Malware Capture Facility. Scenario
CTU-Malware-Capture-Botnet-31

Sebastian Garcia. sebastian.garcia@agents.fel.cvut.cz

August 5, 2014

General Information about the scenario

- Infected Machines:
  - Windows XP Name: WIN10, IP: 10.0.2.110 (Label: Botnet-V31-1 in the files)
  - Windows XP Name: WIN7, IP: 10.0.2.107 (Label: Botnet-V31-2 in the files)
- Binary Used:
  c740789d5b226668f8a37626883fd0b7.exe
- MD5:
  c740789d5b226668f8a37626883fd0b7
- Probable Name:
  Unknown
- Duration:
  56 days
- VirusTotal Link:
  https://www.virustotal.com/en/file/104428ccf005b36edfb62d110203a43bdbb417052b31eb4646395309

Files

Details about the files used in this scenario.

1 Pcap file: 2013-11-25_capture-win10-2.pcap

1.1 Generic Info

- Number of packets: 24 M
- File size: 8794 MB
- Data size: 8401 MB
- Capture duration: 676444 seconds (7.82921 days)
- Start time: Tue Nov 26 10:23:03 CET 2013
- End time: Wed Dec 4 ??:??:??:CET 2013
- Data byte rate: 12 kBp
- Data bit rate: 99 kbps
- Average packet size: 342.53 bytes
- Average packet rate: 36 packets/se
- Bidirectional flowfile size: 705 MB
- Amount of bidirectional flows: 3,047,145

1.2 Related Files

-

1.3 Weblogs

Description of the weblogs

1.4 Graphs of the traffic with RRD

2 Pcap file: 2013-11-25_capture-win10-3.pcap

2.1 Generic Info

- Number of packets: 11 M
- File size: 4272 MB
- Data size: 4082 MB
- Capture duration: 441355 seconds (5.10828 days)
- Start time: Fri Dec 6 10:53:06 CET 2013

- End time: Wed Dec 11 ??:??:?? CET 2013
- Data byte rate: 9250 bytes/s
- Data bit rate: 74 kbps
- Average packet size: 345.08 bytes
- Average packet rate: 26 packets/sec
- Bidirectional flow file size: 343 MB
- Amount of bidirectional flows: 1,477,663

2.2 Related Files

-

2.3 Weblogs

Description of the weblogs

2.4 Graphs of the traffic with RRD

3 Pcap file: 2013-11-25_capture-win10.pcap

3.1 Generic Info

- Number of packets: 42 M
- File size: 15 GB
- Data size: 14 GB
- Capture duration: 1076464 seconds (12.45907407 days)
- Start time: Tue Nov 12 20:00:29 CET 2013
- End time: Sun Nov 24 ??:??:?? CET 2013
- Data byte rate: 13 kBps
- Data bit rate: 107 kbps
- Average packet size: 342.06 bytes
- Average packet rate: 39 packets/sec
- Bidirectional flow file size: 1.2 GB
- Amount of bidirection flows: 5,148,948

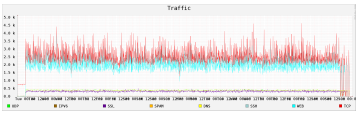
3.2 Related Files

-

3.3 Weblogs

Description of the weblogs

3.4 Graphs of the traffic with RRD



4 Pcap file: 2013-11-25_capture-win7-2.pcap

4.1 Generic Info

- Number of packets:
- File size:
- Data size:
- Capture duration:
- Start time:
- End time:
- Data byte rate:
- Data bit rate:
- Average packet size:
- Average packet rate:
- Bidirectional flow file size:
- Amount of bidirection flows:

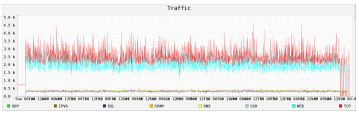
4.2 Related Files

-

4.3 Weblogs

Description of the weblogs

4.4 Graphs of the traffic with RRD



5 Pcap file: 2013-11-25_capture-win7-3.pcap

5.1 Generic Info

- Number of packets:
- File size:
- Data size:
- Capture duration:
- Start time:
- End time:
- Data byte rate:
- Data bit rate:
- Average packet size:
- Average packet rate:
- Bidirectional flow file size:
- Amount of bidirection flows:

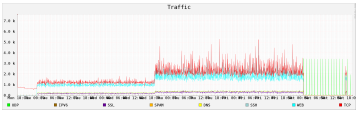
5.2 Related Files

-

5.3 Weblogs

Description of the weblogs

5.4 Graphs of the traffic with RRD



6 Pcap file: 2013-11-25_capture-win7.pcap

6.1 Generic Info

- Number of packets:
- File size:
- Data size:
- Capture duration:
- Start time:
- End time:
- Data byte rate:
- Data bit rate:
- Average packet size:
- Average packet rate:
- Bidirectional flow file size:
- Amount of bidirection flows:

6.2 Related Files

-

6.3 Weblogs

Description of the weblogs

6.4 Graphs of the traffic with RRD

7 Pcap file: 2014-01-10_capture-win10.pcap

7.1 Generic Info

- Number of packets:
- File size:
- Data size:
- Capture duration:
- Start time:

- End time:
- Data byte rate:
- Data bit rate:
- Average packet size:
- Average packet rate:
- Bidirectional flow file size:
- Amount of bidirection flows:

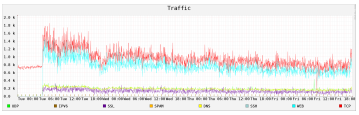
7.2 Related Files

-

7.3 Weblogs

Description of the weblogs

7.4 Graphs of the traffic with RRD



8 Pcap file: 2014-01-10_capture-win7.pcap

8.1 Generic Info

- Number of packets:
- File size:
- Data size:
- Capture duration:
- Start time:
- End time:
- Data byte rate:
- Data bit rate:
- Average packet size:
- Average packet rate:
- Bidirectional flow file size:
- Amount of bidirection flows:

8.2 Related Files

-

8.3 Weblogs

Description of the weblogs

8.4 Graphs of the traffic with RRD

Timeline

Tue Nov 12 20:00:29 CET 2013 start win10

Tue Nov 12 20:12:26 CET 2013 infected win10 with c740789d5b226668f8a37626883fd0b7.exe

Tue Nov 12 20:16:05 CET 2013 started win7

Tue Nov 12 20:17:29 CET 2013 infected win7 with c740789d5b226668f8a37626883fd0b7.exe

Unknown time There was an issue with computer so the vm was powered down.

Tue Nov 26 10:23:03 CET 2013 win10 is powered on again. Already infected. Pcap file: 2013-11-25_capture-win10-2.pcap

Tue Nov 26 10:23:03 CET 2013 win7 vm is powered on again.

Mon Dec 2 13:48:06 CET 2013 running graph with rrd file stopped and started again...

Fri Dec 6 10:48:09 CET 2013 I started win7 again. The linux host was frozzen.

Fri Dec 6 10:53:06 CET 2013 I started win10 again. The linux host was frozzen. Pcap file 2013-11-25_capture-win10-3.pcap

Mon Jan 6 12:48:38 CET 2014 I powered off win10 and started it again infected

Mon Jan 6 12:51:16 CET 2014 I poweredoff the win7 and started again infected.

Traffic Analysis

The traffic pattern of the files 2013-11-25_capture-win7-3.pcap and 2013-11-25_capture-win10-3.pcap are very similar because they are simoultaneous. The

2013-11-25_capture-win7-2.pcap 2013-11-25_capture-win10-2.pcap

2013-11-25_capture-win7.pcap 2013-11-25_capture-win10.pcap

2014-01-10_capture-win10.pcap 2014-01-10_capture-win7.pcap

Analyzying the 4-tuple 10.0.2.107-192.35.51.30-53-tcp we realized that it is a DGA algorithm, using TCP DNS queries to an custom DNS server. The requests are mostly not periodic, and only have a slightly periodicity from time to time. For example: State=11rrrrrArrrrrrrrAArrrrarrrrrrraAArrrAarrArrrrrrrArrbrrrararrrrrrrrrrrrrArrrrrArrrraAA

Furthermore, the time differences of these requests seem to be quite random. So we tested the values of the T1 to see if they follow a distribution. And they seem to be following a distribution.

Disclaimer

These files were generated as part of the Malware Capture Facility Project in the CTU University, Prague, Czech Republic. The goal of the project is to store long-lived real botnet traffic and to generate labeled netflows files. Any question feel free to contact us to sebastian.garcia@agents.fel.cvut.cz.

You are free to use these files as long as you reference this project and the authors. See `http://mcfp.felk.cvut.cz`