***Malware Secure Computers***

**Question:**

Can a Malware Infected, << email, web link, attachment or file >>, be safely opened and processed as, no-longer-infected, without the need or use of detection software?

**Short answer:**

Yes and I have.

**Brief answer:**

Yes, by redesigning how the computers’ hardware processes data.  This is not a software improvement. It is a new Malware Secure Computer hardware design.

I made a series of electronic component discoveries, resulting in a new computer design.

This new computer design is due to:

* my discovery of, a new Information Conduit for computer data to travel on,
* leading to a design of, a New Class of Computer Components (NCoCC),
* leading to a design for, Malware Secure Computers, which SAFELY open and process malware infected files, as no-longer-infected.

This level of malware safely, is actually accomplished without the need or use of, detection software, encryption, VPN, AI or analytics.

The enabling technology has been proven in my lab to <MY> satisfaction. With basically no funding, I am now finally, at the last stage of building a physical Proof of Concept PoC), to be able to publicly demonstrate, this important malware protection discovery.

It is this last stage where a final PoC is so close, but so far. Due to being underfunded.

**Detailed answer:**

By using technology from two satellite projects, which I supplied technical support and electronic components to, I discovered a new, Information Conduit for computer data to travel on.  This new Information Conduit is different from information conduits used today. Common types are, fiber-optics, wire, RF, laser, ULF/sound and Wi-Fi.

This new Information Conduit discovery, enabled my design for a New Class of Computer Components (NCoCC) and its support circuitry, my area of specialty. It is the NCoCC and support circuitry, which enables the new way by which the computers’ hardware, is now able to safely process data and is the core to my Malware Secure Computer discovery.

You need to first know, my Malware Secure Computers are in fact, two electrically and physically isolated desktop computers, contained within one housing. They co-operate with each other and function as one computer.  They are: 1/ a virtual computer, the main input stage, where it is 100% impossible to write to the hard drive (SSD) during normal operating conditions (controversial, but a true fact) and 2/ a standard air-gaped computer, functioning as the main storage and main processing area.

You can think of the NCoCC as a one-way gate for data transfer.  The use of two NCoCCs set in opposite directions, is what enables the air-gaped, bi-directional, malware safe, data communications between these two electrically and physically isolated computers.

One half of the NCoCC (YELP), is on the virtual computer. The YELP communicates the file, via a propitiatory method to the second half of the NCoCC (PHE), located on the air-gaped computer & is set in reverse to enable bi-directional communications & instructions.

Here is the part which you many find difficult to believe or understand, but it has been proven in my lab.  When a malware infected or clean file is presented to the input of the YELP (can be thought of as a transmitter, but does not transmit), when the file is received at the PHE, it is absolutely a no-longer-infected file. (Further detail of how the NCoCC functions, cannot be released at this time, but will be revealed at product launch).

That file, is now in two locations, 1/ unknown if either clean or malware infected in the input stage and 2/ absolutely "NOT infected" in the air-gapped stage.  That file, which is “NOT infected”, may now be safely and confidently, saved, edited or shared with others.

After the file has been safely copied from the virtual (input stage) to the air-gapped computer, the problem is, we do not know if the file in the input stage is clean or Malware infected, therefore, input stage is “hard booted”, removing any potential unknown malware.

As rebooting is normally time consuming, we have five independent RAM / CPU segments (containers) in the virtual computer, which are in a constant state of processing or rebooting.  The user does not see this activity.  The action of constantly rebooting, ensures that any unknown malware present, such as key loggers, are deleted.  After POST, RAM storage locations are cleaned, then are safely reloaded with data in the air-gapped stage.

Removing power from a single RAM / CPU container at a time, makes rebooting times significantly faster.  The main PSU, SSD, BIOS and other parts remain power on.

The development of a physical Proof of Concept (PoC) has been self-funded to date. I am now at the final stage of needing to hire specialized technical help, to build a physical PoC.  Once a PoC is completed we will be able to demonstrate to the world, what has been proven in my lab, a significantly important malware protection discovery.

I am actively pursuing a grant for $20k (us $15k) to complete my four years of research. Until now, my efforts have not been successful.   Wish me luck.  So close, yet so far.

I personally answer the phone 8am - 10pm, Eastern Time Zone, - 4 GMT.  By keeping these hours, we are able to have a minimum of 1 hour business time for all time zones.

I am happy to personally talk with anyone who is interested or just curious.  I use WhatsApp to make it easier for international parties to easily contact me.

Safe Computing,

Ralph Kachur, President

|  |  |
| --- | --- |
|  | **ROATI Technologies Inc.** ***Malware Secure Computers      Protecting Electronic Information*** |
| 64 Bramalea Road, Unit 1216 Brampton, Ontario, L6T 2W8 Canada   |  |  | | --- | --- | | (905) 846-1233 | *EDT,* *-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. |   [roati.com](mailto:roati.com) roati.com/factsheet [ralph@roati.com](mailto:ralph@roati.com)  *Rev 23 08 10 - 00 .*  **ROATI** is an acronym for **R**alphs **O**nto **A**nother **T**echnology **I**nnovation |