ROATI Technologies Inc.
64 Bramalea Road, Unit 1216, Brampton, Ontario, L6T 2W8, Canada
+1 (905) 846-1233, (800) 458-3089 (USA & Canada), -5 GMT, ralph@roati.com

Malware Secure Computers

A rethink for how the computers' hardware processes data

Overview: roati.com/factsheet

Malware Secure Computers which safely open & process both clean and Malware Infected data files, without the need or use of detection software, encryption, VPN, AI or analytics.

This is a new computer hardware discovery, not a software improvement.

We do not detect or remove a malware at entry. We actually safely open and process both clean and malware infected data files. Files in the input stage are later removed, via a new cleaning protocol. Yet data is securely stored, not infected

Background: roati.com/bio

I have 30+ years in electronic components, which included the supply of components to three satellites. My discovery of a New Class of Computer Components led to my design for how our computers' hardware is now able to SAFELY open and processes both clean and malware infected data files *(see file types below).*

The Problem:

Despite the good work made in cyber security, malware still obtain entry, enabling its malicious intent. A rethink was needed, which is why we focused on how the computers' hardware processes data, enabling this discovery.

File types which we safely open & process:

Malware Infected: Web sites, emails, Word, DOCX, PDF, C, CPP, JAVA, RTF, TXT JPG, IOT, IIOT, WPD, XML robot instructions, source code files from repositories & several others.

Complex Password Generator:

It is easy for the user to generate, retrieve or insert complex passwords. Our generator stores complex passwords in a malware safe area of an air-gapped portion of our computers. Here they are securely stored, read & used.

How it works: roati.com/technical

Our computers consist of two physically and electrically separate and isolated computers, contained within one housing. This discovery enables them to function as one.

Computer # 1: is an input stage virtual computer. Here both clean & malware infected files are SAFELY opened. During the process of sending the file to computer #2, is where the file is made malware free. That file is now in two locations, possibly infected in stage #1 & absolutely not infected in stage #2.

What we say in the following paragraph, is contrary to todays' computer thinking.

It's **100% impossible** for a malware to write to the SSD or BIOS during normal usage. This is due to a new SSD circuit design & hardware component discover, yet SSD software and BIOS can be safely read & processed.

Software updates & data are securely loaded via a new and secure software update protocol.

Computer # 2: is an air-gapped computer. It here where the main storage and processing are safely executed. In this stage, we mainly use existing technology & software. As this area is air-gapped, it is immune from intruders.

The core of this discovery:

The core of this discovery, is a New Class of Computer Components (NCoCC), based on a new computer principle discovered at our lab. The NCoCC, is what enables the bi-directional, air-gapped, malware safe, data communications between these two isolated computers, enabling them to safely process data separately, yet operate as one Malware Secure Computer.

Ralph Kachur, President

Protecting Electronic Information
with Malware Secure Computers

Rev 18 – February 7, 2023