American Rescue Plan Act Lures in the Wild

domaintools.com/resources/blog/american-rescue-plan-act-lures-in-the-wild



Executive Summary

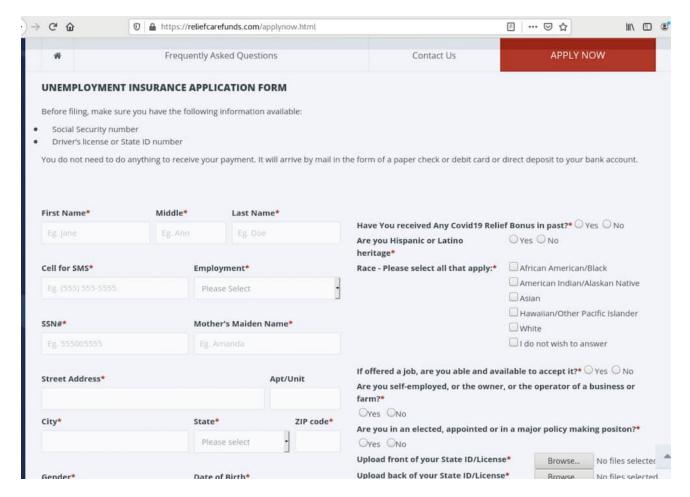
DomainTools researchers discovered a cluster of credential harvesting sites masquerading as American Rescue Plan Act signup sites for those looking to receive their federal aid. Through historical WHOIS information and OSINT techniques DomainTools attributed this campaign to a Nigerian web development 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 <u>American Rescue Plan Act</u> 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.

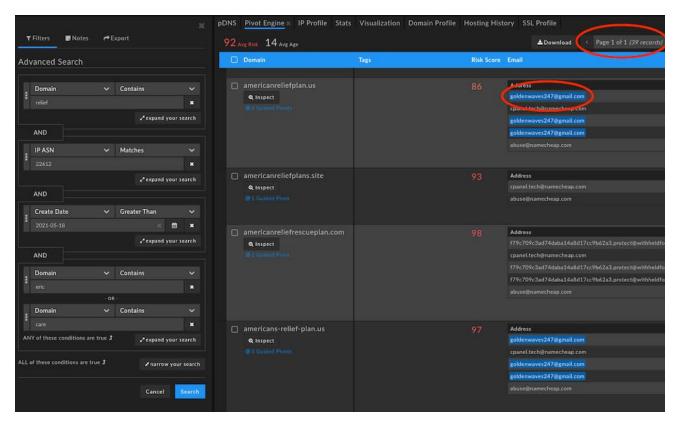


Hunting for More



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" substringRegistration after the signing of the bill into law on March 11, 2021
- · Hosting on NameCheap hosting infrastructure



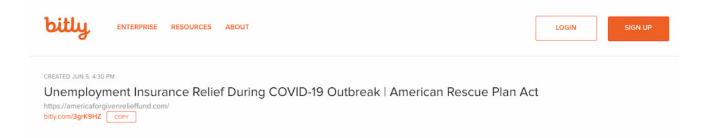
Hunting for this composite in <u>DomainTools Iris Investigate</u>, DomainTools researchers revealed 39 potential domains and an email address associated with a number of them of goldenwaves247@gmail[.]com. To confirm similarities, we used <u>URLScan</u> to search for the list of domains uncovered for 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	~	n
	americanreliefplan.com	4 hours	2 MB	46	3	2	
	american relief funds.com	4 hours	2 MB	48	3	2	
<u>a</u>	americanforgivenrelieffund.com	4 hours	2 MB	48	3	2	
<u>a</u>	americanreliefplan.us	12 hours	2 MB	48	4	2	1-1
۵	americarellefsfund.com	13 hours	2 MB	48	4	2	
	american relief rescueptan.com	13 hours	908 KB	57	6	2	
<u>a</u>	americarellefcarefunds.com	13 hours	2 MB	48	4	2	
<u>a</u>	american relief rescueplan.com	3 days	908 KB	57	5	2	
۵	portal.rescueforgivenrelief.com/applynow.php	3 days	2 MB	44	5	3	_
<u>a</u>	americans relief plan.xyz	4 days	2 MB	52	6	2	
۵	americafundforstimulus.com	4 days	2 MB	48	3	2	
0	americarelleffunds.mrviu.com	4 days	2 MB	48	4	2	=10
<u>a</u>	americansreliefplan.site	5 days	2 MB	48	3	2	
<u>a</u>	americarelieffunds.mrviu.com/home/apply	5 days	958 KB	38	4	2	
a	www.americaforgivenrelief.com	6 days	2 MB	48	4	2	=
	americanrelief-plan.com	6 days	2 MB	48	3	2	
	americarelieffunds.mrviu.com/home/apply	6 days	958 KB	38	5	2	
<u>a</u>	americarelieffunds.mrviu.com/home/apply	6 days	958 KB	38	4	2	
4	american relief plan. site	7 days	2 MB	48	4	2	
	america fund for stimulus.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	-
0	portal.theamericaforgivenrelief.com/index.html	20 days	3 MB	48	3	2	- 11
0	portal.theamericaforgivenrelief.com	22 days	3 MB	48	4	2	11
0	portal,theamericaforgivenrelief.com	22 days	3 MB	48	3	2	- 11
	www.americanreliefplan.com/index.html	23 days	2 MB	48	4	2	
	www.americanrellefplan.com	25 days	2 MB	48	3	2	
	theamericaforgivenrelief.com	a month	3 MB	48	3	2	
4	portal.theamericaforgivenrelief.com	a month	3 MB	48	3	2	111

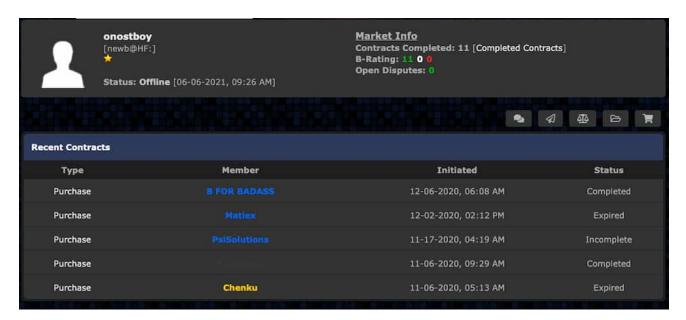
This list of domains then provided another set of important information. For one, DomainTools researchers were able to see that some of these links were being pushed by Bitly link shortening links. With Bitly, appending a "+" to any shortened link provides some data about that link. In this instance, 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.



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:

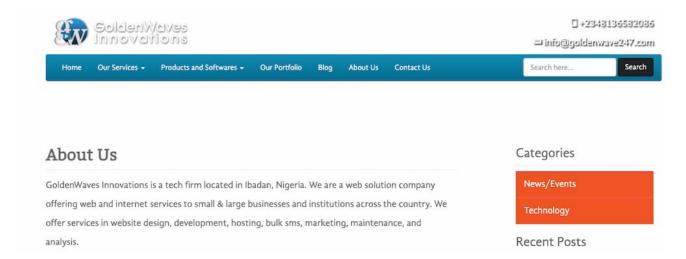
- Registration through NameCheap
- Containing the "relief" substring
- Containing the "eric" as in America substring or the "care" substring
- Registration after the signing of the bill into law on March 11, 2021
- Hosting on NameCheap (AS22612), Garanntor (AS328110), or OVH (AS16276) hosting infrastructure

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.



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 Ag	ge.
	DOMAIN	RISK SCORE ▼
	natwestgroupltd.com americans-relief-plan.us dasaniitablewater.us americansrelief-plan.us dasanitable-water.us americansreliefsplan.us americansreliefs-plan.us americans-reliefplan.us dasanitablewaters.us dasaniclassicwater.us american-reliefplan.us mtndecal-campaign.us dasanipremiumwater.us dasanitablewater.us americanreliefplan.us dasanitablewater.us americanreliefplan.us	100 99 98 98 97 97 97 97 96 96 96 96 95 95 93 93 87 86 85 76 67 65 65 65 37 32 31
□ % □ %	klozprick.com bacpasblog.com	25 25



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.

Companies / Nigeria / GOLDENWAVES INNOVATIONS

GOLDENWAVES INNOVATIONS

GOLDENWAVES INNOVATIONS was incorporated in Ibadan, Nigeria with Registration Number 2394351. It was registered on 18 Feb 2016 and it's 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

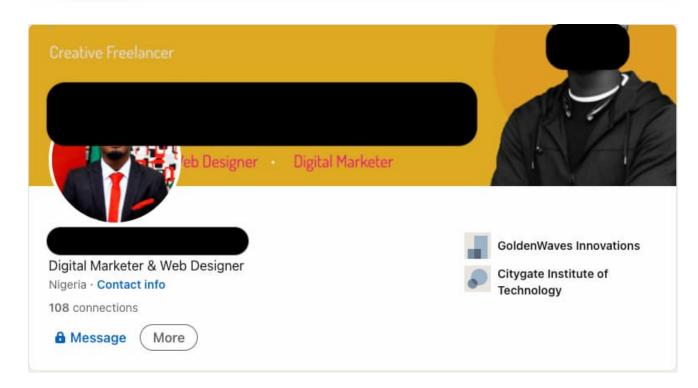
Registered Address

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

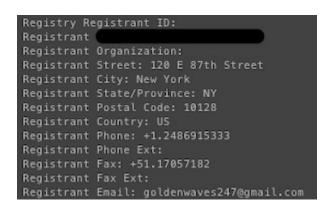
Owners / Directors / Key management personal

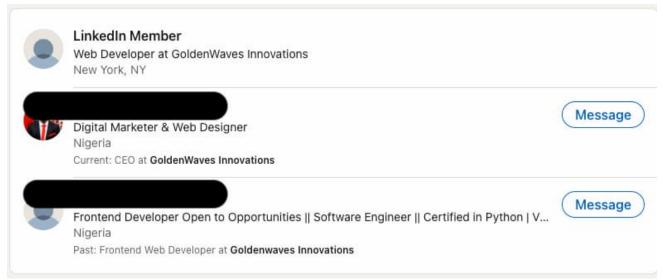
Name Designation

Proprietor



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.





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