to minimize exposure, fully patched
- Used to identify zero days, targeted attacks

Real-Time Alert Mechanism Against Various Threats

The honeypot provides visibility of any kind of activity taking place on the device; therefore, it allows monitoring for a wide range of threats—known and unknown. Monitoring and alerting configurations can be adjusted according to user needs. Among the alert modules are:

Process guard: Alerts upon execution of newly introduced malware
File guard: Alerts upon malware attempts to modify or destroy files on the device
Resource guard (CPU and memory): Alerts upon malware that behaves abnormally in terms of resource consumption
Process termination guard: Alerts upon malware that tries to kill any process that was defined as a protected process
SSH guard + TCP guard: Monitors SSH sessions and new TCP connections
Command injection detection: Alerts upon any attempts to inject shell commands through a web interface
Login detection: Alerts upon login and brute force attempts
Watchdog: Alerts upon relaunch of selected processes or services
Command execution history: Recording of all commands executed on the device

Technical Process

VDOO's research team deploys the honeypots as part of a network, using a tunneling method that allows the honeypot to be located under any desired IP address. After deployment, the user gains a full image of the device and its network environment threats, by integrating the honeypot alert mechanism with any alerts system dashboard. Upon a real attack, the user receives the relevant alerts, based on the chosen configuration, and can utilize the data to perform a deep attack research for better intelligence. In case the user is not qualified for this task, VDOO's research team can perform a deep forensic research and provide the user with a detailed insights report.

Specifications Table

Supported OS	Linux
Supported CPU architecture	MIPS | ARM | x86 (32 and 64 bit)
Deployment	Physical device | Emulated device
Security level	Vulnerable ("Bot") | Hardened ("Zero")

Proprietary Research Approach

The VDOO IoT honeypot was built based on vast research of embedded device threats that includes the device components, hardware, OS, kernel, and software libraries. With successful testing conducted against top IoT malware types, such as Mirai, VPNFilter, Torii, and Chalubo, VDOO is proven to eliminate today's and tomorrow's advanced IoT threats. Implement the essential honeypot security layer—before damage is done.

About VDOO

VDOO was established in 2017 to pioneer embedded systems security, with an end-to-end solution of security automation, certification, and protection. The VDOO founders' backgrounds include an endpoint cybersecurity startup acquired by Palo Alto Networks, as well as notable experience serving in the Israeli Intelligence Elite Unit. For additional information, please contact us at info@vdoo.com or visit our website vdoo.com.

VDOO

Key Features

- Automatically tailored for each device
- Physical or emulated device
- Vulnerable "Bot" and hardened "Zero" versions

Key Benefits

- Understand the device's exposure to risk
- Detect attacks in real-time
- Detect vulnerabilities before exploitation damage is done
- Get alerts for a wide variety of threats

Related Products

- VDOO Vision™
- VDOO CertIoT™
- VDOO ERA™