Study of Botnet spreading in a Network.

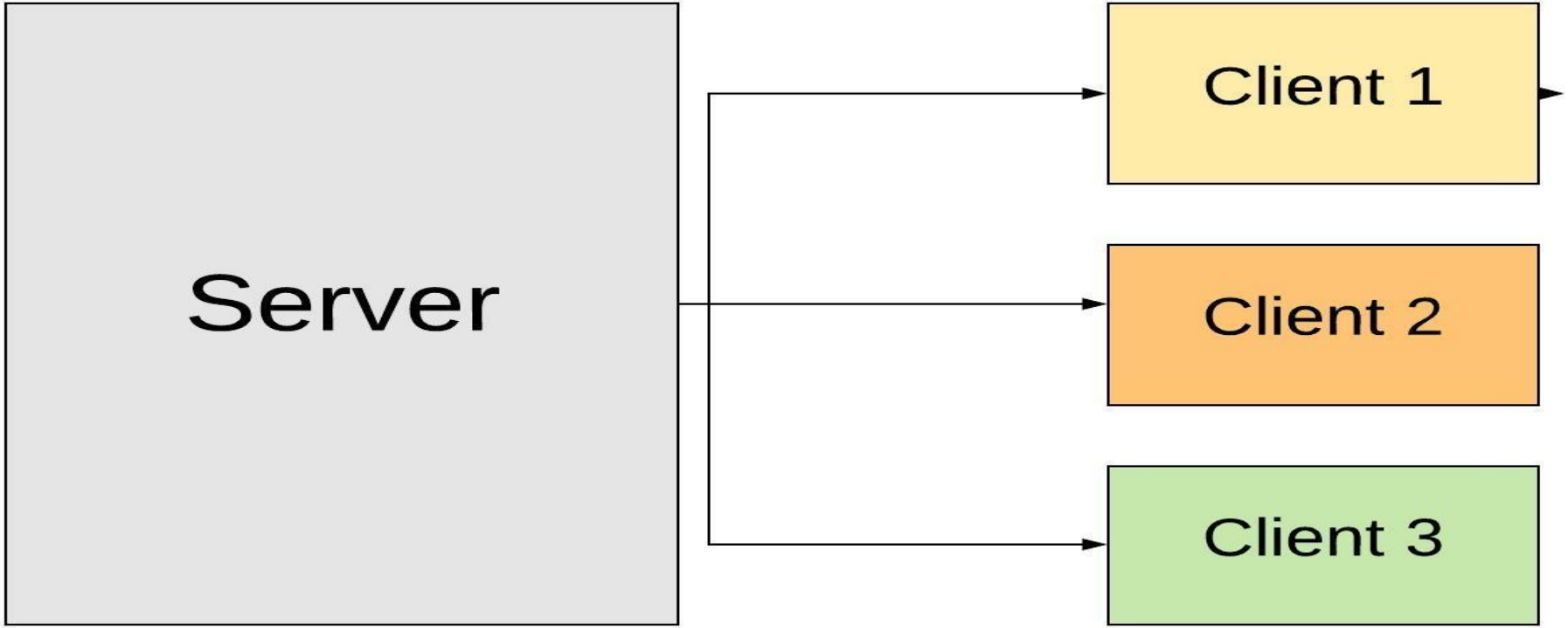
Spreading of zeuS Botnet in a network of Windows Operating system.

What is a Botnet?

- Derived from “robot” and “network”.
- Cybercriminal Performs the role of Botmaster.
- Uses trojan virus to breach the security of the computers.
- Connect the computers into a malicious network.
- Each computer acts as a Bot.
- It is also known as zombie army of computers.

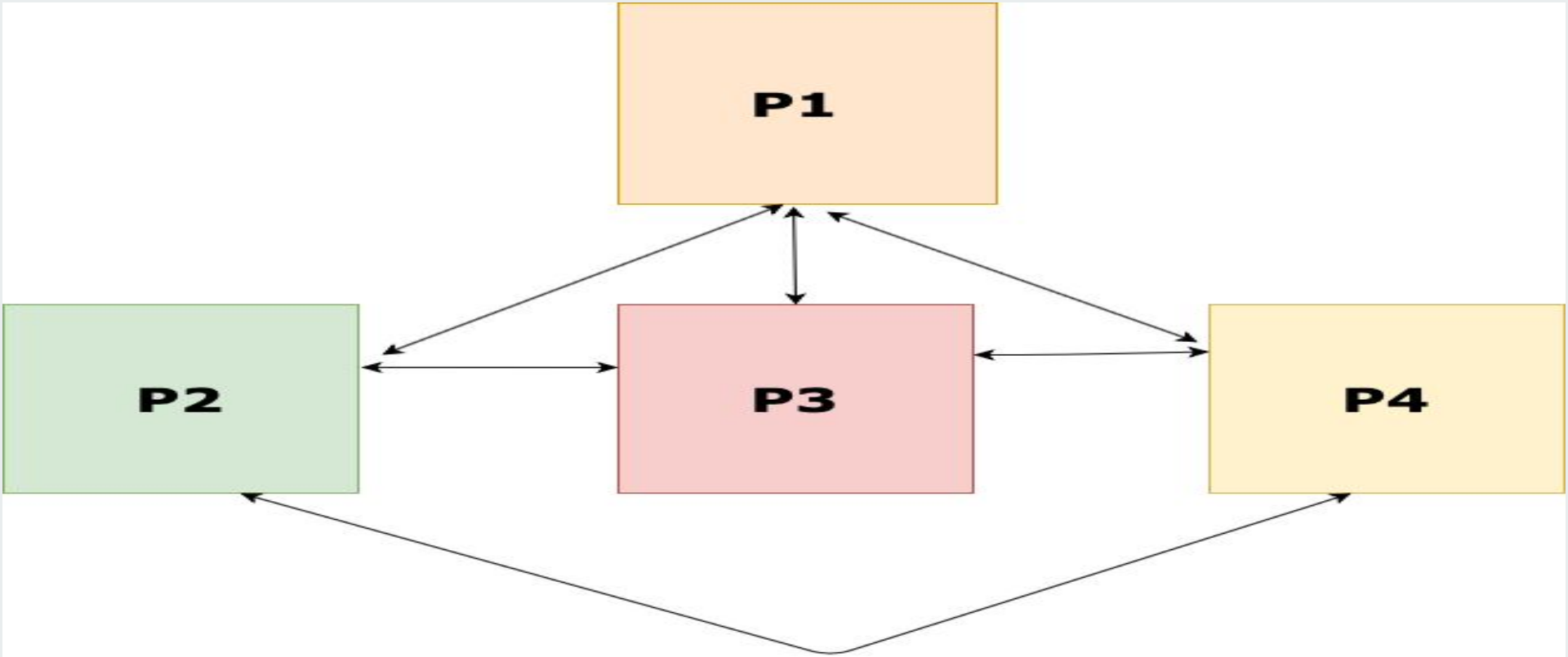
Botnet Structure

1. *Client - Server Model*



Botnet Structure

2. Peer-to-Peer



References

- Sanghamitra De, Mridul Sankar Barik, and Indrajit Banerjee. 2019. A Percolation-based Recovery Mechanism for Bot Infected P2P Cloud. In International Conference on Distributed Computing and Networking (ICDCN ’19), January 4–7, 2019, Bangalore, India. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3288599.3295597

- Qian Chen, and Robert A. Bridges. 2017. Automated Behavioral Analysis of Malware. A Case Study of WannaCry Ransomware.
@misc{chen2017automated, title={Automated Behavioral Analysis of Malware A Case Study of WannaCry Ransomware}, author={Qian Chen and Robert A. Bridges}, year={2017}, eprint={1709.08753}, archivePrefix={arXiv}, primaryClass={cs.CR}}

Problem Definition

Recovery of nodes in a P2P Cloud from botnet attack by running recovery procedures in parallel (to achieve maximum coverage) in separate nodes which can be reached from a given node, using the concept of percolation centrality.

Algorithm Implemented

Algorithm: Recovery procedure to run in each node to recover the node or RECOVERY_PROCEDURE(v).

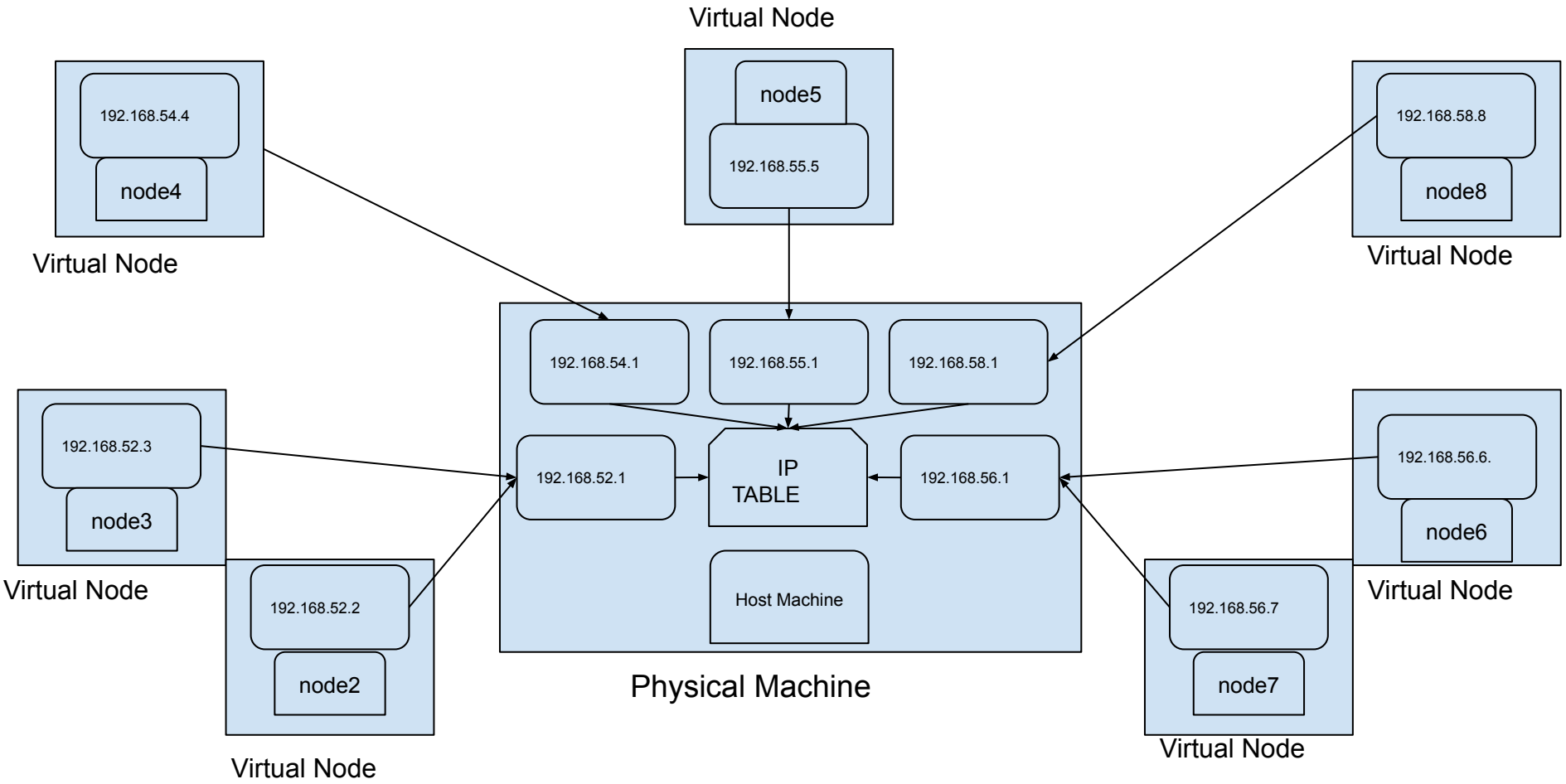
Input: Node under bot attack represented by v

Output: Node recovered from bot attack after running procedure RECOVERY_PROCEDURE.

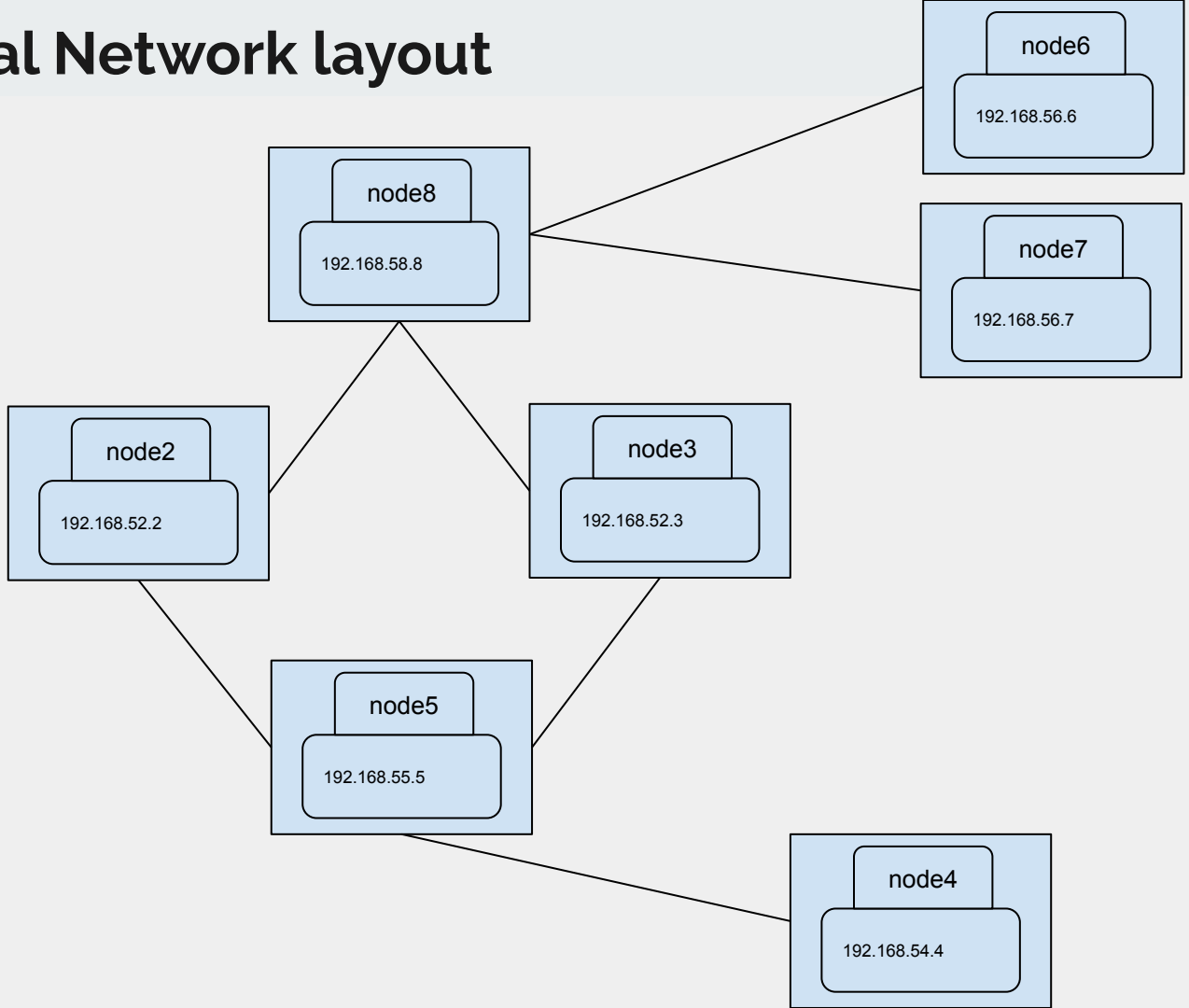
Procedure

```
recover(v)
 if v.isAffected == true:
      v.isAffected=false
      v.loadStableSystemImage()
      for u in v.adjacent:
         recover(u)
```

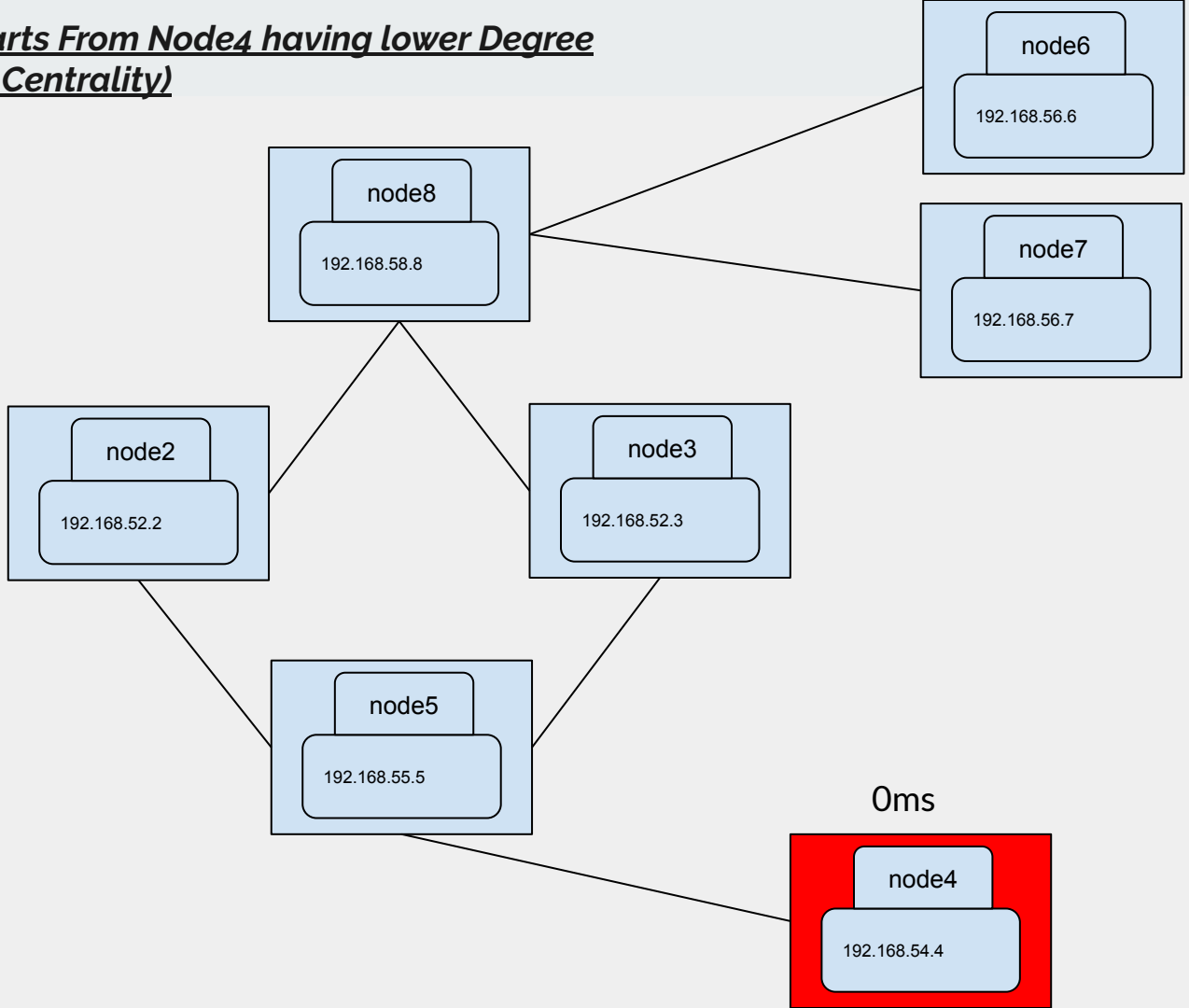
Actual Network Layout



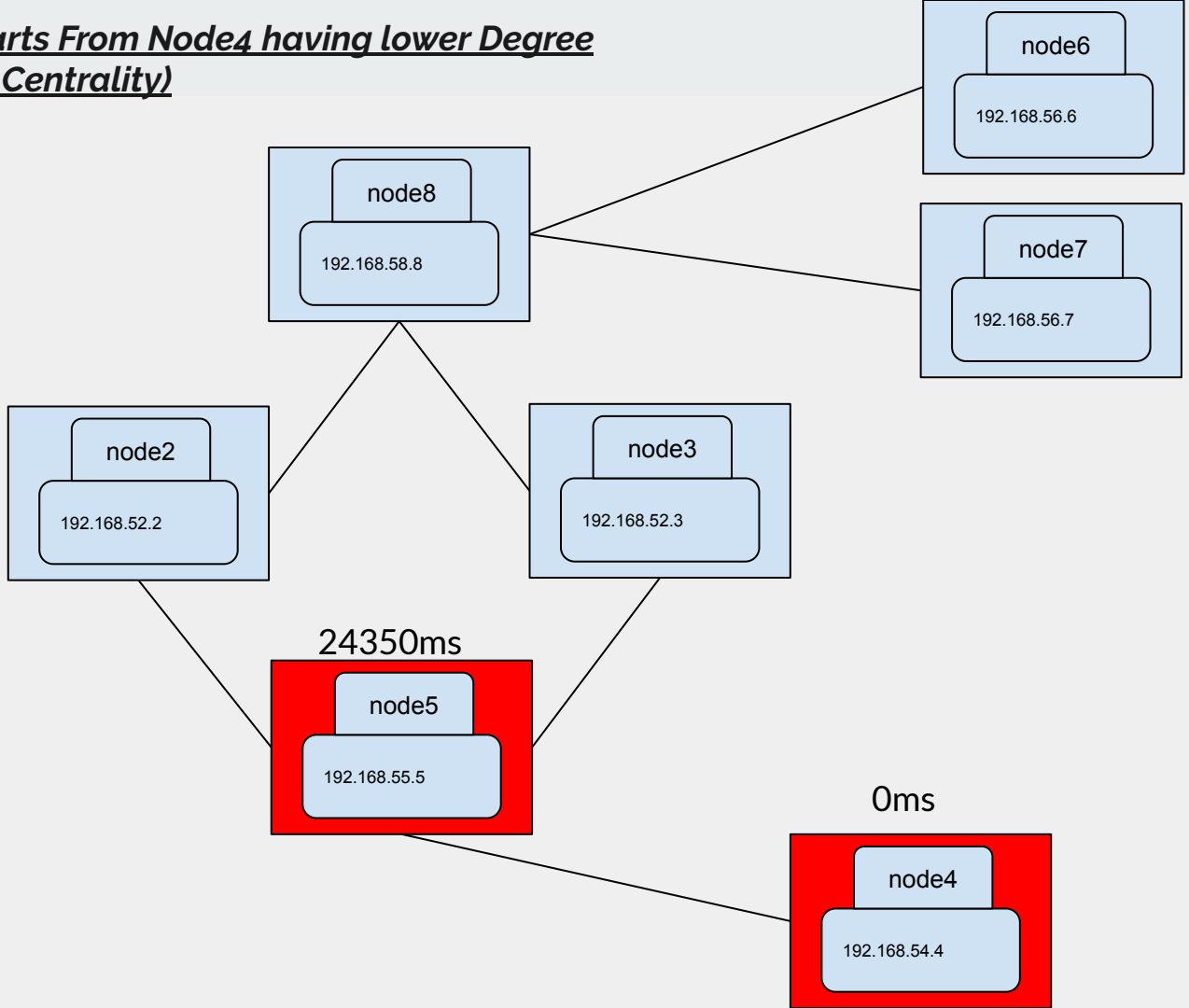
Conceptual Network layout



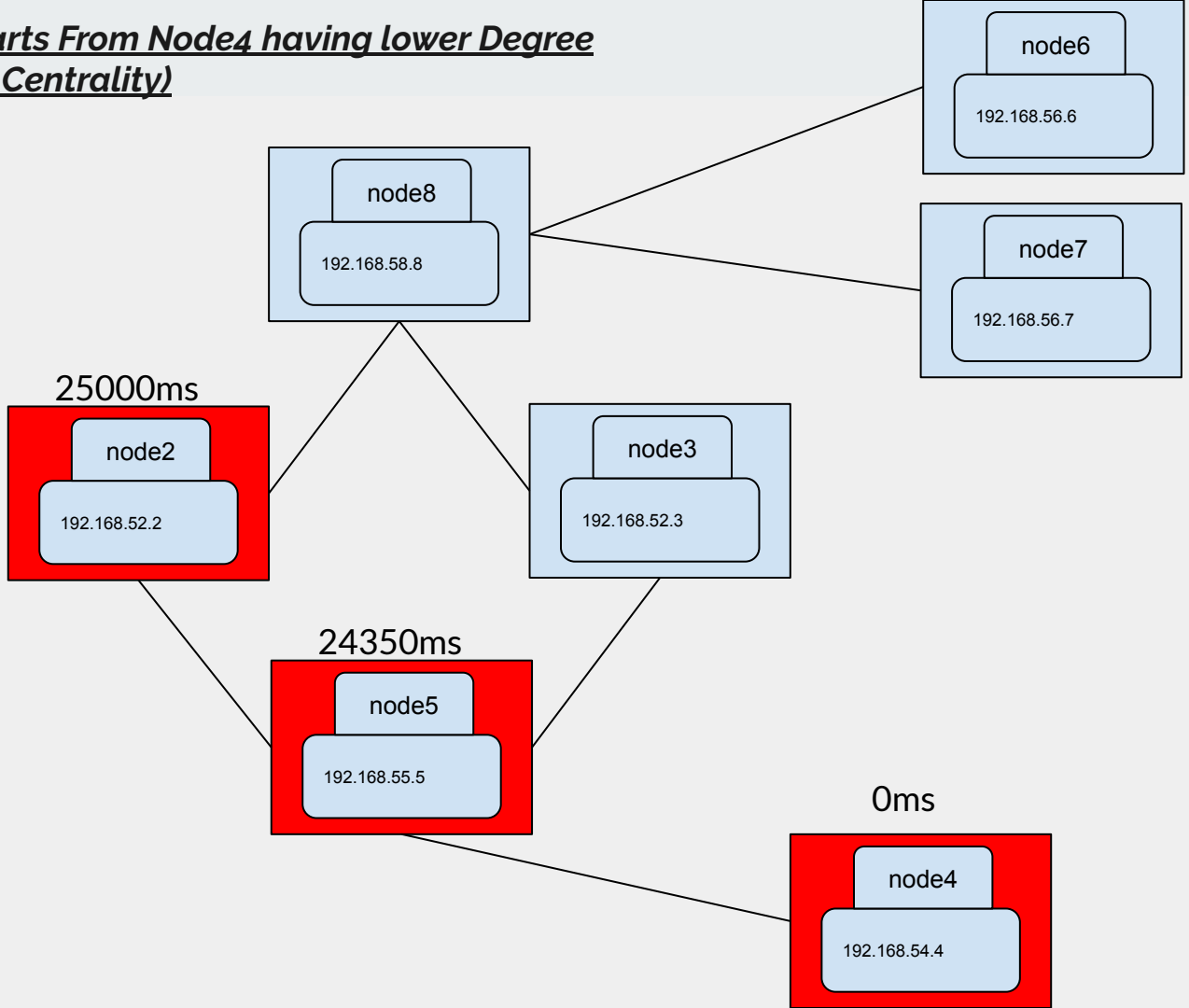
1. ***Recovery Starts From Node4 having lower Degree (Percolation Centrality)***



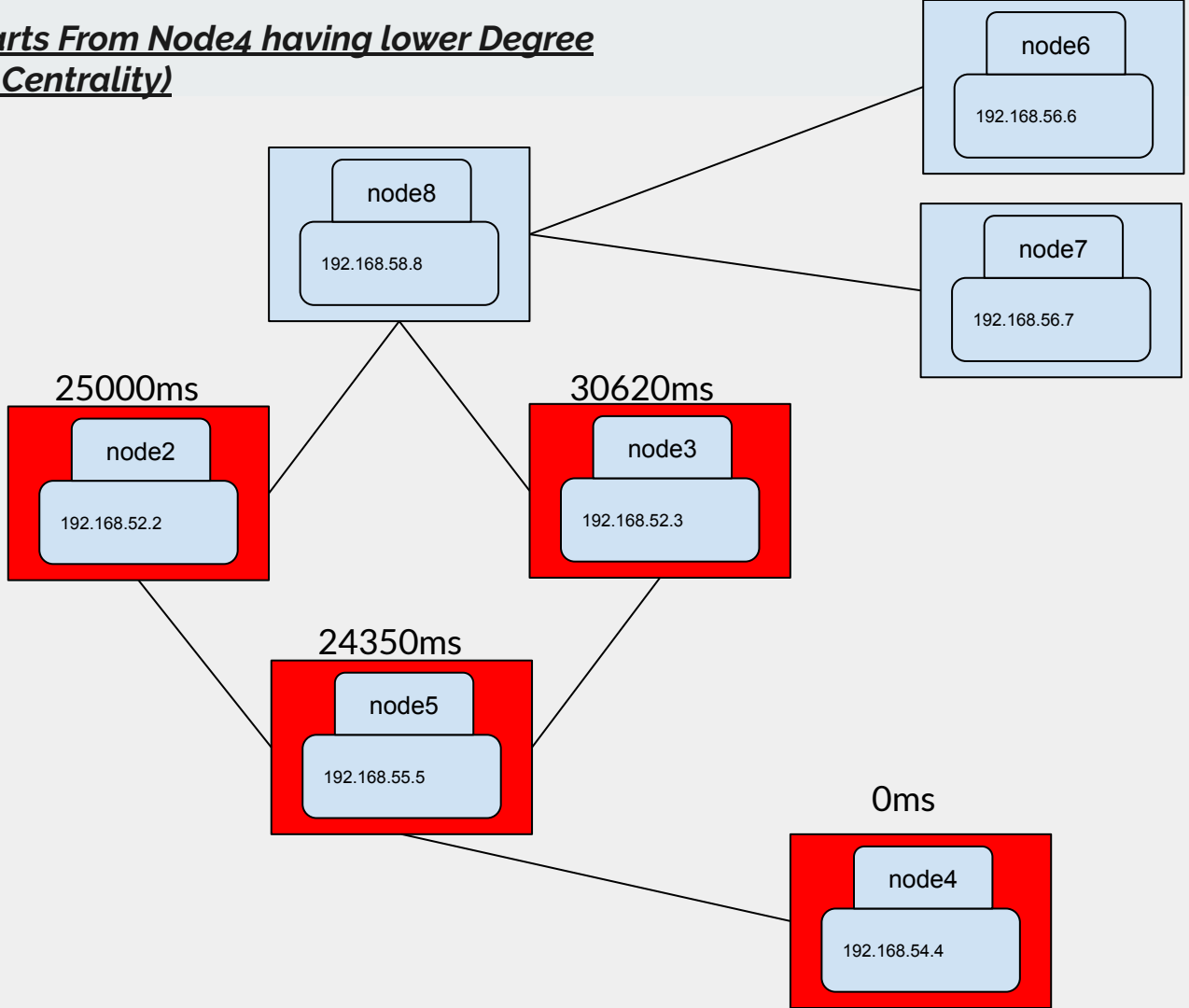
1. ***Recovery Starts From Node4 having lower Degree (Percolation Centrality)***



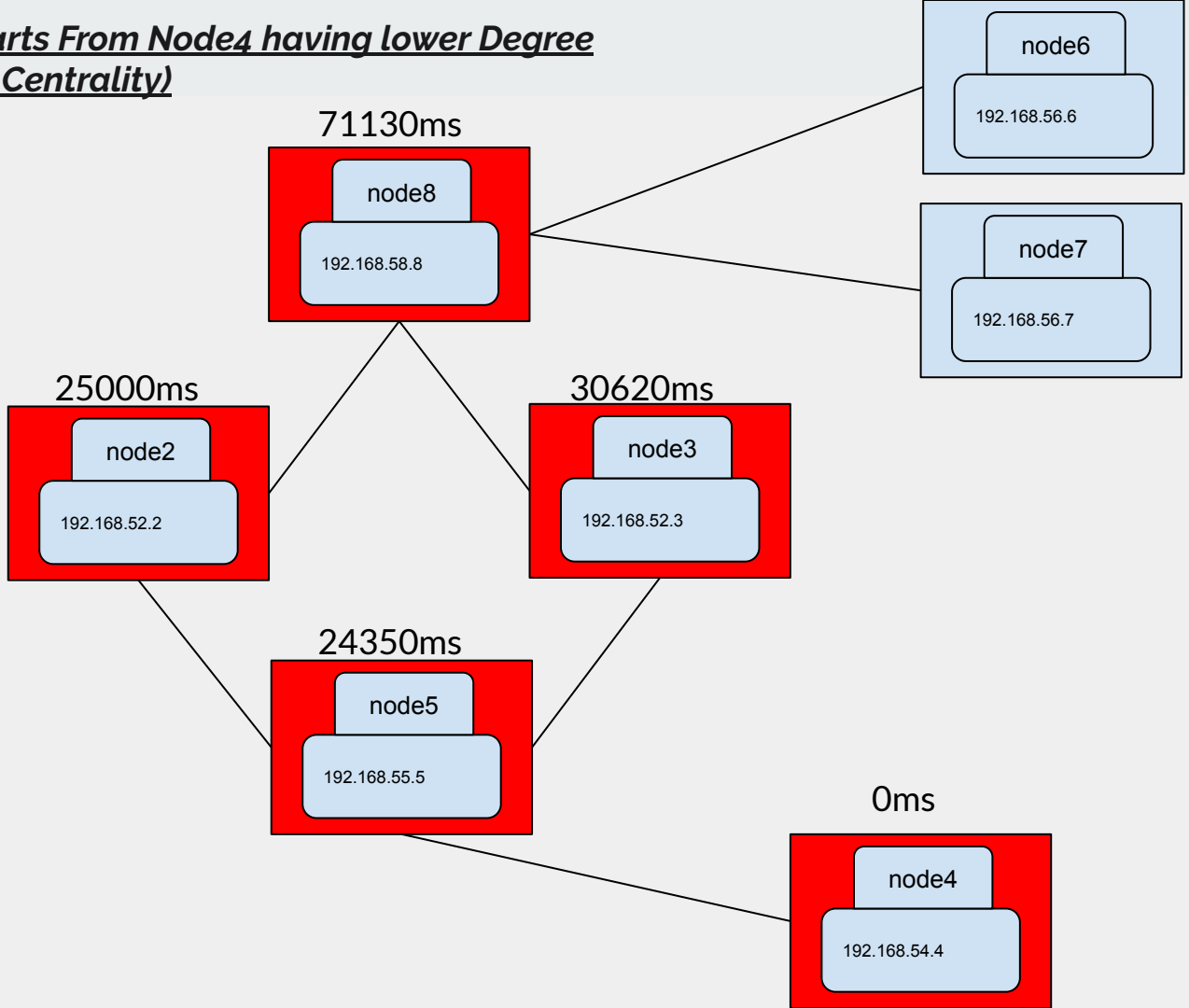
1. ***Recovery Starts From Node4 having lower Degree (Percolation Centrality)***



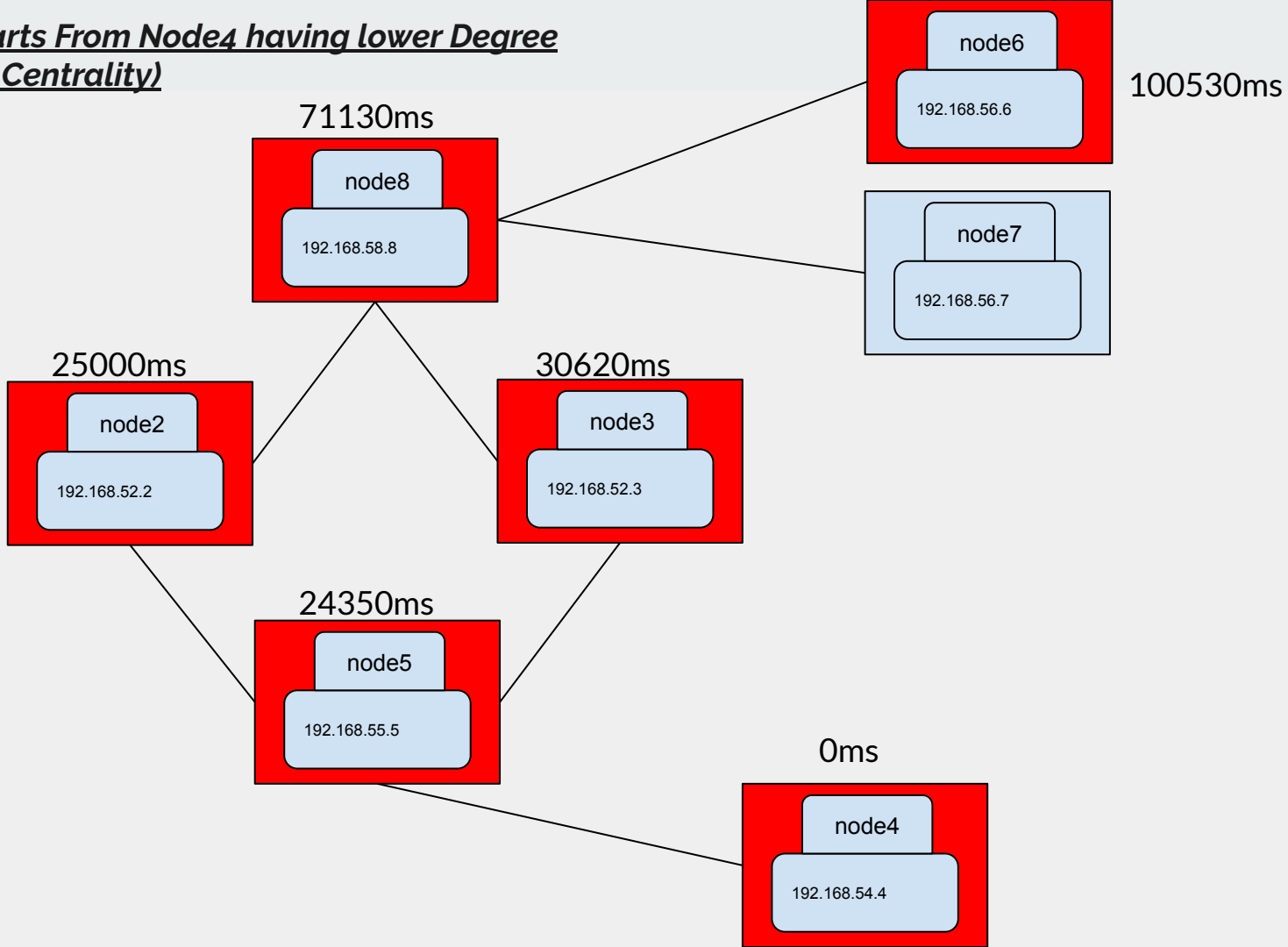
1. ***Recovery Starts From Node4 having lower Degree (Percolation Centrality)***



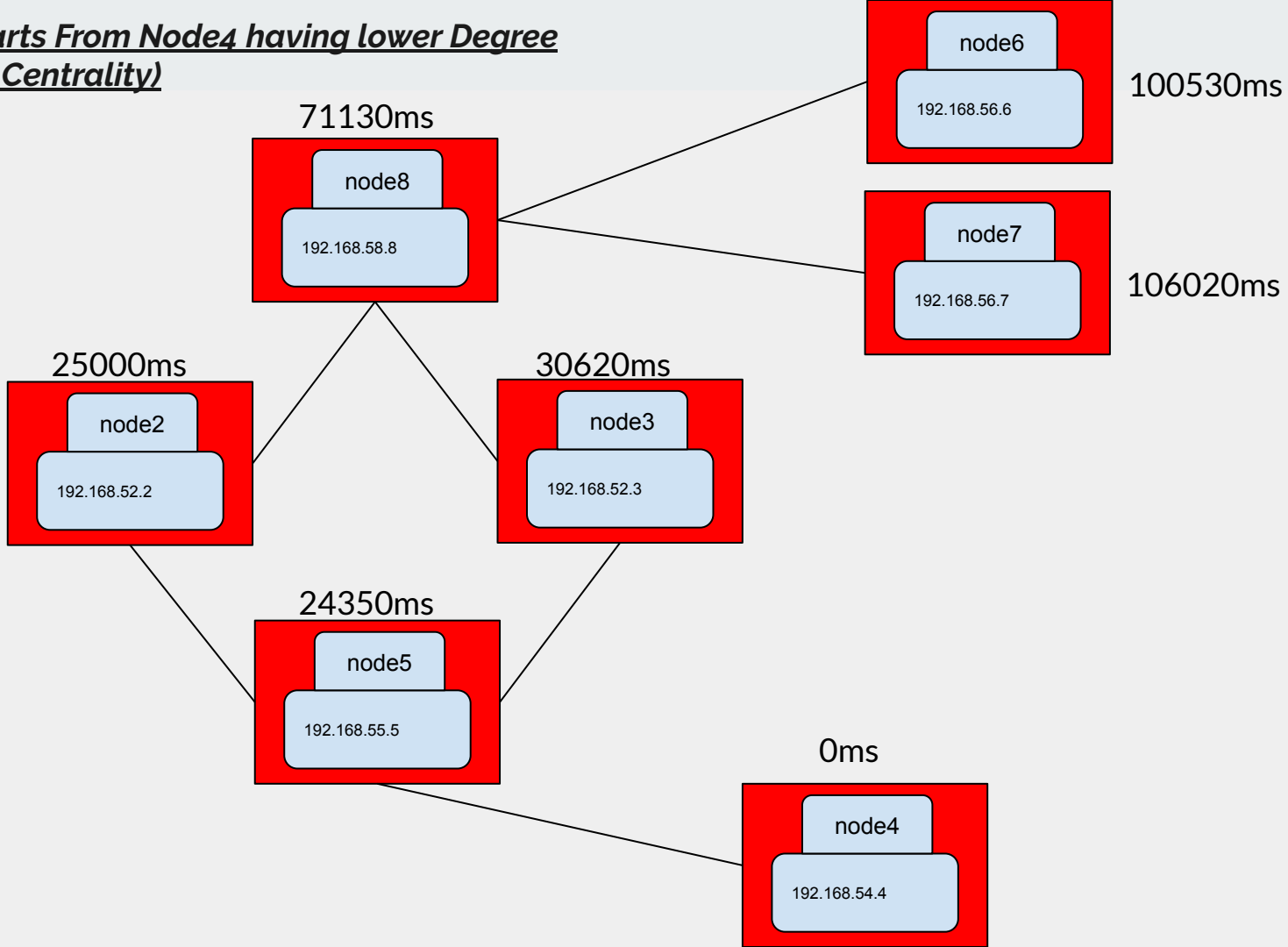
1. ***Recovery Starts From Node4 having lower Degree (Percolation Centrality)***



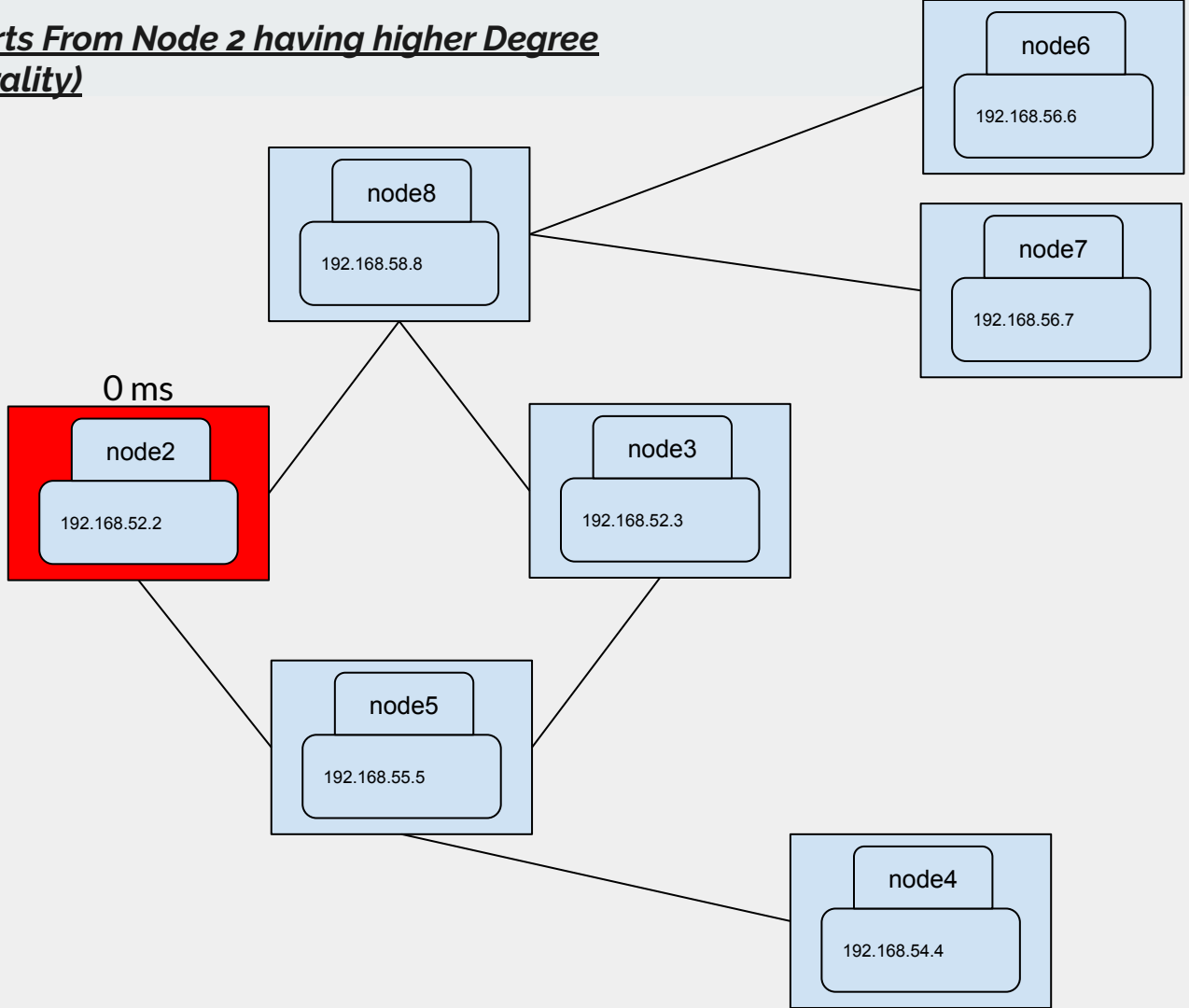
1. ***Recovery Starts From Node4 having lower Degree (Percolation Centrality)***

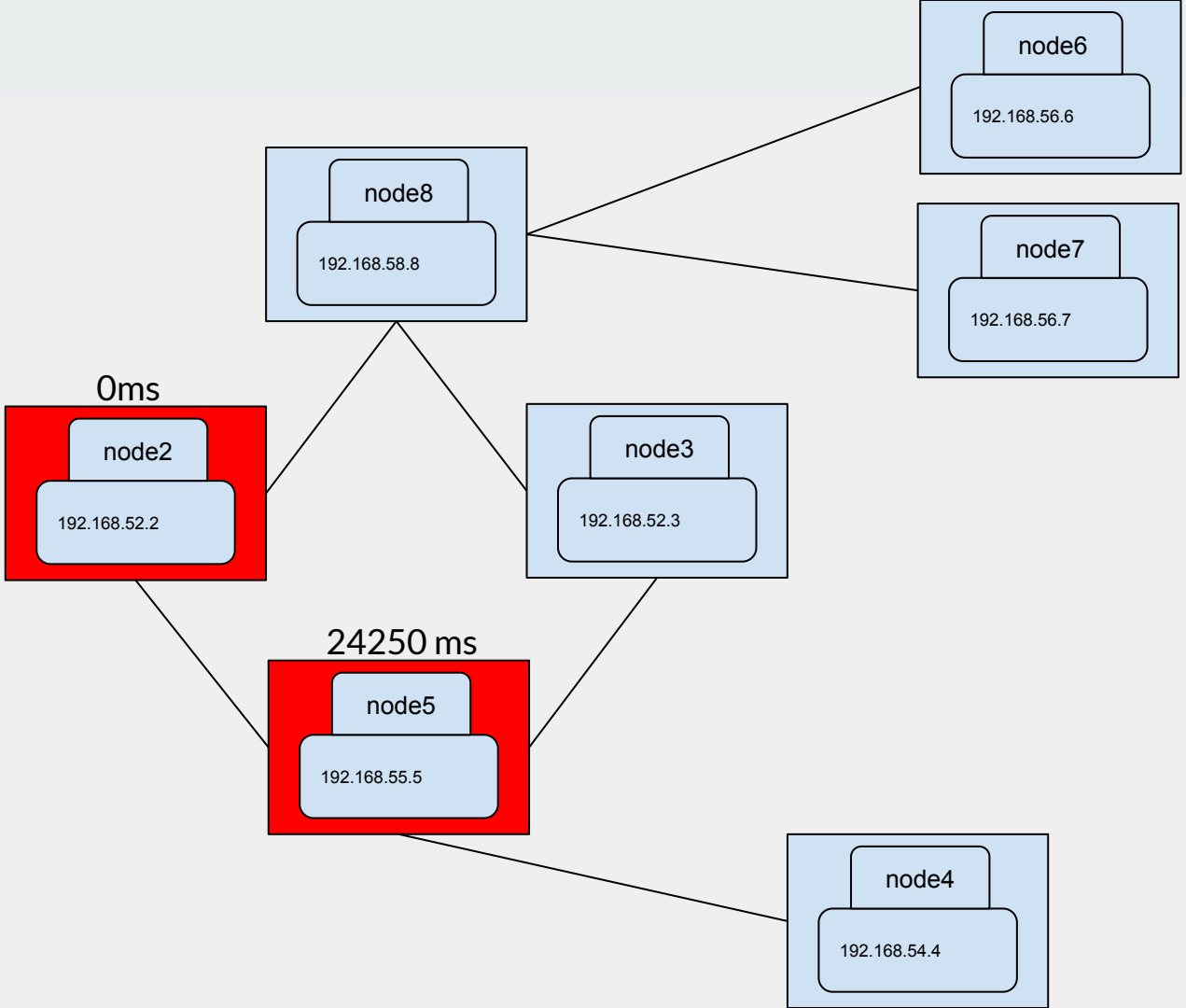


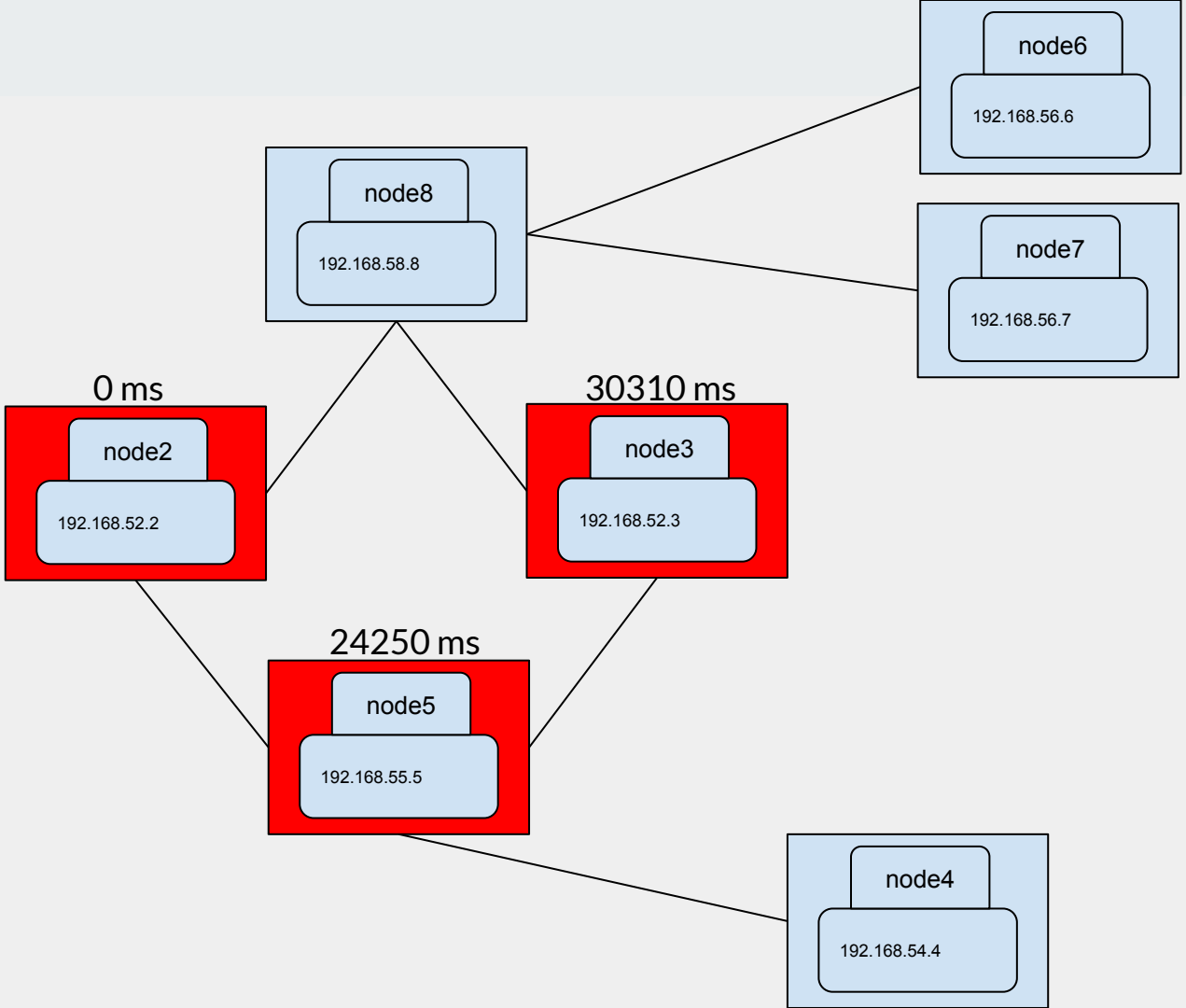
1. ***Recovery Starts From Node4 having lower Degree (Percolation Centrality)***

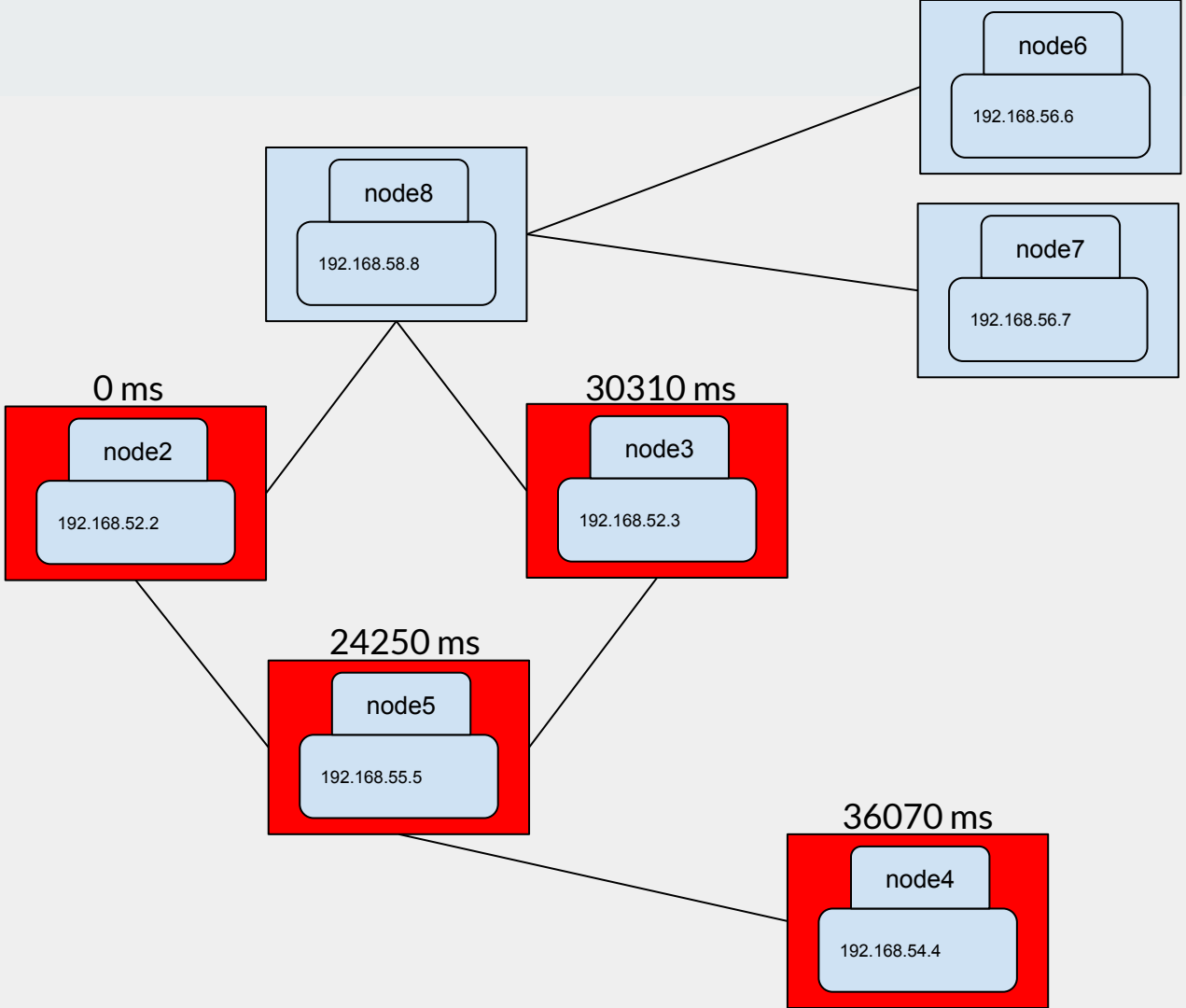


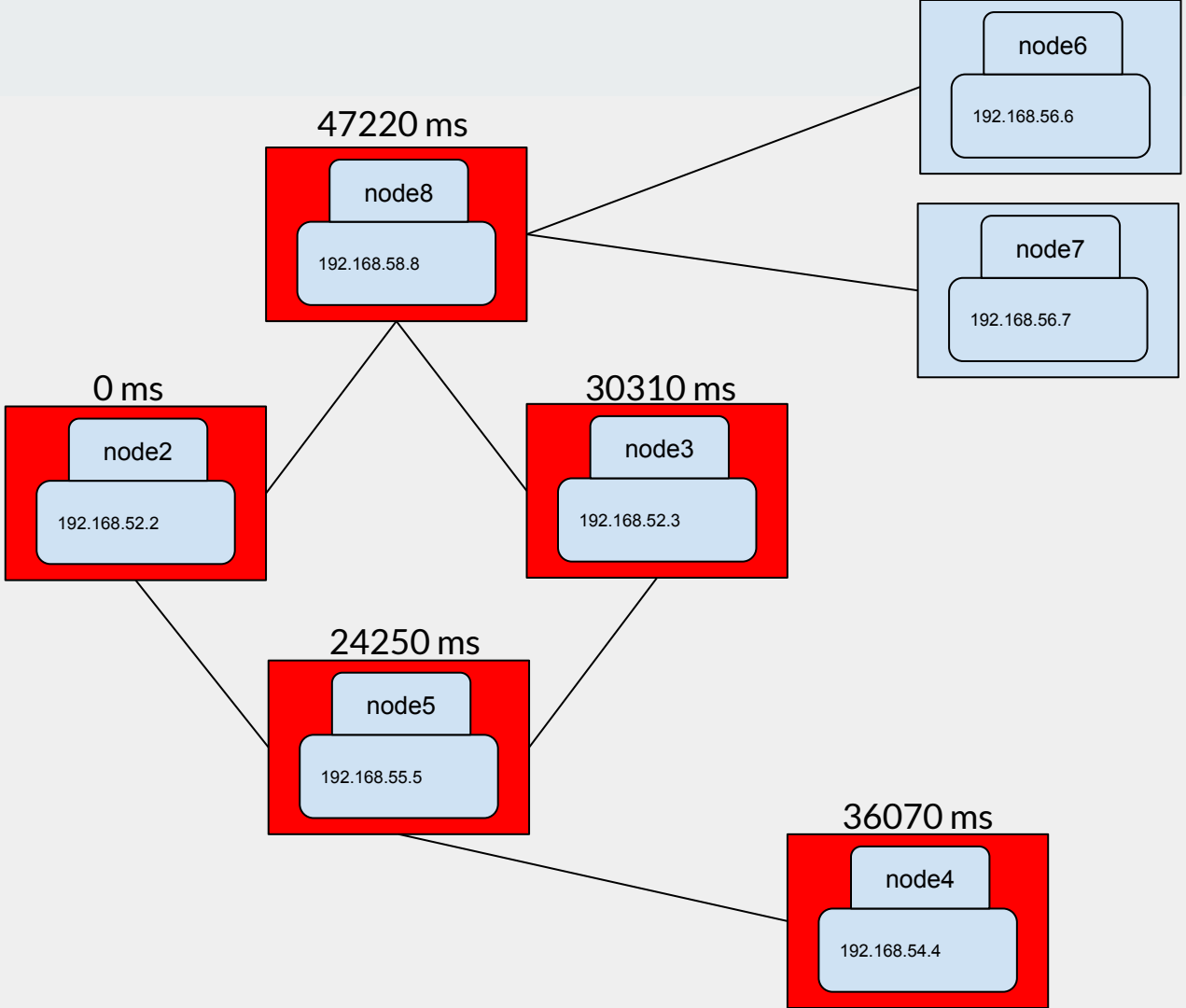
2. ***Recovery starts From Node 2 having higher Degree (Percolation Centrality)***

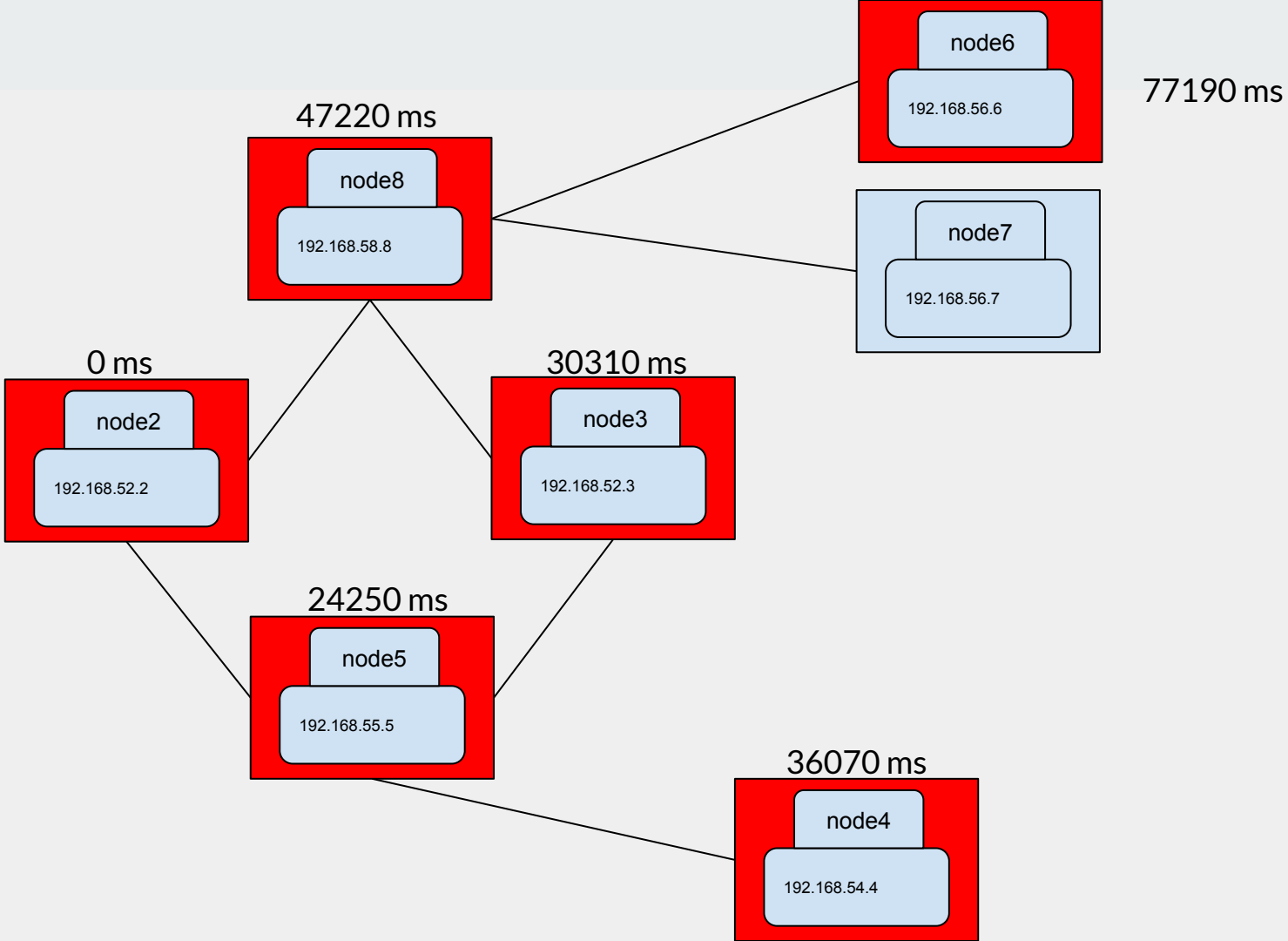


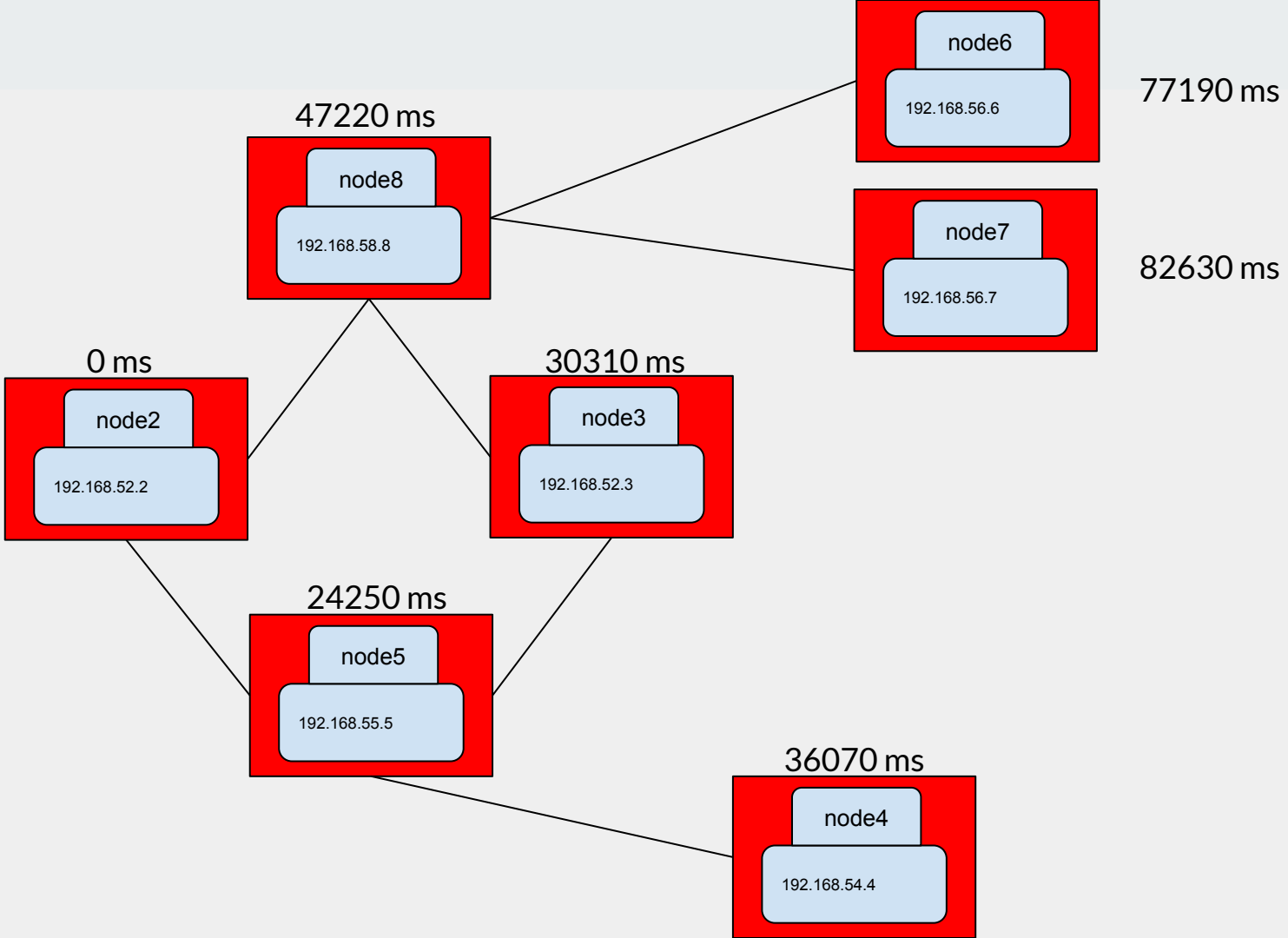

node6
192.168.56.6
node8
192.168.58.8
node7
192.168.56.7
0ms
node2
192.168.52.2
node3
192.168.52.3
24250 ms
node5
192.168.55.5
node4
192.168.54.4


node6
192.168.56.6
node8
192.168.58.8
node7
192.168.56.7
0 ms
node2
192.168.52.2
30310 ms
node3
192.168.52.3
24250 ms
node5
192.168.55.5
node4
192.168.54.4


node6
192.168.56.6
node8
192.168.58.8
node7
192.168.56.7
0 ms
node2
192.168.52.2
30310 ms
node3
192.168.52.3
24250 ms
node5
192.168.55.5
36070 ms
node4
192.168.54.4


node6
192.168.56.6
47220 ms
node8
192.168.58.8
node7
192.168.56.7
0 ms
node2
192.168.52.2
30310 ms
node3
192.168.52.3
24250 ms
node5
192.168.55.5
36070 ms
node4
192.168.54.4

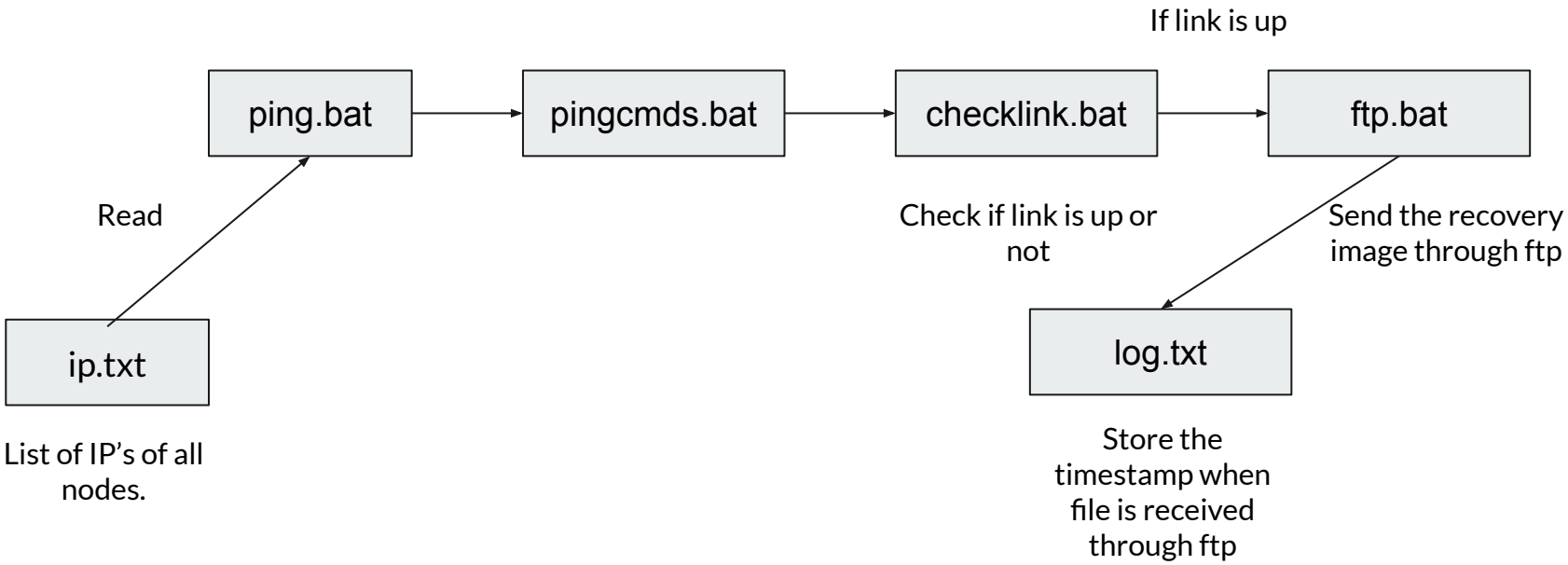

node6
192.168.56.6
77190 ms
47220 ms
node8
192.168.58.8
node7
192.168.56.7
0 ms
node2
192.168.52.2
30310 ms
node3
192.168.52.3
24250 ms
node5
192.168.55.5
36070 ms
node4
192.168.54.4


node6
192.168.56.6
77190 ms
47220 ms
node8
192.168.58.8
node7
192.168.56.7
82630 ms
0 ms
node2
192.168.52.2
30310 ms
node3
192.168.52.3
24250 ms
node5
192.168.55.5
36070 ms
node4
192.168.54.4

[redacted]

How recovery algorithm works

1) Run initiate.bat (background process) on all systems except the starting node. It will keep on checking the receipt status of Desert.jpg (used to emulate the recovery file) in the default ftp folder.



cuckoo Dashboard Recent Pending Search Submit Import

Dropped Files

Name	**6512ae8283fa41e4_5c2c622f-70e9-4194-a7da-033e827365ad** Download Submit file
Filepath	C:\Windows\System32\LogFiles\Scm\5c2c622f-70e9-4194-a7da-033e827365ad
Size	12.0B
Processes	452 (**services.exe**)
Type	MS Windows COFF PA-RISC object file
MD5	bbb8002da3b8be76f88202765ab728a1
SHA1	910e5cbe220b6e3cf1fb2e653bf8ea126544b674
SHA256	6512ae8283fa41e470480593ad1456d84680196595473e545d987bd06f0f3828
CRC32	2B39C8C1
ssdeep	None
Yara	None matched
VirusTotal	Search for analysis

Name	**69e966e730557fde_googleupdate.exe** Download Submit file
Filepath	C:\Program Files\Google\Desktop\Install\{4d567297-202f-6c92-8f4d-ca7703cdfb60}\ \...\exe.etadpUelgooG\{06bfdc3077ac-d4f8-29c6-f202-792765d4}\
Size	247.0KB
Processes	2352 (**invoice_2318362983713_823931342io.pdf.exe**)
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	ea039a854d20d7734c5add48f1a51c34
SHA1	9615dca4c0e46b8a39de5428af7db060399230b2
SHA256	69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
CRC32	B6012D5E
ssdeep	None
Yara	None matched
VirusTotal	Search for analysis

Name	**4ec923270db17db7_edbtmp.log** Download Submit file

1. These are the downloaded files which are referred to as Dropped files. These files are downloaded automatically from random servers and may be malicious.

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

Sign in

61 / 69

Community Score

61 engines detected this file

69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169

myfile.exe

peexe via-tor

247 KB Size

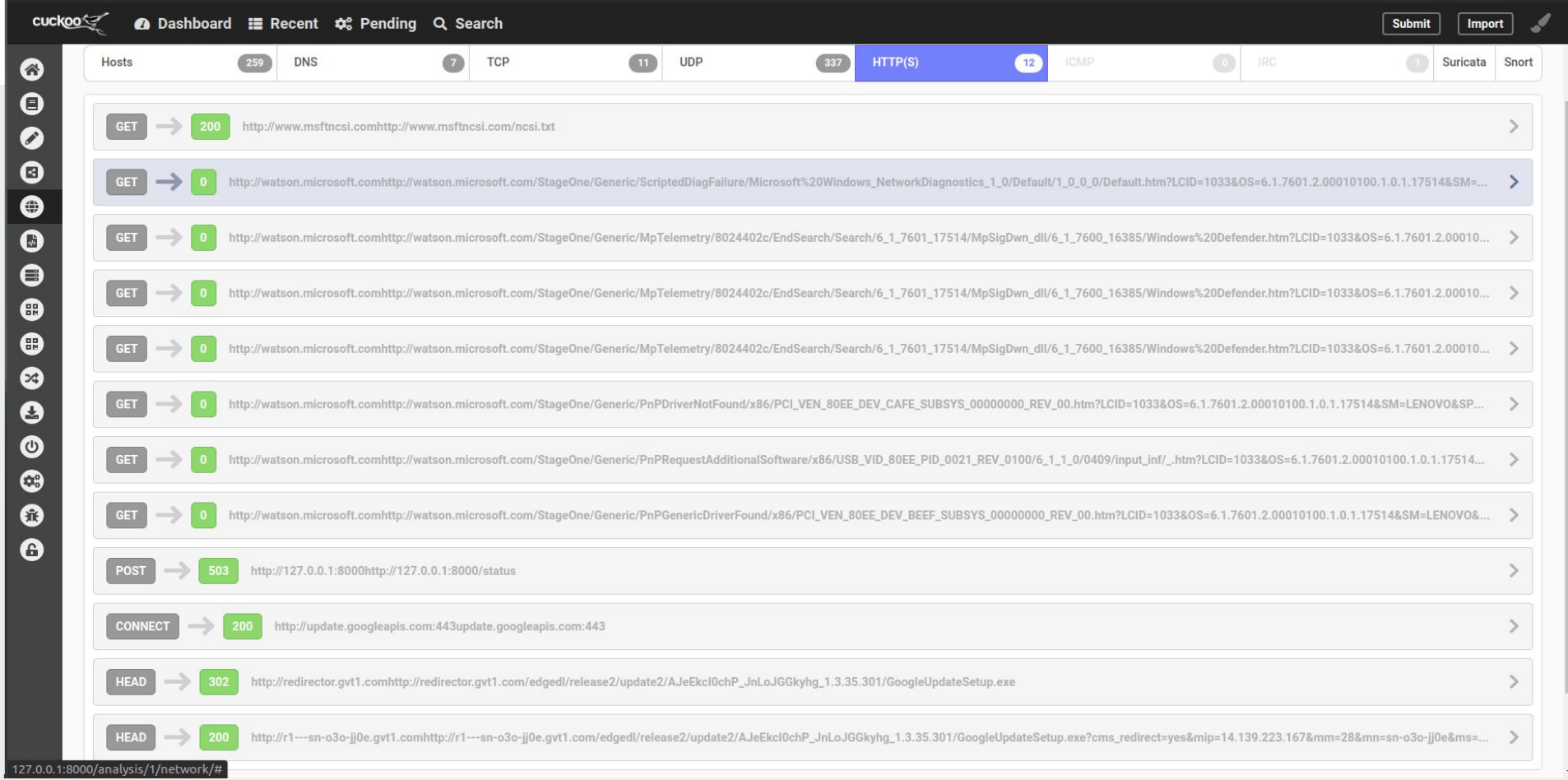
2019-10-31 14:38:21 UTC 7 days ago

EXE

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 10+

Acronis	Suspicious	Ad-Aware	Trojan.WLDCR.C
AegisLab	Trojan.Win32.ZAccess.tnpa	AhnLab-V3	Trojan/Win32.ZAccess.R87034
Alibaba	Backdoor:Win32/ZAccess.d2937015	ALYac	Trojan.ZeroAccess.RN
SecureAge APEX	Malicious	Arcabit	Trojan.WLDCR.C
Avast	Win32:Heim	AVG	Win32:Heim
Avira (no cloud)	TR/Crypt.XPACK.52658	BitDefender	Trojan.WLDCR.C
BitDefenderTheta	Gen:NN.ZexaO.31176.pyW@aqPTyGbO	CAT-QuickHeal	TrojanDropper.Sirefef.A9
CMC	Backdoor.Win32.ZAccess!O	Comodo	Malware@#3cscsamn9ftuw
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.54d20d
Cylance	Unsafe	Cyren	W32/Zbot.QZDC-5119
DrWeb	BackDoor.Maxplus.14813	eGambit	Generic.Malware
Emsisoft	Trojan.WLDCR.C (B)	Endgame	Malicious (high Confidence)
eScan	Trojan.WLDCR.C	ESET-NOD32	Win32/Sirefef.FY
F-Prot	W32/Zbot.BWT	F-Secure	Trojan.TR/Crypt.XPACK.52658

2. One of the Dropped files, when scanned using an online tool for malicious activity, was found to contain Trojans and Adwares.



```
GET → 200 http://www.msftncsi.comhttp://www.msftncsi.com/ncsi.txt
GET → 0 http://watson.microsoft.comhttp://watson.microsoft.com/StageOne/Generic/ScriptedDiagFailure/Microsoft%20Windows_NetworkDiagnostics_1_0/Default/1_0_0_0/Default.htm?LCID=1033&OS=6.1.7601.2.00010100.1.0.1.17514&SM=...
GET → 0 http://watson.microsoft.comhttp://watson.microsoft.com/StageOne/Generic/MpTelemetry/8024402c/EndSearch/Search/6_1_7601_17514/MpSigDwn_dll/6_1_7600_16385/Windows%20Defender.htm?LCID=1033&OS=6.1.7601.2.00010...
GET → 0 http://watson.microsoft.comhttp://watson.microsoft.com/StageOne/Generic/MpTelemetry/8024402c/EndSearch/Search/6_1_7601_17514/MpSigDwn_dll/6_1_7600_16385/Windows%20Defender.htm?LCID=1033&OS=6.1.7601.2.00010...
GET → 0 http://watson.microsoft.comhttp://watson.microsoft.com/StageOne/Generic/MpTelemetry/8024402c/EndSearch/Search/6_1_7601_17514/MpSigDwn_dll/6_1_7600_16385/Windows%20Defender.htm?LCID=1033&OS=6.1.7601.2.00010...
GET → 0 http://watson.microsoft.comhttp://watson.microsoft.com/StageOne/Generic/PnPDriverNotFound/x86/PCI_VEN_80EE_DEV_CAFE_SUBSYS_00000000_REV_00.htm?LCID=1033&OS=6.1.7601.2.00010100.1.0.1.17514&SM=LENOVO&SP...
GET → 0 http://watson.microsoft.comhttp://watson.microsoft.com/StageOne/Generic/PnPRequestAdditionalSoftware/x86/USB_VID_80EE_PID_0021_REV_0100/6_1_1_0/0409/input_inf/_.htm?LCID=1033&OS=6.1.7601.2.00010100.1.0.1.17514...
GET → 0 http://watson.microsoft.comhttp://watson.microsoft.com/StageOne/Generic/PnPGenericDriverFound/x86/PCI_VEN_80EE_DEV_BEEF_SUBSYS_00000000_REV_00.htm?LCID=1033&OS=6.1.7601.2.00010100.1.0.1.17514&SM=LENOVO&...
POST → 503 http://127.0.0.1:8000http://127.0.0.1:8000/status
CONNECT → 200 http://update.googleapis.com:443update.googleapis.com:443
HEAD → 302 http://redirector.gvt1.comhttp://redirector.gvt1.com/edgedl/release2/update2/AJeEkcl0chP_JnLoJGGkyhg_1.3.35.301/GoogleUpdateSetup.exe
HEAD → 200 http://r1---sn-o3o-jj0e.gvt1.comhttp://r1---sn-o3o-jj0e.gvt1.com/edgedl/release2/update2/AJeEkcl0chP_JnLoJGGkyhg_1.3.35.301/GoogleUpdateSetup.exe?cms_redirect=yes&mip=14.139.223.167&mm=28&mn=sn-o3o-jj0e&ms=...
```

3. Over here we can see that the Botnet sends get and post requests to a plethora of IP addresses. These requests may or may not be responded with malicious files.

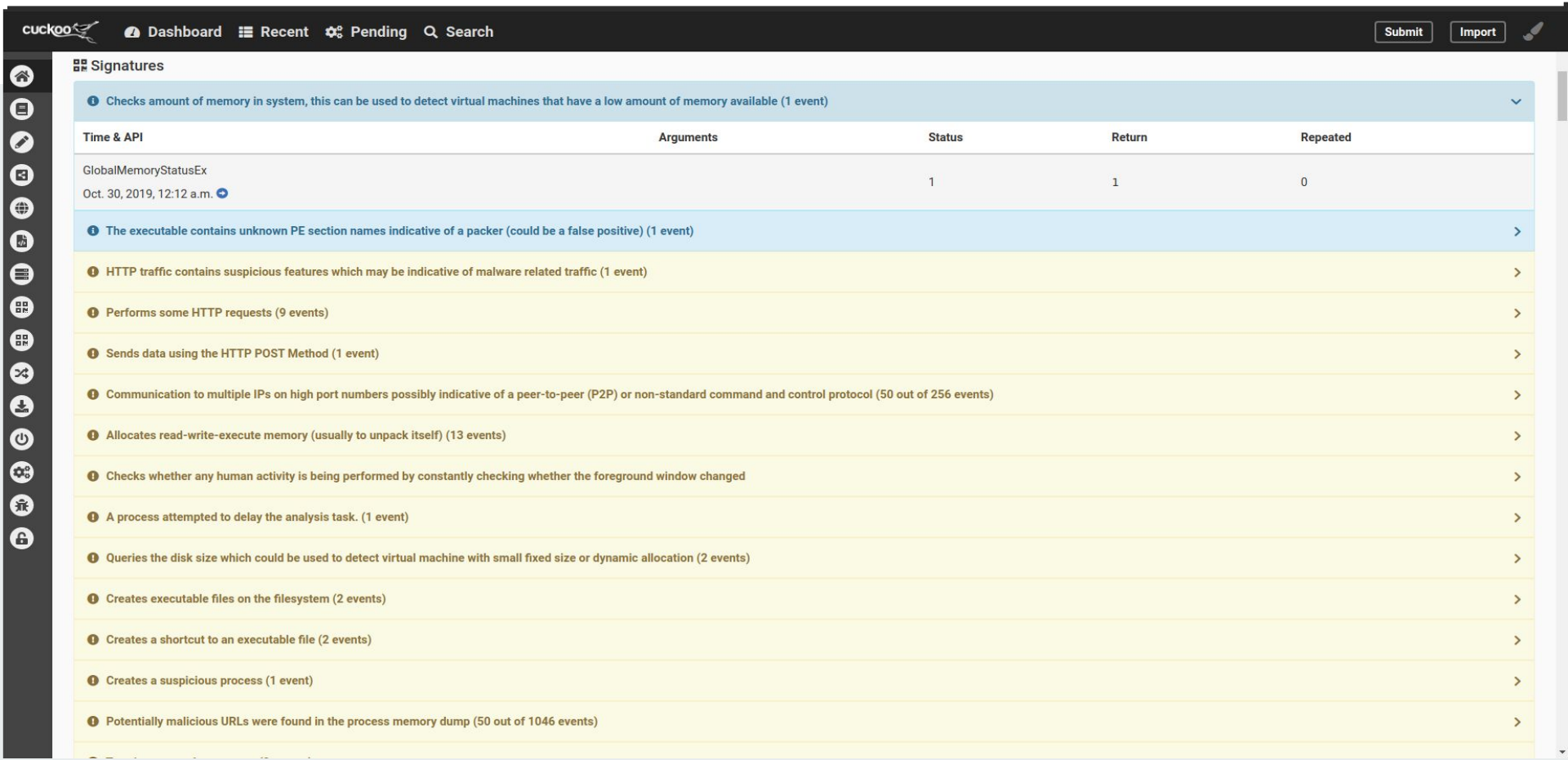
cuckoo Dashboard Recent Pending Search Submit Import

- One or more thread handles in other processes (1 event)
- Connects to an IRC server, possibly part of a botnet
- Communicates with host for which no DNS query was performed (50 out of 257 events)
- Attempts to identify installed AV products by installation directory (1 event)
- Attempts to stop active services (8 events)
- Installs itself for autorun at Windows startup (2 events)
- Manipulates memory of a non-child process indicative of process injection (4 events)
- Creates a windows hook that monitors keyboard input (keylogger) (1 event)
- Used NtSetContextThread to modify a thread in a remote process indicative of process injection (2 events)
- Resumed a suspended thread in a remote process potentially indicative of process injection (4 events)
- Creates known Upatre files, registry keys and/or mutexes (1 event)
- PEB modified to hide loaded modules. Dll very likely not loaded by LoadLibrary (50 out of 67 events)
- Malfind detects one or more injected processes (1 event)
- Stopped Application Layer Gateway service (1 event)
- Executed a process and injected code into it, probably while unpacking (11 events)
- Stops Windows services (10 events)

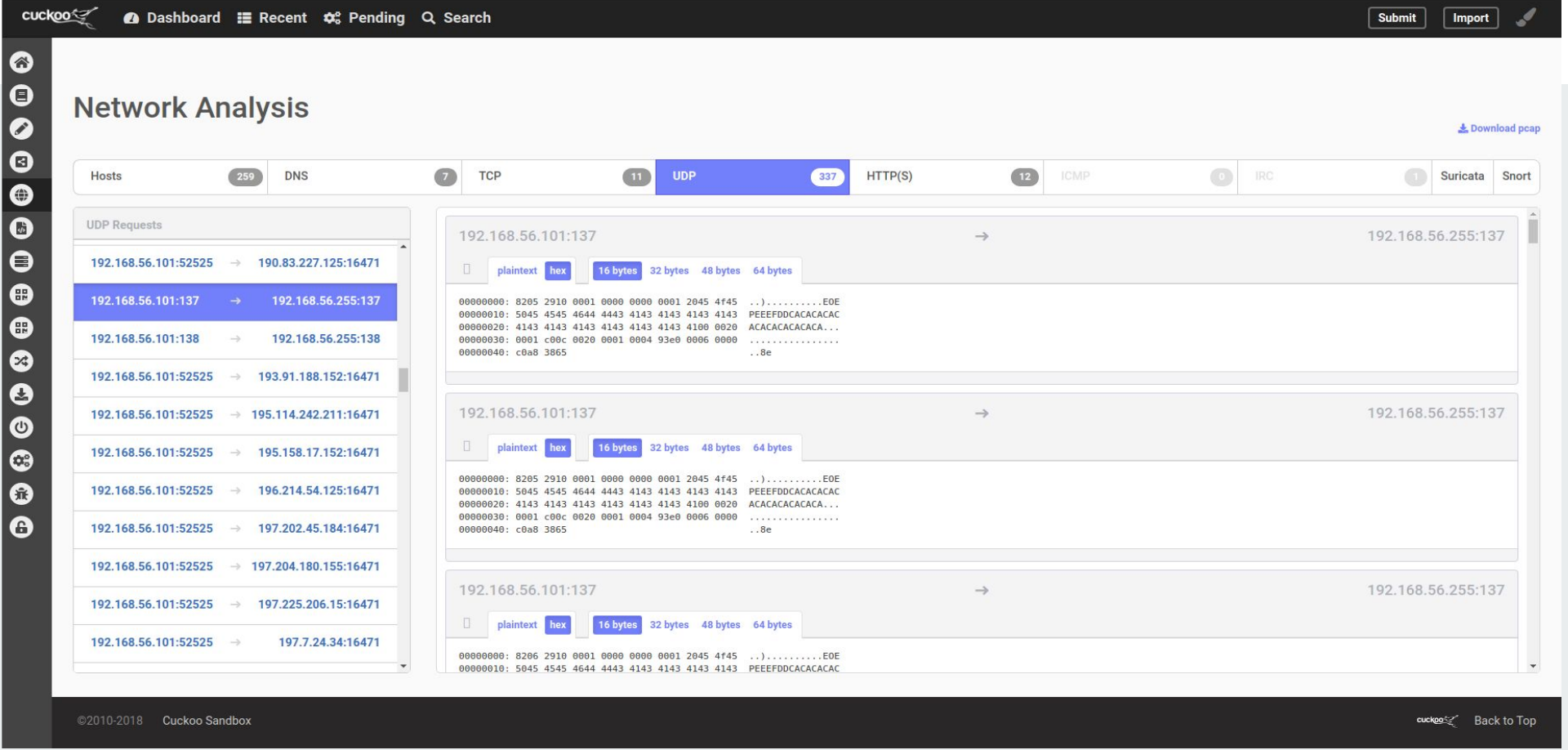
Screenshots

127.0.0.1:8000/analysis/1/summary/#signature_persistence_autorun

4. Collection of malicious activities that were done by the Botnet.
Includes attempts to stop Windows Services like Firewall and installing a keylogger.



5. This shows the list of host and server to which the bots are trying to connect with download files which could contain malware to breach the system data and Information.



6. This shows the Network Analysis of User Datagram Protocol requests trying to establish connection with different servers and hosts.

cuckoo Dashboard Recent Pending Search Submit Import

Communication to multiple IPs on high port numbers possibly indicative of a peer-to-peer (P2P) or non-standard command and control protocol (50 out of 256 events)

ip	1.163.95.182
ip	101.1.96.38
ip	101.5.123.50
ip	103.12.122.101
ip	103.244.13.133
ip	105.237.72.119
ip	109.175.253.31
ip	109.224.46.146
ip	110.138.209.155
ip	110.67.124.169
ip	111.253.73.245
ip	112.134.217.84
ip	112.135.33.165
ip	112.197.104.58
ip	112.200.189.50
ip	112.205.135.107
ip	113.11.27.201
ip	113.21.77.44
ip	114.26.208.155
ip	114.39.95.144
ip	115.187.38.179

7. This is the list of IP addresses to which it is trying to connect.

Thank you