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

Malware Secure Computers

A rethink for how the computer hardware processes data

Overview: *roati.com/factsheet*
Malware Secure Computers which, safely open, process and share incoming Malware Infected data files, as no longer infected.

As impossible as this may sound, we actually do this without the need or use of detection software, encryption, VPN, AI or analytics. This is a computer hardware discovery, not a software improvement.

We use your existing software. Talk to us about possibly using your older heritage software.

Background: *roati.com/bio*
30+ years in electronic components, which included the supply of electronic components and technical support to three satellite projects.

The Problem:
Software is malwares' best friend.

Despite good progress made in cyber security, malicious software (malware / ransomware) can still obtain entry. A rethink was needed.

It was when I realized that the constant stream of software improvements was just not working, as proven by the plethora of malware attacks which we so regularly see. This is the reason I focused on the computers' hardware to be able to safely processes a malware infected data file.

File types we safely open, process & share:

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 complex passwords, in 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 isolated computers, contained within one housing, operating as one computer. A virtual and an air-gaped computer.

Computer #1: is our input stage, virtual computer

Here is where both clean and malware infected files are opened. The file is made malware free during the new hardware process, of actually sending the file to the air-gaped computer #2,

That file is now located in two places, possibly infected in stage #1 and absolutely not infected in stage #2, later the file in #1 is cleaned.

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

It's **100% impossible** for a malware to write to our SSD or BIOS, during normal usage. SSD & BIOS are safely read & processed, without any malware.

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 overview is to say what our discovery does. To discuss how we do this, please be in contact. I answer the phone or I use WhatsApp

Conclusion:
Protecting electronic information, is what our Malware Secure Computers efficiently do

Ralph Kachur, President