Secura
A BUREAU VERITAS COMPANY

Secura Backdoor Detector

INSIGHT INTO YOUR DIGITAL SECURITY

Secura has worked in information security and privacy for over two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

What is the Secura Backdoor Detector?

Secura Backdoor Detector is a toolset that allows the end user to detect unexpected routes from one network (e.g. a secure network) to another network (e.g. the public internet).

Data protection involves securing the network to ensure sensitive data remains inside of the network. **To prevent data exfiltration**, it is important to ensure the secure network does not contain any 'backdoors'. Users within this network can, on purpose or by accident, create backdoors. For instance, a user might need internet access within the secure network and uses a VPN, Proxy or Mobile Hotspot to enable this. Or some peripheral that needs to be accessed from multiple networks by accident creates a route from one network into another. Or a rogue device is hidden inside the network.

Why Secura Backdoor Detector?

The security measures within the network can become severely undermined by both configuration mistakes as well as users that, possibly without overseeing the consequences, create their own connections. Or the network is infiltrated and a rogue device is put in place. Not all of these connections will be permanent. For that reason, it is important to regularly scan the network for unexpected connections. **Secura Backdoor Detector is a toolset that can continuously scan a network and detect connections towards another network** (e.g. the internet).

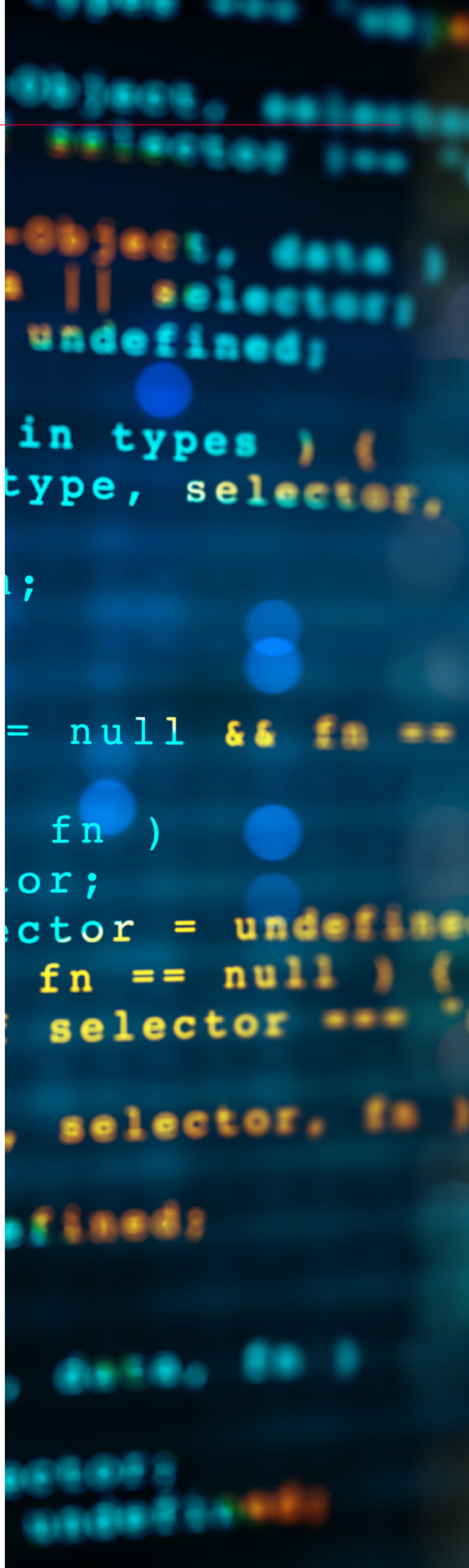
How to Detect and Identify Connections?

The technique the Backdoor Detector toolset uses to detect connections is sending specially crafted so-called IP packets into the network. These packets contain an altered source address. The detection technique relies on the fact that a device will respond back to that source address.

If we change the source address, the packet will not go back to the 'real' source device, but to the address specified in the source address. As this source address is an address outside of the network, the device will try to find a route to that address, and automatically use the 'leaking' connection. The specially crafted packets are created using **the thrower application**, that points the source address of each packet to the catcher application.

The thrower application sends out packets to all devices within a certain network. **The catcher application** runs on a device in the network to which there should be no connection (e.g. the internet). Packets will arrive at the catcher if and only if an unexpected connection exists to the catcher application.

The web application analyzes the packets on **the catcher** and shows the used gateway to connect, as well as the internal IP address of the device that sent out the packet and other information to correlate the received packet to the ones created by the thrower application. The application also allows to notify the user via email when a new connection is detected.



Secura
A BUREAU VERITAS COMPANY

Features of the Backdoor Detector

- **Create and send specially** crafted ICMP, UDP and TCP packets into a network.
- **Easy to configure and deploy** within your own network
- **Catcher application** that receives packets when an unexpected connection is present.
- **Web application** that analyzes and presents gateway and internal IP address of the devices that exposed the unexpected connections.
- **Catcher and Web application** hosted and configured by Secura.
- **Strict separation** between user accounts and corresponding data.
- **Web application** that supports secure account access and supports modern 2FA methods.
- **Email notifications** when a new connection is discovered.
- **Easy and reliable creation, execution and management** of unexpected connections in a network.
- Only the thrower application runs in your network; other components can be hosted by Secura.
- **Fully ready to be used** for continuous/periodic scanning.
- **Easy to use** web application for easy analysis and detection.

Benefits of the Backdoor Detector

1. Notification of an unexpected connection
2. Detect unintended (or malicious) backdoors
3. One time check or continuous scanning
4. Double check network segmentation
5. Double check firewall settings

Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

+31 88 888 31 00
info@secura.com
secura.com

BUREAU VERITAS
Shaping a World of Trust