

Threat Hunting

HW09

Name: 劉定睿 ID: M11409313

Date: 2025-11-17

目錄

- 目錄
 - Shodan
 - Firetix
 - Data source:
 - Tool commands

Shodan

```
country:tw has_screenshot:true
```

SHODAN Explore Downloads Pricing country:tw has_screenshot:true Account

TOTAL RESULTS
5,850

TOP CITIES

Taipei	2,426
Taichung	1,012
Banqiao	603
Kaohsiung	510
Taoyuan City	479
More...	

TOP PORTS

3389	3,594
654	1,829
80	80
3388	48
443	31
More...	

TOP ORGANIZATIONS

Chunghwa Telecom Co., Ltd.	3,242
Ministry of Education Computer Center	403
New Century InfoComm Tech. Co., Ltd.	325
Data Communication Business Group.	307
kbro CO. Ltd.	191
More...	

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

61.219.152.181
61.219.152.181 hinet.g.hinet.net
Chunghwa Telecom Co., Ltd.
Tawan, Kaohsiung

RTSP/1.0 200 OK
Server: HG240VR 1.0
CORS: 1
PUBLIC: OPTIONS, DESCRIBE, SETUP, TEARDOWN, GET_PARAMETER, SET_PARAMETER, PLAY, PAUSE

2025-11-15 09:45:16

- IP/URL: Numerous. This statement is going to find all of the screenshot of the device in Taiwan.
- exposed port/service: Numerous.
- service banner: None.
- why it appears misconfigured or risky: Some CCTV has default password in used. Or the user use the weak password that the scanning robots can crack the device easily.
- risk assessment: High risk. The attack can monitor the camera and try to exploit the camera's vulnerability.

```
country:tw has_screenshot:true city:"Taipei" org:"Ministry of Education Computer Center" product:"VNC"
```

140.112.187.53

Ministry of Education Computer Center

Taiwan, Taipei

RFB 003.008
Authentication disabled

```
Welcome to the Frowmos Virtual Environment. Please use your web browser to
configure this server - connect to:
https://132.168.141.173:500A,
ee 1 login: root
Bu ree WIS-1 6.8.12-4-pve A1 SMP PREEMPTOYNAMIC FM B.5.18-4 (Z004-11-0RT15:6040 1
The programs...
```

```
-----
Welcome to the Proxmox Virtual Environment. Please use your web browser to
configure this server - connect to:
https://192.168.141.172:8006/
-----
```

```
b14902018-1 login: root
Password:
Linux b14902018-1 6.8.12-4-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-4 (2024-11-06T15:04Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 2 01:28:33 CST 2025 on tty1
root@b14902018-1:~# lsblk
NAME        MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
sda          8:0    0    10G  0 disk
├─sda1       8:1    0 1007K  0 part
├─sda2       8:2    0   512M  0 part
├─sda3       8:3    0    9.5G  0 part
├─pve-swap   252:0   0     1G  0 lvm  [SWAP]
└─pve-root   252:1   0    8.5G  0 lvm  /
sr0         11:0    1 1024M  0 rom
vda         253:0   0     20G  0 disk
root@b14902018-1:~# _
```

140.112.187.53

Ministry of Education Computer Center

Taiwan, Taipei

RFB 003.008
Authentication disabled

```
Welcome to the Frowmos Virtual Environment. Please use your web browser to
configure this server - connect to:
https://132.168.141.175:500A.
SCT ek aul hs
edt
Pe H1 SMP PREEMPTONAMIC PME 8.8. 1e-4 (eed-11-86Tisiede)
The programs included with the Debian G...
```

```
-----
Welcome to the Proxmox Virtual Environment. Please use your web browser to
configure this server - connect to:
https://192.168.141.175:8006/
-----
```

```
b13902040-1 login: root
Password:
Linux b13902040-1 6.8.12-4-pve #1 SMP PREEMPT_DYNAMIC PMX 6.8.12-4 (2024-11-06T15:04Z) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 2 21:11:47 CST 2025 on tty1
root@b13902040-1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp1s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master vmlbr0 state UP group default qlen 1000
    link/ether 52:54:00:20:40:01 brd ff:ff:ff:ff:ff:ff
3: enp3s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 52:54:00:20:40:02 brd ff:ff:ff:ff:ff:ff
4: vmlbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 52:54:00:20:40:01 brd ff:ff:ff:ff:ff:ff
    inet 192.168.141.175/24 scope global vmlbr0
        valid_lft forever preferred_lft forever
    inet6 fe80::5054:90ff:fe20:4001/64 scope link
        valid_lft forever preferred_lft forever
root@b13902040-1:~# _
```

- IP/URL: 140.[.112[.]187[.]53
- exposed port/service: VNC

- **service banner:** `Welcome to the Frowmos Virtual Environment. Please use your Web browser to configure this server - connect to: https://132.168.141.175:500A.`

- why it appears misconfigured or risky: VNC (Virtual Network Computing) is based on the RFB (Remote Framebuffer) protocol.

RFB itself does not enforce any encryption mechanism. If you do not configure a password, or if the password mechanism is weak (for example, standard VNC authentication using a DES 8-byte key), then anyone connecting to the VNC port (default 5900/tcp) can:

- Directly view the framebuffer (screen contents)
- Directly send mouse/keyboard events
- Capture a screenshot
- Potentially gain full control of the system

Shodan's scanners simply attempt a legitimate protocol handshake with the target service: VNC → RFB version negotiation.

Firefix

Data source:

```
{
  "type": "bundle",
  "id": "bundle--b5fedce5-4150-4f51-856e-da828de015d1",
  "objects": [
    {
      "type": "identity",
      "spec_version": "2.1",
      "id": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
      "name": "Lab Windows Security Log",
      "identity_class": "system",
      "description": "Windows Security Event Log collected from DC01.lab.local la",
      "created": "2025-11-15T03:23:03Z",
      "modified": "2025-11-15T03:23:03Z"
    },
    {
      "type": "ipv4-addr",
      "spec_version": "2.1",
      "id": "ipv4-addr--94c7e3df-08d0-430f-8fb6-bd74199efa64",
      "value": "192.0.2.55"
    },
    {
      "type": "user-account",
      "spec_version": "2.1",
      "id": "user-account--cc54d6ae-dd77-42d0-9163-b0af64080db3",
      "account_login": "Administrators"
    },
    {
      "type": "user-account",
      "spec_version": "2.1",
      "id": "user-account--232724ff-26c5-499e-ae98-ba105d929164",
      "account_login": "guest"
    },
    {
      "type": "user-account",
      "spec_version": "2.1",
      "id": "user-account--a517067d-63bf-4799-a952-4f4aa790c0b7",
      "account_login": "labadmin",
      "is_privileged": true
    },
    {
      "type": "user-account",
      "spec_version": "2.1",
      "id": "user-account--76cbd2d7-9f93-4d94-a494-011f638c11b1",
      "account_login": "tempadmin",
      "is_privileged": true
    },
    {
      "type": "user-account",
      "spec_version": "2.1",
      "id": "user-account--912c934a-bf91-4cf7-a8cb-d04600414e14",
      "account_login": "testuser"
    }
  ]
}
```

```
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--2cc4572a-61c2-4ce4-afbe-f4a2d7821336",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "created": "2025-11-15T01:10:05.123Z",
  "modified": "2025-11-15T01:10:05.123Z",
  "first_observed": "2025-11-15T01:10:05.123Z",
  "last_observed": "2025-11-15T01:10:05.123Z",
  "number_observed": 1,
  "object_refs": [
    "ipv4-addr--94c7e3df-08d0-430f-8fb6-bd74199efa64",
    "user-account--a517067d-63bf-4799-a952-4f4aa790c0b7"
  ],
  "x_event_meta": {
    "event_id": 4625,
    "record_id": "10001",
    "computer": "DC01.lab.local"
  }
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--0b1c4ad1-2c66-44ed-b6a8-41307784756d",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "created": "2025-11-15T01:10:10.456Z",
  "modified": "2025-11-15T01:10:10.456Z",
  "first_observed": "2025-11-15T01:10:10.456Z",
  "last_observed": "2025-11-15T01:10:10.456Z",
  "number_observed": 1,
  "object_refs": [
    "ipv4-addr--94c7e3df-08d0-430f-8fb6-bd74199efa64",
    "user-account--912c934a-bf91-4cf7-a8cb-d04600414e14"
  ],
  "x_event_meta": {
    "event_id": 4625,
    "record_id": "10002",
    "computer": "DC01.lab.local"
  }
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--0849dbca-7488-4df4-ba15-e2624f42b5ed",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "created": "2025-11-15T01:10:15.789Z",
  "modified": "2025-11-15T01:10:15.789Z",
  "first_observed": "2025-11-15T01:10:15.789Z",
  "last_observed": "2025-11-15T01:10:15.789Z",
  "number_observed": 1,
  "object_refs": [
    "ipv4-addr--94c7e3df-08d0-430f-8fb6-bd74199efa64",
    "user-account--232724ff-26c5-499e-ae98-ba105d929164"
  ],
  "x_event_meta": {
    "event_id": 4625,
    "record_id": "10003",
```

```
    "computer": "DC01.lab.local"
  }
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--edb23eb8-12fc-4857-b7c0-8782ddac3eb7",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "created": "2025-11-15T01:11:00.000Z",
  "modified": "2025-11-15T01:11:00.000Z",
  "first_observed": "2025-11-15T01:11:00.000Z",
  "last_observed": "2025-11-15T01:11:00.000Z",
  "number_observed": 1,
  "object_refs": [
    "ipv4-addr--94c7e3df-08d0-430f-8fb6-bd74199efa64",
    "user-account--a517067d-63bf-4799-a952-4f4aa790c0b7"
  ],
  "x_event_meta": {
    "event_id": 4624,
    "record_id": "10004",
    "computer": "DC01.lab.local"
  }
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--8437e39d-4e4f-404f-8547-944edab655df",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "created": "2025-11-15T01:12:30.000Z",
  "modified": "2025-11-15T01:12:30.000Z",
  "first_observed": "2025-11-15T01:12:30.000Z",
  "last_observed": "2025-11-15T01:12:30.000Z",
  "number_observed": 1,
  "object_refs": [
    "user-account--a517067d-63bf-4799-a952-4f4aa790c0b7"
  ],
  "x_event_meta": {
    "event_id": 4720,
    "record_id": "10005",
    "computer": "DC01.lab.local"
  }
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--a857966f-ffd3-44aa-ab88-0ca9454122b0",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "created": "2025-11-15T01:13:00.000Z",
  "modified": "2025-11-15T01:13:00.000Z",
  "first_observed": "2025-11-15T01:13:00.000Z",
  "last_observed": "2025-11-15T01:13:00.000Z",
  "number_observed": 1,
  "object_refs": [
    "user-account--cc54d6ae-dd77-42d0-9163-b0af64080db3",
    "user-account--a517067d-63bf-4799-a952-4f4aa790c0b7"
  ],
  "x_event_meta": {
    "event_id": 4728,
```

```
    "record_id": "10006",
    "computer": "DC01.lab.local"
  }
},
{
  "type": "observed-data",
  "spec_version": "2.1",
  "id": "observed-data--592a22dc-7c35-4a2e-9d8d-1ce718155a9f",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "created": "2025-11-15T01:14:00.000Z",
  "modified": "2025-11-15T01:14:00.000Z",
  "first_observed": "2025-11-15T01:14:00.000Z",
  "last_observed": "2025-11-15T01:14:00.000Z",
  "number_observed": 1,
  "object_refs": [
    "user-account--76cbd2d7-9f93-4d94-a494-011f638c11b1"
  ],
  "x_event_meta": {
    "event_id": 4672,
    "record_id": "10007",
    "computer": "DC01.lab.local"
  }
},
{
  "type": "indicator",
  "spec_version": "2.1",
  "id": "indicator--1350783b-b3c3-4fb4-87a6-c3ccb8c89614",
  "created": "2025-11-15T03:23:03Z",
  "modified": "2025-11-15T03:23:03Z",
  "created_by_ref": "identity--ff16cbcb-7cf0-4c6c-b4f2-1771211cc8e3",
  "name": "Multiple failed logons and subsequent success from 192.0.2.55 to",
  "description": "Windows Security events show several 4625 failures followed",
  "indicator_types": [
    "anomalous-activity",
    "brute-force"
  ],
  "pattern_type": "stix",
  "pattern": "[ipv4-addr:value = '192.0.2.55' AND user-account:account_login",
  "valid_from": "2025-11-15T03:23:03Z"
},
{
  "type": "attack-pattern",
  "spec_version": "2.1",
  "id": "attack-pattern--051d3848-a47a-40d4-87dc-12ced6ab5465",
  "name": "Password Brute Force Followed by Local Admin Creation",
  "description": "Attacker performs multiple failed logons, succeeds, then c",
  "created": "2025-11-15T03:23:03Z",
  "modified": "2025-11-15T03:23:03Z"
},
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--5b65538e-ae38-4997-9ee2-87a8116183e6",
  "relationship_type": "indicates",
  "source_ref": "indicator--1350783b-b3c3-4fb4-87a6-c3ccb8c89614",
  "target_ref": "attack-pattern--051d3848-a47a-40d4-87dc-12ced6ab5465",
  "created": "2025-11-15T03:23:03Z",
  "modified": "2025-11-15T03:23:03Z"
}
```

```

    },
    {
      "type": "malware",
      "spec_version": "2.1",
      "id": "malware--9a14dc50-686f-45e5-a05d-f27b580022cf",
      "name": "Generic Password Guessing Tool",
      "malware_types": [
        "brute-force"
      ],
      "is_family": false,
      "created": "2025-11-15T03:23:03Z",
      "modified": "2025-11-15T03:23:03Z",
      "description": "Represents a generic external tool used from ATTACKER01 to
    },
    {
      "type": "relationship",
      "spec_version": "2.1",
      "id": "relationship--8c234d98-a984-4915-a40c-a65e18464d16",
      "relationship_type": "uses",
      "source_ref": "attack-pattern--051d3848-a47a-40d4-87dc-12ced6ab5465",
      "target_ref": "malware--9a14dc50-686f-45e5-a05d-f27b580022cf",
      "created": "2025-11-15T03:23:03Z",
      "modified": "2025-11-15T03:23:03Z"
    }
  ]
}

```

Store as filename windows_attack_stix_bundle.json

Tool commands

- create a db that I can import the json into it:
 - `export FIREPITDB=winsec.db`
- create a firepit id. separate the different event:
 - `export FIREPITID=lab-session-1`
- import the json and store the data into winsec.db
 - `firepit cache winsec windows_attack_stix_bundle.json`
- Lookup the tables of winsec.db

- `firepit tables`

```
└─$ firepit tables
identity
observed-data
ipv4-addr
user-account
indicator
attack-pattern
relationship
malware
```

- confirm the source ip

- `firepit lookup "ipv4-addr"`

```
└─$ firepit lookup "ipv4-addr"
id                                                                 value      type
-----
ipv4-addr--94c7e3df-08d0-430f-8fb6-bd74199efa64 192.0.2.55  ipv4-addr
```

- check the timestamped of 192.0.2.55

- `firepit timestamped ipv4-addr value`

```
└─$ firepit timestamped ipv4-addr value
first_observed      value
-----
2025-11-15T01:10:05.123Z 192.0.2.55
2025-11-15T01:10:10.456Z 192.0.2.55
2025-11-15T01:10:15.789Z 192.0.2.55
2025-11-15T01:11:00.000Z 192.0.2.55
```

- `firepit value-counts ipv4-addr value`

```
└─$ firepit value-counts ipv4-addr value
value      count
-----
192.0.2.55      4
```

- firepit timestamped user-account

```

$ firepit timestamped user-account
first_observed      id                                     account_login      is_privileged
-----
2025-11-15T01:10:05.123Z user-account--a517067d-63bf-4799-a952-4f4aa790c0b7 labadmin           1
2025-11-15T01:10:10.456Z user-account--912c934a-bf91-4cf7-a8cb-d04600414e14 testuser
2025-11-15T01:10:15.789Z user-account--232724ff-26c5-499e-ae98-ba105d929164 guest
2025-11-15T01:11:00.000Z user-account--a517067d-63bf-4799-a952-4f4aa790c0b7 labadmin           1
2025-11-15T01:12:30.000Z user-account--a517067d-63bf-4799-a952-4f4aa790c0b7 labadmin           1
2025-11-15T01:13:00.000Z user-account--cc54d6ae-dd77-42d0-9163-b0af64080db3 Administrators
2025-11-15T01:13:00.000Z user-account--a517067d-63bf-4799-a952-4f4aa790c0b7 labadmin           1
2025-11-15T01:14:00.000Z user-account--76cbd2d7-9f93-4d94-a494-011f638c11b1 tempadmin          1

```

- firepit timestamped user-account account-login

```

$ firepit timestamped user-account account_login
first_observed      account_login
-----
2025-11-15T01:10:05.123Z labadmin
2025-11-15T01:10:10.456Z testuser
2025-11-15T01:10:15.789Z guest
2025-11-15T01:11:00.000Z labadmin
2025-11-15T01:12:30.000Z labadmin
2025-11-15T01:13:00.000Z Administrators
2025-11-15T01:13:00.000Z labadmin
2025-11-15T01:14:00.000Z tempadmin

```

- firepit value-counts user-account account-login

```

$ firepit value-counts user-account account_login
account_login      count
-----
Administrators     1
guest              1
labadmin           4
tempadmin          1
testuser           1

```

- firepit lookup "malware"

```

$ firepit lookup "malware"
id                                     name                                     malware_types      is_family      created
-----
modified      type      description
-----
malware--9a14dc50-686f-45e5-a05d-f27b580022cf Generic Password Guessing Tool ["brute-force"] 0 2025-11-15T03:23:03Z 2025-11-15T03:23:03Z Represents a generic external tool used from ATTACKER01 to perform password guessing against LAB accounts. malware

```

- `firepit lookup "attack-pattern"`

```
-$ firepit lookup "attack-pattern"
id                                     name                                     descript
ion                                     modified                                 type
-----
attack-pattern--051d3848-a47a-40d4-87dc-12ced6ab5465 Password Brute Force Followed by Local Admin Creation Attacker
performs multiple failed logons, succeeds, then creates a new local admin account and grants high privileges (events
4625, 4624, 4720, 4728, 4672). 2025-11-15T03:23:03Z 2025-11-15T03:23:03Z attack-pattern
```