2025

THREAT ACTOR PROFILE REPORT: APT41 (A.K.A. WICKED PANDA)

Made by: CyberSentinels

Table of Contents

1 Executive Summary

APT41 is a **Chinese state-sponsored threat group** active since at least **2012**, known for conducting both **cyber espionage** and **financially motivated operations**. The group has targeted a wide range of industries globally, including **healthcare, telecom, technology, finance, education, retail, and video games**. Their dual-purpose operations make them unique among Chinese APTs, blending state objectives with personal profit.

2 Background

- **Aliases:** Wicked Panda, BARIUM, Brass Typhoon, Winnti, Double Dragon
- **Attribution:** People's Republic of China (PRC)
- **Motivation:**
    - **Espionage** – supporting state intelligence objectives.
    - **Financial Gain** – targeting gaming and financial sectors for profit.
- **Notable Activity:**
    - ❖ **2010-2012:** Increased focus on the gaming industry.
    - ❖ **2017**: Notable supply chain attacks via CCleaner, demonstrating sophisticated capabilities.
    - ❖ **2019**: Official identification as APT41; conducted wide-ranging campaigns exploiting zero-day vulnerabilities.
    - ❖ **2020**: U.S. Department of Justice indicted several members for compromising over 100 companies globally.
    - ❖ **2021-2023:** Adapted to and exploited emerging vulnerabilities like Log4Shell and targeted attacks on U.S. state governments

3 Target Profile

- **Industries:** Healthcare, telecom, education, finance, retail, video games, government.
- **Geography:** Global operations, with a strong focus on the **United States** and **Asia-Pacific**.
- **Victimology:**
    - Surveillance of government and defense entities.
    - Theft of intellectual property from private companies.
    - Compromise of video game companies for financial gain.

4 Tactics, Techniques, and Procedures (TTPs)

MITRE ATT&CK Mapping

- **Initial Access:**
  - Exploit Public-Facing Applications (T1190)
  - Spearphishing Attachment (T1566.001)
- **Execution:**
  - Command and Scripting Interpreter: PowerShell (T1059.001)
- **Persistence:**
  - Web Shells (T1505.003)
  - Scheduled Tasks (T1053.005)
- **Privilege Escalation:**
  - Exploitation for Privilege Escalation (T1068)
- **Credential Access:**
  - Credential Dumping with Mimikatz (T1003.001)
- **Defense Evasion:**
  - Obfuscated/Encrypted Files (T1027)
- **Exfiltration:**
  - Exfiltration Over Web Services (T1567.002)

5 Tools and Malware

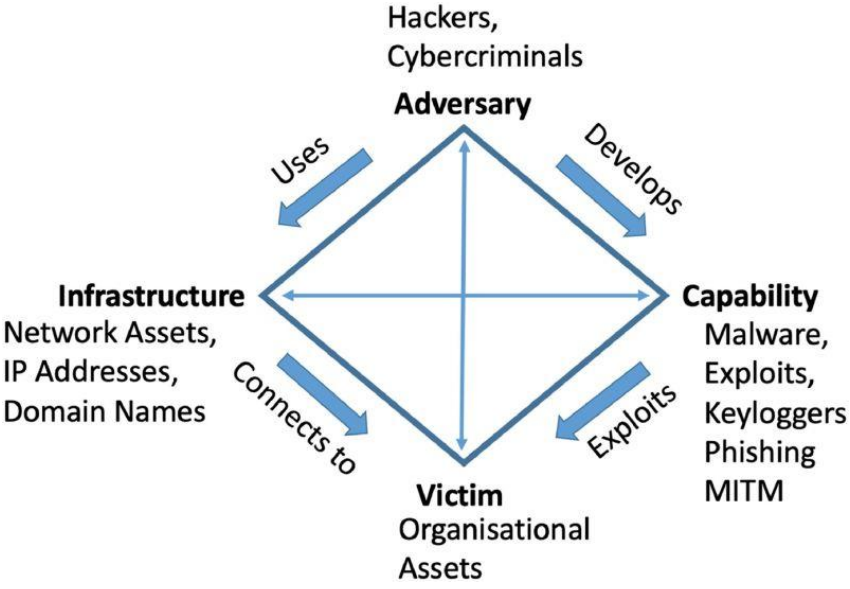
APT41 has used a wide arsenal of malware and tools, including:

- **PlugX**
- **ShadowPad**
- **Cobalt Strike** (beacons)
- **Gh0st RAT**
- **Winnti for Linux** (trojan)
- **Mimikatz** (credential theft)

- **SQLmap** (database exploitation)

6 Diamond Model of Intrusion

- **Adversary:** APT41 (Chinese state-sponsored group).
- **Capability:** Malware families (PlugX, ShadowPad, Winnti), exploitation of zero-days.
- **Infrastructure:** C2 servers, compromised domains, cloud-based exfiltration.
- **Victim:** Global enterprises in healthcare, finance, telecom, and government.



7 Indicators of Compromise (IOCs)

7.1 Normal Table

Type	Indicator
FileHash-MD5	100b463eff8295ba617d3ad6df5325c6
FileHash-MD5	125b257520d16d759b112399c3cd1466
FileHash-MD5	15097a32b515d10ad6d793d2d820f2a8
FileHash-MD5	2cd15977b72d5d74fadedfde2ce8934f
FileHash-MD5	2f9d2d8c4f2c50cc4d2e156b9985e7ca
FileHash-MD5	3021c9bca4ef3aa672461ecadc4718e6
FileHash-MD5	3af014db9be1a04e8b312b55d4479f69
FileHash-MD5	4708a2ae3a5f008c87e68ed04a081f18
FileHash-MD5	740d6eb97329944d82317849f9bbd633
FileHash-MD5	91d10c25497cadb7249d47ae8ec94766
FileHash-MD5	9b00b6f93b70f09d8b35fa9a22b3cba1
FileHash-MD5	9b4f0f94133650b19474af6b5709e773

FileHash-MD5	9d53a0336acfb9e4df11162ccf7383a0
FileHash-MD5	a052536e671c513221f788de2e62316c
FileHash-MD5	a236dce873845ba4d3ccd8d5a4e1aefd
FileHash-MD5	c149252a0a3b1f5724fd76f704a1e0af
FileHash-MD5	c3ed337e2891736db6334a5f1d37dc0f
FileHash-MD5	c7188c39b5c53ecbd3aec77a856ddf0c
FileHash-MD5	f1025fcad036aad8bf124df8c9650bbc
URL	hxxp[://]chyedweeyaxkavyccenwjvqrsgvyj0o1y[.]oast[.]fun/aaa
URL	hxxp[://]github[.]githubassets[.]net/okaqbfk867hmx2tvqxhc8zyq9fy694gf/hta
URL	hxxp[://]toun[.]callback[.]red/aaa
domain	azure[.]online
domain	msn-microsoft[.]org
domain	s3-azure[.]com
domain	upload-microsoft[.]com
hostname	ap-northeast-1[.]s3-azure[.]com
hostname	chyedweeyaxkavyccenwjvqrsgvyj0o1y[.]oast[.]fun
hostname	github[.]githubassets[.]net
hostname	ns1[.]s3-azure[.]com
hostname	ns2[.]s3-azure[.]com
hostname	toun[.]callback[.]red
hostname	www[.]msn-microsoft[.]org
hostname	www[.]upload-microsoft[.]com
IPv4	107[.]182[.]24[.]70
IPv4	108[.]72[.]244[.]95
IPv4	110[.]45[.]165[.]238
IPv4	121[.]126[.]239[.]192
IPv4	144[.]202[.]98[.]198

7.2 Stix 2.1


```
{
  "id": "bundle--55cb46fa-057b-406a-b93f-933a97e38e25",
  "objects": [
    {
      "created": "2025-08-21T07:07:32.474Z",
      "created_by_ref": "identity--ab072f15-9b87-4ee1-898f-b584d41f29b0",
      "id": "report--55cb46fa-057b-406a-b93f-933a97e38e25",
      "labels": [
        "threat-report"
      ],
      "modified": "2025-09-19T10:04:41.410Z",
      "name": "SOC files: an APT41 attack on government IT services in Africa",
      "object_refs": [
```

```
        "identity--ab072f15-9b87-4ee1-898f-b584d41f29b0",
        "indicator--33fda4a5-a93a-4fab-b03e-e8286a75b0d0",
        "indicator--c1763f54-5db9-4fa6-a104-e6e5bf0dd0c2",
        "indicator--8c464136-8879-49bc-a8af-b97948dda265",
        "indicator--5c5c046d-0b51-465e-adfa-1dfb652adf64",
        "indicator--37aef56a-4b13-462e-a63a-6968cd6c7801",
        "indicator--6db8c84d-bc99-47c7-8fd2-68201825faa5",
        "indicator--f895e7ee-d236-4a7f-b1c2-7e3443094915",
        "indicator--fc668c86-9120-4af8-a778-78a1d26a3371",
        "indicator--14d8b921-8931-4ee8-8d10-49b2a11373f9",
        "indicator--75a25aea-9583-4a0d-8966-5139b5f5b8bb",
        "indicator--3ba48cf8-7411-4fbc-9d13-117ed162aba9",
        "indicator--6d106fc7-d6e5-4ed4-bd65-b6e5420ada55",
        "indicator--6a217db0-0b38-47b7-8eae-0c452091ab11",
        "indicator--3021c4f3-1163-4318-9314-356a17f492f2",
        "indicator--251d90d5-7b44-45df-8392-3b426ea0d35c",
        "indicator--7d8531a7-69f4-4271-8c44-fa876f9e6c63",
        "indicator--4673525c-7d7c-40e5-bab1-eefeba3c5bcb",
        "indicator--b95e19f9-483f-46c7-8565-9c9c02a89ebc",
        "indicator--47e1d444-fef8-44b8-b6da-48155397e724",
        "indicator--c1c6b982-021f-4fe2-90aa-3f1996f362a0",
        "indicator--0c1279e4-22f3-4fcf-acb9-ae925f0ec5fd",
        "indicator--fd18ffba-4dd1-48b1-8746-4e901bd9eea1",
        "indicator--c57edcba-a4b9-4f35-9712-f261228cfed5",
        "indicator--b8bad084-de0c-4667-af5f-0366480cc234",
        "indicator--60cd486c-77ea-4a94-bad4-bcefb12e0938",
        "indicator--170924d9-3308-4e47-b9f4-dc0e7f20819d",
        "indicator--babf7622-ee3a-4125-8346-2f0e8526e57b",
        "indicator--03772838-031e-4bee-8ea9-ff0299a4295e",
        "indicator--bd735b4f-235c-45a4-aab7-ff1dd87a4e6f",
        "indicator--36c1257c-2505-4d1e-a4db-4b2bd0ef24ca",
        "indicator--9e3bd99f-a04a-45b6-9845-afdb00f9141b",
        "indicator--cce43c13-1da8-4d9e-b86a-0635c428c300",
        "indicator--03921f71-66b0-4bb4-889c-f743f763ff62",
        "indicator--3452e138-da82-41bd-aef3-cc90b22a6744",
        "indicator--19c7682b-0c11-41be-9a61-74f4dd253262",
        "indicator--258c7ca4-26f8-4409-a069-43c6a53e2f96",
        "indicator--e9bb3831-763f-4d6b-8679-278cbbd81876",
        "indicator--9d28645a-82e9-4945-8a8c-190a2f0f95f7",
        "indicator--10e21d97-4235-404e-b988-e86733c0f260",
        "indicator--0863ca05-03ef-4697-825f-38a06954e327",
        "indicator--66462597-0974-4ce1-a4df-29b217468f9e",
        "indicator--89a620ba-d1dc-4c8b-9e87-aff259f9942e",
        "indicator--cc6b00e3-32b0-48c3-9257-d74ed5673ab9",
        "indicator--fe58efad-2b67-4f28-81b3-af445d5ebf24",
```

```
        "indicator--2e561626-39ce-482a-93ab-1d5a5d23144b",
        "indicator--6dbc0092-bb17-4ed3-8906-7f8ef324f016",
        "indicator--4b2fba9f-a60d-4f78-ad54-c8180f3c1ac5",
        "threat-actor--eb6cf2a7-7aa8-4fd1-b570-d5d8a628b9e8"
      ],
      "published": "2025-08-21T07:07:32.474Z",
      "spec_version": "2.1",
      "type": "report"
    },
    {
      "contact_information": "https://otx.alienvault.com/",
      "created": "2025-08-21T07:07:32.474Z",
      "id": "identity--ab072f15-9b87-4ee1-898f-b584d41f29b0",
      "identity_class": "organization",
      "modified": "2025-08-21T07:07:32.474Z",
      "name": "Open Threat Exchange",
      "spec_version": "2.1",
      "type": "identity"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--33fda4a5-a93a-4fab-b03e-e8286a75b0d0",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '100b463eff8295ba617d3ad6df5325c6']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--c1763f54-5db9-4fa6-a104-e6e5bf0dd0c2",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '125b257520d16d759b112399c3cd1466']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--8c464136-8879-49bc-a8af-b97948dda265",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '15097a32b515d10ad6d793d2d820f2a8']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--5c5c046d-0b51-465e-adfa-1dfb652adf64",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '2cd15977b72d5d74fadedfde2ce8934f']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--37aef56a-4b13-462e-a63a-6968cd6c7801",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '2f9d2d8c4f2c50cc4d2e156b9985e7ca']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--6db8c84d-bc99-47c7-8fd2-68201825faa5",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '3021c9bca4ef3aa672461ecadc4718e6']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--f895e7ee-d236-4a7f-b1c2-7e3443094915",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '3af014db9be1a04e8b312b55d4479f69']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--fc668c86-9120-4af8-a778-78a1d26a3371",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '4708a2ae3a5f008c87e68ed04a081f18']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--14d8b921-8931-4ee8-8d10-49b2a11373f9",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '740d6eb97329944d82317849f9bbd633']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--75a25aea-9583-4a0d-8966-5139b5f5b8bb",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '91d10c25497cadb7249d47ae8ec94766']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--3ba48cf8-7411-4fbc-9d13-117ed162aba9",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '9b00b6f93b70f09d8b35fa9a22b3cba1']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--6d106fc7-d6e5-4ed4-bd65-b6e5420ada55",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '9b4f0f94133650b19474af6b5709e773']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--6a217db0-0b38-47b7-8eae-0c452091ab11",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = '9d53a0336acfb9e4df11162ccf7383a0']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--3021c4f3-1163-4318-9314-356a17f492f2",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = 'a052536e671c513221f788de2e62316c']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--251d90d5-7b44-45df-8392-3b426ea0d35c",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = 'a236dce873845ba4d3ccd8d5a4e1aefd']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--7d8531a7-69f4-4271-8c44-fa876f9e6c63",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = 'c149252a0a3b1f5724fd76f704a1e0af']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--4673525c-7d7c-40e5-bab1-eefeba3c5bcb",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = 'c3ed337e2891736db6334a5f1d37dc0f']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--b95e19f9-483f-46c7-8565-9c9c02a89ebc",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[file:hashes.MD5 = 'c7188c39b5c53ecbd3aec77a856ddf0c']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--258c7ca4-26f8-4409-a069-43c6a53e2f96",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'azure.online']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--e9bb3831-763f-4d6b-8679-278cbbd81876",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'msn-microsoft.org']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--9d28645a-82e9-4945-8a8c-190a2f0f95f7",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 's3-azure.com']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--10e21d97-4235-404e-b988-e86733c0f260",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'upload-microsoft.com']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--0863ca05-03ef-4697-825f-38a06954e327",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'ap-northeast-1.s3-azure.com']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
```

```
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--66462597-0974-4ce1-a4df-29b217468f9e",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value =
'chyedweeyaxkavyccenwjvqrsgvyj0o1y.oast.fun']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--89a620ba-d1dc-4c8b-9e87-aff259f9942e",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'github.githubassets.net']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--cc6b00e3-32b0-48c3-9257-d74ed5673ab9",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'ns1.s3-azure.com']",
      "pattern_type": "stix",
```

```
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--fe58efad-2b67-4f28-81b3-af445d5ebf24",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'ns2.s3-azure.com']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--2e561626-39ce-482a-93ab-1d5a5d23144b",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'toun.callback.red']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--6dbc0092-bb17-4ed3-8906-7f8ef324f016",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'www.msn-microsoft.org']",
      "pattern_type": "stix",
```

```
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "created": "2025-08-21T07:07:32.000Z",
      "description": "",
      "id": "indicator--4b2fba9f-a60d-4f78-ad54-c8180f3c1ac5",
      "labels": [],
      "modified": "2025-08-21T07:07:32.000Z",
      "name": "OTX pulse_name=SOC files: an APT41 attack on government IT
services in Africa",
      "pattern": "[domain-name:value = 'www.upload-microsoft.com']",
      "pattern_type": "stix",
      "pattern_version": "2.1",
      "spec_version": "2.1",
      "type": "indicator",
      "valid_from": "2025-08-21T07:07:32.000Z"
    },
    {
      "aliases": null,
      "created": "2025-08-21T07:07:32.474Z",
      "description": [
        "APT41 is a prolific cyber threat group that carries out Chinese state-
sponsored espionage activity in addition to financially motivated activity
potentially outside of state control."
      ],
      "external_references": [
        [
          {
            "source_name": "MISP Threat Actor list",
            "url": "https://www.fireeye.com/blog/threat-research/2019/08/apt41-
dual-espionage-and-cyber-crime-operation.html"
          },
          {
            "source_name": "MISP Threat Actor list",
            "url": "https://unit42.paloaltonetworks.com/apt41-using-new-
speculoos-backdoor-to-target-organizations-globally/"
          }
        ]
      ],
      "id": "threat-actor--eb6cf2a7-7aa8-4fd1-b570-d5d8a628b9e8",
      "labels": [
        "activist"
```

```
      ],
      "modified": "2025-08-21T07:07:32.474Z",
      "name": "APT41",
      "spec_version": "2.1",
      "type": "threat-actor"
    }
  ],
  "spec_version": "2.1",
  "type": "bundle"
}
```


8 Summary

APT41 remains one of the **most versatile and dangerous Chinese APTs**, capable of both **state espionage** and **criminal operations**. Their use of **supply chain attacks** and **zero-day exploits** demonstrates advanced capabilities. Organizations should prioritize **patch management, network segmentation, and monitoring for ATT&CK techniques** associated with APT41.

8.1 NIST Cybersecurity Framework (CSF) Alignment:

This project was designed and executed in alignment with the five core functions of the **NIST Cybersecurity Framework**, ensuring a structured and standards-based approach to threat intelligence and hunting.

- **Identify → Threat Actor Profiling**
  Conducted detailed profiling of APT41 using MITRE ATT&CK and CTI feeds. This established a clear understanding of adversary motivations, capabilities, and targeted sectors, enabling risk awareness and prioritization.
- **Protect → IOC Enrichment for Proactive Defense**
  Integrated and enriched Indicators of Compromise (IOCs) from AlienVault OTX and MISP. This proactive enrichment supports defensive measures by providing actionable intelligence to block malicious infrastructure and tools before exploitation.
- **Detect → Hunting Lab and Log Analysis**
  Built a controlled hunting lab with simulated adversary activity (red atomic team tool). Leveraged Wireshark and Splunk to analyze logs, validate hypotheses, and detect malicious behaviors mapped to MITRE ATT&CK techniques.
- **Respond → Incident Handling Aligned with ISO/IEC 27035**
  Applied structured incident management principles to assess, contain, and document simulated intrusions. This ensured that detection findings were translated into actionable response steps consistent with ISO/IEC 27035.

- **Recover → Lessons Learned and Remediation**
  Documented detection gaps, evaluated defensive effectiveness, and recommended remediation strategies. These lessons learned feed back into the CTI pipeline, strengthening resilience and supporting continuous improvement.

9 References

- MITRE ATT&CK Group G0096 – APT41
- ATT&CK® Navigator
- FortiGuard Threat Actor Encyclopedia
- Apt41 Arisen from Dust
- https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html#_1j0vun2r7rgb
- https://www.cisa.gov/sites/default/files/2022-12/stix-bp-v1.0.0.pdf
- Johnson, C. , Feldman, L. and Witte, G. (2017), Cyber Threat Intelligence and Information Sharing, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=923332 (Accessed October 20, 2025)
- https://www.iso.org/standard/68427.html
- https://www.iso.org/standard/78973.html
- https://otx.alienvault.com/adversary/APT41
- https://otx.alienvault.com/pulse/68abf0f55f8716f665e33ffd
- https://otx.alienvault.com/pulse/68480e89dbe1f2bc0746a80c
- https://otx.alienvault.com/pulse/68de2cc8e4c38a8cbc7ffc40