

# American Rescue Plan Act Lures in the Wild

---

 [domaintools.com/resources/blog/american-rescue-plan-act-lures-in-the-wild](https://domaintools.com/resources/blog/american-rescue-plan-act-lures-in-the-wild)



## Executive Summary

---

DomainTools researchers discovered a cluster of credential harvesting sites masquerading as American Rescue Plan Act signup sites for those looking to receive their federal aid. Through historical WHOIS information and OSINT techniques DomainTools attributed this campaign to a Nigerian web development firm GoldenWaves Innovations. In this article, DomainTools researchers will walk through the techniques and methods used to enumerate these websites and associated attribution with medium-high confidence.

## Background

---

On March 11, 2021, President Joe Biden signed the [American Rescue Plan Act](#) into law. The COVID-19 pandemic relief bill was designed to provide \$1,400 in immediate relief to working families, emergency paid leave for over 100 million Americans, and expand the child tax credit among a number of other grants and pillars to assist with other budget shortfalls. Since this act was signed into law, DomainTools researchers have monitored for new registrations of domains that targeted relief recipients. Unfortunately, many relief recipients are unaware that this relief will be automatically assigned to them by the IRS, so scammers are using this as an opportunity to collect social security numbers and driver's license photographs to use in identity theft.



https://reliefcarefunds.com/applynow.html

Frequently Asked Questions Contact Us **APPLY NOW**

### UNEMPLOYMENT INSURANCE APPLICATION FORM

Before filing, make sure you have the following information available:

- Social Security number
- Driver's license or State ID number

You do not need to do anything to receive your payment. It will arrive by mail in the form of a paper check or debit card or direct deposit to your bank account.

**First Name\*** **Middle\*** **Last Name\***

Eg. Jane Eg. Ann Eg. Doe

**Cell for SMS\*** **Employment\***

Eg. (555) 555-5555 Please Select

**SSN#\*** **Mother's Maiden Name\***

Eg. 555005555 Eg. Amanda

**Street Address\*** **Apt/Unit**

**City\*** **State\*** **ZIP code\***

Please select

**Gender\*** **Date of Birth\***

**Have You received Any Covid19 Relief Bonus in past?\***  Yes  No

**Are you Hispanic or Latino heritage?\***  Yes  No

**Race - Please select all that apply:\***

- African American/Black
- American Indian/Alaskan Native
- Asian
- Hawaiian/Other Pacific Islander
- White
- I do not wish to answer

**If offered a job, are you able and available to accept it?\***  Yes  No

**Are you self-employed, or the owner, or the operator of a business or farm?\***

Yes  No

**Are you in an elected, appointed or in a major policy making position?\***

Yes  No

**Upload front of your State ID/License\*** Browse... No files selected

**Upload back of your State ID/License\*** Browse... No files selected

The initial domain found by DomainTools researchers was reliefcarefunds[.]com that contained the above application form with a typical upload to a PHP destination on the same domain. However, buried in the code was a comment that the page had been mirrored from americaforgivenrelieffund[.]com and a contact page that submitted to a PHP script on that domain as well. With evidence of more domains, DomainTools researchers took a look at the architecture behind the pages for similarities. As readers of this blog will know, DomainTools is a strong proponent of the composite objects method for building out indicators and through examining these two pages we could see that what they had in common was:

- Registration through NameCheap
- Containing the “relief” substring
- Containing the “eric” as in America substring or the “care” substring
- Registration after the signing of the bill into law on March 11, 2021
- Hosting on NameCheap hosting infrastructure

The screenshot displays the DomainTools Iris Investigate interface. On the left is an 'Advanced Search' sidebar with filters for Domain (relief), IP ASN (22612), Create Date (2021-05-18), and another Domain (eric) OR (care). The main area shows search results for domains with associated risk scores and email addresses. The top navigation bar includes 'pDNS', 'Pivot Engine', 'IP Profile', 'Stats', 'Visualization', 'Domain Profile', 'Hosting History', and 'SSL Profile'. A 'Download' button and 'Page 1 of 1 (39 records)' are visible in the top right. The first result is for 'americanreliefplan.us' with a risk score of 86 and an email address 'goldenwaves247@gmail.com' circled in red. Other results include 'americanreliefplans.site' (93), 'americanreliefrescueplan.com' (98), and 'americans-relief-plan.us' (97).

Domain	Risk Score	Email
americanreliefplan.us	86	goldenwaves247@gmail.com cpanel.tech@namecheap.com goldenwaves247@gmail.com goldenwaves247@gmail.com abuse@namecheap.com
americanreliefplans.site	93	Address cpanel.tech@namecheap.com abuse@namecheap.com
americanreliefrescueplan.com	98	Address f79c709c3ad74daba14a8d17cc9b62a3.protect@withheldfo cpanel.tech@namecheap.com f79c709c3ad74daba14a8d17cc9b62a3.protect@withheldfo f79c709c3ad74daba14a8d17cc9b62a3.protect@withheldfo abuse@namecheap.com
americans-relief-plan.us	97	Address goldenwaves247@gmail.com cpanel.tech@namecheap.com goldenwaves247@gmail.com goldenwaves247@gmail.com abuse@namecheap.com

Hunting for this composite in [DomainTools Iris Investigate](#), DomainTools researchers revealed 39 potential domains and an email address associated with a number of them of [goldenwaves247@gmail.com](mailto:goldenwaves247@gmail.com). To confirm similarities, we used [URLScan](#) to search for the list of domains uncovered for any scans done by others that had encountered these domains over the last month. Unsurprisingly, this revealed an additional set of domains with identical structure to the initial phishing page dating back almost exactly a month.

## 29 structurally similar hits on different domains, IPs and ASNs

Detects websites which have a similar structure but are hosted on different infrastructure, such as Phishing kits  
Please note that this is an *experimental* feature. It might work great for you or the results might not make sense.

🔒	URL	Age	Size	🌐	IPs	📄	🏠
🔒	americanreliefplan.com	4 hours	2 MB	46	3	2	🇺🇸
🔒	americanrelieffunds.com	4 hours	2 MB	48	3	2	🇺🇸
🔒	americanforgivenrelieffund.com	4 hours	2 MB	48	3	2	🇺🇸
🔒	americanreliefplan.us	12 hours	2 MB	48	4	2	🇨🇦
🔒	americarelieffund.com	13 hours	2 MB	48	4	2	🇺🇸
🔒	americanreliefrescueplan.com	13 hours	908 KB	57	6	2	🇺🇸
🔒	americareliefcarefunds.com	13 hours	2 MB	48	4	2	🇺🇸
🔒	americanreliefrescueplan.com	3 days	908 KB	57	5	2	🇺🇸
🔒	portal.rescueforgivenrelief.com/applynow.php	3 days	2 MB	44	5	3	🇷🇺
🔒	americansreliefplan.xyz	4 days	2 MB	52	6	2	🇺🇸
🔒	americafundforstimulus.com	4 days	2 MB	48	3	2	🇺🇸
🔒	americarelieffunds.mrvui.com	4 days	2 MB	48	4	2	🇺🇸
🔒	americansreliefplan.site	5 days	2 MB	48	3	2	🇺🇸
🔒	americarelieffunds.mrvui.com/home/apply	5 days	958 KB	38	4	2	🇺🇸
🔒	www.americaforgivenrelief.com	6 days	2 MB	48	4	2	🇺🇸
🔒	americanrelief-plan.com	6 days	2 MB	48	3	2	🇺🇸
🔒	americarelieffunds.mrvui.com/home/apply	6 days	958 KB	38	5	2	🇺🇸
🔒	americarelieffunds.mrvui.com/home/apply	6 days	958 KB	38	4	2	🇺🇸
🔒	americanreliefplan.site	7 days	2 MB	48	4	2	🇺🇸
🔒	americafundforstimulus.com	8 days	2 MB	48	3	2	🇺🇸
🔒	americansreliefplans.site	9 days	2 MB	48	4	2	🇺🇸
🔒	portal.theamericaforgivenrelief.com	13 days	4 MB	50	3	2	🇺🇸
🔒	portal.theamericaforgivenrelief.com/index.html	20 days	3 MB	48	3	2	🇺🇸
🔒	portal.theamericaforgivenrelief.com	22 days	3 MB	48	4	2	🇺🇸
🔒	portal.theamericaforgivenrelief.com	22 days	3 MB	48	3	2	🇺🇸
🔒	www.americanreliefplan.com/index.html	23 days	2 MB	48	4	2	🇺🇸
🔒	www.americanreliefplan.com	25 days	2 MB	48	3	2	🇺🇸
🔒	theamericaforgivenrelief.com	a month	3 MB	48	3	2	🇺🇸
🔒	portal.theamericaforgivenrelief.com	a month	3 MB	48	3	2	🇺🇸

This list of domains then provided another set of important information. For one, DomainTools researchers were able to see that some of these links were being pushed by Bitly link shortening links. With Bitly, appending a “+” to any shortened link provides some data about that link. In this instance, we could see that the shortener was created at 1630 UTC time on June 5th, 2021 with a specific title of “Unemployment Insurance Relief During COVID-19 Outbreak | American Rescue Plan Act” which matches the titles of the other cloned pages.



CREATED JUN 5, 4:30 PM


Unemployment Insurance Relief During COVID-19 Outbreak | American Rescue Plan Act

<https://americaforgivenreliefund.com/>bitly.com/3grK9HZ [COPY](#)

We can also tell that many of the cloned pages, at the time of their scanning, were not hosted solely on NameCheap's site hosting services, but were also active on both Garanntor (AS328110) and OVH (AS16276). This allowed the set of items we search for to:

- Registration through NameCheap
- Containing the "relief" substring
- Containing the "eric" as in America substring or the "care" substring
- Registration after the signing of the bill into law on March 11, 2021
- Hosting on NameCheap (AS22612), Garanntor (AS328110), or OVH (AS16276) hosting infrastructure

This then revealed a total of 47 domains matching our criteria including the oldest domain on URLScan page similarities and the oldest domain in our search criteria theamericaforgivenrelief[.]com with a registrant email address of onostboy1@gmail[.]com and an unredacted WHOIS record placing the registrant in Ibadan, Nigeria. Searching on that username then reveals a profile on social media site Eskimi of a web developer with an associated Twitter handle of @onostboy with the name Tosyno based in Ibadan, Nigeria. The city of Ibadan is a small, rural town which makes the registration information stand out as almost always technical contacts for Nigerian domains are located in Lagos, the capital city and technology center. Additional searches reveal the same username participating in sales on cybercrime forums, Steam gaming, and other social media sites.



**onostboy**  
[newb@HF:]  
★  
Status: **Offline** [06-06-2021, 09:26 AM]

**Market Info**  
Contracts Completed: 11 [Completed Contracts]  
B-Rating: 11 0 0  
Open Disputes: 0

Recent Contracts

Type	Member	Initiated	Status
Purchase	<b>B FOR BADASS</b>	12-06-2020, 06:08 AM	Completed
Purchase	<b>Matlex</b>	12-02-2020, 02:12 PM	Expired
Purchase	<b>PsiSolutions</b>	11-17-2020, 04:19 AM	Incomplete
Purchase		11-06-2020, 09:29 AM	Completed
Purchase	<b>Chenku</b>	11-06-2020, 05:13 AM	Expired

Pivoting on the previous address of goldenwaves247@gmail[.]com that was surfaced reveals a number of domains including Dasani, Fiji, and Mountain Dew brand sites that looks to be recruiting for various promotional programs in exchange for money, a fake UK bank site at natwestukbank[.]com, and finally a site with the domain goldenwavesng[.]com that contained the email in historical WHOIS records before going private in late 2018. This is the site of GoldenWaves Innovations, a technology company based in Ibadan, Nigeria which DomainTools researchers assume with medium confidence to be the legitimate web design firm in front of the identity document harvesting sites.

**Email (historical)** ✕

**goldenwaves247@gmail.com**

**76** Avg Risk    **469** Avg Age

<input type="checkbox"/>	DOMAIN	RISK SCORE ▾
<input type="checkbox"/>	natwestgroupltd.com	100
<input type="checkbox"/>	americans-relief-plan.us	99
<input type="checkbox"/>	dasaniitablewater.us	98
<input type="checkbox"/>	americansrelief-plan.us	98
<input type="checkbox"/>	dasanitable-water.us	97
<input type="checkbox"/>	americansreliefsplan.us	97
<input type="checkbox"/>	americansreliefs-plan.us	97
<input type="checkbox"/>	americans-reliefplan.us	97
<input type="checkbox"/>	dasanitablewaters.us	96
<input type="checkbox"/>	dasaniclassicwater.us	96
<input type="checkbox"/>	american-reliefplan.us	96
<input type="checkbox"/>	mtndecal-campaign.us	95
<input type="checkbox"/>	dasanipremiumwater.us	95
<input type="checkbox"/>	dasanitablewater.us	93
<input type="checkbox"/>	americanreliefplan.us	93
<input type="checkbox"/>	dasani-tablewater.us	87
<input type="checkbox"/>	fijitablewater.us	86
<input type="checkbox"/>	🌀 revenue-il.us	85
<input type="checkbox"/>	🌀 goldenwaves247.com	76
<input type="checkbox"/>	goldenwavesng.com	67
<input type="checkbox"/>	qliks.link	65
<input type="checkbox"/>	natwestukbank.com	65
<input type="checkbox"/>	🌀 farrahzahra.com	37
<input type="checkbox"/>	🌀 ourgist.com	32
<input type="checkbox"/>	🌀 yomexchange.com	31
<input type="checkbox"/>	🌀 nccmoniya.org	25
<input type="checkbox"/>	🌀 klozprick.com	25
<input type="checkbox"/>	🌀 bacpasblog.com	25

## About Us

GoldenWaves Innovations is a tech firm located in Ibadan, Nigeria. We are a web solution company offering web and internet services to small & large businesses and institutions across the country. We offer services in website design, development, hosting, bulk sms, marketing, maintenance, and analysis.

## Categories

[News/Events](#)[Technology](#)

## Recent Posts

Reading the information on GoldenWaves Innovations' page we can see that they claim to be registered with the Corporate Affairs Commission (CAC) of the government of Nigeria. Searching for that company name on ng-check[.]com, a site for querying CAC information, we can see that GoldenWaves Innovation indeed has a valid registration along with the name of the company's CEO which matches the WHOIS details and who claims to be the company's CEO on LinkedIn. Though the company was registered in February of 2016, their registration is currently inactive.



# GOLDENWAVES INNOVATIONS

GOLDENWAVES INNOVATIONS was incorporated in Ibadan, Nigeria with Registration Number 2394351. It was registered on 18 Feb 2016 and its current status is unknown. Company's registered office address is 59 Ijaye Road, Moniya.

## Basic Info

Name	GOLDENWAVES INNOVATIONS
Status	Unknown
Type of Entity	Business Name
Activity	Computer programming, consultancy and related activities
Registration Number	RC 2394351
Registration Date	18 Feb 2016

## Registered Address

Address	59 Ijaye Road, Moniya
State	OYO
LGA	
City	Ibadan
Phone number	
Website, email	


## Owners / Directors / Key management personal

Name	Designation
[REDACTED]	Proprietor

Creative Freelancer

[REDACTED]

Web Designer • Digital Marketer





[REDACTED]

Digital Marketer & Web Designer  
Nigeria · [Contact info](#)

108 connections

[Message](#) [More](#)

 GoldenWaves Innovations  
 Citygate Institute of Technology

Additionally, the historical WHOIS record unearths an address in New York, New York of 120 E 87th Street. This is an apartment building with condos ranging from \$900,000 to \$13,000,000 in the heart of Manhattan. While at first that seems strange for a company based in Nigeria, we can see from LinkedIn that one of the company's developers claims to live in New York City.

```
Registry Registrant ID:  
Registrant [REDACTED]  
Registrant Organization:  
Registrant Street: 120 E 87th Street  
Registrant City: New York  
Registrant State/Province: NY  
Registrant Postal Code: 10128  
Registrant Country: US  
Registrant Phone: +1.2486915333  
Registrant Phone Ext:  
Registrant Fax: +51.17057182  
Registrant Fax Ext:  
Registrant Email: goldenwaves247@gmail.com
```

The screenshot shows three LinkedIn profiles. The first profile is for a 'LinkedIn Member' who is a 'Web Developer at GoldenWaves Innovations' in 'New York, NY'. The second profile is for a 'Digital Marketer & Web Designer' from 'Nigeria' who is currently the 'CEO at GoldenWaves Innovations'. The third profile is for a 'Frontend Developer Open to Opportunities || Software Engineer || Certified in Python | V...' from 'Nigeria' who was a 'Frontend Web Developer at Goldenwaves Innovations'. Each profile has a 'Message' button.

Looking at the CEO's current contact information on LinkedIn we can see that GoldenWaves Innovations has a new website in goldenwaves[.]com[.]ng which is also tied to the same email address and registration information. This gives DomainTools researchers high confidence that all of these credential harvesting sites are linked to GoldenWaves Innovations in Nigeria. These sites along with any new ones that have cropped up were reported to Google Safe Browsing for blocking.

## Takeaways

Credential harvesting campaigns continue to be a fruitful way for attackers to gain legitimate legal documents they can then resell or use for more sophisticated behavior. When looking for federal aid, those in need the most may not always be fully aware of how that aid is being distributed. In the case of the American Rescue Plan Act that money was coming directly from the IRS, but nonetheless unsuspecting victims could be led into uploading their identification documents to one of these sites.

DomainTools researchers would recommend that security teams utilize internal passive DNS monitoring to alert them of new domains aged less than 90 days that are responding with IP addresses on cloud provider ASNs. That is the most efficient way to discover these domains on your own network. As for end users, DomainTools recommends:

- Reporting the site to Google Safe Browsing if you come across one so that it will be blocked as soon as possible on all major browsers.
- Reporting the malicious site up to your security team along with the phishing email that came with it as there may be a campaign targeting your employees.
- Never upload your documents to a website you are not logged into and particularly not a site claiming to be a federal one without a .gov domain name.

## Iris Hashes for Hunting

---

### GoldenWaves Innovations Domains and Associated Emails

---

U2FsdGVkX1+f4H5GPcY4qa4f5nIuj2vjMY/8shjZ/tasRLRe/sgFkQzNfFJ7EGxjoQYYU9PCo3lgkhHJ/+kas

### Relief-themed Domains Matching Registration and Infrastructure Patterns

---

U2FsdGVkX1+QgEcPUsLxQS18UIt6kBbpnrh0iGN0x4ILTpI03GBI29j+7/Vx6a/Lw82tvNHQEhbWPQEjCk2pC

## IoC Table

---

Domain
americaforgivenrelieffund[.]com
americafundforstimulus[.]com
american-reliefplan[.]site
american-reliefplans[.]site
americancarerelief[.]com
americanforgivenrelieffund[.]com
americanpeoplerelief[.]xyz
americanrelief-plan[.]com
americanrelief-plan[.]site
americanrelief-plans[.]site

---

**Domain**

---

americanreliefcare[.]com

---

americanrelieffunds[.]com

---

americanrelieffunds[.]fund

---

americanreliefplan[.]com

---

americanreliefplan[.]site

---

americanreliefplans[.]com

---

americanreliefplans[.]site

---

americanreliefrescueplan[.]com

---

americans-relief-plan[.]us

---

americans-reliefplan[.]com

---

americans-reliefplan[.]site

---

americans-reliefplan[.]us

---

americans-reliefplan[.]xyz

---

americansrelief-plan[.]us

---

americansreliefplan[.]com

---

americansreliefplan[.]site

---

americansreliefplan[.]us

---

americansreliefplan[.]xyz

---

americansreliefplans[.]site

---

americansreliefplans[.]xyz

---

americansreliefs-plan[.]us

---

americansreliefsplan[.]us

---

americansreliefund[.]com

---

americapandemicrelief[.]com

---

americapandemicrelieffund[.]com

---

---

**Domain**

---

americare-refund[.]com

---

americareliefcarefunds[.]com

---

americarelieffunds[.]com

---

americareliefgrants[.]com

---

americareliefsfund[.]com

---

americareliefstimulus[.]com

---

americareliefstimulusfund[.]com

---

americarescuerelief-id[.]me

---

americarescuerelief[.]com

---

americastimulusfunds[.]com

---

amiericarelieffund[.]com

---

portal-americanrelief[.]com

---

reliefamerican[.]com

---

reliefamericanplan[.]com

---

reliefcarefunds[.]com

---

reliefcaregrant[.]com

---

rescuefundsforamericans[.]com

---

thereliefforamerican[.]com

---