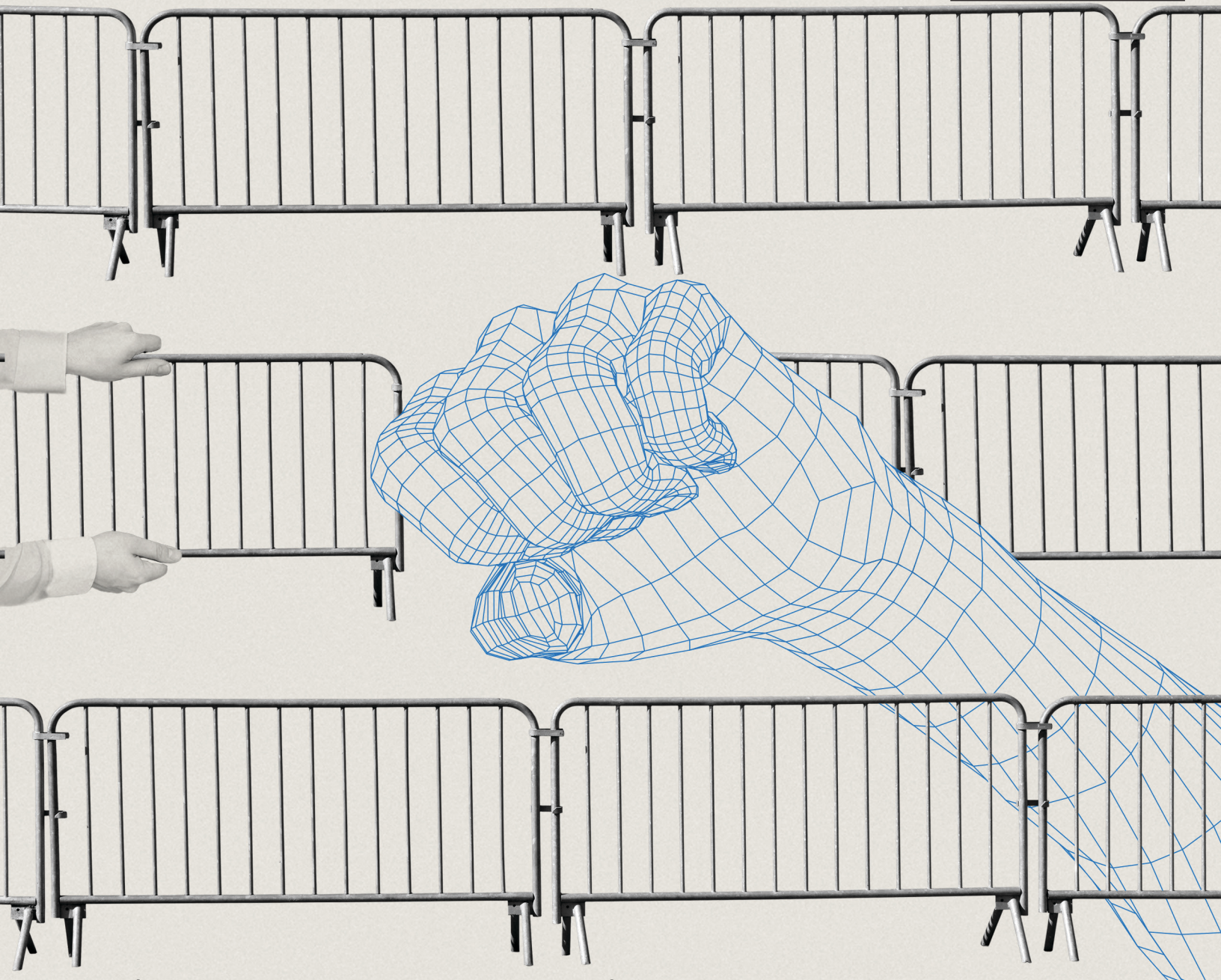
THREAT ANALYSIS

Recorded Future®

By Insikt Group®

March 27, 2024



Violent Extremists Dox Executives, Enabling Physical Threats

Executive Summary

Domestic violent extremists (DVEs) are increasingly doxing senior United States (US) public and private sector leaders — publishing their personally identifiable information (PII) without their consent and with malicious intent. Historically, most DVE doxing attempts have targeted other DVEs and ideologically opposed political activists. However, in recent years, DVEs from a range of different ideologies have also frequently doxed government officials, C-suite executives, and the heads of educational institutions, media outlets, and non-government organizations. These doxes typically follow decisions by the senior leaders' organizations on issues that are controversial among DVEs; notable recent issues include organizations' stance on Israel and its war against Hamas, their support for diversity, equity, and inclusion (DEI) policies, and their real and perceived political alignments. Online negative sentiment directed toward an organization in sources popular among DVEs is a likely predicate of doxing campaigns targeting those entities' leadership.

DVEs almost certainly dox their victims to enable threat activities such as harassment, stalking, demonstrations, surveillance, physical approaches, and violent attacks. When an individual is doxed, DVEs are almost certainly signaling that they view the individual as a legitimate target for attacks and are encouraging other DVEs to take action against the victim. Therefore, the victim of a DVE dox is likely at increased risk for follow-on physical and cyber threat activities. Doxed business leaders and their companies have also suffered financial and reputational damage as a result of doxing, in conjunction with significant online negative sentiment directed toward the company or executive.

According to a January 2024 SafeHome survey, eleven million Americans reported that they had been doxed, and several reports noted a marked increase in doxing attempts against corporate executives during 2023. To protect against successful doxing attempts and mitigate second-order physical and cyber risk to executives, senior public and private sector leaders should adopt strong cyber hygiene practices and utilize the Recorded Future Intelligence Cloud to monitor for such threats. In addition, they should request the removal of senior leaders' and their families' PII from people search websites and similar sites, conduct routine audits of their digital footprints, and develop contingency plans in the event of a successful doxing attempt. If a senior leader or a family member of a senior leader is successfully doxed, the victim should document and archive the information in the dox, conduct a risk assessment based on the published PII, seek to identify the source of such information and remediate it, and, if necessary, report the incident to law enforcement.

Key Findings

- DVEs almost certainly dox targets to enable additional physical and cyber threat operations against the victim.
- DVEs almost certainly only need to obtain basic PII about the target — such as a home address, email address, or phone number — to enable these operations.

- Aside from opposing DVEs and political activists, highly visible leaders of public and private sector organizations are the most likely targets of DVE doxing attempts.
- DVEs frequently leverage people search websites, online property record databases, and victims' (and their families') social media as sources of information for doxes. To avoid online terms of service (ToS) enforcement, DVEs host doxes on an array of online infrastructure, including Telegram channels, DVE-managed blogs and websites, and paste sites.
- DVE doxing campaigns against senior leaders of an organization typically follow controversial, high-profile organizational decisions and reactions to domestic political or geopolitical events. Significant online negative sentiment in DVE sources toward an organization is a likely indicator that DVEs may dox the organization's leadership.
- To reduce the risk of successful doxes and mitigate second-order harms, public and private sector leaders and their families should adopt strong cyber hygiene practices, utilize the Recorded Future Intelligence Cloud to monitor for these threats, request removal of PII from online sources, and develop a doxing response plan.

Doxing by Violent Extremists: Motivations and Methods

Doxing refers to the act of posting an individual's PII online with malicious intent and without the individual's consent. The term and practice originated in hacker communities in the 1990s, but a range of threat actors — including cybercriminals, hacktivists, political activists, violent extremists, pranksters, and journalists — have employed the practice. To dox victims, these threat actors access information about their targets through open sources or illegally obtain information through cyber intrusions, theft, leaks, data breaches, or unlawful use of online investigative tools. The threat actors then post the information they collected online — typically in a text-based "dox file" on a paste site, which is then recirculated and distributed on social media, messaging platforms, and other public-facing web infrastructure.

The almost certain goal of doxing attempts conducted by DVEs is enabling a range of other physical and cyber threat activities against a preferred target.[1] By publicizing even the most basic PII about a victim, such as a home address, email address, or phone number, like-minded DVEs have access to the information they may need to threaten, harass, stalk, protest against, surveil, approach, or attack a target. Certain popular DVE attack vectors, such as "swatting", in which DVEs falsely report threats connected to an individual or location to law enforcement, are wholly dependent on a threat actor's knowledge of an individual's basic PII. Being doxed by a DVE group almost certainly entails that the threat actor in question views the victim as a legitimate target for other physical and cyber threats; as such, doxing could be considered an *ipso facto* threat.

DVEs of various persuasions frequently dox individuals they perceive to be their ideological adversaries, generally corresponding to their preferred targets for physical attacks. Because of their distinct ideologies, doxing targets vary slightly by the DVE group in question. For example, while white supremacist and neo-Nazi DVEs are very likely to dox members of minority racial and religious communities and the LGBTQ+ community, public officials, law enforcement, journalists, and members of opposing DVE groups, single-issue violent extremists motivated by anti-abortion sentiment have historically focused on doxing healthcare workers who provide abortions. Regardless of their specific victims, DVE target selection for doxing typically follows at least one of three motivations:

- **Threatening:** DVEs dox individuals to enable or encourage other physical and cyber threat activity against the victim, signal that the victim is a legitimate target for other threat activity, or directly threaten the victim or the victim's family.
- **Retribution/retaliation:** DVEs dox individuals — particularly journalists and members of opposing DVE groups — in response to these individuals' doxing attempts or journalistic coverage of DVEs.

[1] The US Intelligence Community defines a domestic violent extremist as "an individual based and operating primarily in the United States without direction or inspiration from a foreign terrorist group or other foreign power and who seeks to further political or social goals wholly or in part through unlawful acts of force or violence. This assessment does not evaluate the actions of individuals engaged solely in activities protected by the First Amendment or other rights secured by the Constitution of the United States".

- **Show of capabilities:** DVEs dox individuals — particularly those who have implemented operational security measures — to demonstrate their proficiency with open-source intelligence (OSINT) capabilities and establish *bona fides* within their broader DVE communities.

DVEs almost certainly need to access and publish only a limited amount of a victim's basic PII, such as a home address, email address, or phone number, to enable additional physical or cyber threat operations and accomplish the almost certain goals of doxing. Obtaining this information does not require DVEs to use complicated tactics, techniques, or procedures (TTPs) or leverage sophisticated capabilities, which almost certainly boosts the popularity of doxing as a tactic among DVEs. This factor is particularly salient in the United States (US) and other contexts where address, email, and phone number data are widely available on people search websites and from local governments providing online access to property records. In addition, in many states in the US, as well as in most jurisdictions around the world, doxing itself may not be illegal. In this respect, doxing provides DVEs an alternative to other methods of threatening individuals that are more likely to result in arrests or prosecution.

After obtaining a victim's PII, DVEs compile the information in text format into a "dox file" (or simply, a "dox") and publish the dox online, usually on social media and messaging platforms, paste sites, and DVE-managed websites and blogs. Although doxing may not be illegal in most jurisdictions, many online service providers' ToS prohibit doxing, particularly when it is conducted in furtherance of a DVE movement or ideology. DVEs have several methods of circumventing ToS enforcement to host doxes: they share dox files on numerous online platforms, utilize web archiving services to create stable copies of dox files, and leverage paste services on the dark web and DVE-managed websites to host doxes. Due to frequent ToS enforcement against DVE content on many online platforms, DVEs are almost certainly developing more sophisticated means of hosting text-based content like doxes, likely gleaning insights from cybercriminals and other threat actors who conduct doxing.

While the bulk of DVE targeting for doxes likely focuses on opposing DVE groups, in recent years, several groups — particularly white supremacist and neo-Nazi violent extremists and anarchist violent extremists (AVEs) — have doxed or attempted to dox senior government officials, C-suite executives of major corporations, and the leaders of media outlets, educational institutions, non-governmental organizations, religious and community organizations, and nonprofits.[2] In February 2022, the National Counterterrorism Center detailed executive protection considerations for public officials in the wake of increased DVE doxing campaigns, noting that DVEs "may attempt to monitor (in person and virtually) public officials, as well as their families, to establish patterns. With this in mind, public officials and their families should assess their online presence and any exposure to reduce the risk of a targeted attack".

DVE Doxing Attempts

Insikt Group reviewed three dox files posted by DVEs or distributed within DVE online sources, including on Telegram channels, anarchist counter-information websites, and on the doxing paste site Doxbin. In

[2] The US Intelligence Community defines AVEs as "DVEs who oppose all forms of capitalism, corporate globalization, and governing institutions, which are perceived as harmful to society".

total, the three files include the PII of 39 victims. **Dox #1** involved a white supremacist threat actor targeting a private US citizen with opposing political views; **Dox #2** involved an anarchist threat actor targeting a mayoral advisory council consisting of business and educational leadership; and **Dox #3** involved a white supremacist threat actor targeting a business executive and the executive's family due to the company's advertising campaign. To protect victims, this report does not include specific references to the PII found in these files and refers to all threat actors and victims using numeric indicators, gender-neutral pronouns, and generic descriptions of their demographic backgrounds and roles. In some cases, we have also redacted the names of sources and descriptions of methods to minimize exposure of our analytical process for operational security and harm mitigation purposes.

We used a modified version of the Diamond Model of Intrusion Analysis to assess each dox file.[3] As **Figure 1** shows, doxing is a malicious event that includes four components: an adversary or **threat actor** who conducts the dox due to specific impetuses and motivations, leveraging **capabilities** to find sources of personal information about a **victim** and publishing the information using online **infrastructure.** For the dox files, each of these four aspects of doxing is highlighted in individual sections to analyze DVE threat actors' motivations, TTPs, target selection processes, and methods of publishing and distributing doxes.

[3] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz, "The Diamond Model of Intrusion Analysis". US Department of Defense Technical Report, May 2013.

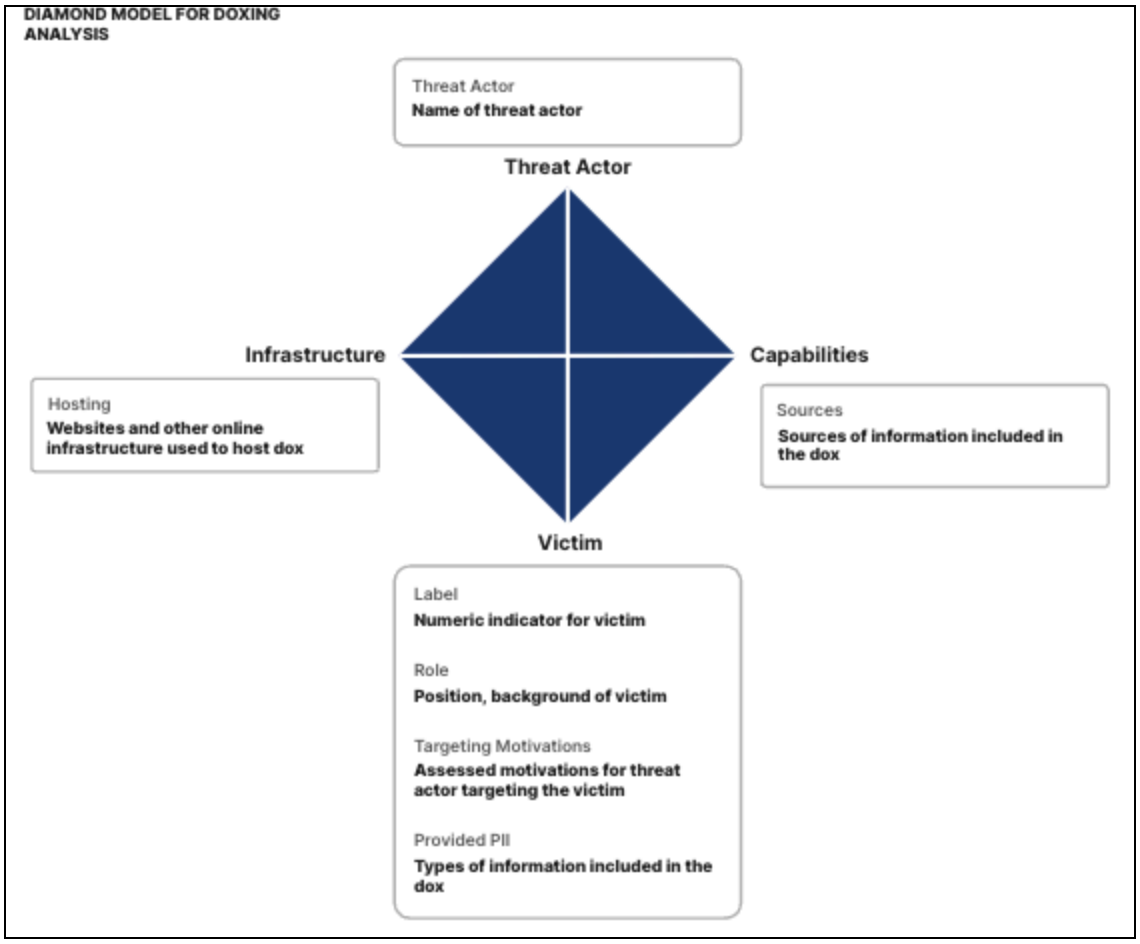


Figure 1: *Template for Diamond Model analysis of doxing attempts (Source: Recorded Future)*

Our assessments of DVE doxing capabilities — the sources of information they used to obtain PII — are predicated on Insikt Group's own OSINT investigations. During this process, we "reverse-engineered" DVE doxing campaigns by conducting our own searches for information on the doxing targets using OSINT tradecraft, with the objective of determining which sources of data DVE threat actors were leveraging to dox their victims.

Dox #1: White Supremacist Threat Actor Targets Political Opponent

In October 2023, DVE Threat Actor #1 doxed Victim #1, a private citizen residing in Tennessee, purportedly because the victim "[attacked] active clubs".[4] DVE Threat Actor #1 published Victim #1's date of birth (DOB), phone numbers, home addresses, social media profiles, email addresses, online account information, and an image of Victim #1's house. The threat actor almost certainly obtained this information through Victim #1's social media profile, people search websites, the online OSINT tool *search[.]0t[.]rocks*, and Google Maps. Dox files for Victim #1 were posted on a PasteBin site, an archived version of the PasteBin site, and in two pastes on dark web paste site *dump[.]li*.

[4] To protect doxing victims and limit further dissemination of terrorist and violent extremist content, this report does not provide external links to this content. All direct quotations from these sources reflect original grammar, syntax, and spelling as reviewed by Recorded Future.

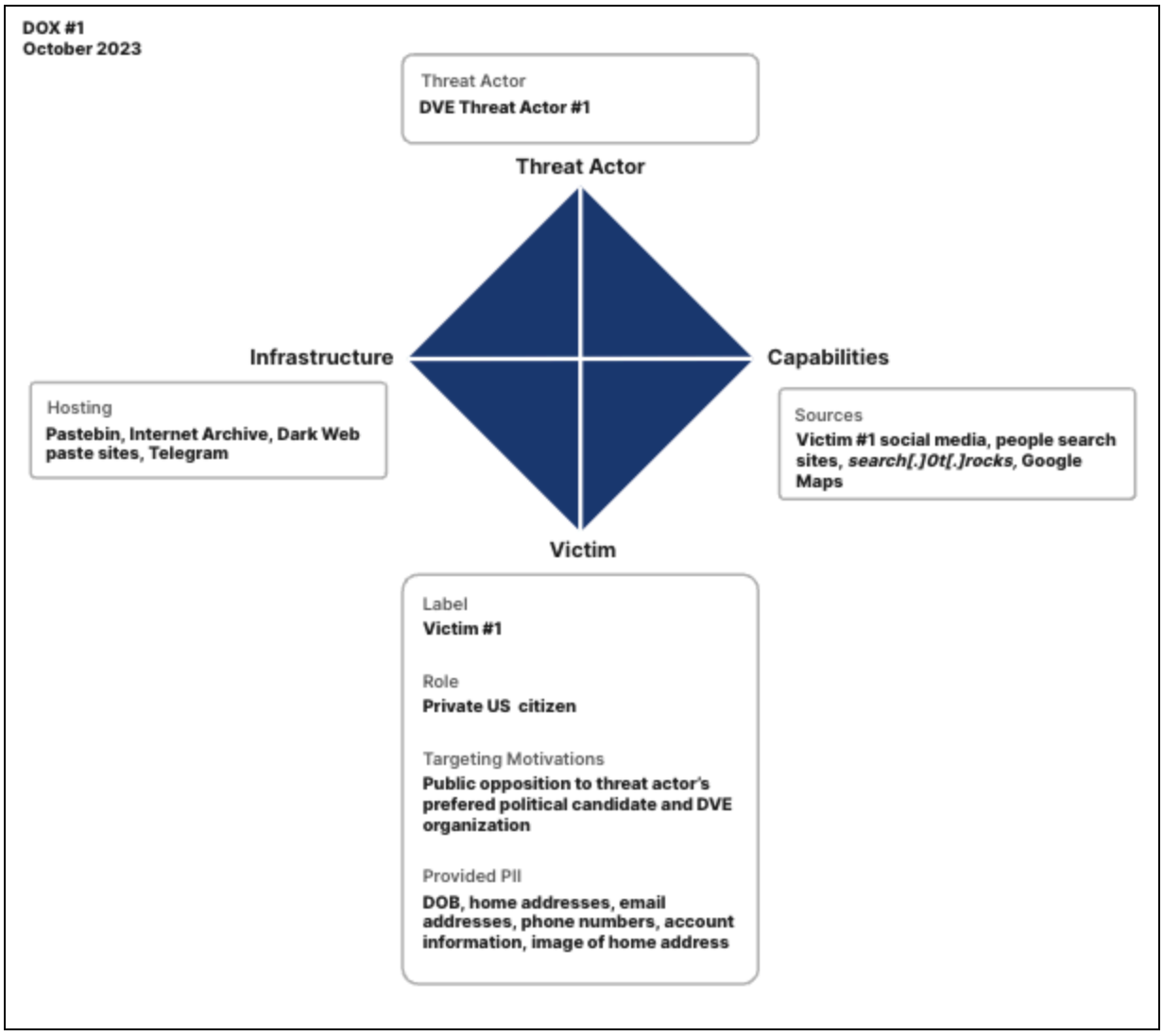


Figure 2: *Diamond model analysis of Dox #1 (Source: Recorded Future)*

DVE Threat Actor #1

DVE Threat Actor #1's activities are concentrated on Telegram. Based on the threat actor's username and frequent interactions with, and praise for, US white supremacist active clubs, particularly in the US Southeast, DVE Threat Actor #1 is very likely an affiliate or member of an active club in the US state of Tennessee, Kentucky, North Carolina, or Virginia.[5] The channel that hosted Dox #1 was initially established in May 2023; it has since been suspended by Telegram and replaced with several other iterations. In addition to distributing DVE ideological material, circulating media from DVE organizations in the US, and providing DVEs with operational security manuals, this channel has also frequently doxed individuals in the US it perceives to be adversaries of the white supremacist and neo-Nazi movements.

[5] In this context, an "active club" refers to a white supremacist, white nationalist, or neo-Nazi organization centered around the "premise of a white supremacist brotherhood" that typically engages in physical training for hand-to-hand combat.

DVE Threat Actor #1 asserts independence from any organization or group but is almost certainly aligned with local active clubs and Patriot Front, a US-wide network of active clubs. Beyond frequently reposting Patriot Front and active clubs' propaganda and messaging, the group has also collaborated with "Patriot Youth", a self-styled Patriot Front youth wing. Most notably, in September 2023, DVE Threat Actor #1 and Patriot Youth doxed members of the American Iron Front (AIF), an AVE group, by infiltrating the AIF's Discord channels, leaking channel conversations online, researching individual accounts, and publishing dox files on several notable members.

DVE Threat Actor #1 almost certainly supports a variety of active clubs operating in the US but has most frequently interacted and collaborated with the Tennessee Active Club (TAC), based in the Nashville, Tennessee, area. Based on the frequency of these interactions and the level of access to the organization, the administrator(s) of DVE Threat Actor #1 are very likely based in Tennessee. TAC, led by Sean Kauffmann, has actively engaged in protests and demonstrations against events for the LGBTQ+ community, has connections to Patriot Front and other local active clubs, and trains from a makeshift gym at a location in Lewis County, Tennessee.

Most notably, TAC was recently involved in a 2023 mayoral campaign in Tennessee. TAC members and social media accounts rallied supporters for a candidate's cause, conducted public shows of support for the candidate at town meetings, and threatened the candidate's political opponents. In October 2023, the candidate appeared in a video interview with Sean Kauffman, highlighting their political campaign and the TAC's goals, objectives, and ideology. This interview was originally published on DVE Threat Actor #1's Telegram channel, which also posted "teasers" of the video in the week before its publication, suggesting DVE Threat Actor #1' almost certain involvement in TAC's propaganda and recruiting operations.

Target (Victim #1)

Dox #1 targeted Victim #1, a private citizen residing in Tennessee. Although DVE Threat Actor #1 claimed to have doxed Victim #1 because the individual "[attacked] active clubs", the threat actor's very likely motivation for targeting Victim #1 was the victim's opposition to the threat actor's preferred mayoral candidate. In the weeks leading up to the October 2023 dox, Victim #1's social media account frequently voiced disapproval for the candidate and the candidate's campaign. After the victim was doxed, Victim #1 acknowledged the dox on social media but claimed to have never publicly spoken out against active clubs on social media, only against the candidate. The activity of the social media account connected to Victim #1 is generally consistent with these statements.

Victim #1 was a notable, though somewhat unusual, doxing target for DVE Threat Actor #1, as the individual is not a member of an opposing DVE group, a counterterrorism or counter-extremism researcher, or an elected official. These attributes typify the victims of many of DVE Threat Actor #1's other doxes. These facts lend credence to the assessment that Victim #1 was targeted solely due to their political advocacy and also likely explain why DVE Threat Actor #1 was able to collect a substantial amount of personal information on Victim #1 in the dox. Victim #1 very likely did not implement or

consider implementing operational security or cyber hygiene measures prior to engaging in online political advocacy because the victim was unaware that this activity would make them a target for violent extremist threat actors.

Capabilities

DVE Threat Actor #1 almost certainly used four sources of information to dox Victim #1: the victim's social media profile, people search websites, Google Maps, and the OSINT tool *search[.]0t[.]rocks*, which collects, scrapes, and aggregates information from online data breaches. The first level of Victim #1's exposure to a dox was very likely the victim's social media account, where the victim most frequently engaged in political advocacy. DVE Threat Actor #1 used this account as one of its "inputs" into the *search[.]0t[.]rocks* search that it publicized, very likely indicating that the account was the starting point of the threat actor's information collection activities. Victim #1 also almost certainly posted about the mayoral campaign and the involvement of active clubs on a Facebook account, but references to this account did not appear in DVE Threat Actor #1's dox. Insikt Group also independently identified several other social media accounts and other sources of online information about Victim #1 that DVE Threat Actor #1 did not include in the dox, very likely suggesting that Victim #1's social media accounts were the entry point but not the main focus of DVE Threat Actor #1's investigation.

After reviewing Victim #1's social media account, DVE Threat Actor #1 almost certainly relied on people search websites to gather information about Victim #1's DOB, home addresses, email addresses, and phone numbers. Data listed in dox files generally correspond to information obtained through common online people search tools. The dox files list a DOB, eight phone numbers, eleven email addresses, fourteen residential addresses, and an account on an educational website that DVE Threat Actor #1 attributed to Victim #1. From this data, the dox file isolates a phone number, residential address, and two email addresses that DVE Threat Actor #1 believes are Victim #1's current information, very likely based on corroborating information from the threat actor's *search[.]0t[.]rocks* search. In addition, DVE Threat Actor #1's Telegram post with links to the dox files also contains an image of Victim #1's house that the threat actor almost certainly obtained from Google Maps Street View.

In a separate file from the main dox, DVE Threat Actor #1 posted information that was almost certainly retrieved from *search[.]0t[.]rocks*, a site that allows users to query a database of over fourteen billion records from data breaches. Formerly known as *illicit[.]services*, the tool was developed as a free alternative to the OSINT search tool Intelligence X, and, according to its developer, it "quickly grew popular in the doxxing and sim-swapping community". *Search[.]0t[.]rocks* allows users to enter a variety of data points and query the database for hits in breach data, yielding further potential PII on the target of an investigation.

The additional information mirrors the layout of data from a *search[.]0t[.]rocks* query, which was conducted using Victim #1's social media username(s), last name, and email address. The tool assigns each search result a similarity score; records that are likely to belong to the same individual receive a score of 10.0 or higher. DVE Threat Actor #1 almost certainly replicated information from this search in the main dox file, especially in corroborating information about Victim #1's email addresses and

determining a DOB. Notably, no people search website contains Victim #1's full DOB — only a month and year combination — but a record in the *search[.]0t[.]rocks* search from the 2021 Unknown Consumer data breach contains a full DOB that mirrors the record in DVE Threat Actor #1's dox file.

Infrastructure

Dox #1 consists of two separate dox files distributed through multiple means, all of which were hyperlinked in an October 2023 post on DVE Threat Actor #1's Telegram channel. The main dox file was hosted on at least three unique URLs: a Pastebin page; an October 2023 archived copy of the Pastebin page in the Wayback Machine; and a *dump[.]li* page with a .onion top-level domain (TLD). The second dox file, which contains the results of the *search[.]0t[.]rocks* query is solely available on a *dump[.]li* page with a .onion TLD. The diversity of formats very likely reflects DVE Threat Actor #1's belief that certain versions of the dox — particularly the Telegram post and Pastebin page — would eventually be subject to ToS enforcement or deletion.

The administrator(s) of DVE Threat Actor #1 have frequently expressed interest in moving their infrastructure for doxing off of clear net websites and messaging applications. This commitment is almost certainly the result of their surface web infrastructure and Telegram channels being subject to removal by online service providers. In September 2023, DVE Threat Actor #1 notified its followers on Telegram that its main page on the platform had been removed and that it intended to move the bulk of its activity away from the surface web. DVE Threat Actor #1 also very likely prefers hosting its doxing infrastructure on dark web platforms because it believes doing so helps it establish *bona fides* in cyber and operational security with other DVEs. The administrator(s) very likely intended to signal their knowledge of cyber tradecraft to assist in achieving their stated mission of being a trusted source of information about cybersecurity best practices for their ideological sympathizers.

In previous doxes, DVE Threat Actor #1 has experimented with other dark web infrastructure for publishing dox files. A September 2023 dox of an antifascist activist was hosted on a Zerobin page with a .onion TLD. The Telegram channel has also shared links to .zip files that were hosted on a FileDump site. DVE Threat Actor #1 has also used Stronghold Paste, a paste site with a .onion TLD, to host dox files, most notably in an August 2023 dox of an individual who was the Chief Executive Officer (CEO) of a research organization and a well-known investigator of US DVE groups.

Dox #2: Anarchist Threat Actor Targets Mayoral Advisory Council

In September 2023, DVE Threat Actor #2 doxed Victims #2-35 — 34 senior executives and leaders of major companies and educational institutions. In a communique, DVE Threat Actor #2 stated it doxed these individuals because they served on an advisory council to the mayor of Atlanta, Georgia, and because they represented what DVE Threat Actor #2 perceived as corrupt corporate interests in Atlanta's local government. The communique included full home addresses for 30 of the individuals on the list and partial home addresses for four individuals, which DVE Threat Actor #2 very likely obtained through data on county assessor sites. They published this communique on a "counter-information" website used by AVEs to post claims of responsibility for attacks, attack manuals, and doxes.

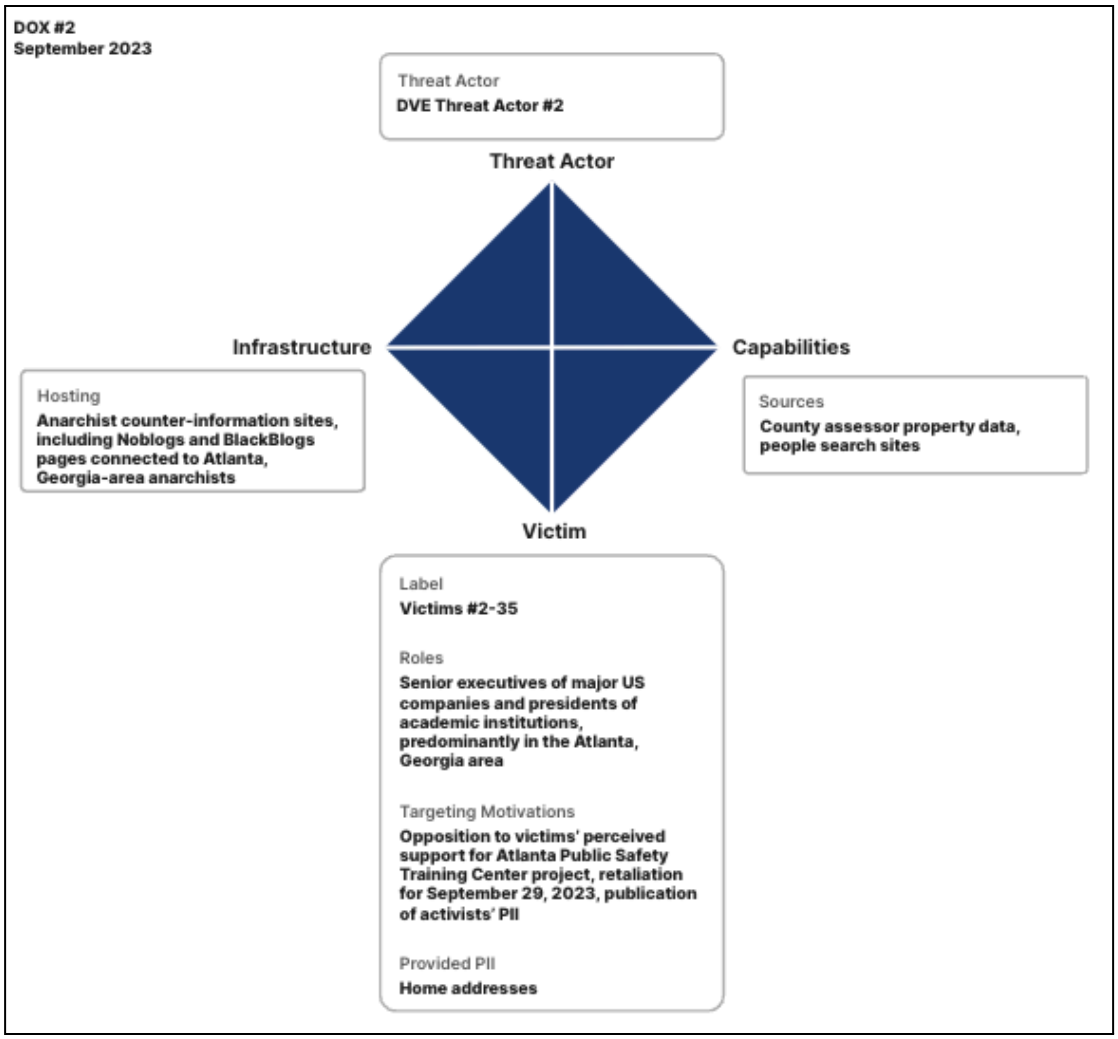


Figure 3: *Diamond model analysis of Dox #2 (Source: Recorded Future)*

DVE Threat Actor #2

DVE Threat Actor #2 is very unlikely to be an established, formalized organization or group of threat actors. DVE Threat Actor #2's unique pen name, doxing targets, and hosting of communications on a website connected to anarchist movements in the greater Atlanta area all suggest that DVE Threat Actor #2 is based in Atlanta.

DVE Threat Actor #2 is almost certainly a participant in an ongoing anarchist campaign against the construction of the Atlanta Public Safety Training Center (APSTC), colloquially known as "Cop City". Resultant protest movements against the center — referred to as "Stop Cop City" or "Defend the Atlanta Forest" — began in 2021, when Atlanta's mayor announced the selection of a site in the South River Forest as the location for the facility. Protests at the site have escalated into violence between AVE demonstrators and police, local law enforcement has charged several dozen violent protesters with state-level domestic terrorism offenses, and AVE groups across the US and the world have mobilized in

solidarity with the “Stop Cop City” movement. On August 29, 2023, the state of Georgia charged over 60 alleged “militant anarchists'' with violations of the state’s Racketeer Influenced and Corrupt Organizations Act (RICO), arguing that the Defend the Atlanta Forest movement constituted an organized conspiracy to perpetrate violent acts against the APSTC.

Activists have also organized other measures to stall construction of the APSTC, including gathering over 116,000 signatures from Atlanta residents to force a referendum on the facility. On September 29, 2023, the Atlanta Municipal Clerk’s office posted a list of all signatories to the referendum, including their names, addresses, and phone numbers, but redacting other PII. The title of DVE Threat Actor #2’s communique and the communique’s arguments indicate that the Atlanta Municipal Clerk’s posting of referendum signatories almost certainly prompted DVE Threat Actor #2’s dox of Victims #2-35 as a retributive act.

Since June 2023, DVE Threat Actor #2 has posted at least five dox files targeting government, law enforcement, and business leaders that the threat actor believes are supporting the APSTC project, totaling over 100 victims. The threat actor has compiled each dox into a single .pdf file available on the same websites hosting the doxes. The file includes addresses for members of several civic councils and local government officials in Atlanta.

Targets (Victims #2-35)

Dox #2 targeted Victims #2-35 — a total of 34 executives of major American companies and academic institutions. All 34 victims were targeted because they serve on a mayoral advisory committee that allows Atlanta’s mayor to consult with senior business, academic, civic, and philanthropic leaders in the Atlanta area. In a communique, DVE Threat Actor #2 claims to have doxed members of this committee due to their perceived influence on the mayor’s office, and that pressure and exposure may coerce them into persuading the mayor to stop the APSTC project.

Victims #2-35 include C-suite executives of companies in twenty different industry sectors and presidents of six higher education institutions. 21 have listed Atlanta, Georgia, addresses; ten have addresses elsewhere in the state of Georgia; and three have addresses outside of Georgia. Notably, the accuracy of the provided addresses for Victims #2-35 significantly decreases when they do not have a listed Georgia address: the dox file does not provide a full address for any of the victims who live outside of Georgia. This supports the theory (described below) that the threat actor primarily relied on county assessor data to dox Victims #2-35.

Capabilities

DVE Threat Actor #2 very likely relied on data available through county assessor sites — especially the Fulton County Board of Assessors — to find information on Victims #2-35. They likely began their investigation through queries of county assessor property data sites and then supplemented this information through people search websites and other open sources. DVE Threat Actor #2 likely relied more on these secondary sources to dox victims without a Fulton County address. This judgment is predicated on three factors:

- All listed addresses for Fulton County residents who are not university presidents (who typically reside in a specific residence designated for the president on campus) are identically formatted to records that appear on the Fulton County Board of Assessors site.
- All but one listed address for non-Fulton County residents of Georgia are identically formatted to records that appear on people search websites.
- All listed addresses for non-Georgia residents refer to places of residence using vague terms (for example, "somewhere in" a major metropolitan area).

The only information about Victims #2-35 published in the dox file are their names, titles, companies, and assessed places of residence. Due to the large number of victims in the dox file, we selected ten of the 34 victims of this dox as a sample for our own investigation, aiming for a diversity of targets to establish the threat actor's doxing TTPs. The sample (Victims #2-11) is broadly representative of the population's residence — six of the ten are Fulton County residents, three are residents of other counties in Georgia, and one does not have a listed Georgia address.

Insikt Group queried the six Fulton County victims (Victims #2-7) in the sample on the Fulton County Board of Assessors' website as well as on people search tools. Data from Dox #2 directly corresponds to addresses listed in the Fulton County database, even following their exact formatting with capitalized addresses and standardized street type abbreviations (for instance, ST for street, DR for drive, and so on). Data on people search websites are typically formatted differently: street names are typically not capitalized, and sites follow different abbreviation types for listing street types. In addition, queries for four of the six Fulton County victims and reverse address searches for their properties on people search websites did not yield any data, likely indicating that these victims requested the removal of their PII from these sites.

For non-Fulton County residents of Georgia (Victims #8-10), we queried respective assessor websites in their counties of residence and people search tools. Data in the dox file for two of these victims matched county assessor information and formatting, while data for one victim (Victim #9) resembled data that appears on a people search website. Notably, Victim #9's address is not in the immediate Atlanta metropolitan area, unlike Victims #8 and #10. While we found a record matching Victim #9 in their county's assessor data, the formatting on that site does not match the record that appears in the dox. This likely suggests that DVE Threat Actor #2 relied on people search tools rather than assessor data for this victim.

DVE Threat Actor #2 did not provide a specific street address for Victim #11, who lives outside of Georgia. They assess that Victim #11 lives "somewhere in" a large metropolitan area outside of the state, similar to the listed addresses for three other victims in the broader dataset — two of whom also live outside of Georgia.

Infrastructure

Dox #2 was initially posted in September 2023, on an anarchist counter-information website. The website, hosted on the "non commercial, antifascist, antisexist, privacy-oriented blog platform" Noblogs, publishes information about anarchist protests, claims of responsibility for attacks by AVE groups, guides for conducting attacks, and communiques from anarchist groups around the world, with a particular focus on AVE activities in the Atlanta area.[6]

The initial post no longer appears on the counter-information site on which it first appeared. It was almost certainly removed due to a complaint that its administrators received from Noblogs. In October 2023, the website's administrators claimed they were removing all PII that appeared on the website due to a notification from Noblogs that the website was violating its terms of service related to doxing. The administrators thereafter created another counter-information website on a similar blog platform, BlackBlogs, that does not prohibit doxing. The site's subtitle claims its purpose is publishing information that would violate NoBlogs' ToS. All of DVE Threat Actor #2's doxes that initially appeared on the Noblogs site — including its September 2023, dox of the Victims #2-35 — were reposted on its BlackBlogs site. Dox #2 has also been distributed on other anarchist counter-information sites, including on one prominent website where it has accrued over 2,100 views since its publication.

Dox #3: White Supremacist Targets Executive and Family Over Advertising Campaign

In April 2023, DVE Threat Actor #3 doxed Victim #36, a senior executive of a major US company, and three members of the senior executive's family (Victims #37-39). In the dox file, "DVE Threat Actor #3" referred to Victim #36 using slurs for Jewish people and transgender individuals and indicated the victims were doxed because of their company's advertising campaign. The dox file lists Victim #36's addresses and phone number as well as the addresses and phone numbers of three of Victim #36's family members. This information was almost certainly obtained through people search websites.

[6] *noblogs[.]org*

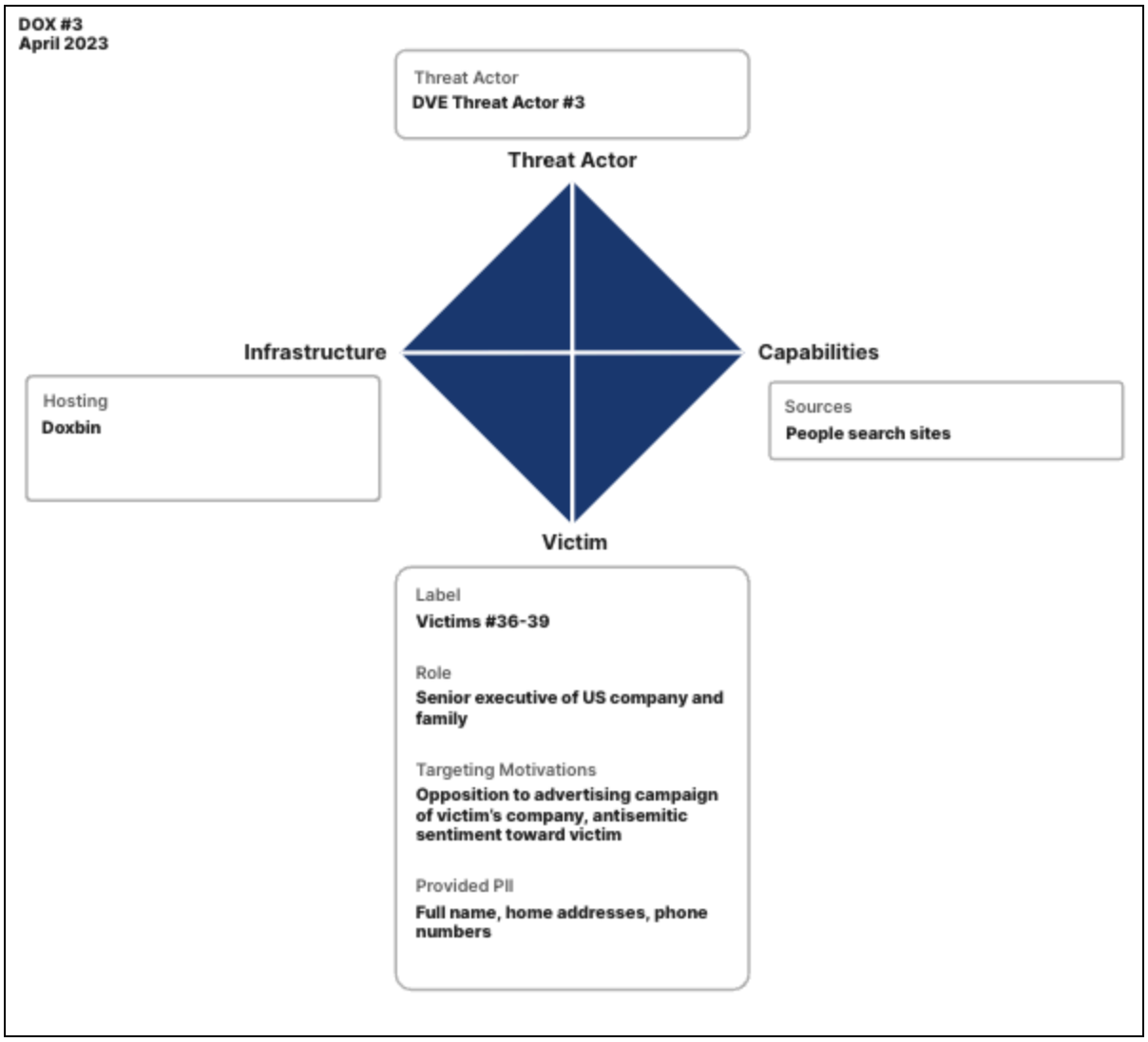


Figure 4: *Diamond model analysis of Dox #3 (Source: Recorded Future)*

DVE Threat Actor #3

DVE Threat Actor #3 is a prolific user of the doxing paste site Doxbin and, at the time of writing, has posted 188 dox files on the site since first becoming active in March 2023. DVE Threat Actor #3 frequently doxes journalists, celebrities, public figures, law enforcement, federal government officials, and members of the Jewish community.

Information from DVE Threat Actor #3's dox of Victim #36 and other doxes suggest that the threat actor follows the Goyim Defense League (GDL), a South Florida-based DVE group that is known for distributing antisemitic flyers and conducting online harassment campaigns against Jewish communities and organizations in the US. In April 2023, the GDL's founder, Jon Minadeo (also known as HandsomeTruth), posted a video of Victim #36 on his Gab channel, referring to the victim using slurs for Jewish people and transgender individuals. This same phrase appeared nearly verbatim, with a link to HandsomeTruth's Gab post, in DVE Threat Actor #3's dox file of Victim #36 on Doxbin.

DVE Threat Actor #3's threat actor profile differs from other DVE threat actors covered in this report. While DVE Threat Actor #3 frequently follows calls by DVE groups to dox individuals and use slurs and other terminology consistent with specific DVE movements, not all of the threat actor's targets are persons of interest for DVE groups; DVE Threat Actor #3 also refers to doxing as a "hobby" in multiple online posts. While certain targets — including Victim #36 — were almost certainly doxed in furtherance of a DVE ideological cause, others were very likely doxed due to the threat actor's personal grievances or other motivations.

Target (Victims #36-39)

Dox #3 targeted Victim #36, a senior executive in a major US company, and the victim's family (Victims #37-39). In April 2023, Victim #36's company launched a new advertising campaign. The campaign was controversial, and, in its wake, political activists, online influencers, and other groups opposed to the decision promoted a boycott of Victim #36's company. A significant portion of the online criticism was directed toward Victim #36, who observers believed was the executive responsible for the advertising campaign.

Among the groups that targeted Victim #36 and the individual's company during the boycott were DVEs. Victim #36, in conjunction with doxing attempts, reportedly received online death threats. White supremacist and neo-Nazi violent extremists, including HandsomeTruth and the GDL, almost certainly operated under the belief that Victim #36 was Jewish. HandsomeTruth's Gab post and DVE Threat Actor #3's dox of Victim #36 both place Victim #36's name within triple parentheses — a symbol commonly used by white supremacists and neo-Nazis to signal that they believe an individual is Jewish. Both posts also refer to Victim #36 using a slur for Jewish people.

In addition to Victim #36, DVE Threat Actor #3 has posted two other dox files targeting members of Victim #36's company. In April 2023, DVE Threat Actor #3 doxed a figure in the company's advertising campaign and their family. In June 2023, DVE Threat Actor #3 doxed five additional executives of Victim #36's company and its parent company, as well as their respective family members. The data in this dox file resembles the dox of Victim #36 and provides home addresses and phone numbers that were almost certainly obtained from people search websites. At the top of the file, however, DVE Threat Actor #3 directs users to their dox of Victim #36 with a link to the victim's file, noting that Victim #36 was the executive responsible for approving the advertising campaign.

Capabilities

DVE Threat Actor #3 is a persistent doxing threat actor but is very unlikely to be a technically sophisticated threat actor based on the contents of DVE Threat Actor #3's dox files and own admissions. The data in the threat actor's dox files is almost exclusively sourced from people search websites, and in a July 2023 dox, DVE Threat Actor #3 admits that everything in these doxes is "public info" and that it "did not take much skill" to dox targets according to DVE Threat Actor #3's method. Other Doxbin users frequently comment on DVE Threat Actor #3's dox files that they were able to

independently obtain the same information in the file through simple searches on people search websites.

In total, the dox file on Victim #36 lists the victim's full name, two addresses, and a phone number, as well as addresses and phone numbers for three members of the victim's family. Insikt Group queried several people search websites using the information in DVE Threat Actor #3's dox file to determine the source(s) of the data. Notably, searches for Victim #36's name and state of residence did not yield any results on several of these sites, likely indicating that Victim #36 or Victim #36's company requested the removal of PII from relevant online sources. We found two records that almost certainly match an address that DVE Threat Actor #3 attributed to Victim #36 on two people search websites, but these are partial records and unlikely to be the source of DVE Threat Actor #3' dox.

Records matching the information that DVE Threat Actor #3 provided for Victims #37-39, however, remain available on a number of people search websites. The three family members in DVE Threat Actor #3's dox are listed as known associates of one another by these sites, but the sites do not list Victim #36 or provide a link to Victim #36's records. This likely demonstrates that Victim #36 requested the removal of PII from relevant online sources. If Victim #36 did remove PII from such sites, the process likely would have focused on removing Victim #36's data from the internet following the April 2023 backlash to the victim's company and the executive but neglected to remove data for Victims #37-39. Threat actors, including DVEs, frequently dox targets' family members to threaten their target by proxy. A threat actor seeking to physically approach or harm a doxed target is likely to investigate further to establish a pattern of life, including monitoring family members to determine whether the target frequently spends time with or cohabitates with a particular person.

Infrastructure

The only known instance of Dox #3 appears on Doxbin's main clear net website. There are no results in the Recorded Future Intelligence Cloud or through other searches of this dox file appearing in other infrastructure, and we were unable to attribute doxing activity on other websites to DVE Threat Actor #3. The Dox #3 file is DVE Threat Actor #3's most-viewed post on Doxbin, with over 1,400 views at the time of writing.

Doxbin's clear net website is distinct from a site with the same name and function that operated using a .onion domain between 2011 and 2014 and was taken down by Operation Onymous, a multinational law enforcement operation targeting illegal activities on the Tor network. As the name suggests, Doxbin is "a document sharing and publishing website for text-based information such as dox, code-snippets, etc, you know the drill, feel free to paste whatever you want", according to its administrator. A WHOIS search for the site's domain indicates it was registered on December 30, 2010, by NiceNIC International Group Co., Limited, a Hong Kong-based hosting and server provider, and is registered to BPW, a company in the Tambov region of the Russian Federation. Doxbin also operates multiple additional clear net domains, as well as a Telegram channel. Its administrators have almost certainly hosted the site on other domains, including on .onion TLDs, due to frequent site takedowns by hosting providers.

DVEs have previously used Doxbin to coordinate doxing, swatting, and other physical threats, and the US Department of Justice claims that at least one former Doxbin administrator was a prominent member of a DVE organization. Between October 2018 and February 2019, five members of the neo-Nazi accelerationist organization Atomwaffen Division (AWD) swatted over 130 locations, targeting government officials — including a US Cabinet member — business executives, and members of the media. According to a government sentencing memorandum for John William Kirby Kelley, one of the co-conspirators, around October 2018, the group began maintaining Doxbin and using the site to conduct doxing and swatting, "placing a gun symbol next to the name of a person to indicate that the individual had been swatted". One of the other co-conspirators was John Cameron Denton, a senior AWD leader.

Mitigations

Aside from opposing DVEs and political activists, high-visibility public and private sector leadership — including senior local, state, and federal government officials, C-suite company executives, and the presidents of academic and non-governmental organizations — are the most likely targets of DVE doxing attempts. To reduce the risk of being doxed, senior leaders who believe they may be targeted should adopt strong cyber hygiene measures. Additionally, senior leaders and executive protection teams should develop response plans in the event that they are doxed to manage follow-on risks.

To reduce the risk of doxing, potential targets should:

- Routinely review and update their online footprint. One particularly helpful method to inform these reviews is a red team exercise, in which individuals attempt to dox themselves or request a trusted third party to dox them; Recorded Future's Analyst on Demand service offers Executive OSINT Investigations for this purpose. Executives can also monitor these threats via the Recorded Future Intelligence Cloud and enable credit monitoring services to ascertain whether their PII is available in data breaches. These steps can reveal what sources of PII a threat actor can leverage and assist in filing removal requests.
- Request removal of personal information — as well as information about family — from people search websites. For a fee, individuals can use a tool like DeleteMe or ReputationDefender; free guidebooks and other resources for sending individual removal requests to people search websites are also available.
- Exercise caution about sharing personal information in open forums. This includes being circumspect about sharing information on the internet and social media, as well as in media interviews, conference presentations, and other open forums where sharing information that could help a threat actor corroborate PII is nonessential.
- Utilize trusted third parties — such as attorneys and limited liability corporations — to conduct real estate transactions to avoid publication of PII in county assessor data.
- Adopt standard personal cybersecurity best practices — including the use of strong and unique passwords, pseudonymous user names on online accounts, and a virtual private network (VPN).

- Develop a doxing response plan. In the event that an individual is successfully doxed, the victim, executive protection team, organization, or company can take action to mitigate potential harm by employing the recommendations below.
- Ensure that cyber hygiene best practices are adopted by the families of officials, executives, or other individuals that may be doxed, for example, by restricting publicly viewable information on social media accounts. Threat actors, including DVEs, are likely to target the families of victims as a proxy. Even if a target has a relatively limited online footprint and employs measures to protect PII, threat actors can leverage data on the target's family to triangulate information about the target.

If you — or executives or officials at your company or organization — are successfully doxed:

- Notify law enforcement if you believe you are in immediate danger or have information about a specific, credible threat attached to the dox.
- Document the dox by collecting a stable copy of the dox file and archiving the information, particularly if you believe that there is a specific, credible threat or evidence of illegal activity.
- Take stock of what PII was included in the dox and use it to conduct a thorough risk assessment. For instance, a threat actor with access to an individual's home address likely increases the victim's personal risk from harassment, stalking, swatting, and physical attacks.
- Report instances of the dox file to the online platforms where it has been posted and request its removal. On most websites — including clear net paste sites like Pastebin and most social media sites — doxing constitutes a ToS violation.
- Contact Google and other search engines to request the removal of PII from search results.

Outlook

While most DVE doxing attempts will almost certainly continue to target members of opposing DVE groups and political activists, DVEs are also almost certain to dox government officials, senior business executives, activists, community leaders, and other visible public figures. By doxing victims, threat actors are almost certainly enabling other DVEs to threaten, harass, stalk, protest against, surveil, approach, or attack the victim. Even if doxes do not explicitly state these threats, DVEs almost certainly intend doxes to be interpreted as implicitly threatening. An individual who is doxed by a DVE threat actor is likely at increased risk of physical threat activity from DVE actors of the same ideological background. The availability of PII about a prominent individual online also likely enables cyber threats, such as the use of personal information for spear-phishing lures, social engineering, account takeover, and digital extortion.

Based on our review of DVE doxing activity, high-profile organizational decisions and reactions to domestic political or geopolitical events are likely to increase doxing risks for public and private sector leadership. Evidence of significant negative sentiment in DVE sources directed toward an individual, agency, company, or organization likely increases the risk of DVEs doxing victims associated with those entities. For local, state, and federal government officials, DVEs are especially likely to dox public sector targets due to their opposition to adopted or proposed policy initiatives, law enforcement operations

against DVEs, or other concerns specific to the DVE ideology in question — such as perceived governmental overreach or racial animus. In contrast, DVEs are most likely to target private sector leadership following controversial business decisions, such as advertising campaigns, relationships between companies and governments, or companies' public displays of support for a political, social, or ideological cause.

In the near- to mid-term, several emerging geopolitical events and business trends are likely to drive efforts by DVEs to dox public and private sector leadership. For instance, DVEs dissatisfied with government and business stances on the Israel-Hamas conflict have already doxed the senior leadership of several prominent cleared defense contractors and are likely to expand their aperture for doxing business leaders as the conflict continues. The forthcoming 2024 US presidential election is also very likely to yield increased DVE doxing activities, particularly targeting candidates, political activists, and election personnel. Finally, as private sector entities more publicly act on social justice issues, develop diversity, equity, and inclusion policies, and make public statements supporting the rights of racial and religious minorities and the LGBTQ+ community, DVEs opposed to these trends may become increasingly likely to dox these companies' senior leadership.

Recorded Future®

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 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com