The impact of MS Windows infection vectors on IP network traffic patterns

John Nguyen
CAIA Winter Intern 2004

Agenda

1. Motivation and Research Goals
2. Building the controlled testbed
3. Selection of viruses
4. Experiments
5. Results and Analysis
   Sasser, Lovesan, MyDoom, NetSky, Gator, SpyBot and SubSeven
6. Conclusions
Motivation & Research Goals

We all know how dangerous & widely spread are some network viruses. But, what is the bottom line of their attacks?

Financial Impact of Major Virus Attacks Since 1999

<table>
<thead>
<tr>
<th>Year</th>
<th>Code Name</th>
<th>Worldwide Financial Impact ($U.S.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>MyDoom</td>
<td>$4 Billion*</td>
</tr>
<tr>
<td>2003</td>
<td>SoBig.F</td>
<td>$2.5 Billion</td>
</tr>
<tr>
<td>2003</td>
<td>Slammer</td>
<td>$1.5 Billion</td>
</tr>
<tr>
<td>2003</td>
<td>Blaster</td>
<td>750 Million</td>
</tr>
<tr>
<td>2003</td>
<td>Nachi</td>
<td>500 Million</td>
</tr>
<tr>
<td>2002</td>
<td>Kiez</td>
<td>750 Million</td>
</tr>
<tr>
<td>2002</td>
<td>BugBear</td>
<td>500 Million</td>
</tr>
<tr>
<td>2002</td>
<td>BadTrans</td>
<td>400 Million</td>
</tr>
<tr>
<td>2001</td>
<td>CodeRed</td>
<td>$2.75 Billion</td>
</tr>
<tr>
<td>2001</td>
<td>Nimda</td>
<td>$1.5 Billion</td>
</tr>
<tr>
<td>2001</td>
<td>Sircam</td>
<td>$1.25 Billion</td>
</tr>
<tr>
<td>2000</td>
<td>Love Bug</td>
<td>$8.75 Billion</td>
</tr>
<tr>
<td>1999</td>
<td>Melissa</td>
<td>$1.5 Billion</td>
</tr>
<tr>
<td>1999</td>
<td>Explorer</td>
<td>$1.1 Billion</td>
</tr>
</tbody>
</table>


Motivation & Research Goals

Questions

- What type of network attacks viruses can do?
- What kind of network traffic viruses can generate?
- How do their traffic patterns really look like?
- How many Mbyte(s) per hour, per day, per month?
- How much does it cost for a normal Internet user if his/her computer system was hit with one or a combination of viruses, worms, trojan horses, spyware?
Motivation & Research Goals

Goals:

- Building a controlled testbed to study Virus, Worm, Trojan, Spyware network behaviours
- Quantitative Analysis of the generated traffic
- Calculation of financial impact imposed on the victims

Building the controlled testbed

1) Victim host running Windows XP (v 5.1 2600  Service Pack 1) with all the latest security updates (as of 29th June 2004)

2) Sniffing host running FreeBSD OS (v 4.10)
   - Bridging and ipfw (Firewall) enabled
   - tcpdump packet sniffer
   - thttpd (Web server)
   - Sendmail (Email server)
   - BIND (DNS server)
   - tinyproxy (Proxy server)
Building the controlled testbed

**BACKHOLE CASE**

HTTP / SMTP → Bridge / Firewall / Packet Sniffer → Internet

Victim Host
Windows XP SP1

Block all outbound traffic

**CONNECTION ESTABLISHED CASE**

HTTP / SMTP → Bridge / Firewall / Packet Sniffer → ACK/RST/DATA

Victim Host
Windows XP SP1

CAIA Seminar  http://www.caia.swin.edu.au  jnguyen@swin.edu.au  21st July 2004

---

Selection of viruses

Selection criteria based on:

- **Popularity**: Sasser, MyDoom
- **Financial impact**: Lovesan, MyDoom
- **Types of propagation and attack**: NetSky (mass mailing worm), Gator (Spyware), SpyBot (P2P Worm) and SubSeven (Trojan)
Selection of viruses

Where to get Virus Samples?
- Virus Exchange Board (VX Board)
- Virus Collection Website (e.g. vx.netlux.org)
- Virii collection hobbyist and trader

Some of you might reasonably say that it is illegal to offer such content on the net. Or that this information can be misused by "malicious people". I only want to ask that person: "Is ignorance a defence?" (vx.netlux.org)

Experiments

The Process
- Baseline the test
- Execute & observe behaviours of viruses on the victim host
- Sniff traffic from/to the victim host
- Analyse captured traffic
- Refine the experiment
Experiments

The Tools:
- Fport: display all victim's opened ports
- Process Explorer: display processes & threads
- Tcpdump: sniff traffic
- Ethereal: analyse traffic patterns and flows

Results & Analysis: Process & Tools

Process:
- Understand Virus Traffic Patterns
- Graph its Traffic Profile
- Calculate Results in GBs & $AUD / month

Tools:
- Ethereal
- Excel
- Packet Plotter
Results & Analysis: Assumptions

 Typical Home broadband ISP scenario 1:
• Telstra ADSL 500MB Limited Plan
• 256/64 Kbps speed (in real life ~ 217/54 Kbps max for 85% efficiency factor)
• 15 cent for extra Megabyte upload / download

 Typical Home broadband ISP scenario 2:
• Optus ADSL Value 1GB Plan
• 512/128 Kbps speed (~ 435/108 Kbps)
• Rate limited to 28.8 Kbps until the rest of the month when quota exceeded

Results & Analysis: Sasser.A

<table>
<thead>
<tr>
<th>Type</th>
<th>Virus: attempts to exploit Windows Directory Service vulnerability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Increment by 1, <strong>5554</strong> (FTP server)</td>
</tr>
</tbody>
</table>
| **Destination Address** | 1. 25% of the time, the last two octets of the IP address are changed to random numbers.  
    136.186.C.D; where C and D are random – **136.186.193.166**  
    2. 23% of the time, the last three octets of the IP address are changed to random numbers.  
    136.B.C.D; where B, C and D are random – **136.110.221.199**  
    3. 52% of the time, dest address as A.B.C.D where A,B,C and D are completely random – **104.92.54.75** |
| Destination Port      | **445** (microsoft-ds), **9996** (to transfer worms)          |
| **Propagation Mechanism** | 1. Connects to the generated IP address on TCP port **445** to determine if a remote computer is online.  
    2. If a connection is made to a remote computer, the worm will send shell code to it to open a remote shell on TCP port **9996**.  
    3. Uses the shell on the remote computer to reconnect to the infected computer's FTP server, running on TCP port **5554**, and retrieve a copy of the worm. |

CAIA Seminar http://www.caia.swin.edu.au  jnguyen@swin.edu.au 21st July 2004
Results & Analysis: Sasser.A

Traffic Profile

![Graph showing traffic profile over time](image)

<table>
<thead>
<tr>
<th>Time(s)</th>
<th>Traffic(bytes)</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.000420</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>62</td>
<td>12827 &gt; microsoft-ds [SYN]</td>
</tr>
<tr>
<td>0.000890</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>63</td>
<td>12828 &gt; microsoft-ds [SYN]</td>
</tr>
<tr>
<td>0.000891</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>62</td>
<td>12827 &gt; microsoft-ds [SYN]</td>
</tr>
<tr>
<td>0.000892</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>62</td>
<td>12827 &gt; microsoft-ds [SYN]</td>
</tr>
<tr>
<td>0.000893</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>62</td>
<td>12827 &gt; microsoft-ds [SYN]</td>
</tr>
<tr>
<td>0.000894</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>62</td>
<td>12827 &gt; microsoft-ds [SYN]</td>
</tr>
<tr>
<td>0.000895</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>62</td>
<td>12827 &gt; microsoft-ds [SYN]</td>
</tr>
<tr>
<td>0.000896</td>
<td>136,186,219,212</td>
<td>TCP</td>
<td>62</td>
<td>12827 &gt; microsoft-ds [SYN]</td>
</tr>
</tbody>
</table>

CAIA Seminar  http://www.caiainternet.ac.uk  jinguyen@swin.edu.au  21st July 2004

Results & Analysis: Sasser.A

Accumulative traffic generated by Sasser.A

![Graph showing cumulative traffic](image)

Upstream
- 99.9% TCP
- 1.146 Kbyte/sec
- 3.06 Gbyte/month
- 17% BW (256/64 Kbps)

Max Charge
$458 / month

CAIA Seminar  http://www.caiainternet.ac.uk  jinguyen@swin.edu.au  21st July 2004
## Results & Analysis: Lovesan

### Type
- **Virus:** Blaster variant, exploit MS NETBIOS vulnerability

### Source Port
- Increment by 1, **69** (TFTP)

### Destination Address
- 1. In 3 of 5 cases the worm chooses a random "base IP address" (A.B.C.D) where D is set to zero and A,B,C are random selected from range 1-255. So the base address is in range: [1-255],[1-255],[1-255],[0].
- **In the experiment:** 175.200.[35-103].[0-255]
- 2. In 2 of 5 cases the worm scans subnet: the worm gets local machine IP address (A.B.C.D) sets D to zero and modifies C.

### Destination Port
- **135** (emap), **4444** (to transfer worms)

### Propagation Mechanism
- 1. The worm sends a buffer-overrun request to TCP port **135** to a vulnerable victim machine. If this succeeds, the victim machine starts a command shell on **4444** TCP port.
- 2. The worm runs the thread that opens the connection on port **4444** and waits for FTP "get" request from victim machine.
- 3. The worm then sends a special request to the victim machine to force it to send this "FTP get" request to downloads the worm copy from infected machine, and then activated it.

### Traffic Profile

**Blackhole mode**

#### ACK/RST packets returned

![Graph showing ACK/RST packets returned](image-url)
Results & Analysis: Lovesan

| Upstream          | 0.7 Kbytes/sec  
|                  | 1.86 Gbytes/month  
|                  | 10.3% BW (256/64 Kbps)  
| Max Charge       | $279 / month  

| Upstream          | 2 Kbytes/sec  
|                  | 30.5% BW (256/64 Kbps)  
| Downstream        | 2 Kbytes/sec  
|                  | 7.7% BW (256/64 Kbps)  
| Max Charge        | 11.13 GB  
|                  | $2320 / month  

Results & Analysis: MyDoom.E

| Type                          | Worm: can do mass mailing / DoS attack  
|-------------------------------|---------------------------------------  
| Source Port                   | Increment by 1, 1080 for backdoor access  
| Destination Address           | 1. Mass mailing to email addresses found on the infected machine or random name @ popular public domain. 
|                               | kaiser@acm.org,shipmana@acm.org,skiingprep@angelfire.com  
|                               | 2. DoS attack (between 17th and 22nd of the month) targeting at origin2.microsoft.com  
| Destination Port              | 25 (smtp-mass mailing), 80 (http-DoS attack/multiple GET)  
| Propagation Mechanism         | 1. Query MX record of recipient's email server IP address  
|                               | 2. Use its own SMTP engine to construct outgoing messages with attached copy of viruses and send it directly to the recipient's email server. 
|                               | Email Subject: generated from a list e.g: Read it immediately!, Important, Acident, For you, Expired Account. etc  
|                               | Attachment: details.zip, notes.zip, product.zip .etc.  

CAIA Seminar  http://www.caia.swin.edu.au  jnguyen@swin.edu.au  21st July 2004
Results & Analysis: MyDoom.E

Traffic Profile

Mass mailing mode (Blackhole)

Mass mailing mode - (smtp conn established)

DoS attack mode (Blackhole)

DoS attack mode - (http connection established)
Results & Analysis: MyDoom.E

Upstream
52.02% DNS request
0.15 Kbytes/sec
0.38 Gbytes/month
2.2% BW (256/64 Kbps)
Max Charge
$57 / month

Upstream
56% SMTP, 9% DNS
5.78 Kbytes/sec
15.47 Gbytes/month
78.8% BW (256/64 Kbps)
Max Charge
$2320 / month

Upstream
99.4% TCP
0.72 Kbytes/sec
1.9 Gbytes/month
9% BW (256/64 Kbps)
Max Charge
$285 / month

Upstream
23.67 Kbytes/sec
100% BW (256/64 Kbps)

Downstream
27(>709) Kbytes/sec
100% BW (256/64 Kbps)
Max Charge
$19500/month for 130 Gbytes
Results & Analysis: NetSky.R

<table>
<thead>
<tr>
<th>Type</th>
<th>Worm: Mass mailing (similar to myDoom)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source Port</strong></td>
<td>Increment by 1, 5554 (FTP server)</td>
</tr>
<tr>
<td><strong>Destination Address</strong></td>
<td>Mass mailing to email addresses found on the infected machine with extension: txt, asp, php, jsp, cgi, htm, html, xml, msg, doc, xls, ppt, etc.</td>
</tr>
<tr>
<td><strong>Destination Port</strong></td>
<td>25 (smtp-mass mailing)</td>
</tr>
<tr>
<td><strong>Propagation Mechanism</strong></td>
<td>1. Query MX record of recipient's email server IP address worldpromoters.com, one.com, email.com, etc.</td>
</tr>
<tr>
<td></td>
<td>2. Use its own SMTP engine to construct outgoing messages with attached copy of viruses and send it directly to the recipient's email server.</td>
</tr>
</tbody>
</table>

Traffic Profile

Blackhole case

![Traffic Profile Graph]

Time(s) vs Traffic(bytes)
Results & Analysis: NetSky.R

Cumulative Traffic generated by NetSky.R

<table>
<thead>
<tr>
<th>Upstream</th>
<th>0.547 Kbytes/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1.45 Gbytes/month</td>
</tr>
<tr>
<td></td>
<td>8% BW (256/64 Kbps)</td>
</tr>
<tr>
<td>Max Charge</td>
<td>$217 / month</td>
</tr>
</tbody>
</table>

Results & Analysis: Gator

<table>
<thead>
<tr>
<th>Type</th>
<th>Adware / Spyware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>1157</td>
</tr>
<tr>
<td>Destination Address</td>
<td>bc2.gator.com; ss.gator.com .etc.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>80 (http)</td>
</tr>
<tr>
<td>Propagation Mechanism</td>
<td>Bundled with software like DivX player; ask for downloading and installation from website</td>
</tr>
<tr>
<td>Characteristic</td>
<td>GAIN displays lots of pop-up advertising. It also gather extensive details about user’s computer setup and browsing habits.</td>
</tr>
</tbody>
</table>
"While we don't know the identity of GAIN-Supported Software users, the GAIN AdServer and TGC collect and use the following kinds of anonymous information: Some of the Web pages viewed; The amount of time spent at some Web sites; Response to GAIN Ads; Standard web log information (excluding IP Addresses) and system settings; What software is on the personal computer; First name, country, city, and five digit ZIP code; Non-personally identifiable information on Web pages and forms; Software usage characteristics and preferences."
### Results & Analysis: Gator

**Cumulative Traffic generated by Gator**

<table>
<thead>
<tr>
<th>Downstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>62 bytes/sec</td>
</tr>
<tr>
<td>150 Mbytes/month</td>
</tr>
<tr>
<td>0.2% BW (256/64 Kbps)</td>
</tr>
<tr>
<td><strong>Max Charge</strong></td>
</tr>
<tr>
<td>$22 / month</td>
</tr>
</tbody>
</table>

---

### Results & Analysis: SpyBot

<table>
<thead>
<tr>
<th>Type</th>
<th>P2P worm / Keylogger. More than 1000 variant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Random</td>
</tr>
<tr>
<td>Destination Address</td>
<td>List of IRC server IP addresses</td>
</tr>
<tr>
<td>Destination Port</td>
<td>6667 (IRC)</td>
</tr>
</tbody>
</table>
| Propagation Mechanism | 1. The worm copies itself "kazaabackupfiles" subdirectory. Copies have enticing names (like "porn.exe", "Matrix Screensaver 1.5.scr", "Smart Ripper v2.7.exe", etc.) so other people may download the worm through P2P file sharing program. Once the downloaded copy of the worm is executed the cycle repeats itself.  
2. Access several IRC servers to report successful infection via a built-in IRC channel. Connects to specified IRC servers and joins a channel to receive commands. (DoS attacks, copy itself to hardcoded Windows folders)  
3. Presence of a short text file in the Windows folder (frequently -"keylog.txt") that holds current user's keylogging records |
Key logger

[13:23:14] [CTRL] (Changed window)
[13:29:04] C:\WINDOWS\System32\cmd.exe - fport -a [Up] (Return)
[13:34:17] Save Process Explorer Data... [Process] (Changed window)
[13:43:28] C:\\John\Spybot [Print Screen] (Changed window)
[13:47:37] C:\WINDOWS\System32\cmd.exe - netstat [Up] (Return)
[13:47:45] C:\WINDOWS\System32\cmd.exe - netstat [Up] (Return)
[13:48:22] C:\WINDOWS\SYSTEM32\kaazaabackupfiles [F5] (Changed window)

Results & Analysis: SpyBot

Traffic Profile

![Traffic Profile Graph]

CAIA Seminar http://www.caia.swin.edu.au  jnguyen@swin.edu.au 21st July 2004
**Results & Analysis: SpyBot**

![Cumulative Traffic Generated by SpyBot](image)

<table>
<thead>
<tr>
<th>Upstream</th>
<th>0.344 Kbytes/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.91 Gbytes/month</td>
</tr>
<tr>
<td></td>
<td>5% BW (256/64 Kbps)</td>
</tr>
<tr>
<td>Max Charge</td>
<td>$136 / month</td>
</tr>
</tbody>
</table>

**Results & Analysis: SubSeven**

<table>
<thead>
<tr>
<th>Type</th>
<th>Trojan Horse (Backdoor.SubSeven family)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Depends on the trojan, can be set as any number</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Victim’s IP address</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Depends on the trojan, can be set as any number</td>
</tr>
<tr>
<td>Propagation Mechanism</td>
<td>There is software package to create the server component of the worm. The icon of the server can be changed. Server .exe file can be binded with other files (mp3, jpeg,etc) and icq can be set to notify hacker when victim first run it.</td>
</tr>
<tr>
<td>Characteristic</td>
<td>When the server portion of the program runs on a computer, the individual who is remotely accessing the computer can do the following:</td>
</tr>
<tr>
<td></td>
<td>- Set it up as an FTP server</td>
</tr>
<tr>
<td></td>
<td>- Browse/Delete files on that system</td>
</tr>
<tr>
<td></td>
<td>- Capture real-time screen information</td>
</tr>
<tr>
<td></td>
<td>- Open and close programs</td>
</tr>
<tr>
<td></td>
<td>- Edit information in currently running programs</td>
</tr>
<tr>
<td></td>
<td>- Remotely restart a computer</td>
</tr>
<tr>
<td></td>
<td>- Edit the registry information</td>
</tr>
</tbody>
</table>
Results & Analysis: SubSeven

Program to create SubSeven Trojan

Control Program

Traffic Profile

0 0.000136 136.186.229.243 136.186.229.251 TCP 60 1333 > 1119 (ACK) Seq=12239 Ack=5
42 0.000150 136.186.229.243 136.186.229.251 TCP 75 1129 > 1133 (ACK) Seq=6229 Ack=5
43 0.000194 136.186.229.243 136.186.229.251 TCP 2293 1333 > 1119 (ACK) Seq=91963 Ack=5
45 0.000246 136.186.229.251 136.186.229.243 TCP 75 1128 > 1132 (ACK) Seq=12344 Ack=3
46 0.000289 136.186.229.243 136.186.229.251 TCP 50 1120 > 1131 (ACK) Seq=7867 Ack=32
47 0.026455 136.186.229.243 136.186.229.251 TCP 2293 1333 > 1119 (ACK) Seq=31205 Ack=5
48 0.026455 136.186.229.243 136.186.229.251 TCP 2293 1333 > 1119 (ACK) Seq=31789 Ack=5
49 0.026455 136.186.229.243 136.186.229.251 TCP 1229 1333 > 1119 (ACK) Seq=31831 Ack=5
50 0.026455 136.186.229.243 136.186.229.251 TCP 2293 1333 > 1119 (ACK) Seq=31895 Ack=5
51 0.026455 136.186.229.243 136.186.229.251 TCP 2293 1333 > 1119 (ACK) Seq=31945 Ack=5
52 0.026455 136.186.229.243 136.186.229.251 TCP 1229 1333 > 1119 (ACK) Seq=31995 Ack=5

You have been infected with Sub733000.

http://www.caia.swin.edu.au  jnguyen@swin.edu.au 21st July 2004
Results & Analysis: SubSeven

Acumulative Traffic Generated by SubSeven

<table>
<thead>
<tr>
<th>Upstream</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.346 Kbytes/sec</td>
</tr>
<tr>
<td>0.91 Gbytes/month</td>
</tr>
<tr>
<td>8% BW (256/64 Kbps)</td>
</tr>
</tbody>
</table>

Max Charge

$137 / month

Can be substantial if victim instructed to download files or function as FTP Server

Conclusion: Load Comparison

Acumulative Traffic generated in one hour

<table>
<thead>
<tr>
<th>Total Traffic [Mb]</th>
<th>Time [1 hour]</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- Sasser.a
- Lovesan.a (Blackhole)
- Lovesan.a (RST/ACK)
- MyDoom.e (Blackhole)
- MyDoom.e (ACK)
- MyDoom.e (DoS/Blackhole)
- MyDoom.e (DoS/ACK)
- NetSky.r
- Gator
- SpyBot
- SubSeven
Conclusion: Load Comparison

![Load Comparison Chart]

Conclusion: Financial Impact

![Financial Impact Chart]
Conclusion: Financial Impact

<table>
<thead>
<tr>
<th>Service</th>
<th>Days Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gator</td>
<td>31</td>
</tr>
<tr>
<td>MyDoom.e (Mass mailing/Blackhole)</td>
<td>31</td>
</tr>
<tr>
<td>Spy Bot</td>
<td>31</td>
</tr>
<tr>
<td>SubSeven</td>
<td>31</td>
</tr>
<tr>
<td>NetSky:1</td>
<td>21</td>
</tr>
<tr>
<td>Lovesan.a (Blackhole)</td>
<td>17</td>
</tr>
<tr>
<td>MyDoom.e (DoS/Blackhole)</td>
<td>16</td>
</tr>
<tr>
<td>Sasser.a</td>
<td>10</td>
</tr>
<tr>
<td>Lovesan.a (RST/ACK)</td>
<td>3</td>
</tr>
<tr>
<td>MyDoom.e (Mass mailing/ACK)</td>
<td>2</td>
</tr>
<tr>
<td>MyDoom.e (DoS/ACK)</td>
<td>1</td>
</tr>
</tbody>
</table>

How many days to use up my monthly quota? (based on Optus ADSL 512/128 1GB Limited Plan)

Conclusion

Researching about network-aware viruses and their traffic patterns can be FUN & REWARDING

Future Research on this topic can contribute to CAIA’s “IP Network security and resilience” research goal

- Defend ourselves from attacks
- Develop Commercial Sandbox Product
- Forensics & Security Auditing work for Businesses and Corporations