Nazca

Detecting Malware Distribution in Large-Scale Networks

Luca Invernizzi
Christopher Kruegel
Giovanni Vigna

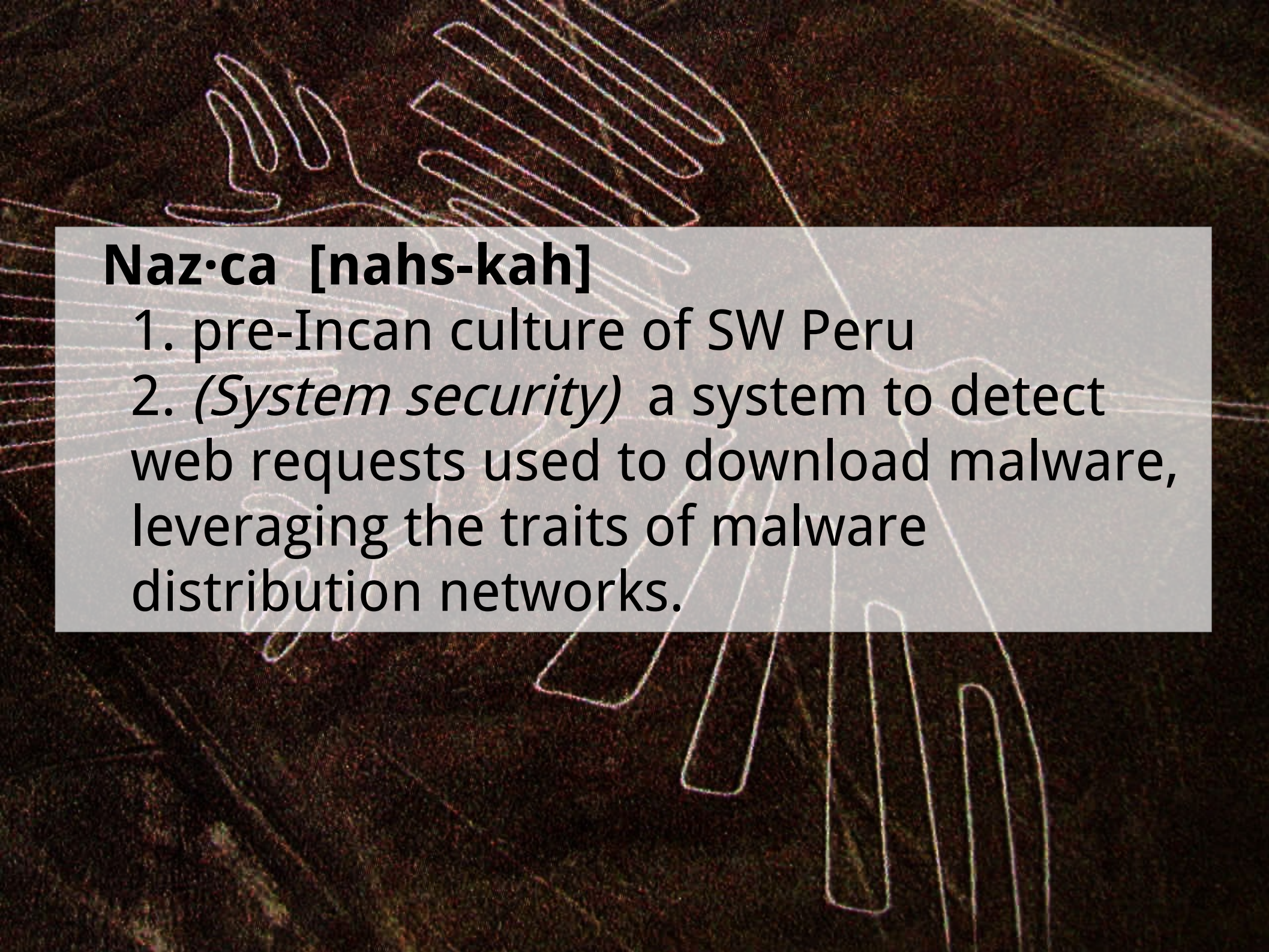
UC Santa Barbara

Stanislav Miskovic
Ruben Torres
Sabyaschi Saha
Sung-Ju Lee

Narus, Inc.

Marco Mellia

Politecnico di Torino



Naz·ca [nahs-kah]

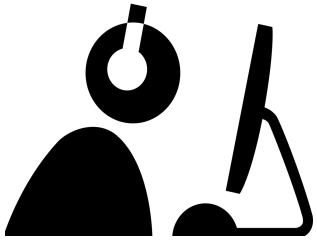
1. pre-Incan culture of SW Peru
2. *(System security)* a system to detect web requests used to download malware, leveraging the traits of malware distribution networks.

GET /

winzip.in

GET /[..]/UpSJvusS/WinZip180.exe

install.winzip.com



GET /down/game_setup.exe

soft.taobao91.com

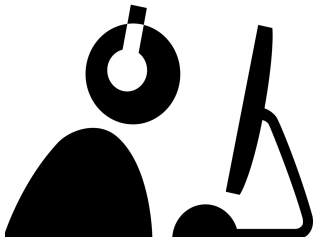
GET /

winzip.it

GET /

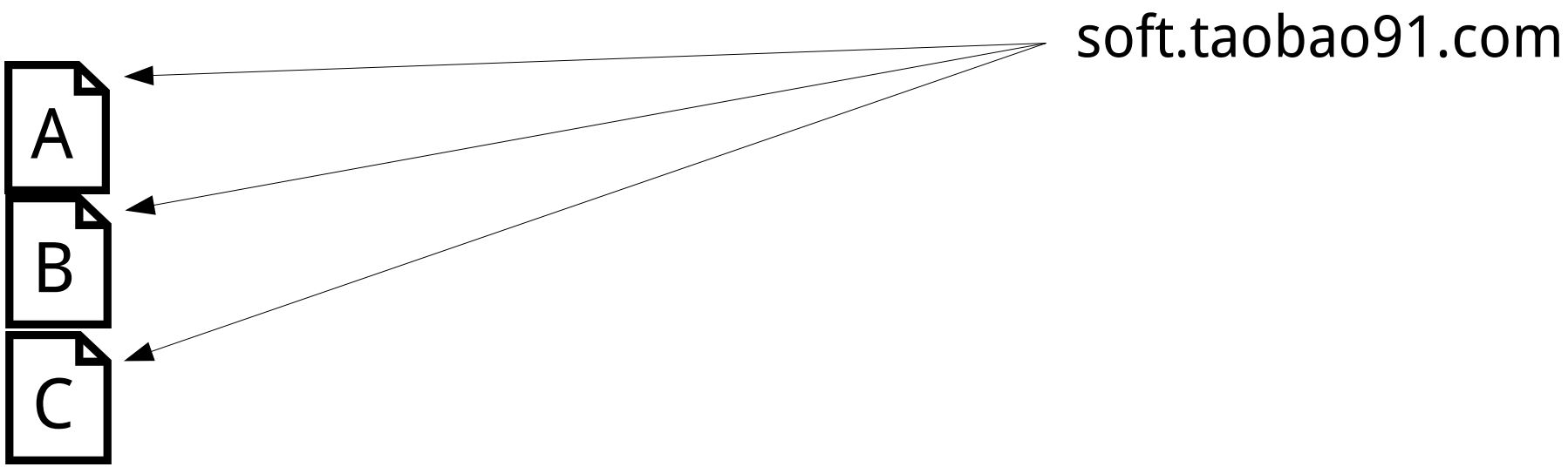
winzip.ir

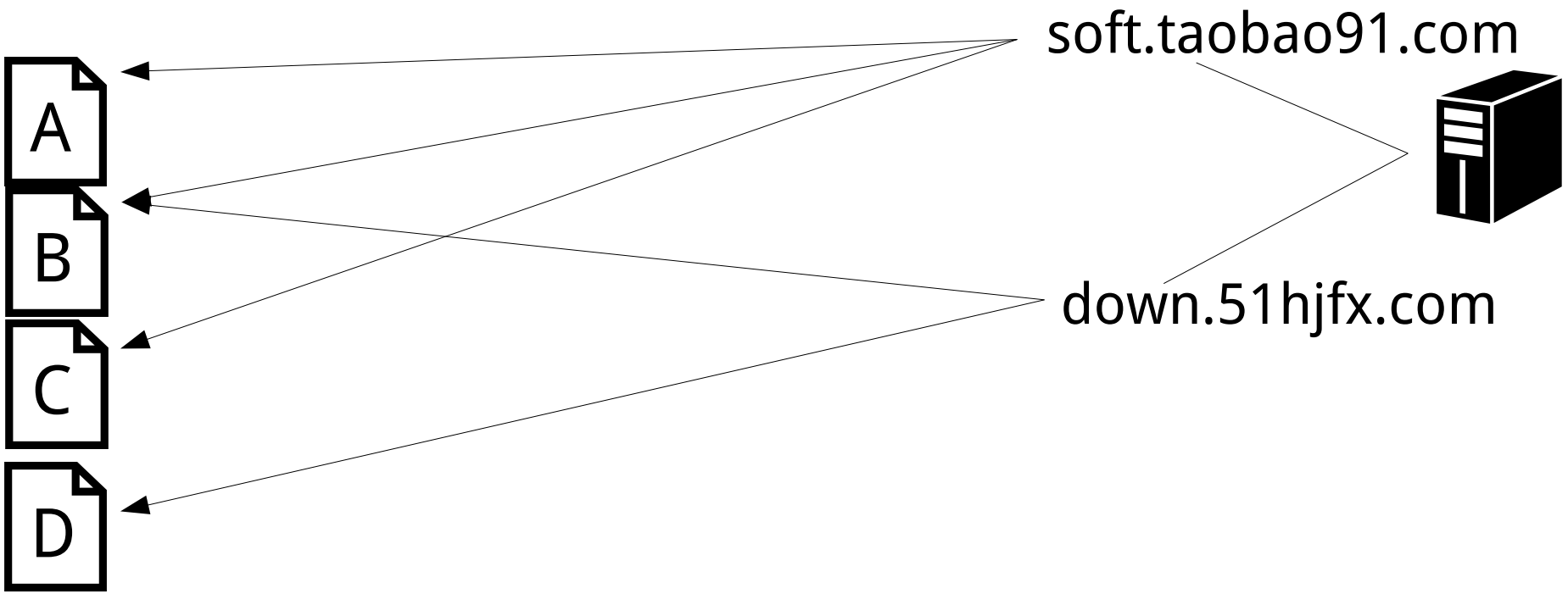
Who's infected?

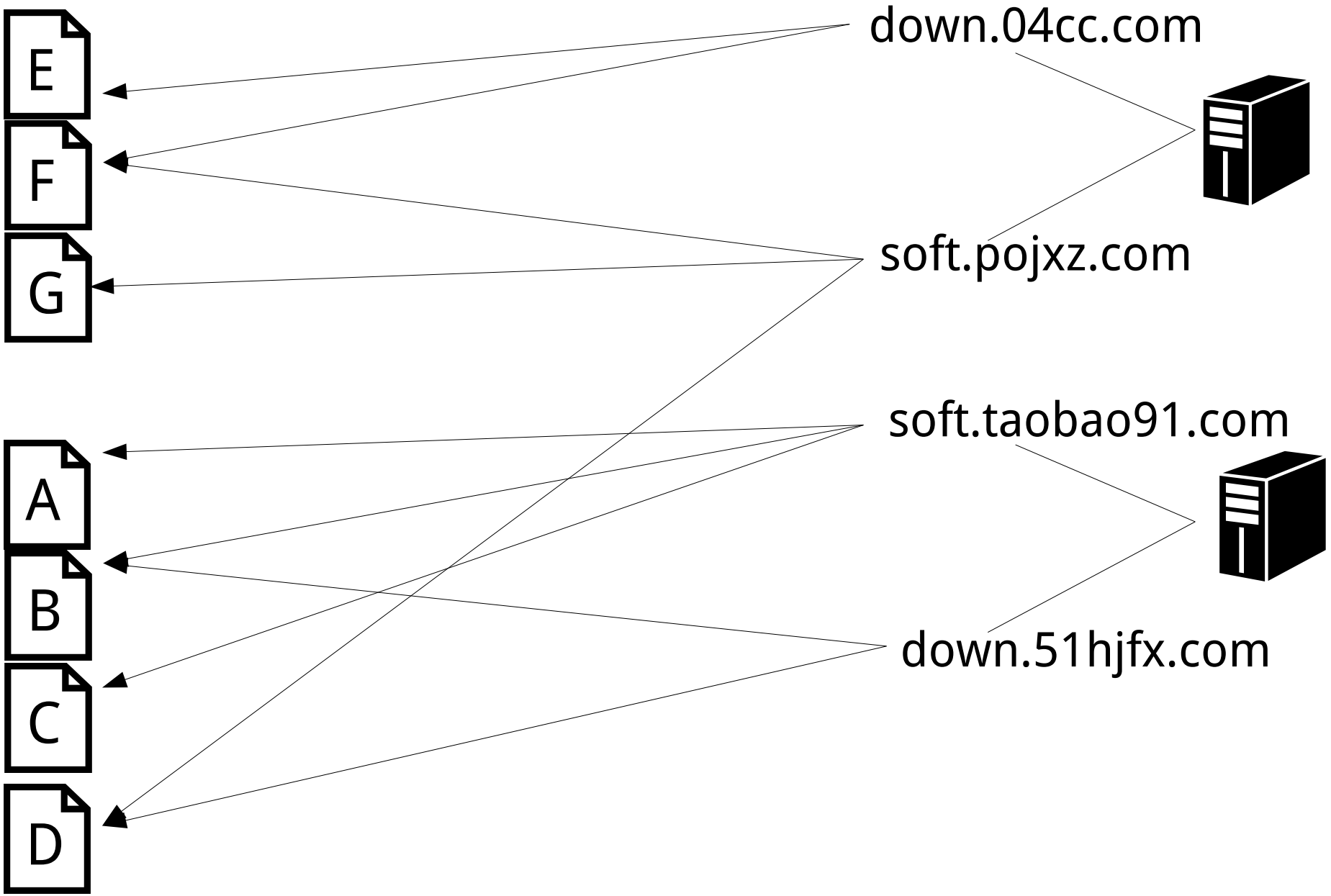


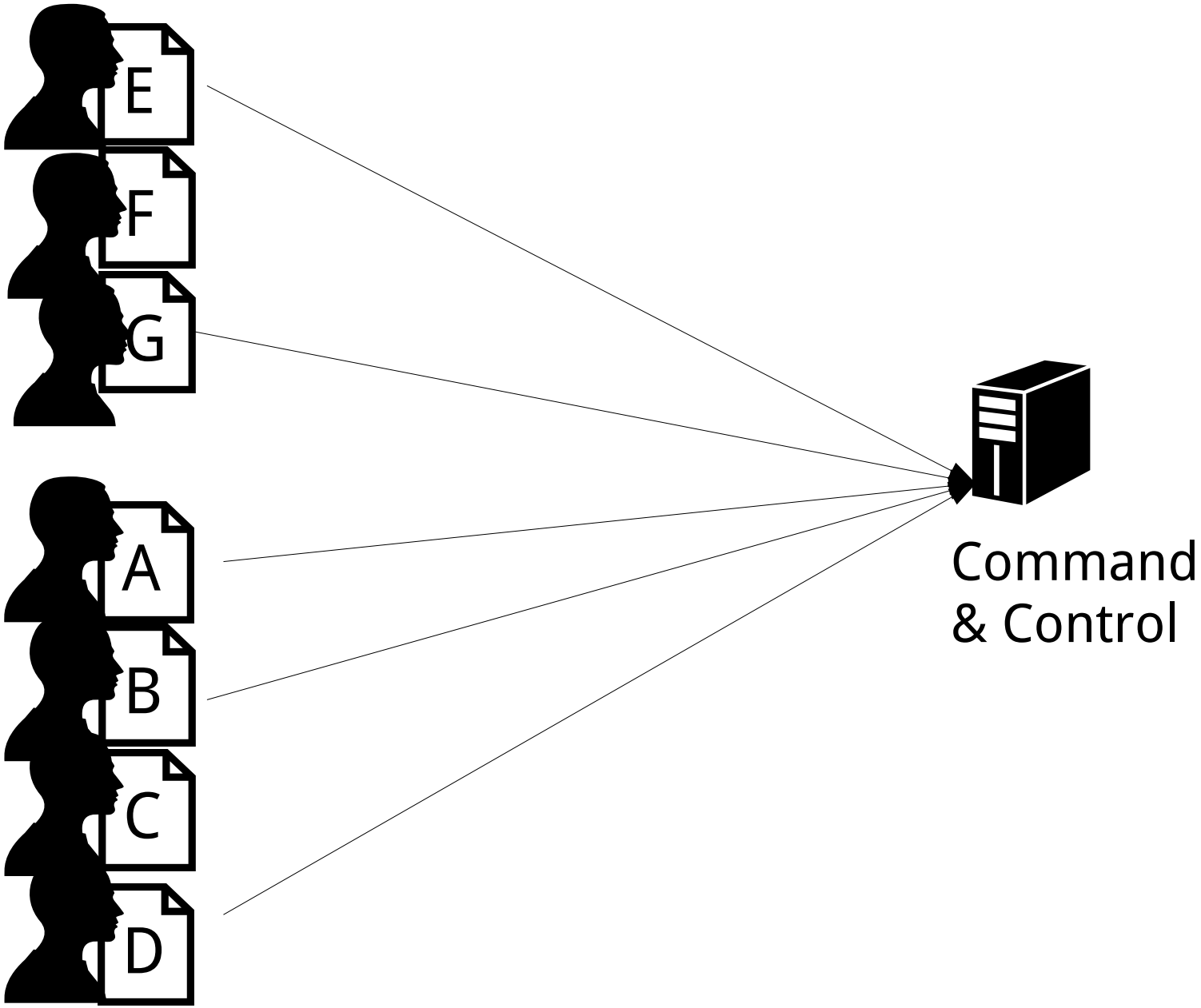
GET /down/game_setup.exe

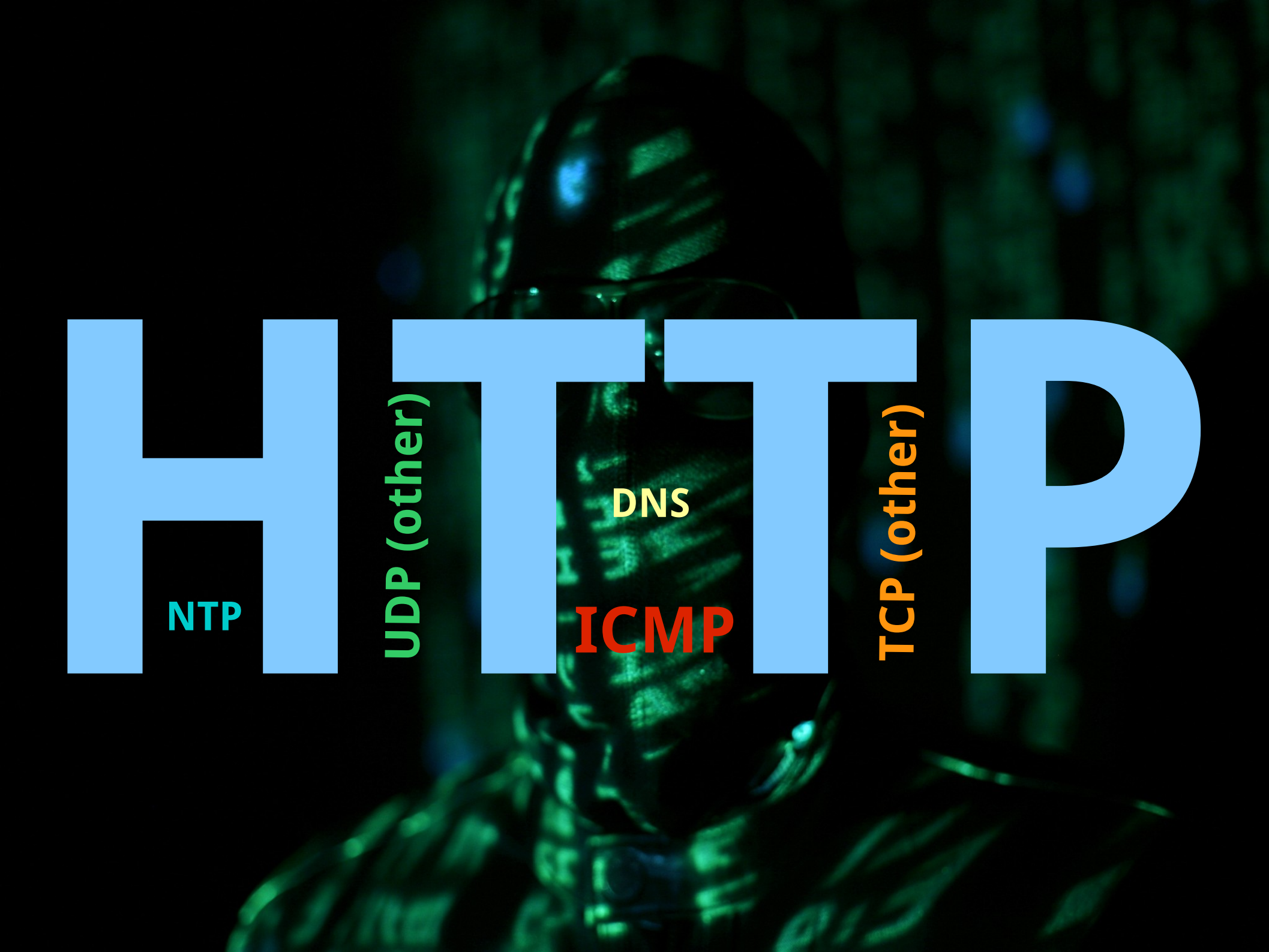
soft.taobao91.com


soft.taobao91.com
A
B
C


soft.taobao91.com
down.51hjfx.com
A
B
C
D


down.04cc.com
E
F
G
soft.pojxz.com
soft.taobao91.com
A
B
C
D
down.51hjfx.com


E
F
G
A
B
C
D
Command
& Control


HTTP
NTP
UDP (other)
DNS
ICMP
TCP (other)


HTTP=

Nazca's

3 STEPS

EXTRACTION

of HTTP-connection metadata

CANDIDATE SELECTION

identifying blacklisting evasions

DETECTION

of malware distribution infrastructures

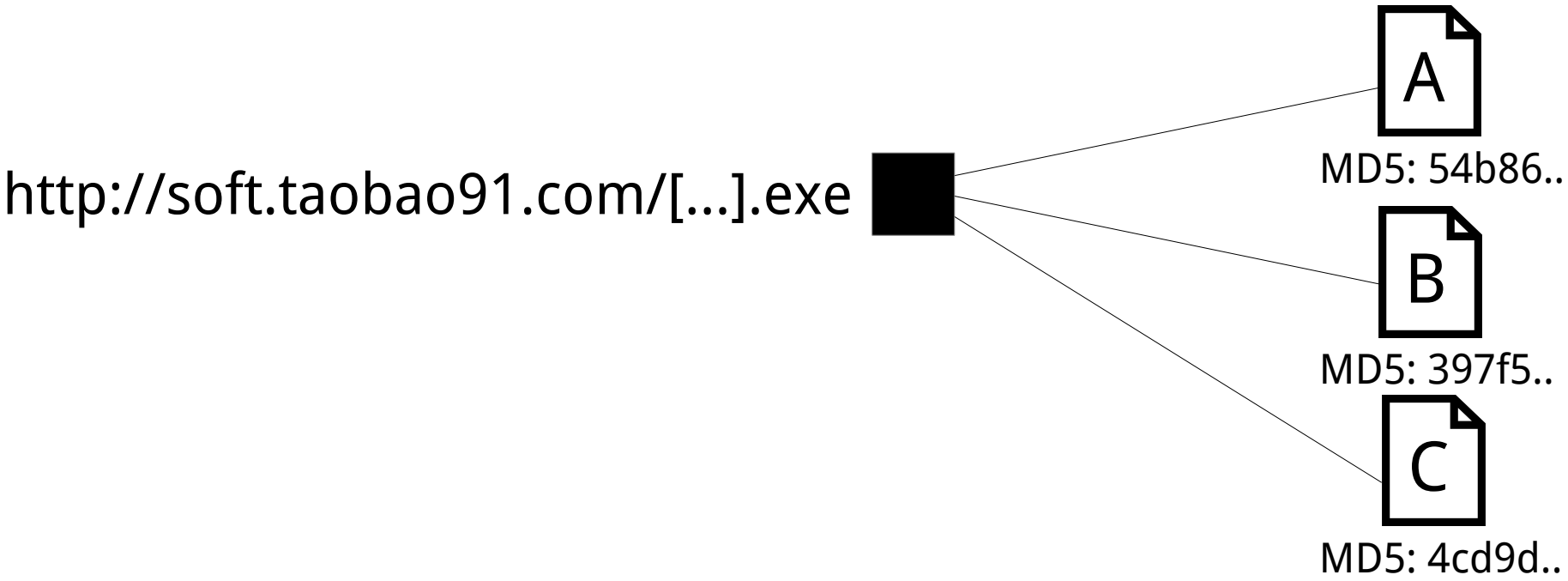
KEEP

- Sender/receiver metadata
- Declared Content-Type and sniffed MIME type
- MD5 of first *k* bytes of payload, uncompressed if necessary

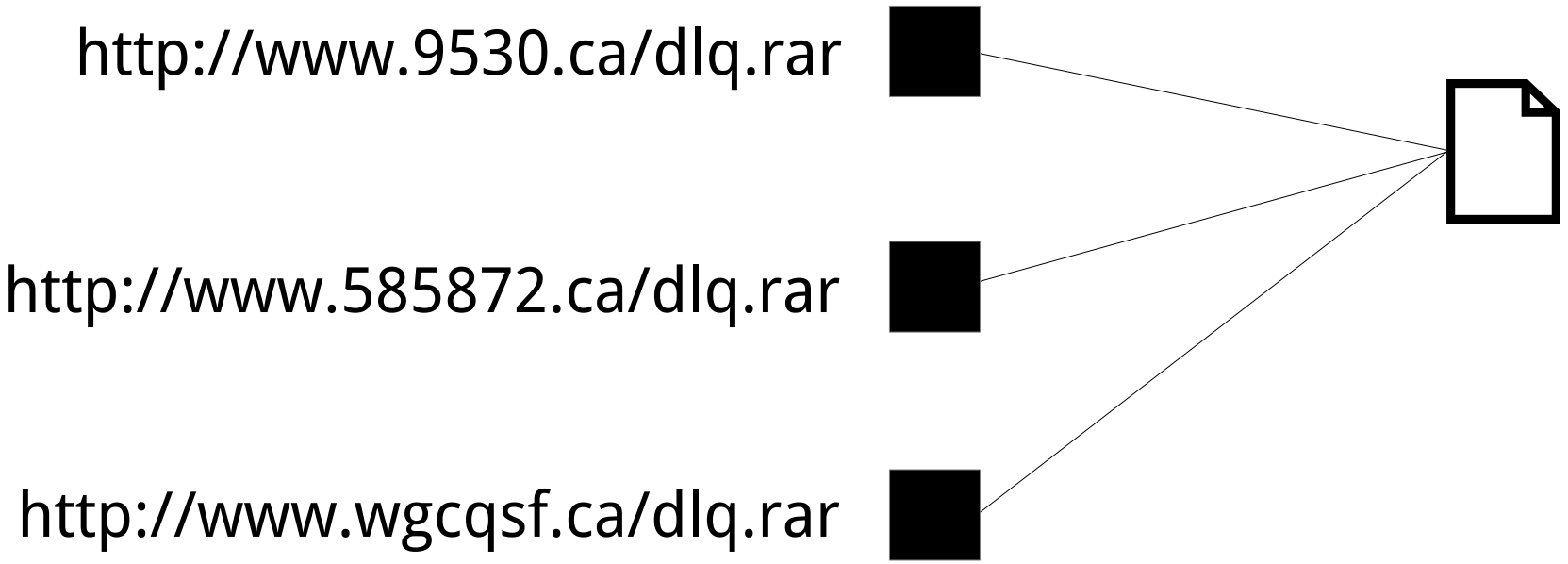
DISCARD

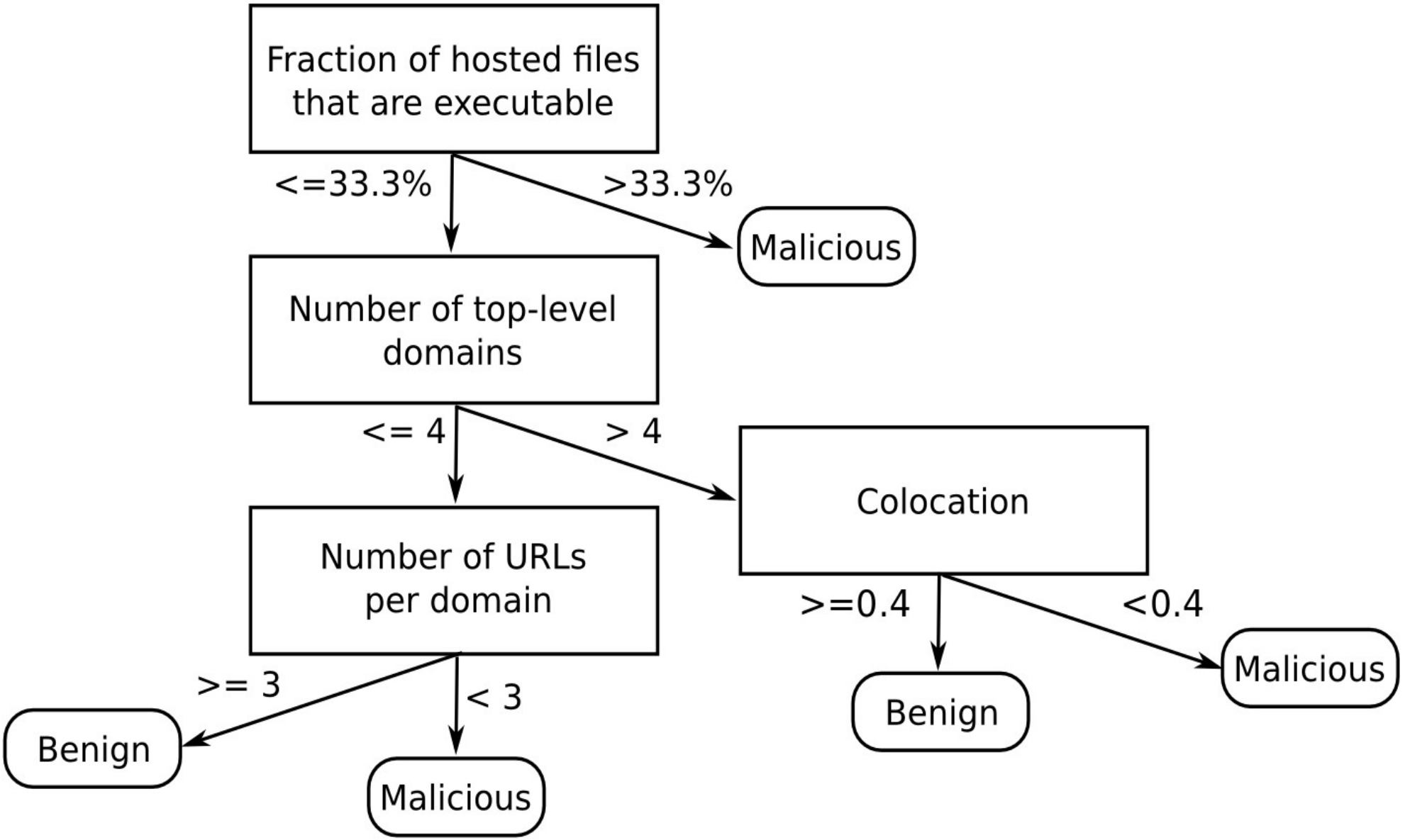
- Any non-HTTP packet
- Any HTTP packet delivering whitelisted MIME types (HTML, videos, photos...) - just keep a tally

FILE MUTATIONS

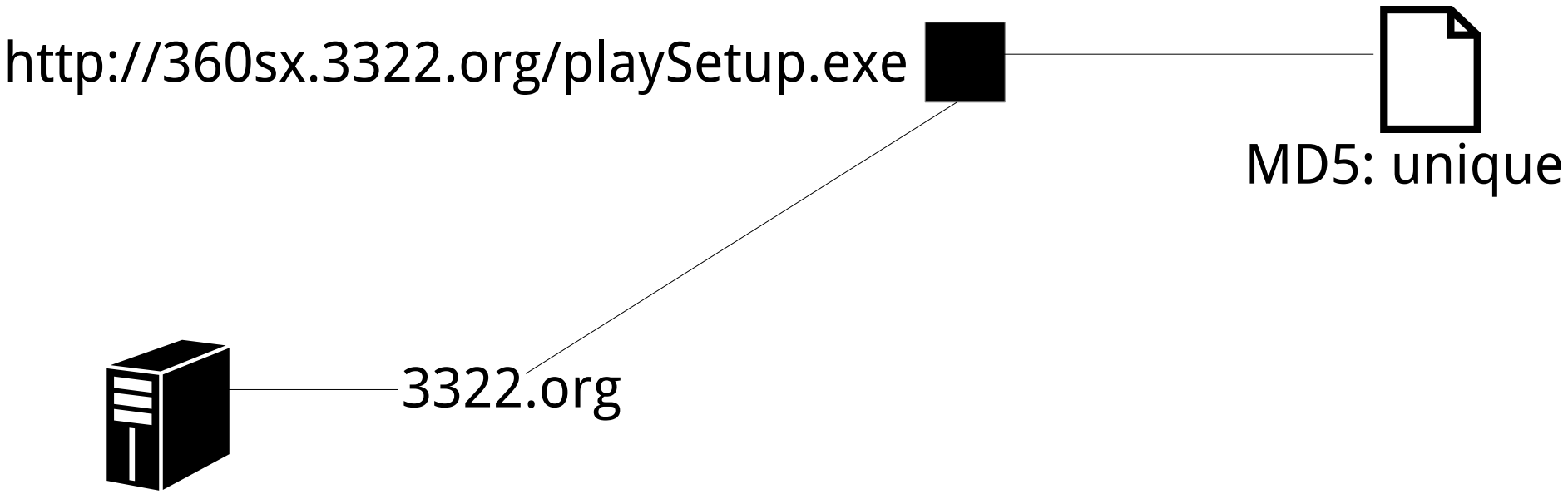


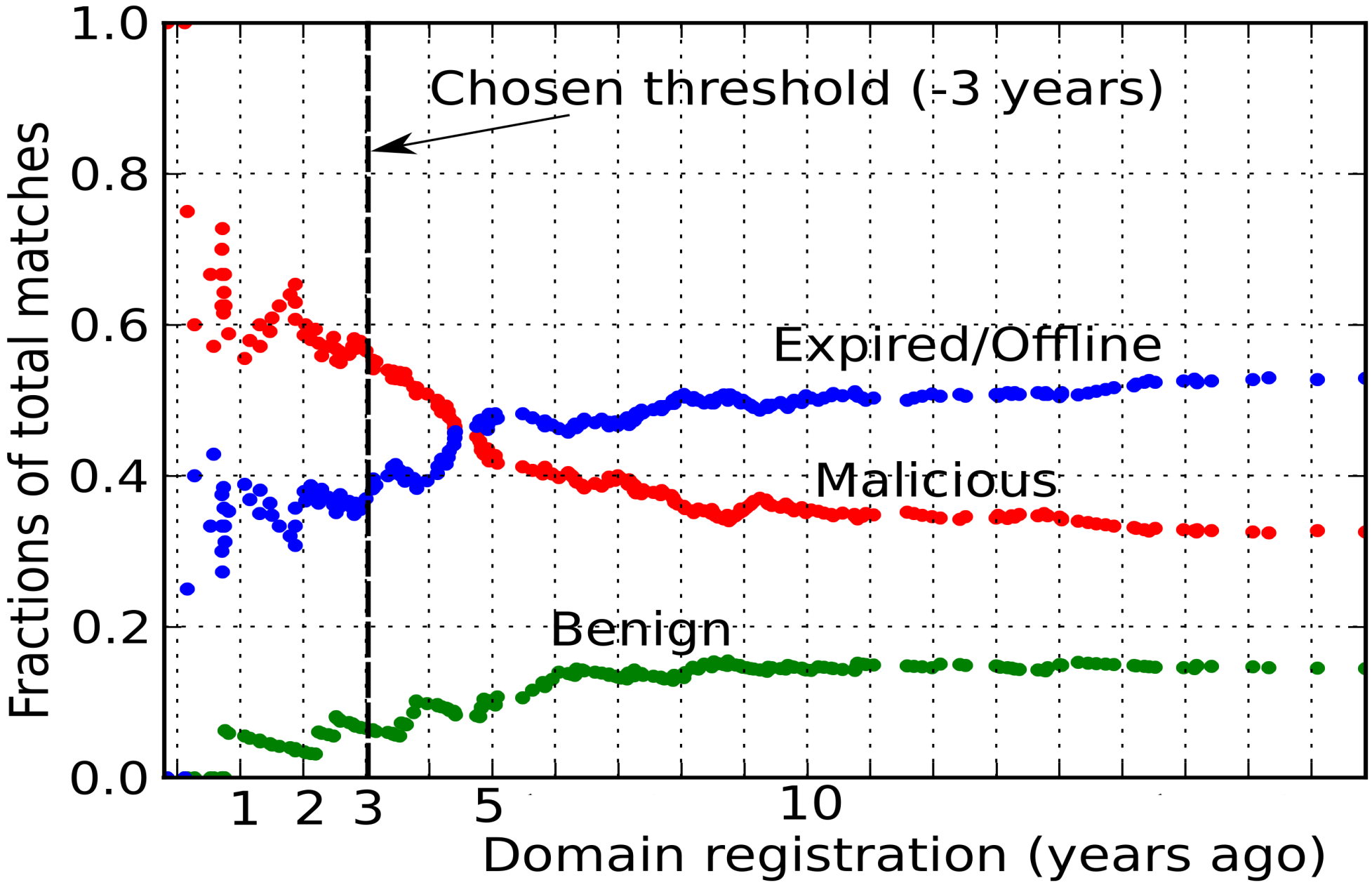
DISTRIBUTED HOSTING



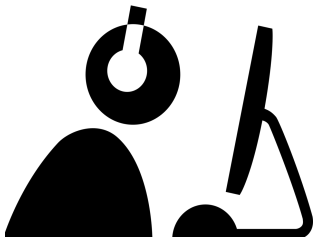

Fraction of hosted files that are executable
<=33.3%
>33.3%
Malicious
Number of top-level domains
<= 4
> 4
Colocation
Number of URLs per domain
>=0.4
<0.4
Malicious
Benign
>= 3
< 3
Benign
Malicious

DEDICATED MALWARE HOSTING




Chosen threshold (-3 years)
Expired/Offline
Malicious
Benign
Fractions of total matches
1.0
0.8
0.6
0.4
0.2
0.0
1
2
3
5
10
Domain registration (years ago)

EXPLOIT/DOWNLOAD HOSTS



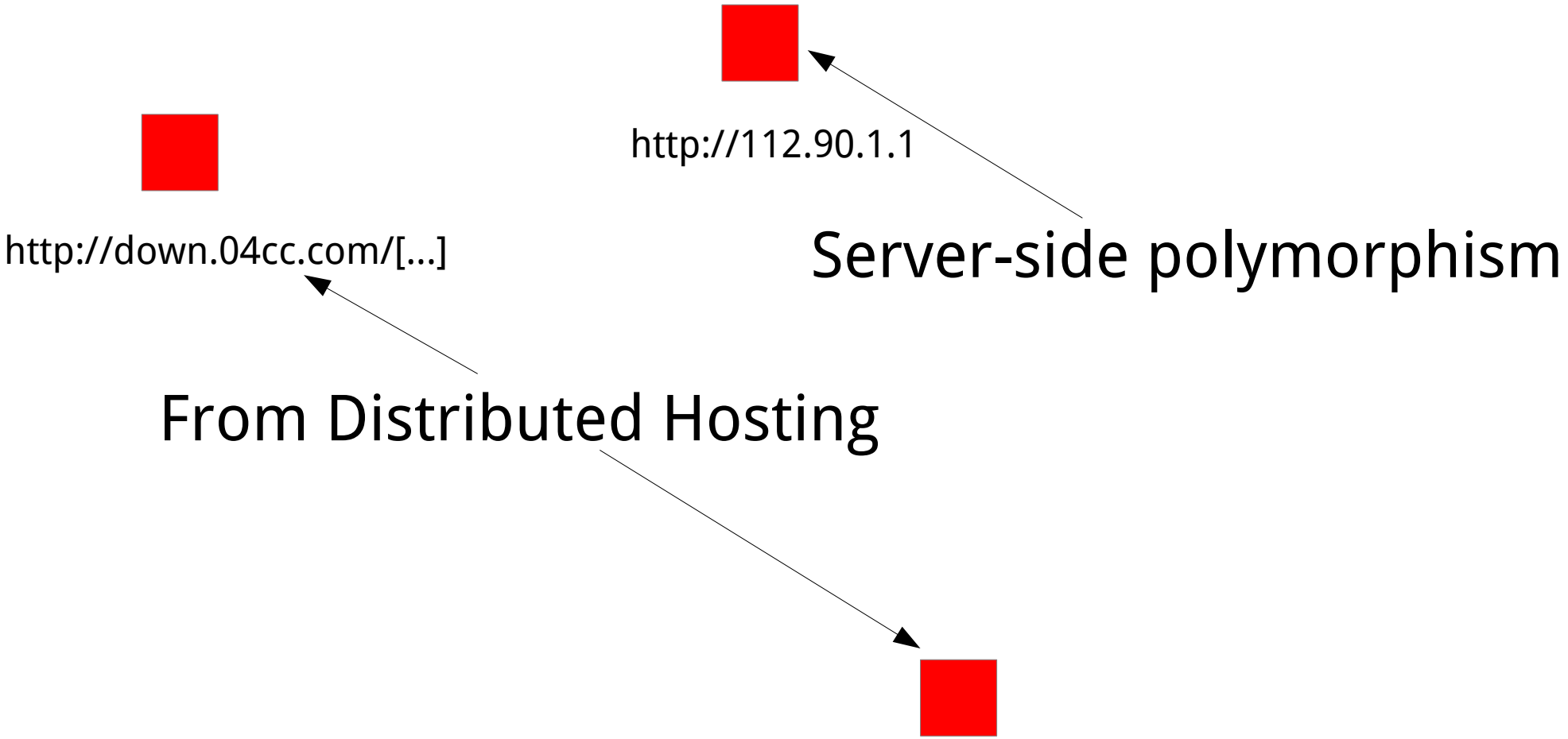
GET /software/gzip2.exe → cmp.freesportsapp.com

User-Agent: Internet Explorer

GET /funtool → cmp.freesportsapp.com

User-Agent: NSISDL/1.2

GRAPH BUILDING



GRAPH BUILDING

http://112.90.1.1

http://down.04cc.com/[...]

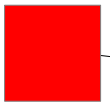
http://soft.taobao91.com/down/game_setup.exe

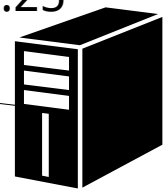
GRAPH BUILDING

http://112.90.1.1

http://down.04cc.com/[...]

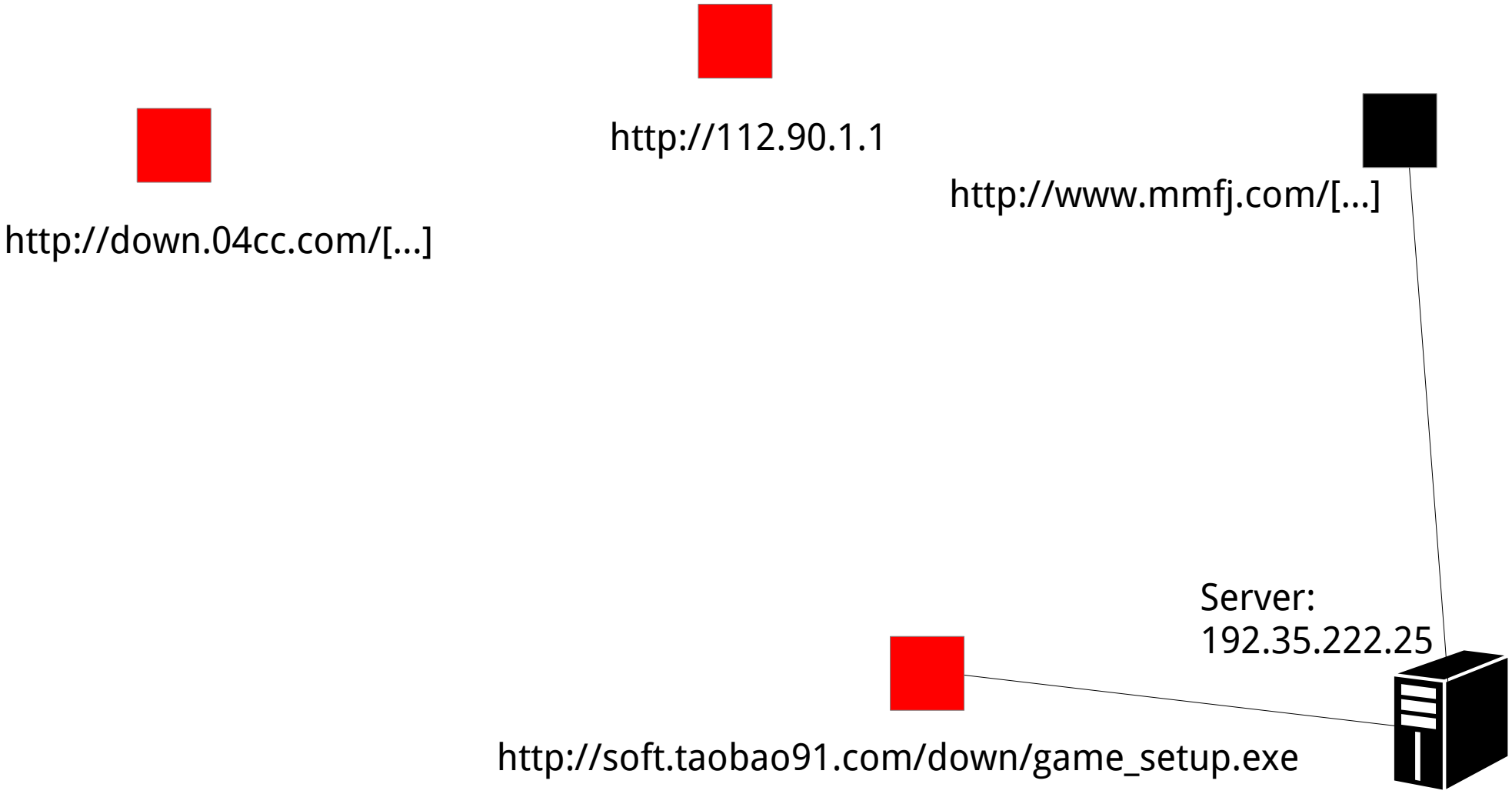
Server:
192.35.222.25



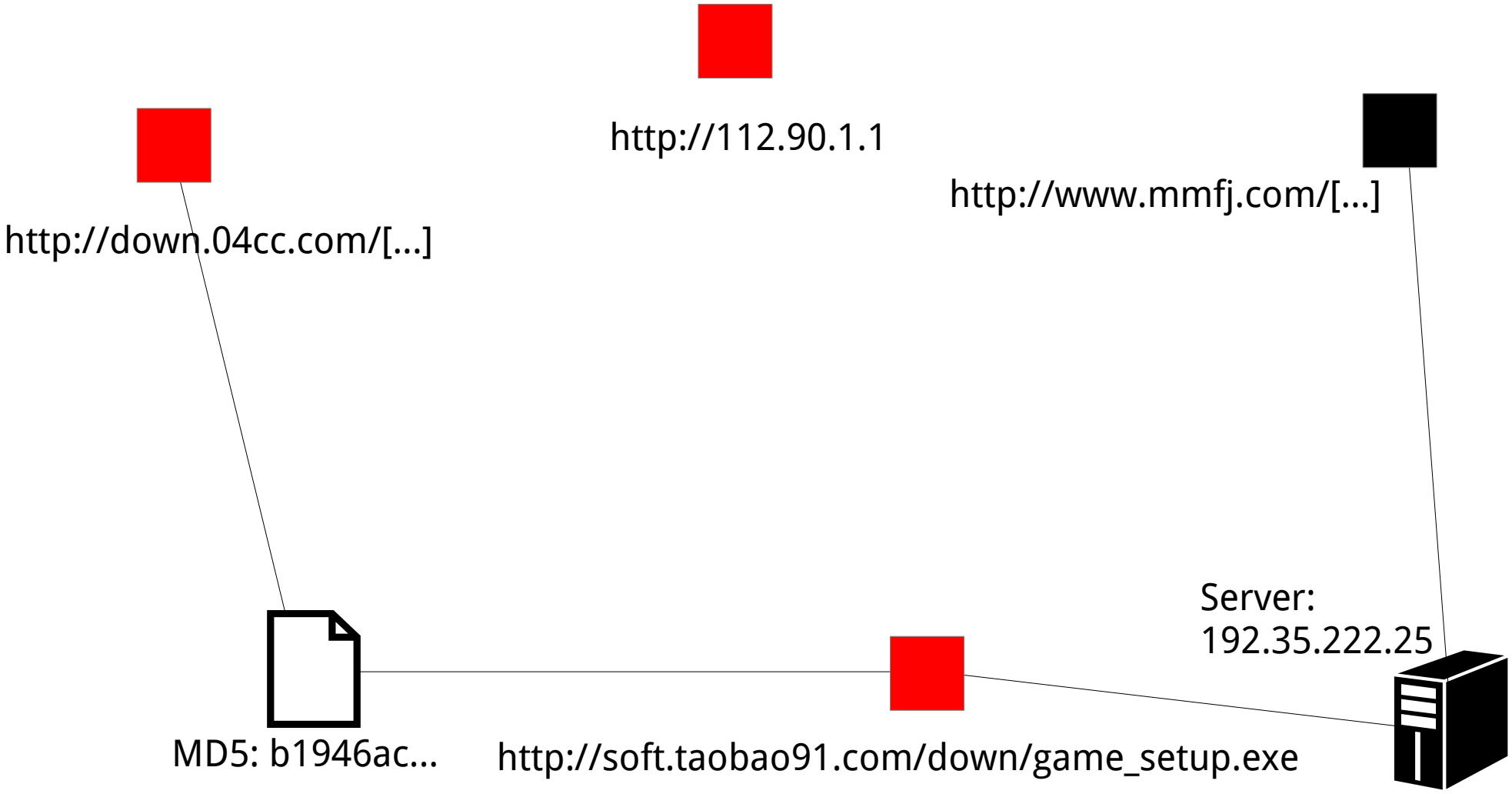


http://soft.taobao91.com/down/game_setup.exe

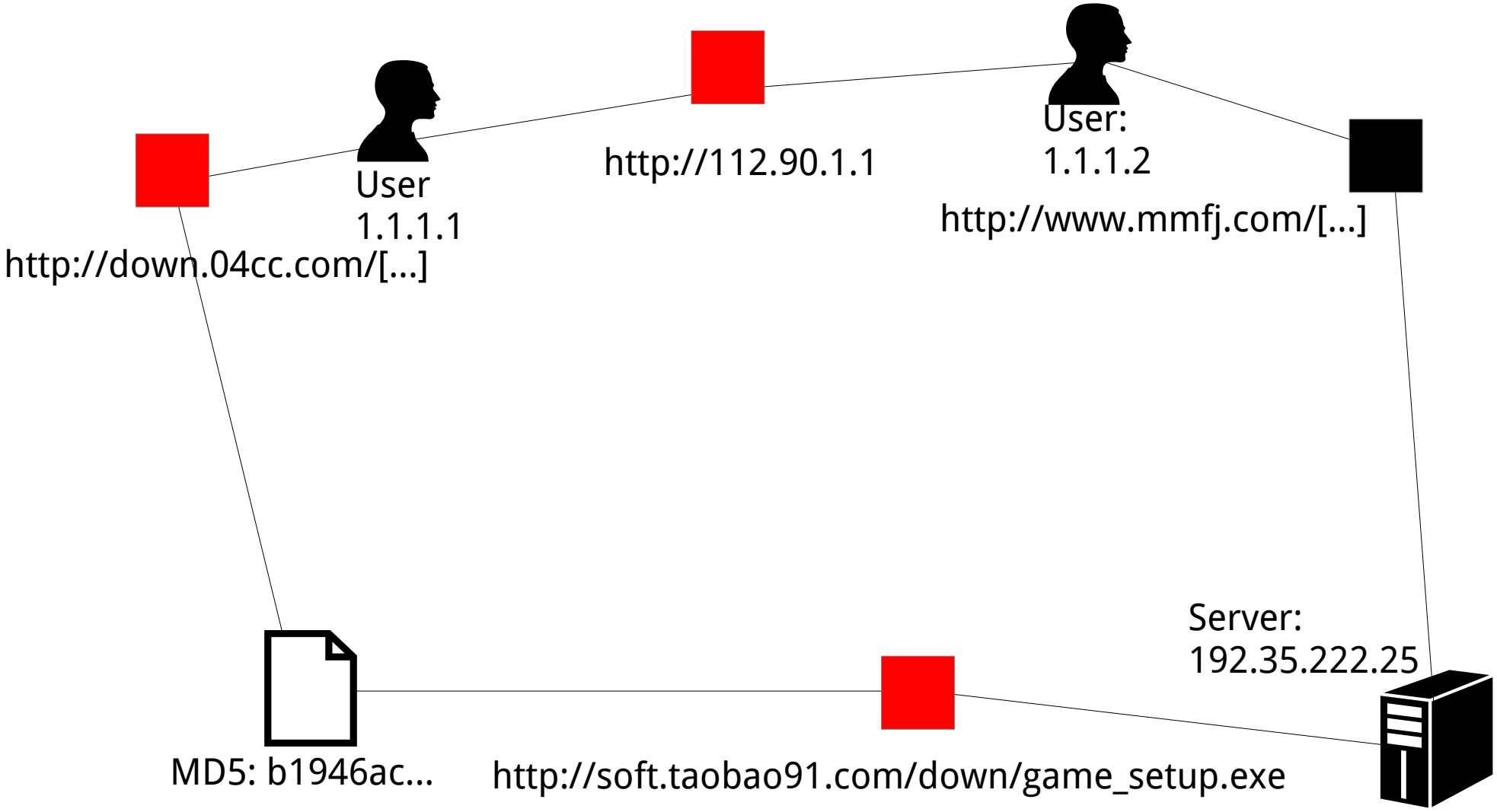
GRAPH BUILDING



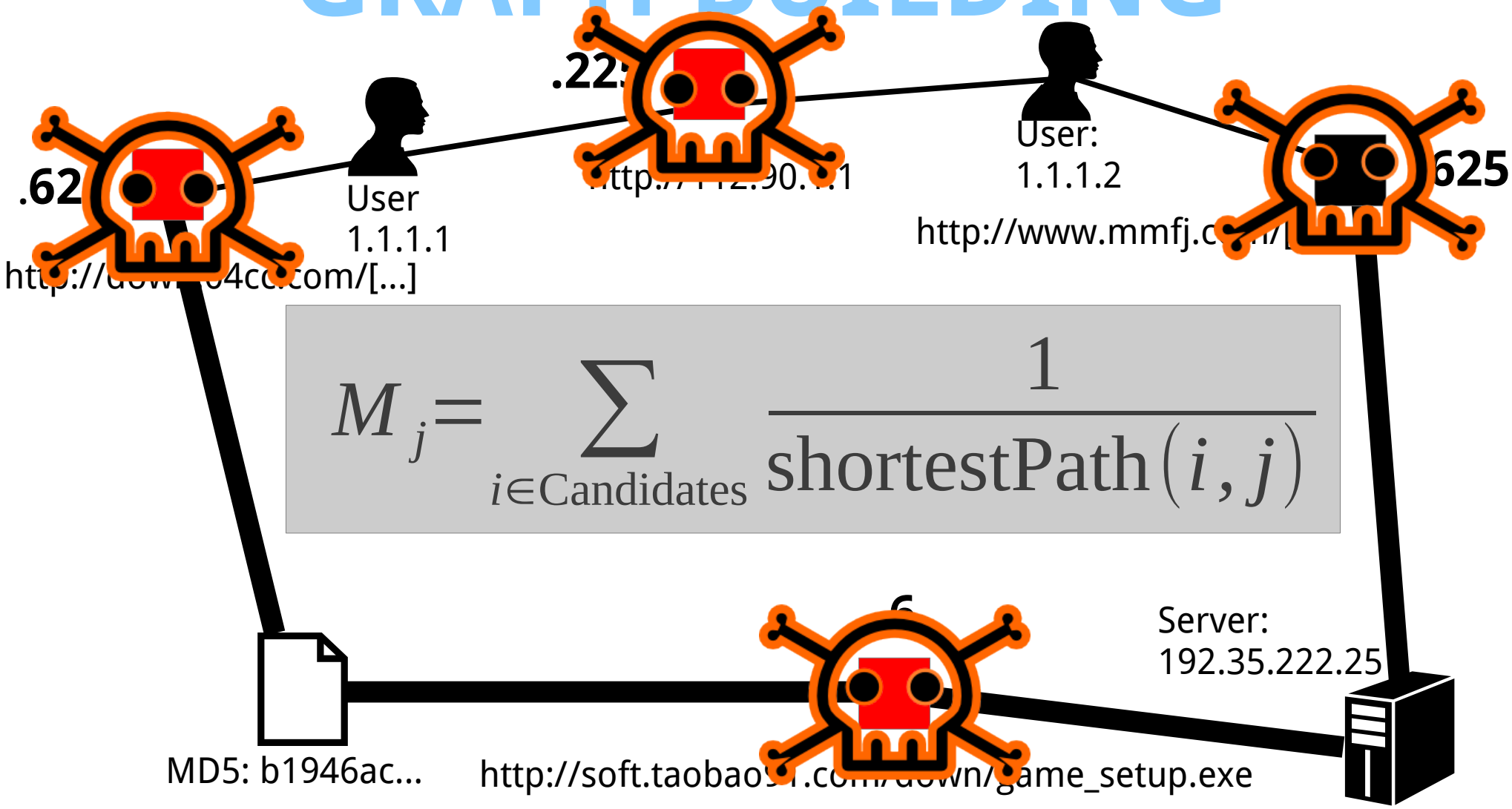
GRAPH BUILDING



GRAPH BUILDING

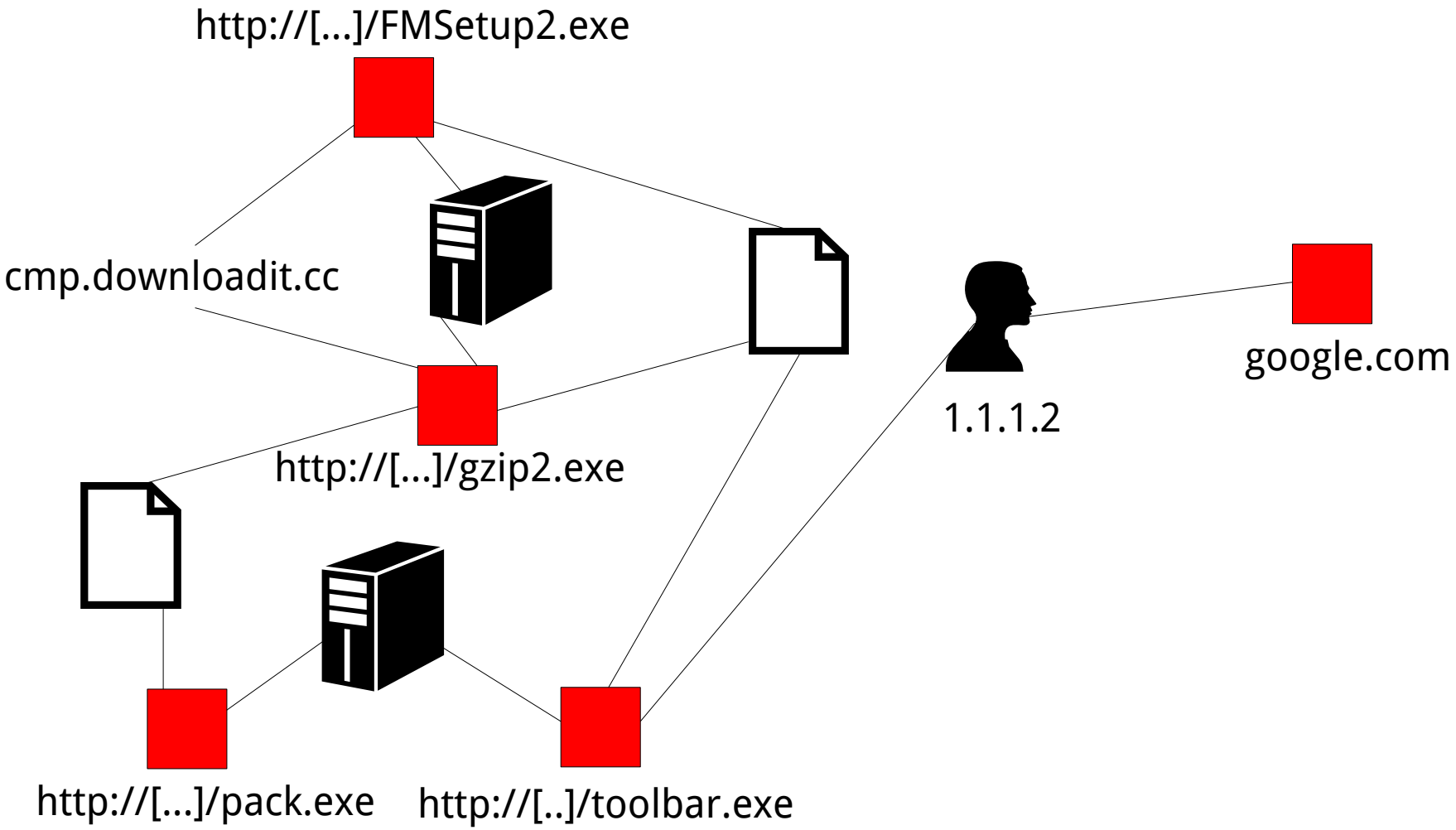


GRAPH BUILDING

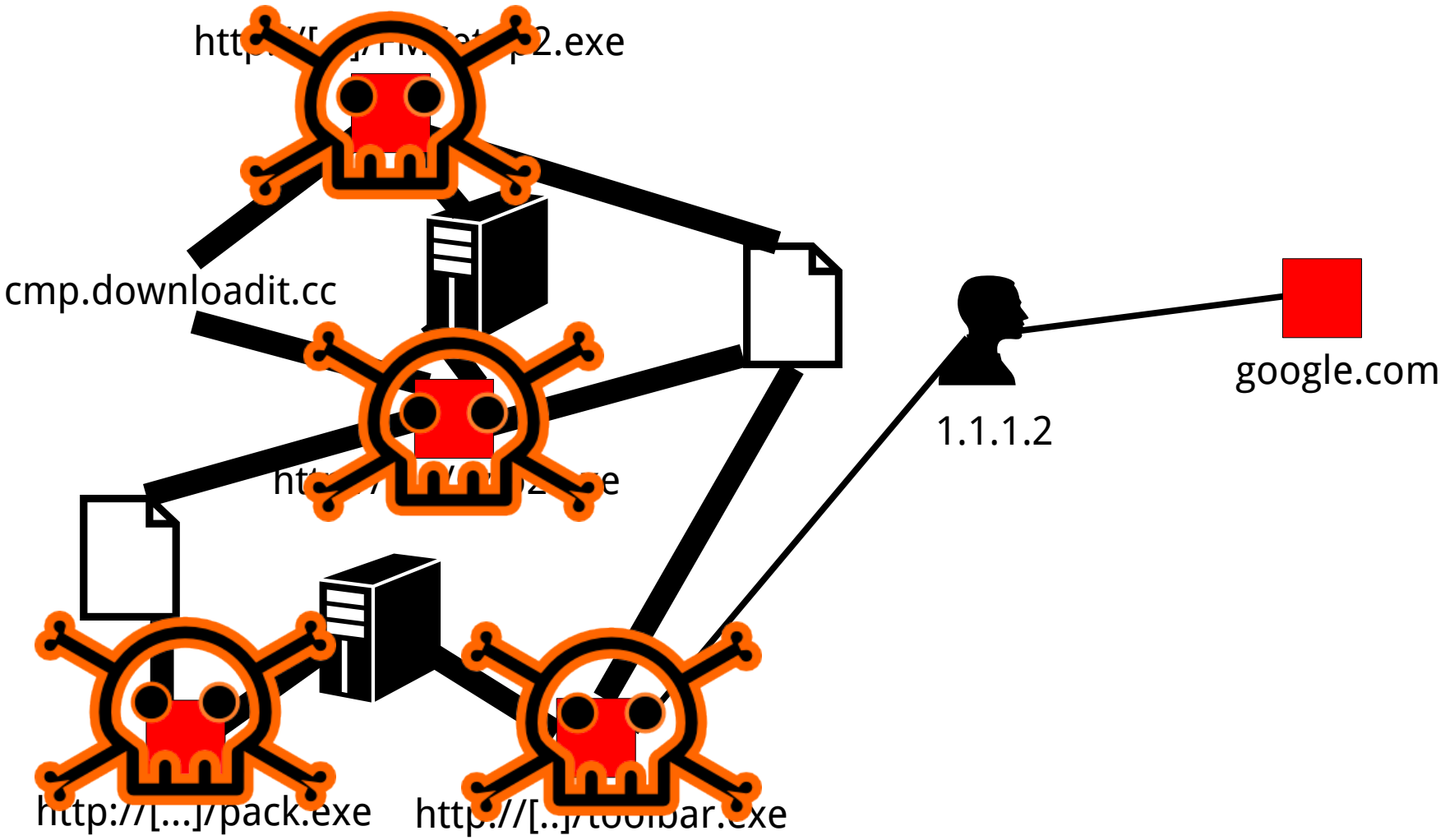


$$M_j = \sum_{i \in \text{Candidates}} \frac{1}{\text{shortestPath}(i, j)}$$

IDENTIFY MALWARE



IDENTIFY MALWARE



Nazca's

EVALUATION

7 DAYS

of traffic from an European ISP

58,335

Unique IP addresses

3,618,342

Unique files downloaded

Nazca's

EVALUATION

4

malware URLs detected by blacklists on the wire

58

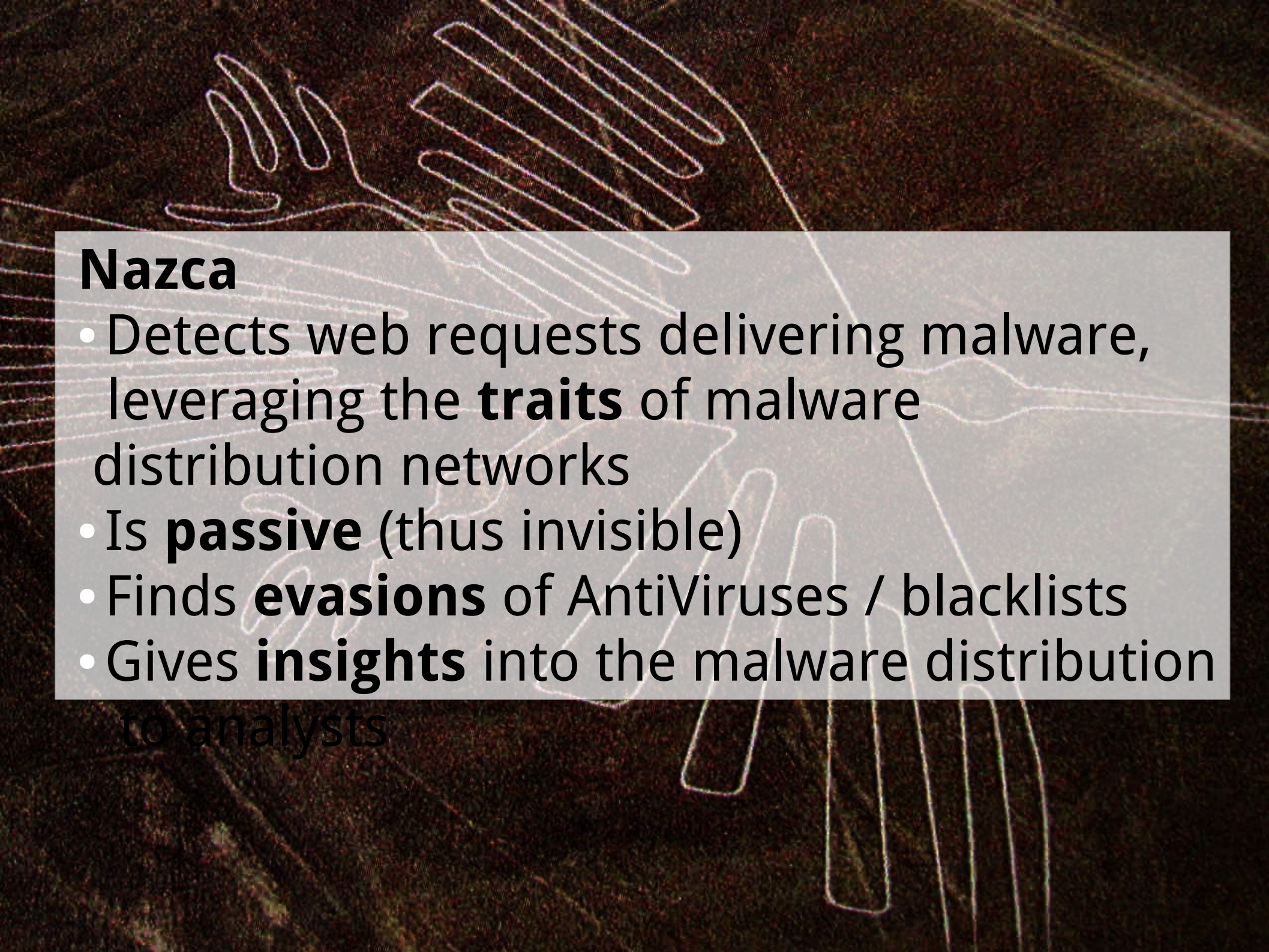
non-singleton graphs produced

54

hosted on ISP caching servers

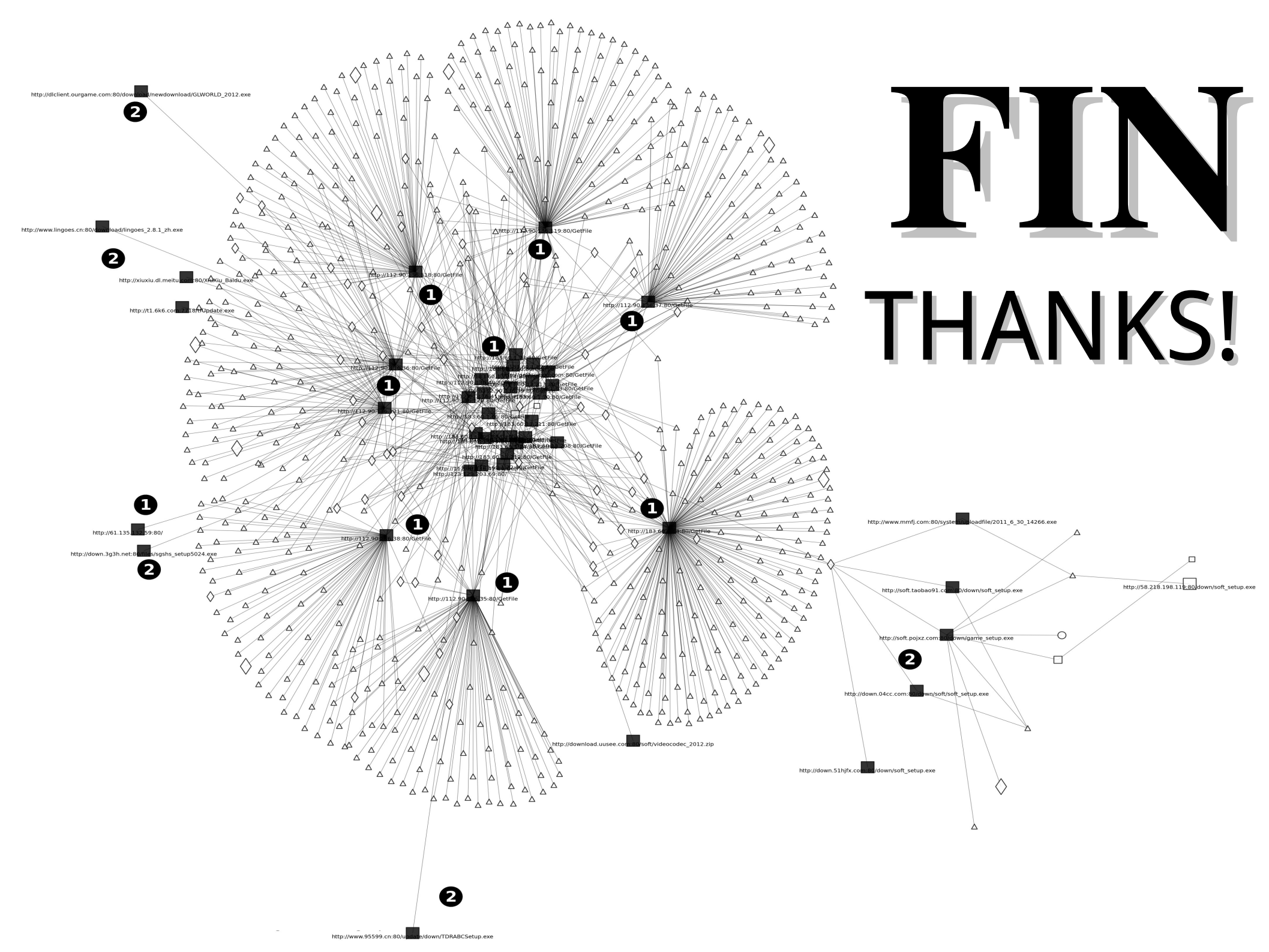
292

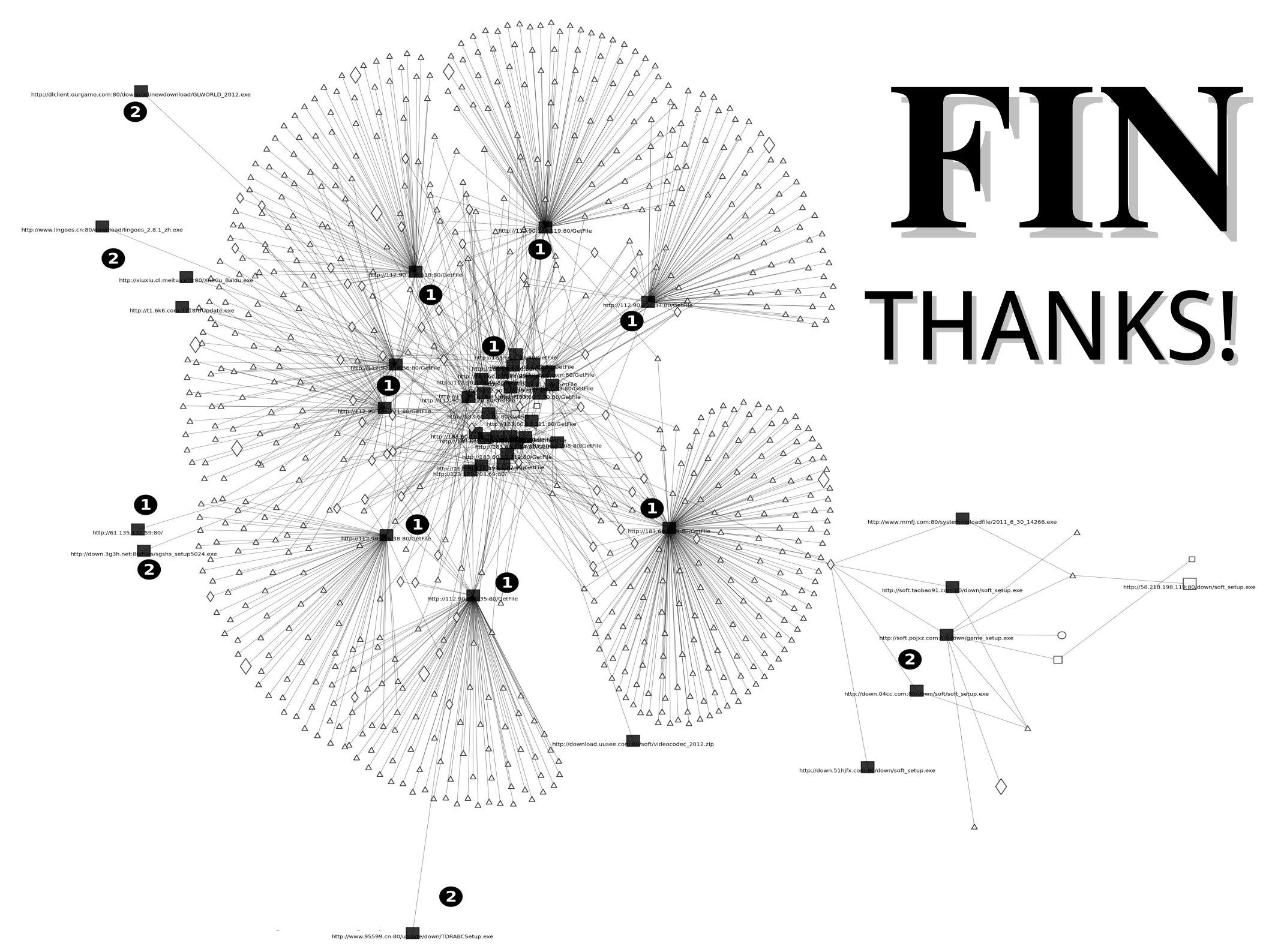
malware URLs detected by Nazca on the wire



Nazca

- Detects web requests delivering malware, leveraging the **traits** of malware distribution networks
- Is **passive** (thus invisible)
- Finds **evasions** of AntiViruses / blacklists
- Gives **insights** into the malware distribution to analysts


FIN
THANKS!
http://dlclient.ourgame.com:80/download/newdownload/GLWORLD_2012.exe
http://www.lingoes.cn:80/download/lingoes_2.8.1_zh.exe
http://xiuxiu.dl.meitu.com:80/XiuXiu_Baidu.exe
http://t1.6k6.com:8118/InUpdate.exe
http://down.3g3h.net:80/sgshs/sgshs_setup5024.exe
http://www.mmfj.com:80/systemdownloadfile/2011_6_30_14266.exe
http://soft.taobao91.com:80/down/soft_setup.exe
http://58.218.198.119:80/down/soft_setup.exe
http://soft.pojxz.com:80/down/game_setup.exe
http://down.04cc.com:80/down/soft/soft_setup.exe
http://down.51hjfx.com:80/down/soft_setup.exe
http://download.uusee.com:80/soft/videocodec_2012.zip
http://www.95599.cn:80/upgrade/down/TDRABCSetup.exe


FIN
THANKS!
http://dlclient.ourgame.com:80/download/newdownload/GLWORLD_2012.exe
http://www.lingoes.cn:80/download/lingoes_2.8.1_zh.exe
http://xiuxiu.dl.meitu.com:80/XiuXiu_Baidu.exe
http://t1.6k6.com:8118/InUpdate.exe
http://down.3g3h.net:80/sgshs/sgshs_setup5024.exe
http://www.mmfj.com:80/systemdownloadfile/2011_6_30_14266.exe
http://soft.taobao91.com:80/down/soft_setup.exe
http://58.218.198.119:80/down/soft_setup.exe
http://soft.pojxz.com:80/down/game_setup.exe
http://down.04cc.com:80/down/soft/soft_setup.exe
http://down.51hjfx.com:80/down/soft_setup.exe
http://download.uusee.com:80/soft/videocodec_2012.zip
http://www.95599.cn:80/upgrade/down/TDRABCSetup.exe