Research Report On

Phishing Site Replicating
Territorial Army, Govt. Of India Website
This report is purely based on technical findings made by the research team during an investigation. It does not intend to malign or in any way target any country, actor or person. All the information provided in this report has been extracted during the investigation and information might be changed after generating the reports.
The Research Wing of CyberPeace Foundation received a link via Whatsapp pretending itself as the legitimate site of the Territorial Army, Govt. of India and asking users to login to the site.

**Link:**

http://jointerritorialarmygov[.]com

**Case Study:**

The Research Wing of CyberPeace Foundation along with Autobot Infosec Private Limited have looked into this matter to reach a conclusion that the website is either legitimate or an online fraud.

On the landing page an error related message “**404 Page Not Found...............**” appears which (error code 404) usually means the page is either removed or not available on the server.
IN DEPTH INVESTIGATION:

Some of the key findings are as follows:

<table>
<thead>
<tr>
<th>Domain</th>
<th>jointerritorialarmygov[.]com</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Status Code</td>
<td>200 OK [Active]</td>
</tr>
<tr>
<td>IP Address</td>
<td>184.168.99.241</td>
</tr>
<tr>
<td>ISP</td>
<td>GoDaddy.com, LLC</td>
</tr>
<tr>
<td>ASN</td>
<td>26496</td>
</tr>
<tr>
<td>Country</td>
<td>United States</td>
</tr>
<tr>
<td>Continent</td>
<td>North America</td>
</tr>
</tbody>
</table>

*Note: Geo Location data might differ after generating the report due to Load balancing technologies.*

**Domain Name:** jointerritorialarmygov[.]com

**Registry Domain ID:** 2676566878_DOMAIN_COM-VRSN

**Registrar WHOIS Server:** whois.godaddy.com

**Registrar URL:** https://www.godaddy.com

**Registrar:** GoDaddy.com, LLC

**Registrar IANA ID:** 146

**Updated Date:** 2022-02-21T00:58:45Z

**Creation Date:** 2022-02-21T00:58:44Z **

**Registry Expiry Date:** 2023-02-21T00:58:44Z

**Registrant Organization:** Domains By Proxy, LLC **

**Registrant State/Province:** Arizona

**Registrant Country:** US
Name Server: NS09.DOMAINCONTROL.COM
NS10.DOMAINCONTROL.COM

** Domain name was registered very recently.
** Domain name owner is in any way not linked with the Indian army or Govt. of India.

![HTTP RESPONSE HEADER]

→ http://jointerritorialarmy.gov[.]com

<table>
<thead>
<tr>
<th>HTTP/1.1 200 OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
</tr>
<tr>
<td>Server:</td>
</tr>
<tr>
<td>Upgrade:</td>
</tr>
<tr>
<td>Connection:</td>
</tr>
<tr>
<td>Last-Modified:</td>
</tr>
<tr>
<td>ETag:</td>
</tr>
<tr>
<td>Accept-Ranges:</td>
</tr>
<tr>
<td>Content-Length:</td>
</tr>
<tr>
<td>Vary:</td>
</tr>
<tr>
<td>Content-Type:</td>
</tr>
</tbody>
</table>

In source code analysis we found, the error message “404 Page Not Found.............” was created manually using html tag <h1> by the owner of the website. In the HTTP Response Header, the http response code shows 200/OK which means the site is reachable from the internet whereas upon opening the site it shows 404 response code. That means the error response does not originate from the server side and Cyber criminals tried to trick users by saying the site is down.

```html
<html>
<head>
<title>Errorr........</title>
</head>
<body>
<h1>404 Page Not Found.............</h1>
</body>
</html>
```

Using the fuzzing technique we found two pages /login.html and /contactus.html on the site. After comparing the pages with the actual Territorial Army website i.e https://www.jointerritorialarmy.gov.in/, we found that both of the pages are simply cloned from the real one.

Image: Contact us page of original Territorial Army website.

In background analysis it was found, the /login.html page harvests the entered credentials by the user and redirects to the original Territorial Army page. In our case we used dummy credentials.
Request:

POST /home/eligibility_signup HTTP/1.1
Host: www.jointerritorialarmy.gov.in
Content-Length: 190
Cache-Control: max-age=0
Sec-Ch-Ua: "*(Not.A.Brand");v="9", "Chromium";v="88"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://jointerritorialarmy.gov.in
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.82
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://jointerritorialarmy.gov.in/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
ci_csrf_token=test40@gmail.com&password=7b8f39f9f5e77cb1d562c519266b177d4f5f7ce139d6da12ebea604c8740852dd2f92
de4c4c8a5f57a785a33426b6086e627f29e0e24973419b6772zc0be8&login=
login

Response:

HTTP/1.1 303 See Other
Date: Fri, 11 Mar 2022 08:49:21 GMT
Server: Apache
Upgrade: h2
Connection: Upgrade, close
X-FRAME-OPTIONS: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'; script-src 'self';
Set-Cookie: ci_session=0317qj6v9gacmzjifcuddq3x3d7m; expires=Fri, 11-Mar-2022 05:05:21 GMT; Max-Age=1200; path=/; SameSite=strict; secure; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Location: https://www.jointerritorialarmy.gov.in/home/login
Content-Length: 0
Content-Type: text/html; charset=UTF-8

The “HTTP/1.1 303 See Other” means the site has to redirect to a different location.
CONCLUSIVE SUMMARY:

The official website of Territorial Army is https://www.jointerritorialarmy.gov.in/ which has the domain name ending with .gov.in that clearly indicates as Government of India property, whereas the shared link has the domain name ending with .com which makes it more suspicious.

Usually any of the Government of India websites are hosted by the National Informatics Centre (NIC) or in any way linked with NIC, whereas in this case it is hosted by a third party entity.

The domain used in this case study has been registered very recently on 21st February 2022.

The whole campaign uses plain http protocol instead of the secure https. This means anyone on the network or internet can intercept the traffic and get the confidential information in plain text to misuse against the victim.

Overall layout and the functionalities of the web page used in the campaign are kept similar to the official Territorial Army site to lure laymen.

The site has been created using site cloning techniques with the intention of duping the Indian Army personnel by harvesting their official credentials.
CYBERPEACE ADVISORY:

CyberPeace Foundation and Autobot Infosec recommend that people should avoid opening such messages sent via social platforms.

Before you click, look at the URLs very carefully and verify it with the real one.

If at all, user gets into this trap, it could lead to whole system compromise such as access to microphone, Camera, Text Messages, Contacts, Pictures, Videos, Banking Applications etc as well as financial losses.

Do not share confidential details like login credentials, banking information with such a type of phishing scam.

Do not share or forward fake messages containing links without proper verification.

ISSUED BY:

Research Wing, CyberPeace Foundation.
Research Wing, Autobot Infosec Private Limited.