

# Analysis of ArcaneDoor Threat Infrastructure Suggests Potential Ties to Chinese-based Actor

: 5/1/2024

---

## Executive Summary:

- Cisco Talos identified three zero days in **two Cisco firewall products** as part of an investigation into a larger **threat actor campaign called “ArcaneDoor”** that targeted **government-owned perimeter network devices globally**, with exploitation going back to January 2024
- The zero day vulnerabilities identified are tracked as **CVE-2024-20353, CVE-2024-20359, and CVE-2024-20358** – of these, only CVE-2024-20353 and CVE-2024-20359 were exploited in the ArcaneDoor campaign
- While the initial access vector leveraged in this campaign is still unknown, Cisco has released **software updates** & has provided steps for customers to check the integrity of their Cisco Firewall devices in their [event response advisory](#)
- When we investigated the actor-controlled IPs provided by Talos in Censys data and cross-referenced the with other certificate indicators, we discovered compelling data suggesting the **potential** involvement of **an actor based in China**, including links to multiple major Chinese networks and the presence of Chinese-developed anti-censorship software. It’s tough to draw definitive conclusions at this stage.

As the investigation into ArcaneDoor continues, further data about the victims of these attacks are expected to emerge. In the interim, please consult our [Rapid Response advisory](#) for comprehensive insights into the scale of exposed Cisco ASA devices and guidance on remediation.

## Understanding the ArcaneDoor Campaign

On April 24, [Cisco Talos released a report](#) shedding light on a campaign by a previously unknown state-sponsored threat actor tracked as “**UAT4356**”. The campaign, dubbed “**ArcaneDoor**,” targeted government-owned perimeter network devices from various vendors as part of a global effort.

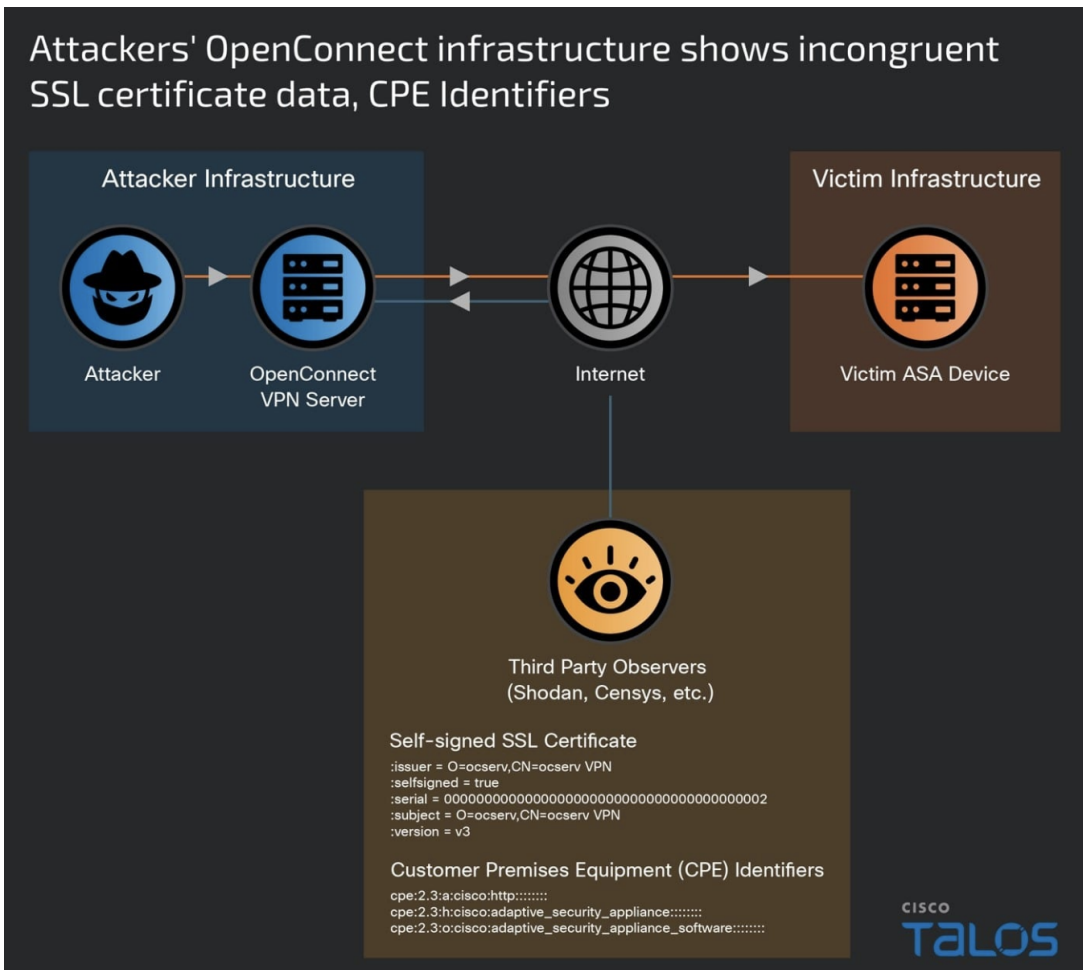
Talos’ investigation found that actor infrastructure was established between November and December 2023, with initial activity first detected in **early January 2024**. While the initial access vector used in this campaign remains unknown, Talos uncovered three zero-day vulnerabilities affecting Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) software that were exploited as part of the attack chain: [CVE-2024-20353](#), [CVE-2024-20359](#), and [CVE-2024-20358](#).

## Analyzing UAT4356’s Threat Actor Infrastructure

In their excellent [investigation](#) into ArcaneDoor in collaboration with other organizations, Talos shared some interesting indicators within the attacker infrastructure leveraged by UAT4356 in this campaign.

### Examining Associated Certificate Indicators:

# Attackers' OpenConnect infrastructure shows incongruent SSL certificate data, CPE Identifiers



## UAT4356 Certificate and Software Indicators ([Source](#))

Talos identified a specific pattern in both the issuer and subject names of the SSL certificates:

Certificate Pattern:

```
:issuer = O=ocserv,CN=ocserv VPN
```

```
:selfsigned = true
```

```
:serial = 0000000000000000000000000000000000000000000000000000000000000002
```

```
:subject = O=ocserv,CN=ocserv VPN
```

```
:version = v3
```

“Ocserv” is associated with [OpenConnect VPN Server](#), an open-source VPN client commonly used to connect to VPNs like Cisco ASA. It’s plausible that OpenConnect was used by the threat actor to initially connect to the targeted network devices and carry out this exploit chain.

As of April 29, 2024, only 5 hosts were online presenting this certificate in Censys:

services: (tls.certificate.parsed.issuer\_dn: “O=ocserv,CN=ocserv VPN” and tls.certificate.parsed.subject\_dn: “O=ocserv,CN=ocserv VPN”)

Host Filters

Labels:

- 4 network.device
- 4 network.device.firewall
- 1 open-dir
- 1 remote-access

Autonomous System:

- 2 TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited
- 1 AS-CHOOPA
- 1 CHINANET-BACKBONE No.31,Jin-rong Street
- 1 TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue

Location:

- 3 China
- 1 Canada
- 1 Hong Kong

Service Filters

Service Names:

- 9 HTTP
- 1 SSH
- 1 UNKNOWN

Ports:

- 2 443
- 2 4433
- 2 8443

Hosts

Results: 5 Time: 0.28s

1.14.13.178

Cisco Adaptive Security Appliance TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited (45090) Sichuan, China

network.device.firewall network.device

1 Matched Service

443/HTTP

182.254.195.125

Cisco Adaptive Security Appliance TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited (45090) Guangdong, China

network.device.firewall network.device open-dir

2 Matched Services

4433/HTTP 8443/HTTP

2 Other Services

81/HTTP 8088/HTTP

124.156.100.221

Cisco Adaptive Security Appliance TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue (132203) Sham Shui Po, Hong Kong

network.device.firewall network.device

1 Matched Service

8443/HTTP

113.108.136.75

Cisco Adaptive Security Appliance CHINANET-BACKBONE No.31,Jin-rong Street (4134) Guangdong, China

network.device network.device.firewall

2 Matched Services

4433/HTTP 6688/HTTP

1 Other Service



Hosts presenting certificates associated with "ocserv" in Censys on April 29, 2024

The fact that there are so few hosts presenting this certificate could imply various things, but nonetheless, it's significant. When a Censys pivot yields only a handful of results, each host holds greater significance — it means you've stumbled upon something distinctive in an investigation.

From this screenshot, you'll notice that some of these hosts also appeared to be running ASA software or operating systems themselves, which aligns with observations from Talos. These are the unique CPE identifiers associated with ASA among these hosts:

```
cpe:2.3:h:cisco:adaptive_security_appliance:*:*:*:*:*:*:*
```

```
cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*
```

We determined that these hosts were running ASA based on various indicators, including the presence of a Set-Cookie HTTP response header containing the string `webvpncontext`, a characteristic associated with ASA.

**This raises the question:** why do these hosts seem to be running Cisco ASA, one of the software products they were attempting to exploit? Is it somehow involved in the methods used to carry out the exploit, or is this an attempt to obfuscate their infrastructure?

Another notable clue here is the distribution of these hosts across different autonomous systems.

Networks Hosting IPs Displaying "ocserv" Certificate Indicators

Autonomous System	Host Count
TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited (45090)	2
AS-CHOOPA (20473)	1

CHINANET-BACKBONE No.31,Jin-rong Street (4134)	1
TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue (132203)	1

**Four out of the five hosts are based in China.** “TENCENT-NET-AP” is associated with Tencent, a Chinese multinational conglomerate headquartered in Shenzhen, while “CHINANET-BACKBONE” is run by ChinaNet, a major Chinese telecommunications company. Networks like Tencent and ChinaNet have extensive reach and resources, so they would make sense as an infrastructure choice for a sophisticated global operation like this one.

## Investigating Actor-Controlled IPs:

Let’s now take a look at the list of 22 potentially actor-controlled IPs provided by Talos and [plug them into Censys](#). Analyzing attacker infrastructure proves more advantageous compared to shared infrastructure, since it’s easier to isolate distinctive characteristics specific to the threat actor’s behavior.

As of Monday, April 29, 2024, 11 of the 22 hosts originally provided by Talos remained online in Censys scans, indicating ongoing activity within the identified infrastructure.

The screenshot shows the Censys search interface. At the top, there's a search bar with the IP list: ip:{192.36.57.181, 185.167.60.85, 185.227.111.17, 176.31.18.153, 172.105.90.15}. The search results are displayed in a list format. On the left, there are filters for Hosts, Labels, Autonomous System, Location, and Service Filters. The main content area shows details for several hosts, including their IP addresses, operating systems, and associated services.

**Host Filters**

Labels:

- 11 remote-access
- 1 database
- 1 email
- 1 file-sharing
- 1 network-administration

Autonomous System:

- 3 GHOST
- 2 AS-CHOOPA
- 1 ACCELERATED-IT
- 1 AKAMAI-LINODE-AP
- 1 ASNET
- 1 LIMESTONENETWORKS
- 1 STARK-INDUSTRIES
- 1 TSRDC-AS-AP Truxgo S. R.L. de C.V.

Location:

- 5 Germany
- 4 France
- 2 Mexico

**Service Filters**

Service Names:

- 14 HTTP
- 10 SSH
- 3 SMTP
- 2 DNS
- 2 IMAP

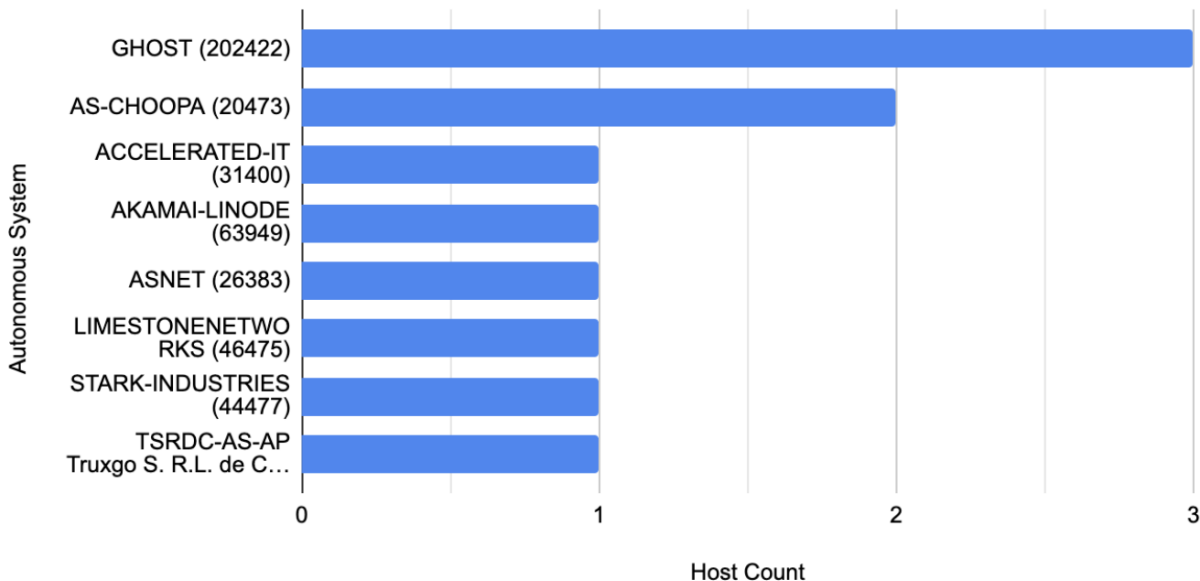
**Hosts**

Results: 11 Time: 0.21s

- 216.238.75.155 (216.238.75.155.vultrusercontent.com)**  
 Ubuntu Linux AS-CHOOPA (20473) Querétaro, Mexico  
 file-sharing database network.device.web-ui web.control-panel.hosting email remote-access  
 21/FTP 22/SSH 25/SMTP 53/DNS 80/HTTP  
 110/POP3 143/IMAP 443/HTTP 465/SMTP 587/SMTP  
 993/IMAP 995/POP3 3306/MYSQL 4190/PIGEONHOLE 8443/HTTP  
 8880/HTTP
- 194.4.49.6 (vm2425572.stark-industries.solutions)**  
 Ubuntu Linux STARK-INDUSTRIES (44477) Île-de-France, France  
 remote-access  
 22/SSH
- 45.86.163.224**  
 Ubuntu Linux ACCELERATED-IT (31400) Hesse, Germany  
 remote-access  
 22/SSH 80/HTTP 8080/HTTP
- 45.77.52.253 (45.77.52.253.vultrusercontent.com)**  
 Ubuntu Linux 20.04 AS-CHOOPA (20473) Hesse, Germany  
 remote-access  
 22/SSH 27015/VALVE
- 89.44.198.196 (cdg03.q753930.uk)**  
 Linux GHOST (202422) Hesse, Germany  
 remote-access  
 22/SSH 2053/HTTP
- 172.105.94.93 (172-105-94-93.ip.linodeusercontent.com)**  
 AKAMAI-LINODE-AP Akamai Connected Cloud (63949) Hesse, Germany


Let’s first look at what networks these hosts are concentrated in:

# Networks Hosting Attacker-controlled Infrastructure



- **GHOST**: A Luxembourg-based cloud services provider associated with G-Core Labs S.A.
- **AS-CHOOPA**: A network known for high-performance network services, also known as Vultr
- **ACCELERATED-IT**: Provider of accelerated or high-speed internet.
- **AKAMAI-LINODE**: Akamai’s cloud computing infrastructure.
- **ASNET**: A generic-named entity, seemingly owned by “Baxet Group Inc.”
- **LIMESTONENETWORKS**: A hosting provider based in Dallas, Texas.
- **STARK-INDUSTRIES**: A Russian autonomous system believed to operate as a [bulletproof hosting provider](#)
- **TSRDC-AS-AP Truxgo S. R.L. de C.V**: A telecom giant based in Mexico.

When we generate a [report on the issuer common names](#) on the certificates of these hosts, there are some interesting results:



Search

[Register](#)  
[Log In](#)

---

Results

[Report](#) | [Docs](#) | [Subscriptions](#)

## Report on Hosts

This tool allows you to generate a report on the breakdown of a value present on the Hosts returned by your query. For example, to generate a report on ports seen on Hosts with HTTP services, you could query for `services.service_name: HTTP` and then generate a report on the breakdown of the field `services.port`

Breakdown Field

`services.tls.certificates.leaf_data.issuer.common_name`

Number of Buckets

50

BUILD REPORT

### Report for Hosts

services.tls.certificates.leaf_data.issuer.common_name	services	
<a href="#">Plesk</a>	7	17.07%
<a href="#">R3</a>	3	7.32%
<a href="#">Gozargah</a>	2	4.88%
<a href="#">Kubernetes Ingress Controller Fake Certificate</a>	1	2.44%
<a href="#">WIN-16HD0VMNND5</a>	1	2.44%
<a href="#">ZeroSSL ECC Domain Secure Site CA</a>	1	2.44%
<a href="#">Ike155316-227342-104695750000-ca@1707338035</a>	1	2.44%
<b>Total</b>	<b>41</b>	<b>100.0%</b>

While many of these certificates appear familiar, there are a few that initially look less recognizable.

First up: **WIN-16HD0VMNND5**. After some digging, this looks like it may be an auto-generated RDP cert – corroborated by the fact that when we pivot to look for hosts with similar certificates in Censys ([services.tls.certificates.leaf\\_data.subject\\_dn:"CN=WIN-\\*](#)), they are predominantly on RDP services.

**Ike155316-227342-104695750000-ca@1707338035**: This looks machine-generated, and matches a pattern observed in Akamai LINODE host certificates ([services.tls.certificates.leaf\\_data.subject\\_dn:"CN=Ike\\*](#)).

Among these, one certificate common name stands out as particularly unusual: **Gozargah**. Initially, this term wasn't familiar to us.

What's more, the two services presenting it are both on this host: [212.193.2\[.\]48](#) based in a network called ASNET, and both show up as "UNKNOWN" services in our data on TCP ports 3630 and 3631, meaning they did not fit any protocol specification we're aware of.

## UNKNOWN 3630/TCP

04/29/2024 13:19 UTC

### Details

[VIEW ALL DATA](#)

### TLS

#### Handshake

**Version Selected** TLSv1\_3  
**Cipher Selected** TLS\_AES\_256\_GCM\_SHA384

#### Certificate

**Fingerprint** [354bb0dee3ee9fac15cea5a2e62f3b13d2c9e018f974d34f4212f77c1c7cdb67](#)  
**Subject** CN=Gozargah  
**Issuer** CN=Gozargah

#### Fingerprint

**JARM** [2ad2ad0002ad2ad00042d42d00000ad9bf51cc3f5a1e29eecb81d0c7b06eb](#)  
**JA3S** [15af977ce25de452b96affa2addb1036](#)  
**JA4S** [t120200\\_544c535f4145535f3235365f47434d5f534841333834\\_9f090db0cf15](#)

## UNKNOWN 3631/TCP

04/28/2024 23:46 UTC

### Details

[VIEW ALL DATA](#)

### TLS

#### Handshake

**Version Selected** TLSv1\_3  
**Cipher Selected** TLS\_CHACHA20\_POLY1305\_SHA256

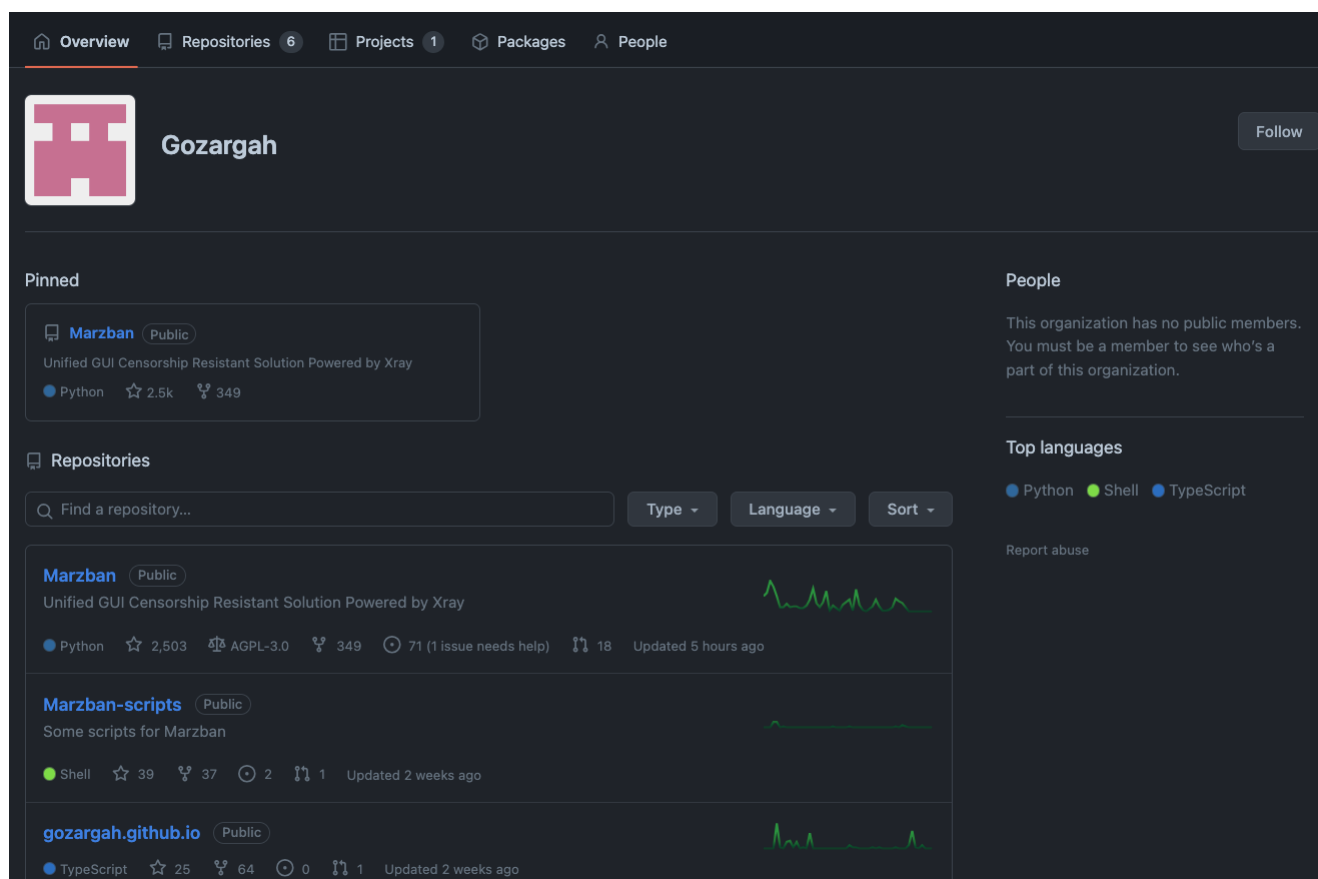
#### Certificate

**Fingerprint** [354bb0dee3ee9fac15cea5a2e62f3b13d2c9e018f974d34f4212f77c1c7cdb67](#)  
**Subject** CN=Gozargah  
**Issuer** CN=Gozargah

#### Fingerprint

**JARM** [3fd3fd20d0000000043d3fd3fd43d74078efd0be48797e5998f0bb92eb873](#)  
**JA3S** [475c9302dc42b2751db9edcac3b74891](#)  
**JA4S** [t120200\\_544c535f43484143484132305f504f4c59313330355f534841323536\\_9f090db0cf15](#)

Searching “Gozargah” in a web search engine takes us to this GitHub organization: <https://github.com/Gozargah>.



Their pinned repo is called “**Marzban**” (<https://github.com/Gozargah/Marzban>), described as “Unified GUI Censorship Resistant Solution Powered by Xray”.

What’s “**Xray**”?

It’s this open source project: <https://github.com/XTLS/Xray-core> that seems to have been developed by a community called “Project X” that’s been around since 2020: <https://xtls.github.io/>. Its description reads: “Xray, Penetrates Everything. Also the best v2ray-core, with XTLS support. Fully compatible configuration.”

Most of Project X’s GitHub page is written in Chinese.



## Project X

不畏浮云遮望眼·金睛如炬耀苍穹

[由此开始 →](#)

[配置指南 →](#)

### 极速协议

原创 VLESS 与 XTLS 协议，摆脱冗余加密，释放 CPU 算力

### 自由组合

完善的回落机制，有效防止主动探测，多服务共享端口

### 超低占用

OpenWRT RaspberryPi 等各种精简设备皆可使用

### 强大路由

高定制化的路由系统，满足各类使用需求，充分发挥网络性能

### 完整兼容

完整兼容 v2ray-core 配置文件与 API 调用

### 亲和力

活跃的社区讨论及贡献，MPL 2.0 开源许可协议

**XTLS**, or Extended Transport Layer Security, is an extension of TLS 1.3 that uses some more advanced cryptographic techniques, obfuscates its protocol signature (making it harder to identify) and allows concealed VPN endpoint access. It makes sense that it's being used in anti-censorship tools, since it's most often used for bypassing firewalls. Given that it was developed by Chinese developers, it's ostensible that it was created for the purpose of bypassing The Great Firewall, or the national firewall operated by the Chinese government.

When we pivot to look at other hosts with this certificate common name "Gozargah", there are around 4,800 Censys-visible IPs presenting that cert ([services.tls.certificates.leaf\\_data.issuer.common\\_name="Gozargah"](https://search.censys.io/hosts/54.179.113.92)). Interestingly, ports 3630 and 3631 do not make the top 20 common ports list – it seems like TCP 62050 and 62051 are more popular for this service. There are only 2 other hosts with that certificate common name that have the same ports 3630 and 3631 open.

This is interesting, but is even more interesting when we go back and look at one of the hosts presenting a certificate with an "ocserv" issuer\_dn flagged as an indicator by Talos: <https://search.censys.io/hosts/54.179.113.92>.

On TCP port 8888, this host is running some HTTP service with an HTML title reading: "Trojan Panel"





Q Hosts v



54.179.113.92



Search

Register  
Log In

## HTTP 8888/TCP

05/01/2024 13:15 UTC

### Software

nginx 1.20.2

VIEW ALL DATA

GO

### Details

https://54.179.113.92:8888/

Status 200 OK

Body Hash sha1:7d281060b11ef2ce99e4507a10f0e737968173a3

HTML Title Trojan Panel

Response Body

EXPAND

**\*\*We're sorry but Trojan Panel doesn't work properly without JavaScript enabled. Please enable it to continue.\*\***

### TLS

#### Handshake

Version Selected TLSv1\_3

Cipher Selected TLS\_AES\_256\_GCM\_SHA384

#### Certificate

Fingerprint b8415dc3f25e81fa6a2e2381ad077f5233b8539de78cd7de4cd68fcea4c1bc5b

Subject CN=video.gtlx.org

Issuer C=US, O=Let's Encrypt, CN=R3

Names video.gtlx.org

This appears to be related to this [GitHub project called "trojanpanel"](#), which also has a website mostly written in Chinese:



## Trojan Panel

支持Xray/Trojan-Go/Hysteria/NaiveProxy的多用户  
Web管理面板

快速上手 →

### 极速搭建

一键安装脚本，降低部署门槛，快速搭建系统

### 分布式

前后端分离开发，减少模块之间耦合度，可以自由组合部署在多个服务器

### 国际化

系统语言支持中文/English/한국인/فارسی

### 功能强大

支持登录注册/用户管理/节点管理/邮件管理/黑名单管理/自定义伪装网站/系统看板等

### 多代理支持

节点类型支持Xray/Trojan-Go/Hysteria/NaiveProxy

### 所见即所得

支持多节点管理，自动化管理远程节点，自动化申请/续签证书，面板内编辑节点，远程服务实时修改节点配置

### 🚀 安装

- 联机 (推荐)

It describes itself as a “multi-user web management panel supporting Xray/Trojan-Go/Hysteria/NaiveProxy.”

That makes for two mentions of this “Xray” tool linked with services running on this infrastructure.

**Let’s summarize the evidence we’ve gathered so far:** by cross-referencing the actor-controlled IPs and other certificate indicators identified by Talos with Censys data, we’ve discovered that (a) some of these hosts were running services associated with anti-censorship software likely intended to circumvent The Great Firewall, and (b) a significant number of these hosts are based in prominent Chinese networks.

## What Does This All Mean?

Our strongest clues as to who is potentially behind this campaign come from analyzing the actor-controlled IPs in Censys, as well as pivoting off of other hosts that present the certificate indicators flagged by Talos.

The results of this preliminary investigation show a few indications that this may be the work of an actor based in China. We may see continued activity and/or changes in these hosts in our data over the coming days.

Determining whether cyber attacks are state-sponsored demands a comprehensive approach. While analyzing the networks hosting threat actor infrastructure is a piece of the puzzle, there are other factors to consider like attack methods, victims, and geopolitical context. The murky nature of this threat actor’s identity, combined with the fact that the initial access vector leveraged in this campaign is still unknown, are a cause for continued monitoring of the situation.

It’s likely that this investigation will continue to unfold as we get more details about the targets of these attacks. In the meantime, please refer to our [Rapid Response advisory](#) for more details on the scope of exposed Cisco ASA devices and remediation guidance.

## References:

- <https://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/>
- [https://sec.cloudapps.cisco.com/security/center/resources/asa\\_ftd\\_attacks\\_event\\_response](https://sec.cloudapps.cisco.com/security/center/resources/asa_ftd_attacks_event_response)
- <https://securityboulevard.com/2024/04/agent-tesla-unmasked-revealing-interrelated-cyber-campaigns/>
- <https://censys.com/cve-2024-20353/>