**Malware Protection Discovery**

**Overview:***May 16, 2022*

Malware Secure Computers which "safely" open and process, "both" clean and "malware infected" files, including malware infected, web sites, emails, attachments, Word, PDF, SQL and ORACLE files, to name a few.

We open and process malware infected files in the input stage. Then "safely" transfer that file to the main processing and storage stage as a "no-longer infected file".  This is accomplished without the need or use of detection software.

You could think of this as a malware cleaning process, but it is certainly not.  It is a totally new way for how the actual hardware of the computer itself "safely" processes data.

**Simplified Technical Detail:**

|  |  |
| --- | --- |
|  | The core of this new discovery and design, is our in-house discovery of a new information conduit for computer data to travel on, which we named the r-conduit.  It is a different type of information conduit from fiber-optics, Wi-Fi, RF or wire  The way the r-conduit transports data, led us to the development a New Class of Computer Components (NCoCC), in turn leading us to a design for Malware Secure Computers, which enables the "safe" opening of malware infected files |

Our computers are in fact two computers in one. First is the input computer, which is "physically and electrically" isolated from the second computer, the main processing and storage computer.

The input computer is described as a Linux based, sandbox, virtual, input computer where all incoming files are opened. Under normal operating conditions, it is "100% impossible" for a malware to write to the Hard Drive or BIOS. Safely opening a malware infected file will seem counter intuitive, when you base your thinking on existing cyber and computer technology.  However, for our new input computer design, malware infected files are "absolutely safely opened".

The main processing and storage computer, is basically a standard type of desktop PC, with new security features which our discovery now makes possible..

The problem was, how to facilitate the malware safe, bi-directional, air-gapped data communications between these two physically & electrically isolated computers.  It was the discovery of the r-conduit and NCoCC design, which enabled our Malware Secure Computer discovery.  Our Malware Secure Computers discovery is now an important cyber safe reality.

I am seeking support to move from the startup and discovery stages, to the manufacturing and business stages, starting and building a North American Malware Secure Computer manufacturing industry.

Safe Computing  
Ralph Kachur  
President

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | [roati.com/elevator](http://www.roati.com/elevator) | ***Recommended first read -*** Short Overview of Discovery | | [roati.com/business](http://www.roati.com/business) | Business Overview  *(technical language minimized)* | | [roati.com/technical](http://www.roati.com/technical) | Technical Detail  *(technical language used)* | | [roati.com/bio](http://www.roati.com/bio) | My Business & Technical Background |   ***Copy of this web page as a two page*** [***MS Word file***](Malware%20Secure%20Computers-16.docx) |

|  |  |
| --- | --- |
|  | **ROATI Technologies Inc.** ***Malware Secure Computers     Protecting Electronic Information*** |
| 1216 - 64 Bramalea Road Brampton, Ontario, L6T 2W8, Canada   |  |  | | --- | --- | | (905) 846-1233 | *Eastern Time,  -4 GMT, -4 UTC* | | (800) 458-3089 | *USA  &  Canada* |  |  |  |  | | --- | --- | --- | | *Phones answered* | *8:00 am - 10:00 pm* | *Eastern Time,* ***7 days / week*** | |  | *5:00 am -  7:00 pm* | *Pacific Time* | |  | ≥ 1 hour | All time zones |   [www.roati.com](http://www.roati.com/)  [ralph@roati.com](mailto:ralph@roati.com)  **ROATI**  is an acronym for   **R**alphs **O**nto **A**nother **T**echnology **I**nnovation |