



**LIFARS**  
your digital world, **secured**

## IOC CHECKER

EXTERNAL NETWORK & INTERNAL NETWORK PENETRATION TEST DEVICE CONFIGURATION REVIEW

[www.lifars.com](http://www.lifars.com)

# WHAT IS IT



- Scans for indicators of compromise (IOCs)
- Full stack application
  - CLI client + Backend + Web admin console
- Our own IOC tree-based format
  - Can also convert from MISP & OpenIOC

# APPLICATION STACK

```
Administrator: C:\Windows\system32\cmd.exe

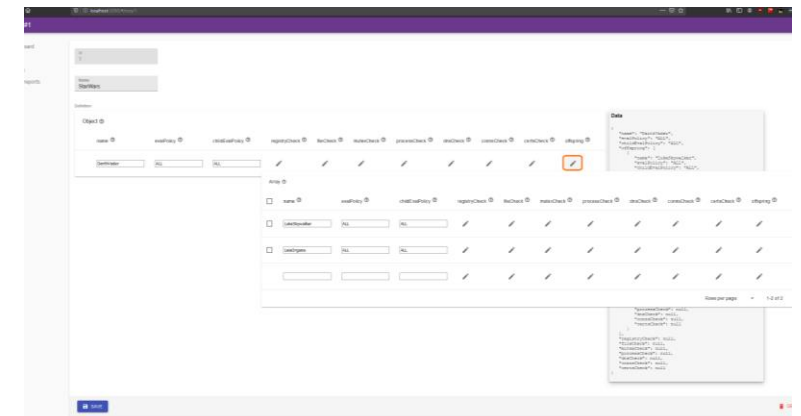
Users\IEUser\Desktop>ioc-checker-probe.exe
18:47 [ INFO] Loaded properties
18:47 [ INFO] No IOC definitions specified.
18:47 [ INFO] Loaded 0 IOC definitions from file
18:47 [ INFO] Running in online mode. Establishing communication with server
18:47 [ INFO] Loaded 2 IOC definitions from server
18:47 [ INFO] Total loaded IOC definitions: 2
18:47 [ INFO] Searching IOCs using file search.
18:47 [ INFO] Found 2 IOCs out of 2 search parameters
18:47 [ INFO] Searching IOCs using open DNS search.
18:47 [ INFO] Searching IOCs using registry search.
18:47 [ INFO] Found 1 IOCs out of 1 search parameters
18:47 [ INFO] Searching IOCs using open network connection search.
18:47 [ INFO] Searching IOCs using open process search.
18:48 [ INFO] Searching IOCs using certificate search.
18:48 [ INFO] Report saved

Users\IEUser\Desktop>_
```

IOC Probe (CLI client)



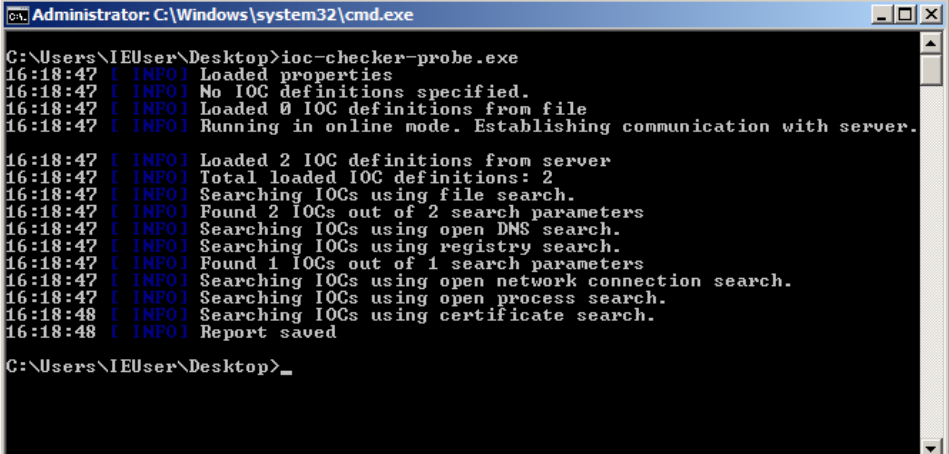
Server



IOC Admin

# IOC PROBE

- Small CLI utility (2.5 MB) deployed on a client machine
  - Written in Rust
  - Fully native app, no external dependencies
- Downloads IOCs from server and checks if some is present
- Afterwards uploads result on server
- Supports also **offline** mode – no connections from server
  - IOC definitions are specified manually (JSON format)



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\IEUser\Desktop>ioc-checker-probe.exe
16:18:47 [ INFO] Loaded properties
16:18:47 [ INFO] No IOC definitions specified.
16:18:47 [ INFO] Loaded 0 IOC definitions from file
16:18:47 [ INFO] Running in online mode. Establishing communication with server.

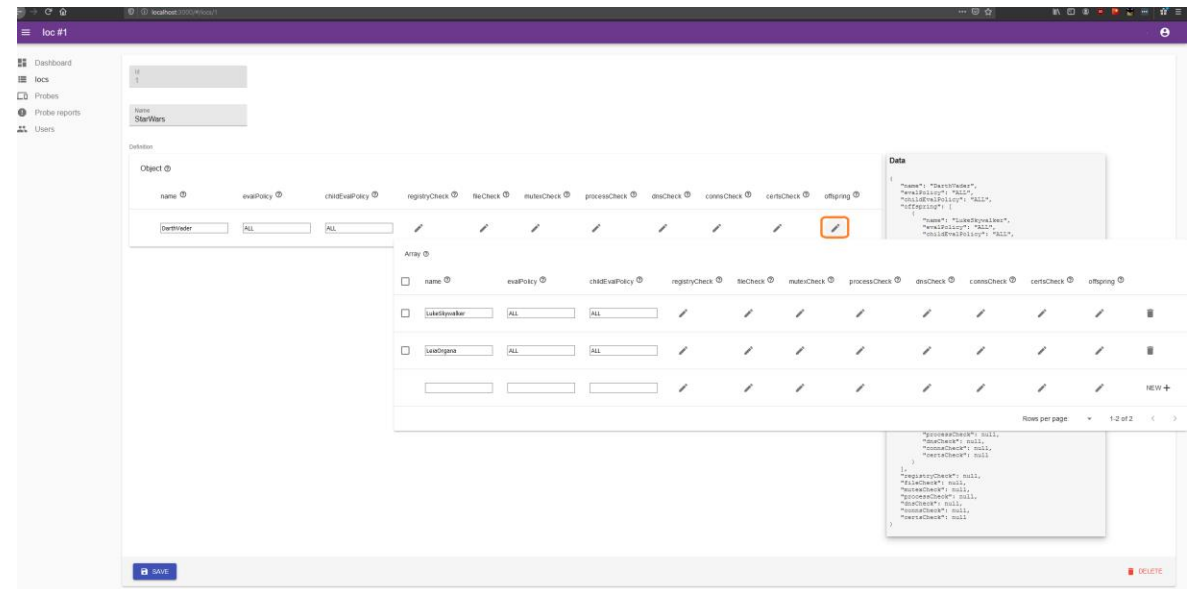
16:18:47 [ INFO] Loaded 2 IOC definitions from server
16:18:47 [ INFO] Total loaded IOC definitions: 2
16:18:47 [ INFO] Searching IOCs using file search.
16:18:47 [ INFO] Found 2 IOCs out of 2 search parameters
16:18:47 [ INFO] Searching IOCs using open DNS search.
16:18:47 [ INFO] Searching IOCs using registry search.
16:18:47 [ INFO] Found 1 IOCs out of 1 search parameters
16:18:47 [ INFO] Searching IOCs using open network connection search.
16:18:47 [ INFO] Searching IOCs using open process search.
16:18:48 [ INFO] Searching IOCs using certificate search.
16:18:48 [ INFO] Report saved

C:\Users\IEUser\Desktop>_
```

# IOC PROBE

- Able to detect IOCs by
  - File name
  - File using MD5, SHA1 & SHA256 hash
  - Running process name
  - Windows Registry
  - DNS address
  - Network connection
  - Certificate name
  - Process mutex
- Supports also regex search

- It can
  - Manually create/edit IOC definitions (on image)
  - Register new probe access tokens
  - View scan reports
  - Manage feed sources for externally defined IOCs
    - Periodically downloads new IOCs
    - MISP & OpenIOC formats supported ATM



THANK YOU  
**LIFARS**  
your digital world, secured  
**QUESTIONS?**