

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

November 16, 2021



CYBER THREATS TO VETERANS IN 2021: Spam and Scams Exploit Support for Veterans



This report provides a high-level overview of cyber threats affecting veteran charity organizations in 2021 to include analysis of sample malicious domains, who is affected, and what individuals can do to protect themselves and others from falling for these types of scams.

Executive Summary

Veterans and their charitable donors have become the targets of many types of financial scam operations in recent years. These operations benefit from two emotional avenues by which to exploit victims: veterans struggling to support themselves, and those who wish to help veterans through charitable giving. Per Recorded Future data, we have found that veterans and their supporters are likely targeted by scams or spam associated with newly registered domains. We also identified an example of a scam operation called Protect Our Veterans SP, which uses several vectors to target veterans and their supporters, including fake charity, political action committee (PAC), and job scams. Finally, through psycholinguistic analysis, we have identified words, phrases, and syntax used on scam sites that indicate malicious intent by scam operators. To help those seeking to help veterans avoid falling prey to these operations, we offer several recommendations, such as how to research charitable organizations effectively and how to spot potential scams or spam based on their language and platform.

Key Judgments

- Per a review of potential domain abuse targeting veterans and their supporters, Recorded Future uncovered several domains linked to spam or phishing and a group of domains referencing “veteran affairs” that were linked via website infrastructure to a much larger group of domains targeting individuals interested in financial assistance or better work and educational opportunities.
- We found a possible scam operation advertising itself as a nonprofit charity organization called Protect Our Veterans SP, which bears several common characteristics of different types of scams, including fake charity, political action committee (PAC), and job scams.
- Together, these examples show that veterans and their supporters face cyber threats from several sources.

Trends in Domain Abuse Show Targeting of Veterans and Their Supporters

Domain Abuse: Methodology and Initial Results

As a demographic that often faces elevated economic instability due to difficulties in [finding work](#) or acclimating to life after military service, veterans can also be uniquely vulnerable to scams operated by cyberattacks that target victims with the promise of financial assistance. Our research into general trends in domain registrations uncovered several domains linked to spam or phishing and a group of domains referencing “veteran affairs” linked via website infrastructure to a much larger group of domains targeting individuals interested in financial assistance or better work and educational opportunities. Together, these examples show that veterans and their supporters face cyber threats from several sources.

As one method to identify potential cyber threat activity targeting veterans or their supporters, we analyzed our technical reporting on DNS and domains from January to early November 2021. In particular, we looked for any reference to the string “veteran” appearing in the names of domains that were registered, or for which certificates were registered, in this timeframe. Our initial query returned nearly 24,000 references. We believe that this high number includes a much larger set of indicators beyond our findings below.

Out of this large amount of data, we further subdivided domains by including other text strings like “support”, “protect”, and “affairs”, and then with a set of text strings related to monetary assistance like “money”, “fund”, and “charity”. Specific to the US withdrawal from Afghanistan in late summer 2021, we investigated domains that also referenced the string “afghan”. Finally, based on an independent lead regarding a scam-like campaign offering financial assistance to veterans via cryptocurrency and non-fungible tokens (NFTs), we further looked for domains that referenced “crypto” and “nft”.

These narrower queries returned approximately 500 domains. While we found no single cyber threat campaign incorporating language and topics related to all of the text strings above, we found multiple separate instances of suspicious or outright malicious activity, as described in more detail below. All of these queries are accessible to Recorded Future users in the clients-only version of this report.

Spam and Scams Feature Financial Assistance Lures

We first isolated any domains that were reported by others as exhibiting suspicious activity. These domains largely came from our queries for the string “support” and strings linked to financial assistance, which we suspect indicates that cyber spam or scams targeting veterans are likely to highlight a financial component and commitment early.

All dates are in 2021 and refer to when we saw the domains being registered:

- January 22: fiveveteranbenefitsinfosupport[.]site, which was reported as spam by Bitdefender in February
- April 24: college-money-for-veterans[.]site, which was reported as spam by Bitdefender in August
- November 2: principledveteransfund[.]biz and electprincipledveteransfund[.]biz, which were reported as spam by Bitdefender in November
- October 13: stlveteransupportnetwork[.]com, which triggered Recorded Future’s Phishing Lure risk rule in October
 - As of November 6, this domain features no hosted content and appears to be parked.
 - This domain is hosted on the IP address 34.102.136[.]180, which has a risk score of 64 due to recent links to intrusions, brute-forcing, and phishing. Hundreds of thousands of domains are hosted on this IP address, many of them corresponding to suspect naming conventions for queries informing both this report and other reports on minority groups from Recorded Future in the last 2 years.

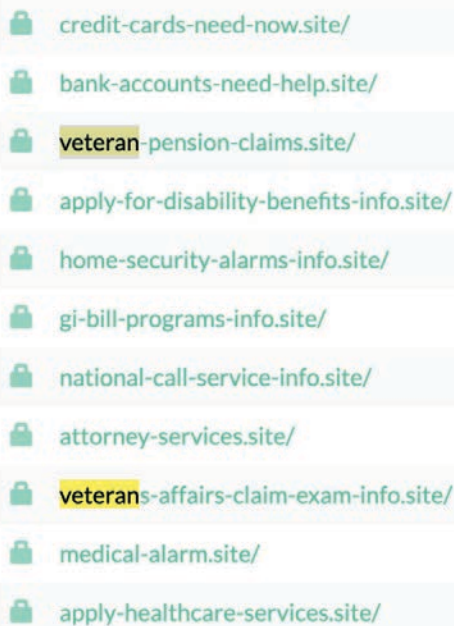
“Veterans Affairs” Spam Domains Linked to Larger Group of Around 1,500 Suspect Domains

In July 2021, Indiana Attorney General Todd Rokita warned veterans and military service members of “recent scams” that included “bogus military charities; calls, texts or emails attempting to impersonate the US Dept. of Veterans Affairs (VA); copy-cat recruiting websites; and crowdfunding scams”. Per a query in the Recorded Future Platform for the terms “veteran” and “affairs”, we confirmed that in July, many domains were registered featuring a version of the string “veterans-affairs” and flagged by Bitdefender as spam. These domains referenced veteran benefits, claims, and disabilities, and included:

- veteran-affairs-find-here[.]site
- veterans-affairs-benefits-types[.]site
- veterans-affairs-locations-find[.]site
- veterans-affairs-information-here[.]site
- veterans-affairs-disability-ratings-info[.]site
- veterans-affairs-claim-exam-info[.]site

Outside of Bitdefender’s reports, we found several other indicators of suspicious activity from this set of domains. All 6 domains were registered via domain anonymization services (such as Domains by Proxy), and all are currently hosted on the IP range 172.66.xx.xx, a Cloudflare IP range that masks a site’s ultimate source.

Per URLscan, the domain veterans-affairs-claim-exam-info[.]site used an icon hosted on Google’s Static File Front End service. Based on its [hash](#), within the last several months, this icon has appeared on hundreds of other domains with the .site top-level domain (TLD), with their names indicating the targeting of veterans, the military, seniors, and individuals in financial trouble related to credit cards and debt who are looking to benefit from government assistance. The screenshot below shows a sample of these websites:



credit-cards-need-now.site/
 bank-accounts-need-help.site/
 veteran-pension-claims.site/
 apply-for-disability-benefits-info.site/
 home-security-alarms-info.site/
 gi-bill-programs-info.site/
 national-call-service-info.site/
 attorney-services.site/
 veterans-affairs-claim-exam-info.site/
 medical-alarm.site/
 apply-healthcare-services.site/

Figure 1: Sample of list of around 1,500 domains associated with an icon hash and almost all using the .site TLD. References to "veteran" are highlighted. (Source: URLscan)

Based on their more unusual .site TLD and shared hash, we consider these domains likely linked to a single operator or registrar. The text strings in these domain names reference various subjects with a dominant theme of service or assistance for veterans, military service members, and seniors. Such topics include debt consolidation and grants, credit cards or bank accounts, government assistance, mortgage refinancing, legal representation, cybersecurity education, and homeland security.

Outside of the domains flagged by Bitdefender above, other suspicious domains from this set per URLscan included veteran-pension-claims[.]site and gi-bill-programs-info[.]site. Based on these findings, we recommend that in the near future, veterans, and especially US veterans, exercise caution with any domains referencing veterans' affairs that end in the .site TLD.

Additional Queries: Afghanistan, Crypto, and NFTs

Searching the Recorded Future Platform, we found little evidence of widespread registration of domains referencing both "veteran" and "afghan" in a manner to suggest targeting veterans of this war. A more general search for domains just featuring the term "afghan", however, did show a spike in late July to late August, corresponding roughly to the final withdrawal and media attention to the Taliban's speed of taking over cities of strategic value up to Kabul.

An independent lead within our Insikt Group disclosed a [suspicious campaign](#) on Instagram (pictured below) that features some likely targeting of US veterans with the promise of using cryptocurrency and NFT investments to escape debt. Although our research for this report could not accommodate full investigation of this campaign, per this lead, we created queries for the terms "crypto" or "nft" along with the term "veteran" in domains registered in the past year. These returned few results to indicate cyber threat activity; however, most of the domains in this data set for the term "nft" were hosted on IP addresses with elevated Recorded Future risk scores.

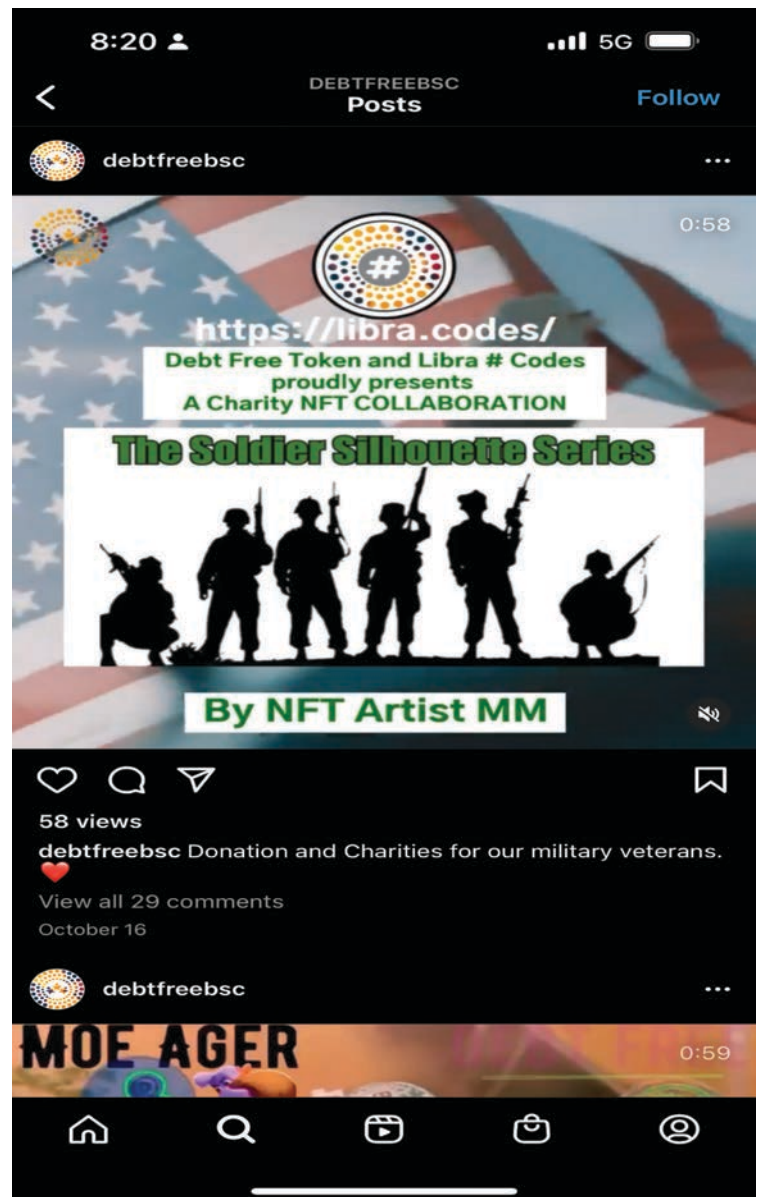


Figure 2: Instagram campaign featuring veteran-related imagery. A separate, although incomplete, investigation of this campaign found suspicious indicators of missing web infrastructure and high-volume bot engagement with posts. (Source: Instagram)

“Protect Our Veterans SP” Website Bears Classic Features of a Variety of Scams

Fake Charity, PAC, and Job Scams

We found evidence of a possible scam operation advertising itself as a nonprofit charity organization called Protect Our Veterans SP, which bears several characteristics common to different types of scams. The first is a charity scam, a fraudulent attempt to direct funds intended for communities in need into the pockets of criminals. Scams of this type can range from individuals masquerading as worthy and reputable beneficiaries to complex enterprises that look and operate similar to a legitimate charitable organization.

The operators of the Support Our Veterans SP web page may also be carrying out a Political Action Committee (PAC) scam. A [PAC scam](#) exploits political donors by posing as a PAC registered as a nonprofit, charity organization aligned with a particular political group. While donors believe they are giving to a cause they believe in, in reality the money goes straight to various illegitimate enterprises.

The developers of the website appear to be using the site to carry out fake job scams. A fake job scam involves a scammer making phony job postings, offering high wages in exchange for seemingly low effort from a victim. The scammer hopes to exploit the victim in a variety of ways, all of which end in the victim either losing money, providing goods or services for free, or finding themselves in legal trouble.

The following is an analysis of the ProtectOurVeterans[.]org webpage, which we believe shows that the site is actively using multiple vectors to exploit different groups of people, most notably veterans, their families, and their charitable donors.

Use Case: Protect Our Veterans SP

Protect Our Veterans SP advertises itself as a nonprofit charity organization for veterans and their families. Protect Our Veterans SP is not accredited with the Better Business Bureau (BBB), nor does it appear in reporting produced by GuideStar, an information services organization that tracks US nonprofit organizations. Analysis of imagery found on protectourveterans[.]org revealed an association between Protect Our Veterans SP and a social media account actively endorsing the organization. The owner of the account appears to be an author promoting several conspiracy theories. A [GoFundMe page](#) for the organization also exists. These may be attempts by the operator to add legitimacy to the organization, as more references across different sources can instill a false sense of confidence in victims.

The web page reveals very little about the initiative. The site offers no contact information for the organization, nor does it offer information regarding its 501(c)3 nonprofit organization status.

Protect Our Veterans, SP

[f](#)
[t](#)
[i](#)
[HOME](#)
[CONTACT US](#)
[EVENTS](#)
[PROTECT OUR VETERANS BLOG](#)
[MORE ▼](#)



MYBASEGUIDE.COM ENDORSES PROTECT OUR VETERANS

Click on the logo for more information

This website uses

We use cookies to analyze and optimize your website and accepting our use of cookies will be aggregated with a data.

Figure 3: Screenshot of protectourveterans[.]org homepage (Source: Recorded Future)

Protect Our Veterans SP appears to be a subsidiary of an organization called mybaseguide[.]com, which claims to be a nonprofit organization that helps veterans and active duty service members with duty station relocation. Like Protect Our Veterans SP, mybaseguide[.]com is not BBB accredited and does not appear in GuideStar reporting. Mybaseguide[.]com does have a profile on BBB, receiving a rating of 1 out of 5 stars from 6 client reviews. All 6 reviews make references to mybaseguide[.]com representatives misrepresenting themselves and misleading their clients.

The page's script includes 3 application programming interfaces (APIs) running in the background that return information to the site's domain registrant regarding the victim user's internet browser type and version. According to Recorded Future Platform data, the domain ProtectOurVeterans[.]org is hosted on the IP address 198.71.232[.]3, considered suspicious due to its association with recent botnet traffic and historical links to phishing attacks. Because of dynamic web hosting, in which multiple domains can be hosted on the same IP address, this is not sufficient evidence that this domain is actively participating in cyber threat activity. However, due to the domain's current web page resolution status and its association with recent botnet activity, we believe that this domain represents an immediate risk to charitable donors and recommend donors avoid interacting with the site.

Dissecting the Language of the Scammer

Figure 4 was taken from the Protect Our Veterans SP homepage, with suspicious wording circled. These types of scams are often run either by someone who is not a native English speaker or someone running multiple scam operations simultaneously and who is less concerned with content quality. For scammers, the quantity of scams they run matters more than the quality.

The wording of the first sentence immediately raises concerns. Legitimate charity organizations generally have web page content editors who would notice such an egregious grammatical error almost immediately. The second sentence includes an example of a trick used across all forms of scams. The content creator attempts to invoke a sense of urgency in the reader by asking the reader to "please send anyone you know" to the website. In this case specifically, the scammer is also attempting to manipulate victims into becoming recruiters of their friends and families without their knowledge. The scammer's hope in this scenario is that successfully scamming one individual will encourage the victim to bring more traffic to the site.

Throughout, words and phrases that do not appear to have been written by a native English speaker are used. The section titled "Our Focus" states, "We focus on making the maximum positive effort for our veterans". This sentence's odd syntax may indicate that the writer does not have a fluent grasp of the English language. As mentioned previously, this does not appear to be the work of a professional, English-speaking content developer.

The "Protect Our Veterans, SP" section includes another typo in the first sentence and something noteworthy in the last sentence. The organization appears to be advertising itself as a political action committee (PAC), stating that it "will elect the best of the best to lead this country in the 21st century". This tactic aligns with a recent trend reported by the Daily Beast [involving](#) scam PACs posing as charity organizations. Operators of these scams attempt to evoke an emotional response from the reader based on their political affiliation. The author of the Protect Our Veterans SP mission statement is implying that donating to their cause will help elect political leaders who align with the donor's political beliefs. Currently, there is no Super PAC registered with the name "Protect Our Veterans SP".

Further analysis of the website identified a tab leading to a page called "Honor a Veteran", which contained politically charged language targeting supporters of veterans initiatives. References throughout the page are made to the "shameful" treatment of veterans in the US, unsubstantiated statistics on veteran homelessness, healthcare, and incarceration rates, and more calls to donate to help elect "like-minded individuals who care about our soldiers and veterans". The statements are backed by vague references to "countless publications" and "a study", but no concrete evidence is provided to support any of these claims. As has been a trend highlighted thus far, the page is riddled with English grammar and syntax errors. The page also contains an image of a patriotic meme, potentially meant to elicit a sense of nationalistic duty from donors.

WHAT WE'RE ABOUT

Our Mission

Please join us in our to help veterans live a better life and make sure that veterans are receiving every privilege they are entitled to for putting on the uniform of the Red, White, and Blue. Please send anyone you know to www.protectourveterans.org and have them donate what they can. This mission is so important for far too many people. We have made it our mission to help those who helped us when we needed it most. WE cannot thank you enough for all of your help.

Our Focus

We focus on making the maximum positive effort for our veterans. Our members and volunteers provide the momentum that helps us affect change. Using data driven models, we provide solutions that make a long-lasting difference.

Protect Our Veterans, SP

Our amazing team of regulars and part-time volunteers are committed to helping others. We take our convictions and turn them into action. Think you would be a good fit? Get in touch for more information. The Protect Our Veterans Super PAC's main goal is to elect like minded individuals to protect the rights of our soldiers and veterans. Your generous gift will support programs which will elect the best of the best to lead this country in the 21st century.

Figure 4: Screenshot of protectourveterans.org mission statement (Source: ProtectOurVeterans)

HONORING SERVICE

Hug a Veteran

US VETERANS ARE TREATED LIKE SECOND-CLASS CITIZENS

Countless publications have shed light on the shameful treatment of veterans by the general public and the United States government. No one who has put their life on the line for our country deserves to....

- LIVE ON THE STREETS: UNFORTUNATELY, BETWEEN 529,000 AND 840,000 veterans experience homelessness, according to the National Coalition for Homeless Veterans
- MEDICAL CARE in a timely manner. An audit of the VA found that 120, 000 veterans for waiting far too long for medical care.
- BEING TREATED UNFAIRLY by the criminal justice system. A study has concluded there are 300 members of the military on death row without ever having their mental health evaluated.

Turn your conviction into action, donate to our cause today for us elect like-minded individuals who care about our soldiers and veterans



Figure 5: Screenshot taken from <https://protectourveterans.org/honor-a-veteran> (Source: protectourveterans.org)

FREEDOM IS NOT FREE!!

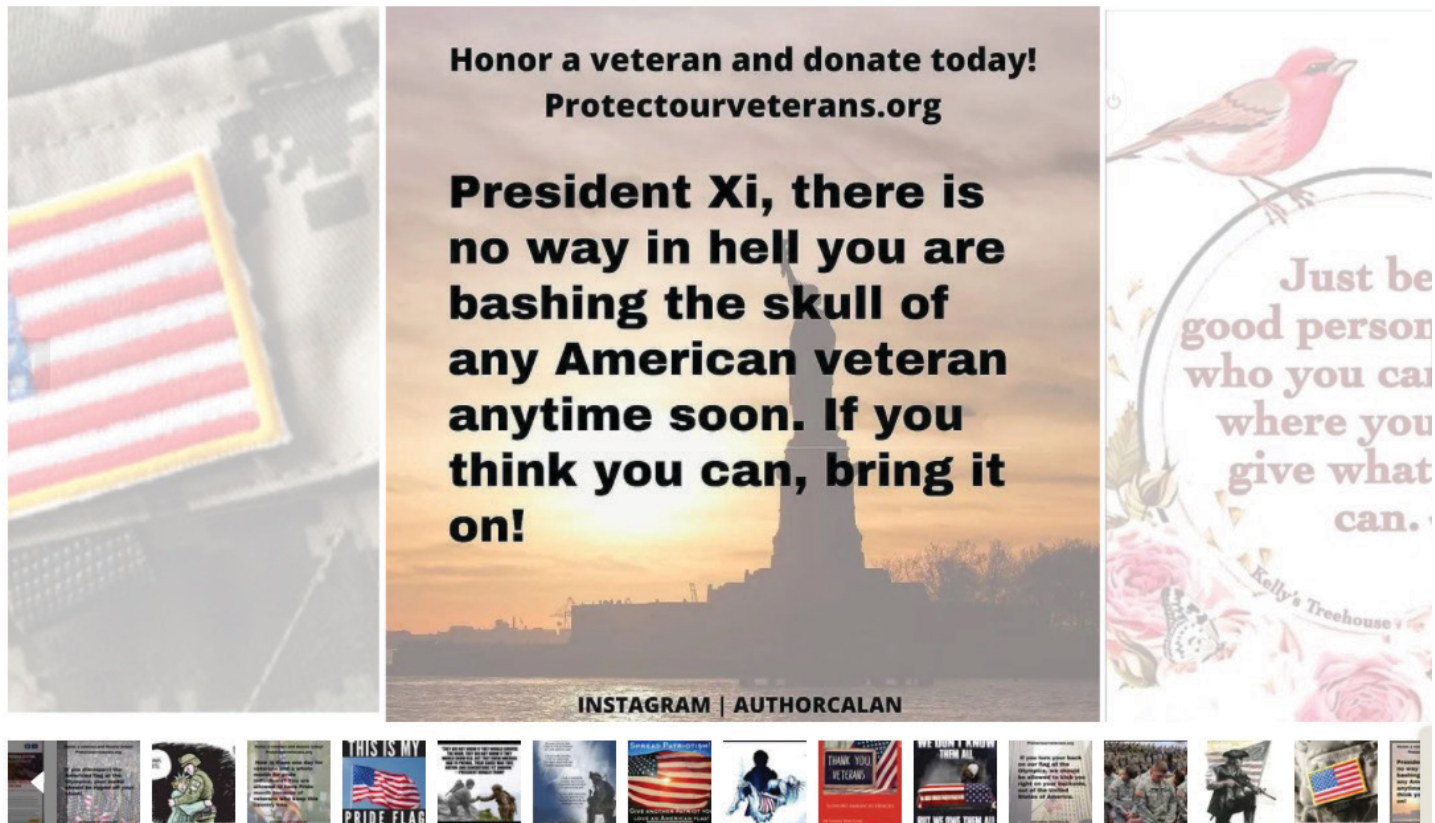


Figure 6: Example of xenophobic imagery displayed on the Protect Our Veterans SP webpage (Source: protectourveterans[.org])

The site also contains jingoistic and xenophobic imagery, such as the example in Figure 5. Invoking an individual's sense of patriotic duty and fear of the outside world are common tactics used by scammers to bait victims who believe they are donating to a cause that aligns with their political and moral beliefs. In this example, the image creator, an Army veteran, is attempting to invoke a sense of anti-Chinese sentiment, or Sinophobia, in the reader. Since the beginning of the COVID-19 pandemic, sinophobic rhetoric, as well as threats toward other Asian communities, have risen dramatically, particularly in English-speaking regions of the world, as detailed in Recorded Future's research on [Threats to Asian Communities in North America, Europe, and Oceania](#).

In the current political climate in the United States, patriotism and political affiliation are attractive fraud lures for scammers. The site includes a blog with posts referencing right-wing extremist ideologies, indicating that the target of this scam operation may be those who align themselves with the right end of the political spectrum. Imagery and iconography used on the site could very well be the work of a domestic operation, but the imagery appears to align with noteworthy influence campaigns [carried out](#) by Russia's Internet Research Agency (IRA) targeting veterans in the past. This is not sufficient evidence to confirm that this is an influence operation, but there do appear to be overlaps in [imagery and iconography](#) used by Protect Our Veterans SP and the IRA.

THOUGHTS AND OPINIONS OF PROTECT OUR VETERANS



October 23, 2021

Veterans are the backbone of this country!!

Please do not forget veterans need our help. The organization best positioned to help veterans is protectourveterans.org

[Continue Reading](#)



October 11, 2021

What We Truly Do!

Go to protectourveterans.org to donate. We landed in Facebook jail for a post we made. Facebook returned over 50k in donations for memes "allegedly" against their arse-kissing Biden rules. The post and memes were made be...

[Continue Reading](#)



September 1, 2021

Shame on you, Mr. Biden, shame on you!

We've been getting a lot of emails recently from individuals wondering why we all work so hard to raise money to bring awareness to the plight of a veteran. The woke crowd has spent a considerable amount of time try...

[Continue Reading](#)

Figure 7: Screenshot of [protectourveterans\[.\]org](https://protectourveterans.org) blog with posts alluding to right-wing extremist ideology (Source: [protectourveterans\[.\]org](https://protectourveterans.org))

Double-Dipping: How One Scam Can Lead to Another

It is not uncommon for a scammer to leverage one scam to carry out another. In addition to the charity and PAC scams described above, Recorded Future analysts were able to identify evidence that the operators of Protect Our Veterans SP are using the organization to carry out a fake job scam as well.

From a post in the Reddit community r/scams, user u/ghostgoddess7 describes their interaction with a Protect Our Veterans SP representative (the following is quoted verbatim):

Last week I applied for a Communications/Fundraising Assistant Manager for an org called Protect Our Veterans. The founder posted the job and contacted me through messenger and then told me to call him anytime this week. I called him and we had a 50 minute conversation in which he initially told me that the organization is a non-profit and Super PAC that donates all donations to veterans. However, based on how many people/amounts are donated, I get 25% commission through my money receiving system of choice (Venmo, pay pal, etc). That sounded a bit sketchy to me because it just seemed like the position consisted of calling people for donations. On top of that he said that he has considered buying lists of people's phone numbers but instead opted for the white pages because the previous was too expensive.

After he realizes that I'm not sold for the calling and finding donors idea, he asks me what I want. I tell him that I'm looking for a full time position where I can use my education (BA & MA) and skills. Then, he comes back and tells me that he's talked with a business partner of his and has established a task for me before the initial hiring. He said that if I'm able to raise 1500 dollars by Friday and be able to present a PowerPoint on how my skills could help the org, I'll get hired at the first guy's media company and receive 135,000 dollars salary as Vice President of Business Development. I thought this was a bit far fetched because I wasn't able to find much info on the org or the person I talked to other than his author pseudonym that he gave me, his author website, and a vague LinkedIn page. On his LinkedIn page, he only mentions his education and his books business. There is no mention of Protect Our Veterans fundraising drives or anything.

First, the scammer reaches out to the applicant via Facebook Messenger. Most legitimate organizations will communicate via email or phone, not public messaging platforms. Social media exploitation is a popular tactic used by advanced persistent threat (APT) groups and scammer gangs due to the increased likelihood that potential victims will interact with a fake social media account as opposed to answering a call or text message from an unknown phone number. The applicant describes that the role is commission-based, depending on the number of people the applicant recruits to donate to the organization. This aligns with the recruitment theory outlined in the Dissecting the Language of the Scammer subsection above and is a tactic used to get the applicant to recruit their friends and families.

After the applicant expresses skepticism, the representative changes course and asks the applicant to carry out a task before the hiring process can be completed. As referenced above, the scammer attempts to invoke a sense of urgency in the applicant, declaring that the job offer is contingent upon the applicant raising \$1,500 USD and presenting how they were able to raise the money in exchange for the role as the organization's Vice President of Business Development with a salary of \$135,000 USD. The Reddit user states that they located the representative's pseudonym and author website, which may correlate with the social media account above, considering the representative is referred to as an author in both the Reddit post and the social media account. The user's inability to find additional intelligence on the representative indicates that they are likely using a fake identity and that the organization does not exist. This leads us to believe that Protect Our Veterans SP is being used as a front for a fake job scam as well.

Outlook and Recommendations

A thriving market exists for scam operators who have begun to see the veteran community as an easily exploitable target. The ease with which scammers can carry out scam operations against veterans is exacerbated by the current state of US government policy and its failure to care for veterans adequately. As economic inequality in America further divides the country, veterans are finding survival after their military service an increasingly difficult proposition.

Scams targeting veterans and veterans organizations are only part of the problem. The real obstacle Americans face in defending veterans from scams and fraud lie in the standards, policies, and norms in place today which have created an environment where scams, such as those highlighted in this report, are able to thrive. It stands to reason that making veterans' charities a luxury and not a necessity by providing veterans the healthcare and support they have earned would make the operating costs of a fake charity scam untenable in relation to its return on profit. Government policies that provide clearer paths toward debt-free living for veterans would reduce the need for them to seek out increasingly risky and desperate measures to get by. Fewer unemployed veterans would equal fewer opportunities where fake job scams can succeed. Improve the living conditions of veterans and reduce the attack surface for criminals targeting veterans.

The policies in place today do not inspire hope in the veteran community, who increasingly [view](#) government institutions such as the VA as corrupt and inefficient. This is creating an opportunity for foreign and domestic influence operations, such as Russia's IRA, to further the divide between Americans and their government by spreading hateful rhetoric under the guise of patriotic vigilance. As a result, veterans and their supporters are viewing more extreme ideologies as reasonable alternatives to their growing dissatisfaction toward the status quo.

Perhaps the most effective solution to eliminating scams targeting veterans and their supporters is to establish government policy that improves the livelihoods of veterans so much so that targeting the veteran community would no longer be a viable option for criminals. So long as we have veterans in need of support, we will have criminals seeking out new ways to exploit them.

For veterans seeking to reduce the likelihood that they will be targeted by a scam operation, we offer the following recommendations:

- Be wary of organizations that appear to be provoking emotional or urgent reactions from you. Legitimate organizations do not pressure customers into decision-

making, and non-partisan organizations will refrain from using politically charged rhetoric to influence customer opinion.

- If an organization is asking for payment, consider the method of payment. Scammers will request money be sent via means from which the funds cannot be retrieved, such as wire transfers or gift cards.
- Organizations making financial offers that appear too good to be true, such as immediate debt payoffs or payday loan services, may be attempting to lure veterans and service members who find themselves in financially desperate situations. We recommend seeking out legitimate government and non-profit organizations such as [Military OneSource](#) or [Disabled American Veterans](#) for assistance.

For those seeking to help veterans through charitable giving, consider the following recommendations:

- When researching a charitable organization, take a moment to look them up using resources such as [your state consumer protection office](#), [GuideStar](#), or the [Better Business Bureau](#). Legitimate charities take pride in their 501(c)3 nonprofit status, and will often display it on their homepage. If a basic search does not yield information regarding the organization's nonprofit status, then it may be an attempt by the organization to hide their lack of credentials.
- Legitimate charity organizations will have a website designed by a professional content developer, meaning the content on the page will have been reviewed before being published. Basic grammar and syntax errors can be a warning sign that the site is not professionally set up.
- Attempts by an organization, either through rhetoric on their website or through direct contact, to incite a strong emotional or urgent response may be an indication that the organization is trying to manipulate donors in a manner that may represent malicious intent. If an offer feels too good to be true, or if it feels like you are being rushed to judgment, it may be an attempt to expedite the scam's process for a quicker payout.
- Scammers often communicate and ask for payment by unconventional means. For example, a social media account may directly message a target via messaging apps like Messenger or Instagram. They may ask for payment via payment sites like PayPal, cryptocurrency, or even gift cards. Legitimate charitable organizations will often have an official payment portal, such as this one belonging to the [Wounded Warrior Project](#).

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.