Threat Hunting

HW09

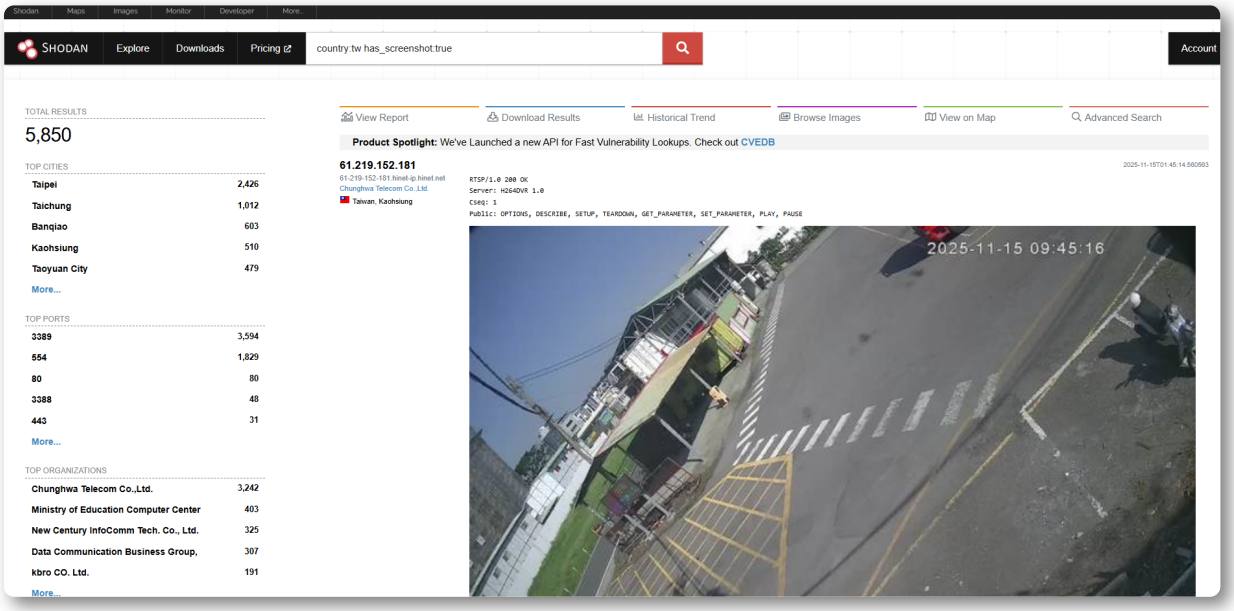
Name: 劉定睿 ID: M11409313

Date: 2025-11-17

目錄

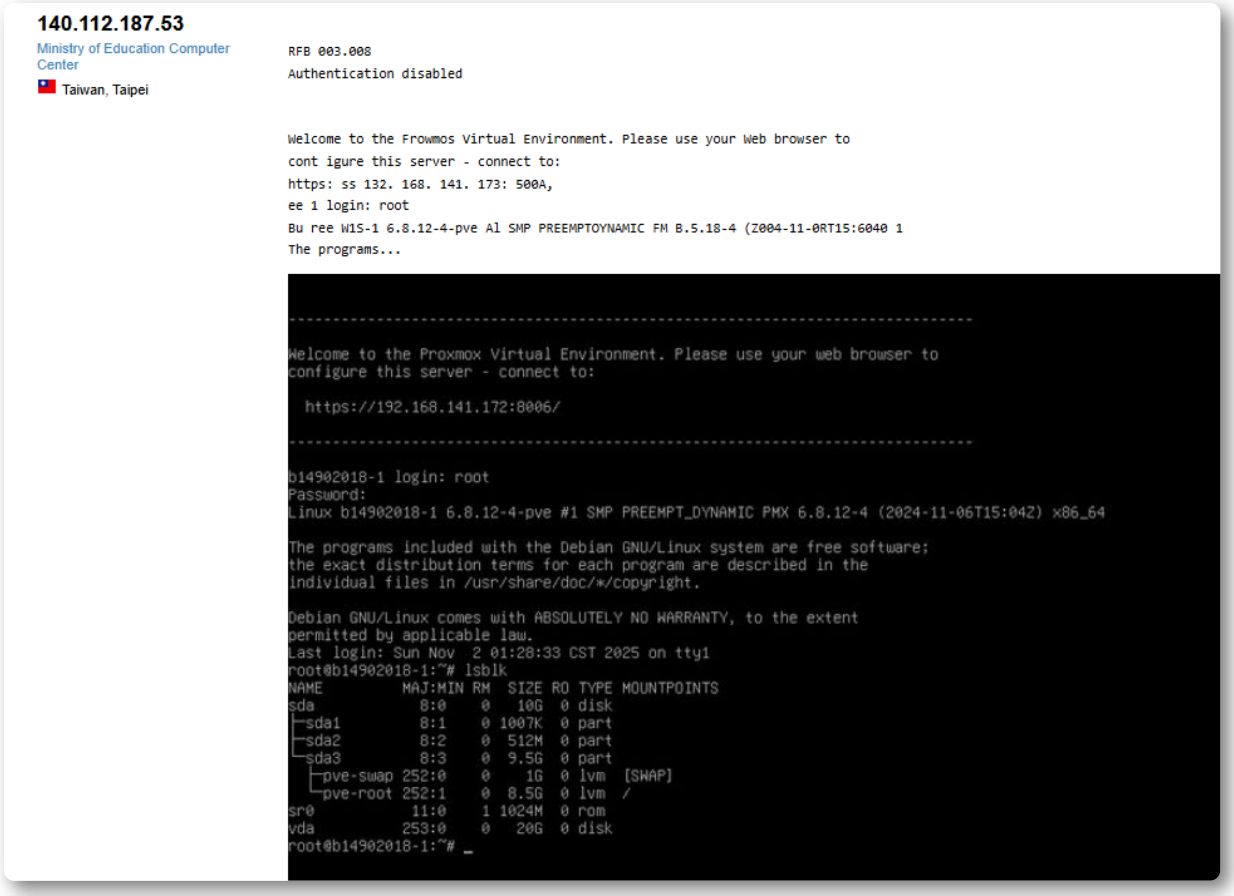
Shodan

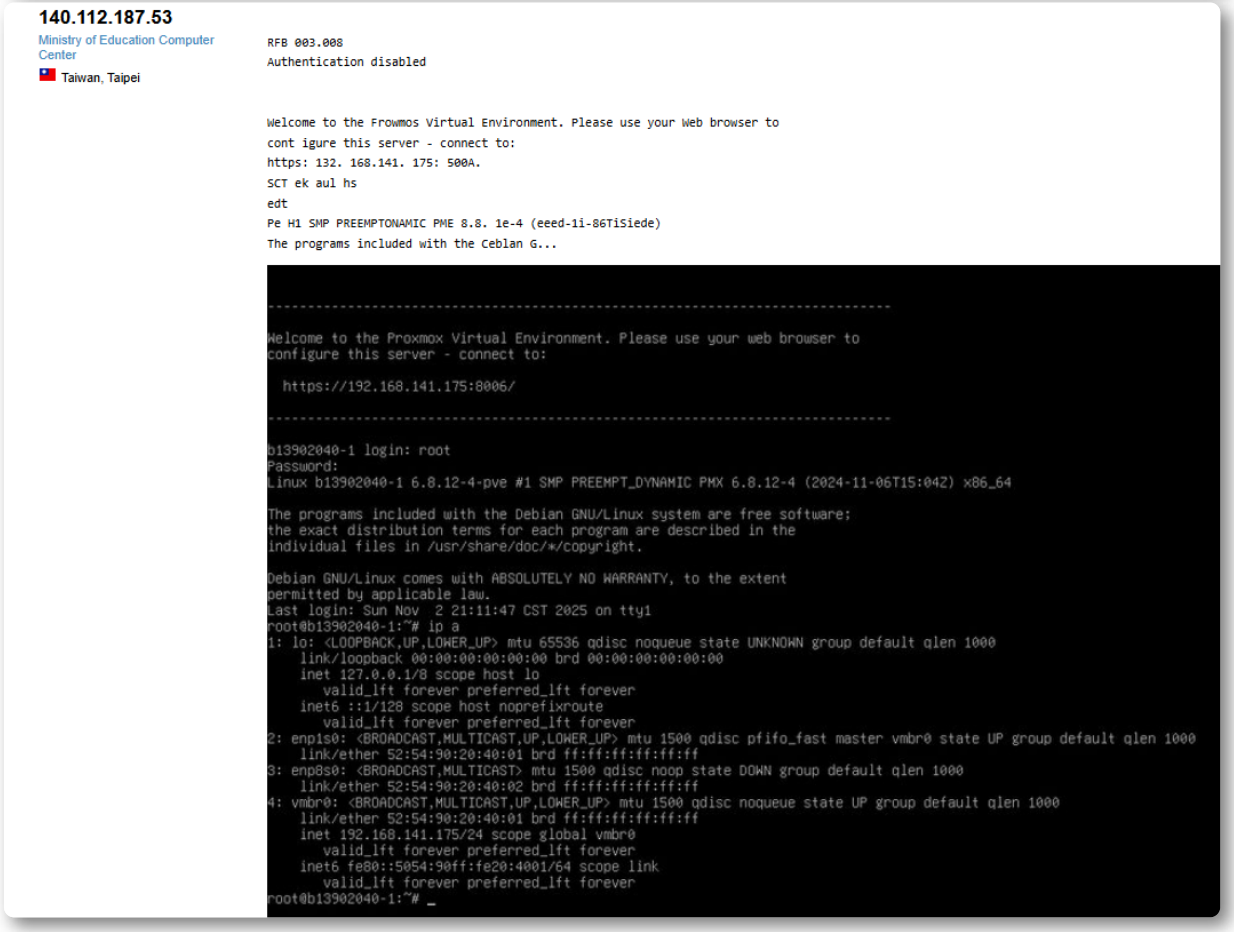
`country:tw has_screenshot:true`



- 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"`





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

- service banner: `Welcome to the Frowmos Virtual Environment. Please use your Web browser to cont igure 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.

Firetix

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 1
      "description": "Windows Security events show several 4625 failures followe
      "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. seperate 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             description
                        type
----------------------------------------  --------------------------  ---------------  -----------  --------
------------  -------------------  ------------------------------------------------------------------------
------------------------  -------
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 guess
ing against LAB accounts.  malware
```

- `firepit lookup "attack-pattern"`