Inside "Winnyp"
- Winnyp Internals and Concepts of Network Crawling

Fourteenforty Research Institute, Inc.
http://www.fourteenforty.jp

Senior Software Engineer
Toshiaki Ishiyama
Summary

• Winnyp is an anonymous P2P filesharing software based on Winny.

• Winnyp is compatible with Winny, it can communicate with Winny.

• Encryption key generation algorithm of Winnyp is more difficult than Winny.

• The report of having analyzed Winnyp has not gone up up to now.

• I report on the analytical result of the cryptographic algorithm of Winnyp and the outline of crawling system (WinnypRadar).
Agenda

1. Internal Winnyp.

2. The approaches to the statical analysis for anonymous P2P filesharing systems.

3. WinnypRadar – Winnyp network crawler-
1. Internal Winnyp
Outline of Winnyp

- Winnyp is an anonymous P2P filesharing software based on Winny.
- Winnyp is compatible with Winny. It communicates with Winny protocol. But Winnyp uses original algorithm in encryption key generation process.
Outline of Winnyp

- Winnyp lets the executable file of Winny read winnyp.dll.
- Modified file calls the init function of winnyp.dll.
Outline of Winnyp

- Rewrite instruction for calling init function
Initialization of Winnyp

- Read configuration file for Winnyp (disper.ini)
- Create parameter for generating encryption key
- Create parameter for sending packet
- Patching Winnyp.exe
Initialization of Winnyp

- In the patch processing to Winnyp.exe, the rewriting processing in about 200 places is executed.

- The majority of the rewriting processing are changes in the referred character string. ex) Noderef.txt → Noderefp.txt
Encryption key generation algorithm

- In Winny, we could analyze the cryptographic algorithm easily. Because it's easy.

- In Winnyp, the cryptographic algorithm is RC4. However, the encryption key generation algorithm combines two or more algorithms, and the analysis is difficult.
Encryption key generation algorithm  – Outline –

- Winnyp’s main routine for generating encryption key
- Very complex, very long
Encryption key generation algorithm – Outline –

- The flow which divided by the processing block.
- More complex than Winny.
Encryption key generation algorithm – Stage 1 –

- **SEED**
  - 4 byte
  - 128 byte
  - 64 byte

- **Global value**
  - 4 byte

- **DES**
  - 128 byte

- **Original algorithm #1**
  - 24 byte

- **Original algorithm #2**
  - 92 byte

- **MD5**
  - 16 byte
Encryption key generation algorithm – Stage 2 –

- 64-byte input
- CAST
- 124-byte output
- SHA1
- 20-byte output
- 16-byte output
- Original algorithm #3
- 72-byte output
Encryption key generation algorithm – Stage 3 –

- Original algorithm #4:
  - 1 - 31 byte
  - 20 byte

- RC4:
  - 256 byte

- Global value:
  - 256 byte

- Encryption key:
  - 256 byte
Sending packet

- In winnyp’s packet sending process, add dummy data after winny packet.

- Encryption key generation algorithm is chosen by Winnyp configuration file. (for Winny or Winnyp)

- Dummy data are added when kind of packet is connection establishing or connection closing.

<table>
<thead>
<tr>
<th>Length(4byte)</th>
<th>Data</th>
</tr>
</thead>
</table>

| Length(4byte) | Dara | Dummy |
Sending packet

- Initial packet with dummy bytes
Receiving packet

- Winnyp creates three encryption keys when initialization packet received. (Winny v2.0b7.1, Winnyp v2.1b7.27, Winnyp v2.1b7.28)

- Specifies the version of connected node by using each keys.

- Winnyp can communicate with multiple version by these feature.
Specifying target node

- Decrypt the first 5 bytes.

- Some checks are done to decrypted 5 bytes.

<table>
<thead>
<tr>
<th>Check #</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check #1</td>
<td>Length is greater than 0</td>
</tr>
<tr>
<td>Check #2</td>
<td>Length is less than 131,072</td>
</tr>
<tr>
<td>Check #3</td>
<td>Length plus 4 is less than the receiving packet length</td>
</tr>
<tr>
<td>Check #4</td>
<td>Command number is less than 100</td>
</tr>
</tbody>
</table>

- If all checks was succeeded, the version of connected node was specified.

- If check was failed, checks are done again with other encryption key.
The approaches to the statistical analysis for anonymous P2P filesharing systems
Building analytical environment

• When the P2P application is connected with a usual network, there are a lot of connections, and the analysis is difficult.
• Therefore, the environment that can be communicated by one-on-one is necessary.
Anti debugging, packing

- To improve the anonymity of the P2P software, Anti debugging and packing are given.

- To evade these, it doesn't start by the debugger but it is made to attach by the debugger after the P2P application starts.

- Even if the analysis of initialization flies to some degree, the analysis by this method is possible because it is unquestionable when communication processing is analyzed.
Analysing network process

• Because the execution file cannot be read with IDA Pro, it is difficult to specify communication processing.

• The location where communication processing is done is specified by setting the breakpoint to API, and tracing the stack.

• Specific in the file access part etc. is also possible by a similar method
Guessing encryption algorithm

- Even if the assembly code of the cryptographic algorithm is analyzed, specific of the algorithm is difficult.
- Code Search Engine can be used to guess the cryptographic algorithm.
3. WinnypRadar

- Crawling Winnyp network -
WinnypRadar

- Connect to Winnyp network as one of the Winnyp node.
- Collects "Key information" from connected node by using Winnyp protocol.
- WinnypRadar can connect to both winny node and winnyp node.
Distinction between Winny node and Winnyp node

- There is a possibility including the Winny node in the Winnyp network, because Winnyp has compatibility with Winny.
- In WinnypRadar, the version of connected node is specified based on an initial packet of the connected node.
Collected information

- Collected key information includes file name and IP address.
- What kind of file which IP address has opened to the public can be investigated.

<table>
<thead>
<tr>
<th>IP address</th>
<th>Port</th>
<th>File size</th>
<th>File time stamp</th>
<th>File name</th>
<th>Hash</th>
<th>…</th>
</tr>
</thead>
</table>
Crawling

- IP address in the collected key information is used to the new connection destination.
- Connects at the new connection destination, and key information is acquired.
Result

- Proportion of Winnyp node in Winny network
  - Be judged whether connected node is Winnyp when WinnypRadar connects it, and records.
  - The ratio of Winnyp is calculated from the number of connected all nodes.
- Result of measurement during a day by using WinnypRadar

<table>
<thead>
<tr>
<th>Node count</th>
<th>198,000 node (exclude Port0 setting)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proportion of Winnyp node</td>
<td>8% (16,000 node)</td>
</tr>
</tbody>
</table>

※From analysis result by CROSSWARP, Inc
http://www.scat.or.jp/stnf/contents/p2p/p2p080910_4.pdf
Conclusion

- I analyzed the encryption key generation algorithm and packet processing of Winnyp v2.1b7.28

- In Winnyp, the encryption key generation algorithm is more complex than Winny.

- Develop Winnyp network crawler “WinnypRadar” based on the analytical result.

- The investigation concerning the Winnyp node that was not able to be detected up to now by the use of WinnypRadar became possible.
Further tasks

• This time, because an enough node investigation period was not able to be taken, it is necessary to investigate the node for the long term.

• It seems that a more accurate number of Winnyp nodes can be measured by investigating the node that connects it only with Winnyp though the Winnyp node that was able to be connected with the Winny network was investigated in this investigation.
Thank you!

Fourteenforty Research Institute, Inc.
http://www.fourteenforty.jp

Senior Software Engineer
Toshiaki Ishiyama
ishiyama@fourteenforty.jp