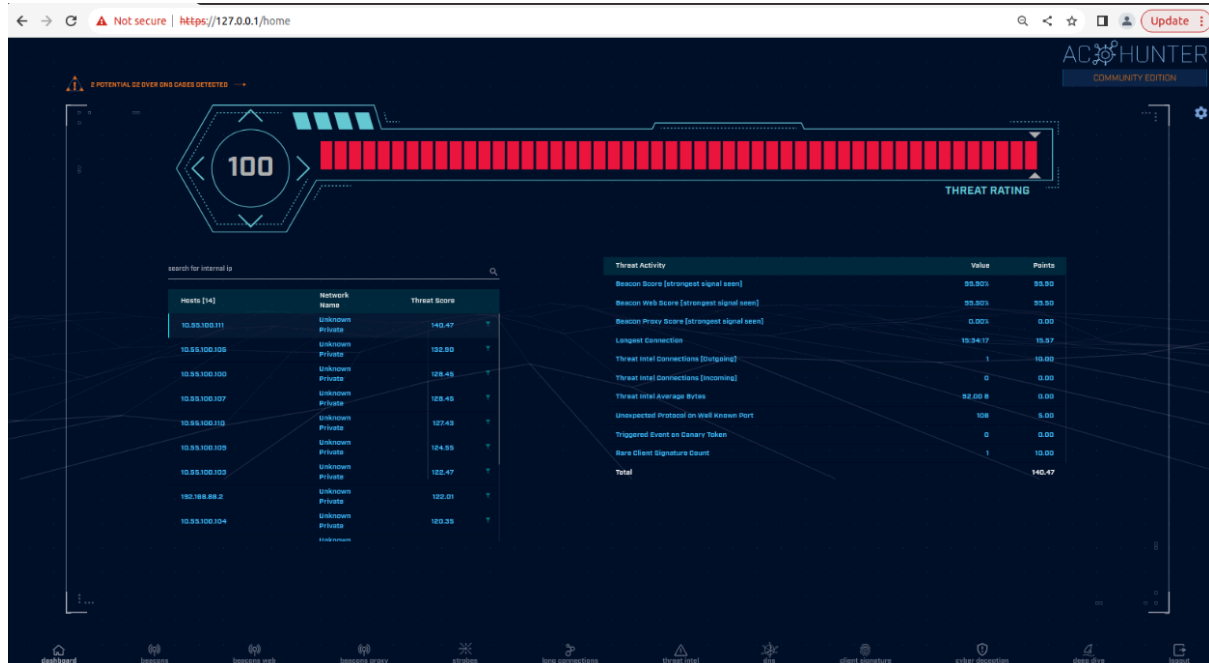


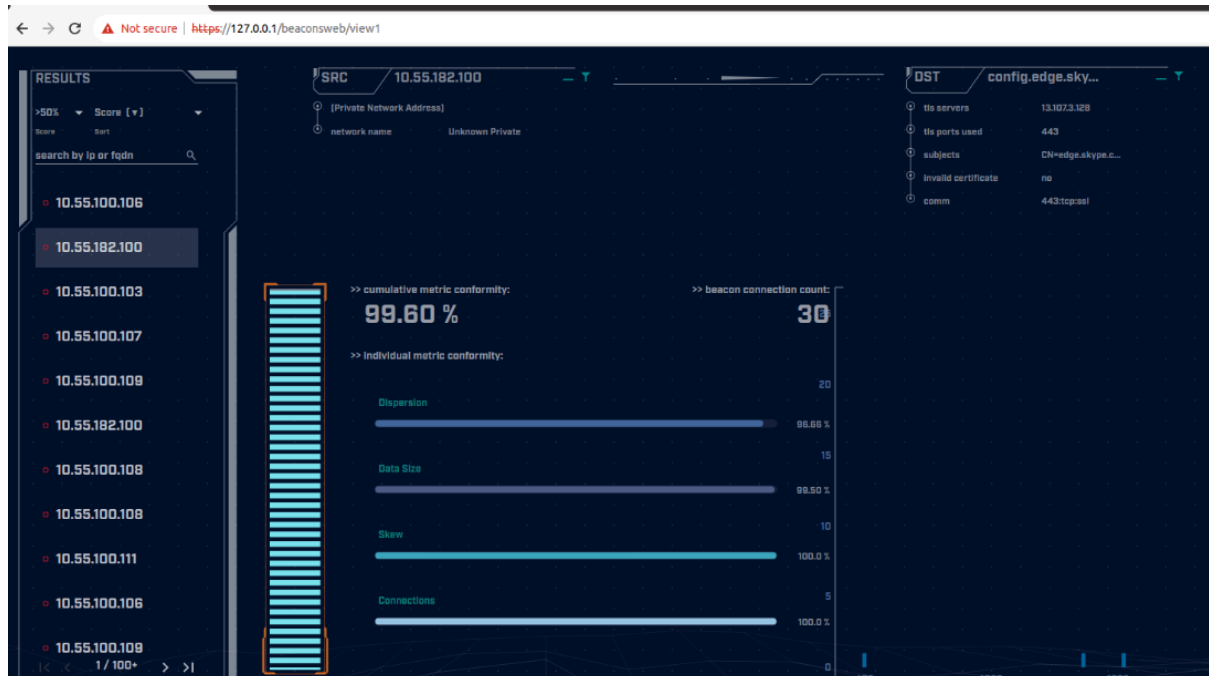
Практическая работа №4. Network Threat Hunting

Выполнил студент группы ББМО-01-23 Асатрян Д.Р.

Выбранная БД



Добавление в safelist адреса скайп



Safelist this Entry?

SRC

DOMAIN

Safelist by Domain

View/edit your full safelist in Home > Settings > Safelist.

Safelist From ...

- ☒ Safelist FQDN for all internal hosts
- ☐ 10.55.182.100
- ☐ 10.55.182.0/24

Select A Resolved FQDN ...

config.edge.skype.com ▼

Match Type ...

☒ enable wildcard

Safelist Pattern ...

.config*.edge.skype.com



Comment

Cancel

Safelist

Импорт логов 1

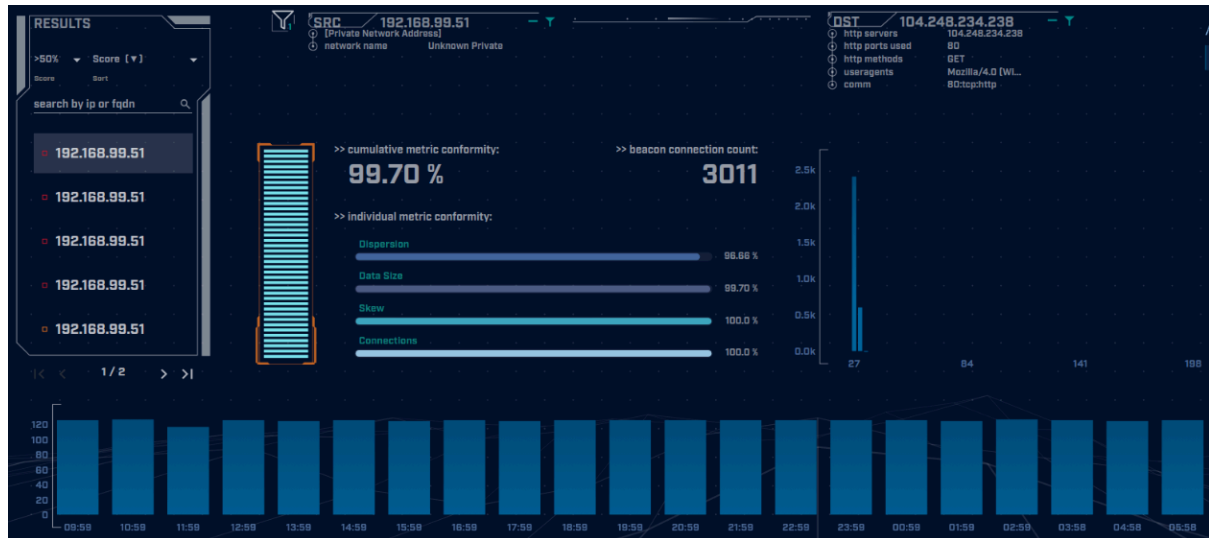
```
threat@ubuntu: ~/labs/lab1
Documents labs Pictures snap Videos
threat@ubuntu:~$ cd labs/lab
lab1/ lab2/ lab3/
threat@ubuntu:~$ cd labs/lab1/
threat@ubuntu:~/labs/lab1$ rita import *log lab1
[sudo] password for threat:
Creating achunter_api_run ... done

[+] Importing [/home/threat/labs/lab1/capture_loss.log /home/threat/labs/lab1/conn.log /home/threat/labs/lab1/dhcp.log /home/threat/labs/lab1/dns.log /home/threat/labs/lab1/files.log /home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_hosts.log /home/threat/labs/lab1/known_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.log /home/threat/labs/lab1/ntp.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/software.log /home/threat/labs/lab1/ssl.log /home/threat/labs/lab1/stats.log /home/threat/labs/lab1/x509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...
[-] Processing batch 1 of 1
[-] Parsing logs to: lab1 ...
[-] Parsing /home/threat/labs/lab1/conn.log -> lab1
[-] Parsing /home/threat/labs/lab1/dns.log -> lab1
[-] Parsing /home/threat/labs/lab1/http.log -> lab1
[-] Parsing /home/threat/labs/lab1/ssl.log -> lab1
```

Database Selection

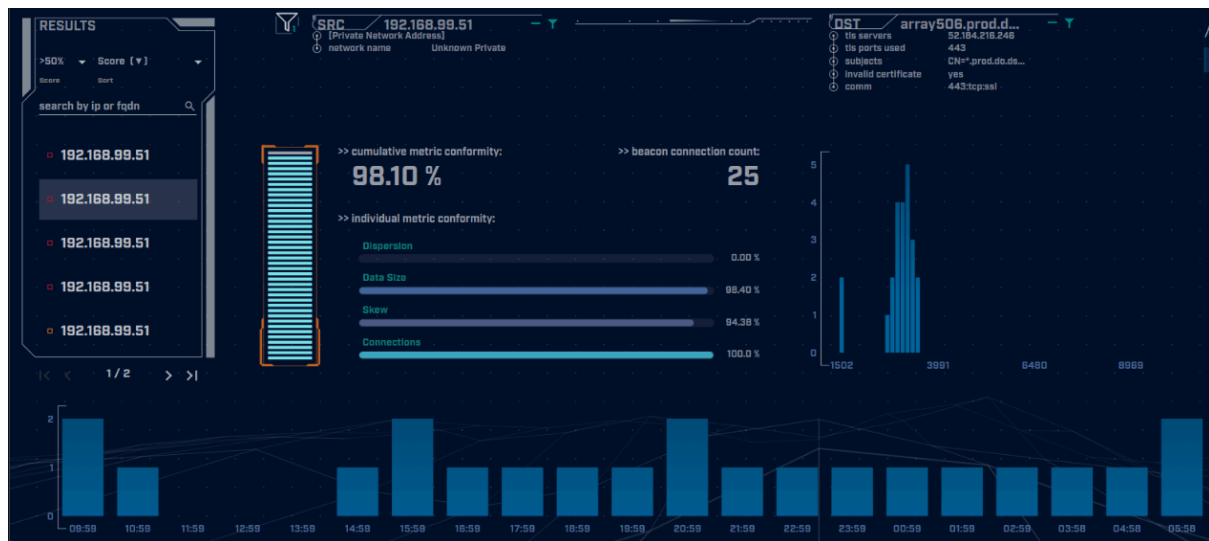
| NAME | TIMESTAMP RANGE | DELETE |
|---|----------------------------------|--------|
| <input type="radio"/> localhost-rolling | 07/25/23 11:56 -- 07/26/23 11:56 | × |
| <input checked="" type="radio"/> lab1 | 06/04/20 09:59 -- 06/05/20 09:58 | × |

Первая запись



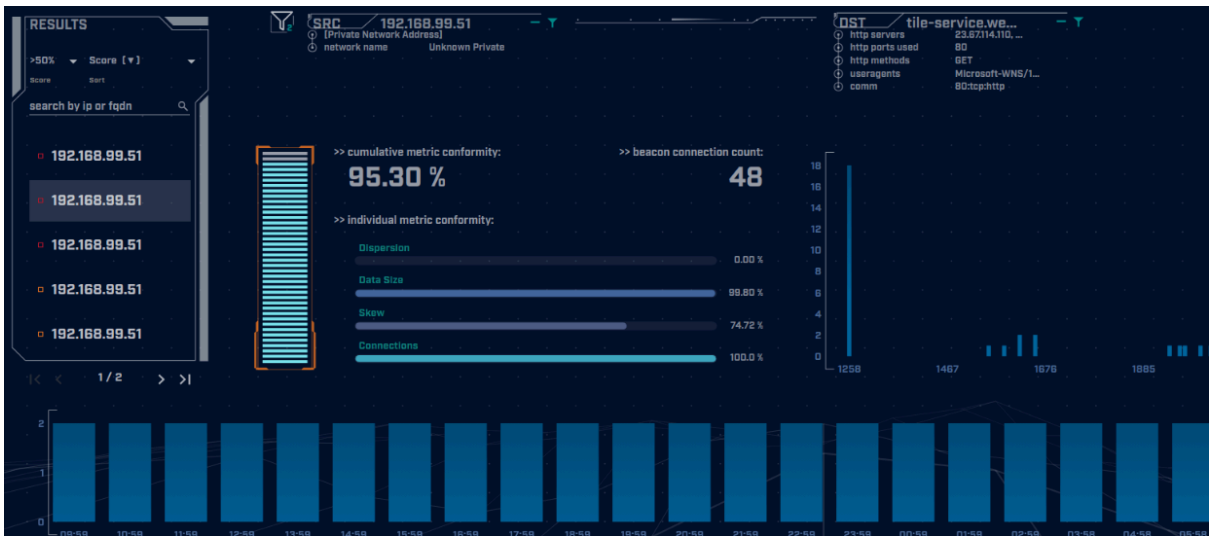
- Большое количество подключений за последние 24 часа (3 011)
- Ровная гистограмма
- Отсутствует строка хостинга. Необходимо указать полное доменное имя

Вторая запись



- Является узлом оптимизации доставки MS, который используется для установки исправлений.
- Цифровой сертификат вполне легитимный, следовательно, можно внести данную запись в safelist.

Третья запись



Итого safelist

| VIEW / EDIT GLOBAL SAFELIST | |
|---|----------------|
| Search | |
| name ↑ | type |
| *.array503.prod.do.dsp.mp.microsoft.com | domain_pattern |
| *.array506.prod.do.dsp.mp.microsoft.com | domain_pattern |
| *.config.edge.skype.com | domain_pattern |
| *.ctldl.windowsupdate.com | domain_pattern |
| *.tile-service.weather.microsoft.com | domain_pattern |
| array509.prod.do.dsp.mp.microsoft.com | domain_literal |

Просмотр записей с помощью VirusTotal

1 / 94
Community Score

1/94 security vendor flagged this IP address as malicious
167.71.97.235 (167.71.0.0/16)
AS 14061 (DIGITLOCEAN-ASN)
US
Last Analysis Date
13 days ago

ReanalyzeSimilarGraphAPI

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---------------------|-----------|-------------|-------|
| Criminal IP | Malicious | Abusix | Clean |
| Acronis | Clean | ADMINUSLabs | Clean |
| ALLabs (MONITORAPP) | Clean | AlienVault | Clean |
| alphaMountain.ai | Clean | Antiy-AVL | Clean |
| benkow.cc | Clean | BitDefender | Clean |
| Blueliv | Clean | Certego | Clean |

0 / 94
Community Score

No security vendor flagged this IP address as malicious
52.179.224.121 (52.160.0.0/11)
AS 8075 (MICROSOFT-CORP-MSN-AS-BLOCK)
US
Last Analysis Date
15 days ago

ReanalyzeSimilarGraphAPI

DETECTIONDETAILSRELATIONSCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Passive DNS Replication (12)

| Date resolved | Detections | Resolver | Domain |
|---------------|------------|-------------------------------------|---|
| 2022-04-28 | 0 / 94 | VirusTotal | micssitestp16lq.eastus2.cloudapp.azure.com |
| 2022-03-11 | 0 / 94 | VirusTotal | avsrp.eastus2.avststage.azure.com |
| 2022-01-10 | 0 / 94 | VirusTotal | micssitestn7ult5.eastus2.cloudapp.azure.com |
| 2021-02-06 | 0 / 94 | Georgia Institute of Technol ogy | americas2.wns.notifytrafficmanager.net |
| 2021-02-03 | 0 / 94 | Offensive Security | skydrive.wns.windows.com |
| 2021-01-31 | 0 / 94 | Georgia Institute of Technol ogy | wns.notifytrafficmanager.net |
| 2021-01-24 | 0 / 94 | Georgia Institute of Technol ogy | bn3p.wns.notifytrafficmanager.net |

Импорт логов 2

```
threat@ubuntu:~/labs/lab1$ rita import *log lab2
[sudo] password for threat:
Sorry, try again.
[sudo] password for threat:
Creating achunter_api_run ... done

[+] Importing [/home/threat/labs/lab1/capture_loss.log /home/threat/labs/lab1/conn.log /home/threat/labs/lab1/dhcp.log /home/threat/labs/lab1/dns.log /home/threat/labs/lab1/files.log /home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_hosts.log /home/threat/labs/lab1/known_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.log /home/threat/labs/lab1/ntp.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/software.log /home/threat/labs/lab1/ssl.log /home/threat/labs/lab1/stats.log /home/threat/labs/lab1/x509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...
[-] Processing batch 1 of 1
[-] Parsing logs to: lab2 ...
[-] Parsing /home/threat/labs/lab1/http.log -> lab2
[-] Parsing /home/threat/labs/lab1/ssl.log -> lab2
[-] Parsing /home/threat/labs/lab1/conn.log -> lab2
[-] Parsing /home/threat/labs/lab1/dns.log -> lab2
[-] Finished parsing logs in 49ms
[-] Host Analysis: 111 / 111 [=====] 100 %
[-] Unique Connection Analysis: 110 / 110 [=====] 100 %
[-] Unique Connection Aggregation: 1 / 1 [=====] 100 %
[-] No Proxy Uconn data to analyze
[-] SNI Connection Analysis: 40 / 40 [=====] 100 %
[-] Exploded DNS Analysis: 116 / 116 [=====] 100 %
[-] Hostname Analysis: 116 / 116 [=====] 100 %
[-] Beacon Analysis: 110 / 110 [=====] 100 %
[-] Beacon Aggregation: 1 / 1 [=====] 100 %
[-] No Proxy Beacon data to analyze
[-] SNI Beacon Analysis: 40 / 40 [=====] 100 %
```

Database Selection

| NAME | TIMESTAMP RANGE | DELETE |
|---|----------------------------------|--------|
| <input type="radio"/> localhost-rolling | 11/23/24 22:57 -- 11/24/24 22:57 | × |
| <input checked="" type="radio"/> lab2 | 12/31/69 16:00 -- 12/31/69 16:00 | × |
| <input type="radio"/> lab1 | 06/04/20 09:59 -- 06/05/20 09:59 | × |

| FDQNs Count | Lookups | Domain | |
|-------------|---------|--|---|
| 2074 | 2074 | honestimnotevil.com | T |
| 21 | 21 | 5da2b7f90908b408ac43ab80a.honestimnotevil.com | T |
| 21 | 21 | 8808da908228a33b29e65071a0448bc751d46292ac22b38bb5781c2762.5da2b7f90908b408ac43ab80a.honestimnotevil.com | T |
| 7 | 7 | 80a5291b4324545e080e82a0ea.honestimnotevil.com | T |
| 7 | 7 | 8a22df8d08b5032f6c2408382b70ddc5943efb182168d82ac78631d760b5291b4324545e080e82a0ea.honestimnotevil.com | T |
| 4 | 4 | 77b3a0c8a03782e440552c8f82228aed1c0a42d6b5d5f9b0c1b2cc0.3e37edc81c2394d237f9f9f8.honestimnotevil.com | T |

DNS Queries [1]

Host

172.31.28.157

Direct Connections [0]

Можно заметить большое количество обращений на различные поддомены honestimnotevil.com. Это может указывать на потенциальный C2 через DNS.

Импорт логов 3

```
threat@ubuntu:~/labs/lab1$ rita import *log lab3
creating achunter_api_run ... done

[+] Importing [/home/threat/labs/lab1/capture_loss.log /home/threat/labs/lab1/conn.log /home/threat/labs/lab1/dhcp.log
/home/threat/labs/lab1/dns.log /home/threat/labs/lab1/files.log /home/threat/labs/lab1/http.log /home/threat/labs/lab1/known_
hosts.log /home/threat/labs/lab1/known_services.log /home/threat/labs/lab1/loaded_scripts.log /home/threat/labs/lab1/notice.lo
g /home/threat/labs/lab1/ntp.log /home/threat/labs/lab1/packet_filter.log /home/threat/labs/lab1/software.log /home/threat/lab
s/lab1/ssl.log /home/threat/labs/lab1/stats.log /home/threat/labs/lab1/x509.log]:
[-] Verifying log files have not been previously parsed into the target dataset ...
[-] Processing batch 1 of 1
[-] Parsing logs to: lab3 ...
[-] Parsing /home/threat/labs/lab1/conn.log -> lab3
[-] Parsing /home/threat/labs/lab1/dns.log -> lab3
[-] Parsing /home/threat/labs/lab1/http.log -> lab3
[-] Parsing /home/threat/labs/lab1/ssl.log -> lab3
[-] Finished parsing logs in 89ms
[-] Host Analysis: 111 / 111 [=====] 100 %
[-] Unique Connection Analysis: 110 / 110 [=====] 100 %
[-] Unique Connection Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Uconn data to analyze
[-] SNI Connection Analysis: 40 / 40 [=====] 100 %
[-] Exploded DNS Analysis: 116 / 116 [=====] 100 %
[-] Hostname Analysis: 116 / 116 [=====] 100 %
[-] Beacon Analysis: 110 / 110 [=====] 100 %
[-] Beacon Aggregation: 1 / 1 [=====] 100 %
[!] No Proxy Beacon data to analyze
[-] SNI Beacon Analysis: 40 / 40 [=====] 100 %
[-] SNI Beacon Aggregation: 1 / 1 [=====] 100 %
[-] UserAgent Analysis: 8 / 8 [=====] 100 %
[-] UserAgent Aggregation: 8 / 8 [=====] 100 %
[-] Invalid Cert Analysis: 24 / 24 [=====] 100 %
[-] Indexing log entries ...
[-] Updating metadatabase ...
[-] Done!
```

Database Selection

| NAME | TIMESTAMP RANGE | DELETE |
|---|----------------------------------|--------|
| <input type="radio"/> localhost-rolling | 11/23/24 22:57 -- 11/24/24 22:57 | × |
| <input checked="" type="radio"/> lab3 | 06/26/20 12:17 -- 06/27/20 12:17 | × |
| <input type="radio"/> lab2 | 12/31/69 16:00 -- 12/31/69 16:00 | × |
| <input type="radio"/> lab1 | 06/04/20 09:59 -- 06/05/20 09:58 | × |

Данная запись нестандартна для домен “Skype”



Просмотр записи через VirusTotal

5
/ 94
Community Score

5/94 security vendors flagged this domain as malicious

newb02.skypetm.com.tw
skypetm.com.tw

Reanalyze Similar Graph API

Last Analysis Date
1 month ago

DETECTIONDETAILSRELATIONSCOMMUNITY1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Last DNS records

| Record type | TTL | Value |
|-------------|-------|---------------|
| A | 21600 | 210.71.232.11 |

Whois Lookup

Domain Name: skypetm.com.tw
Domain Status: ok
Registrant: 3432650ec337c945
Registration Service URL: http://www.net-chinese.com.tw
cns1.net-chinese.com.t: cns1.net-chinese.com.tw
cns2.net-chinese.com.t: cns2.net-chinese.com.tw