**Non-Digital Method of Data Processing**

Enabling Malware Secure Computing

**Executive Summary:**

A computer hardware discovery, which SAFELY opens and processes, malware infected files.

This new level of cyber safety is accomplished, without the need or use of detection software, encryption, VP, AI or analytics.

This new level of cyber safely is due to our discovery of, a new and non-digital method of data extraction, transport and processing, which works in tandem with standard digital processing methods of today..

We are in the early stages of this important Malware protection discovery and are seeking support to build a Proof of Concept of the enabling technology proven in our lab.

Our main objective is, to start a North American, Malware Secure Computer and related products, manufacturing industry.

**OVERVIEW**:

Our hardware discovery enables, a non-digital & non-analog method of data extraction and transport. We extract and process, ONLY the data of an incoming file and DO NOT process the digital portion of that incoming file in the final stages. By not processing the digital portion, we also don’t process or spread any malware. The result is, malware secure computing.

In a separate container, the non-digital form of the data is inserted into a new digital file. Once the new data only digital file is confirmed, all traces of the original incoming file is totally erased

That new and malware free file, may now be safely processed, saved or shared with others. This is not a Malware cleaning process but rather a new way of processing data.

This discovery also enables the malware safe processing of emails, Internet activity, plus the many other forms of industrial, military and commercial data communications.

**TECHNICAL  OVERVIEW:**

Two computers are physically and electrically isolated from each other, within one housing.  Both operating co-operatively as, one computer.

The first computer, is a new design for a virtual computer, which contains five isolated SandBox Containers (SBCs).  It is these virtual computers that we use to communicate, to the malware infested cyber sphere.

The second computer, is a new type of air-gaped computer, where data is processed, stored or shared. This area is also where, our new design for a password generator resides and its’ passwords are stored. Our new password generator, is discussed under separate cover.

Although, both computers are electrically and physically isolated from each other, they are able to share data and control processes with each other.  This is due to our new non-digital form of data extraction and transport, where ONLY the data is transported, NOT the digital portion of the file, which might also contain a malware. This non-digital discovery, inserts a type of open circuit into the digital only highway, preventing malware from spreading.

This discovery enables, new types of safe, computer hardware circuits to exist.

Incoming files are received and isolated in one of the five isolated Sand Box Containers (SBCs) of the virtual computer. That Incoming file, is then presented to a New Class of Computer Components (NCoCC).  The NCoCC consists of two halves, one half in the virtual computer (YELP and support circuitry) and the other in the air-gaped computer (PHE and support circuitry).  Another NCoCC is set in reverse, to enable bi-directional communications. In order to help you understand the two halves of the NCoCC, you may think of them as a one-way transmitter and receivers, but they are not.

* The hardware of the YELP, in the virtual computer, executes a non-digital method of data extraction from that incoming digital file.
* That non-digital form of data, is then transported to the PHE in the air-gaped computer, which is then inserted into a new digital file, of the original incoming files type.
* Once the new file has been confirmed as being built in the air-gaped computer, all traces of the original file in that virtual computers' SBC, are totally erased, via a hard boot of just that SBC
* After a hard boot of that SBC and after POST, a complete RAM cleaning process is run.  This is done, in order to remove any persistent malware, which may still remain persistent in RAM.
* Then o/s is loaded.
* That SBC is now ready for the safe and normal processing of the next file.
* Due to the time needed for a complete RAM cleaning, is why we have five SBCs'.

     We still recommend you consider using analytics software.  Although our discovery will significantly reduce malware attacks, we are yet able to prevent, stupidity, insider threats or other forms of non-malware related cyber threats.

Our discovery is a monstrous step forward in the fight against Malware / Ransomware attacks.

Discussion and suggestions are sincerely invited.

Ralph Kachur,   
President

[*ROATI.com/bio*](http://WWW.ROATI.com/bio)  - To add credibility to my discovery

[*ROATI*.*com/non-digital*](http://www.ROATI.com/non-digital)  *-* These two pages on the internet

This web page as MS Word[*ROATI non-digital Word Doc-250505-00.docx*](ROATI%20non-digital%20Word%20Doc-250505-00.docx)

|  |
| --- |
| **ROATI Technologies Inc. *Malware Secure Computers     Protecting Electronic Information*** |
| 35 Kingknoll Drive, Unit KT-403 Brampton, Ontario, L6Y 5G5, Canada   |  |  | | --- | --- | | (905) 846-1233 | *- 4 GMT, Eastern Time Zone* | | (800) 458-3089 | *USA & Canada* | |