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

Rethinking how computer hardware processes data

Overview: *roati.com/factsheet*
Malware Secure Computers which safely open and 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.

The input stage is where both clean and malware infected files are SAFELY opened. It is the actual hardware process of transferring the file to an air-gaped secure area of the computer, where all data files are made clean & safe to share.

Background: *roati.com/bio*
I have 30+ years in electronic components, which included the supply of electronic components used in three satellites.

The Problem:
Despite the good work made in cyber security, malware can still obtain entry, enabling its malicious intent. A rethink was needed, which is why we focused on the computers' hardware.

It is due to our new hardware redesign, why our computers are able to SAFELY open and processes both clean and malware infected data files without using malware detection software, encryption, VPN, AI or analytics.

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 & other data file types

Complex Password Generator:
It is easy for the user to generate, retrieve or insert complex passwords. Our password generator, stores and calls complex passwords from a malware safe area, of an air-gapped portion, of our computers.

How it works: *roati.com/technical*
Our computers consist of two physically and electrically separate computers, contained within one housing. Our discovery, is what enables these two separate computers to function as one. One is used to open files & the other to store data safely. How they communicate with each other is what our discovery does.

Computer #1: our virtual computer, input stage.

This is where both clean and malware infected files are SAFELY opened and used. It is the hardware process of sending the file to computer #2 where the file is made malware clean. That file is now located in two stages, possibly infected in stage #1 and 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 discovery, yet SSD software and BIOS can be safely read & processed.

Software updates & data are loaded via our new and secure, software update protocol.

Computer #2: is an air-gapped computer. This is the main storage and processing area.

It is our discovery of a New Class of Computer Components which enables the malware safe, bi-directional, air-gapped, data communications between these two isolated computers.

Note: This fact sheet is written to state what our discovery does. To discuss how we do this, please be in contact. We are anxious to share our discovery and protect the worlds' data against the plethora of malware attacks, such as ransomware

Ralph Kachur, President

Protecting Electronic Information
with Malware Secure Computers

Rev 21 – February 27, 2023